



وزارة التعليم العالي والبحث العلمي

الجامعة المستنصرية / كلية التربية



وقائع

المؤتمر العلمي التخصصي الثالث والعشرين

تحت شعار

الرياضيات والحاسبات مرآة

للتنمية والتطور

26-27 نيسان 2017

عدد خاص - المجلد (2)

مجلة كلية التربية

مجلة - متخصصة - محكمة
تصدرها كلية التربية / الجامعة المستنصرية



سعر النسخة الواحدة

داخل البلد : (١٢,٥٠٠) اثنا عشر ألفاً وخمسمئة دينار عراقي
خارج البلد : (٦٠ \$) ستون دولاراً

الاشتراك السنوي

داخل البلد : (٨٥٠٠٠) خمسة وثمانون ألف دينار عراقي
خارج البلد : (٥٥٠ \$) خمسمئة وخمسون دولاراً

الاسم :-

العنوان :-

يكتب الصك باسم مجلة كلية التربية / الجامعة المستنصرية

العنوان البريدي :- الجامعة المستنصرية / كلية التربية

مجلة كلية التربية

مكتب بريد الجامعة المستنصرية

ص.ب ٤٦٢١٩

اللجنة التحضيرية

أ. م. د. د. احمد شيال غضيب/ عميد كلية	(رئيساً)
أ. د. رياض فاخر حميد/ معاون العميد للشؤون العلمية والدراسات العليا	(عضواً)
أ. م. د. د. عبد الجليل مزعل بنيان/ معاون العميد للشؤون الإداري	(عضواً)
م. د. قاسم خليف عمار/ معاون العميد لشؤون الطلبة	(عضواً)
أ. م. د. د. سمير قاسم حسن/ رئيس قسم الرياضيات	(عضواً)
أ. م. د. د. عماد عيسى عبد الكريم/ رئيس قسم علوم الحاسبات	(عضواً)
أ. د. د. زياد محمد عبود/ قسم الفيزياء	(عضواً)

اللجنة العلمية

أ. د. صلاح حمزة عبد/ قسم الرياضيات	(رئيساً)
أ. م. د. د. منير عبد الخالق عزيز/ قسم الرياضيات	(عضواً)
أ. م. د. د. صلاح مهدي صالح/ قسم الرياضيات	(عضواً)
أ. م. د. د. سعد شاكر محمود/ قسم الرياضيات	(عضواً)
أ. م. د. د. عماد عيسى عبد الكريم/ قسم علوم الحاسبات	(عضواً)
أ. م. د. د. سعد عبدالرضا مكي/ قسم علوم الحاسبات	(عضواً)
أ. م. د. د. عبد الوهاب سامي إبراهيم/ قسم الحاسبات	(عضواً)
أ. م. د. د. خالد علي حسين/ قسم علوم الحاسبات	(عضواً)

محاور قسم الرياضيات

- (1) الرياضيات الصرفة Pure Mathematics
- (2) الرياضيات التطبيقية Applied Mathematics
- (3) الإحصاء والمعدولية Statistics and Reliability
- (4) بحوث عمليات Operation Research

محاور علوم الحاسوب

- 1) Mobile and Multimedia Networks
- 2) Computer Vision and Pattern Recognition
- 3) Artificial Intelligence and Robotics System
- 4) Information Security
- 5) Network Security
- 6) Soft Computing
- 7) Cloud Computing
- 8) Data Mining
- 9) Digital Forensics
- 10) Internet of Things

توصيات المؤتمر الثالث والعشرون للرياضيات والحاسبات 26-27-2017 / محور الرياضيات

١. التأكيد على البحوث في الجانب التطبيقي والتي تحقق متطلبات سوق العمل.
٢. مفاتحة المؤسسات والدوائر والقطاع الخاص للحصول على مشاكل بحثية لتكون النواة لعمل البحوث في المؤتمرات على سبيل المكاتب الاستشارية.
٣. دعم البحوث العلمية من خلال تخصيص موازنة خاصة من قبل الجامعة او الكلية لدعم البحث العلمي.
٤. تحديث قاعدة بيانات خاصة بتدريسي الرياضيات واختصاصاتهم لغرض الاستفادة منها في التقييم والمناقشات وامور اخرى.
٥. التشجيع على فريق العمل في انجاز البحوث التي تعالج مشاكل الواقع حتى لا يصبح خمول وتترف في البحث العلمي.
٦. دعوة الباحثين الخارجيين من انحاء العالم وحثهم على المشاركة في المؤتمرات المحلية وذلك لدعم الباحثين العراقيين في لقاء بحوثهم امام باحثين اجانب وعرب.
٧. انشاء مؤتمرات من خلال التنسيق مع مؤسسات نشر عالمية للنشر فيها وذات معامل تأثير عالي.
٨. تحديث المناهج وبما يتناسب مع المستوى البحثي وسوق العمل في العراق.
٩. تعيين مساعد رياضيات ومن ثم باحث رياضيات كدرجه وظيفيه في الوحدات العلمية.
١٠. انشاء بحوث مشتركة تطبيقية بين قسمي الرياضيات والحاسبات بما يتطلبه سوق العمل.

توصيات المؤتمر العلمي لكلية التربية الثالثة والعشرون (مؤتمر الرياضيات والحاسبات) / محور الحاسبات

١. تناول محاور أخرى بالإضافة إلى التي تناولها المؤتمر وهي التجارة الإلكترونية وأنظمة محاكاة التطبيقات والتجارب العلمية والروبوت وغيرها من فروع علوم الحاسوب.
٢. بناء صناعة برمجية وطنية رصينة وتقليل الاعتماد على المستورد بالتعاون ما بين الجامعة والمجتمع بالاعتماد على قدرات الاساتذة والطلبة المبدعين في هذا المجال .
٣. توحيد أنظمة قواعد البيانات على مستوى بيانات ومعلومات وزارة التعليم العالي والبحث العلمي وربطها بشبكات إتصالات داخلية أو مفتوحة بتحويل حسب مستويات المستفيدين لمواكبة التطور الحاصل بالمنطقة
٤. بناء أنظمة خبيرة صناعية وطبية وتعليمية مبنية على حاجة المجتمع وبالتعاون مع الوزارت ذات العلاقة كوزارة الصحة ووزارة الصناعة .
٥. دعم وسائل حماية البيانات والمعلومات وبناء برامجيات منع الفيروسات والقرصنة المعلوماتية.
٦. زيادة الاعتماد على أنظمة التشغيل كنظام MAC TECHNOLOGY نظام مشروع قانوناً ويتمتع بحماية امنية جيدة تتجاوز الاستخدام الغير قانوني للبرامجيات الجاهزة من إنتاج الشركات العالمية.
٧. إستحداث فروع في أقسام علوم الحاسوب في تخصص شبكات الحاسوب تتناول كافة تفاصيل هذا التخصص للحاجات الماسة والمتنامية بسرعة كبيرة على مستوى العالم.
٨. تشجيع التعليم الإلكتروني وأساليبه ووسائله للإرتقاء به كوسيلة تعليمية ذاتية تعزز وتساند التعليم المباشر (التقليدي) وليس بديلاً عنه.
٩. تكرار عقد مؤتمرات تخصصية لعلوم الحاسوب على غرار هذا المؤتمر وبشكل دوري سنوي أو كل سنتين لمواكبة التقدم العلمي ولتهيئة الفرصة إلى باحثينا وملاكنا التدريسي للبحث والدراسة.
١٠. الإهتمام بالدراسات العليا واعتماد مبدأ التخصصات الدقيقة لمواكبة التطور العلمي.
١١. التأكيد على حوسبة ومكننة كافة الأعمال الإدارية وبناء قاعدة إلكترونية تمهد لتأسيس الحكومة الإلكترونية على مستوى الجامعة والكلية.

المحتوى (المجلد الثاني)

بحوث محور علوم الحاسبات		
730	Image Steganography Using Modified RSA and Moore Neighbor Tracing Dr. Saad Abdual Azize Sana Ahmed Kadhom	.84
737	Using the principle of definite double integral in cryptography Basim Najm Al-Din Abed	.85
746	Proposal of Enhancement the LOKI97 Algorithm Assist. Prof. Dr. Alaa Kadhim Shahad Husham	.86
755	New Block Cipher Algorithm Depend on Hybrid Operation Assist. Prof. Dr. Alaa Kadhim Ghadah Ali	.87
764	Chaos and OcTree based for Multiple Image Encryption Jolan Rokan Naif Shymaa Mohammed Jameel	.88
770	Image in Image Hiding Using Wavelet Transform Iman M. G. Alwan Enas Muzaffer Jamel	.89
781	Fingerprint Encryption Based on Feature Extraction QR Code Ali Hussein Fadhil Raniah Ali Mustafa	.90
795	AES Cipher Key Generation Based on Exponential Chaotic System Ahmed Kareem Shibeeb Mohammed Hussein Ahmed	.91
803	Cipher Text Hiding in Image Based on new Generation Key Method of 3DES Algorithm Zainab khyioon Abdalrdha Zahraa Salah Dhaief Hashem B. Jehlol	.92
814	Image Encryption Using 3D-CHEN's Map and 3D-Henon Map for Secure Transmission Dr. Abdul-Wahab Sami Ibrahim Majed Ismael Sameer	.93
823	A New Approach of Color Image Encryption Based on RC4 algorithm and Chaotic Map Dr. Abdul-Wahab Sami Ibrahim Majed Ismael Sameer	.94
834	Cloud Security Implementation by a Chaotic Key and XOR Israa M. Abdalameer Al-Khafaji	.95
837	Enhanced Color Plane Permutation for Satellite Imagery Encryption Fadhil Hanoon Abbood Rana Saad Mohammed Intisar Abid Yousif	.96
844	A New Algorithm for Image Encryption Based on A New Hyper Chaotic system Asst. Prof. Dr. Sadiq A. Mehdi Hayder A. Qasim	.97
853	Design System to Perform and Measures Stream Cipher Algorithms Prof. Dr. Salim Ali Abbas Ali Jumaa Hashim	.98
861	Use PSO and IPSO in Cryptanalysis: Comparative Study Riyam N. J Kadhum Prof. Dr. Salim Ali Abbas	.99
871	A New Image Cipher Method Based on some Statistical Properties Dr. Anwar Abbas Hattab Maha Ali Hussian	.100
879	A Novel Block Audio Encryption Algorithm Based on 2D Standard map and 2D Baker map Dr. Ekhlas Abass Albahrani Dr. Sawsen Abdulhadi Mahmood	.101

888	Data Security in Cloud Computing Architecture Based on Modified AES Asst. Lecturer Amal Abdulbaqi Maryoosh	.102
896	Proposed E-mail system based on multi-chaos maps Dr. Haider K. Hoomod Arkan Mohammed Radi	.103
904	Image Denoising Based on Modify Radial Basis Function Neural Network and Noise Estimation Level Dr. Haider K. Hoomod Saja Hikmat Dawood	.104
913	Region of Interest Detection Using Scale Invariant Feature Transform Dr. Ekhlal Khalaf Gbashi1 Suha Mohammad Saleh	.105
923	A Comparative Study between BM25 and TF-IDF for Feature Extraction on Twitter Ammar Ismael Kadhim, Yu-N Cheah, Baydaa Jaffar Al-Khafaji, Salah Talib	.106
929	New approach to image encryption depend on substitutions operation and DNA computing Assist. Prof. Dr. Matheel Emadaldeen Zena Mohammad Saadi	.107
938	Verification Consistency Based Multi-Focus Image Fusion Using Berkeley Wavelet Transform Iman M. G. Alwan	.108
945	التعرف على الوجوه أ.م. د. رحاب فليح حسن سري رحيم عيدان	.109
958	Detection Citrus Aurantium Musty Using First Order Statistics Feature Assist. Prof. Amel H. Abbas Marwa A. Shamel	.110
966	Edge Detection of Ear Image Based on Canny Method Prof. Dr. Jamila Harbi S Sara Salman	.111
973	Vertex Neighborhood Detection Based on Connectivity Information Sawsen Abdulhadi Mahmood Amal Abbas Kadhim Lamyaa Mohammed Kadhim Sally Ali Abdu Lateef	.112
978	Fuzzy - Lagrange Techniques With Slantlet Transform For Image De-blurring Ahmed Othman Khalaf Waleed Rasheed Humood Shaimaa Khudhair Salih	.113
988	The K-SVD Algorithm for Image Denoising Depending on Weighted Median Filter with Slantlet Transform Ahmed Othman Khalaf Waleed Rasheed Humood Shaimaa Khudhair Salih	.114
994	Impact of computer applications in construction industry of Iraq Dr. Hassan Issa Abdul-Kareem	.115
999	An Efficient Data Reduction Technique for Image By Using Multiwavelet and Run Length Encoder Elham Fadel Aqeel	.116
1007	Image Dehazing using modified fast visibility restoration with HSV color space Hazim G. Daway Hana H. Kreem Haitham S. Chyed Dhuha A. Abdulabbas	.117
1016	تحسين إضاءة وتباين الصورة الطبية بواسطة معادلات عددية أ. د. زياد محمد عبود م. م. فلاح عابر بيده	.118
1027	Color Image Enhancement For The Objects Immersed in Turbid Water Using Adaptive Retinex Algorithm Based on Gamma Correction Fatima I. Abbas Ali Abid D. Al-Zuky Hazim G. Dway Radhi Sh. Al-Taweel	.119

1044	Modification CB (Center-to-Boundary) Filter to Remove Noises in Color Images Based on Parallel Hybrid Algorithm Khalid Ali Hussein Abed Ali H. Altaee Haider K. Hoomod	.120
1053	Iris Recognition Based on fusion of Multi-features Rafid. E. Haleot Kawther. T. Saleh Raniah Ali Mustafa Haitham S. Chyad	.121
1061	Enhancement Human Face Recognition Based on Fusing of Infrared and Visible Images Ziad M. Abood Ghada S. Karam Rafid. E. Haleot	.122
1069	Categorization Quranic Text Using NB algorithm Geehan Sabah Hassan Faris Mahdi	.123
1074	New Facial Imprint Detection Algorithm Based on Ycbr Model and Ant Colony Dina Riadh Alshibani Samar Amil Kassir	.124
1082	Modify Multi-Connect Architecture (MMCA) Associative Memory Rusul Hussein Hasan Emad I. Abdul Kareem	.125
1096	Must Frequency Frequent pattern-Tree Algorithm for Mining Association Rules Enas Mohammed Hussien Media Noaman Solagh	.126
1104	Stream Data Classification Using Various Mining Algorithms Enas Mohammed Hussein Hind Raad Ibrahim	.127
1110	Skin Cancer Detection Using Artificial Neural Network Iman Hussein AL-Qinani Mushtaq Talib Ajjah Mustafa H. Ali	.128
1120	Iris Recognition Using Neural Network Assist. Prof. Safana Hyder Abbas Eman Abdulmunem	.129
1126	Master Eye Region Based on Multiwavelet Transform Using Association Rules Raniah Ali Mustafa Zahraa Salah Dhaief	.130
1140	الخوارزميات الجينية ومعايير الضبط المثلى للأداء المنفصل جنان رضا مطر	.131
1151	Braille character recognition using Modify Bidirectional Associative Memory (MBAM) Assist. Prof. Safana H. Abbas	.132
1159	Archaeology Areas Selecting independent of GIS with Fuzzy logic Samira A. Hussain Sundos A. Hameed Al-Azawi Muna Jaffer	.133
1165	Modulation and Energy Components for Speaker Recognition System Tariq A. Hassan Ammar M. Kamel	.134
1174	Design Concept of Vehicle Alarming System using Smartphone Sensors and Bluetooth Technology Dr. Eng. Asst. Prof. Saad A. Makki	.135
1183	A Review of Personalization Techniques for Recommender Systems Asst. Prof. Dr. Ahmed Hashim Mohammed Ahmed Rashid Abdullah	.136
1190	Cloud Based Iraqi E-Government Rawaa M. Abdulhussein Asst. Prof. Dr. Ahmed H. Mohammed	.137
1197	A Review on Fog Computing and Quality of Services (QoS) Ammar Abdulateef Hadi	.138



Image Steganography Using Modified RSA and Moore Neighbor Tracing

Associate Prof Dr. Saad Abdul Azize

Sana Ahmed Kadhom

Al_Mamon University College, Baghdad, Iraq

saadabdualazize@yahoo.com

sana_ahmed73@yahoo.com

Abstract:

Due to the extreme expansion in internet and data communication, security became an essential problem that must be considered in any transmission process, especially if the transmitted data meant to be secured. In this research an improved crypto method is used. Data to be hidden is encrypted using modified RSA, then the encrypted data will be hidden within an object's boundaries in a covered image, the boundaries determined using Moore neighbored method. The proposed method was tested by PSNR was greater than 70%, MSE was less than 10^{-3} , and correlation was close to 1.

Keywords: steganography, public key cryptosystem, Moore neighbored boundary search.

اخفاء بيانات في صورة باستخدام طريقة مطورة من RSA مع طريقة "موور" لتتبع المجاور

م. سناء احمد كاظم استاذ مشارك د. سعد عبد العزيز

المستخلص

نتيجة التطور السريع في مجال الانترنت وتواصل البيانات، أصبح أمن المعلومات من المشاكل الاساسية التي يجب اخذها بنظر الاعتبار مع كل عملية نقل للبيانات، خصوصا البيانات التي يراد الحفاظ على سريتها وذلك لأهميتها الخاصة. في هذا البحث يتم استخدام طريقة تشفير وتوليد مفاتيح مطورة تعتمد على اساسيات طريقة RSA، عملية الاخفاء تعتمد على ايجاد حدود شكل معين ضمن الصورة الغطاء واخفاء البيانات في هذه الحدود، يتم ايجاد الحدود باستخدام طريقة موور لتتبع المجاور. الطريقة المقترحة تم فحصها من خلال عدة معاملات فحص مثل PSNR, MSE, CORR لقياس جودة النتائج.

I. Introduction

Cryptography is the science of converting readable text into unreadable one using strong, unbreakable algorithms (or keys). RSA is one of the cryptographic algorithms used frequently in data security [1]; its strength depends on the secrecy of certain numbers used in encryption and decryption. Steganography, in other hand, is the science of hiding secret information within a cover media (image, audio, video); the strength of stego-systems depends on the inability for the attackers to discover the existence of the hidden information [2]. To increase the complexity of any stego-system, both concepts are used together, where the message to be hidden is encrypted then hidden.

When using image as a cover media, many issues should be taken in consideration; hidden message should be invisible, therefore the hiding process should try to keep the changes as minimum as possible to ensure that changes caused by hiding process are subjectively insensible. Another issue is the difference between the original and the received image, this difference should be unnoticeable and the measures should be convincing and the thought to be caused by transmission only; therefore, finding positions to hide the secret message is an important issue.

Any cover image contains one or more object where the color of that object(s) differs from the background color (gray scale images). This characteristic will be employed in hiding process by finding the boundaries of an object within the cover image and use these boundaries in hiding process. To find the object boundaries, a well-known method, "Moore Neighbored" is used[3]; in this method finding the start point to start looking for boundaries is very important, then continuo with the method until all object's boundaries are found. The boundaries usually have values in between the object color and the background color, these are the most suitable values to be used in hiding without affecting the image.

Bhavna and Shrikant [4] proposed a stego-method by using RSA for encryption and hide encrypted message in skin region to get the minimum modification on the covered image. Megha S. Lahase, S. A. Dhole [5] proposed a method for hiding encrypted data using RSA in the LSB in specific positions within the cover image.

1- RSA algorithm

Is an algorithm used to encrypt and decrypt messages using secure keys which are generated and exchanged using the following method [6]:

1-1 Key generation

To generate keys, first two large prime numbers (p,q) must be selected; then (n) should be calculated by $n=p*q$. another value should be calculated which is $\Phi(n)$ and that equals to $(p-1)(q-1)$. Now a number should be selected from the range of integers between 1 and $\Phi(n)$ with a condition that $\gcd(\Phi(n), e) = 1$. Then the value of (d) should be calculated by $d \equiv e^{-1} \bmod \Phi(n)$. the two key which are going to be used for encryption and decryption [7].

The public key which is used for encryption message is $KU = \{e, n\}$, and the private key which is used to decrypt cipher text is $KR = \{d, n\}$.

1-2 Encryption and decryption process

To encrypt a message M:

$$C = M^e \pmod{n} \dots\dots\dots (1)$$

To decrypt cipher text C

$$M = C^d \pmod{n} \dots\dots\dots (2)$$

2- Moore Neighbored

The Moore algorithm is used for finding the boundaries of an object within an image. The algorithm depends on the variation between the object's boundary color and the image's background color. That variations controls the tracing process of finding next point in the boundary after the start point. The algorithm first has to select the start point which actually affect the searching process; ten for each current point, nine neighbors points are determined; the next selected point to be from boundary will be selected and the same steps will be repeated until all boundary points are found[8].

3- Verification measurement's:

The measurements that are used to verify the proposed method are mean square error(MSE) which should be as minimum as possible, Peak signal to noise ratio(PSNR) which should be greater than 50%, and correlation coefficient(CC) which should be close to one[4].

$$MSE = \frac{1}{m*n} \sum_{i=1}^m \sum_{j=1}^n (A_{ij} - B_{ij})^2 \dots\dots\dots (3)$$

$$PSNR = 10 * \log_{10} \frac{(Max)^2}{MSE} \dots\dots\dots (4)$$

The correlation coefficient (CC) can be computed by using the following equation

$$CC = \frac{\sum_{i=1}^N (x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^N (x_i - E(x))^2} \sqrt{\sum_{i=1}^N (y_i - E(y))^2}} \dots\dots\dots (5)$$

Where:

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i \dots\dots\dots (6)$$

x and y are the numerical representation of the original and stego images.

4- Modified RSA (SRSA) Algorithm

The modification on RSA is done by using matrices instead of simple integers in creating the keys and in encryption-decryption processes.

The first steps of RSA are the same where the two large prime numbers p, q are selected and n, $\Phi(n)$ are calculated in the same original RSA method. The modified steps of SRSA is as follows:

Select integer matrix E(m*m) where: $\gcd(\Phi(n), E_{i,j}) = 1$; then calculate another matrix D(m*m), where each element of D comes from:

$$D_{i,j} \equiv E_{i,j}^{-1} \bmod \Phi(n) \dots (7)$$

(Note: $i=1,2,\dots,m, j=1,2,\dots,m$)

The public key which is used for encryption message is $KU = \{E, n\}$, and the private key which is used to decrypt cipher text is $KR = \{D, n\}$, where both D and E are matrices.

II. The proposed method

The proposed method has many steps in which the message to be send will first be encrypted using SRSA, the boundaries of an object will be found by Moore neighbored, then the proposed hiding process will be sued to hide encrypted message in an object boundaries. Figure (1) shows the proposed algorithm steps.

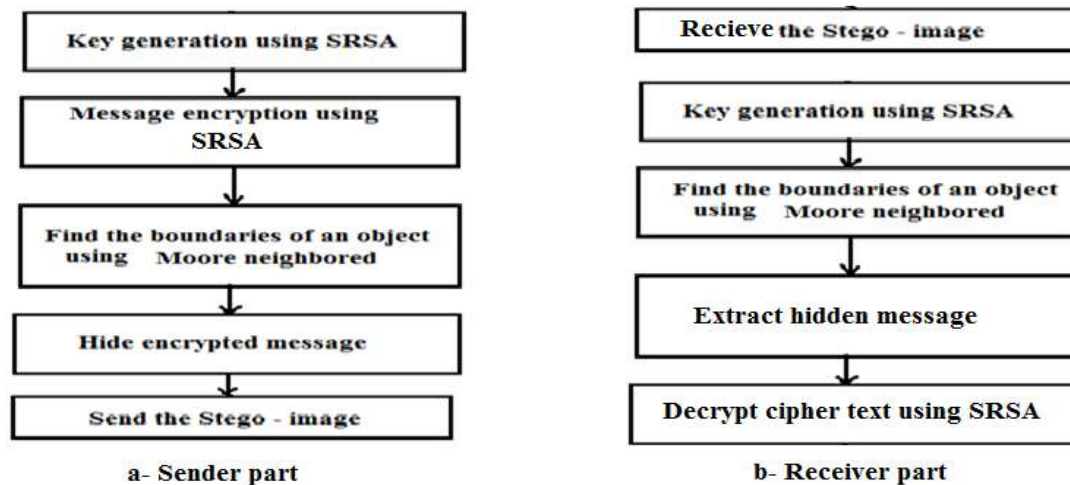


Fig. (1): The proposed algorithm steps (a- sender, b- receiver)

The detailed steps of the proposed algorithm:

- 1- Convert the letters of the message M to their equivalent numbers (A:0, B:1,..., Z:25).
- 2- Apply SRSA to produce keys.
- 3- For each four numbers

$$M_{1..4} = \begin{bmatrix} m1 & m2 \\ m3 & m4 \end{bmatrix}$$

Apply SESA encryption to get cipher text

$$C_{1..4} = \begin{bmatrix} c1 & c2 \\ c3 & c4 \end{bmatrix}$$

- 3- Convert each C to binary (C: $b_8b_7b_6b_5b_4b_3b_2b_1$).

- 4- Convert each three successive bits to a number (it will be between 1 and 7).

- 5- Apply Moore-Neighbored method to find the boundaries of an object.

Since the image is a gray scale image, then the all pixels have values between zero (black) and fifteen (white); the boundaries have a gray color which is either seven or eight, some of these values will be replaced by the secret encrypted message.

- 6- Determine the start hiding point. The sequenced pixels used for hiding are found by scanning process for the first boundary point, the start position of scanning (x, y) is determined by equation (4); since that equation depends not only on the public key 'E' but also on the covered image size, then with each image (new transmission), a new scanning position is determined and therefore different hiding positions used.

$$\left. \begin{array}{l} \text{If image has the size } (R * C), \text{ then} \\ \text{Start point}(x) = (E_{1,1} * n) \bmod R \\ \text{Start point}(y) = (E_{2,2} * n) \bmod C \end{array} \right\} \dots \dots \dots (4)$$

- 7- Hide the cipher text in boundary points selected.

- 8- Receiver will apply steps 2,5,6 then extract the hidden values, decrypt them to get the plain text of secret message.

III. Implementation

- Let the message be: M = "MOHMED CRYPTOGRAPHY"
- Convert each letter to its equivalent number:

M=12, O=14, H=7, M =12, E= 4, D =3, C=2, R=17, Y=24, P=15, T=19, O=14, G=6, R=17, A=0, P=15, H=7, Y=24.

- Let $p=3$, $q=7$, $n=p*q=21$, $\Phi(n)=(p-1)(q-1)=12$

$$E = \begin{bmatrix} 17 & 1 \\ 11 & 5 \end{bmatrix}$$

$$D = \begin{bmatrix} 5 & 1 \\ 11 & 5 \end{bmatrix}$$

- Each four numbers will be encrypted together:

$$M = \begin{bmatrix} 12 & 14 \\ 7 & 12 \end{bmatrix}$$

$$C = \begin{bmatrix} 3 & 14 \\ 7 & 3 \end{bmatrix}$$

- Convert cipher numbers to binary:

3=00000011 14=00001110 7=00000111 3=00001100

Binary: 000000011000011100000011100001100

- Each three bits converted to decimal:

000 = 0, 000=0, 011=3,

(Note: If the number of bits is not module 3, then add 0(s) to the left.)

- The numbers produced from previous step will be hidden within the boundaries of an object extracted from the covered image. Suppose the cover image in figure 1 below with size (88 * 87).

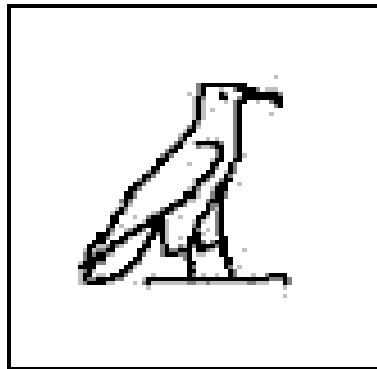


Fig. (1): gray scale image

The start point of hiding will be:

$R=88$, start point(x) = $17 * 21 \bmod 88 = 5$

$C=87$, start point(y) = $5 * 21 \bmod 87 = 18$

The point (5,18) will be the position where scanning the image is started to find the first boundary point for hiding process.

- Apply Moore neighbored to determine the boundaries of the bird. The boundaries extracted will look like the shape in figure (2) below:
- Replace the required sequence of boundary points with the secret message.
- After that the stego-image is ready to be sent.

IV. Results and Analysis

The proposed algorithm was applied on four different images with four different messages with lengths between 20 and 30 letters each. Figures 3, 4, 5 and 6 represent the four tested images before and after hiding process.

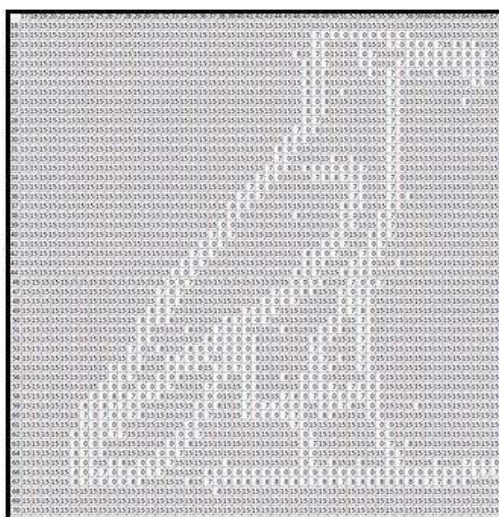
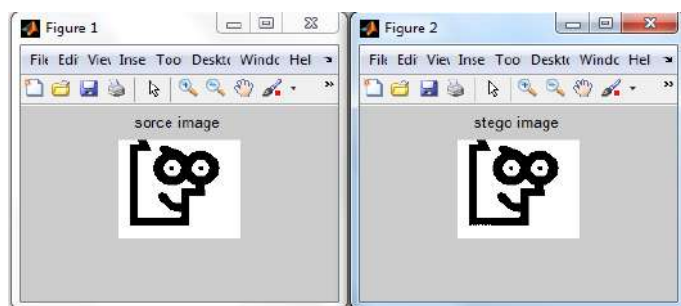
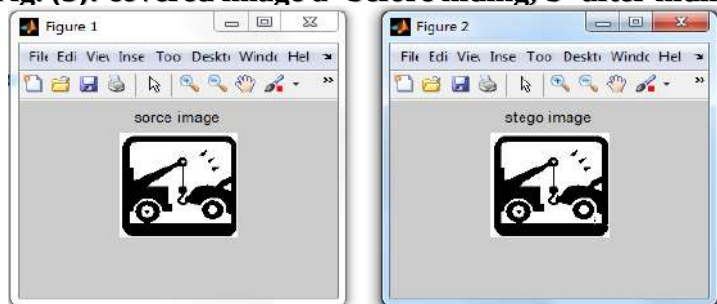


Fig. (2): boundaries of image "bird"



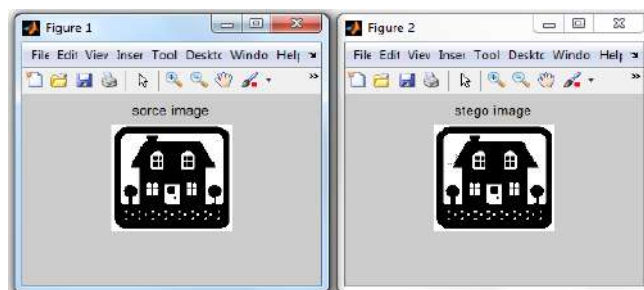
a: original image, b: stego-image

Fig. (3): covered image a- before hiding, b- after hiding



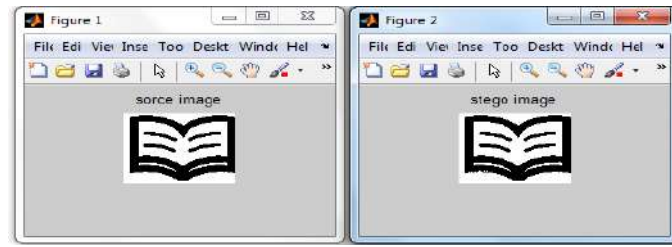
a: original image, b: stego-image

Fig. (4): covered image a- before hiding, b- after hiding



a: original image, b: stego-image

Fig. (5): covered image a- before hiding, b- after hiding



a: original image, b: stego-image

Fig. (6): covered image a- before hiding, b- after hiding

The stego-images were tested and verified with different metrics, the results are shown in table (1).

Table (1) Analysis of four images with the proposed method

Image	PSNR	MSE	CC
Image1	78.5383	9.1044e-004	0.9978
Image2	79.5043	7.2887e-004	0.9985
Image3	78.9972	8.1913e-004	0.9982
Image4	77.4884	0.0012	0.9976

The 'peak signal to noise ratio PSNR' measures the ratio of original image pixels to the noise caused by hiding process; this value as greater than 50 as better, with the proposed method all values greater than 70.

MSE 'mean square error' should be as minimum as possible, here, the largest value is 0.0012 which is very small as it should be.

The similarity between the original and stego images measured by the correlation coefficient C, it has to be close to 1.

V. Conclusion

Steganography became one of the most important fields of security, it is used for authenticating documents and verifying media ownership. In this research a new steganography method is proposed, messages are encrypted using modified RSA algorithm, then embedded within covered image in the boundaries of an object within that image; this method gave good results with minimum modification, the MSE were very small (less than 10^{-3}), PSNR was greater than 70%, and the CC was close to 1.

Reference

- [1] Sos Agaian and Yicong Zhou. **"Image Encryption using the image steganography concept and PLIP model"**, IEEE International conference on System Science and Engineering. pp. 699-703. 2011.
- [2] Stalling, **"Cryptographic and N/W security: Principles and Practices"**, Prentice Hall, 2nd Edition 2005.
- [3] G. l. Liang, S.-z. Wang, and X.-p. Zhang. **"Steganography in binary image by checking data-carrying eligibility of boundary pixels"**. Journal of Shanghai University (English Edition), 11(3):272–277, 2007
- [4] Bhavna Sharma, Shrikant Burje, **" A Steganography Scheme using RSA and Opalgorithms with Histogram Modification in Skintone Decetion"**, IJARE, EIE, Vol. 2, Issue 8, August 2013.
- [5] Megha S. Lahase, S. A. Dhole, **"Hybrid Encryption and Decryption Method using LSB and RSA in Steganography"**, COE, Bharti Vidyapeeth, Deemed University, Pune, Special Issue-1 April-2015.
- [6] Ahn, L.V. and N.J. Hopper, 2004. **"Public-key steganography"**. In Lecture Notes in Computer Science, Vol. 3027 / 2004 of Advances in Cryptology – EUROCRYPT, Springer-Verlag Heidelberg, 2004, pp: 323–341.
- [7] Prof. Samir Kumar, Sarthak Parui, **"A Method for Public Key Method of Steganography"**, International Journal of Computer Applications (0975 – 8887), Volume 6– No.3, September 2010
- [8] David Doria, **"Moore Neighbor Tracing"**, The Insight Journal, 2011.
- [9] Min Wu, and B. Liu., **"Data hiding in digital binary image"**. IEEE transactions on multimedia. 6(4). 2004.
- [10] Venkatraman, S., Abraham, A. & Paprzycki, M., **"Significance of Steganography on Data Security"**, Proceedings of the International Conference on Information Technology: Coding and Computing, 2004.
- [11] Nameer N. EL-Emam, **"Hiding a large amount of data with high security using steganography algorithm"**, Journal of Computer Science. April 2007, pp. 223 – 232.
- [12] B. J. Mohd, S. Abed and T. Al-Hayajneh; **"FPGA Hardware of the LSB Steganography Method"**, IEEE computers 2014, pp. no.978-1-4673-1550-0/12.
- [13] Anil Kumar, Rohini Sharma; **" A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique"**; International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013, pp. no.363- 372.

Using the principle of definite double integral in cryptography

Basim Najm Al-Din Abed

Diyala university/college of education for pure sciences/computer science department

basim007@yahoo.com

Abstract:

Today all the information are exchange over the Internet, so, finding the secure ways which produce the necessary protection against the different types of attacks becomes one of the important parameters of many researches. Many researches focus on the main role in information security systems which is the Encryption algorithms.

The main goal of any cryptosystem is to make it difficult to find the correct plain text without knowing the key. So for this type of cryptosystem, the decryption of the cipher text is very hard without knowing the key used in encryption process.

Sometimes, many algorithms seems very strong and complex, but in fact it is very easy to break, through using the proper attack. To select an encryption algorithm, it is necessary to select the one that have strength against different types of attacks.

In this research, a new encryption method is proposed to encrypt text by using the standard of definite double integration. The sender and the recipient will share an equation to be integrated and four randomly constants represent the boundaries of the double integration. The result of the integration added to the value of the character and xored with randomly shared value between both sides to get finally the cipher text of the proposed method.

Keywords: definite double integral, autocorrelation attack, side channel attack.

استخدام مبادئ التكامل المحدد المزدوج في التشفير

باسم نجم الدين عبد

المستخلص

في هذه الايام يتم تبادل المعلومات عبر الانترنت، لذا فان ايجاد طرق امانة التي توفر الحماية الضرورية ضد مختلف انواع الهجمات اصبح احد المعايير الرئيسية للعديد من الابحاث. العديد من الابحاث تركز على الدور الرئيسي في نظام امنية المعلومات والذي هو خوارزمية التشفير.

ان هدف الرئيسي لكل نظام تشفير هو جعلها صعبة في ايجاد النص الصريح من دون معرفة المفتاح. لذا فانه لمثل هكذا نوع من انظمة التشفير، فان عملية فك تشفير النص المشفر تكون صعبة من دون معرفة المفتاح المستخدم في عملية التشفير.

في بعض الاحيان فان العديد من الخوارزميات تبدو صعبة ومعقدة ولكنها في الحقيقة تكون سهلة الكسر من خلال هجوم فعال. فعند اختيار خوارزمية تشفير فإنه يجب اختيار تلك التي تمتلك قوة ضد مختلف انواع الهجمات.

في هذا البحث فانه تم اقتراح طريقة تشفير جديدة باستخدام مقياس التكامل المحدد المزدوج. في هذه الطريقة فإن المرسل والمستقبل سوف يتشاركون في المعادلة، التي سوف يتم ايجاد التكامل لها بالاضافة لاربعة قيم ثابتة تمثل حدود التكامل المزدوج، بعد اجراء التكامل سوف يتم اضافة قيمة الحروف الى ناتج التكامل كثابت لعملية التكامل من اجل تشفير الرسالة ومن ثم عمل XOR للناتج مع مفتاح يتم مشاركته بين الطرفين للحصول على النص المشفر النهائي.

الكلمات المفتاحية: التكامل المزدوج المحدد، هجوم الارتباط الذاتي، هجوم ذا قناة اتجاه واحدة.

I. Introduction

The cryptography is the science and art of hiding the real meaning of the information to protect this information from intruders, the encryption is the process of hiding the information in the way such that only the authorized parties can decrypt it. The information or message in the cryptography is called plaintext, that is encrypted using an encryption process to generate the cipher text. An encryption scheme use a random key that generated by an encryption algorithm. Without having the key it is difficult to decrypt the message. Authorized parties can decrypt the message easily with the key shared between two parties [4].

Cryptology is an art and science of hidden or secret writing [5]. It has two main parts: cryptography and cryptanalysis [7]. Cryptography mainly related to altering data to make them secure and insusceptible to attacks. Cryptanalysis is related to breaking the different cryptography methods and get the original data [2].

1- Types of the Encryption Algorithms

The encryption algorithms are divided into two types: modern and classical encryption algorithms as shown in fig.1. The classical encryption algorithms is divided into substitution and transposition algorithms [1]. The modern encryption algorithms is divided into asymmetric and Symmetric key encryption which is use the block cipher, where data is divided into blocks of the specific length, or stream cipher where data is divided into single bits [3].

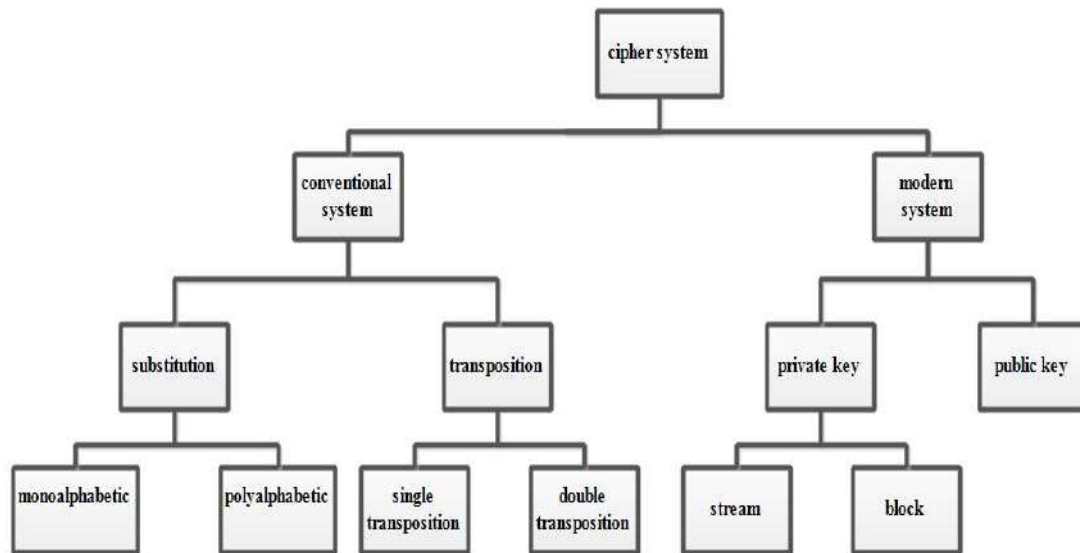


Fig. (1): Classification of the Encryption Algorithms

1-1 Types of classical encryption algorithms

1-1-1 Substitution technique

A substitution cipher changes characters in the plaintext by substitute the character in the plain text with the character from the alphabet to produce the cipher text. [3].

1-1-2 Transposition Technique

A transposition cipher rearranges the characters in the plaintext to form the cipher text. The letters are not changed. [3].

1-2 Types of modern encryption algorithms

1-2-1 Secret key or Symmetric encryption

In the symmetric key, the encryption and decryption keys are the same keys. The communicating parties shared the same keys before accomplishing the communication as shown in fig.2. (DES, TDES and AES) are different symmetric encryption algorithms [6].

1-2-2 Public key or asymmetric encryption

In the public key encryption schemes, the encryption key is public for everyone. But, only the recipient has the decryption key that make the cipher text to be decrypt. This called the private key as shown in fig.3. (E.g. RSA - Rivest-Shamir-Adleman; El Gamal).

2- Classification Of Attacks

The main objective of a cryptanalyst is to get maximum information about the original data to use it to know the correct key. (Saroja, M. V., Mor, S., & Malik, J., 2012).

2-1 Most common types of cryptographic attacks

1. Known plain text attack: involve breaking successfully one cipher-text and obtaining plain-text to be used for finding relation between the new coming cipher-text.
2. Chosen plain-text attack: the adversary may ask that specific plaintexts be enciphered. She is given the corresponding cipher texts. Her goal is to find the key that was used.
3. Cipher text only attack: involve accessing only the cipher-text by cryptanalyst, so the attacker will try to decrypt cipher-text to get its plain-text by other means like using frequency distribution.

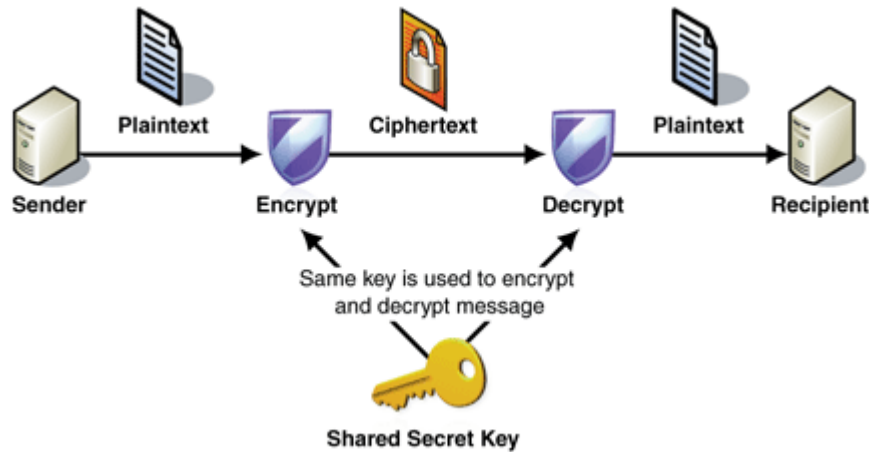


Fig. (2): Private Key encryption

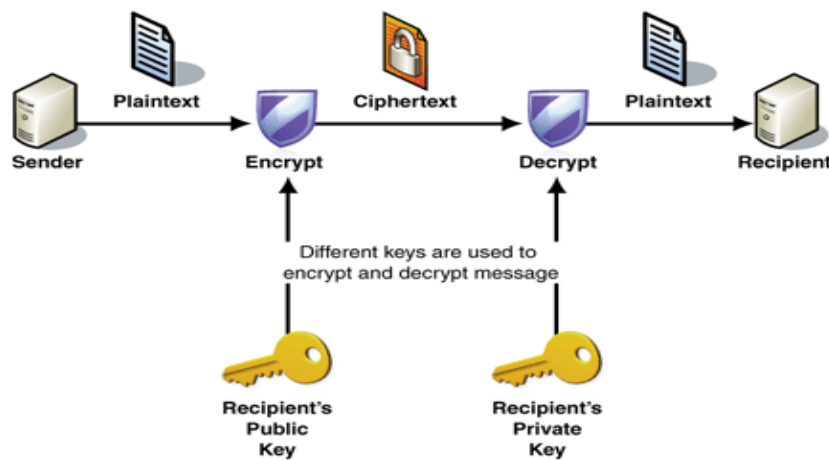


Fig. (3): Public key encryption

4. Chosen cipher-text attack: involve choosing any cipher-text by cryptanalyst and searching for some matching plain-text with a well-known and analyzed cipher-text.

5. Adaptive chosen cipher-text attack: involve adapting the attack by cryptanalyst through sending alternate cipher-text to be decrypted. Depending on the result, further cipher texts can be chosen.

In this research we propose a new encryption method to encrypt text by using the principle of definite double integration where the sender and the recipient will agree up on any double integration form and the boundaries of the integration, taking in account to be unbreakable by the different cryptanalysis methods.

2-2 Operational Definitions

In the proposed algorithm based on definite integral many variables and a function of power n must be clearly define.

Let f be a function of x and $a \leq x \leq b$, the interval $[a, b]$ divide into n subintervals

$\Delta x = (b - a) / n$. Let $x_0 (=a), x_1, x_2, \dots, x_n (=b)$

$x_1^*, x_2^*, \dots, x_n^*$ be any sample points in these subintervals

x_i^* lies in the i th subintervals $[x_{i-1}, x_i]$.

Then the definite integral of f from a to b is

$$\int_a^b f(x) dx = \lim_{n \rightarrow \infty} \sum_{i=1}^n f(x_i^*) \Delta x \dots \dots \dots (1)$$

II. Problem Statement

The data transmitted over the internet need always to protect its content from the intruder, and since the cryptanalyst develop ways and methods to decrypt the different cipher texts that encrypt by different algorithms. So, it's necessary to develop the cryptographic algorithms to prevent the

unauthorized parties to break the cipher text in order to protect the data transmitted over internet. Also, most of the cryptographic algorithms focused on using one particular equation to encrypt and decrypt process, and in the proposed method there is no particular equation, but select the equation that be integrated according to the n value which represent the order of the equation that be integrated, to increase the difficulty of breaking this cipher. In addition, using number of random keys instead of using a single key add more complexity and security to the proposed scheme.

III. Research Objectives

The objective of this research is to use the principles of the definite double integral in the cryptography to add more security to the text when transmitted over the internet. And to increase the complexity of guessing the correct plain text through applying a cryptanalysis methods on this text. Moreover, to evaluate the inevitability of the proposed encryption technique against different cryptanalyses is attack.

VI. Methodology

The proposed encryption algorithm that is depend on definite integral form, implemented in matlab 2010b. At the beginning, it allows two users to exchange a secret key and a function of power n with four randomly selected numbers; the keys are shared between the sender and receiver securely through secure channel.

1- Key generation phase

1-1 Choosing four random numbers a,b,c,d

1-2 Choosing an integration formula $ax^n \pm bx^{n-1} \pm \dots \pm z$ (2)

1-3 Choosing a key=k

2- Encryption phase

2-1 Global a, b, c, d, k

num=0;

while num==0

A=input('input your message to be encrypted, 's');

if size(A)<= length(A);

num=1;

end

end

2-2 for I=0:size(A)

C(I)=int(int(x,a,b),x,c,d)

2.1. B = de2bi(d)

2.2. C = bitxor(b,k)

Break;

End

2.3. cipher text

3- Decryption phase

3-1 Receive cipher text from internet

3-2 Compute XOR between character binary value and key=k value

3-3 Convert character binary format into numeric value

3-4 Substitute a, b, c, d values in the double integral:

$$\left[\frac{aB^{n+1}}{n+1} \pm \frac{bB^n}{n} \pm \dots \pm z \right] - \left[\frac{aA^{n+1}}{n+1} \pm \frac{bA^n}{n} \pm \dots \pm z \right] \dots \dots \dots (3)$$

to obtain (c) value which is the numeric value for the message character

3-5 Convert the numeric value of the message character into corresponding character

3-6 Apply all five steps above to all message characters

3-7 Obtaining plain text

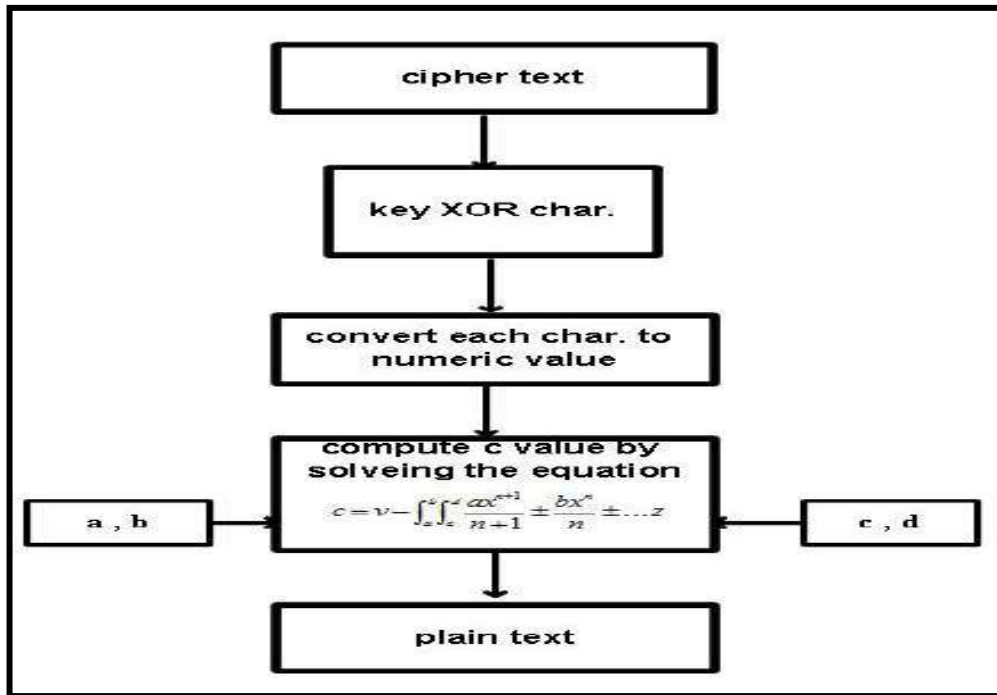


Fig. (4): Encryption phase

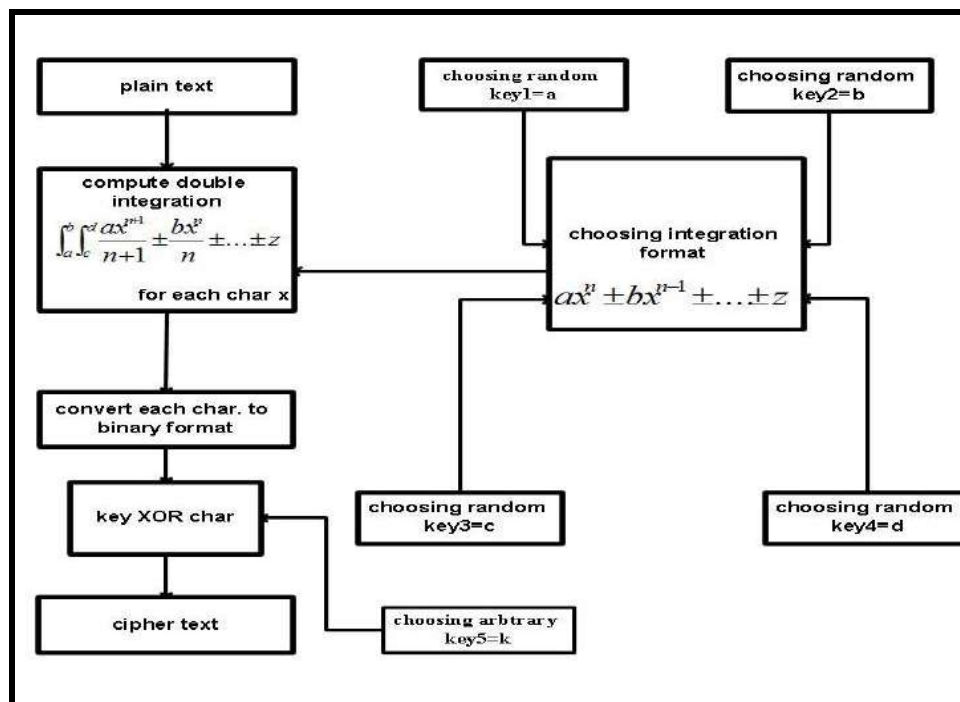


Fig. (5): Decryption phase

VII.Implementation

1- Key generation phase

1-1 Choosing a=5, b=1, c=2, d=4

1-2 Choosing integral formula $2x^2 - 4$

1-3 Choosing key=10.10

2- Encryption phase

2-1 Plain text is = "Yarmouk University"

2-2 Compute the integral $\int_1^5 \int_2^4 2x^2 + 4dxdy \dots \dots \dots (4)$

2-3 Let we take the first character in the message which is Y where the value of Y=89

2-4 Compute the integral value

First we compute the entire integral

$$\int_2^4 2x^2 + 4dx \dots \dots \dots (5)$$

$$\text{Compute the indefinite integral } \int 2x^2 + 4dx = \frac{2x^3}{3} + 4x + c \dots \dots \dots (6)$$

Then we compute the definite integral

$$\int_2^4 2x^2 + 4dx = \frac{136}{3} \dots \dots \dots (7)$$

$$\text{Now we compute the outer integral } \int_1^5 \frac{136}{3} dy \dots \dots \dots (8)$$

$$\text{Compute the indefinite integral } \int \frac{136}{3} dy = \frac{136}{3} y + c \dots \dots \dots (9)$$

$$\text{Compute the boundaries } \int_1^5 \left(\frac{136}{3} \right) dy \dots \dots \dots (10)$$

$$\int_a^b f(x)dx = F(b) - F(a) = \lim_{x \rightarrow b-} (F(x)) - \lim_{x \rightarrow a+} (F(x)) \dots \dots \dots (11)$$

$$\lim_{y \rightarrow 1+} \left(\frac{136y}{3} \right) = \frac{136}{3} \dots \dots \dots (12)$$

$$\lim_{y \rightarrow 5-} \left(\frac{136y}{3} \right) = \frac{680}{3} \dots \dots \dots (13)$$

$$\int_1^5 \left(\frac{136}{3} \right) dy = \frac{680}{3} - \frac{136}{3} \dots \dots \dots (14)$$

$$= \frac{544}{3}$$

$$= 181.33$$

Add character ascii code for "Y" which is 89 as integral constant(c) to the double integral value as
 $181.33 + 89 = 270.33$

$$\int_1^5 \int_2^4 2x^2 + 4dxdy = 181.33 + 89 = 270.33 \dots \dots \dots (15)$$

2-5 Convert the numeric value obtained from previous step into binary format

$$270.33 = 100001110.010101000$$

2-6 Convert the numeric value for key =10.10 into binary format

$$10.10 = 000001010.000110011$$

$$2-7 \quad 100001110.010101000$$

XOR

$$\underline{000001010.000110011}$$

$$100000100.010011011$$

2-8 Cipher text is

$$\begin{array}{cccc} 100000100.010011011 & 100011100.010011011 & 100101101.010011011 & 100101000.010011011 \\ 100101110.010011011 & 100100000.010011011 & 100101010.010011011 & \\ 100100001.010011011 & 100010100.010011011 & 100101001.010011011 & 100000000.010011011 \\ 100010100.010011011 & 100101110.010011011 & 100101101.010011011 & 100010000.010011011 \\ 100100100.010011011 & 100101111.010011011 & & \end{array}$$

3- **Decryption phase**

$$3-1 \quad 100000100.010011011$$

XOR

000001010.000110011

100001110.010101000

3-2 converts the binary format from above step into numeric value 100001110.010101000=270.33

3-3 computes the double integral value $\int_1^5 \int_2^4 2x^2 + 4xdy + c = 270.33.....(16)$

3-4 C=270.33-181.33

C=89

3-5 Convert the numeric value obtained from the previous step into corresponding character "Y=89"

3-6 apply all five steps above to all message characters to obtain the plain text

3-7 Plain text is = "Yarmouk University"

Cryptanalysis tests

By applying the brute force attack on the proposed method the results showed this cryptanalysis couldn't guess the correct cipher text, so it fail to break the cipher text of the proposed method as it shown in the results below of this cryptanalysis technique.

100101000.010011011 100101101.010011011 100011100.010011011 100000100.010011011
100101010.010011011 100100000.010011011 100101110.010011011
100100001.010011011 100010100.010011011 100101001.010011011 100000000.010011011
100010100.010011011 100101110.010011011 100101101.010011011 100010000.010011011
100100100.010011011 100101111.010011011

By using frequency attack the results showed that this cryptanalysis also fails to break the cipher text of proposed method as shown below in the Figures (5, 6, and 7):

E	T	A	O	I	N	S	H	R	D	L	C	U	M	W	F	G	Y	P	B	V	K	J	X	Q	Z
12.7	9.1	8.2	7.5	7.0	6.7	6.3	6.1	6.0	4.3	4.0	2.8	2.8	2.4	2.4	2.2	2.0	2.0	1.9	1.5	1.0	0.8	0.15	0.15	0.10	0.07

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN

The most common digraphs in the english language are
TH,HE,AN,IN,ER,ON,RE,ED,ND,HA,AT,EN

The most common digraphs in the message are

Fig. (6): Frequency attack- digraphs

E	T	A	O	I	N	S	H	R	D	L	C	U	M	W	F	G	Y	P	B	V	K	J	X	Q	Z
12.7	9.1	8.2	7.5	7.0	6.7	6.3	6.1	6.0	4.3	4.0	2.8	2.8	2.4	2.4	2.2	2.0	2.0	1.9	1.5	1.0	0.8	0.15	0.15	0.10	0.07

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN

The most common trigraphs in the english language are
THE,AND,THA,ENT,ION,TIO,FOR,NDE,HAS,NCE,TIS,OFT,MEN

The most common trigraphs in the message are

Fig. (7): Frequency attack- trigraphs

E	T	A	O	I	N	S	H	R	D	L	C	U	M	W	F	G	Y	P	B	V	K	J	X	Q	Z
12.7	9.1	8.2	7.5	7.0	6.7	6.3	6.1	6.0	4.3	4.0	2.8	2.8	2.4	2.4	2.2	2.0	2.0	1.9	1.5	1.0	0.8	0.15	0.15	0.10	0.07

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN

The most common double letters in the english language are
SS,EE,TT,FF,LL,MM,OO

There are no double letters

Fig. (8): Frequency attack- double letter

Also by applying m-138 cipher text only attack, the results showed the fail of this type of cryptanalysis to break the cipher text of the proposed method and guessing the correct plain text as shown below:

The plain text obtained from the m-138 cipher text only attack for the cipher text obtained from proposed method is:

D T H E R E D I N A N D O N O F T H E R S A N D E D T H E R E D I N A N D O N O F T H E R S A N D E D T H E R E D I N A
 N D O N O F T H E R S A N D E D T H E R E D I N A N D O N O F T H E R S A N D E D T H E R E D I N A N D O N O F T H E R
 S A N D E D T H E R E D I N A N D O N O F T H E R S A N D E D T H E R E D I N A N D O N O F T H E R S A N D E D T H E R
 E D I N A N D O N O F T H E R S A N D E D T H E R E D I N A N D O N O F T H E R S A N D E D T H E R E D I N A N D O N O
 F T H E R S A N D E D T H E R E D I N A N D O N O F T H E R S A N D E D T H E R E D I N A N D O N O F T H E R S A N D E
 D T H E R E D I N A N D O N O F T H E R S A N D E D T H E R E D I N A N D O N O F T H E R

By applying the Berlekamp Massey cryptanalysis to guess the correct equation used in the proposed method and the linear feedback shift register to obtain the feedback polynomial to guess the correct keys and obtain the correct plain text for the proposed method, the results showed that the cryptanalysis technique couldn't guess the correct equation used in the proposed method, so it's very difficult to break the cipher text as it shown in the Figures (9, 10) bellow:

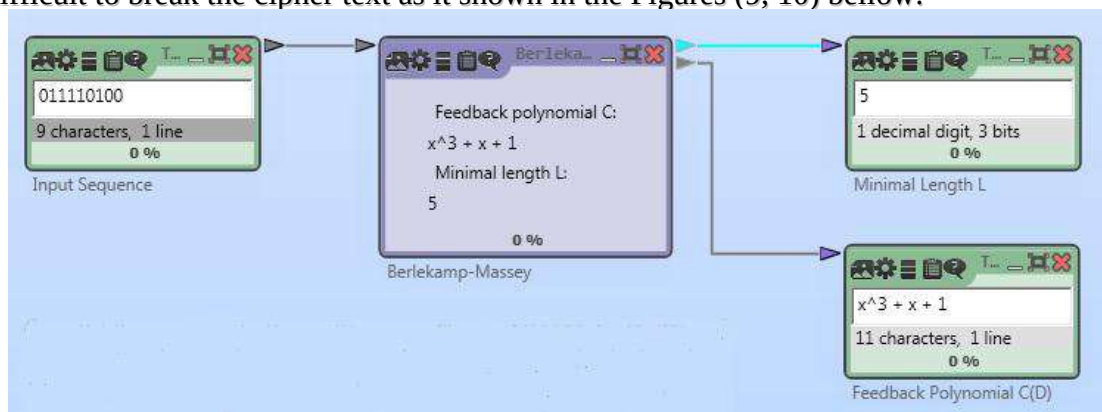


Fig. (9): Berlekamp Massey cryptanalysis

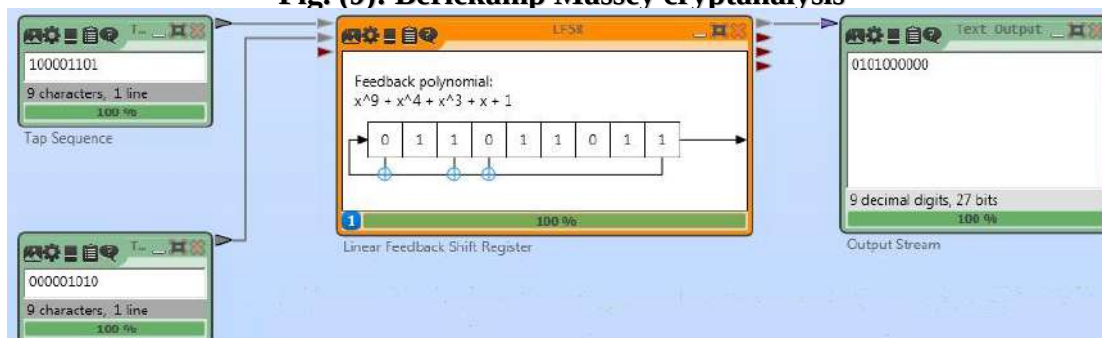


Fig. (10): Linear feedback shift register obtained from Berlekamp Massey

also by using auto correlation attack in order to trying to break the cipher text of the proposed method, the results showed that the correlation between the characters is very poor so it means that, it's difficult to guess the correct characters of the cipher text as it shown below in the Figure (11):

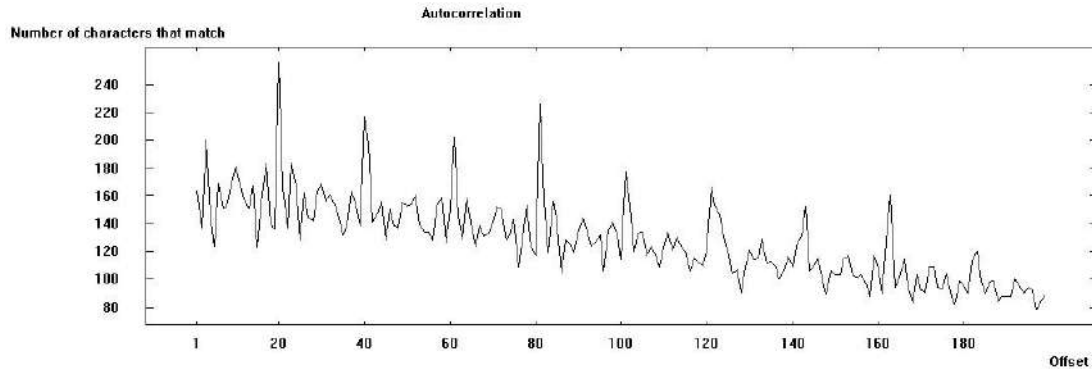


Fig. (11): Auto correlation attack

Finally, by applying the one of the most powerful cryptanalysis technique which is side – channel attack on the proposed method, the results showed incapability to break the cipher text of the proposed method even with this cryptanalysis technique as it shown in the Figure (12) below:

```
Ciphertext: M.d...2 ir@..
Dg...3...-z...3...m.rq
kt...7|...n*U.$./g.Uk-F.h
=...%...a...9u...{vB.%nD.kn...
o.Y.p...f...3.W*...P0FO
a...Z...m...E.y.R.=~
".F...d.q.j.5.Q9EN...QbU
).F.NW...0.H.y...).H.}
p.$4\...J.8...!BJ...N
[...F}.23'...ca.iC.I.nU.@|
N...~...J^...u.-?^8.\...K
m.g...9mB...'k.X...p...Q
j~/...lKuMq.CO'(...#^W.5.Sy
0..H$.&U...{(F'O.I.z...A.b
```

Fig. (12): Side – channel attack

VIII. Conclusion

This research propose a new technique to encrypt and decrypt the message using a definite double integral and four numbers which is the boundaries of the double integral as a keys and xored the result of the equation with the fifth shard value as a fifth key to increase the complexity of the cipher text.

By using different types of cryptanalysis methods such as berlekamp Massey cryptanalysis, linear feedback shift register (LFSR), autocorrelation attack, brute force attack, frequency attack, m-138 cipher text only attack and side – channel attack on the proposed algorithm, the results showed that this method investable against this types of cryptanalysis, and couldn't guess the correct formula of the integral and doesn't guess the correct keys, because of guessing the correct boundaries of the integral and fifth key requires number of attempts which requires many years to break the cipher text, from the result above we concluded the strength of proposed algorithm and strength of the key generation technique.

Reference

- [1] Asif, A. M. A. M., & Hannan, S. A. A Review on Classical and Modern Encryption Techniques.
- [2] Atul Kahate (2009), "**Cryptography and Network Security**", 2nd edition, McGraw-Hill.
- [3] Jeeva, A. L., Palanisamy, D. V., & Kanagaram, K. (2012), "**Comparative analysis of performance efficiency and security measures of some encryption algorithms**". *International Journal of Engineering Research and Applications (IJERA)* ISSN, 2248-9622.
- [4] Luciano D, Prichett G. Cryptology: "**from caesar ciphers to public-key cryptosystems**". The College Mathematics Journal 1987; 18(1):2–17
- [5] Saroha, M. V., Mor, S., & Malik, J. (2012), "**A Review of Various Techniques of Cryptanalysis**". *International Journal of Advanced Research in Computer Science and Software Engineering*, 2(10).
- [6] Scripcariu, L. (2015, July), "**A study of methods used to improve encryption algorithms robustness**". In *Signals, Circuits and Systems (ISSCS), 2015 International Symposium on* (pp. 1-4). IEEE.
- [7] William Stallings (2003), "**Cryptography and Network Security**", 3rd edition, Pearson Education.

Proposal of Enhancement the LOKI97 Algorithm

Assist. Prof. Dr. Alaa Kadhim Shahad Husham
University of Technology/ Computer Science Department
shahadhusham93@yahoo.com

Abstract:

As it's known, any cryptographic algorithm could be vulnerable to breakdown and cryptanalysis, but this is contrary to the basic aim of cryptographic algorithm which is the protection of the confidentiality of the message which are sent over insecure channel. So, the algorithm should be devised to be more intricate through increase the number of rounds or improve the internal functions components or any perplexity and complexity of the algorithm, to make this algorithm more robust to break by the adversary.

In this paper, have been design a proposal of development the LOKI97 standard, by developing some of its functions, and adding some sub-functions, to increase its complexity and making it possess high confusion and diffusion to be more robust against the penetration.

Keywords: Cryptography, LOKI97, F-function, Block Cipher.

مقترح لتحسين خوارزمية LOKI97

ا. م. د. علاء كاظم فرحان شهد هشام كامل

المستخلص

كما هو معروف، أن أي خوارزمية تشفير يمكن أن تكون عرضة للكسر والتحليل، ولكن هذا يتعارض مع الهدف الاساسي من خوارزمية التشفير الذي هو حماية سرية الرسالة التي يتم إرسالها عبر قناة غير آمنة. لذلك يجب تصميم الخوارزمية لتكون أكثر تعقيداً من خلال زيادة عدد الدورات، أو تحسين مكونات الدوال الداخلية، أو أي تعقيد للخوارزمية، لجعل هذه الخوارزمية أكثر قوة ضد الكسر من قبل المهاجم. في هذا البحث، تم تصميم اقتراح تطوير خوارزمية LOKI97، من خلال تطوير بعض دوالها لزيادة درجة تعقيدها مما يجعلها تمتلك أرتباك وانتشار عالي، لتكون أكثر قوة ضد الاختراق.

I. Introduction

The security is basically about the process of preservation the critical and sensitive information that transmitted over the unsafe canal from unlawful utilization and illicit disclosure. On the other hand, most data will devalued over time. It's important that the value of the data always remain less than the cost to break the security protecting it [1]. The security is aims to provide some criteria of information security such as the authentication, confidentiality, and data integrity, and these goals have been achieved by the using of the cryptography [2].

Cryptography is the art of achieving security by encoding messages to make them non-readable [2], because the cryptography's task is protection of information from all individuals except the intended recipient, who is the only person (to some extent) able to retrieve it later to the explicit text of the original by using the same algorithm that used in the encryption with the employment of secret keys. Therefore, that the cryptography plays a serious part of any security system [3].

II. Loki Overview

The family of a block cipher of (Loki89, Loki91) is Designed to be as replacing of data encryption standard (DES) algorithm, and it is very similar to DES in its structure.

LOKI97 is one member of the LOKI family, designing by Lawrie Brown. It is a new 16 round Feistel cipher on 128-bit data using a complex non-linear function f. [4]. It is using 128, 192, or 256-bit keys. The LOKI97 is designing as a development of Loki 91, by increasing the number of rounds up to 16 and increase the data input from 64-bits to 128-bits, and made the function (F-function) more complicated that is using also in the key schedule. The following figure (1) shown the main F-function of LOKI97.

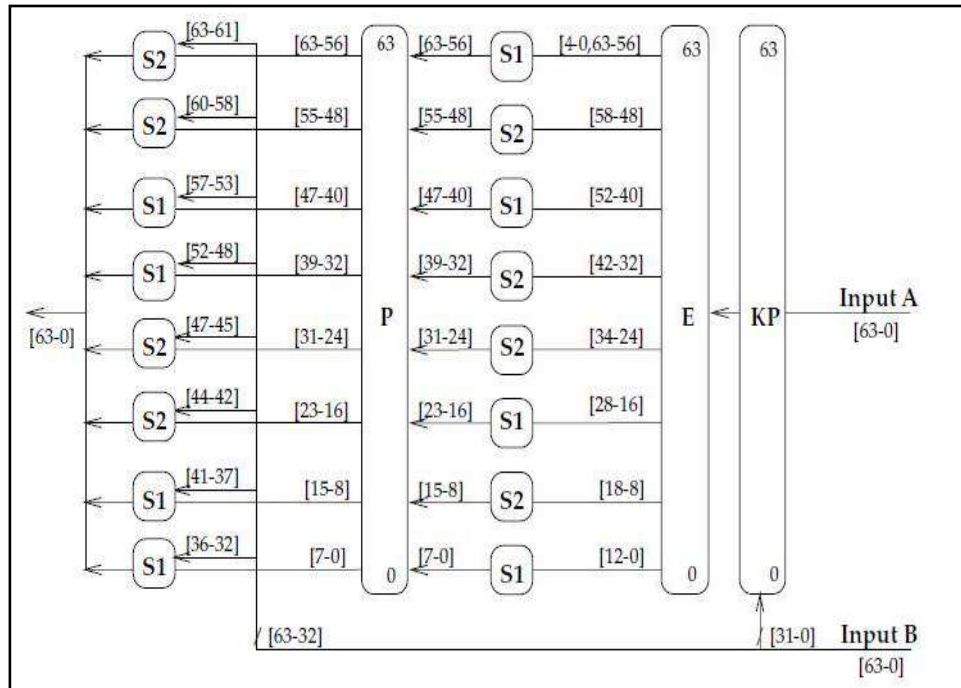


Fig. (1): F-function of LOKI97 algorithm

1- The Proposal of Loki97 algorithm

In Loki89,91 some weaknesses appeared such as key scheduling that have been handled in Loki97, it has also been increasing the length of the block as well as the complexity of the F-function and use this function in its Key scheduler. In Loki97 algorithm, there are some fragility in internal functions component. In this paper, the proposal have improve some functions which are keyed-permutation, permutation function, S-box. On the other hand, to increase the complexity of the proposal, some functions were replaced by other functions, such as the expansion function have replaced by the circular left shift function, also adding the swap function which is similar to the keyed-permutation function in the LOKI97 standard. Through the use of some improvements, The proposal will be presented as the following shown figure (2).

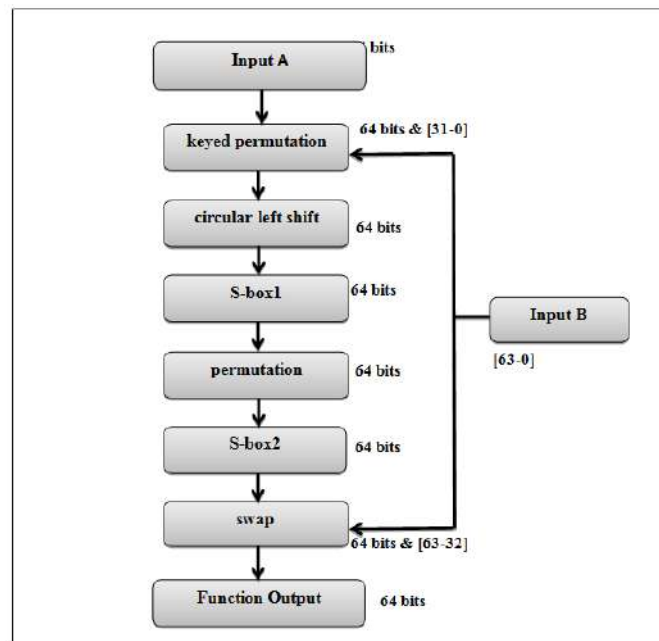


Fig. (2): The proposal of F-function of Loki97

1-1 Proposal Ked Permutation Function (KP -Function)

The ked permutation function of the LOKI97 standard is updating. The kp-function is used the two entrance of the main F-function (A and B). The input A is dividing into blocks of (2-bits). The subsequent step will be the conversion process of the binary code of this part into the DNA codes, where the block of 00 is represent as A and the blocks of 01,10,11 will represent the codes C, G, T respectively. As the following DNA-table:

DNA - Code	Complementary
A	T
T	C
C	G
G	A

Fig. (3-1): Binary to DNA-Code transformation

Then the block of B is dividing into 16 (4-bits) blocks, and convert them to equivalent decimal and taking the modular of (3), because the subsequent process needed only three transformation. Then each number of these blocks will be considered as a control switch of the conversion process of A, based on the complement method as that, the A code in DNA sequence is converted to T, and T converted to C, C to G, while G is complemented to A, based on the control switch of each blocks. If the number of control switch is (1) so that the equivalent block is complemented (once), if the number equal to two so the process will apply twice and so on, as the following complement cycle and table:

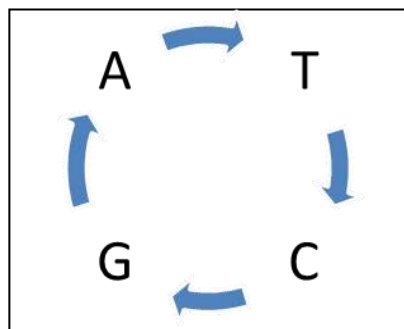


Fig. (3-2): DNA complement

Binary-code	DNA-code
00	A
01	C
10	G
11	T

Figure (3-3): Complementary code of DNA

(KP) Algorithm (1): DNA of ked-permutation

Input: two sequences A and B of 64-bit to each one.

Output: one sequence of C after the DNA and complement conversion.

begin

1. Divided A-block into blocks of (2-bit).

2. Set DNA code: 00=A, 01=C, 10=G, 11=T to A-blocks.

3. Divided B-block into 16-blocks of (4-bit).

4. Convert B-blocks to decimal mod 3.

5. Set the above result as control switch to new A-blocks.

6. Complemented A-DNA as A=T, T=C, C=G, G=A as the control switch.

7. Retrieve binary code as inverse of step 2.

End.

2- Proposal Circular Left-Shift Function

In this proposal, the circular left shift function is compensating for the expansion function in the standard LOKI97 algorithm. This function will receive 64-bits as an input and produce 64-bits as an output. The first step is dividing the block of 64-bits into 8-blocks of 8-bits, then picked up 4-bits from each new block (the core of the block) from the third bit to the sixth bit, and set a circular left shift by 1 to these sub blocks, then replace these resulted blocks after shifting to those sub blocks that have been deducted.

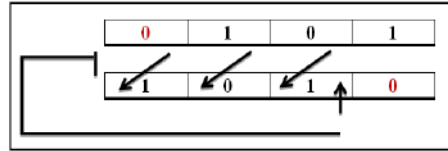


Fig. (4): Circular left shifting of 4-bits

Algorithm (2): Circular left shift function

Input: block of 64 bits.

Output: block of 64 bits after shifting process.

begin

1. Dividing the block of 64-bits into 8 blocks of (8-bits).

2. Picked up the 4-bits from 3rd to 6th and put in (a).

3. Apply circular left shift to (a):

3.1 Put $s = a(0)$

3.2 for $i = 0$ to 3

3.3 $a(i) = a(i+1)$

3.4 $a(3) = s$

3.5 next i

4. These new blocks after shifting are replaced by the old blocks before shift.

5. Produce a sequence of 64-bits.

End.

3- Proposal Substitution Box (S-Box)

The Loki97 algorithm have an eight (S-boxes) and receive the input bits of 96-bits, that have been compressed to 64-bits as an output. The substitution box (S-box) in LOKI97 algorithm has been replaced by a proposal S-box. In this paper, have been used the S-box method of the AES algorithm. So The proposal S-box will receive 64-bits as input and produce the same number of bits of 64-bits. The first step will be dividing the 64-bits (entrance of S-box) to 8-blocks of length (8-bits). Then convert the these blocks from the binary code to hexadecimal code. Then dividing the blocks into two chunks, Set the most significant chunks to the row of the AES-table, and set the least significant chunks to the column. The next step will be replacing the intersection of rows and columns with the numbers of lookup table figure (5-2).

Algorithm (3): Proposal S-box

Input: block of 64 bits.

Output: block of 64 bits with high confusion.

begin

1. Dividing 64-bits into 8-blocks of length 8-bits.

2. Convert the blocks from binary to hexadecimal code.

3. Dividing the first block into two chunks.

4. Consider the row as the most significant chunk of the hexadecimal block and set the column as the least significant chunk.

5. Replace the numbers of row and column with the intersection of these numbers of the lookup table.

6. Repeat the steps 3,4,5 to each block along (64-bits), and construct a hexadecimal sequence.

7. Return the hexadecimal sequence to the binary sequence.

End.

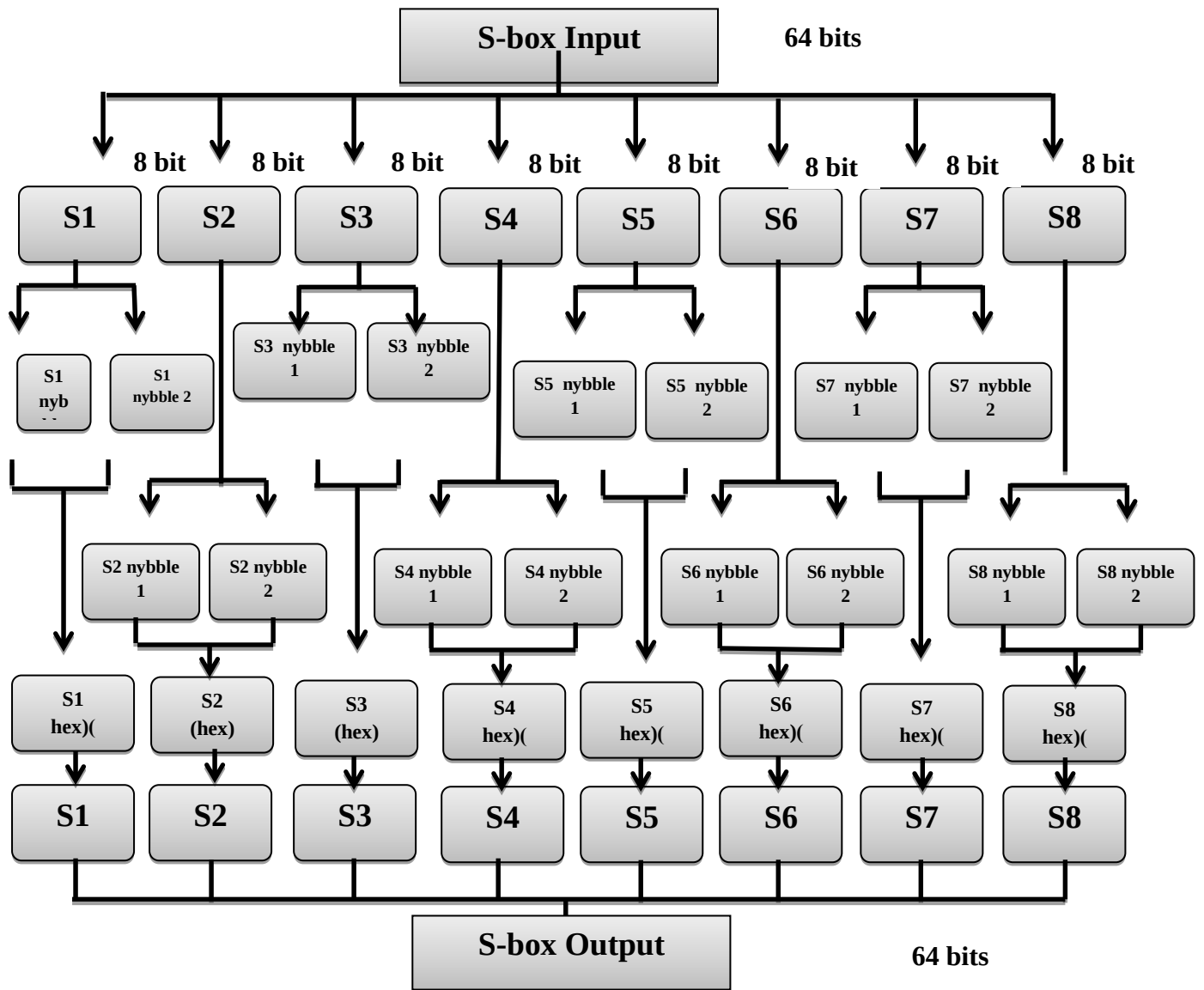


Fig. (5-2): AES S-box Lookup Table [5]

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Note: Must using the same lookup table in the S-box and S-box inverse. It will reverse the steps in S-box inverse to retrieving the 64 bits.

4- Proposal Permutation Function (P-Function)

In the proposal, the permutation function of LOKI97 algorithm has been improved. The proposal permutation function has 64-bits as the entrance to its function. The first step will split the input block into 16-blocks (4-bits), and then converted them to a matrix of (4*4). The second step is taking the even-row, and apply left shifting on each block according to the ones in these block (if the numbers of ones in the block is one, so shifting the bits in the block once, if the ones is two, the shifting will be twice and so on), this is for the even-rows. Regarding to the odd-rows, the process of swapping will be on them, according to a specific plan, (set the first block of a second-row as a control switch to the swapping process of in the first row, if the number of ones is zero or one, no swapping will occur, if the numbers of ones is two, the first block will be swapping with the second block, if the ones is three, the first block will swapping with the third block and so on). The previous process will be apply on the third-row also, (while setting the second block of the second-row as a control switch to the third-row), that is presented as following:

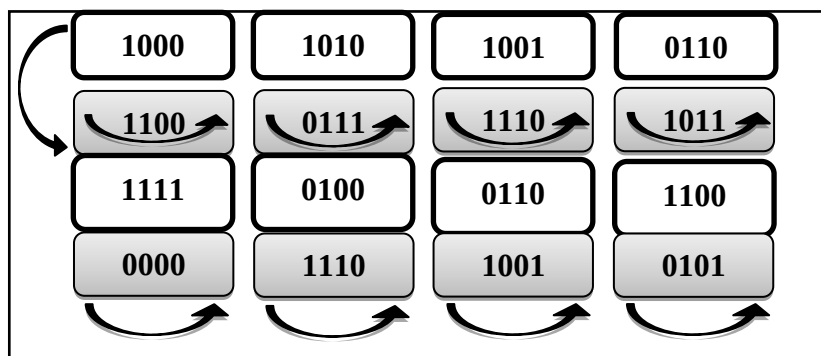


Fig. (6-1): The matrix input before processing

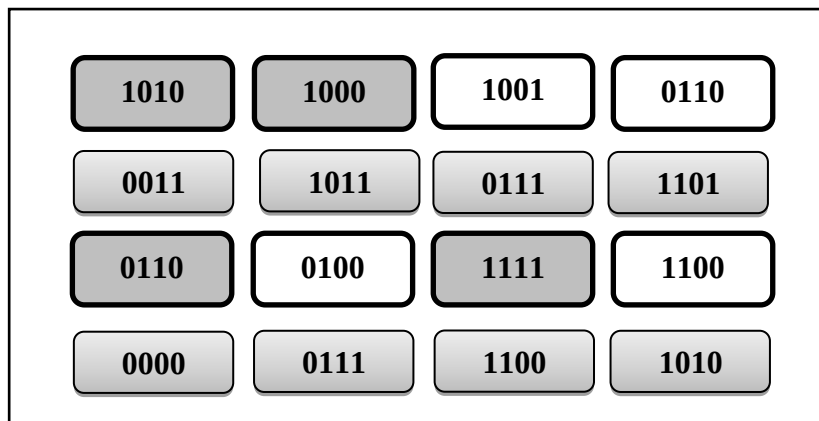


Fig. (6-2): The matrix input after shifting and swapping

Algorithm (4): Permutation function

Input: sequence A of 64-bits.

Output: sequence of 64-bits with high confusion.

begin

1. Dividing the A sequence into 16 blocks of length 4-bits.

2. Convert the blocks to a matrix of (4*4).

3. Applied the swapping process on the first block of the first and third row.

3.1 Set a control switch to make the swapping of two blocks (the second block is based on the ones in this control switch).

3.2 Set the first block of the second row as control switch to the first row.

3.3 Set the second block of the second row as control switch to the third row.

4. Applied the circular left shifting process on the even rows regarding to the ones in the same blocks.

End.

5- Proposal Swapping function

In the proposal of LOKI97 algorithm, there is an addition function, which is a swapping function. It has been takes two inputs A of (64-bits) and B of (32-bits), the first input was the output of the second layer of S-box, and the second input was a key. This function is similar to the keyed-permutation function in the LOKI97 standard. It will divided the A-input into two parts (left and right), and making a swapping between the bits of them depending on the bits of B-sequence. If the bit of B sequence is (one), so replace the bit from the left with bit of the right part, but if the bit of B sequence is (zero), the swapping doesn't occur. The figure (7) presented the swapping function.

Algorithm (5): Proposal Swapping function

Input: two sequences: A (64-bits), B(32-bits).

Output: one sequence with high diffusion.

Begin

1. Dividing the A-block into two parts (L, R).

2. for i = 1 to 32

2.1 if the bit of B-block = 1 then swapping the bit of L with the bit of R.

2.2 if the bit of B-block = 0 then no swapping.

2.3 next i

3. concatenating L and R

End

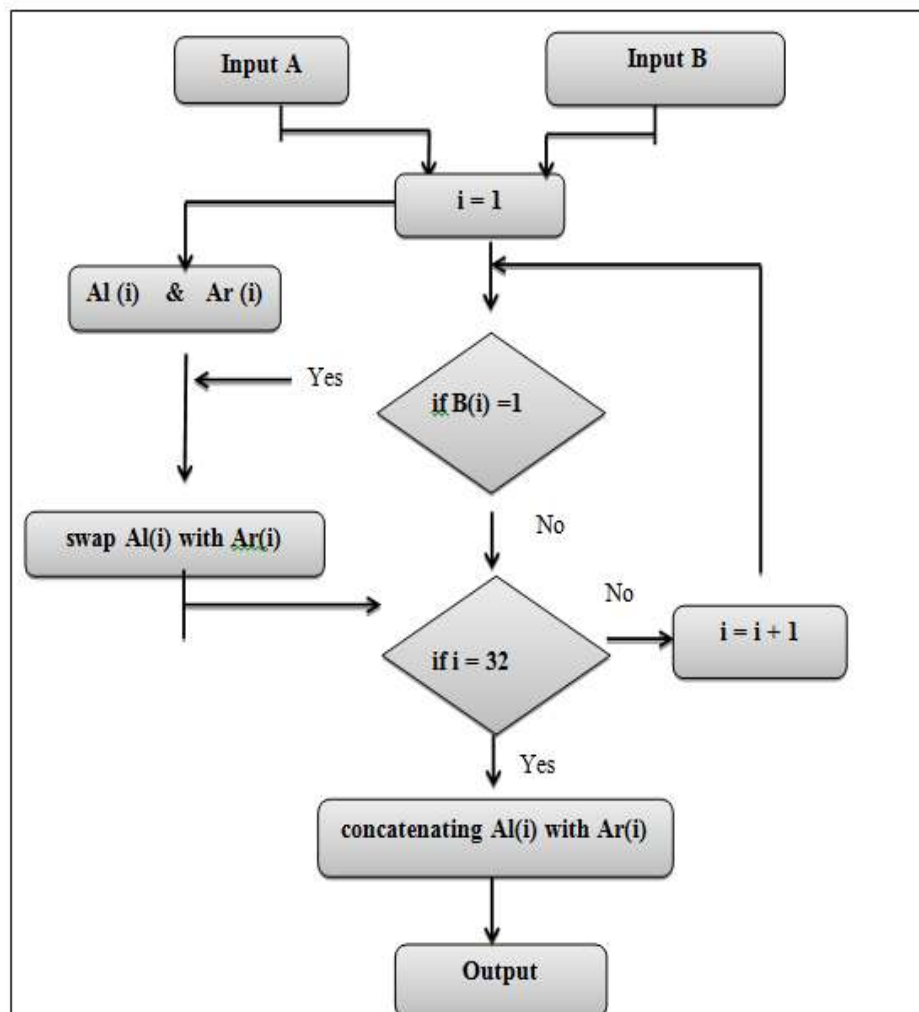


Fig. (7): Proposal swapping function

III. Complexity and Evaluation

As an evaluation of the proposed algorithm In compared with the LOKI97 standard, in this paper it have been used the same number of the rounds as the LOKI97 algorithm which is a 16 rounds and used the same input of (128-bits) of input block as plaintext and the cipher text, and also the same key length of 128-bit.

The main difference between the two algorithms, that the proposed use a 64-bits along the F-function. This is contrary to the LOKI97 standard, because it used the (expansion function), where it produces a 96-bits as an input to the first layer of S-box, but this expansion function is absent in the proposal, and it is replaced by (Circular left-shift function), that receive and produce 64-bits only.

Also, the S-box in the LOKI97 is used two S-boxes S1 and S2, consisting of two layers. In every layer used the S1 and S2 four times, but, in our proposal that used eight S-boxes [S1, S2, S3, S4, S5, S6, S7, S8], in also two layers. The proposed S-box function have received 64 bits as an input and produced 64 bits as an output. This means that the proposed S-box doesn't apply the compression in its work.

Besides that, the main function of LOKI97 consist of five sub-functions, to increase its complexity, the proposal have six sub-functions in the main F-function, where another function was added, which is the swapping function. Although the swapping function is similar in its content to the keyed permutation function in LOKI97 standard, but, in this case, it is considered as an extra function. In addition to that, the LOKI97 have using a static latin square pattern in permutation process, but the proposed permutation function have been more complex, because it using a mix of two processes (shifting and swapping) according to a specific plan. So, this will affect the properties of diffusion and making the proposal have high diffusion.

Regarding to the brute force attack, the LOKI97 standard used in F-function, one key of the size of 64-bits, so the brute force attack required (2^{64}) possible key. The proposed have the same complexity for the brute force attack is (2^{64}), because it used the same key size.

The run time of encryption is an evaluation scale. In this paper, it have been measured the run time of a proposed LOKI97 algorithm, by encrypt a block cipher of 128 bits of 5KB file, 10KB file, 15KB file and 20KB file, as shown in table (1).

Table (1) The run time of a proposed LOKI97 algorithm

Text Size	Proposal LOKI / in second
5K / Sec	5
10K / Sec	9
15K / Sec	15
20K / sec	20

another evaluation scale in this paper have been used is a five statistical tests (randomness tests) to check the randomness. Using a block cipher (cipher text) of 128 bits and then check the results with the LOKI97 standard. The following table (2) was shown the results.

Algorithm	Frequency Test ≤ 3.84	Serial Test ≤ 7.81	Poker Test ≤ 11.1	Run Test ≤ 13.784	Correlation Test ≤ 3.84
Proposed LOKI97	Pass = 0.633	Pass= 0.891	Pass=1.975	Pass =12.032	Pass = 0.469
Standard LOKI97	Pass = 0.001	Pass = 0.750	Pass = 3.225	Pass = 10.688	Pass = 2.343

IV. Conclusion

In this paper, it have been presented a new approach to develop an aspect of the LOKI97 standard, which is the main F-function, to provide a higher confusion and diffusion. The new design have been used 128-bit of a plaintext, and a key length of 265-bit as that in the LOKI97 standard. Although the absence of the expansion function from the main F-function of LOKI97 standard, this is doesn't affect the strength of the proposed algorithm, because it is replaced by two functions. The proposal have solved the weakness of the (static) permutation function in LOKI97 algorithm, by a more efficient function (dynamic), which a mixing between (shift and swapping processes). Also proposing a development of Loki97 that consist of the following functions (keyed-permutation, circular left-shift, two layers of s-box, swapping function) and resulted a new developing F-function with high confusion and diffusion.

References

- [1] Bruce Schneier, "**Applied Cryptography**". Second Edition, 1996.
- [2] Ayushi., "**A Symmetric Key Cryptographic Algorithm**". International Journal of Computer Applications (0975 - 8887), Volume 1 – No. 15, 2010.
- [3] Huy Hoang Ngo, Xianping Wu, Phu Dung Le, Campbell Wilson, and Balasubramaniam S., "**Dynamic Key Cryptography and Applications**", International Journal of Network Security, Vol.10, No.3, PP.161-174, May 2010.
- [4] Lawrie Brown, Josef Pieprzyk, "**Introducing the new LOKI97 Block Cipher**", 1997.
- [5] Yasser Ali Yasser, "**Improve E-Services Security Level by Modifying AES Algorithm**", 2016.

New Block Cipher Algorithm Depend on Hybrid Operation

Assist. Prof. Dr. Alaa Kadhim Ghadah Ali
University of Technology/ Computer science department
ghadahali.23@yahoo.com

Abstract:

The allocation of frequencies in some languages is famed for the message therefore these information can be used to break a cryptographic algorithm by cryptanalysis system, that require strength cryptographic method to product the message, serpent algorithm is a block cipher algorithm put it break. In this paper, the algorithm improved by use principals of loki97 and Advanced Encryption Standard (AES) techniques to design a new structure for serpent algorithm, this make algorithm more complexity because of the principal of confusion and diffusion of loki97, AES techniques where the confusion and diffusion are the power point of the block cipher algorithm. This design use 512-bits as plaintext also the cipher text will be 512-bits that make the time that used for the proposal algorithm is less than the standard serpent algorithm.

Keywords: serpent algorithm, loki97 (f) function, block cipher, AES

تصميم جديد لخوارزمية التشفير الكتلي اعتماداً على عدة عمليات
ا.م.د. علاء كاظم غاده علي عبيد

المستخلص

ترددات الحروف تكون معروفة في بعض اللغات. وبالتالي يمكن استخدام هذه المعلومات لكسر خوارزمية التشفير من قبل المهاجم. مما يتطلب، طريقة تشفير قوية، عنصراً الارتباك والنشر هما نقطة قوة خوارزمية التشفير. وتعتبر خوارزمية Serpent هي إحدى خوارزميات نظام التشفير الكتلي ولكن قد تم كسرها. في هذا البحث تم تحسين هذه الخوارزمية باستخدام تقنيات مبادئ loki97 وتقنيات التشفير الحديث AES لتصميم هيكلية جديدة لخوارزمية Serpent. وهذا ما يجعل الخوارزمية الناتجة أكثر تعقيداً بسبب خصائص النشر والارتباك العالية. في هذا التصميم تم استخدام 512-bits كنص صريح ونص مشفر. وهذا ما يجعل الوقت اللازم لتنفيذ هذا التصميم المقترح هو أقل من الوقت المطلوب لتنفيذ الخوارزمية الأصلية.
الكلمات المفتاحية: خوارزمية Serpent، دالة loki97، التشفير الكتلي، AES.

I. Introduction

The concern of unauthorized access or fake changes, that require to protect the sensitive information from this concern. Where the important data can be obtained by connect over networks. This can be addresses by cryptology. Cryptology can be divided into: Cryptography which is encryption itself, while cryptanalysis that is the breaking of cryptosystems [1]. The problem of cryptography is that insecure channel. The symmetric key method is the solution to this trouble [2].

1- Block cipher

The principal of block cipher method is that a numbers of bits of plaintext change to new numbers bits. In this method, random and reversible relationship between the plaintext and the cipher text. So, one-to-one relationship, this mean that only one block cipher for each block of plaintext [3].

1-1 The Advanced Encryption Standard

AES is an algorithm of the block cipher, it use 128-bits as input plaintext and 128, as key. There is 10 round that the algorithm included can be also include 12 or 14 rounds depended on key length as 192 or 256-bits key this mean for each number of round have its key length. All rounds are similar except the last round. Each round consist four function S-box based substitution step, Shift-row permutation step, Mix column mixing step, and Add round key. For encrypt and decrypt processing this function are different executed. [4].

1-2 LOKI97

Introduction

LOKI97 is a block cipher algorithm this algorithm consists about 16 rounds that used 128 bits as plaintext. It's have been used a complex non-linear function f, the master key is 256-bit key that can be started as 128 or 192 keys also. It enhancement for the LOKI89 and LOKI91, with complexity design [5].

1-3 Serpent

The serpent is a block cipher algorithm that used a 128 bit as input plaintext and a 256 bit as master key. The algorithm formation of three main functions. These functions are an initial permutation of bits was named the (IP), a round function was named R, and a final permutation of bits named FP. The initial permutation of bits is often performed by the table lookup to decide which bit to put in the position. The round function have been performed 32 times on B_i (it will start with B_0). In every round of this function, B_i is firstly mixed with one key of the 32 keys and then pass into one of eight S-Boxes 32 times in parallel. In each rounds except the last round, it is then applied to a linear transformation and produce (B_{i+1}) . In the last round, instead of performing the linear transformation, the text is mixed with an additional 33rd key. A final permutation of bits is applied to put the bits back into the correct position [6].

1-4 Diffusion

Basing on the suggestion of Claude Shannon, that the statistical attacks to be complicated, the cryptographer could be wasted the statistical structure of the plaintext in the long range statistics of the ciphertext. This process named a diffusion. The diffusion making the statistics of the ciphertext more complicated, and makes it difficult to detect the key of the cryptographic process [7].

1-5 Confusion

The confusion process making the use of the keys more complex, that even when an adversary knows the statistics, it is still difficult to deduce the key. The confusion could be achieved by the using of complex substitution process [7].

2- The Proposal Method

In proposal design 512-bits used to input block as plaintext, 256-bits as master key and 64-bits as secondary key, this design consist of loki97 (f) function, a Round Function, invers loki97 (f) function.

The plaintext (512-bits) divided into four 128-bits blocks each one with 64-bits key are inserted in loki97 (f) function the output is 64-bits from each loki97 (f) function then we will marge each two blocks to obtain two 128-bits blocks this blocks will be processed in 8 round.

Each round have left (L) and right (R) side functions and 256-bits key. in The right side (R) have 128-bits passed through one of eight S-Boxes, it is then subjected to a linear transformation, the output mixed with 128-bits key via XOR operation also the left side (L) is work in parallel, it have 128-bits that is mixed with 128-bits key via XOR operation the output shifted by using shift-row function that belong to AES after that reordered in (IP) initial permutation function for each round except the last round the left and right blocks are swapped, $L_i = R_{i-1}$ & $R_i = L_{i-1}$.

After the last round finished the right and left blocks divided into two 64-bits blocks each block with 64-bits key are passed through invers loki97 (f) function to get 128-bits this blocks marge to get 512-bits as cipher text from this proposal. Can explain the proposal design in the figure (1) and below algorithm:

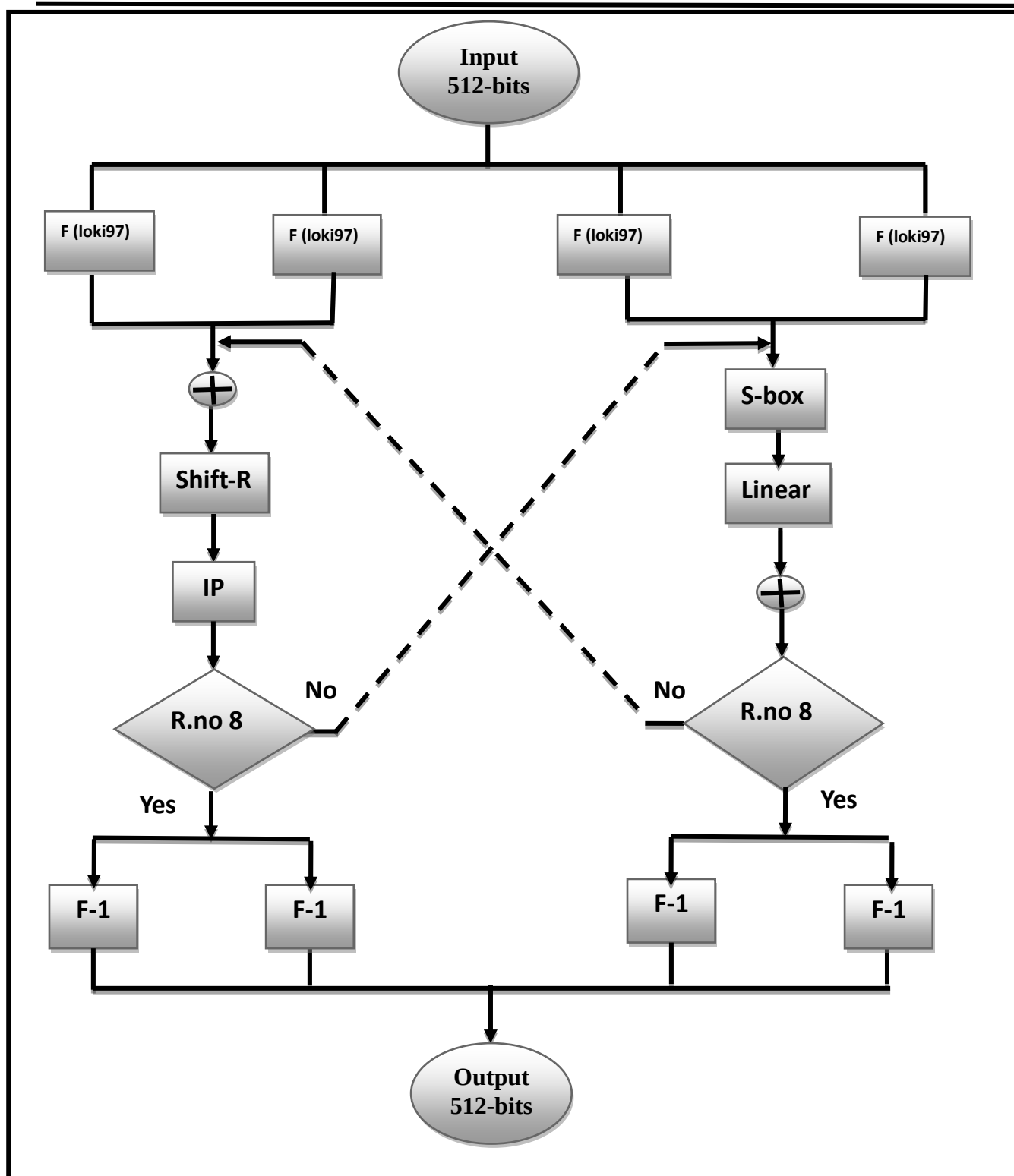


Fig. (1): The proposal Serpent Algorithm Structure

3- The new proposal loki97 (F) Function

In the F (loki97) function 128-bits plaintext and 64-bits key as input, the plaintext divided into left

Algorithm: serpent algorithm proposal

Input: plaintext = 512-bits, K1 = 265bits, K2 = 64-bits

Output: ciphertext = 512-bits

Process:

1. (Key schedule) Compute thirty-two 128-bit round keys K_i , from K
2. Plaintext divided in to $\rightarrow (LL, LR, RR, RL) \rightarrow$ loki97 (F) (for each block)
3. LL and LR marge to get L as well as the RR and RL marge to get R
4. (8 rounds) for i from 1 to 8, compute L_i and R_i as follows:
 - 4.1 $L_i = (IP(\text{Shift-R}(L_i \text{ XOR } K_j))) \dots \dots \dots$ (where $j=1$)
 - 4.2 $R_i = (K_j + 1 \text{ XOR } (\text{linear}(S\text{-box}(R_i))))$
 - 4.3 If $i < 8$ then $L_i + 1 = R_i$, $R_i + 1 = L_i$
5. $(L \rightarrow (LL, LR), R \rightarrow (RR, RL)) \rightarrow$ invers loki97 (F)..... (for each block)
6. LL & LR & RR & RL $\rightarrow$ 512-bits as ciphertext

64-bits block and right 64-bits block.

The left 64-bits block and the 64-bits key are passed into (KP) function also the right 64-bits block mixed with 64-bits key by using (XOR) operation, the output of (KP) will be mixed with copy of the output of right 64-bits.

The output of this will be passed into (Mixcolumn) function, this function belong to advance encryption stander (AES), copy of the output of (Mixcolumn) function will mixed with the output of right 64-bits block by (XOR) operation the output of this operation are saved for the invers loki97 (F) function. The output of the (Mixcolumn) function passed into the (P) function to get 64-bits as output from the loki97 (F) function. Can explain in the following figure:

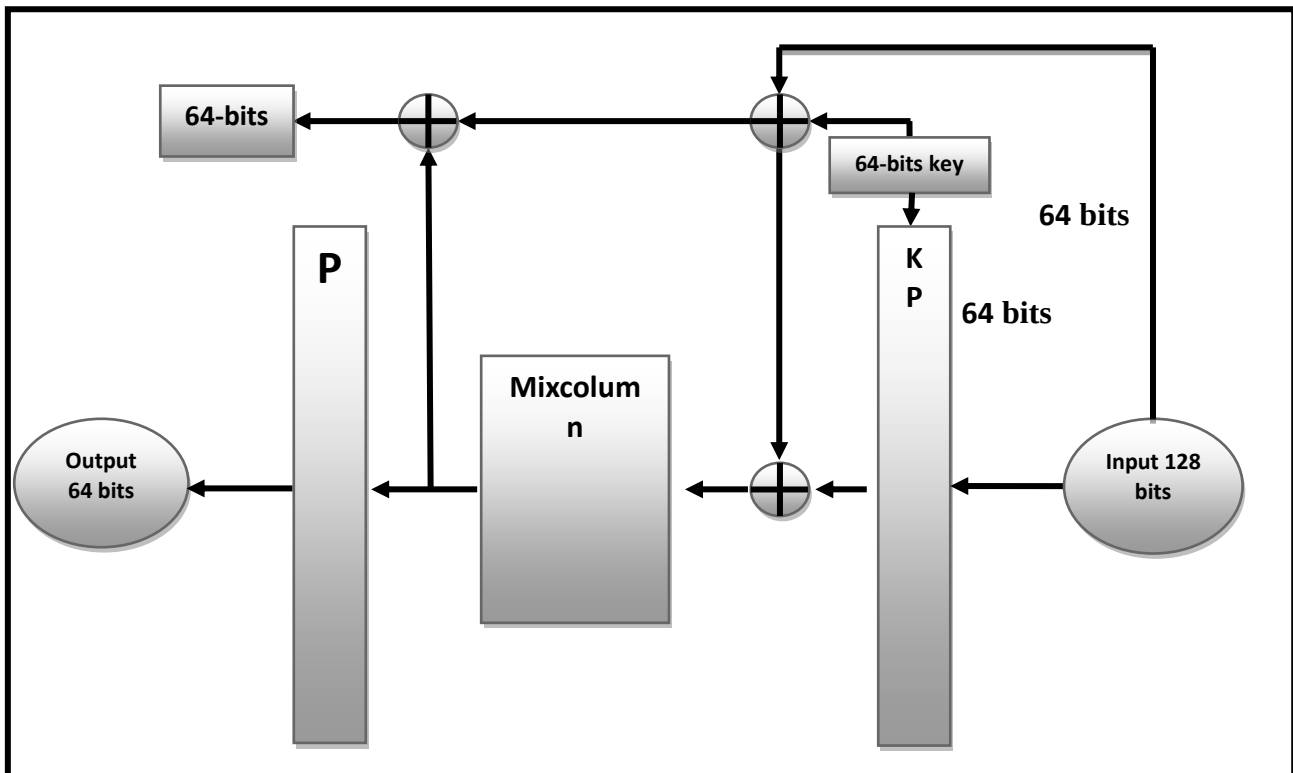


Fig. (2): The proposal loki97 (F) function

3-1 The Initial Permutation

The cryptographic doesn't applied on the initial and final permutations. They are used to simplify an optimized implementation of the cipher. Both these two permutations and the linear transformation are to increase complexity [8]. Can explain the initial permutation and final permutation in the following figures:

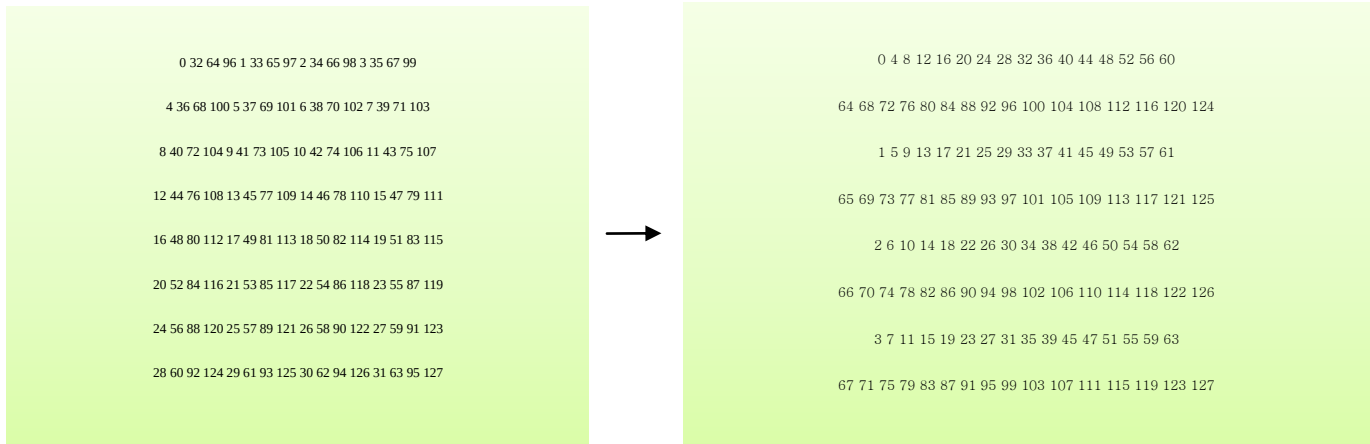


Fig. (3): The initial and final permutations

3.2 The S-box

The set eight S-boxes are used four times. Thus after using S7 in round 7, we use S0 again in round 8, then S1 in round 9, and so on. The last round R31 is slightly different from the others, apply S7 on $\wedge B_{31}$ XOR $\wedge K_{31}$, and XOR the results with $\wedge K_{32}$ rather than applying the linear transformation. The result $\wedge B_{32}$ is then permuted by FP, giving the cipher text. Thus the 32 rounds use 8 different S-boxes each of which maps four input bits. Each S-box is used in precisely four rounds, in each of these it is used 32 times in parallel [8]. Can explain the in the following figure.

$S_0 = 8\ 8\ 15\ 1\ 10\ 6\ 5\ 11\ 14\ 13\ 4\ 2\ 7\ 0\ 9\ 12$	$IS_0 = 13\ 3\ 11\ 0\ 10\ 6\ 5\ 12\ 1\ 14\ 4\ 7\ 15\ 9\ 8\ 2$
$S_1 = 15\ 12\ 2\ 7\ 9\ 0\ 5\ 10\ 1\ 11\ 14\ 8\ 6\ 13\ 3\ 4$	$IS_1 = 5\ 8\ 2\ 14\ 15\ 6\ 12\ 3\ 11\ 4\ 7\ 9\ 1\ 13\ 10\ 0$
$S_2 = 8\ 6\ 7\ 9\ 3\ 12\ 10\ 15\ 13\ 1\ 14\ 4\ 0\ 11\ 5\ 2$	$IS_2 = 12\ 9\ 15\ 4\ 11\ 14\ 1\ 2\ 0\ 3\ 6\ 13\ 5\ 8\ 10\ 7$
$S_3 = 0\ 15\ 11\ 8\ 12\ 9\ 6\ 3\ 13\ 1\ 2\ 4\ 10\ 7\ 5\ 2$	$IS_3 = 0\ 9\ 10\ 7\ 11\ 14\ 6\ 13\ 5\ 12\ 2\ 4\ 8\ 15\ 1$
$S_4 = 1\ 15\ 8\ 3\ 12\ 0\ 11\ 6\ 2\ 5\ 4\ 10\ 9\ 14\ 7\ 13$	$IS_4 = 5\ 0\ 3\ 3\ 10\ 9\ 7\ 14\ 2\ 12\ 11\ 6\ 4\ 15\ 13\ 1$
$S_5 = 15\ 5\ 2\ 11\ 4\ 10\ 9\ 12\ 0\ 3\ 14\ 8\ 13\ 6\ 7\ 1$	$IS_5 = 8\ 15\ 2\ 9\ 4\ 1\ 13\ 14\ 11\ 6\ 5\ 3\ 7\ 12\ 10\ 0$
$S_6 = 7\ 2\ 12\ 5\ 8\ 4\ 6\ 11\ 14\ 9\ 1\ 15\ 13\ 3\ 10\ 0$	$IS_6 = 15\ 10\ 1\ 13\ 5\ 3\ 6\ 0\ 4\ 9\ 14\ 7\ 2\ 12\ 3\ 11$
	$IS_7 = 3\ 0\ 6\ 13\ 9\ 14\ 15\ 8\ 5\ 12\ 11\ 7\ 10\ 1\ 4\ 2$

Fig. (4): S-box and S-box invers

3-3 Linear transformation

Linear is the linear transformation. Linear transformation the 32-bits in each of output words are linearly mixed, by the equation:

$X_0, X_1, X_2, X_3 := S_i (B_i \text{ (XOR) } K_i)$

$X_0 := X_0 \lll 13$

$X_2 := X_2 \lll 3$

$X_1 := X_1 \text{ (XOR) } X_0 \text{ (XOR) } X_2$

$X_3 := X_3 \text{ (XOR) } X_2 \text{ (XOR) } (X_0 \lll 3)$

$X_1 := X_1 \lll 1$

$X_3 := X_3 \lll 7$

$X_0 := X_0 \text{ (XOR) } X_1 \text{ (XOR) } X_3$

$X_2 := X_2 \text{ (XOR) } X_3 \text{ (XOR) } (X_1 \lll 7)$

$X_0 := X_0 \lll 5$

$X2 := X2 \lll 22$

$B_{i+1} := X0, X1, X2, X3$

Where $\lll$ denotes rotation, and $\ll$ denotes shift. In the last round, this linear transformation is replaced by an additional key mixing: $B32 = S7 (B31(XOR) K31) XOR K32$ [8].can explain in the following figure.

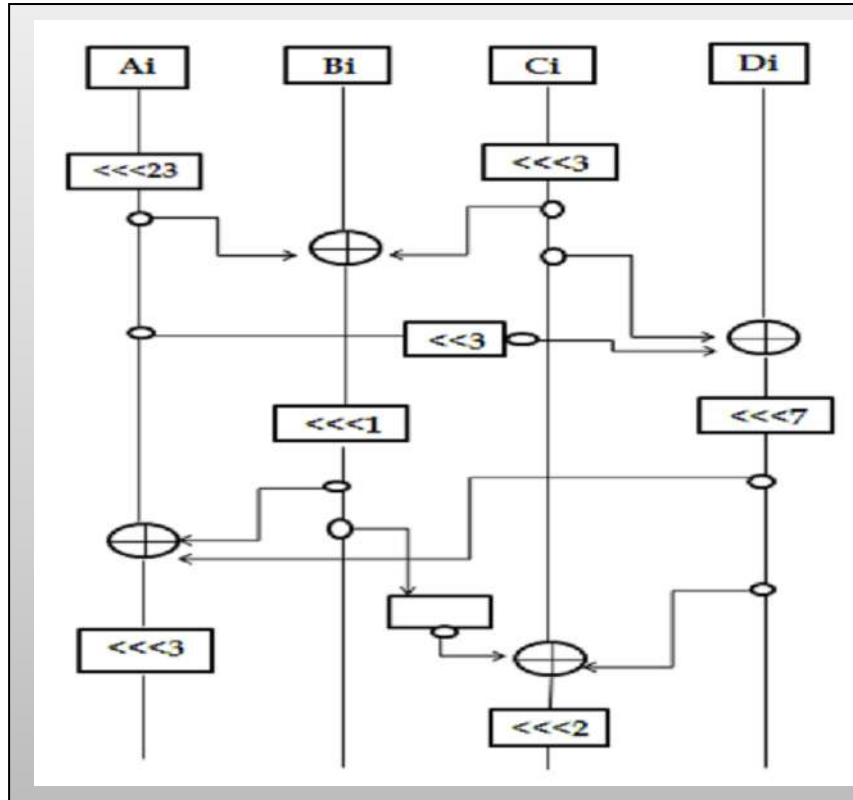


Fig. (5): Linear transformation function

3.4 Key Schedule

Our cipher requires 132 32-bit words of key material. we first pad the user supplied key to 256 bits, if necessary. We then expand it to 33 128-bit sub keys $K0 \dots K32$, we write the key the key K as eight 32-bit words $w-8 \dots w-1$ and expand these to an intermediate key (which we call pre key) $w0 \dots w131$ by the following affine recurrence:

$$W_i = (w_{i-8} XOR w_{i-5} XOR w_{i-3} XOR w_{i-1} XOR \phi XOR i) \lll 11$$

Where ϕ is the fractional part of the golden ratio $(\sqrt{5}+1)/2$ or 0x9e3779b9 in hexadecimal.

The round keys are new calculated from the pre keys using the S-boxes, again in bits lice mode [8].can used the S=boxes to transform the pre keys W_i into words K_i of round key in the following way:

$$\{K0, K1, K2, K3\} = S3 (W0, W1, W2, W3)$$

$$\{K4, K5, K6, K7\} = S1 (W4, W5, W6, W7)$$

.....

.....

$$\{K128, K129, K130, K131\} = S3 (W128, W129, W130, W131)$$

$$K_i = \{K_{4i}, K_{4i+1}, K_{4i+2}, K_{4i+3}\}$$

II. Complexity and Time

In the new design we used many different techniques as nonlinear and linear functions. In the proposal IP function used in each round, also used many another function (loki97 (F), shift row, Mix column) all these function used in proposal so the number of functions is more than the

original serpent, we use two different key in each round and use proposal function based on loki97 technics with different key, this make the new design more complexity than original serpent where the brute force attack need to try ($2^{2048} * 2^{64}$) key, the proposal consume time less than original serpent because used only 8 round and also used (F) function, that is a proposal function based on loki97 (f) function, this function shorthand block from 128-bits to 64-bits. Can explain the experiments the deferent in time by used many text files (6k, 12k, and 24k) for encryption and decryption operation, explain in the following table:

Table (1) Time Measure

Text size	Operation	Serpent in Sec	New proposal in Sec
6K	Enc	15	5
	Dec	34	8
12K	Enc	32	10
	Dec	68	15
24K	Enc	66	22
	Dec	149	30

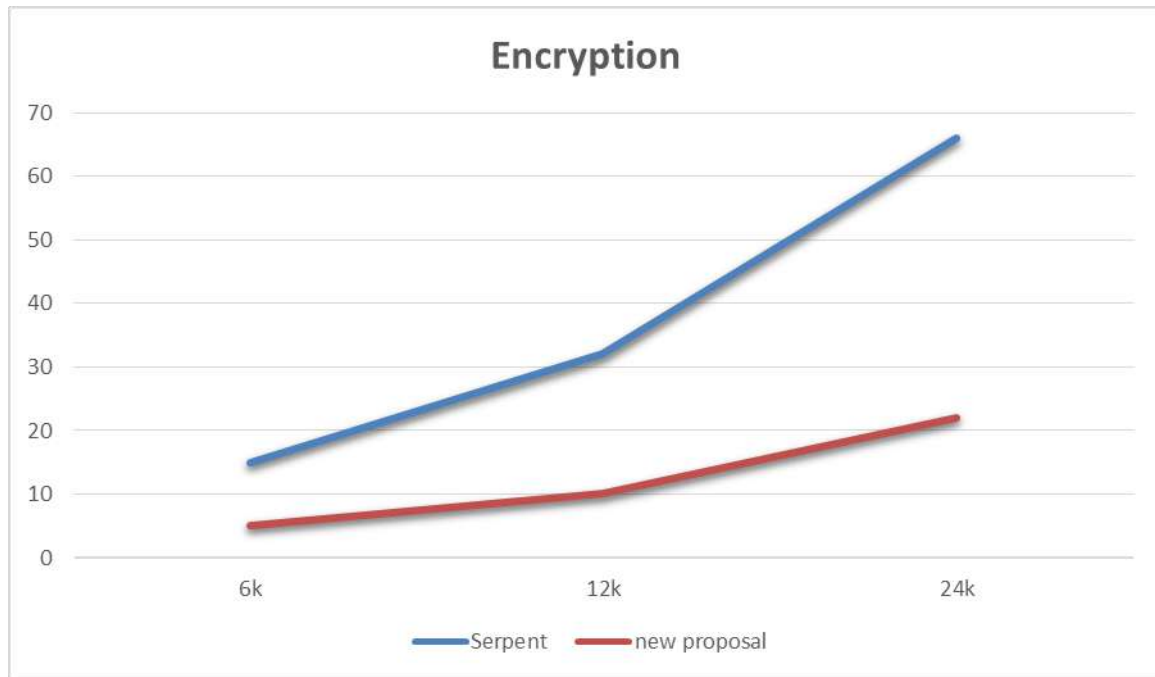


Fig. (6): Encryption Time

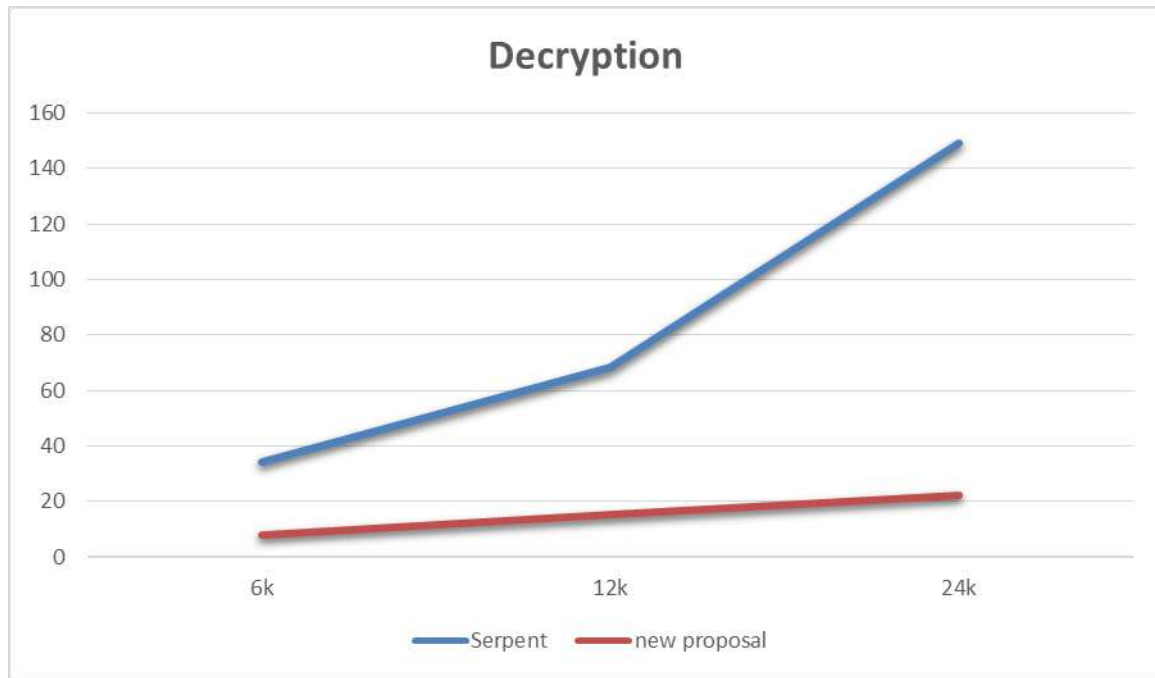


Fig. (7): Decryption Time

Also the results of applying the basic five statistical tests on the new proposal output (ciphertext), show the success of all tests, as shown in Table (2) and figure (8):

Table (2) Results of the Five Tests Applied to Standard Serpent and New Proposal

Basic Five Statistical Tests			Serpent	New proposal
Tests		Freedom Degree		
Frequency Test		Must Be ≤ 3.84	Fail=(5.231)	Pass =(0.008)
Run Test	T0	Must Be ≤ 12.309	Pass=(3.492)	Pass = (6.859)
	T1	Must Be ≤ 13.784	Pass=(9.901)	Pass = (4.781)
Poker Test		Must Be ≤ 11.1	Pass=(6.044)	Pass=(2.494)
Serial Test		Must Be ≤ 7.81	Pass=(7.334)	Pass=(0.031)
Auto-Correlation Test	Shift No. 1	Must Be ≤ 3.84	Pass=(0.314)	Pass=(0.159)
	Shift No. 2		Pass=(0.370)	Pass=(1.129)
	Shift No. 3		Pass=(0.000)	Pass=(0.018)
	Shift No. 4		Pass=(0.495)	Pass=(0.197)
	Shift No. 5		Pass=(0.714)	Pass=(0.857)
	Shift No. 6		Pass=(0.638)	Pass=(0.957)
	Shift No. 7		Pass=(0.319)	Pass=(2.156)
	Shift No. 8		Pass=(0.180)	Pass=(0.286)
	Shift No. 9		Pass=(0.080)	Pass=(0.718)
	Shift No. 10		Pass=(0.002)	Pass=(1.147)

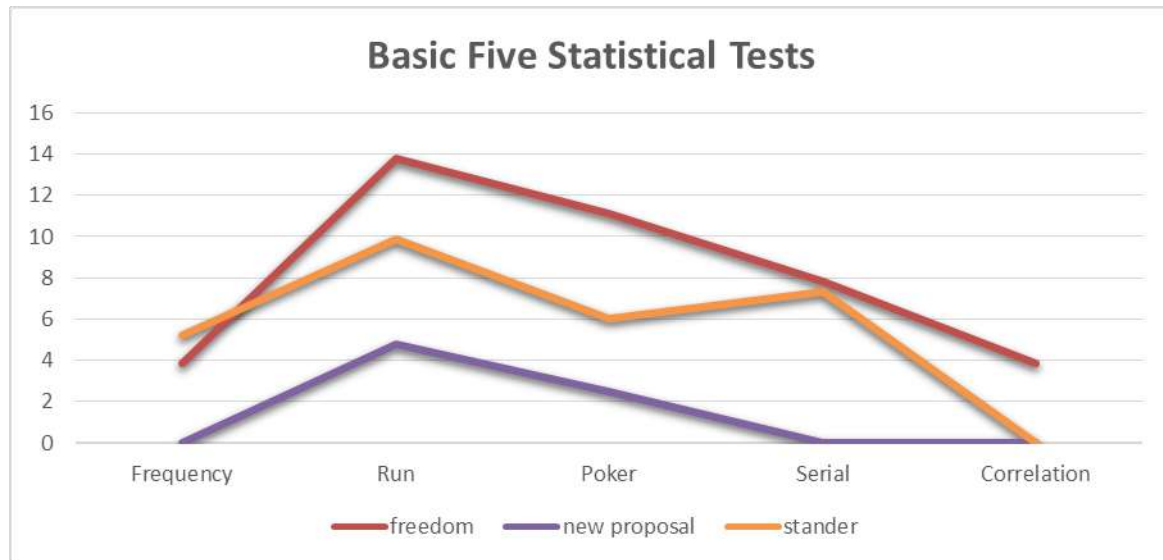


Fig. (3): Results of the Five Tests Applied to Standard Serpent and New Proposal.

III. Conclusions

The new approach of block cipher algorithm enhancing confusion and diffusion (use IP function in each round and proposal function) that are standard block cipher and the numbers of keys that make new approach of block cipher algorithm more complexity degree against the attacker task. Also the new approach of block cipher algorithm decrease the time that need for execution that increase it fast and can used in real time encryption depending on numbers of round.

References

- [1] C. A. Henk., "**Fundamentals Of Cryptology**". Eindhoven University of Technology, the Netherlands, Kluwer Academic Publishers Boston/Dordrecht/London, 2006.
- [2] Shafi Goldwasser and Mihir Bellare, "**Lecture Notes on Cryptography**", Cambridge, Massachusetts, July 2008.
- [3] Avinash Kak, "**Block Ciphers and the Data Encryption Standard**", Purdue University, January 2017
- [4] Avinash Kak, "**The Advanced Encryption Standard**", Purdue University, February 2017.
- [5] Lawrie Brown, Josef Pieprzy, "**Introducing the new LOKI97 Block Cipher**", University of Wollongong, Wollongong, NSW 2522, Australia, June 1998.
- [6] Ross Anderson, Eli Biham and Lars Knudsen, "**Serpent: A Proposal for the Advanced Encryption Standard**". Cambridge University, England, Technion, Haifa, Israel, University of Bergen, Norway. 1998
- [7] William Stallings, "**Confusion and Diffusion**", Prentice Hall, 2003.
- [8] Dr. Alaa Kadhim, M.Sc. semaa, israa and gada, "**new approach for serpent block cipher algorithm based on multi techniques**". Iraqi information technology magazine, 2017.

Chaos and OcTree based for Multiple Image Encryption

Jolan Rokan Naif Shymaa Mohammed Jameel
University of Information Technology and Communications
Informatics Institute for Postgraduate Studies
newjolan@gmail.com

Abstract:

An encryption technique proposed to cipher the private and secure (2D-3D) colored image for secure data transmission through the Internet. This propose technique was contain the Lorenz and Rossler keys generation encryption. There are three steps used in the proposed encryption technique based on (coding and encryption): Coding (using OcTree), key generation(using chaos Lorenz and Rossler), and encryption (using AES and Xor). A good time in operation with a good visual encryption view was get from implement the proposed technique with standard processing time and accepted measurements.

Keyword: image encryption, chaos encryption, chaos key generating, image coding, OCTree.

د. جولان روكان نايف شيماء محمد جميل

المستخلص

تقنية مقترحة تستخدم لتشفير الصورة الخاصة والسرية (ثنائية -ثلاثية الابعاد) لاجل نقل معلومات أمن في شبكة الانترنت. هذه التقنية المقترحة احتوت على مولد مفاتيح التشفير باستخدام لورنز وروزلر. ثلاث مراحل اقترحت ضمن الطريقة لاجل التشفير والترميز لاكمال تشفير الصورة الخاصة: الترميز (باستخدام التشجير الثماني (OcTree))، توليد المفاتيح (باستخدام الفوضوية ل لورنز وروزلر، والتشفير (باستخدام خوارزمية التشفير القياسية المطورة (AES) والدالة المنطقية (XOR)). نتائج جيدة في التشفير المرئي حصلنا عليه من تنفيذ الطريقة المقترحة وبوقت قياسي ونتائج مقاييس مقبولة.

الكلمات المفتاحية: تشفير الصور، التشفير الفوضوي، توليد المفاتيح الفوضوية، ترميز الصورة، التشجير الثماني.

I. Introduction

The growth of internet services technology makes easier to get transferred image passing in networks to specific service and applications. Digitals services obtain user conveniences, in the other side, its obtain attackers and illegal users chance to changing and modification. The is encryption methods are more powerful techniques to protect the images with different algorithms and numerical system like chaotic encryptions. [1]

The digital image security contains different approaches such as copyrights protections, authentications, confidentiality's and accesses controls. otherwise, confidentiality's and accesses controls are gathered by encryptions. only authorizer user has the decryption keys can be accessing the protected content(encrypted). [2]

Zhang et. al. suggested an image protection based on the encryption techniques using the improving DES and the chaos.

The logistic chaos sequencer proposed to use in generation the pseudo-random sequences to encrypt the RGB. Improvement DES used also to encrypt the image in double time encryption processing. There proposed has high encryption speeds, with high securities properties and keys sensitivity. [3]

Some mathematical random number generator used in encryption key generation as a component of the encryption systems. In [4] suggest an n-array key streams generators from multiple maps. The key generator designed based on hierarchical collection of 3-chaos maps. These chaotic equations system were used to produce key sequences have streams behavior with powerful statistical measurements and characteristics in order to prevent some various attacks methods and tools. [4]

In the paper, an image encryption system was proposed to protect different images using the combination of the encoding technique (Ocree) and (AES and XOR) encryption techniques feed by keys from two chaotic maps (Lorenz and Ressler) key generators.

II. Image Encryption [2,5]

Multimedia data encryption is not soft and easy depending on the multimedia types and content and encryption algorithms. Some algorithm used until today like Data Encryption Standard DES, Advanced Encryption Standard AES, and Ideal Data Encryption Algorithm IDEA.

These conventional cryptographic algorithms have some clear limitations for multimedia applications. Firstly, they require a lot of computational resources which can be feasible in desktop computers but difficult in low power wireless channels. Secondly, delay is introduced in real time communications using these block based encryption techniques. Thirdly, encrypting the image in spatial domain with these techniques prevents the use of certain advanced processing operations which can be easily implemented in transform domain. Lastly, these conventional encryption algorithms do not consider the structural and statistical properties of multimedia data as they were initially developed for text data. Several other encryption techniques like SCAN based, chaos based, optics based methods are proposed in the literature.

Due to the use of encryption or decryption process of multimedia contents, its speed is often critical in real time applications.

In order to make encryption system useful in real time communication is the use of partial encryption providing a certain degree of transparency. Selective encryption is also the requirement of many applications like Pay-TV or IP network, as confidential/total encryption of visual data is not required in such applications. Instead, it requires the content to be transparent to a certain extent to attract possible customers by providing a low quality version of multimedia content.

Only a subset entire data can be encrypting not all data just sensitive parts of data. The subset should be chosen in such a way that it introduces a desired level of degradation in the multimedia data.

A selected portion encryption of the multimedia data stream decreases the computational complexity and time load. Selective encryption helps in reduced the computational complexity, but not to maximum security.

III. OcTree Decomposing

In this type of tree, there are eight children's (at maximum) in every node. An octant is called for each node in octree and each octant without any child called leaf. but the root is the node without parent. Siblings is an octant with the same parent.

Grandchildren, octant's children and other indicate to octant's descendants and may be acts as an ancestor of its descendants.

The octant depth from the root node indicate to be location levels. The root node tree is located at level 0, while their children are locating at one level higher than the parent.

Partitions cuboidal and rectangular regions can perform by using Octrees. The tree domain composed from these regions. An octants set can be acts as complete if the regions unions collected by them covers the entire domain. The leaf nodes complete list is stored ca be used to reduce costs of the storage and called linear octrees.

In linear representation the octants locational codes must identify. A locational code ca be defining as the code that contains the position and octant level in the tree[6].

Figure 1 shows an example of OcTree structure.

IV. The Proposed System

The aim of this paper is to design and implement an image encryption system based on the Octree coding and the chaos key generation stages. The proposed system builds from two three stages (as shown in Figure (2)):

- a. **First stage:** applied the OcTree to loaded image in order to encoding the private image and extract the OcTree parameters. There are many possible data structures for a given OcTree and many parameters can be used in OcTree like the finest OcTree S_h^0 is nested in any other OcTree discretization of Ω , OcTree collection of discretization points x_j . The Octree is stored as a sparse d dimensional array S. The relative size is (h_j) of each cell is stored in the upper left corner of the cell.
- b. **Second Stage:** encrypted the encoding parameters resulted from OcTree algorithm for private image by using the Lorenz chaos key generation and XOR operation.

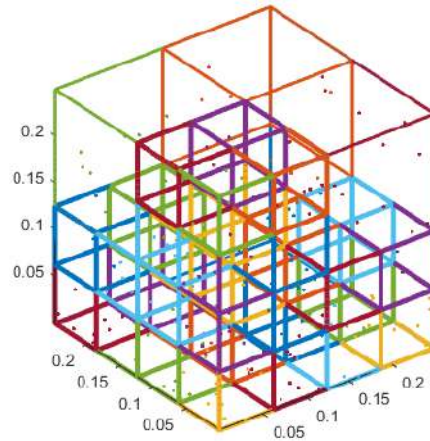


Fig.(1): OcTree example of Decompose 200 random points into bins of 20 points or less, then display each bin with its points in a separate color.

The Lorenz chaos key generation used the Lorenz equations:

$$\left. \begin{aligned} \dot{x}(t) &= \sigma(y(t) - x(t)) \\ \dot{y}(t) &= x(t)(\rho - z(t)) - y(t) \\ \dot{z}(t) &= x(t)y(t) - \beta z(t) \end{aligned} \right\} \dots(1)$$

where the parameters - model parameters $[\sigma, \rho, \beta]$ and was used to generate the encryption key. The encryption operation for this stage is by using the XOR logic gate.

c. **The third stage** is encrypting the resulted parameters from the stage two and whole resulted trees by using the AES algorithm. In this stage, the AES key will have generated by using the Rossler chaos key generation to used in the AES algorithm.

The Rossler chaos key generation used the Rossler equations:

$$\left. \begin{aligned} \dot{x}(t) &= -y(t) - z(t) \\ \dot{y}(t) &= x(t) + a y(t) \\ \dot{z}(t) &= b + z(t)(x(t) - c) \end{aligned} \right\} \dots(2)$$

The OcTree encoding method was used due to ability of this method to coding 2D and 3D images without error and with high speed efficient coding representation. The proposed system will work efficient with two types of image (2D and 3D) but the encoding in 3D images have a little time more than 2D images type.

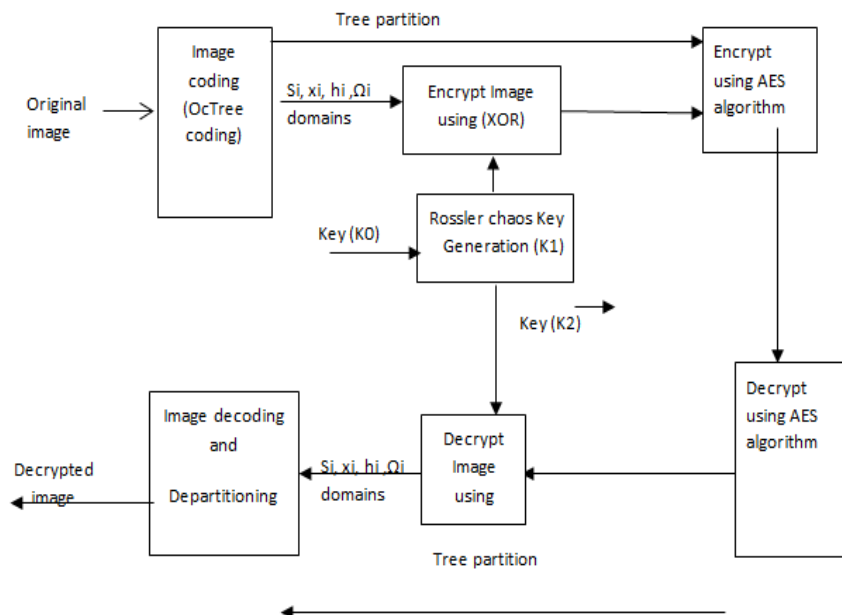


Fig. (2): The proposed Image Encryption System

The AES is extended to support a key stream generator for image encryption which can overcome the problem of textured zones existing in other known encryption algorithms. Figure 5 shows the block diagram of the proposed system. The steps of the proposed system are:

The encryption phase:

- Loading the colored image and extract image: size, length, width, no. of color depth, and name.
- Image coding using OcTree algorithm.
- Encrypt the coding parameters (X_i , Ω_i , S_i , and h_i) for each space using the Lorenz chaos key generation and XOR logic gate.
- Encrypt the whole coding trees with parameters (encrypted in the above step) using AES algorithm with 128 bit key generated by Rossler chaos system.
- Display the resulted image and save it.

The Decryption Phase:

- Loading the secure image and extract image: size, length, width, no. of color depth, and name.
- Decrypt the whole coding trees with parameters using AES algorithm with 128 bit key generated by Rossler chaos system.
- Decrypt the coding parameters (X_i , Ω_i , S_i , and h_i) for each space using the Lorenz chaos key generation and XOR logic gate.
- Image decoding using OcTree algorithm.
- Display the resulted image and save it.

V. Results

Some results of the proposed system are as show in figure 3, 4 and 5. The encryption time calculation is as shown in table 1.

Table (1) The encryption time results

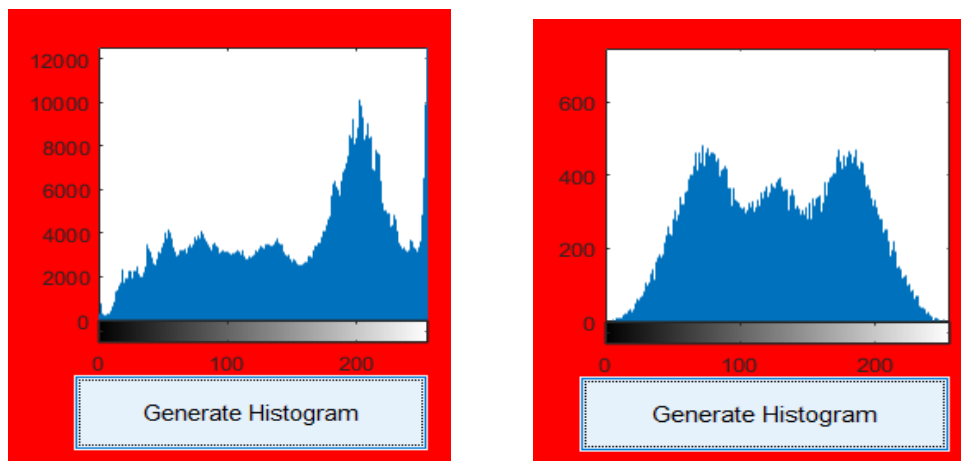
Image Sample	Image Size	PSNR (db)	Encryption Time
Sample 1	1280 ×800	9.13	3.203sec
Sample 2	600×442	11.15	1.082sec
Sample 3	980×880	5.89	2.119sec
Sample 4	1280 ×800	10.78	3.451sec
Sample 5	1280 ×768	12.67	3.312sec
Sample 6	512×512	10.90	0.980sec



(a) original image (b) Encrypted Image by XOR (Stage 2)



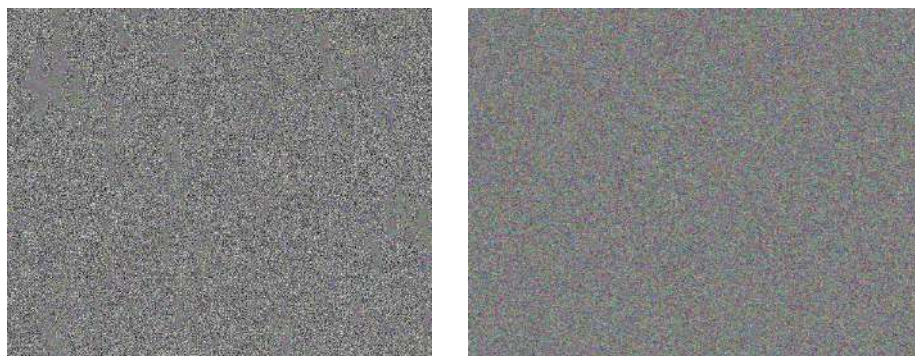
(b) Encrypted Image (Stage 3) (c) Decrypted Image



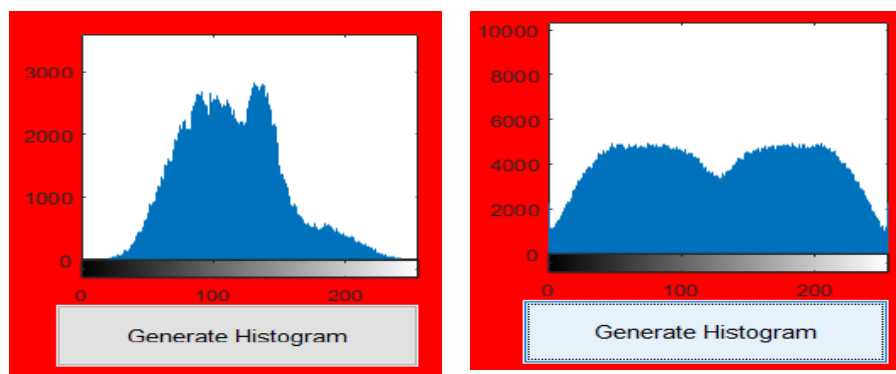
(d) Original Image Histogram (e) Encrypted Image (Stage 3) Histogram
Fig.(3): Some Result of The proposed system



(a) original image(b) Encrypted Image by XOR (Stage 2)



b) Encrypted Image (Stage 3) (c) Decrypted Image



(d) Original Image Histogram (e) Encrypted Image (Stage 3) Histogram
Fig.(4): Some Result of The Proposed System

IX. Conclusions

In this paper we have proposed new technique for encryption for a private image depending on the encoding technique (OcTree) and the chaos keys generation. This proposed system method given good results in visual encryption image views and structure.

The combination between the encoding (OcTree) and encryption (AES, Xor, and chaos keys) gives an acceptable speed encryption system.

The chaos keys (Rossler and Lorenz) generate chaos number keys in very small time, high speed, and wide range of numbers used in encryption and decryption.

In this proposed system, a good speed for encoding and encryption for three stages in implements and test results. The decrypt image lost some of the visual resolution due to encoding (OcTree).

References

- [1] Linhua Zhang, Xiaofeng Liao, Xuebing Wang, "An image encryption approach based on chaotic maps", Elsevier Ltd, Chaos, Solitons and Fractals 24 (2005) 759–765.
- [2] Nidhi S Kulkarni, Balasubramanian Raman, And Indra Gupta, "Selective Encryption of Multimedia Images", National Systems Conference, NSC 2008, December 17-19, 2008.
- [3] Bidyut Jyoti Saha¹, Kunal Kumar Kabi², Arun³, "Digital Image Encryption using ECC and DES with Chaotic Key Generator", International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 11, November – 2013. ISSN: 2278-0181
- [4] Kamel Faraoun, "Chaos-Based Key Stream Generator Based on Multiple Maps Combinations and its Application to Images Encryption", the International Arab Journal of Information Technology, Vol. 7, No. 3, July 2010
- [5] Haider K. Hoomod, "Least Square Interpolation and OcTree for 2D-3D Image Encrytion", Iraqi Association of Information Technology IAIT, 2011.
- [6] Henning Eberhardt, Vesa Klumpp, Uwe D. Hanebeck, "Density Trees for Efficient Nonlinear State Estimation", Proceedings of the 13th International Conference on Information Fusion, Edinburgh, United Kingdom, July, 2010.
- [7] Xinmiao Zhang and Keshab K. Parhi, "High-Speed VLSI Architectures for the AES Algorithm", Ieee Transactions On Very Large Scale Integration (Vlsi) Systems, Vol. 12, No. 9, September 2004.
- [8] Eldad Haber, Stefan Heldmann and Jan Modersitzki, "An OcTree Method for Parametric Image Registration", Mathematics and Computer Science, Emory University, June 9, 2006.

Image in Image Hiding Using Wavelet Transform

Iman M. G. Alwan Enas Muzaffer Jamel

Baghdad University/ College of Education for Women / Department of Computer Science

Ainms_66@coeduw.uobaghdad.edu.iq enasm.altai@gmail.com

Abstract:

Steganography is the art of hiding the existence of data in another transmission medium to achieve secret communication. Steganography can be applied on different file formats, such as audio, video, text, image etc. In image steganography, data in the form of image is hidden under some image by using transformation. In this paper, a steganography system based on Wavelet Transform is proposed. It depends on applying one level discrete Wavelet Transform to the cover image and hiding the secret image (1/4 size of cover one) in the details subbands of the cover one. The proposed system consists of three parts. First, the secret image is hidden in either LH, or HL, or HH. The results of PSNR for stego-image shows that best results are obtained when HH subband is used. Secondly, two secret images are hidden in both LH HL, or LH HH, or HL HH of the cover one. The results in terms of PSNR show that the hiding process in LH HH subbands is the best. Thirdly, three secret images are used to be hidden in LH, HL, HH subbands. PSNR of the stego-image and cover one are the lowest among the three-proposed systems but with highest amount of information to be hidden.

Keywords: Image Hiding, Steganography System, Wavelet Transform.

إخفاء صورة في صورة باستخدام تحويل الموجة
إيمان محمد جعفر علوان ايناس مظفر جميل

المستخلص

إخفاء المعلومات هو فن إخفاء وجود البيانات في وسط انتقال آخر لتحقيق التواصل السري. يمكن تطبيقها على مختلف صيغ الملفات، مثل الصوت والفيديو والنص والصورة الخ. في هذا البحث تم اقتراح خوارزمية إخفاء لصورة في صورة باستخدام تحويل الموجة. وتطبيق مستوى واحد من تحويل الموجة على الصورة المضيفة (cover) و إخفاء الصورة السرية (secret) بأبعاد (4/1) حجم الصورة المقترحة يتضمن ثلاثة أجزاء، أولاً إخفاء صورة اما في LH او HL او HH وتبين نتائج PSNR ان افضل النتائج تم الحصول عليها عند الإخفاء في HH. ثانياً إخفاء صورتين اما في LH HL او LH HH او HL HH ونتائج PSNR تبين ان افضل النتائج في LH HH. ثالثاً إخفاء ثلاث صور في LH HL HH وتبين نتائج PSNR إنها الادنى من بين الانظمة الثلاثة المقترحة لكن مع امكانية إخفاء اكبر قدر من المعلومات.

الكلمات المفتاحية: إخفاء صورة، نظام إخفاء البيانات، تحويل الموجة.

1.Introduction

Steganography is the art of passing information in a manner that the very existence of the message is unknown. The word steganography comes from the Greek steganos (cover or secret) and graphy (writing or drawing) and means literally covered writing [1, 2, 3].

It has been used in various forms for 2500 years, and used variously in military, diplomatic, personal and intellectual property applications [4]

Each steganography communication system consists of an embedding algorithm and an extraction algorithm. To accommodate a secret message, the original image, also called the cover –image, is slightly modified by the embedding algorithm. As a result, the stego-image is obtained [5] Hiding information may require a stego - key which is additional secret information, such as a password, required for embedding the information to complicate the recovered hiding information if happened to detect such information [6]

Steganalysis is the art of discovering hidden data in cover objects. As in cryptanalysis, we assume that the steganographic method is publicly known with the exception of a secret key. The method is secure if the stego - images do not contain any detectable artifacts due to message embedding. In other words, the set of stego- images should have the same statistical properties as the set of cover-images. If there exists an algorithm that can guess whether or not a given image contains a secret

message with a success rate better than random guessing, the steganographic system is considered broken [3, 7].

The entire process of steganography for image can be presented graphically as shown in fig (1).

Hsu, C.T. and Wu, J.L. [8] presented a DCT-based algorithm is used to implement the middle-band embedding. The original gray-level image and the digital signature data S be a binary image, where the marked pixels are valued as 1's and the others are 0's. Solanki, k., Dabeer, O. [9] proposed a simple hybrid analog-digital hiding technique. The secret image is compressed efficiently (using Jpeg) into a sequence of bits, which is hidden in the cover image. Jafar A.A. [10] proposed a system to hide color image into a cover image by using DWT for cover image. A secure system implemented by generation of three PN-sequences for embedding and ciphering process.

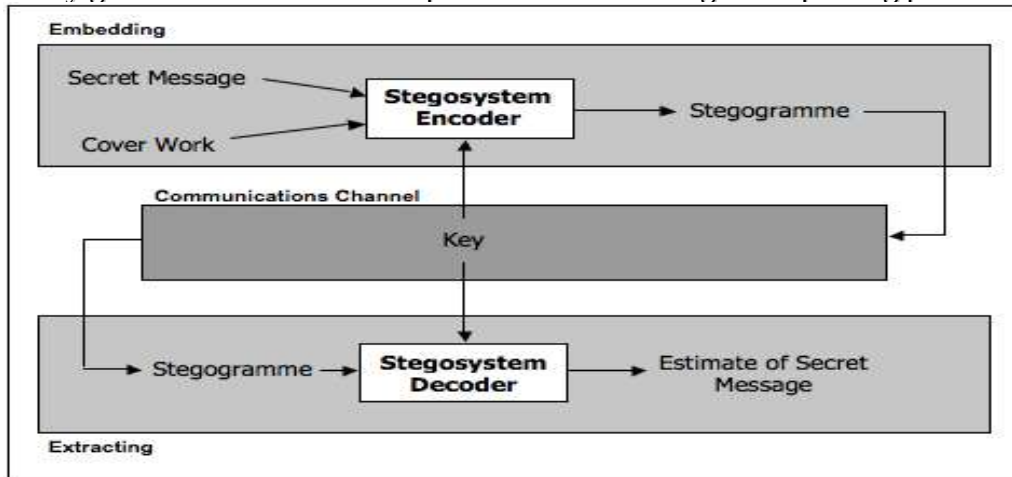


Fig. (1): The Process of Steganography

II. The Discrete Wavelet Transform

The Discrete Wavelet Transform (DWT) is a linear transformation that operates on a data vector whose length is an integer power of two, transforming it into a numerically different vector of the same length. It is a very useful tool in time-frequency analysis because of its excellent localization both in time and frequency. In frequency domain, it is a tool that separates data into different frequency components, coefficients are slightly modified. This will make some unnoticeable changes in the whole image and makes it more robust to attack compared with spatial methods.

The Calculation of the discrete wavelet transform involves a convolution, but experience shows that the quality of this type of transform depends heavily on two factors, the choice of scale factors and time shifts, and the choice of wavelet [11]

According to wavelet transform, a set of time series $f(t)$ can be approximated by the smooth version projection onto multiple scaling subspace and the detailed version projection to the wavelet subspaces, as in [11]:

$$f(t) = \sum_k c_{j_0}(k) 2^{j_0/2} \phi + \sum_k \sum_{j=1}^{j_0} d_j(k) 2^{j/2} \Psi(2^j - k) \dots (1)$$

$\phi(t)$'s are scaling function in multiple scales and $\Psi(t)$'s are wavelet functions. They form an orthogonal basis of the signal space. In eq. (1), j is the index of scale with a range form $\{0, j_0\}$ and k is the time shift factor. Given the orthogonal basis, signal $f(t)$ can be represented by a set of scaling coefficients $\{c_{j_0}(k)\}$ and wavelet coefficients $\{d_j(k)\}_1^{j_0}$ where j_0 is a desired scale. Mallat's pyramid algorithm is considered the most important algorithm to calculate DWT coefficients. It states that the coefficients $\{c_{j_0}(k)\}$ and $\{d_j(k)\}_1^{j_0}$ can be calculated by cascade FIR with a pair of filters: low-pass filter $h_0(w)$ derived from the scaling function and high-pass filter $H_1(w)$ derived from wavelet functions [11]. One important property of the discrete wavelet transform is the relationship between the impulse responses of the high pass and low pass filter. The high pass and low pass filters are not independent of each other, and they are related by

$$h_1[l - 1 - n] = (-1)^n \cdot h_0[n] \dots (2)$$

Where h_0, h_1 are the impulse response of low pass and high pass filters respectively, L is the filter length (in number of points).

Filters satisfying this condition are commonly used in signal processing, and they are known as the quadrature mirror filters [12]. The computation constitutes of two steps recursively: initially the original signal $f(n)$ with length $N(N = 2^J)$ is considered as the scale 0. They are both low-pass filtered by coefficients at every level are up sampled by two, passed through the low pass and high pass synthesis filters and then added, this process is continued through the same number of levels as in the decomposition process to obtain the original signal[11], that shown in Figure (2).

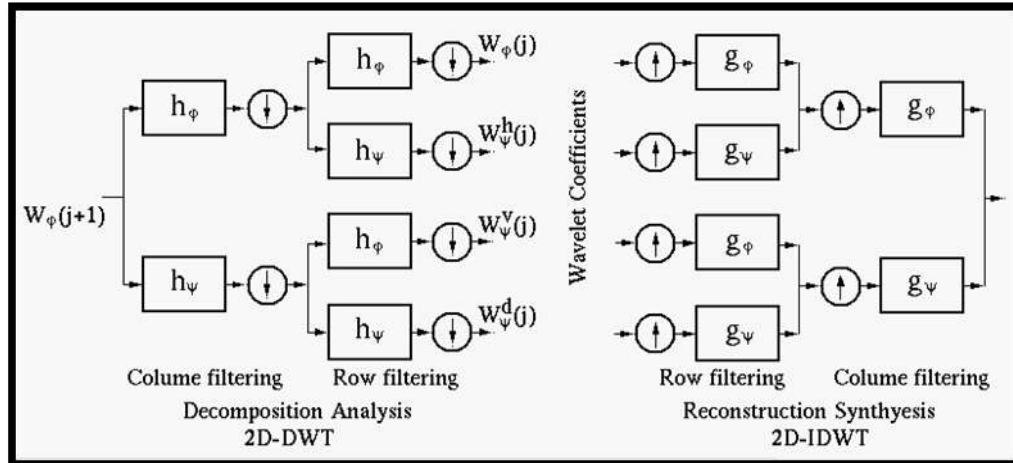


Fig. (2): Diagram of Decomposition Analysis and Reconstruction Synthesis

DWT analysis splits signal into two classes (i.e. Approximation and Detail) by signal decomposition for different frequency bands and scales. DWT employs two function sets: scaling and wavelet which associate with low and high pass filters orderly. Decomposition follows the manner of dividing time separability. Meanly, only half of the samples in a signal are sufficient to represent the whole signal, doubling the frequency separability [13].

Haar wavelet operates on data by calculating the sums and differences of adjacent elements. This wavelet operates first on adjacent horizontal elements and then on adjacent vertical elements. One important feature of the Haar wavelet transform is that the transform is equal to its inverse. Each transform computes the data energy in relocated to the top left hand corner [13].

Figure 3 shows, the original image as shown in Figure (3-a), the Lena image after one Haar wavelet is given in Figure (3-b).



Fig. (3) a: original image, b: One Level Decomposition

After each transform is performed the size of the square which contains the most important information is reduced by a factor of 4 [13], as seen in Figure 4. In Figure (4-a), the decomposition for three levels is shown, Figure (4-b) shows the decomposition for Lena image example.

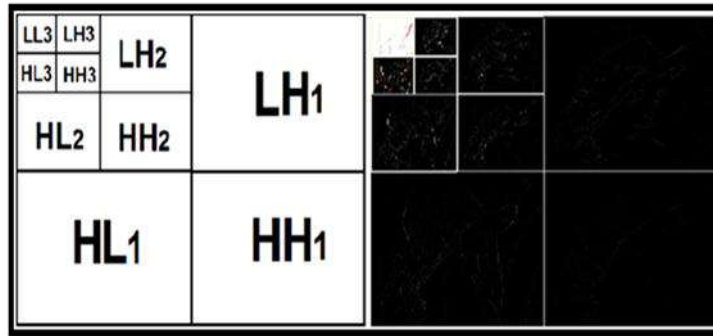


Fig. (4) a:Three Level Decompositionb: Three Level of Decomposition of Lena Image

III. Performances Evaluation of the Proposed System

This is a quantifiable measurement of how finely a secret message has been embedded into given cover image without anyone knowing about its existence at all. It is scaled to measure the invisibility of hidden information in a stego image. The higher the imperceptibility, the higher its invisibility, and the better the quality of the image is. It is one of the most widely used criteria to evaluate the performance of any steganography technique, which is measured using the Peak Signal to Noise Ratio (PSNR).

PSNR is a metric used for the measurement of imperceptibility or for the quality of a stego image. Its units are decibels (dB). The higher the value of the PSNR, the higher the imperceptibility or the quality of the image will be. So, all steganography techniques work to acquire more and more PSNR value. It is measured as:

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \text{ dB} \dots(3)$$

$$MSE = \left(\frac{1}{M \times N} \right) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (P(x, y) - P'(x, y))^2 \dots(4)$$

Here, M designates number of rows and N is the number of cover image columns. P(x, y) and P'(x, y) are the pixel values for the cover and stego image, respectively. MSE stands for "Mean Square Error" [14].

1- The Proposed System

The system is proposed to hide one secret image, two secret images and three secret images each of (1/4 size of the cover image) in the wavelet domain of the cover one and find the effect of hiding in the different three sub bands (LH, HL, HH). The proposed system consists of two parts, the hiding part and the extracting part.

1-1 The Proposed Steganography System for Hiding One Secret Image

First hiding system is to hide one secret image in either (LH, HL, HH) sub band. Figure (5) shows the block diagram of the hiding process. The algorithm consists of two processes; hiding process and extracting process. They are as follows:

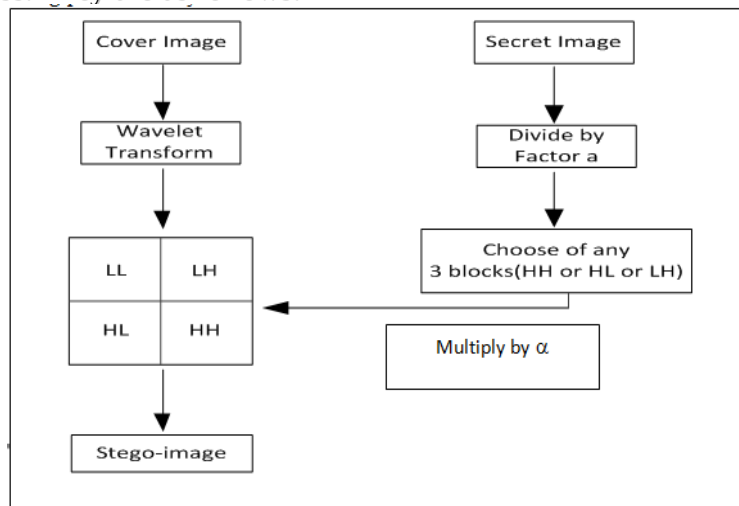


Fig. (5): Hiding One Secret Image

a- Hiding Algorithm:

Input: Secret image, Cover image. **Output:** Stego-image.

Step 1: Apply DWT to cover image to obtain LL, LH, HL, HH by using Haar wavelet Transform.

Step 2: Multiply the coefficients of secret image by factor α , where α ranges from 0.01 to 0.002 (best results empirically is α equal to 0.0025).

Step 3: Replace secret image in LH or HL or HH subband.

Step 4: Take inverse DWT (LH or HL or HH) for image in step 3.

b- Extracting Algorithm:

Input: Stego-image, factor α . **Output:** Secret image.

Step 1: Apply DWT to stego image to obtain LL, LH, HL, HH by using Haar wavelet transform.

Step 2: multiply the coefficients of DWT sub bands where the secret image is hidden in (LH or HL or HH) by the factor $(1/\alpha)$. The result is the secret image.

Figure (6) represent the test secret and cover color images. Table (1) represent the PSNR of the stego images for hiding process in different detail subbands.

Table (1) shows test Images and PSNR values for hiding one secret image

Test Images		PSNR of Hiding in (LH) subbands	
			
Secret image 1	Secret image 2	Secret image 1	Secret image 2
			
Cover image 1	Cover image 2	Stego image 1	Stego image 2
		PSNR=38.663	PSNR=33.053

PSNR of Hiding In (HL) subband		PSNR of hiding In (HH) subband	
			
Secret image 1	Secret image 2	Secret image 1	Secret image 2

			
Stego image 1	Stego image 2	Stego image 1	Stego image 2
PSNR= 36.682	PSNR=34.794	PSNR=45.470	PSNR=47.326

Typical PSNR values range between 20-40 dB for good image quality [12], From the results, one can notice that best results are obtained from hiding in HH subbands. The value of PSNR is ranges from (45-47) dB which is large value and indicate good perceptibly. Hiding in LH and HL subbands offers lower PSNR values because of the existence of the low frequency.

1-2 The Proposed Steganography System for Hiding Two Secret Images

In this section, hiding of two secret images are involved. The hiding process is implemented in either LH HL, LH HH, or HL HH sub bands. Figure (6) shows the algorithm block diagram.

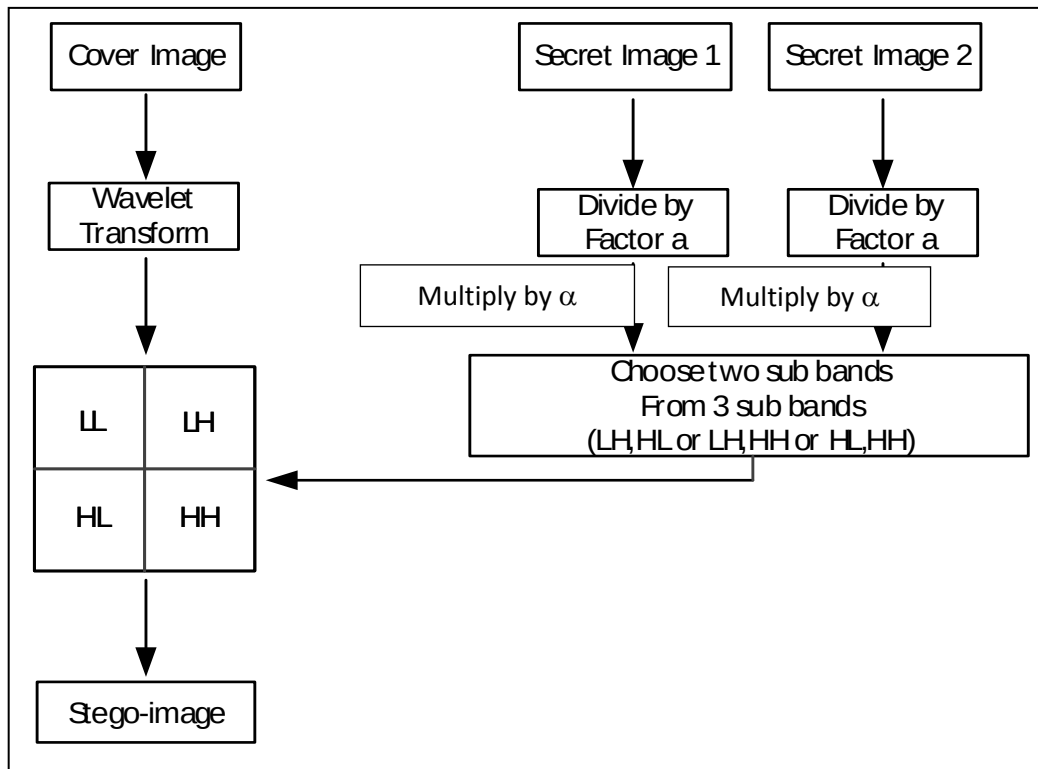


Fig. (6) Hiding Two Secret Image

a-Hiding Algorithm:

Input: Secret image1, Secret image2, Cover image. **Output:** Stego-image.

Step 1: Apply DWT (Haar Wavelet) to the cover image to obtain LL, LH, HL, HH subbands.

Step 2: Multiply the coefficients of secret images by factor α , where α ranges from 0.01 to 0.002 (best results empirically is α equal to 0.0025).

Step 3: Hide the two secret images in LH, HL or HL, HH, or LH, HH, of the cover image.

Step 4: Apply inverse DWT to get the stego-image.

b- Extracting Algorithm:

Input: Stego-image, factor α .

Output: Secret image 1, secret image 2.

Step 1: Apply DWT to the cover image to obtain LL, LH, HL, HH by using Haar wavelet transform.

Step 2: Divide the coefficients of DWT sub bands where the secret images are hidden (LH, HL or HH, HL or HH, LH) by the factor α . The result is the secret images.

Table (1) shows the PSNR results of hiding the tulips and penguin secret images in the two cover images Lena and flower images for different two bands (LH, HL), (HL, HH), and (LH, HH) respectively.

Table (2) represent the PSNR of the stego images for hiding process in different detail sub bands

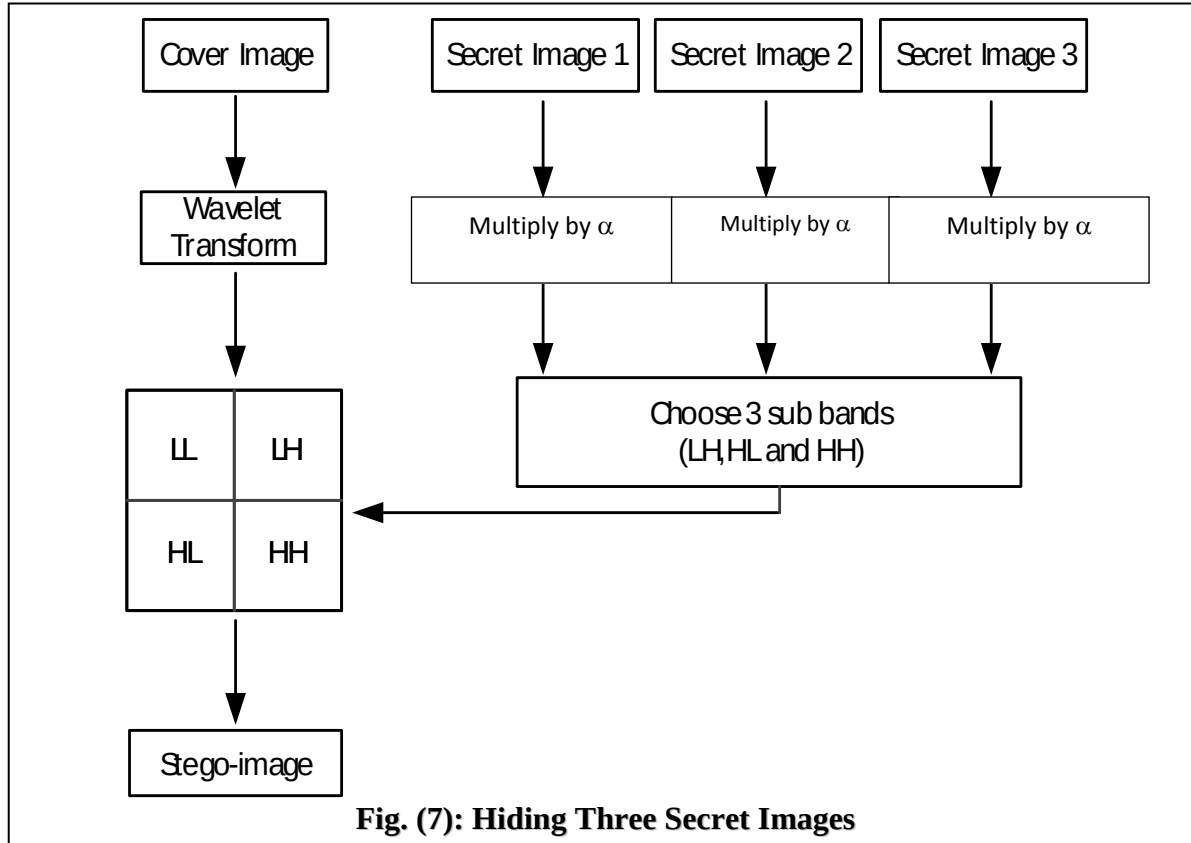
Test images		PSNR of Hiding In (LH, HL)	
			
First secret image 1	First secret image 2	First secret image 1	First secret image 2
			
Second secret image 1	Second secret image 2	Second secret image 1	Second secret image 2
			
Cover image3	Cover image1	Stego- image 1 PSNR= 34.5688	Stego-image 2 PSNR=31.186

PSNR of Hiding In (HH, HL)		PSNR of Hiding In (HH, LH)	
			
First secret image 1	First secret image 2	First secret image 1	First secret image 2
			
Second secret image 1	Second secret image 2	Second secret image 1	Second secret image 2
			
Stego image 1	image Stego 2	Stego image 1	image Stego 2
PSNR=36.1711	PSNR=34.217	PSNR= 37.8801	PSNR=33.337

From the results, the value of the PSNR is between (31-37) dB. The range is 6 dB for the different used test images. The best hiding bands are (LH,HH) and (HL, HH) because the using of HH sub band in which only high frequencies reside.

1-3 The Proposed Steganography System for Hiding Three Secret Images.

In this section, the process of hiding three secret images in LH, HL, and HH subbands are implemented. The block diagram of the proposed algorithm is shown in figure (7).



a- Hiding Algorithm:

Input: Secret image 1, Secret image 2, Secret image 3, Cover image.

Output: Stego-image.

Step 1: Apply DWT to the cover image to obtain LL, LH, HL, HH by using Haar wavelet transform.

Step 2: Multiply the coefficients of secret images by factor α , where α ranges from 0.01 to 0.002 (best results empirically is α equal to 0.0025).

Step 3: Hide secret images in LH, HL and HH.

Step 4: Take inverse DWT to get the stego-image.

b- Extracting Algorithm:

Input: Stego-image, α factor.

Output: Secret image 1, secret image 2, secret image 3.

Step 1: Apply DWT to stego image to obtain LL, LH, HL, HH by using Haar wavelet transform.

Step 2: Divide the coefficients of DWT sub bands where the secret images are hidden (LH, HL and HH) by the factor α . The result is the secret images

Table (3), shows the cover and secret test images and the value of PSNR for the two stego-images that chosen in the experimental test.

From the results of hiding three test secret images in one cover one in which each secret one is of (1/4) size of the cover image, one can notice that the value of PSNR is acceptable since it approximately 34 dB. So in this proposed algorithm good imperceptibility with large amount of data are obtained.

Table (3) shows the PSNR of the stego images for hiding three secret image

Test images		PSNR of Hiding in (LH, HL, HH)	
			
First secret image 1	First secret image 2	First secret image 1	First secret image 2
			
Second secret image 1	Second secret image 2	Second secret image 1	Second secret image 2
			
Third secret image 1	Third secret image 2	Third secret image 1	Third secret image 2
			
Cover image1	Cover image2	Stego image 1 PSNR= 34.2139	image Stego 2 PSNR=34.649

IV. Conclusion

In this paper, a hiding process is proposed. It depends on hiding one, two, and three secret images into cover one. The size of the secret image is of $\frac{1}{4}$ size of the cover image. The hiding process is blind because no cover image is required in extraction process. The PSNR values of the resultant stego-images is very good which indicate good imperceptibility, also the algorithm offers good capacity since three secret images can be hidden in one cover image.

References

- [1] J. Watkins, "**Steganography – Messages Hidden in Bits**". 2nd Annual CM316 Conference on Multimedia Systems, based at Southampton University, UK, 2002.
- [2] M. Bachrach, and F.Y. Shih, "**Image steganography and steganalysis**". Wiley Interdisciplinary Reviews: Computational Statistics, Vol. 3, pp. 251-9, 2011.
- [3] D. Sellars, "**An Introduction to Steganography**".
<http://www.cs.uct.ac.za/courses/CS400W/NIS/papers99/dsellars/stego.ps.gz>
- [4] N.F. Johnson, Z. Duric, S. Jajodia, "**Information Hiding: Steganography and Watermarking-Attack and Countermeasures**". Kluwer Academic Publisher, 2001.
- [5] J. Fridrich, M. Goljan, and R. Du, "**Detecting LSB steganography in color and gray-scale image**". In IEEE Multimedia, vol. 8, no. 4, pp. 22 - 28 · November 2001. DOI: 10.1109/ 93.959097 ·
- [6] N.F. Johnson., S. Jajodia, "**Steganolaysis of Images Created Using Current Steganography Software**". Proc. Information Hiding Workshop, Portland, Oregon, USA, April 1998.
- [7] J. Fridrich, M. Goljan, and D. Hoge, "**Steganalysis of JPEG Images: Breaking the F5 Algorithm**". Proc. 5th Int'l Workshop Information Hiding, Springer-Verlag, 2002.
- [8] C.T. Hsu, J.L. Wu, "Hidden Signatures in Images", IEEE International Conference on Image Processing, vol. 3, pp. 223-226, 1996.
- [9] K. Solanki, and B.S. Manjunath, "**A Joint Source-channel coding Scheme for Image-IN-Image DATA Hiding**". IEEE International Conference on Image Processing (ICIP), Barcelona, Spain, 2003.
- [10] A.A. Jafar, "**Image Steganographic Algorithm Based on DWT and Turbo coding**". M.Sc. Thesis, Electrical Engineering Department, College of Engineering AL-Mustansiriya University, 2008.
- [11] S. Mallat, "**A wavelet Tour of Signal Processing**". Academic Press, 1999.
- [12] D. Salmon, "**Data Compression**". The complete reference, Fourth Edition, Springer- Verlag London Limited, 2007.
- [13] E. H. Houssein, M. A. S. Ali, A. E. Hassanien, "**An Image Steganography Algorithm using Haar Discrete Wavelet Transform with Advanced Encryption System**". IEEE Proceedings of the Federated Conference on Computer Science and Information Systems, Vol.8, pp. 641–644, 2016.
- [14] M. Juneja, P. S. Sandhu, "**A New Approach for Information Security using an Improved Steganography Technique**". KIPS J Inf Process Syst, Vol.9, No.3, September 2013.

Fingerprint Encryption Based on Feature Extraction QR Code

Ali Hussein Fadhil¹

Raniah Ali Mustafa²

¹Computer Science Dept., College of Education, University of Diyala,

²Computer Science Dept., College of Education, Mustansiriyah University

alifoxpro2012@gmail.com

rania83computer@yahoo.com

Abstract:

Fingerprint is one of the most well-known and publicized biometrics. Because of their uniqueness and consistency over time. QR-Code is extremely secure as all the sensitive data stored and transmitted is encrypted, but it is also easy to use and cost-efficient solution. The goal of this paper is encryption fingerprint using QR code. The main idea of the proposed system depends on the generation of QR code depending on the input text and then extracts features into QR code which was generated depending on convolution. These features are used to generate the key which is used in the encryption process images fingerprints and decryption. In this paper, the proposed system was tested in two phases: The first phase on a random key in the encryption process and depending on the measure NIST (National Institute of Standards and Technology), the second phase on measures of image quality depending on)MSR, PSNR, MAE, UACI, NPCR, Correlation, Entropy). The proposed approach is tested on a CASIA Fingerprint image database Version 5.0, and the proposed system implemented in programming language Visual Basic.NET. Experimental results show that our approach offer best encryption and decryption and that the safety and confidentiality of the fingerprint images can be guaranteed without any leak of the fingerprint ridge information.

Keywords: QR code, Histogram Equalization, Binarization, Convolution, NIST, MSR, PSNR, MAE, UACI, NPCR, Correlation, and Entropy.

تشفير بصمات الأصابع بالاعتماد على أستخراج الخصائص لـ QR code

علي حسين فاضل رانية علي مصطفى

المستخلص:

بصمات الأصابع هي واحدة من القياسات الحيوية الأكثر شهرة وانتشاراً. وبسبب تفردا وتناسقها مع مرور الوقت. QR code آمن للغاية لتشفير لكل البيانات الحساسة المخزنة والمرسلة، ولكن هو أيضا سهلة الاستخدام والحل فعالة من حيث التكلفة. الهدف من هذا الورقة هو تشفير بصمات الأصابع بأستخدام QR code. الفكرة الرئيسية لنظام المقترح تعتمد على توليد QR code يعتمد على النص المدخل ومن تم أستخراج الخصائص من QR code الذي تم توليده بالاعتماد على convolution. هؤلاء الخصائص تستخدم لتوليد المفتاح الذي يستخدم في عملية التشفير صور بصمات الأصابع وفك التشفير. في هذ الورقة تم اختبار النظام المقترح على مرحلتين المرحلة الأولى على عشوائية المفتاح في عملية التشفير وبالا اعتماد مقياس (National Institute of Standards and Technology) MSR، PSNR، MAE، UACI، NPCR، Correlation، Entropy. النهج المقترح أختبار على CASIA Fingerprint image database Version 5.0، وتم تنفيذه بلغة البرمجة Visual Basic.NET. وتظهر النتائج التجريبية أن نهجنا نقدم أفضل التشفير وفك التشفير، وأنه يمكن ضمان سلامة وسرية صور بصمات الأصابع دون أي تسرب للمعلومات التلاعب بصمات الأصابع.

الكلمات المفتاحية: رمز الاستجابة السريعة، الرسم البياني معادلة، binarization، التفاف، NIST، Mean Squared Error، UACI، NPCR، Correlation، Entropy، Mean Absolute Error، Peak Signal to Noise Ratio.

1. Introduction:

With the latest development in technology there has been many ways of ensuring the access to particular space. The widely used technologies are Fingerprint, Face-recognition, Bar-code, Username-password method. Fingerprint and Face recognition been costly, is not common man's

cup of cake. Barcode on the other hand is one dimensional and becomes unreadable when damaged. Barcode have some limitations like bar code only stores up to 20 digits. So in bar code we are not able to store complex phrases or passwords, hence it doesn't provide best authentication method [1]. Hence QR code was selected as fit for the paper.

2. Fingerprint Image

Fingerprints have been used for over a century and are the most widely used form of biometric identification. Fingerprint identification is commonly employed in forensic science to support criminal investigations, and in biometric systems such as civilian and commercial identification devices. Despite this widespread use of fingerprints, there has been little statistical work done on the uniqueness of fingerprint minutiae. In particular, the issue of how many minutiae points should be used for matching a fingerprint is unresolved [2].

The fingerprint of an individual is unique and remains unchanged over a lifetime. A fingerprint is formed from an impression of the pattern of ridges on a finger. A ridge is defined as a single curved segment, and a valley is the region between two adjacent ridges. The minutiae, which are the local discontinuities in the ridge flow pattern, provide the features that are used for identification. Details such as the type, orientation, and location of minutiae are taken into account when performing minutiae extraction [3]. Figure.1 shows collection of samples of from one finger of a person with 8 impressions [4].



Fig. (1): Fingerprint with one finger with 8 impressions

3. Encoding of QR Code

3.1 Features of QR Code

The Quick Response (QR) Code was designed as an improvement in comparison to its predecessor, the 1D barcode because it can contain more information. It was first designed for the automotive industry in Japan but later it become so popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard UPC code [5].

A QR code, as shown in Fig.2 is read by an imaging device, such as a camera, and formatted algorithmically by underlying software using Reed-Solomon error correction until the image can be appropriately interpreted. Data is then extracted from patterns present in both horizontal and vertical components of the image. Figure.2 shows a sample of an unencrypted QR code that will be needed by the proposed system [6]. QR Code has many advanced features.



Fig. (2): Quick Response Code

1. High capacity encoding of data QR Code has high capacity encoding of data, its maximum symbol can encode 7089 characters; while PDF417 only encode 2710 characters.
2. High-speed reading Adapted with CCD reading, it can recognize more QR Code symbol per second than PDF417 symbol for encoding same data capacity.
3. Chinese encoding capability Chinese and Japanese characters are represented by a two byte combination in other two dimensional barcode. But in QR Code, there is a specific Chinese mode; it can use 13 bits encoding a Chinese character. So the efficiency of Chinese represented improved 20% in QR Code compared with PDF417.
4. Readable from any direction from 360 degree QR Code is a matrix two dimensional barcode; it can be readable from any direction from 360 degree. But the stack two-dimensional barcode, for example PDF417, is very difficult to realize the readable from 360 degree.

QR Code has been approved as an AIM Standard, a JIS Standard and an ISO standard. So QR Code is being used in a wide variety of applications, such as manufacturing, logistics, and sales applications. In 2000 years, QR Code is being issued as National standard in China [7].

QR codes are versatile. A piece of long multilingual text, a linked URL, an automated SMS message, a business card or just about any information can be embedded into the two-dimensional barcode. Coupled with moderate equipped mobile devices, QR Codes can connect the users to the information quickly and easily. We explore how QR codes can be used in security purpose. The information in the code can be encrypted, which needs special software to decipher and decode, which ensure better security. Quick Response codes, QR code for short, is a two dimensional barcode with high information density, error correction ability and convenient encryption mechanism [8].

3.2 Encoding of QR Code

Each QR Code symbol consists of an encoding region and function patterns, as shown in Figure.3. Finder, separator, timing patterns and alignment patterns comprised function patterns. Function patterns shall not be used for the encoding data. The finder patterns located at three corners of the symbol intended to assist in easy location of its position, size and inclination [9].

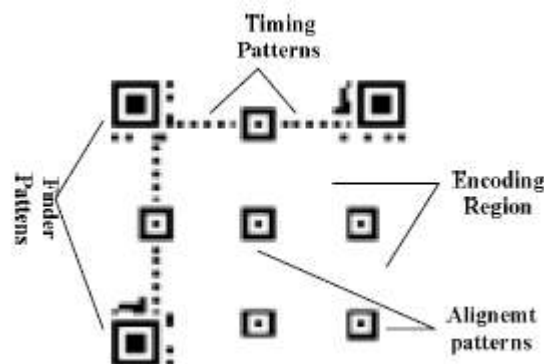


Fig. (3): the structure of QR Code

The encode procedure of QR Code including follows steps. Firstly input data is encoded in according to most efficient mode and formed bit stream. The bit streams are divided into code words. Then code words are divided into blocks, and add error correction code words to each block. All these code words are put into a matrix and are masked with mask pattern. Finally function patterns are added into the QR symbol. A QR Code symbol is formed [8].

4. Related Work

Some of the published works related to the objectives of this work are given in the following paragraphs:

Maykin Warasart and Pramote Kuacharoen (2012) In this paper, an implementation of paper-based document authentication is presented. The integrity of the text message and the author of the document can be verified with the use of a digital signature and QR code. The proposed method can be automatic or semi-automatic. It is semi-automatic when the OCR is not accurate and it requires the user to visually compare the text message on the paper and the one obtained from the QR code; however, this method does provide convenience for the user in dealing with a large amount of documents [10].

Nitu Mujumdar, Pooja Shinde, Karishma Thigale and Sanjay Agrawal (2014) the system issue tickets in 2D barcode format. This can be used to automate the workflow of ticket Authentication. The emergence of 2D code provides a kind of effective method for anti-counterfeit. Through real-time collection of the certificate holder's fingerprint and QR code, deciphering the information to authenticate the validity of the holder, the function of dual anti-counterfeit is realized. Using universal equipment like mobile phones to acquire QR code pictures is facile and practical. The user of the system 1st need to register to the central server. On successful registration the user can login and can buy airline tickets. On confirm reservation the system converts the ticket data into a 2D barcode format. This barcode is in the image form. The customer simply has to download the ticket and should store it in his mobile phones and should carry ticket while travelling. While traveling the ticket checker when demands the ticket the customer has to show the 2D barcode ticket image. The ticket checker will scan the data of the image through his mobile. Agent software is installed on the checker mobile phone. The agent software decodes the ticket data and can validate the passenger details [8].

Tejas Mohod, Linu Thomas and Ranjit Thorat (2016) this system takes the best suitable characteristics of both iris and QR code; this enhances the isolation of the system, where implemented a cost effective and reliable security system [1].

Revathi M K, Annapandi P and Ramya K P (2013) our system consists of QR reader and Biometrics finger print readers which are used to verify the certificate originality in order to eradicate fraudulent certificate. The procedure involved in this paper is getting the QR code the certificate and finger print of the person during the run time. Then the fingerprint is verified with that of the stored one, if it matches then the approved mark statement will be provided. As a result of completing the above procedure the security if identification document is increased. A running version of the system will have only one Administrator but it typically has multiple end users like educational institution, industries and etc. The administrator is responsible for managing user accounts, system resources and logs and for the health and safekeeping of the system. Educational institution, industries and other users have the responsibility of verifying the certificate as assigned by the administrator [11].

5. Dataset

To gain a finger print image which is need to encryption taking a clear and good image. Here we use the CASIA Finger Print Image Database version 5.0 (or CASIA- Finger Print V5) contains 20,000 finger print images of 500 subjects. The finger print images of CASIA-Finger Print V5 were captured using URU4000 finger print sensor in one session. The volunteers of CASIA-Finger Print V5 include graduate students, workers, waiters, etc. Each volunteer contributed 40 finger print images of his eight fingers (left and right thumb/second/third/fourth finger), i.e. 5 images per finger. The volunteers were asked to rotate their fingers with various levels of pressure to generate significant intra-class variations. All finger print images are 8 bit gray-level BMP files and the image resolution is 328*356 [12].

6. Random Number Generation Tests

The NIST Test Suite is a statistical package consisting of 15 tests that were developed to test the randomness of (arbitrarily long) binary sequences produced by either hardware or software based cryptographic random or pseudorandom number generators. These tests focus on a variety of different types of non-randomness that could exist in a sequence. Some tests are decomposable into a variety of subtests. The 15 tests are [13]:

a. Frequency (Monobit) Test

The focus of the test is the proportion of zeroes and ones for the entire sequence. The purpose of this test is to determine whether the number of ones and zeros in a sequence are approximately the same as would be expected for a truly random sequence. The test assesses the closeness of the fraction of ones to $\frac{1}{2}$, that is, the number of ones and zeroes in a sequence should be about the same. All subsequent tests depend on the passing of this test [14].

b. Frequency Test within a Block

The focus of the test is the proportion of ones within M-bit blocks. The purpose of this test is to determine whether the frequency of ones in an M-bit block is approximately $M/2$, as would be expected under an assumption of randomness. For block size $M=1$, this test degenerates to test 1, the Frequency (Monobit) test [15].

c. Runs Test

The focus of this test is the total number of runs in the sequence, where a run is an uninterrupted sequence of identical bits. A run of length k consists of exactly k identical bits and is bounded before and after with a bit of the opposite value. The purpose of the runs test is to determine whether the number of runs of ones and zeros of various lengths is as expected for a random sequence. In particular, this test determines whether the oscillation between such zeros and ones is too fast or too slow [16].

d. Test for the Longest Run of Ones in a Block

The focus of the test is the longest run of ones within M-bit blocks. The purpose of this test is to determine whether the length of the longest run of ones within the tested sequence is consistent with the length of the longest run of ones that would be expected in a random sequence. Note that an irregularity in the expected length of the longest run of ones implies that there is also an irregularity in the expected length of the longest run of zeroes. Therefore, only a test for ones is necessary [17].

e. Binary Matrix Rank Test

The focus of the test is the rank of disjoint sub-matrices of the entire sequence. The purpose of this test is to check for linear dependence among fixed length substrings of the original sequence. Note that this test also appears in the DIEHARD battery of tests [18].

f. Discrete Fourier Transform (Spectral) Test

The focus of this test is the peak heights in the Discrete Fourier Transform of the sequence. The purpose of this test is to detect periodic features (i.e., repetitive patterns that are near each other) in the tested sequence that would indicate a deviation from the assumption of randomness. The intention is to detect whether the number of peaks exceeding the 95 % threshold is significantly different than 5 % [19].

g. Non-overlapping Template Matching Test

The focus of this test is the number of occurrences of pre-specified target strings. The purpose of this test is to detect generators that produce too many occurrences of a given non-periodic (aperiodic) pattern [20].

h. Overlapping Template Matching Test

The focus of the Overlapping Template Matching test is the number of occurrences of pre-specified target strings [21].

i. Maurer's "Universal Statistical" Test

The focus of this test is the number of bits between matching patterns (a measure that is related to the length of a compressed sequence). The purpose of the test is to detect whether or not the sequence can be significantly compressed without loss of information. A significantly compressible sequence is considered to be non-random [22].

j. Linear Complexity Test

The focus of this test is the length of a linear feedback shift register (LFSR). The purpose of this test is to determine whether or not the sequence is complex enough to be considered random. Random sequences are characterized by longer LFSRs. An LFSR that is too short implies non-randomness [23].

k. Serial Test

The focus of this test is the frequency of all possible overlapping m-bit patterns across the entire sequence. The purpose of this test is to determine whether the number of occurrences of the 2mm-bit overlapping patterns is approximately the same as would be expected for a random sequence. Random sequences have uniformity; that is, every m-bit pattern has the same chance of appearing as every other m-bit pattern. Note that for $m = 1$ [24].

l. Approximate Entropy Test

The focus of this test is the frequency of all possible overlapping m-bit patterns across the entire sequence. The purpose of the test is to compare the frequency of overlapping blocks of two consecutive/adjacent lengths (m and m+1) against the expected result for a random sequence [25].

m. Cumulative Sums (Cusum) Test

The focus of this test is the maximal excursion (from zero) of the random walk defined by the cumulative sum of adjusted (-1, +1) digits in the sequence. The purpose of the test is to determine whether the cumulative sum of the partial sequences occurring in the tested sequence is too large or too small relative to the expected behavior of that cumulative sum for random sequences. This cumulative sum may be considered as a random walk. For a random sequence, the excursions of the random walk should be near zero. For certain types of non-random sequences, the excursions of this random walk from zero will be large [26].

n. Random Excursions Test

The focus of this test is the number of cycles having exactly K visits in a cumulative sum random walk. The cumulative sum random walk is derived from partial sums after the (0,1) sequence is transferred to the appropriate (-1, +1) sequence. A cycle of a random walk consists of a sequence of steps of unit length taken at random that begin at and return to the origin. The purpose of this test is to determine if the number of visits to a particular state within a cycle deviates from what one would expect for a random sequence. This test is actually a series of eight tests (and conclusions), one test and conclusion for each of the states: -4, -3, -2, -1 and +1, +2, +3, +4 [27].

o. Random Excursions Variant Test

The focus of this test is the total number of times that a particular state is visited (i.e., occurs) in a cumulative sum random walk. The purpose of this test is to detect deviations from the expected number of visits to various states in the random walk. This test is actually a series of eighteen tests (and conclusions), one test and conclusion for each of the states: -9, -8, ..., -1 and +1, +2, ..., +9 [28].

7. Fundamentals of the Image Quality Criteria

There are large varieties of these metrics. Some of existing measures of image quality are listed below:

a. Mean Squared Error (MSE): One obvious way of measuring this similarity is to compute an error signal by subtracting the test signal from the reference, and then computing the average energy of the error signal. The mean-squared-error (MSE) is the simplest, and the most widely used, full-reference image quality measurement. This metric is frequently used in signal processing and is defined as follows [29]:-

$$MSE = \frac{1}{NM} \sum_{i=1}^M \sum_{j=1}^N (x(i,j) - y(i,j))^2, \dots \dots \dots (1)$$

Where $x(i, j)$ represents the original (reference) image and $y(i, j)$ represents the distorted (modified) image and i and j are the pixel position of the $M \times N$ image. MSE is zero when $x(i, j) = y(i, j)$.

b. Peak Signal to Noise Ratio (PSNR): The PSNR is evaluated in decibels and is inversely proportional the Mean Squared Error. It is given by the equation[29]:-

$$PSNR = 10 \log \frac{(2^n - 1)^2}{MSE}, \dots \dots \dots (2)$$

c. Mean Absolute Error (MAE): MAE is average of absolute difference between the reference signal and test image. It is given by the equation[29]:

$$MAE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N |x(i, j) - y(i, j)|, \dots \dots \dots (3)$$

d. Correlation: is a quality analysis used to measure the similarity between the plain image and the cipher image. The correlation can be calculated from equation[30]:

$$corr = \frac{\sum_{r=1}^N \sum_{c=1}^M (I_1(r, c) - I_1)(I_2(r, c) - I_2)}{\sqrt{[\sum_{r=1}^N \sum_{c=1}^M (I_1(r, c) - I_1)^2][\sum_{r=1}^N \sum_{c=1}^M (I_2(r, c) - I_2)^2]}}, \dots \dots \dots (4)$$

The best preferred value of correlation is near the zero.

e. Entropy: is the expected value (or average of information) that can be extracted from the message, and expressed by equation [30]:

$$H(s) = - \sum_{i=0}^{2^N-1} P(s_i) \log_2 P(s_i), \dots \dots \dots (5)$$

f. NPCR determines the number of pixels that their values change during the encryption operation, while, UACI determines the ratio of changes between two cipher-images. The scale of NPCR is [0, 1], the value 0 shows that there is no change in pixels of image1 and image2. Value 1 show that all pixels in image2 are different from image1. The scale of UACI is [0, 1], the most preferred value is near to zero [30].

8. The Proposed System

The main idea of the proposed system depends on the generation of QR code depending on the input text and then extracts features into QR code which was generated depending on convolution. These features are used to generate the key which is used in the encryption process images fingerprints and decryption. Before select secret image (fingerprint sample) there is need to process and extract features for QR code which has been generated and encrypt it. The proposed system is done in following steps:

1. Load text
2. Generation QR code
3. Preprocessing (Histogram Equalization, Binarization)
4. Feature Extraction Using Convolution
5. Key Generation
6. Select Secret Image (Finger Print)
7. Finger Print Encryption
8. Finger Print Decryption
9. Measure of Image Quality

8.1 In this paper, each steps in the proposed system will explained with the results and result for test key and result measure of image quality. The proposed system depends on features for QR code to generate key. Where it will get a stronger key to encrypt. The figure.4 illustrates the each step for the proposed system. **Load text**

The fingerprint images are used to be extracted from sensor and saved in database from which any random sample is selected for processing.

8.2 Generation QR code and preprocessing

In this step, the proposed system will generation of QR code depending on the any input text, and then proposed system will preprocessing.

Step1: QR Code

In this step, the proposed system will enter any text. This input text will transform QR code for purpose obtains to features for QR code will used to generate a random key. And then used the key generate according to standards, will get a stronger key used in the encrypt process.

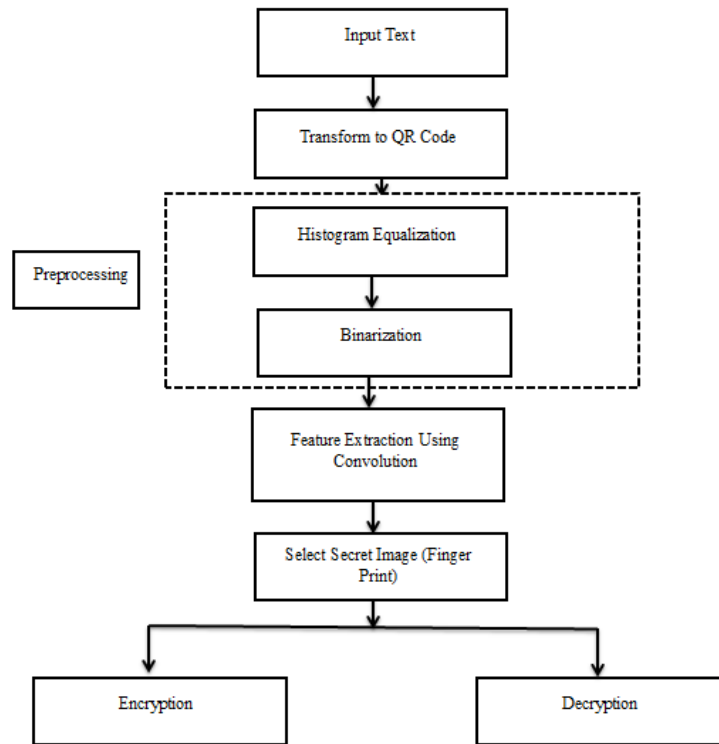


Fig. (4): the proposed system for fingerprint

Step2: Histogram Equalization

Histogram equalization is a technique for adjusting image intensities to enhance contrast. Let f be a given image represented as a m_r by m_c matrix of integer pixel intensities ranging from 0 to $L - 1$. L is the number of possible intensity values, often 256. Let p denote the normalized histogram of f with a bin for each possible intensity. So [31].

$$P_n = \frac{\text{number of pixels with intensity } n}{\text{total number of pixels}} \quad n=0, 1, \dots, L-1, \dots \quad (6)$$

The histogram equalized image g will be defined by

$$g_{i,j} = \text{floor}((L - 1) \sum_{n=0}^{f_{i,j}} p_n) \quad (7)$$

Where $\text{floor}()$ rounds down to the nearest integer. This is equivalent to transforming the pixel intensities, k , of f by the function

$$T(k) = \text{floor}((L - 1) \sum_{n=0}^k p_n) \quad (8)$$

In this paper, after transform any input text to QR code, the next step is Histogram Equalization and the result this step in the table.1.

Step3: Binarization

Binarization is an important process for accurately recognizing black-and-white module in QR code images. Therefore, we propose binarization method to extracts features into QR code which was generated depending on convolution. In this method, the QR code is divided into certain blocks, say (16X16). The intensity value of these blocks is analyzed and accordingly the pixel value is marked as 1 if intensity value of that pixel is greater than mean intensity of that block and 0 otherwise. The table (1) shows the result for QR code and Histogram Equalization and Binarization for number bit of text (8bit, 16bit, 24bit, 32 bit, 40bit, 48bit).

Table (1) the Result for QR code and Histogram Equalization and Binarization

No bit of text	8	16	24	32	40	48
QR Code						
Histogram Equalization						
Binarization						

8.3 Feature Extraction Using Convolution

The convolution of two functions $f(x), g(x)$ which we denote by $(f * g)(t)$ the convolution is an important construct because of the Convolution Theorem which gives the inverse Laplace transform of a product of two transformed functions [32]:

$$L^{-1}\{F(s)G(s)\} = (f * g)(t) \dots \dots \dots (9)$$

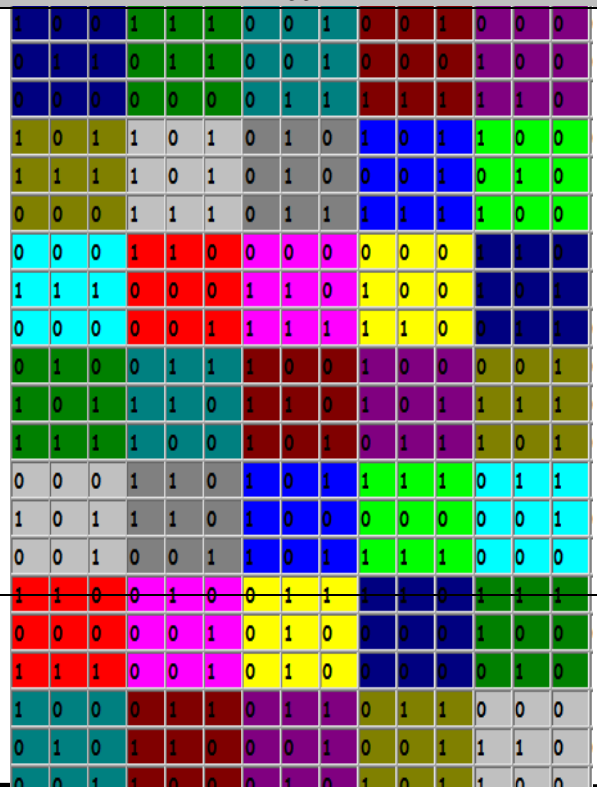
Let $f(x)$ and $g(x)$ be two functions of t . The convolution of $f(x)$ and $g(x)$ is also a function of t , denoted by $(f * g)(t)$ and is defined by the relation.

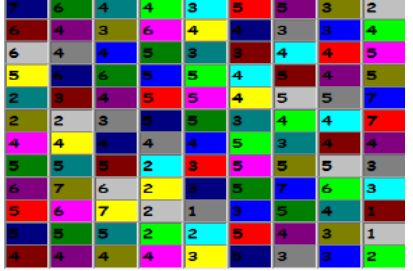
If $f(x)$ and $g(x)$ are causal functions then their convolution is defined by:

$$(f * g)(t) = \int_0^t f(t-r)g(r)dx, \dots \dots \dots (10)$$

In this paper, after step binarization, the proposed system used convolution for extract the features for QR code for to generate the key, the table.2. Show the masks used in the convolution (the result the convolution).

Table (2) the masks used in the convolution

Matrix	N0	mask	Convolution Matrix
	1		
	2		

	3		
	4		

In this paper, used mask (3x3), the system proposed used many mask and the best result histogram equalization and convolution illustrate in the table.3. Show the best result histogram equalization and convolution.

Table (3). the best result histogram equalization and convolution

mask		1	2	3	4	5	6	7	8	9
1										
	Hist	73	217	386	271	270	490	225	93	0
2										
	Hist	0	56	455	520	444	495	55	0	0
3										
	Hist	95	211	320	225	252	291	243	121	161
4										
	Hist	121	243	291	252	225	320	211	95	106

8.4 Key Generation and Test key

In this paper, the key generation after extraction the features for QR code. In the table.4 show result for test key and illustrate the strongest tests to obtain a stronger key used in the encrypt process.

Table (4). the result test key

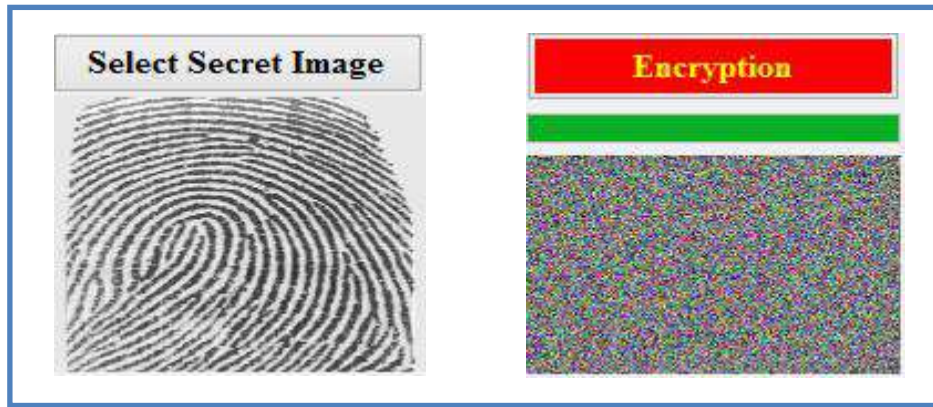
	Type Test	Parameterize test	No Test	Success	Failure	%
1	G using SHA-1	Approximate Entropy TEST	255	255	0	100%
		BLOCK FREQUENCY TEST	255	255	0	100%
		CUMULATIVE SUMS TEST	510	503	7	98%
		Discrete FFT TEST	255	255	0	100%
		Frequency TEST	255	253	2	99%
		LEMPEL-ZIV COMPRESSION	255	253	2	100%

		TEST				
		linear-complexity	255	255	0	100%
		Non periodic-templates	255	255	0	95%
		overlapping-templates	37740	35855	1885	100%
		random-excursions	255	255	0	100%
		runs	255	255	0	98%
		Serial	255	252	3	98%
2	Linear Cingruential	Approximate Entropy TEST	128	128	0	100%
		BLOCK FREQUENCY TEST	128	123	5	96%
		CUMULATIVE SUMS TEST	256	248	8	96%
		Discrete FFT TEST	128	128	0	100%
		FREQUENCY TEST	128	123	5	96%
		LEMPEL-ZIV COMPRESSION TEST	128	0	128	0%
		linear-complexity	128	128	0	100%
		Non periodic-templates	18944	16675	2269	88%
		overlapping-templates	128	128	0	100%
		RANK TEST	128	128	0	100%
		RUNS TEST	128	126	2	98%
		SERIAL TEST	256	250	6	97%
3	Blum-Blum-Shub	Approximate Entropy	128	128	0	100%
		BLOCK FREQUENCY TEST	128	125	3	97%
		CUMULATIVE SUMS	256	253	3	98%
		Discrete FFT	128	128	0	100%
		FREQUENCY TEST	128	125	3	97%
		LEMPEL-ZIV COMPRESSION TEST	128	128	0	100%
		linear-complexity	128	128	0	100%
		Non periodic-templates	18944	16705	2239	88%
		overlapping-templates	128	128	0	100%
		RANK TEST	128	128	0	100%
		RUNS TEST	128	128	0	100%
		SERIAL TEST	256	255	1	99%
4	Xor	Approximate Entropy	181	181	0	100%
		BLOCK FREQUENCY TEST	181	181	0	100%
		CUMULATIVE SUMS	362	362	0	100%
		Discrete FFT	181	181	0	100%
		FREQUENCY TEST	181	180	1	99%
		LEMPEL-ZIV COMPRESSION TEST	181	181	0	100%
		LONGEST RUNS OF ONES TEST	181	181	0	100%
		NONPERIODIC TEMPLATES TEST	26788	21429	5359	79%
		RANK TEST	181	181	0	100%
		RUNS TEST	181	178	3	98%
		SERIAL TEST	362	357	5	98%

9. Encryption and Decryption

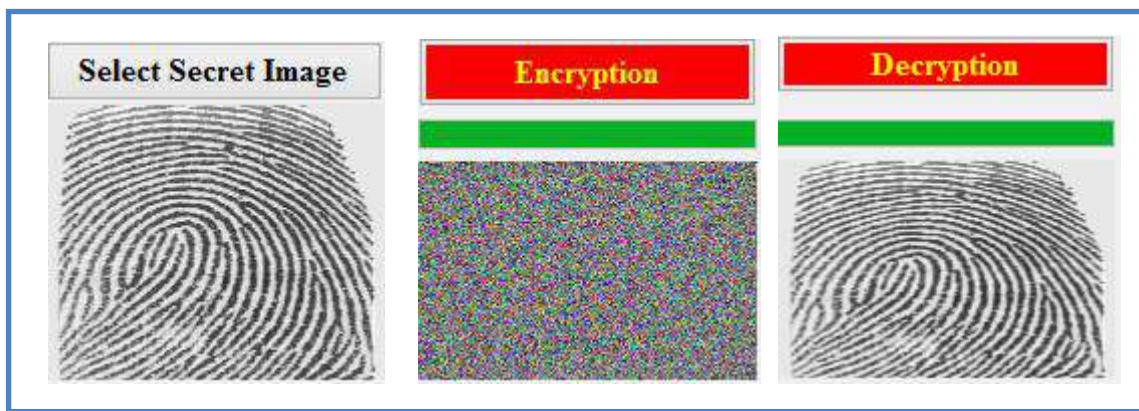
9.1 Finger Print Encryption

The fingerprint images are used to be encrypted where the proposed system will selected secret image from the CASIA Finger Print Image Database version 5.0. The result for encryption process illustrate below:



9.2 Finger Print Decryption

After encryption for finger print image, the proposed system will decrypt. The result for encryption process illustrate below:



10. Measure of Image Quality

In this paper, after finger print encryption will applied many of measures such as (MSE, MAE, PSNR, UACI, and NPCR) to find out the best image quality measurements. In this table.5. Will show the result measure of image quality after applied many of fundamentals of the image quality criteria where applied equations for MSE, MAE, PSNR, UACI, and NPCR for obtain error metrics.

Table (5) The result measure of image quality

	Image		Error Metrics				
	Original	Encryption	MSE	MAE	PSNR	UACI	NPCR
1			17198.506	111.355	5.7758	43.498	0
2			14740.530	100.685	6.4456	39.330	0.31150
3			14014.633	98.9053	6.6649	38.634	0
4			15640.655	105.215	6.1882	41.099	0

11. Conclusion

These days it is required to keep up with the latest technologies. The proposed system performing better in the fingerprint encryption and decryption. Where the system proposed used measure NIST (National Institute of Standards and Technology) for random key, where give result excellent in the several measures in the test key reach for (100%, 99%, 98%, 97%). Also the system proposed give result excellent in the measures of image quality depending on)MSR, PSNR, MAE, UACI, NPCR, Correlation, Entropy), for encryption and decryption. In this paper through the use of fingerprint images the results of encryption and decryption were good compared with all biometrics images.

References

- [1] K. Mohod, L. Thomas and R. Thorat, " **Security System based on QR Code with Iris Recognition** ", International Journal of Computer Applications (0975 – 8887), National Conference on Advances in Computing, Communication and Networking (ACCNet), 2016.
- [2] R. Thai, " **Fingerprint Image Enhancement and Minutiae Extraction** ", 2003.
- [3] Jain, A., Hong, L., Pankanti, S., and Bolle, R. " **An identity authentication system using fingerprints** ", In *Proceedings of the IEEE*, vol. 85, pp. 1365–1388, September 1997.
- [4] I. P. WARDHANI, S. A. SUDIRO and BHETA AGUS WARDIJONO, " **Fingerprint dataset development For Biometric Recognition System Evaluation** ", Proceedings of Fifth The IER-SCIENCE PLUS International Conference, Singapore, ISBN: 978-93-84209-62-9, 08th, November 2014.
- [5] A. Singhal and R.S Pavithr, " **Degree Certificate Authentication using QR Code and Smartphone** ", International Journal of Computer Applications (0975 – 8887), Vol 120, No.16, June 2015.
- [6] F. Masalha and N. Hirzallah, " **A Students Attendance System Using QR Code** ", International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 5, No. 3, 2014.
- [7] N. Poompaval and R. Balasubramanian, " **A Novel Binarization Method For QR-Codes Under ILL Illuminated Lightings** ", International Journal of Advanced Research in Computer Science and Applications, ISSN 2321-872X Online 2321-8932 Print, Vol. 2, Issue 10, October 2014.
- [8] N. Mujumdar, P. Shinde, K. Thigale and S. Agrawal, " **Application Of Smart Phone QR Code And Fingerprint For Anti-Counterfeiting** ", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 2 Issue 4, April –2013.
- [9] Y. Liu and M. Liu, " **Automatic Recognition Algorithm of Quick Response Code Based on Embedded System** ", IEEE Proceedings of the Sixth International Conference on Intelligent Systems Design and Applications (ISDA'06), April 16, 2009.
- [10] M. Warasart and P. Kuacharoen, " **Paper-based Document Authentication using Digital Signature and QR Code** ", 4TH International Conference on Computer Engineering and Technology, 2012.
- [11] M. K. Revathi, P. Annapandi and K. P. Ramya, " **Enhancing Security in Identity Documents Using QR Code** ", IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 5, Oct-Nov, 2013.
- [12] CASIA-Database. <http://www.cbsr.ia.ac.cn/english/Finger Print Database.asp>.
- [13] A. Rukhin, J. Soto, J. Nechvatal, and etc., " **A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications** ", Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930, April 2010.
- [14] K. L. Chung, Elementary Probability Theory with Stochastic Processes. New York: Springer-Verlag, 1979.
- [15] N. Maclaren, " **Cryptographic Pseudo-random Numbers in Simulation** ", Cambridge Security Workshop on Fast Software Encryption, Dec. 1993.
- [16] J. D. Gibbons, Nonparametric Statistical Inference, 2nd ed. New York: Marcel Dekker, 1985.
- [17] A. P. Godbole and Stavros G. Papastavridis (ed), *Runs and Patterns in Probability: Selected Papers*. Dordrecht: Kluwer Academic, 1994

- [18] George Marsaglia, DIEHARD: a battery of tests of randomness. <http://www.stat.fsu.edu/pub/diehard/>.
- [19] W. Killman, J. Schüth, W. Thumser, and I. Uludag, A Note Concerning the DFT Test in NIST Special Publication 800-22, T-Systems, Systems Integration, July 2004.
- [20] A. D. Barbour, L. Holst, and S. Janson, Poisson Approximation (1992).
- [21] K. Hamano and T. Kaneko, The Correction of the Overlapping Template Matching Test Included in NIST Randomness Test Suite, IEICE Transactions of Electronics, Communications and Computer Sciences 2007.
- [22] J-S Coron and D. Naccache, "**An Accurate Evaluation of Maurer's Universal Test**", Proceedings of SAC '98 (Lecture Notes in Computer Science). Berlin: Springer-Verlag, 1998.
- [23] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, 1997.
- [24] D. E. Knuth, the Art of Computer Programming. Vol. 2, 3rd ed. Reading: Addison-Wesley, Inc., pp. 61-80, 1998.
- [25] A. Rukhin, "**Approximate entropy for testing randomness**", Journal of Applied Probability, Vol. 37, 2000.
- [26] Pal Revesz, Random Walk in Random and Non-Random Environments. Singapore: World Scientific, 1990.
- [27] P. Revesz, Random Walk in Random and Non-random Environments. Singapore: World Scientific, 1990.
- [28] M. Baron and A. L. Rukhin, "**Distribution of the Number of Visits for a Random Walk**", Communications in Statistics: Stochastic Models, Vol.15, 1999.
- [29] C. S. Varnan, A. Jagan, J. Kaur, D. Jyoti, and D. S. Rao, "**Image Quality Assessment Techniques pn Spatial Domain**", IJCST Vol. 2, Issue 3, September 2011.
- [30] H. M. Al-Mashhadi, "**Quality Assessment for Image Encryption Techniques using Fuzzy Logic System**", International Journal of Computer Applications (0975 – 8887), Volume 157 – No 5, January 2017.
- [31] M. S. Khalefa, Z. A. Abduljabar and H. A. Zeki, "**Fingerprint Image Enhancement by Develop Mehtre technique**", Advanced Computing: An International Journal (ACIJ), Vol.2, No.6, November 2011.
- [32] D. Heeger, "**Signals, Linear Systems, and Convolution**", and Young (1983), and Oppenheim and Schafer (1989), September 26, 2000.

AES Cipher Key Generation Based on Exponential Chaotic System

Ahmed Kareem Shibeb¹ Mohammed Hussein Ahmed²

¹Middle Technical University, Technical Institute -Suwaira, Department of Computer Systems, kahmad35@yahoo.com

²Mustansiriyah University, College of Education, Department of Computer Science
mhmi8586@yahoo.com

Abstract:

The key generation operation considers as the great significance parameter in improving the level of security of the AES algorithm. In other hand, the remarkable characteristics of exponential chaotic system like its ability to produce very complex patterns of behavior, all the control parameters and initial conditions can be made as the secret-key, high-dimensional feature and its mastery to generate chaotic sequences made it more convenient than the low-dimensional and high-dimensional chaotic system for the key generation process due to use exponent term ($d^{\wedge}(z^{\wedge}2)$) which made it very complex. Thus, this paper proposes a novel approach that uses an exponential chaotic system with one nonlinear term ($d^{\wedge}(z^{\wedge}2)$) to generate the cipher key of the AES algorithm. The experimental results indicate that the pseudorandom bits of the proposed chaotic generator has been passed the statistical tests of randomness as well as the proposed system provide a high key sensitivity and key space, reasonable PSNR values and reduces the correlation coefficient between the adjacent pixels of the color images in addition to the system resistance against the differential attack.

Keyword: AES, CNG, Key Expansion, Exponential Chaotic System.

توليد مفتاح التشفير لخوارزمية التشفير القياسي المتقدم اعتمادا على نظام فوضوي اسي

احمد كريم شبيب محمد حسين احمد

المستخلص

تعتبر عملية توليد المفاتيح عامل ذا اهمية كبيرة في تحسين امن خوارزمية التشفير القياسي المتقدم. ومن ناحية اخرى، فان الخصائص البارزة للنظام الفوضوي الاسي مثل قدرته على انتاج انماط معقدة جدا من السلوك و امكانية جعل القيم الابتدائية والمتغيرات كمفاتيح سرية. فضلا عن خاصية الابعاد العالية والتي تجعلها ملائم اكثر من الانظمة ذات الابعاد القليلة و بعض الانظمة ذات الابعاد العالية نظرا لاستخدام الحد الاسي ($d^{\wedge}(z^{\wedge}2)$) و الذي يجعلها اكثر تعقيدا. لذلك هذا البحث يقترح طريقة جديدة تستخدم النظام الفوضوي الاسي بحد غير خطي واحد ($d^{\wedge}(z^{\wedge}2)$) لتوليد مفتاح التشفير لخوارزمية التشفير القياسي المتقدم. نتائج الاختبار تشير الى ان بتات المولد الفوضوي المقترح قد اجتازت الاختبارات الاحصائية للعشوائية فضلا عن ان النظام المقترح يوفر سعة مفتاح عالية وكذلك حساسية عالية لكل تغيير في مفتاح التشفير، ويعطي قيم (PSNR) منطقية و يقلل معامل الارتباط بين البكسلات المتجاورة للصور الملونة بالاضافة الى قوة النظام ضد الهجوم التفاضلي.

الكلمات المفتاحية: خوارزمية التشفير القياسي المتقدم، مولد الارقام الفوضوي، توسيع المفتاح، النظام الفوضوي الاسي.

I. Introduction

Cryptography is an effective art to secure the information that transmitted via the communication networks [1]. Cryptanalysis is the way or art of gaining the hidden messages into cipher texts [2]. Both of cryptography and cryptanalysis are part of a science called cryptology which is the most general term. The main usage of cryptography is transferring the information in a secure way from the source to the destination. The cryptography system components are a clear-text, cipher-key, cipher algorithm that takes a clear-text and cipher-key as input and cipher-text as output for the cipher algorithm. The cryptography is an effective way to secure the multimedia applications which is the multimedia applications are applications which utilize a combination of multimedia elements like image, animation, text, audio and video [3].

According to the number of keys, the cryptography is divided into broad categories which are: symmetric key algorithms and asymmetric key algorithms, where the symmetric algorithms has one key for encryption and decryption processes and two keys are used for encryption and decryption

processes through the asymmetric algorithms [4]. The Advanced Encryption Standard is one of most popular symmetric block cipher algorithm designed by two young Belgian, John Daemen and Vincent Rijmen in 1998. The AES cipher was announced by the NIST to take the place of the old Data Encryption Standard as new Advanced Encryption Standard. The AES according to the FIPS publication 197 [5] that described more details of AES by The NIST has a plaintext with fixed block size of 128 bits, the data have passed through 10, 12 and 14 rounds, this number of rounds determined by flexible key sizes of 128 bits, 192 bits and 256 bits, respectively. In other hand, the chaos defined as an inherent property of a class of nonlinear systems, which is deterministic system that exhibits great sensitivity to initial conditions and contains an infinite number of unstable periodic motions [6].

The chaos theory has many maps with different dimension like, one-dimensional map (Logistic Map), two-dimensional map (Henon Map) and three-dimensional map (Lorenz system). Due to the important of the key generation operation in AES algorithm, there are many related works with this proposed system focused on the AES key generation. In [7] the performance and security of image encryption have been enhanced by appending a weak key stream generator (W7,A5/1) to AES algorithm with respect of avoiding the textured zones problem which exists in other renowned cryptosystems. As obtained in detailed analysis of this proposed cryptosystem [7], it can be achieved readily in both software and hardware but it requires more time. However, M. K. Khan, M. Usama, and F. Muhaya use six chaotic maps (Tent, Logistic, Sine, Chebyshev, Henon and Cubic maps) to increase the complexity of the AES key generation by XOR'ing the output of these maps. Despite the long time consumed in the key generation due to the large number of chaotic maps and the proposed scheme is applied to encrypt the satellite images that featured with large size and redundant data, it provides a good diffusion and confusion characteristics and ideal for real time applications in addition to enhance the key generation of the AES algorithm [8]. And also the chaotic maps are used in [9], so that the proposed system permutes the pixel positions of satellite images by using a two-dimensional map called Arnold map to reduce the correlation among adjacent pixels, then encrypt it by using AES algorithm that depend on Henon map for key generation. This proposed system requires long time for encryption and decryption processes due to the permutation operation and the large size of the satellite images so that the sample size of this system is 652094 bytes at 10-meter resolution. While S. M. Wadi and N. Zainal encrypt high definition image (HD) with modified AES which proposes three modifications. In addition to propose a simple and low secure method for S-box construction and reduce the mix columns transformation of the encryption rounds, one of these modifications increases the security of key schedule operation by adding the mix columns transformation to the existing key schedule transformations, but this modification will decrease the encryption/decryption time [10]. This paper proposes an effective method for AES key generation by applying a certain equation for the exponential chaotic system output which saved in real array and took the array numbers from the last number toward the first number, and then expand the master key that had been generated with key expansion routine for each encryption round.

II. Transformations of AES Algorithm

The AES has four basic transformations (Substitution Bytes, Shift Rows, Mix Columns and Add Round Key) used in each encryption round except the last round which doesn't have the Mix Columns transformation. Before the encryption rounds that depend on the key size, the Add Round Key transformation is applied between the master key and the data block (state array). These transformations are explained as followed [11]:

- Substitution Bytes:** The Substitution Bytes transformation is a non-linear byte substitution that acts on every byte of the state in isolation to produce a new byte value using an S-box substitution table and InvS-box table through encryption and decryption process, respectively.
- Shift Rows:** During the forward shift rows transformation, the bytes in the last three rows of the state array are cyclically shifted; on the other hand, offset of the left shift varies from one to three bytes. However, the same operation is used in backward transformation, but the shifting toward the right side instead of the left side.
- Mix Columns:** This transformation counters to the previous transformation so that it operates on the state column-by-column instead of row-by-row. Each byte of a column interacts with every

other byte of the column. In encryption and decryption process, each column is multiplied over Galois Field (GF) by a fixed matrix.

d. Add Round Key: The last transformation of a round carries out XOR operation between the round key and the state array. This step is its own inverse.

III. The Key Expansion of AES Algorithm

The key expansion or the key schedule routine is an operation of generating a number of sub-keys from the cipher key for each round to be used in the AddRoundKey operation. Therefore, the number of needed sub-keys is equal to the number of rounds (NumRound) and hence the round keys contain 44,52 and 60 words will be generated for AES-128, AES-192 and AES-256, respectively. Where each word equal to four bytes. The words are indexed from 0 to 43. The first four word (W_0, W_1, W_2, W_3) are filled with the given cipher key, however columns in locations that are a multiple of 4 ($W_4, W_8, W_{12} \dots W_{40}$) will be computed by three operations which are:

a. The RotWord: this operation performs one cyclic permutation on a four-byte word, If the input word is (1, 2, 3, 4), the output word of this operation (RotWord) is (2, 3, 4, 1).

b. The SubWord: applies a byte substitution operation as described in Substitution Bytes transformation on each byte of its input word.

c. Perform XOR operation for the result of a RotWord and SubWord operations with word W_{i-4} and with a Round Constant ($Rcon[i]$).

However, the remaining words of sub-key will be created by using an XOR operation between the previous words W_{i-1} with the word W_{i-4} , where the W_i is the current Word.

IV. Chaos Exponential System

Recently, the exponential chaotic system has attracted a great attention to induce more complex chaotic attractor. In [12], a new three dimensional exponential chaotic system is designed with one exponential nonlinear term that has simple mathematical structure compared with other exponential chaotic system as expressed through the following three ordinary differential equations (ODE):

$$\frac{dx}{dt} = -\alpha y + (d^{\wedge} (z^{\wedge} 2))$$

$$\frac{dy}{dt} = \nu y + x$$

$$\frac{dz}{dt} = x - \beta z$$

(1)

Where (α, ν, β and d) are all real values which consider as the parameters for this chaotic system, while (x, y, z) are the system states. The best chaotic behavior for this system attractor appears when the parameters values are ($\alpha = 10.0, \beta = 3.5, \nu = 0.65$ and $d = 4.7$) as shown in Fig. (1) where the initial values of x, y and z are 0.1, 0.1 and 0.01 respectively.

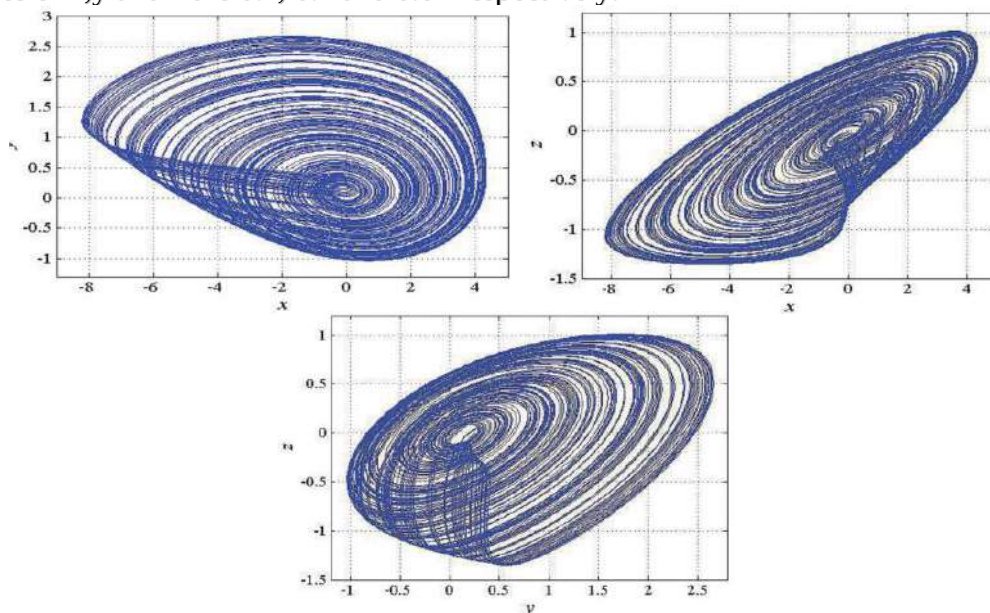


Fig. (1): Phase portraits of chaotic attractors of system.

V. The proposed Method

Before obtaining the sequences of the exponential chaotic system equations those expressed in equation (1), the equations of exponential system must be solved by numerically solving. One of the simplest and best performance numerical techniques that have been recently used for solving the

chaos system is Euler technique. Thus, the proposed system will be used Euler technique to solve the exponential system during key generation process. To increase the complexity of the key generation and due to the high changing in the last numbers of outputs real values. Chaotic Numbers Generator (CNG) depends on solving the exponential chaotic system and saving its result in a certain array, and then taking the elements of the array beginning of the last element to the first element down to the key size to apply the below equation for them.

$$Z(i) = \text{Round}((X(i) * 10^9) - \text{Floor}(X(i) * 10^9)) \quad (2)$$

Where the Floor and Round are mathematical functions used for rounding of numerical data to the largest integer that is less than or equal to $X(i)$ and to the nearest integer number, respectively. While the $X(i)$ is the element of the exponential chaotic system array and $i = 0, 1, 2, \dots$ key size. The result of the above equation is a sequence of bits (0,1) whose represent the key size after converting each four adjacent bits to a hexadecimal number. The cipher key that generated based on exponential chaotic system will be expanded with a key expansion routine which described with its transformations in section (III). The Fig. (2) Shows how the cipher key has been generated and expanded.

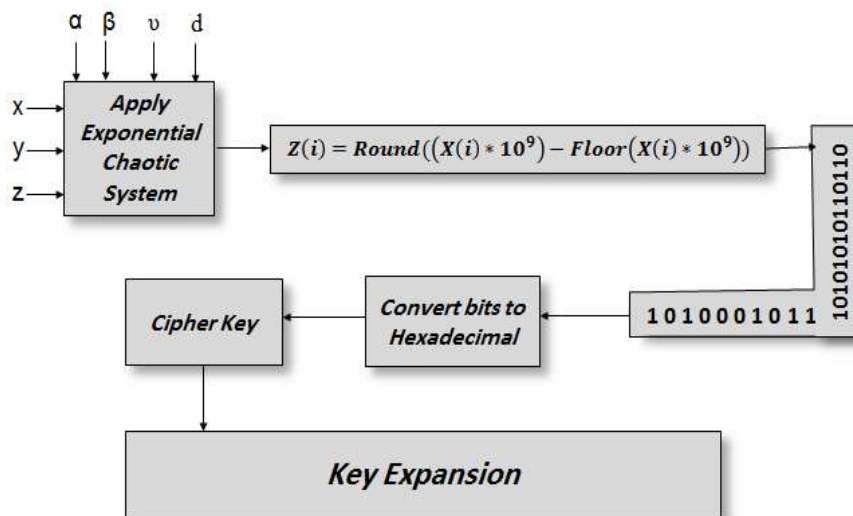


Fig. (2): Block diagram of the proposed scheme.

VI. Security Analysis

A. Statistical Tests of the Pseudorandom Bit Generator

In the generation of any bit sequence must be subordinated to the set of tests to ensure the power of the generator. Tests of statistical experiment present that are commonly used tests in determine whether the binary sequence has some specific properties [13]. These statistical tests represented by the randomness tests that included on only five tests: frequency test, serial test, poker test, run test and autocorrelation test which are applied on the different key sizes that generated based on exponential chaotic system when the initial conditions and parameters values of the exponential chaotic system are ($x = 0.0000001$, $y = 0.0000001$, $z = 0.0000001$, $\alpha = 10.0$, $\beta = 3.5$, $\gamma = 0.65$, $\delta = 4.7$ and max step = 300). The generated bits passed the statistical tests as shown in Table (1) which explains the result of statistical tests and the passed values for each test (Threshold) for different AES key sizes.

Table (1) The (χ^2) of statistical tests for different key sizes.

Statistical Test	Key Size	χ^2	Threshold
Frequency Test	128 bits	0.3011	Must be ≤ 3.84
	192 bits	0.3644	
	256 bits	0.2666	
Serial Test	128 bits	1.8841	Must be ≤ 5.9915
	192 bits	0.7229	
	256 bits	0.2474	

Poker Test	128 bits	3.1842	Must be ≤ 14.0671
	192 bits	3.896	
	256 bits	4.9201	
Auto Correlation Test	128 bits	1.0722	Must be ≤ 3.841
	192 bits	1.5613	
	256 bits	1.0271	
Run Test	128 bits	9.8734	Must be ≤ 22.362
	192 bits	7.7141	
	256 bits	16.2862	

B. Key Analysis

1. Key Space

The large key space is required to realize a high degree of security for the proposed system, which would be impractical for the attacker in attempting knowing the proposed system key by simply trying all possible keys. The key space of chaotic key generator which used for the cipher key of modified AES algorithm is 2^{128} , 2^{192} , or 2^{256} . Thus, the proposed system provides high resistance against the brute force attack.

2. Key Sensitivity

The major requirement of any key in the system is high key sensitivity, which means that the encrypted image cannot be decrypted correctly albeit there is only a slight difference between encryption or decryption keys. Any slight change for the secret key will lead to another cipher text quite different from the previous cipher text for example when the ($x = 0.0000001$, $y = 0.0000001$, $z = 0.0000001$, $\alpha = 10.0$, $\beta = 3.5$, $v = 0.65$ and $d = 4.7$), the key sensitivity test of the modified AES algorithm has been performed on Girl image by using the same cipher key that is used in the encryption process except that the (x) value is changed to 0.0000002. The Fig. (3) shows the plain image, encrypted image and decrypted image which decrypted with incorrect key and with the correct key.



A. Original Image



B. Cipher Image



C. Image decrypted with incorrect key



D. Image decrypted with correct key

Fig. (3): The result of key sensitivity analysis.

C. Peak Signal to Noise Ratio (PSNR)

The quality of encryption can be estimated by using PSNR measure which checks the changes in the pixel value between the cipher image (noise) and the plain image (signal) [14]. The perfect encryption quality relies at the lower value for PSNR. In other words, the small value of PSNR is best than the large value of PSNR. Hence the proposed scheme introduces an excellent encryption quality as obtained in Table (2).

Table (2) Encryption quality analysis for different plain and cipher images.

Image	PSNR of Cipher Image
Girl	7.3404
Pepper	7.4445
Lena	8.9779
Baboon	8.6926

D. Image Histogram

The pixel values distribution of each image can be reflected by image histogram. The histogram of the encrypted image should be as uniform distribution as possible, which means that the probability of existence of any color scale value is the same, and it is fully messy [15]. Fig. (4) shows the RGB histograms of the original Girl image and the cipher image. We can see that; the histogram of the cipher image is fairly uniform distribution. Hence the proposed method does not present any clue to employ any statistical attack on the encrypted image.

E. Correlation Coefficients Analysis

The major problem with images is the relationship among the adjacent pixels in the original image. In order to overcome this problem and to increase a cryptosystem resistance against the expected attacks, the correlation coefficient between the adjacent pixels either in horizontal, vertical or diagonal direction should reduced to be close to zero. Wherever, the correlation coefficient of the original image closes to one, while the minus one means the encrypted image is the converse of the original image [16]. The proposed method reduces the correlation coefficient among adjacent pixels as illustrated in Table (3).

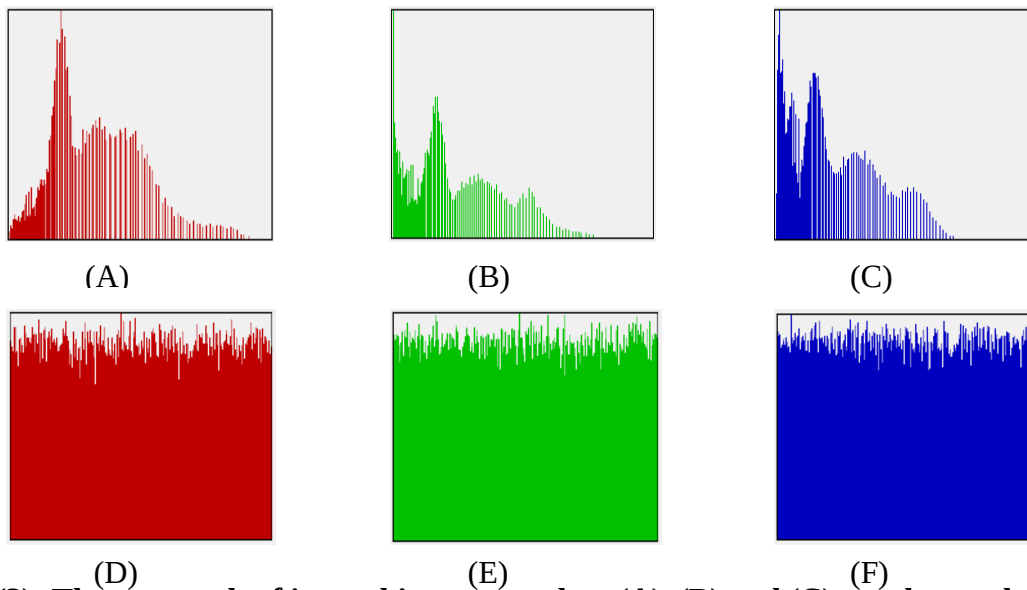


Fig. (3): The test result of image histogram, where (A), (B) and (C) are the result of the original Image (Red, Green and Blue channels). (D), (E) and (F) are the result of the cipher Image for the same channels.

Table (3) Correlation coefficients of the adjacent pixels.

Image		Horizontal	Vertical	Diagonal
Girl	Plain	0.959	0.9781	0.8319
	Cipher	0.0036	0.0065	0.0211
Pepper	Plain	0.9512	0.9492	0.8942
	Cipher	0.0076	- 0.0041	- 0.0727
Lena	Plain	0.9512	0.9349	0.8945
	Cipher	- 0.0012	- 0.0028	- 0.0397
Baboon	Plain	0.7317	0.6698	0.6512
	Cipher	0.0086	0.0061	0.0075

F. Resistance to Differential Cryptanalysis

The differential cryptanalysis is one of the most powerful cryptanalysis against block cipher, the differential cryptanalysis attempts to observe differences of the cipher image in the tiny change of the original image to find the relationship between the original image and the cipher image. To evaluate the cryptosystem resistance against differential attack, two measures (NPCR) and (UACI) commonly used, whereas the (NPCR) means that the change in rate of the pixels number of the encrypted image when only one pixel of the original image is changed and the (UACI) means the unified average changing intensity which gauges the average intensity of variations between the original image and encrypted image. The ideal NPCR and UACI values for 8-bit gray scale image are 99.609% and 33.464%, respectively [17]. Table (4) shows the test results of NPCR and UACI, respectively. Generally, it is discovered that the NPCR and UACI values of the proposed method is close to their ideal values.

Table (4) Measurements of NPCR and UACI for different images

Frame	NPCR (in %)	UACI (in %)
Girl	99.6268	33.5091
Pepper	99.5271	33.4751
Lena	99.708	33.5279
Baboon	99.6493	33.4011

VII. Conclusion

Actually, the AES is most efficient block cipher algorithm and the key generation is an important operation in AES algorithm. In another hand, the key expansion routine depends on the cipher key and it has fast and secure transformations to expand the master key into set of sub keys known as round keys to utilize them during add round key transformations for each encryption round. Therefore, the proposed method uses the complex exponential chaotic system to generate the cipher key which added with the data block and used as master key for key expansion routine. The pseudo random number generator passed the randomness tests as well as the proposed method provides high key space, high key sensitivity, and reasonable PSNR values for different frames in addition to reduce the correlation coefficient between adjacent pixels and the system resistance against the differential attack.

References

- [1] M. Bishop, **"Introduction to Computer Security"**, Pearson Publications, First Edition, 2005.
- [2] M. E. Whitman and H. J. Mattord, **"Principles of Information Security"**, Thomson course technology, 2007.
- [3] Z. Li, J. Liu and M. S. Drew, **"Fundamentals of Multimedia"**, Springer International Publishing, Second Edition, 2014.
- [4] Bruce Schneier and Niels Ferguson, **"Practical Cryptography"**, Wiley Publishing, Inc., First Edition, 2003.
- [5] National Institute of Standards and Technology, **"Advanced Encryption Standard"**, NIST FIPS PUB 197, November 2001.
- [6] S. A. Abaas and A. K. Shabeeb, **"A New Approach for Video Encryption Based on Modified AES Algorithm"**, IOSR Journal of Computer Engineering, June 2015.
- [7] M. Zeghid and et al, **"A Modified AES Based Algorithm for Image Encryption"**, World Academy of Science, Engineering and Technology, March 2007.
- [8] F. Bin Muhaya, M. Usama, and M. Khurram Khan, **"Modified AES Using Chaotic Key Generator for Satellite Imagery Encryption"**, 5th International Conference on Intelligent Computing, Springer, September 2009.
- [9] F. Bin Muhaya, **"Chaotic and AES cryptosystem for satellite imagery"**, Telecommunication Systems, Springer, June 2011.
- [10] S. M. Wadi and N. Zainal, **"High Definition Image Encryption Algorithm Based on AES Modification"**, Wireless Personal Communications, Springer, June 2014.
- [11] Jianyong Houg, **"On the internal structure of the advanced encryption standard and two AES-based cryptographic constructions"**, Ph.D Thesis, University of Wollongong, School of Computer Science and Software Engineering, May 2012.
- [12] B. Cai, G. Wang, and F. Yuan, **"Pseudo Random Sequence Generation from a New Chaotic System"**, Proceedings of ICCT2015, IEEE, 2015.
- [13] A. Menezes, P. Oorschot and S. Vanstone **"Handbook of Applied Cryptography"**, First Edition, CRC Press, October 1996.
- [14] G. Hanchinamani and L. Kulkarni, **"An Efficient Image Encryption Scheme Based on a Peter De Jong Chaotic Map and a RC4 Stream Cipher"**, 3D Display Research Center, Springer, July 2015.
- [15] J. Chen and et al, **"A fast image encryption scheme with a novel pixel swapping-based confusion approach"**, Nonlinear Dynamics, Springer, April 2014.
- [16] M. A. Shreef and H. K. Hoomod, **"Image Encryption Using Lagrange-Least Squares Interpolation"**, International Journal of Advanced Computer Science and Information Technology (IJACSIT), 2014.
- [17] J. Ahmad, S. Hwang and A. Ali, **"An Experimental Comparison of Chaotic and Non-chaotic Image Encryption Schemes"**, Wireless Personal Communications, Springer, May 2015.

Cipher text Hiding in Image Based on New Generation Key Method of 3DES Algorithm

Zainab khyioon Abdalrdha¹ Zahraa Salah Dhaief¹ Hashem B. Jehlol²

¹Mustansiriyah University, College of Education, Dept. of Computer Science

²Mustansiriyah University, Avicenna Center for E-learning

zainabkhyioon83@yahoo.com zehraa_84@yahoo.com

Abstract:

Information hiding represents a class of processes used to embed data into various forms of digital data such as image, audio, and video. In digital images the information hiding applications could be divided groups depending on the relationship between the embedded message and the cover image. This Search aims to provide the user with a technique to increase the information security level by using a cryptography steganography and combination. Cryptography is the term that involves encryption method to make information secure in this work presents a new session key generation stage by using Message Digest Version5 (MD5) Algorithm then the combining MD5 Algorithm output with Triple Data Encryption Standard (Triple DES) Algorithm to reduce the key generation stage in Triple DES and also to increase the security for Triple DES Algorithm, Information is encryption by using 3DES algorithm to provide cipher text that can be recovered. Steganography here comes with the effect of transmission without revealing the secure information the text in the image being hidden by using LSB techniques that are optimized by XOR method which increases the security of the text before it send across the medium because of using password as key of XOR to be tested with cipher text.

The proposed system in this work is made by using visual basic.net 2010 and it was designed for color image.

Keyword: Cryptography, Steganography, MD5 Message-Digest Algorithm, 3DES (Triple Data Encryption Standard Algorithm).

أخفاء النص المشفر في الصورة بالاعتماد على طريقة جديدة لتوليد مفاتيح خوارزمية 3DES

زينب خيون عبد الرضا زهراء صلاح ضايف هاشم بدر جهلول

المستخلص

إخفاء المعلومات يمثل نوع العمليات المستخدمة لتضمين البيانات في مختلف أشكال البيانات الرقمية مثل الصورة، التسجيل الصوتي، والفيديو. في الصور الرقمية تطبيقات إخفاء المعلومات يمكن ان تقسم بالاعتماد على العلاقة بين الرسالة المضمنة وصورة الغطاء.

النظام المقترح في هذه الرسالة يزود المستخدم بالية لزيادة مستوى سرية المعلومات بواسطة استخدام "cryptography and steganography" مجتمعه. الكتابة المشفرة هو مصطلح الذي يتضمن العديد من طرق التشفير التي تصنع سرية المعلومات في هذا العمل قدم مرحلة جديدة لتوليد مفتاح الجلسة بواسطة خوارزمية MD5 ثم الدمج ما بين مخرجات خوارزمية MD5 مع خوارزمية Triple DES لتقليل مرحلة توليد المفاتيح في خوارزمية Triple DES، وذلك لزيادة أمانة خوارزمية Triple DES اذ خوارزمية 3DES. استخدمت في هذه الرسالة لتشفير المعلومات التي تزودنا بنص مشفر وبعد ذلك نستطيع استرجاع النص الأصلي Steganography يأتي هنا مع تأثير الإرسال بدون تشويه المعلومات السرية، اذ تم أخفاء نص في الصورة بواسطة استخدام تقنية البتات الأقل أهميه "LSB" والتي تم تحسينها عن طريق استخدام طريقة XOR التي تزيد السرية والتعقيد للرسالة قبل الإرسال عبر الوسط بسبب استخدام كلمه مرور كمفتاح لا XOR لتي يتم اختبارها مع النص المشفر لنقرر ما نوع البت الذي سيضمن (0 أو 1). لذلك المرسل والمستلم للرسالة سوف يكون امن وسري مع زيادة بالموثوقيه، النظام المقترح في هذه الرسالة تم كتابته بواسطة اللغة البرمجية الفيجول بيسك دوت نت 2010، وهو مصمم للصور الملونة.

الكلمات المفتاحية: التشفير، الإخفاء، خوارزمية الرسالة المبعثرة، خوارزمية بيانات التشفير القياسية

I. Introduction

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication, Cryptography is not the only means of providing information security, but rather one set of techniques [1]. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications, and the development of Internet technologies. In data and telecommunications, cryptography is necessary when communicating over any entrusted medium, which includes as authentication and privacy conditions in any network, particularly the Internet [2]. A cryptographic scheme for a given task is secure if no adversary of a specified power can achieve a specified break [3]. In this work, both symmetric and asymmetric cryptographic mechanisms are used together in order to take advantage of the strengths of each; specifically, the ability to distribute public keys without concerns of confidentiality (a strength of asymmetric key cryptography), and the faster encryption/decryption speed of secret keys (a strength of symmetric key cryptography relative to asymmetric). Cryptography is not the only means of providing information security, instead of the traditional method that used in new method stages. The proposed algorithm based on generation key from MD5 algorithm then encryption text by 3DES algorithm increase the security of the system.

II. Cryptography

Cryptography is one of the traditional methods used to guarantee the privacy of communication between parties. This method is the art of secret writing, which is used to encrypt the plaintext with a key into cipher text to be transferred between parties on an insecure channel. Using a valid key, the cipher text can be decrypted to the original plaintext. Without the knowledge of the key, nobody can retrieve the plaintext. Cryptography plays an essential role in many services, like: confidentiality, key exchange, authentication and non-repudiation. Cryptography provides these services for secure communication across insecure channels; Figure 1 shows the cryptography system [4]. There are three types of cryptographic schemes for securing the data: public-key cryptography, secret key cryptography, and hash functions. These schemes are used to achieve different objectives. The length and type of the keys used depend on the type of encryption algorithm [4].

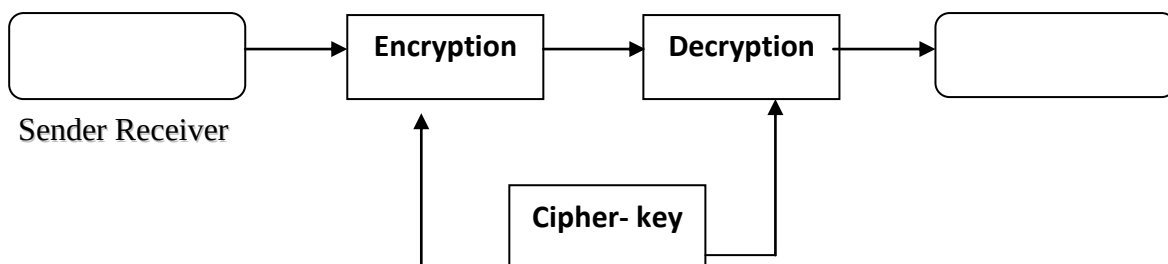


Fig.(1): Cryptography System [5]

2.1 Symmetric-Key Cryptography

The technique of symmetric-key encryption is also known as the symmetric-key, shared key and single-key encryption. In this technique, the same secret-key is used for both encryption and decryption sides [6].

The original information or plaintext is encrypted with a key by the sender. Then the same key is used by the receiver to decrypt the message and obtain the plaintext. The key is known only by those two parties who are authorized to do the encryption and decryption [6]. The technique provides good security for transmission. However, there is a difficulty in the key distribution. If the key is stolen the whole data security is compromised. Moreover, a secure mechanism is needed for safe key-exchange process. Examples of symmetric-key schemes include DES and AES algorithms [6].

2.2. Asymmetric-Key Cryptography

Asymmetric / Public Key Cryptography The asymmetric cryptosystem (or public key cryptosystem), employs two keys that are mathematically related, use separate for the encryption and decryption of data [4].

In this technique with the single key, it is not possible to access the information or easily determine the other key. The both of keys are required for the process to work. The key used for encryption is kept public and so as called public key, and the decryption key is kept secret and called private key. The keys are generated in such a way that it is impossible to derive the private key from the public key. Few examples of Asymmetric-Key Algorithms are RSA, Diffie Hell man, Digital Signature Algorithm (DSA), Public-Key Cryptography Standards (PKCS), Key Exchange Algorithm (KEA) etc[4].

2.3 Hash Functions

A hash function is a one-way collision-free function with a fixed-length output. Hash functions are also called message digests. A hash function is an algorithm that does not use any key. However, a fixed-length hash value is calculate based on the input data such that it computationally infeasible to obtain the input data from the hash value, or even any input string that matches the given hash value. Hash functions are usually used to produce digital fingerprints of files and to guarantee the integrity of the files [4].

3. Triple Data Encryption Standard Algorithm (Triple DES)

Triple DES is popular in Internet-based applications, including PGP and S/MIME. The possible vulnerability of DES to a brute-force attack brings us to find an alternative algorithm [7]. 3DES is an enhancement of DES; it is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that 3DES is slower than other block cipher methods [8].

Triple DES is a widely accepted approach which uses multiple encryptions with DES and multiple keys, as shown in Figure (2). The three-key triple DES is the preferred alternative, whose effective key length is 168 bits [9]. Triple DES was the answer to many of the shortcomings of DES. Since it is based on the DES algorithm, it is very easy to modify existing software to use Triple DES. It also has the advantage of proven reliability and a longer key length that eliminates many of the shortcut attacks that can be used to reduce the amount of time it takes to break DES. However, even this more powerful version of DES may not be strong enough to protect data for very much longer [7].

Triple DES is simply another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. Triple DES with two keys ($K_1 = K_3$, K_2) is a relatively popular alternative to DES [9].

3.1 Triple DES Encryption/Decryption

Triple DES with three keys (K_1 , K_2 , K_3) is preferred, as it results in a great increase in cryptographic strength. However, this alternative raises the cost of the known-plaintext attack to 2^{168} , which is beyond what is practical. Referring to Figure (2), the cipher text C is produced as

$$C = E_{K_3}[D_{K_2}[E_{K_1}(P)]]$$

The sender encrypts with the first key K_1 , then decrypts with the second key K_2 , and finally encrypts with the third key K_3 . Decryption requires that the keys are applied in reverse order:

$$P = D_{K_1}[E_{K_2}[D_{K_3}(C)]]$$

The receiver decrypts with the third key K_3 , then encrypts with the second key K_2 , and finally decrypts with the first key K_1 . This process is sometimes known as Encrypt Decrypt-Encrypt (EDE) mode [8]. Note that although the input key for DES is 64 bits long, the actual key used by DES is only 56 bits in length. The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits. This means that the effective key strength for Triple DES is actually 168 bits because each of the three keys contains 8 parity bits that are not used during the encryption process [7].

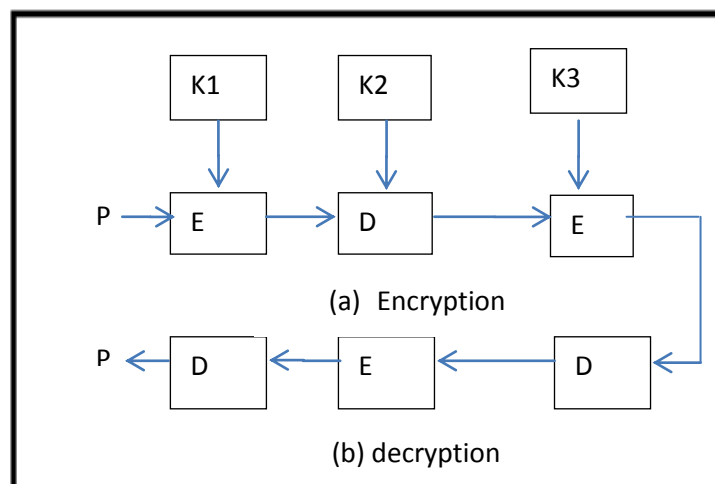


Fig. (2): Triple DES Encryption/Decryption

4. MD5 Method:

MD5 [10] consists of 64 of these operations, grouped in four rounds of 16 operations. F is a nonlinear function; one function is used in each round. M_i denotes a 32-bit block of the message input, and K_i denotes a 32-bit constant, different for each operation. S is a shift value, which also varies for each operation [11]. MD5 processes a variable length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks; the message is padded so that its length is divisible by 512. The padding works as follows: first a single bit, 1, is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message up to 64 bits less than a multiple of 512. The remaining bits are filled up with a 64-bit integer representing the length of the original message [12].

The main MD5 algorithm operates on a 128-bit state, divided into four 32-bit words, denoted A , B , C and D . These are initialized to certain fixed constants. The main algorithm then operates on each 512-bit message block in turn, each block modifying the state. The processing of a message block consists of four similar stages, termed rounds; each round composed of 16 similar operations based on a non-linear function F , modular addition, and left rotation.

5. Steganography

Steganography can be defined as the art of hiding data and communicating hidden data through apparently reliable carriers in attempt to hide the existence of the data itself. So, there is no knowledge of the existence of the message in the first place. Steganography techniques often use a cover, like an image or another file, to hide the secret information. If a person views the cover which the information is hidden within, there shall be no clue that there is any hidden data under the cover. In this way, the individual won't endeavor to decode the data. Figure 3 shows an overview of steganography system [4]. The secret information can be inserted into the cover media by the stego system encoder with using certain algorithm. A secret message can be plaintext, an image, cipher text, or anything which can be represented in the form of a bit string. After the secret data is embedded in the cover object, the cover object is called a stego object. The stego object is sent to a receiver by selecting the suitable channel, where a decoder system is used with the same stego method to extract the secret information [4].

There are various types of steganography. Here are some of the common types:

1. Text Files: The technique of embedding secret data inside a text is identified as text stego.

Text steganography needs a low memory because this type of file can only store text files. It affords fast transfer or communication of files from a sender to receiver [13].

2. Image Files: It is the procedure in which we embed the information inside the pixels of image. So that, the attackers cannot observe any change in the cover image. The least significant bit (LSB) approach is a common image steganography algorithm [13].

3. Audio Files: It is the process in which we hide the information inside an audio media. There are many approaches to hide secret information in audio files, like: Phase Coding and LSB [13].

4. Video Files: It is the process of hiding some secret data inside the frames of a video [13].

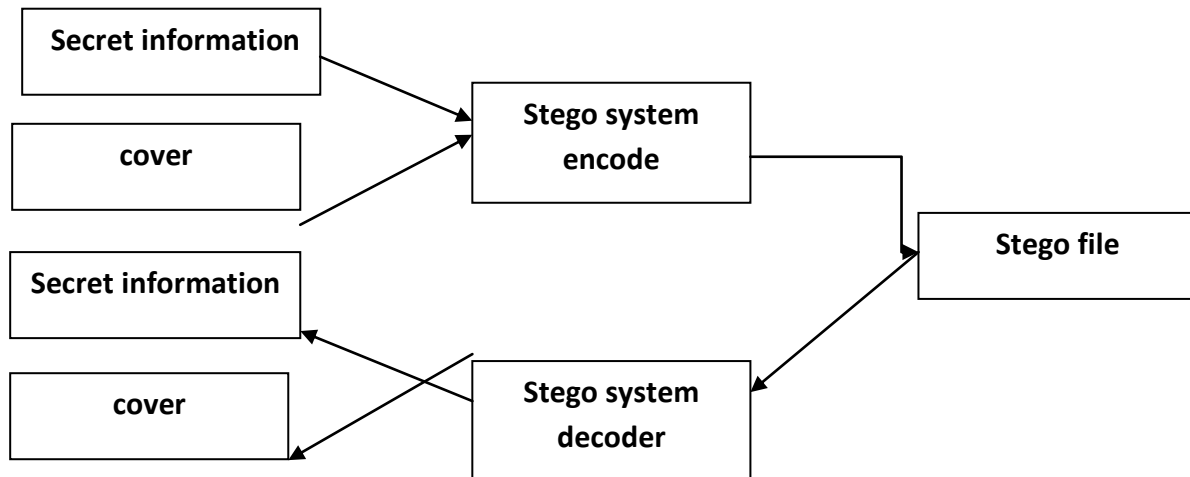


Fig. (3): Steganography System

6. Benefits of combine the Steganography and Cryptography

It is noted that steganography or cryptography alone is insufficient for the security of information in all scenarios. However, if we combine these systems, we can generate more reliable and strong systems [14]. The combination of these two strategies will improve the security of the secret information. This combination will fulfill some desired features, like: memory usage, security, and strength for sensitive information transmission across an open channel. Also, it will be a powerful mechanism which enables people to communicate without dragging the attention of eavesdroppers who does not even know of the existence of the secret information being transmitted [15].

7. Proposed Method of Encryption and Hide cipher text

In section will be explaining proposed method of encryption and the proposed XOR method to hide a cipher text:

7.1 Proposed Method of Encryption:

The works with New- begin when a user encrypts plaintext. First, creates a generation key by MD5. Second. Key generated by MD5 be as keys to 3DES, third, plaintext encrypted using 3DES depending on key generated by MD5 Forth, Hide cipher text image and six Decryption of the cipher text by 3DES Algorithm the result is plain text. As shown in figure (4)

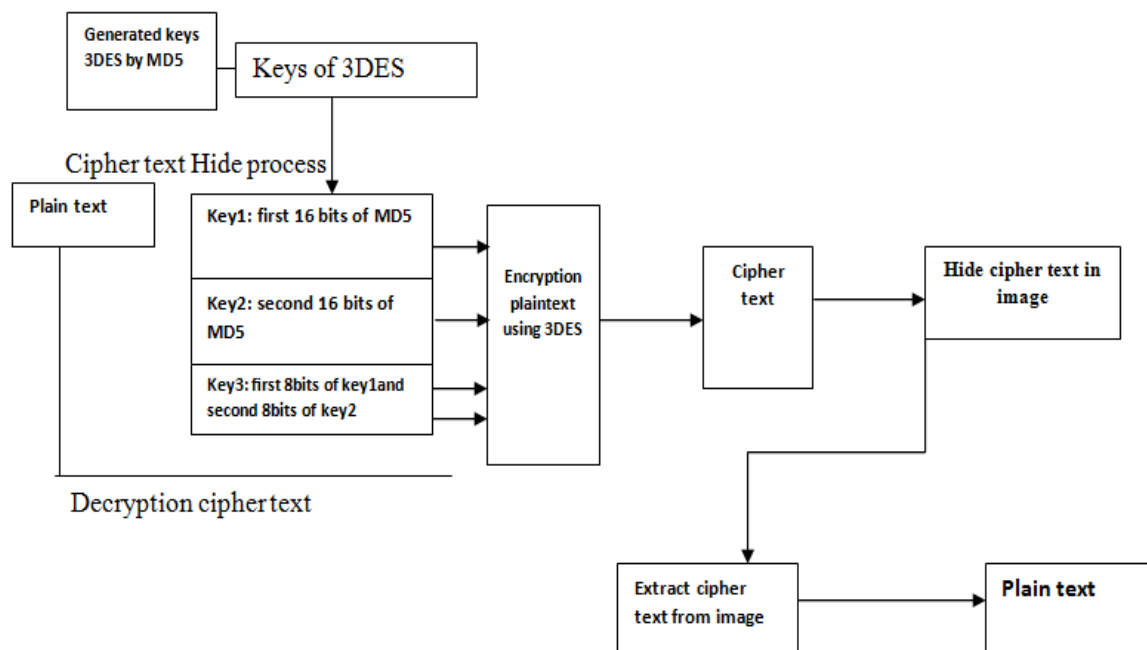


Fig (4): Structure of Proposed Method.

7.2 The Proposed XOR Method to Hide a Text:

The XOR operator is extremely common as a component in more complex ciphers. By itself, using a constant repeating key, a simple XOR cipher can trivially be broken using frequency analysis. If the content of any message can be guessed or otherwise known then the key can be revealed. In steganography the hidden information is important, steganography is to hide a message in such a way that no one except the sender and intended recipient knows about the existence of the message. This approach is different from cryptography whose goal is to make information unreadable. The embedding process is achieved by converting cipher text “the result of encryption operation” to binary and then using password (as key of XOR method) and repeating the password along cipher text. XOR method test of cipher text and then decides 0 or 1 to be embedded. XOR is known as ‘Exclusive-OR’ and it is a bitwise operator from binary mathematics. The XOR operator is used to “flip” bits (zeroes and ones) in a piece of plaintext to create a cipher text. The XOR operators return (1) when the value of either the first bit or the second bit is (1). The XOR operators return (0) when either or both of the bits are (1).

The XOR operator is extremely common as a component in more complex ciphers. A simple repeating XOR cipher is therefore sometimes used to hide information. Eventual embedding starts by embedding the result from XOR operation into the image and beginning from location 100 of pixel by using Least Significant Bit (LSB). Least significant bit insertion is a common and simple approach to embed information in a cover image in sequence. The message stored in the LSB is pixel of the RGB value. The main difference of the proposed code is the fact that data is now one dimensional array of integer. One integer from this array is associated with each pixel. This integer is 32 bits wide, so it has the capacity to hold the 8-bit red, green and blue components of a pixel value. The remaining 8 bits are used for the alpha component, which represents pixel transparency, and this part of alpha is used to hide information inside the proposed system. The ordering of red, green, blue and alpha is shown in Figure (5).

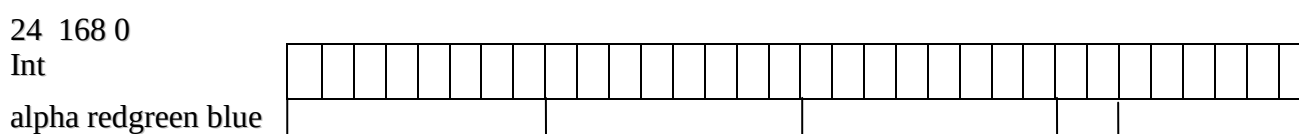


Fig (5): Red, Green, Blue and Alpha Values of Digital Image

The detailed algorithm for the proposed described in algorithm1.

Algorithm 1: Proposed method Algorithm

Input: Message (Plain text)
Output: Message (Cipher text hide in image)
Process:
Step1: start
Step2: Enter the text
Step3:Encryption the text by MD5
Step4:The result from MD5 is key of length 128 bit and takes three 64-bit keys (key1,key2,key3),which (key1 is first 16 bits from session key), (key2 is second 16 bits) and (key3 is first 8bits from key1and first 8bits from k2.
Step5: Enter the message.
Step6: Encryption the message by 3DES Algorithm the result cipher text.
Step7: Hide of the message encrypted in image for security
Step8:Excreta cipher text from image
Step9: Decryption of the cipher text by 3DES Algorithm the result is plain text.
Step10: End.

8. Experimental work of proposed method

Each step in algorithm (1) will be described in the following example:

Step1: Choose a short message to generated keys of 3DES From MD5 “Computer Science” the result is “0f3f29bf94e0d868215a5fc3561cffe6” is length 128bits. As shown in figure (6).



Fig. (6): Generation Key from MD5Algorithim

Step2: The result from md5 is key “0f3f29bf94e0d868215a5fc3561cffe6” because the length of key 128bits and used as keys to 3DES Algorithm.

Key1: 0f3f29bf94e0d868

Key2: 215a5fc3561cffe6

Key3: 0f3f29bf215a5fc3, as shown in figure (7).

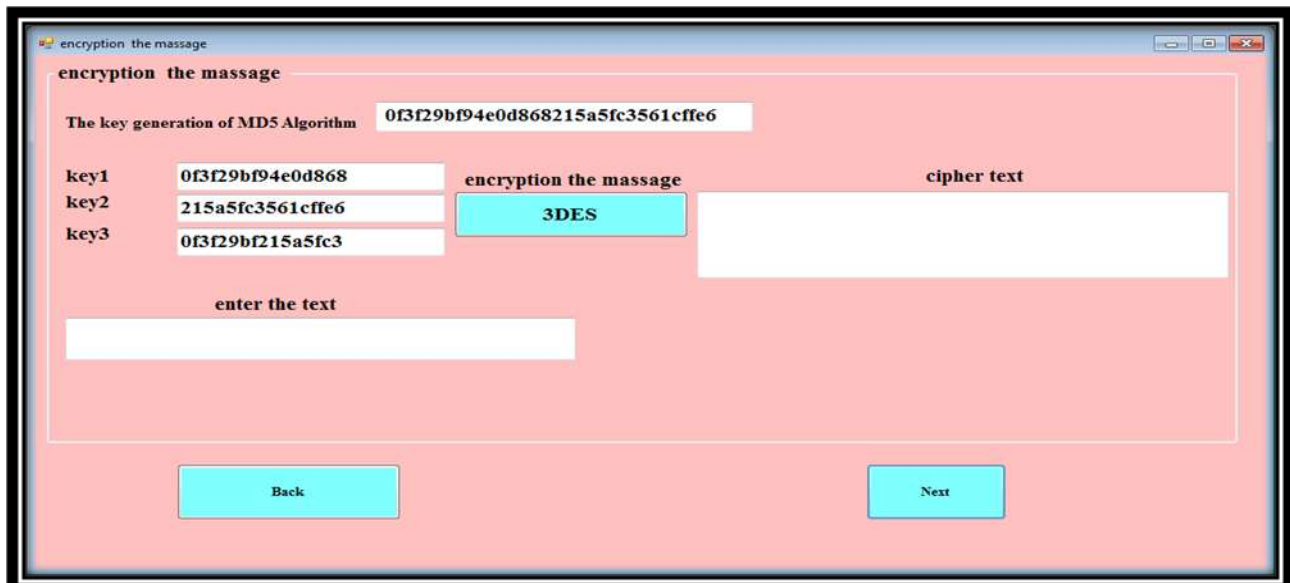


Fig. (7): Generation of keys 3DES

Step3: Choose a short message “The conference will be held in College of Education Tuesday 25.04.2017 at 10 am” as shown in figure (8).

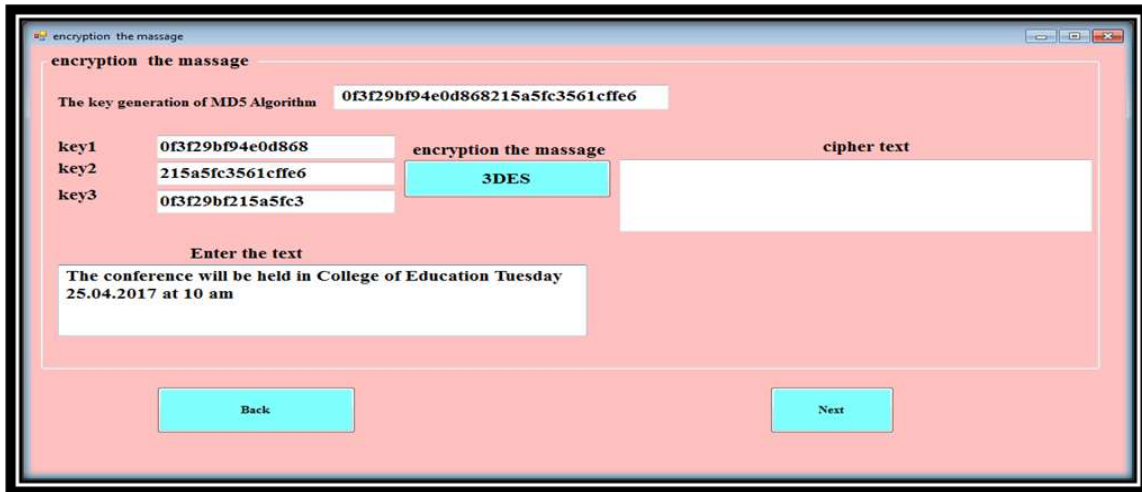


Fig. (8) Enter the message

Step4: encryption message “The conference will be held in College of Education Tuesday 25.04.2017 at 10 am” using 3DES the result encryption message “HLMYmKhdMVh/1+bkM8REEi3xVfu VDniEm14qVHJHshN2luzs M9ovCWUyeUVKchlH0QDt80iBaQ /ssgeg2kmiPe6CPoU+GA2aJQZ2gO2YBU=” As show in figure (9).

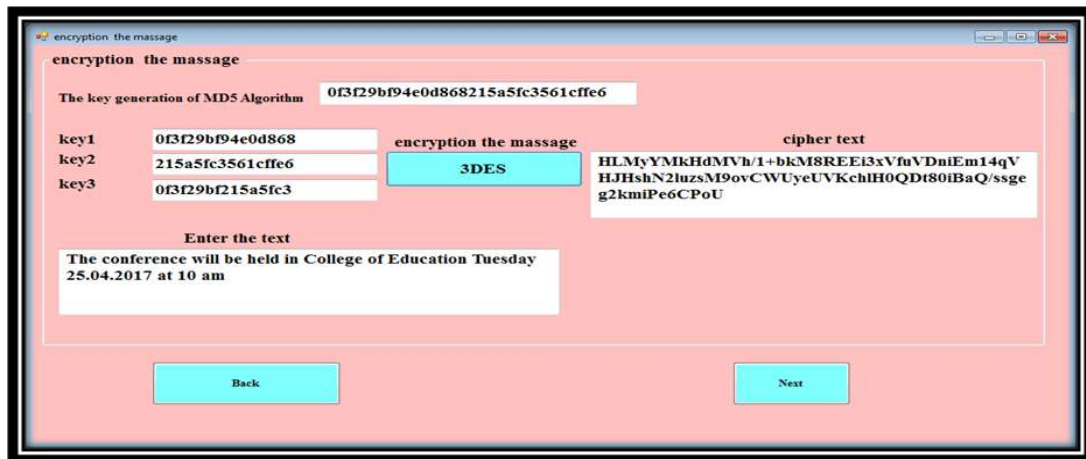


Fig. (9): Encryption of Message

Steps 5: Hide the cipher text in image for security as shown in figure (10)

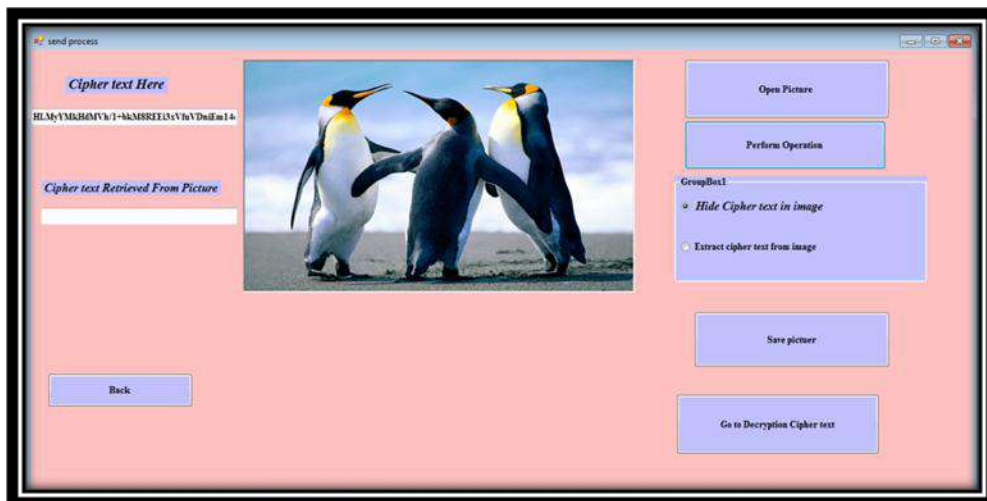


Fig. (10): Hide the cipher text in image

Step6: Load image from computer that include cipher text to as shown in figure (11).



Fig. (11): Load image

Step7: Extract the cipher text from image as shown in figure (12).

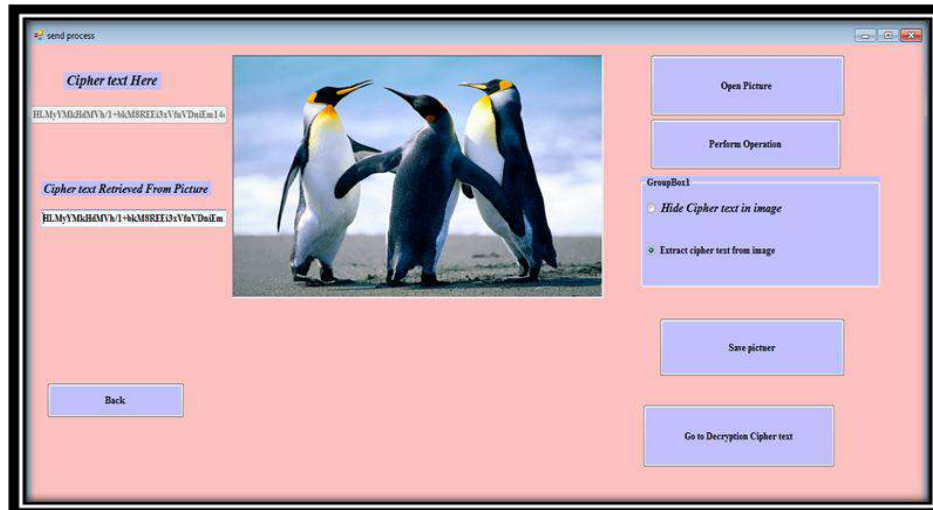


Fig. (12): Extract the cipher text from image

Step8: Enter the cipher text

“HLMYyMkHdMVh/1+bkM8REEdi3xVfuVDniEm14qVHJHshN2luzsM9ovCWUyeUVKchlH0QDt80iBaQ/ssgeg2kmiPe6CPoU+GA2aJQZ2gO2YBU=“as show in figure (13)

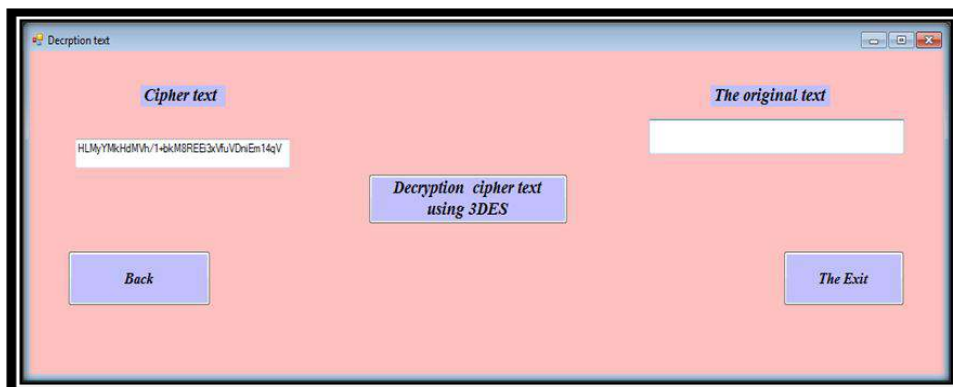


Fig. (13)

Step9: decryption the cipher text as result plain text Plain text = “Will be the International Conference at exactly 10 am” as show in figure (14).

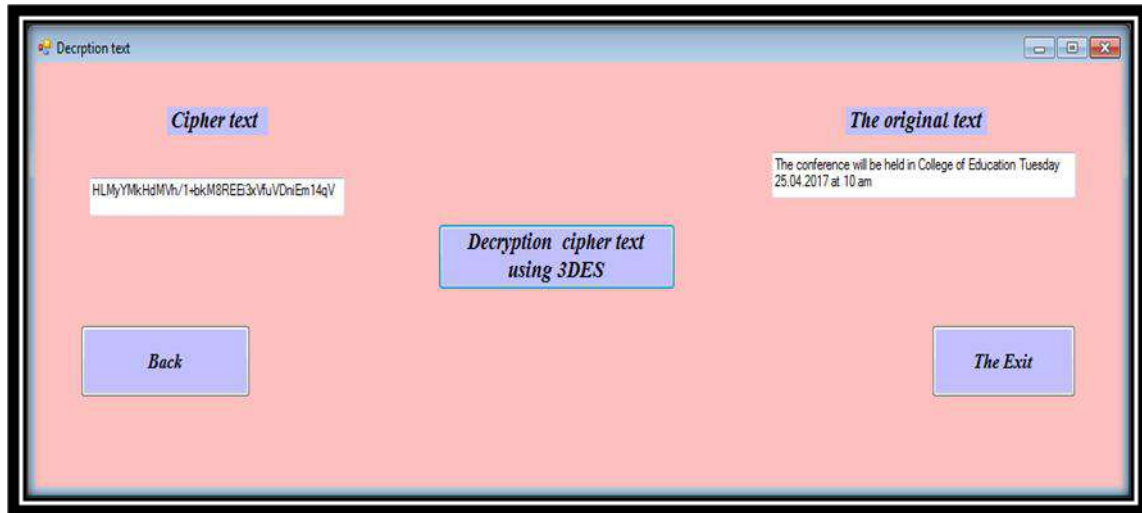


Fig. (14): Decryption of Message

Step10: End.

9. Experiment Test of the Proposed System

This section illustrates the results that obtained by executing the proposed system, and its testing results using PSNR and MSE. The tests were applied to color images with format (BMP) and size (256*256) to select the highest (PSNR) value with its minimum value of (MSE). For all the experiments presented the following tables compare the maximum PSNR and minimum MSE of 3DES algorithm of the proposed system. As shown in figures (15) & (16) the images before embedding text and after embedding a text.



Fig (15): The Images before Embedding a Text

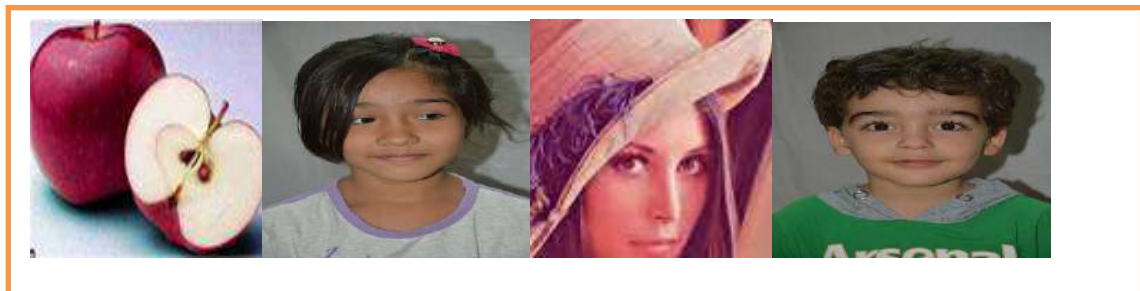


Fig (16): The Images after Embedding a Text

The result of test, after apply encryption on a text using 3DES algorithm and embedding the text in the image, found that the image cover boy, and Lena are the best using the image format (Bmp) as shown in table (1).

Table (1) Values of PSNR and MSE after Using Algorithm of BMP Images

Image Cover	PSNR Value	MSE Value
	3DES Algorithm	3DES Algorithm
APPlE	50.0445	2.1247
Boy	61.0112	0.1225
Lena	62.1734	0.1256
Girl	53.6625	3.1132

10. Conclusions

From the New-Proposed method, reached to the following conclusions, It is difficult to break the encrypted message in 3DES Algorithm because the algorithm uses keys which are obtained from MD5 Algorithm. This is very important. The longer the key size, the more difficult it is to break encrypted message, and enter this key to 3DES. The combination of cryptography and steganography provides an effective scheme to achieve high level of data security. It is very difficult for the unauthorized users to identify the changes in the stego image.

References

- [1] M. P. van Oorschot, and S. Vanstone, "**Handbook of Applied Cryptography**", CRC Press, 1996.
- [2] <http://www.garykessder.net/library/crypto.html> "overviewofcryptography", may1998-17 January 2007
- [3] J. Katz, Y. Lindell, "**Introduction to Modern Cryptography**", Chapman & Hall/CRC, 2008.
- [4] P. Kumar and V. K. Sharma, "**Information security based on steganography & cryptography techniques: A review**", International Journal, vol. 4, no. 10, 2014.
- [5] J. K. Saini and H. K. Verma, "**A hybrid approach for image security by combining encryption and steganography**", in Image Information Processing (ICIIP), 2013 IEEE Second International Conference on. IEEE, 2013, pp. 607-611.
- [6] H. Sharma, K. K. Sharma, and S. Chauhan, "**Steganography techniques using cryptography- a review paper**", 2014.
- [7] "**Data Encryption Standard (DES)**", NIST FIPS publication 46-3, 1999.
- [8] G. Ramesh R. Umarani, Dr. "**Performance Analysis of Most Common Encryption Algorithms on Different Web Browsers**", internet paper, I. J. Information Technology and Computer Science, 12, 60-66, 2012.
- [9] John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, "**Internet Security Cryptographic Principles, Algorithms and Protocols**", School of Electrical and Computer Engineering Seoul National University, Republic of Korea, Copyright -2003.
- [10] B. den Boer and A. Bosselaers, "**Collisions for the compression function of MD5**", Advances in Cryptology, Eurocrypt., 07, pages 293-304, Springer-Verlag, 2007.
- [11] S. Subasreeand N. K. Sakthivel." **Design a New of Security Protocol using Hybrid Cryptography Algorithms**", internet paper, IJRRAS 2010.
- [12] H. Dobbertin, "**The Status of MD 5 after a Recent Attack**", Crypto Bytes, 2(2): 1-6, 2007.
- [13] M. K. I. Rahmani and N. P. Kamiya Arora, "**A crypto-steganography: A survey**", International Journal of Advanced Computer Science and Application, vol. 5, pp.149 {154, 2014.
- [14] C. P. Shukla, R. S. Chadha, and A. Kumar, "**Enhance security in steganography with cryptography**", 2014.
- [15] H. Abdulzahra, R. Ahmad, and N. M. Noor, "**Combining cryptography and steganography for data hiding in images**", ACACOS, Applied Computational Science, pp. 978 {960, 2014.

Image Encryption Using 3D-CHEN's Map and 3D-Henon Map for Secure Transmission

Dr. Abdul-Wahab Sami Ibrahim

Majed Ismael Sameer

AL-Mustansiriya University/ College of Educational / Computer Science Department

alfaqaerme@gmail.com

majed_772003@yahoo.com

Abstract

Image Encryption is important for protecting image information. In this paper a proposed an algorithm the two functions as a function of the chaotic Henon map and the Chen 's map, each in three dimensions to encrypt color images each of which used an XOR operation between the output of the process between the Henon MAP and outputs with Chen 's MAP for output to be used in this output in the encryption and decryption process color of the image, the performance of the algorithm has been analyzed and results show that the algorithm has a very long key space, and high sensitivity for small changes in key which makes the algorithm Immune to Brute force attacks, and it can resist the differential and statistical attacks , in addition to having very high encryption and decryption speed , the receiver can detect any changes to the encrypted image during transmission. The algorithm has been implemented and analysis done by using Mat Lab R2008a software.

Keywords: Chaos, Image Encryption, Henon map, Chen's map, XOR operation.

المستخلص

من المعلومات المهمة لحماية الصور الملونة هي التشفير، وفي هذه الورقة اقترحنا خوارزمية لاثان من الدوال الفوضوية كدالة Henon map والـ Chen's map كل منهما بثلاثة ابعاد لتشفير الصور الملونة وكل منهما استخدمنا إجراء عملية الـ XOR operation بين مخرجات الـ Henon MAP مع مخرجات Chen's MAP للحصول على ناتج ليستخدم هذا الناتج في عملية التشفير وفك التشفير للصورة الملونة، وكانت أداء هذه الخوارزمية للنتائج والتحليلات بفضاء مفتاح طويل وبحساسية عالية جداً للتغيرات القليلة جداً للمفتاح ضد هجمات القوة الغاشمة، وهي ضد الهجمات الإحصائية والتفاضلية. إذ إن المستلم يستطيع الكشف عن أي تغير حصل في الصورة المشفرة أثناء النقل. فضلاً عن وجود سرعة عالية جداً في التشفير وفك التشفير، وقد تم التنفيذ والتحليل الخوارزمية باستخدام برنامج ماتلاب R2008a.

الكلمات المفتاحية: تشفير الصور Henon MAP، عملية Chen's MAP، XOR.

1. Introduction

Security of multimedia information is used to protect the multimedia content from unauthorized access.[1] Today images are not only the way to represent or to provide the clear view of some object. But the image information can be critical enough to provide the authentication to some secure system [2].

Chaotic maps are very complicated nonlinear dynamic systems, which are applied for encryption [12], because they are very sensitive to initial conditions and can generate good pseudorandom sequences.

Cryptography scheme is of two types. One is known as symmetric key cryptography [10] in which a single secret key is used for both, encryption at sender's end and decryption at receiver's end. the other scheme known as public key cryptography system is based on asymmetric key cryptography but this paper used symmetric key cryptography.

Recently, a number of chaos-based encryption schemes have been proposed. Some of them are based on three-dimensional chaotic henon maps and CHEN's Map For image encryption.

This paper is organized as follows. Section 2, presents an overview on Henon map and CHEN's Map chaotic system. In section 3 we will discuss the proposed algorithm (Henon map and CHEN's Map Chaotic). Section 4 will present experimental results and analysis. In section 5 we conclude the paper.

2. overview on 3D- Henon chaotic map 3D-CHEN's Map

In this section, an overview on 3D- Henon chaotic map and 3D-CHEN's Map system as important sequences as equations, which is used in this work. Henon chaotic map system is described by formula 1 and CHEN's map system is described by formula 2. [19, 12]

$$\begin{aligned} x(i+1) &= a - (y(i)^2) - b * (z(i)) \\ y(i+1) &= x(i) \end{aligned} \quad (1)$$

$$z(i+1) = y(i)$$

when initial values $1.54 < |a| < 2$, $0 < |b| < 1$, and $-0.9 \leq (x \text{ or } y \text{ or } z) \leq 1$ [18].

x(1)=1; y(1)=0; z(1)=0; %% Initial conditions The initial value are $x=1$, $y=0.1$, $z=0$,

N=5000; %% let N is the number of iterates example

a=1.6; b=0.2; %% Sets the parameters example

It has a chaotic attractor as shown in Fig.(1). It has been experienced that Henon chaotic system is relatively difficult due to the prominent three-dimensional and complex dynamic property [15]

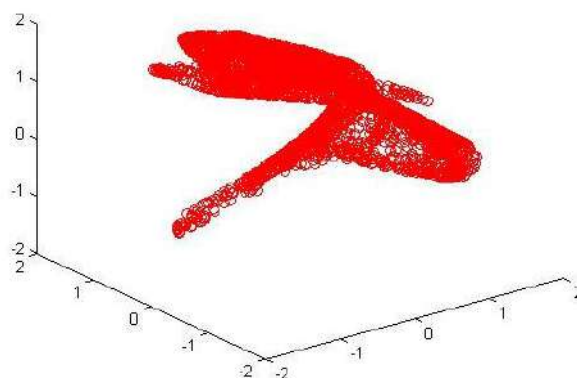


Fig.(1): Three dimension of henon map

Fig. (1) Shows 3D Henon mapping generates $x(n)$, $y(n)$ and $z(n)$, which is random sequence of Henon map. CHEN's map system is described by formula 2.

$$\begin{aligned} x(i+1) &= a * (y(i) - z(i)) \\ y(i+1) &= (c - a) * x(i) - x(i) * z(i) + c * y(i) \\ z(i+1) &= x(i) * y(i) - b * z(i) \end{aligned} \quad (2)$$

Where $a > 0$, $b > 0$ and c such that $(2c > a)$ are parameters of the system [12,3,20]. Chen's system is chaotic when the parameters have the values; $a = 35$, $b = 3$ and $c \in [20, 28.4]$.

When $a = 35$, $b = 3$, and $c = 28$; it has a chaotic attractor as shown in Fig.2. It has been experienced that Chen's chaotic system is relatively difficult due to the prominent three-dimensional and complex dynamic property [14]. Recently, the study about Chen's chaotic map system has attracted many researchers' attention.

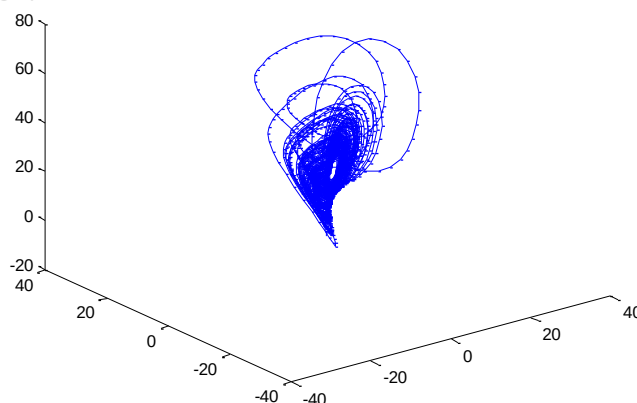


Fig. (2): Chaotic behavior of Chen's system

The following program generates a graphic shown in the figure(2)

```
ax=35;
```

```
b=3;
```

```
c=28;
```

```
f = @(t,a) [ax*(a(2)-a(1));(c-ax)*a(1)-a(1)*a(3)+c*a(2); a(1)*a(2)-b*a(3)];
```

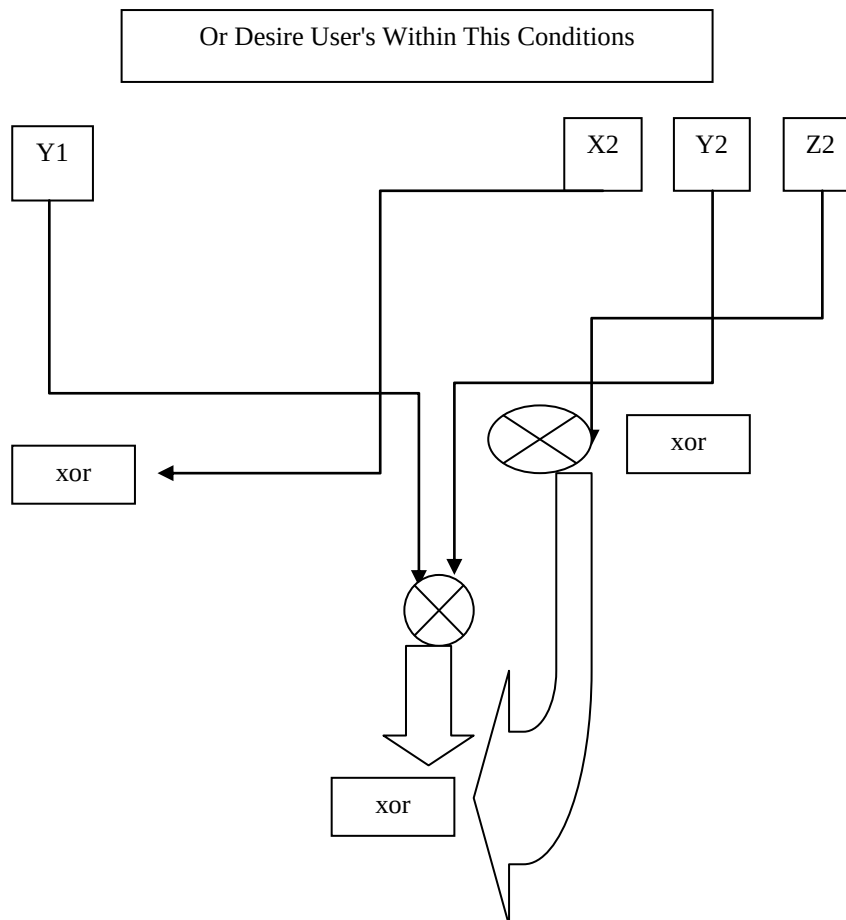
%'f' is the set of differential equations and 'a' is an array containing values of x, y, and z variables.

%'t' is the time variable

[t, a] = ode45 (f, [0 40],[0 1 -1.8]);%'ode45' uses adaptive Runge-Kutta method of 4th and 5th order to solve differential equations

plot3(a(:,1),a(:,2),a(:,3)) %'plot3' is the command to make 3D plot

3. Proposed algorithm (Henon map and CHEN's Map Chaotic) for image encryption



Steps of algorithm:

Step 1: here used chaotic (henon and CHEN's Map) three dimension then select proper initial values and system parameters to create chaotic variable sets.

(x > -0.9) or x < 1.0)

(y> -0.9) or (y < 1.0)

(z > -0.9) or (z < 1.0)

else

'Input out of range!' print,'Error'

Step 2: Prepare the chaotic sequences for range iteration number.

N=number of iteration

for Henon map

a = 1.4 initial value condition

b = 0.3 initial value condition

and CHEN's Map[13]

where $a > 0$, $b > 0$ and c such that $(2c > a)$ are parameters of the system [11,12]. Chen's system is chaotic when the parameters have the values; $a = 35$, $b = 3$ and $c \in [20, 28.4]$.

step 3: Extracting a single value from step 2 for both chaotic (henon and CHEN's Map) single value for x_1 and single value for y_1 and z_1 for henon map and single value for x_2 and single value for y_2 and z_2 for CHEN's Map then convert the variables of fraction number $(x_1, y_1, z_1, x_2, y_2, z_2)$ to bits binary as according to the user's desire by number of bits requirement.

step4: A process operation XOR between chaotic henon and CHEN's Map

between $X=x_1$ with x_2 , $Y=y_1$ with y_2 and $Z=z_1$ with z_2

obtain to results X, Y and Z

Then an operation XOR to all three of them X, Y , and Z in order to obtain to results single value

step 5:

send result from step4 inlet to function generation key have been obtain keys variable for steps part program below:

```
nn=p*q ....p=image width q=image height
```

```
key = keyGen(bb,nn);
```

```
function [key] = keyGen(bb,nn)
```

```
n = nn*8;
```

```
bi = zeros(n,1,'uint8');
```

```
NN= 0;
```

```
for m = 1: n
```

```
    NN = 1 - 2* bb* bb; %based on  $1-2*bb^2$ 
```

```
    if (NN > 0.0)
```

```
        bi(m) = 1;
```

```
    end
```

```
    bb = NN;
```

```
end
```

```
%Intended to produce a binary bits the size of the
```

```
%image *8.....>>>bi
```

```
key = zeros(n/8,1,'uint8'); %Reset keys
```

```
for k = 1: n/8
```

```
    for j = 1: 8 % here reason to use 8
```

```
        key(k) = key(k) + bi(j*k)* 2 ^ (j-1); %based on levels color  $2^8$ 
```

```
    end
```

```
end
```

```
here generated keys by size nn=p*q .....p=image width q=image height
```

step 6: stage encryption when we got the keys to the image size from step 5

for $p*q$ then we will encryption image and So based on Operation XOR for keys

(cipher image = plain image xor keys) each component of the three color components red, green and blue Based on these relations Confusion

step 7: stage decryption take the relation (decryption image=image encryption xor keys) same as keys.

4. Experimental Results and Analysis

In this paper, a practical programs of a proposed algorithm and a practical programs of all experimental and security analysis tests are designed by using MATLAB language release R2008a for 64bit Windows 7 Ultimate SP1 operating system. The computer used to perform these tests is a Dell Laptop with Intel @Core™ @ 1.8GHz 1.8GHz and 6 GB installed memory.

Here, we have taken the standard Lena image (256 X 256) as the original image for the projected scheme The initial values and key parameters for Chen's map [20] have taken ; $a = 35$, $b = 3$ and $c \in [20, 28.4]$.

And the Henon map and the system parameters a and b are also used as secret keys, where values initial $1.54 < |a| < 2$, $0 < |b| < 1$, and $-0.9 \leq (x \text{ or } y \text{ or } z) \leq 1$ [18]. For our experiment we have chosen the

iteration value as 6000. Figure (4a). Shows the result of proposed scheme. The result shows that there is no connection between the origin image and the cipher image [4].

4.1 Statistical Analysis

Original and encrypted image relationship can be determined by analyzing data statistically. In this manner, image after encryption must be totally differentiated from the original. Because of Shannon hypothesis. It is conceivable to illuminate numerous sorts of images by statistical investigation. For an image there are a few approaches to figure out if the ciphered image releases any data about the first one or not [8].

4.1.1 Histogram Analysis

Histogram analysis of three channels (red, green, and blue) of the plain and encrypted images is given. Figure (4a) shows the histograms of the 256×256 plain and encrypted. It is observed that the histograms of the encrypted image are significantly different from that of the plain image (lena.png) Figure (4b).

From these results, it is clear that although some plaintext images are of much tilted histograms, the cipher text image histograms become after encryption. In other words, the cipher text images are random-like [9].

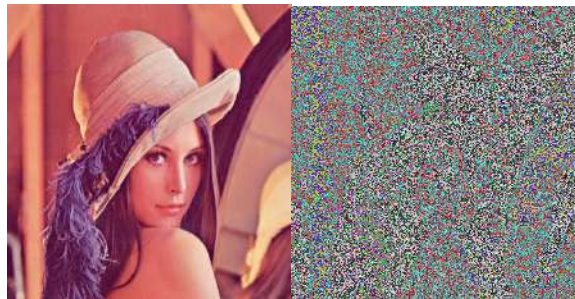


Fig.(4a): Plain image (lena.png) and encrypted image

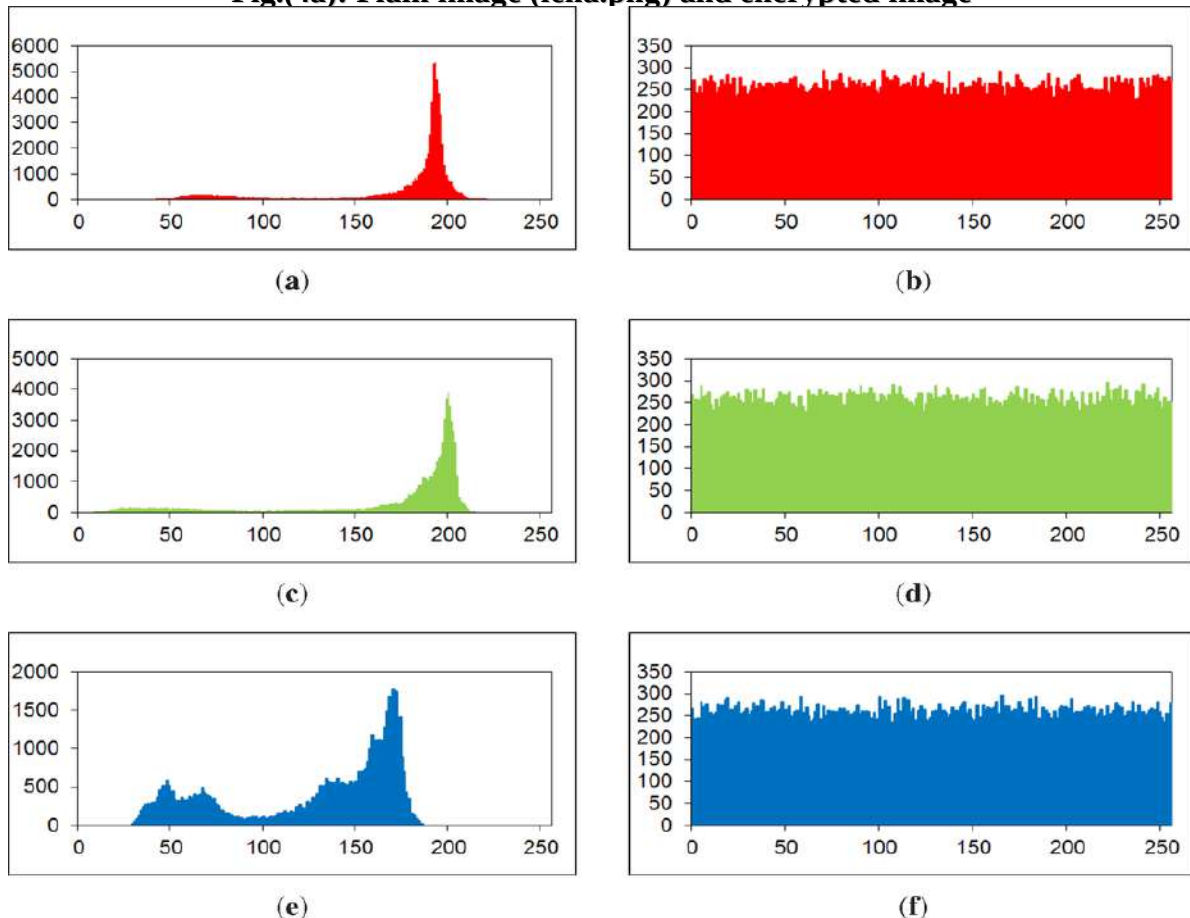


Fig. (4b): The histograms of the 256×256 plain and encrypted.

A. Key Space Analysis

Key space is the total number of different keys that can be used in the cryptographic system. A cryptographic system should be sensitive to all secret keys [7, 6]. There are total eight initial conditions of chaotic Chen's map used in the algorithm and the initial conditions for x_0 , y_0 , z_0 , a , b , c , m and n can be used as secret keys of encryption and decryption. Where m =number of bits, n =number of iteration. In our case, the precision is 10^{-14} , the key space size is $(10^{14})^8$ i.e. 10^{112} , which is extensively large enough to resist the exhaustive attack.

also, for chaotic Henon map but There are total seven initial conditions of chaotic Henon map used in the algorithm and the initial conditions for x_0 , y_0 , z_0 , a , b , m and n can be used as secret keys of encryption and decryption. Where m =number of bits, n =number of iteration.

In our case, the precision is 10^{-14} , the key space size is $(10^{14})^7$ i.e. 10^{98} , then total the key space size is $(10^{14})^{(7+8)}$ i.e. 10^{210}

B. Key Sensitivity Analysis

A good cryptosystem should be sensitive to a small change in secret keys i.e. a small change in secret keys in decoding process results into a completely different decoded image. Our proposed encryption algorithm is sensitive to a tiny change in the secret keys. If we change a little (10^{-14}) any of the initial conditions then the decrypted image is totally different from the plain-image. As an example, consider the original Lena

image, shown in Figure 5, it is encrypted using the proposed algorithm using the initial conditions given earlier for $x_0, y_0, z_0, a, b, c, m, n$ to CHEN's Map and Henon Map $x_0, y_0, z_0, a, b, m, n$ for the encrypted image is shown in figure 6. The decrypted image shown in Figure 7 is decrypted using the correct secret keys, the image obtained after decryption is shown in figure 6. It is noted that the decrypted image and its histogram are exactly same as that of the plain-image and its histogram, respectively. Hence, we can say that the proposed algorithm can successfully encrypt and decrypt the digital images without any loss of inherent information of the images.

Now, if we change one of the initial conditions, say x_0 OR Y_0 OR Z_0 oretc. a little key (10^{-14}) then the decrypted images obtained are shown in figure 8(a)-(c). As we can see that the images shown in figure 8(a-c) are totally different from the plain-image shown in figure 5.

Hence, we can say that the proposed encryption scheme is highly sensitive to a small change in secret keys.



Fig. (5): the original image (Lena.png)

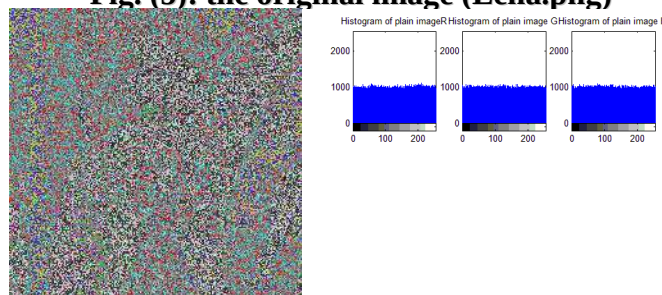


Fig. (6): the encrypted image (Lena.png)

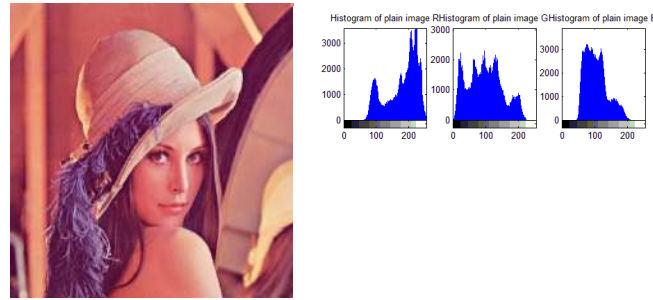


Fig.(7): decrypted image from figure(6)

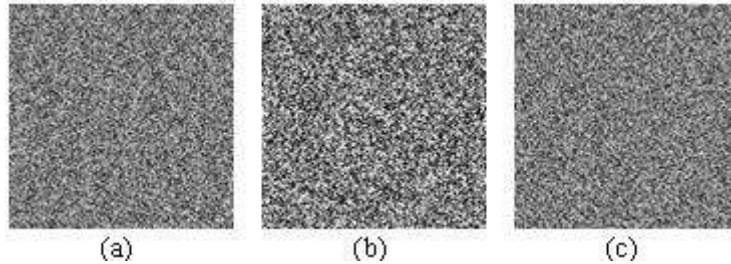


Fig. (8): Key sensitivity analysis (a) decrypted image with $x_0=0.100500000000001$; (b) decrypted image with $y_0= 0.300000000000001$; (c) decrypted image with $a = 1.220000000000001$

C. Information Entropy Analysis

The entropy H of a symbol source S can be calculated by following equation in formula 3.[16,9]. It is defined as follows [17]:

$$H(S) = -\sum_{i=1}^{255} p(S_i) \log_2 p(S_i) \dots \dots \dots (3)$$

where S is a discrete random variable, $p(S)$ is the probability density function of the occurrence of the symbol S , and the entropy is expressed in bits. If the source S emits 2^8 symbols with equal probability, i.e.

$S = \{S_1, S_2, \dots, S_{256}\}$, then the result of entropy is $H(S) = 8$, which corresponds to a true random source and represents the ideal value of entropy for message source S . Information entropy of an encrypted image can show the distribution of gray value. [7] According to the results shown in Table (1), the proposed system achieved a high permutation and substitution, and it is strong enough against the Entropy Attack because the information entropy value for the encrypted images are very close to the idealism value mentioned above. [20]

Table (1)The Information Entropy for the Plain and Encrypted Image

Plain Image	File Name	Entropy Test Average Value for 3 Bands of Plain Image	Entropy Test Average Value for 3 Bands of Encrypted Image
	4.2.03.tiff	7.6444	7.9993
	4.2.04.tiff	7.2719	7.9993

D. Correlation coefficient Analysis

The extensive study of the correlation between image and its corresponding encrypted image by using the proposed encryption algorithm. The correlation between two vertically adjacent pixels, two horizontally adjacent pixels, and two diagonally adjacent pixels [5], as expressed by Figure 9 and Table (2). Which implies the correlation coefficient of the adjacent pixels in original ("lena.png") image is very high, and the correlation coefficient in the encrypted image processed is very low, which is close to 0. From the above experiment, it can be seen that the presented image encryption algorithm have a good performance. [11]

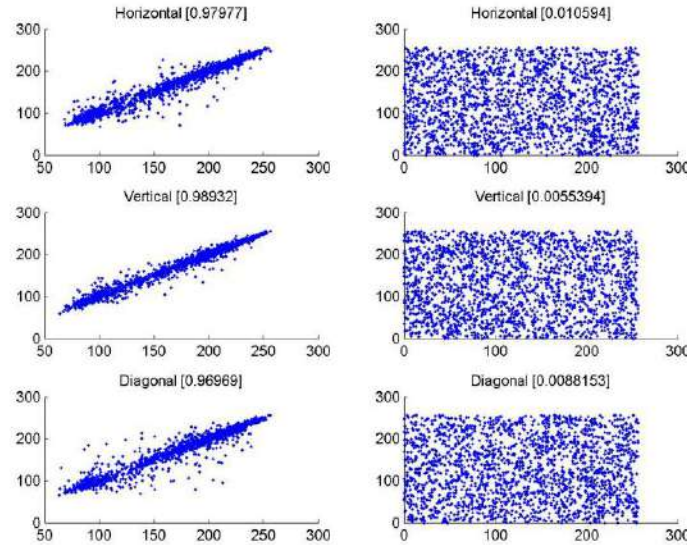


Fig.(9): Correlations of two diagonal, horizontally and vertical adjacent pixels in the plain image and in the cipher-image

Table (2) Correlation coefficient of two adjacent pixels in plain image and encrypted image for 'lena.png' 256*256*3 size image

State	Plane image	Encrypted image
Horizontal	0.9798	0.0106
Vertical	0.9893	0.0055
Diagonal	0.9697	0.0088

5. Conclusions

In this paper, we presented a new algorithm of encryption and decryption of images. The algorithm is based on the concept of Extraction triple keys of each chaotic map (Henon map and CHEN's map) using the initial condition of the user's desire. Then Process, including XOR of them, and again XOR between three results and It is this resulting value leads to the encryption and decryption process images very successful so that and by work of procedure the statistical analyzes and differential, And measuring and analyzing the efficiency of encryption key length and its sensitivity to change and measure the speed of implementation of the algorithm. The results showed robustness against the attacks statistical, the sensitivity is sufficient to change the secret keys for resist generally brute force...

6. Future suggestions

Possible development of research to be the work of more than two chaotic functions as use of three functions to be chaotic or four instead of two, and for the purpose of increasing the strength of the key to resist brute force attack.

References

- [1] A. Anto Steffi¹, Dipesh Sharma, " **Modified Algorithm of Encryption and Decryption of Images using Chaotic Mapping**", International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064
- [2] Perna Dureja¹, Bhawna Kochhar, " **Image Encryption Using Arnold's Cat Map and Logistic Map for Secure Transmission**", Perna Dureja et al, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.6, June- 2015, pg. 194-199
- [3] Guanrong Chen a, Yaobin Mao b, Charles K. Chui c, d, " **A symmetric image encryption scheme based on 3D chaotic cat maps**", Chaos, Solitons and Fractals 21 (2004) 749–761
- [4] R. Sujarani, 2D. Manivannan, " **A Secure Image Cryptosystem Using 2d Arnold Cat Map And Logistic Map**", International Journal of Pharmacy & Technology, 25-09-2016

- [5] Omar A. Saraereh¹, Qais Alsafasfeh² & Aodeh Arfoa², " **Improving a New Logistic Map as a New Chaotic Algorithm for Image Encryption**", Modern Applied Science; Published by Canadian Center of Science and Education Vol. 7, No. 12; 2013 ISSN 1913-1844 E-ISSN 1913-1852
- [6] Jean De Dieu Nkapkop¹, Joseph Yves Effa¹, Jean Sire Armand Eyebe Fouda², Mohamadou Alidou³, 4, Laurent Bitjoka⁵ and Monica Borda⁶, " **A Fast Image Encryption Algorithm Based on Chaotic Maps and the Linear Diophantine Equation**", Comput. Sci. Appl. Volume 1, Number 4, 2014, pp. 232-243 Received: July 30, 2014; Published: October 25, 2014
- [7] Musheer Ahmad, M. Shamsheer Alam, " **A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping**", Musheer Ahmad et al /International Journal on Computer Science and Engineering, Vol.2(1), 2009, 46-50
- [8] Amber Shaukat Nasim, " **Chaos Based Cryptography And Image Encryption**", M.Sc., University of Applied Sciences, Luebeck, Germany, 2012
- [9] Yue Wua, Gelan Yangb_, Huixia Jinb and Joseph P. Noonana, " **Image Encryption using the Two-dimensional Logistic Chaotic Map**", Journal of Electronic Imaging · January 2012
- [10] N. S. RAGHAVA & ASHISH KUMAR, " **Image Encryption Using Henon Chaotic Map With Byte Sequence**", International Journal of Computer Science Engineering and Information Technology Research (IJCEITR) ISSN (P): 2249-6831; ISSN(E): 2249-7943 Vol. 3, Issue 5, Dec 2013, 11-18
- [11] Sudhir Keshari, 2Dr. S. G. Modani, " **Image Encryption Algorithm based on Chaotic Map Lattice and Arnold cat map for Secure Transmission**", IJCST Vol. 2, Iss ue 1, March 2011
- [12] Mohamed A.AL-Refaiy, Moussa Demba, Osama M, Abu Zaid, " **Confusion Algorithm based on 3-D Chaotic Map System for Securing the Colored Images**", International Journal of Computer Applications (0975 – 8887) Volume 72– No.10, June 2013
- [13] Huibin Lu, Xia Xiao., " **A Novel Color Image Encryption Algorithm Based on Chaotic Maps**". Advances in information Sciences and Service Sciences (AISS), Vol. 3, No. 11, 2011
- [14] Cahit Cokal, Ercan Solak, " **Cryptanalysis of a chaos-based image encryption algorithm**". Elsevier Physics Letters A, Vol. 373, pp. 1357–1360, 2009.
- [15] S. V. Gonchenko, I. I. Ovsyannikov, C. Sim´O, D. Turaev, " **Three-Dimensional H´Enon-Like Maps And Wild Lorenz-Like Attractors**", International Journal of Bifurcation and Chaos, Vol. 15, No. 11 (2005) 3493–3508
- [16] X. Tao, X. F. Liao, G. P. Tang, " **A novel block cryptosystem based on iterating a chaotic map**", Physics Letter A, vol. 349, no. 1-4, pp. 109-115, 2006.
- [17] A. Anto Steffi, Dipesh Sharma, " **Modified Algorithm of Encryption and Decryption of Images using Chaotic Mapping**", International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064, Volume 2 Issue 2, February 2013
- [18] Alia Karim Abdul Hassan, " **Proposed Hyperchaotic System for Image Encryption**", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 1, 2016
- [19] Pianhui Wu a, Weihua Zhao, Zhengxu Zhao, " **Hyperchaotic Based-on Henon Map**", Journal of Information & Computational Science 11:12 (2014) 4055{4063 August 10, 2014.
- [20] Sadiq A. Mehdi, Rabiha Saleem Kareem, " **Using Fourth-Order Runge-Kutta Method to Solve Lü Chaotic System**", American Journal of Engineering Research (AJER), e-ISSN: 2320-0847 p-ISSN: 2320-0936 Volume-6, Issue-1, pp-72-77, 2017.

A New Approach of Color Image Encryption Based on RC4 algorithm and Chaotic Map

Dr. Abdul-Wahab Sami Ibrahim Majed Ismael Sameer
Mustansiriyah University/ College of Educational / Computer Science Department
alfaqeerme@gmail.com majed_772003@yahoo.com

Abstract:

Image Encryption is important for protecting image information, In this paper A chaos based on RC4 algorithm has been proposed to encrypt color Images, It is chaotic Henon function have created three keys, depending on the initial conditions to generate numbers dynamic function of the chaotic conditions in addition to the user's desire three dimensions of which mechanically operated from within the initial condition, and then working process distortion of the bits of the three keys Using the RC4 algorithm and results new in the process of XOR them to generate a unique key of binary bits one and zero and then turn it into a digital fracture and after the intervention to Phase image to encrypted so they generate the keys again, and the size of the desired image In order to encrypt it.

the performance of the algorithm has been analyzed and results show that the algorithm has a very long key space, and high sensitivity for small changes in key which makes the algorithm Immune to Brute force attacks, and it can resist the differential and statistical attacks, in addition to having very high encryption and decryption speed, the receiver can detect any changes to the encrypted image during transmission. The algorithm has been implemented and analysis done by using Matlab R2008a software.

Keywords: Chaos theory, Image Encryption, henon map, symmetrical encryption.

المستخلص

تعتبر تشفير الصور من المعلومات المهمة، في هذا البحث تم اقتراح دالة فوضوية ثلاثة إبعاد Henon تعتمد على جزء من خوارزمية RC4 لغرض تشفير الصورة الملونة. ومن الدالة الفوضوية أوجدنا ثلاثة مفاتيح بالاعتماد على الشروط الابتدائية لتوليد أرقام الديناميكية للدالة الفوضوية بالإضافة إلى شروط رغبة المستخدم للإبعاد الثلاثة والتي تعمل ألياً من ضمن شروط الابتدائية، ومن ثم تعمل بعملية تشويه للبتات للمفاتيح الثلاثة عن طريق خوارزمية RC4 والنتائج الجديدة تقوم بعملية XOR بينهم لتوليد مفتاح فريد من البتات الثنائية واحد وصفر ومن ثم نحوله إلى الكسر الرقمي وبعدها تدخل إلى مرحلة الصورة لتشفيرها وذلك بتوليدها إلى مفاتيح مرة أخرى ولحجم الصورة المطلوبة لأجل تشفيرها.

تم تحليل أداء الخوارزمية بإجراء التحليلات التفاضلية والتحليلات الإحصائية وقياس كفاءة التشفير، وتحليل طول المفتاح وحساسيته وإيجاد سرعة أداء الخوارزمية، أثبتت النتائج امتلاك الخوارزمية المقترحة للصفات المطلوبة لصد الهجمات الإحصائية والتفاضلية وهجمات القوة الوحشية مع إمكانية الاسترجاع التام للصورة عند المستلم وتقديم آلية عند المستلم لمعرفة إذا ما تعرضت الصورة المشفرة للتغيير أثناء نقلها بالإضافة لسرعة التشفير والاسترجاع، استخدم برنامج Matlab 2008a لتنفيذ الخوارزمية وإجراء التحليلات.

الكلمات المفتاحية: التشفير المتناظر، الدالة henon، نظرية الفوضى RC4.

1. Introduction

Multimedia communications; such as, images, audio and video has become significantly more important, since communications of digital products over the network (wired/ wireless) has expanded [1]. There is therefore, any information shared over Internet needs high level of protection from intruders [2].

The cryptography was used only for the military purposes and diplomatic circles, Cryptography itself divides into two broad categories which are: Asymmetric key algorithms and Symmetric key algorithms [3,4].this paper is used as symmetric key cryptography [5] in which a single secret key is used for both, encryption at sender's end and decryption at receiver's end.

Chaotic maps are very complicated nonlinear dynamic systems, which are applied for encryption [6], because they are very sensitive to initial conditions and can generate good pseudorandom sequences.

Chaotic systems have many important properties, such as the sensitive dependence on initial conditions and system parameters, pseudorandom property, non-periodicity and topological transitivity, [7].

Recently, a number of chaos-based encryption schemes have been proposed. Some of them are based on three-dimensional chaotic Henon maps for image encryption.

This paper is organized as follows. Section 2, presents an overview on Henon chaotic map system. In section 3 we will discuss the proposed algorithm (RC4 with Chaotic map). Section 4 will present experimental results and analysis. In section 5 we conclude the paper.

2. An over View On Henon Chaotic Map system

In this section, an overview on Henon chaotic map system as important one of the 3-D chaotic map systems, which is used in this work.

Henon chaotic map system is described by formula 1 which illustrates a set of the three function of Henon chaotic map system. [8,1]

$$x(i+1)=a-(y(i)^2)-b*(z(i))$$

$$y(i+1)=x(i) \quad \text{.....(1)}$$

$$z(i+1)=y(i)$$

When initial values $1.54 < |a| < 2$, $0 < |b| < 1$, and $-0.9 \leq (x \text{ or } y \text{ or } z) \leq 1$

x(1)=1; y(1)=0; z(1)=0; %% Initial conditions The initial value are **x=1, y=0.1, z=0,**

N=5000; %% let N is the number of iterates example

a=1.6; b=0.2; %% Sets the parameters example

It has a chaotic attractor as shown in Fig.1. It has been experienced that Henon chaotic system is relatively difficult due to the prominent three-dimensional and complex dynamic property [9].

Fig. (1) shows 3D Henon mapping generates $x(n)$, $y(n)$ and $z(n)$, which is random sequence Henon map.

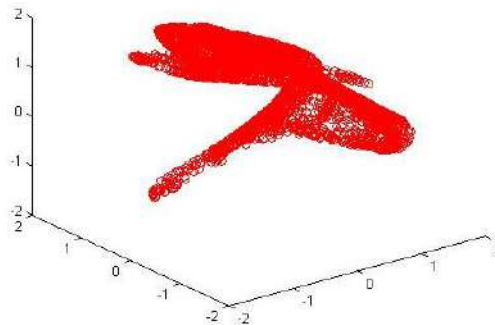


Fig. (1): Three dimension Henon map

3. A proposed chaotic map and RC4 Algorithm

This paper is dedicated for the designing and implementation of the proposed digital image encryption system. Generally, the proposed system encrypts a colored squared digital image using the advantage of chaotic properties to make the encryption more secure and robust against the most known attacks represents the block general diagram for the proposed system in figure (2).

Algorithm Scheme

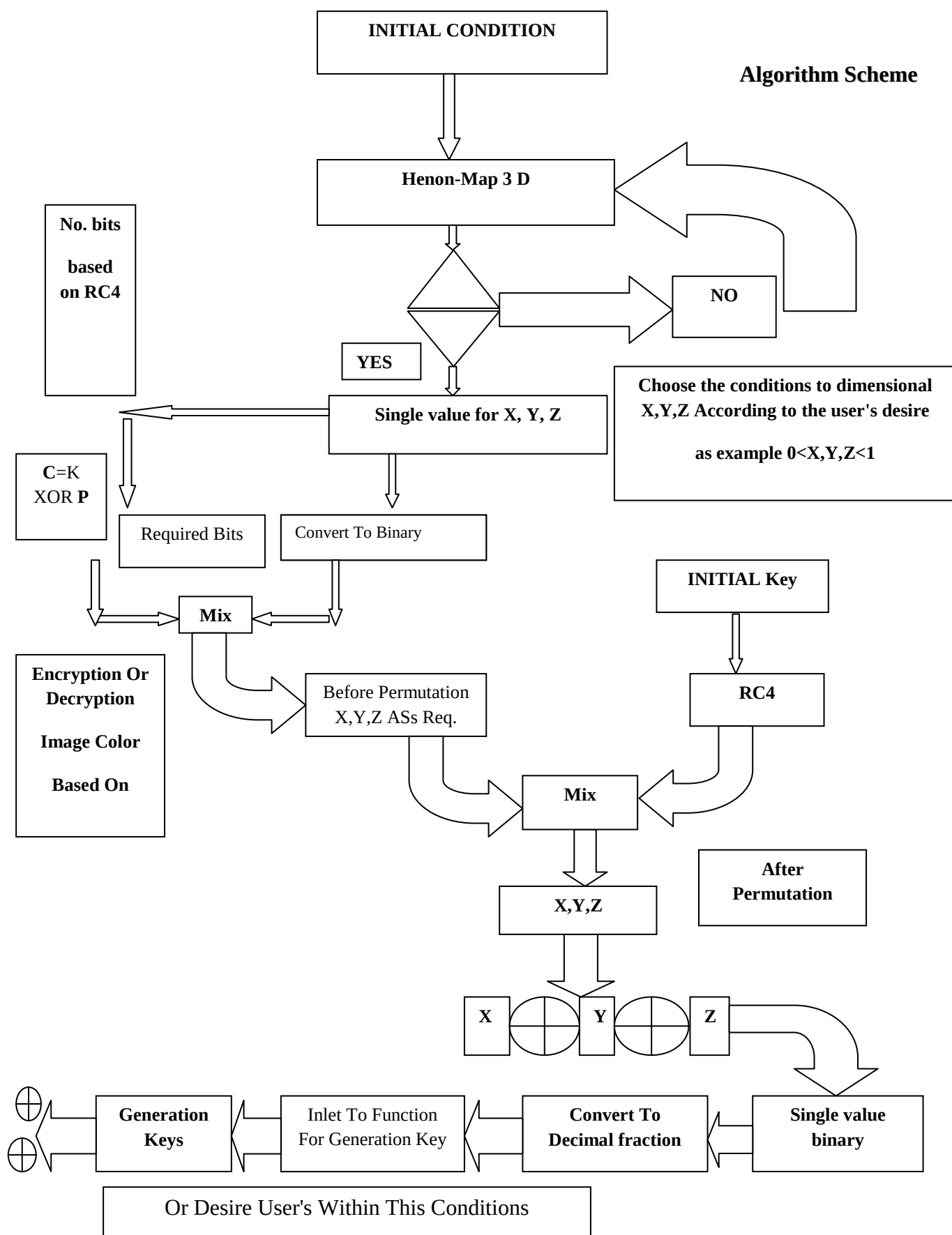


Fig. (2): Block diagram of the proposed chaotic and RC4

The steps for the chaotic and RC4 can be outlined as follows:

Step 1: here used chaotic Henon map three dimension then Select proper initial values and system parameters to create chaotic variable sets.

$$(x > -0.9) \text{ or } (x < 1.0)$$

$(y > -0.9) \text{ or } (y < 1.0)$

 $(z > -0.9) \text{ or } (z < 1.0)$

else

```
'Input out of range!' print,'Error'
```

Step 2: Prepare the chaotic sequences for range iteration number.

N=number of iteration

a = 1.4 initial value parameter

b = 0.3 initial value parameter

Step 3: Extracting a single value from step 2

single value for x and single value for y and z

Through the use of condition in step 1 for desire of user condition

Step 4: convert results of step 3 to binary

by using function convert decimal fraction to binary

Step5: Determine the number of bits specified by the RC4

To create the integer numbers values BY number of bits required BEFORE the PERMUTATION process for X, Y and Z

Step6: Process RC4 Private with permutation is:

X	Y	Z
0	0	0
0	1	1
1	1	0
1	0	1

Part of RC4 algorithm used

```
function [s]=RC41(m) [10]
```

```
s=[1:m+1];
```

[illegible]

j=0;

```
for i=1:m-1
```

```
a=j+s(i+1)+T(i+1);
```

```
j=mod(a,m+1);
```

```
x=s(i+1);
```

```
s(i+1)=s(j+1);
```

```

s(j+1)=x;

```

end

end

where Initial Permutation = S and T= Initial state

step7: link step4 with step 6 for X,Y and Z

for example 4 bit to step6 is

X=k(yy))	Y=v(yy)	Z=t(yy)
2	1	2
3	4	1
1	2	4
4	3	3

Where $yy=1$ to 4 but step 4 binary for X, Y and Z

X	Y	Z
1	0	1
0	1	0
0	0	1
1	1	0

Then have been obtain

Step 8: operation XOR between X, Y and Z We obtain with binary bits is XYZ(i) where i number of bits.

step 9: convert result for step 8 to decimal fraction By

format long

bb=0;

for i=1:m

bb=bb+XYZ(i)*2⁽⁻ⁱ⁾;

end

bb

step 10: send result from step9 to function generation key

where bb=result from step 9

nn=p*qp=image width q=image height

key = keyGen(bb,nn);

function [key] = keyGen(bb,nn)

n = nn*8;

bi = zeros(n,1,'uint8');

NN= 0;

for m = 1: n

NN = 1 - 2* bb* bb; %based on 1-2*bb²

if (NN > 0.0)

bi(m) = 1;

end

bb = NN;

end

%Intended to produce a binary bits the size of the

%image *8.....>>>bi

key = zeros(n/8,1,'uint8'); %Reset keys

for k = 1: n/8

for j = 1: 8 % here reason to use 8

key(k) = key(k) + bi(j*k)* 2^(j-1); %based on levels color 2⁸

end

end

here generated keys by size nn=p*qp=image width q=image height

step 11: stage encryption

When we got the keys to the image size from step 10 for p*q then we will encryption image and so based on Operation **XOR** for keys from step 10 with each component of the three color components red,green and blue Based on these relations **Confusion**

step 12: stage decryption

Take the image encryption based on the same key for plain image with XOR **operation** to obtain plain image.

3. Experimental Results and Analysis

In this paper, a practical programs of a proposed algorithm and a practical programs of all experimental and security analysis tests are designed by using MATLAB language release R2008a for 64bit Windows 7 Home Premium operating system. The computer used to perform these tests is a Dell Laptop with Intel (R) Core™ i3-3217u CPU@ 1.8GHz and 6 GB installed memory.

4.1 Statistical Analysis

4.1.1 Histogram Analysis

Histogram analysis of three channels (red, green, and blue) of the plain and encrypted images is given. Figure (3) shows the histograms of the 512×512 plain and encrypted. It is observed that the histograms of the encrypted image are significantly different from that of the plain image (lena.png).

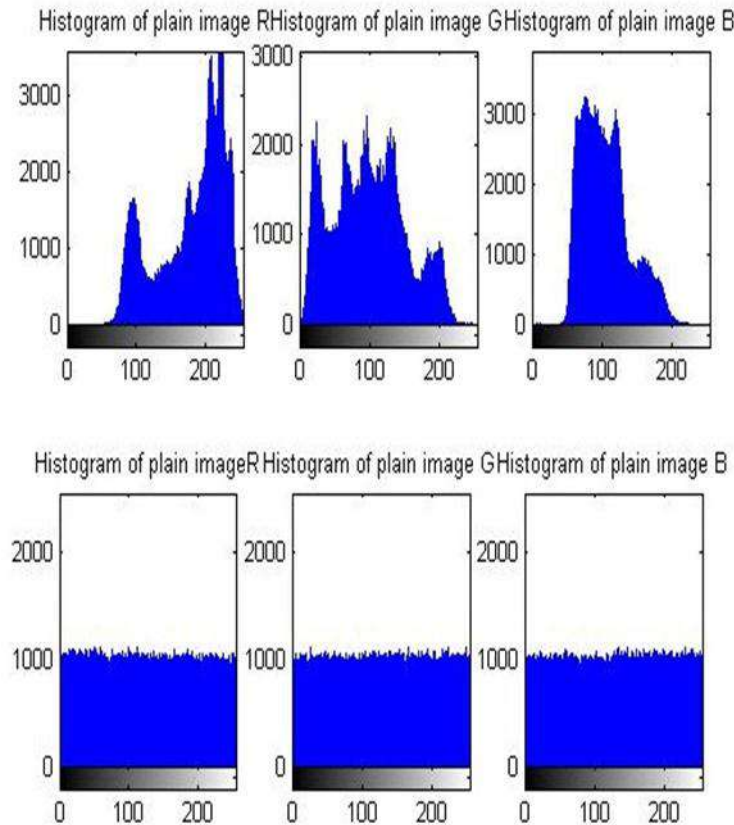
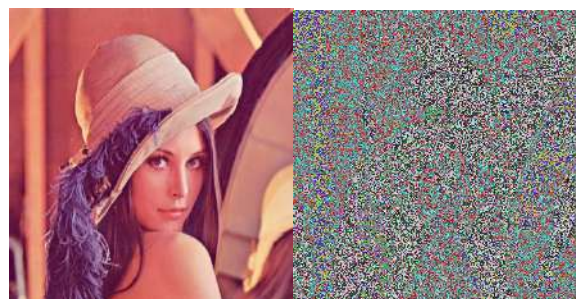


Fig. (3): shows the histograms of the 512×512 plain and encrypted.

4.1.2 Correlation coefficient Analysis

In this section the horizontal, vertical and diagonal correlation coefficient of the pixels studied. To do this we choose 2048 pairs of horizontal, vertical and diagonal adjacent pixels randomly. Figure (4) show the distribution of two **horizontally**, **vertically** and **diagonally** adjacent pixels in plain image and encrypted image [11]



Plain image encrypted image

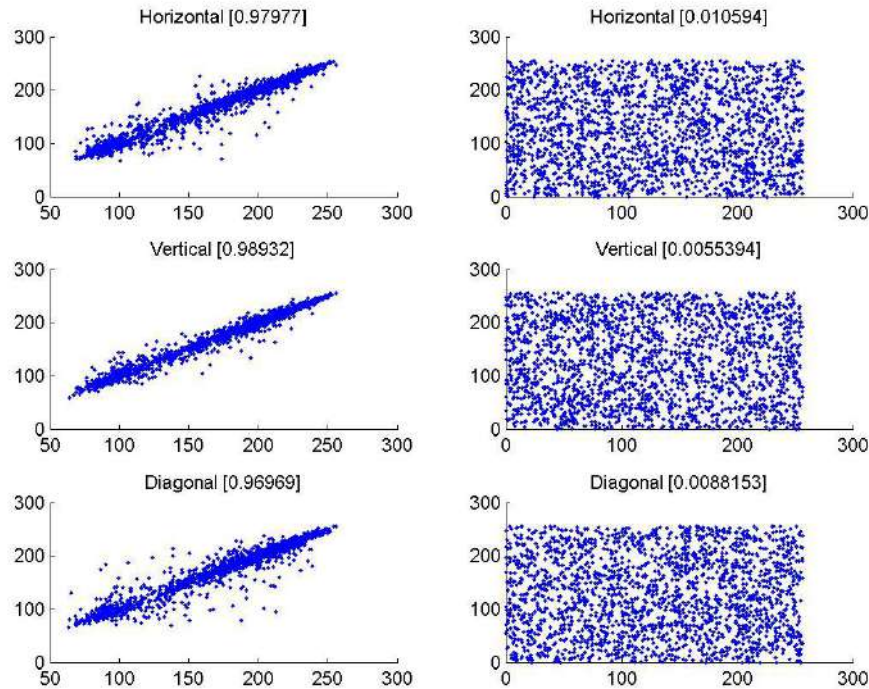


Fig. (4): Correlations of two diagonal, horizontally and vertical adjacent pixels in the plain image and in the cipher-image

The correlation coefficient of two adjacent pixels calculated using in[12,11] formula 2

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2$$

$$\text{cov}(x,y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)) \dots \dots \dots (2)$$

$$R_{xy} = \frac{\text{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

where x and y are the value of two adjacent pixels in the image and N is the total number of pixels selected from the image for the calculation[21], following results for found for various standard images in table (1).

Table (1) Correlation coefficient of two adjacent pixels in plain image and encrypted image for 'lena.png' 256*256*3 size image

State	Plane image	Encrypted image
Horizontal	0.9798	0.0106
Vertical	0.9893	0.0055
Diagonal	0.9697	0.0088

In Table (1) have been obtain the correlation coefficient for the plain and encrypted images shown in figure 4(a) , 4(b) and 4(c). It is clear from the Table (1) that there is negligible correlation between the two adjacent pixels in the encrypted image. However, the two adjacent pixels in the plain image are highly correlated. [11]

4.1.3 The Information Entropy Analysis

Entropy is a measure of uncertainty association with random variable. As for an image, the encryption decreases the mutual information among pixel values and thus increases the entropy value. A secure system should satisfy a condition on the information entropy that is the cipher

image should not provide any information about the original image. [13]. It is defined as follows in formula 3:

$$H(X) = -\sum_{i=0}^{255} p(X_i) \log_2 p(X_i) \dots (3)$$

Where X is a discrete random variable, p(x) is the probability density function of the occurrence of the symbol x. Its value for gray scale encrypted image should be very close to ideal value 8. Information entropy analysis is applied on the standard test images and their encrypted images. The results are listed in the Table (2). The values listed in the Table (2) are the average value for the three color bands for the plain images and the encrypted images.

According to the results shown in Table (2), the proposed system achieved a high permutation and substitution, and it is strong enough against the Entropy Attack because the information entropy value for the encrypted images are very close to the idealism value mentioned above.[14]

Table (2) The Information Entropy for the Plain and Encrypted Image

Plain Image	File Name	Entropy Test Average Value for 3 Bands of Plain Image	Entropy Test Average Value for 3 Bands of Encrypted Image
	4.2.03.tiff	7.6444	7.9993
	4.2.04.tiff	7.2719	7.9993

4.2 Security Differential Attack Analysis

One minor change in the plain image causes large changes in the cipher image then differential analysis may become useless thus, much difference between encrypted forms is expected in order to keep high security [15] it is a common measure used to check the effect of one pixel change on the entire image. this will indicate the percentage of different pixels between two images[16] Often the attacker slight change such as changing the value of a pixel one point in the image the encrypted using the algorithm and concludes the relationship between the two pictures encryption image before and after the change, this is called chosen plaintext attack (differential attack) attack to find a certain relationship between the encrypted image and the original image to infer the secret key according to this differential attacks do not be successful relationship, If a major change is the work the following differential.

Analysis to measure the efficiency of the algorithm against differential attacks [17, 18] so that used: NPCR and UACI.

NPCR measures the percentage of different pixels numbers between two cipher-images whose plain images only have one-pixel difference. UACI measures the average intensity of differences between two cipher images. to resist difference attacks, the values of NPCR and UACI should be large enough Value has changed one bit of image Baboon The calculated ratios before and after change And bring the same accounts after changing the value of a pixel one point or 8 bits, and the results obtained were within the specified percentages Ideal for encryption in [19].Table (3) show the results obtained.

Table (3) values of NPCR and UACI at change pixel I(250,250,2) FROM 147 TO 2

Compound color	NPCR	UACI
R	99.5841979980469	33.2961452708525
G	98.6638011	32.9332814
B	99.6021270751953	33.2787173402076
TOTAL	99.6093750000000	33.4635416666667

4.2.1 Key space analysis

The used key must not be long or short. Short key can be easily obtained when applying brute - force attack or analysis. security encryption system that is dependent on the key according to the laws Kirchhoff As long key reduces the speed of system performance This is undesirable because the encryption of important specifications for the design speed of the encryption system. Must not be less than the key space 2^{100} , to provide a high level of safety. In the proposed algorithm has been used chaotic Henon function maps were generated keys, and each requires a series initial value

and control value for chaotic map. Where they are used as keys for encryption, if the primary control variables and values accurately in 10^{14} , the total area of the key:

$10^{14} * 10^{14} * 10^{14} * 10^{14} * 10^{14} = 10^{70} = 2^{232}$ that length 232 bit very good for resistant brute attack.

In addition to the keys to the sensitivity of algorithm RC4 FOR X,Y,Z

for example in X DIMENSION

[illegible]

in RC4, and also

Y DIMENSION

[illegible]

and also

Z DIMENSION

```
T=[1 2 5 6 1 2 5 6 1 2 5 6 1 2 5 6 1 2 5 6 1 2 5 6 1 2 5 6 1 2 5  
6 1 2 5 6];
```

Any change in the value of values the keys will be sensitive to those changes decryption when change any value key in case of attack. then the total area of the keys

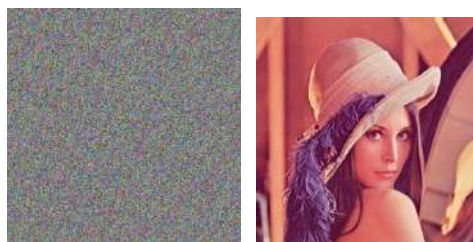
$$10^{14} \cdot 10^{14} \cdot 10^{14} \cdot 10^{14} \cdot 10^{14} \cdot 10^{14} \cdot 10^{14} = 10^{112} = 2^{372}$$

These keys are the very least it is possible to the increment depend on user's desire. As well as sensitivity to the number of iterations and the number of bits required for all anti-brute force attacks.

4.2.2 Key sensitivity analysis

In addition to being long enough to give the key safety system, the ideal encryption system must be very sensitive to any A slight change in the secret key, and any slight change in the used key must lead to the generation of an entirely different encrypted image before the change in the key image encrypted, and this ensures that the system resistant to brute force attack, done several experiments to test Over the system's sensitivity to a change in the key as follows[20]:

1. Initial value use as X as a key to generate a first series of numbers chaotic, It was obtained on image encryption fig (5.b) from plain image (5. a)
2. Use the same key with a few differences by $X + 10^{(-13)}$ as an experiment to decode the encrypted to image encryption, but we got another encrypted image to fig (5. c). This shows how the algorithm immunity against brute force attacks as the slight change in the key $1 * 10^{-14}$ to extract the original image failure.



Plain image encryption image by use key X
Fig (5. a) Fig(5. b)



Fig. (5.c) image extract after using the wrong key By Differentiate a little by.00000000000001 for the correct key the same processes as possible having to RC4 for X or Y or Z

4.3 Performance analysis

Encryption of the important requirements of the system performance of the system speed after a safety investigation, the table (4) Includes average time it takes Windows 7 environment within Matlab R2008a to encrypt and decrypt images standard listed in the table using a program 6GB RAM processor 1.8 Ghz and Intel core quickly on a personal calculator has the following specifications in table(4).

Table (4) The average time taken to implement encryption algorithm and decryption

Image and size 512*512*3	Time of encrypted	Time of decode the encrypted
Lenna.png	13	4
Baboon.png 512*512*3	12	4
Airplane.png 512*512*3	11	4

4. Conclusions

It has been proposed algorithm to encrypt the image of color, Using chaotic theory with part of the algorithm RC4. Henon function used of three dimensions of the function chaotic, The encryption and decryption process images very successful so that and by work of procedure the statistical analyzes and differential, And measuring and analyzing the efficiency of encryption key length and its sensitivity to change and measure the speed of implementation of the algorithm. The results showed robustness against the attacks statistical, the sensitivity is sufficient to change the secret keys for resist generally brute force. As well as the results proved to possess the speed of implementation of the algorithm high of close to real time. While providing a mechanism if it's been encrypted during transfer to a change in the values of image points, or manipulated by knowing NPCR and UACI

References

- [1] Alia Karim Abdul Hassan, "**Proposed Hyper chaotic System for Image Encryption**", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 1, 2016.
- [2] N. S. Raghava & Ashish Kumar, "**Image Encryption Using Henon Chaotic Map With Byte Sequence**", International Journal of Computer Science Engineering and Information Technology Research (IJCEITR) ISSN (P): 2249-6831; ISSN(E): 2249-7943 Vol. 3, Issue 5, Dec 2013, 11-18.
- [3] B. A. Forouzan, "**Cryptography and Network Security**", Mc Graw Hill, International Edition, 2008
- [4] B. Schneier and N. Fergusson, "**Practical Cryptography**", Wiley Publishing, Inc., First Edition, 2003.
- [5] W. Stallings, "**Cryptography and Network Security Principles and Practice**", Fifth Edition, Pearson Education, Prentice Hall publishing, 2011.
- [6] Osama M. Abu Zaid, Moussa Demba, Mohamed A. AL-Refaiy, "**Confusion Algorithm based on 3-D Chaotic Map System for Securing the Colored Images**", International Journal of Computer Applications (0975 – 8887) Volume 72– No.10, June 2013
- [7] Zhang LH, Liao XF, Wang XB, "**An image encryption approach based on chaotic maps**", Chaos, Solitons & Fractals, Vol. 24, pp. 759–765., 2005
- [8] Pianhui Wu, Weihua Zhao b, Zhengxu Zhao c, "**Hyper chaotic Based-on Henon Map**", Journal of Information & Computational Science 11:12 (2014)
- [9] S. V. Gonchenko Inst. Appl. Math. and Cyb., Nizhny Novgorod State Univ., 10 Ulyanova st., Nizhny Novgorod, 603005, Russia gosv100@uic.nnov.ru, "**Three-Dimensional H'Enon-Like Maps And Wild Lorenz-Like Attractors**", Received October 15, 2004; Revised February 15, 2005, International Journal of Bifurcation and Chaos, Vol. 15, No. 11 (2005) 3493–3508
- [10] Ricardo Goulart, "**Considerações sobre o algoritmo RC4.**", Universidad Federal do Rio Grande do Sul PGCC - Pós-graduação em Computação, 2000

- [11] Kamal Jadidy Aval, Morteza Sabery Kamarposhty, Masumeh Damrudi, "A Simple Method for Image Encryption Using Chaotic Logistic Map", Journal of Computer Science & Computational Mathematics, Volume 3, Issue 3, September 2013.
- [12] Mintu Philip, "An Enhanced Chaotic Image Encryption", International Journal of Computer Science, Engineering and Information Technology (IJCEIT), Vol.1, No.5, December 2011
- [13] Rakesh S, Ajitkumar A Kaller, Shadakshari B C and Annappa B, "Multilevel Image Encryption", Department of Computer Science and Engineering, National Institute of Technology Karnataka, Surathka, 2003
- [14] Mustafa A. Hussain AL-Nuaimi, "Color Image Encryption Based on Chaotic Maps", Submitted to the College of Science / Al-Mustansiriyah University, 1999
- [15] Narendra K Pareek, "Design And Analysis Of A Novel Digital Image Encryption Scheme", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012
- [16] Amber Shaukat Nasim, "Chaos Based Cryptography And Image Encryption", M.Sc., University of Applied Sciences, Luebeck, Germany, 2012
- [17] Fakhrulddin H. Ali, Maha Basher Hussein, "Colored Image Encryption Algorithm Using DNA Code and Chaos Theory", Second Engineering Conference, the Golden Jubilee of the College of Engineering - University of Mosul, 2013.
- [18] Dr. S. Ramahrishnan, B. Elakkiya R. Geetha, P. Vasuki, "Image Encryption Using Chaotic Maps in Hybrid Domain", International Journal of Communication and Computer Technologies Volume 02 – No.13 Issue: 05 June 2014 ISSN NUMBER: 2278-9723
- [19] Yue Wu, Joseph P. Noonan, Sos Agaian, "NPCR and UACI Randomness Tests for Image Encryption", Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), April Edition, 2011
- [20] Narendra K Pareek, "Design And Analysis Of A Novel Digital Image Encryption Scheme", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012.
- [21] Narendra K Pareek, Vinod Patidar, K. K. Sud, "Image encryption using chaotic logistic map", publication at: <https://www.researchgate.net/publication/215658784>, January 2006

Cloud Security Implementation by a Chaotic Key and XOR

Israa M. Abdalameer Al-Khafaji
Mustansiriyah university- College of Arts
Israam82@yahoo.com

Abstract:

Database security is important technology to protect sensitive data stored in database. One of security features is encryption, which transforms data to unreadable data; the encrypted data should decrypt in order to read them. This paper provides a proposed scheme for database encryption and decryption processes. The proposed scheme uses chaotic approach for increasing randomization of cryptography key. Cryptography key acts a backbone of proposed scheme security, which is characterized, with simplicity of design and implementation. The scheme is implemented in MATLAB with Microsoft SQL Server.

المستخلص

أمن قاعدة البيانات هو التكنولوجيا الهامة لحماية البيانات الحساسة المخزنة في قاعدة البيانات. ومن ميزات الأمان هو التشفير الذي يحول البيانات المقروءة إلى بيانات غير قابلة للقراءة، يجب أن يتم فك تشفير البيانات المشفرة من أجل قراءتها. ويقدم هذا البحث مخططاً مقترحاً لعمليات تشفير قواعد البيانات وفك التشفير. يستخدم المخطط المقترح نهج الفوضى لزيادة عشوائية مفتاح التشفير. مفتاح التشفير هو العمود الفقري لأمن المخطط المقترح الذي يتميز ببساطة التصميم والتنفيذ. يتم تنفيذ المخطط باستخدام برنامج مختبر المصفوفات (MATLAB) مع لغة الاستعلامات البنوية (SQL) Structured Query Language.

1. Introduction

A database may contain important data related to finance, sales, marketing or product manufacturing. A modern principle is available which provides structure of Database as a Service (DBaaS)[1]. DBaaS is a technique to introduce database accessible on demand over the Internet using cloud computation. The database is an essential technique in cloud technology, while in the past the latency and cost for transmitting large amount of data over gangly distance has inadequate considerably [2]. This scheme purveys managing of DBMS via data owner and response on query of the user straight. Compared to traditional architecture of client-server the DBaaS counters a significant problem is represented by security issue [3]. Measurement of database security has to assure user requirement, which includes integrity, confidentiality and availability. In cloud computation, one of major features of database security, which are data, has to be secured in transit, usage and access control to the data [4]. Database encryption is one of database security techniques; it uses to secure valuable data, because it provides data confidentiality. Database encryption is used to ensure data integrity, which means the ability to detect any modifications [1]. The encryption of cloud database can be partial relays on techniques of standard encryption, encrypting database fully relays on standard techniques of encryption or based on techniques of cloud providers [5].

2. Related works

Cloud computing data are not saved in PC but are saved in Cloud Media, which is hosted by anther parties. Many research works has suggested and accomplished on security of Clouding. Ravi Shankar Dhakar et. Al [1].

Chaos algorithm is a branch in mathematics applications in various disciplines such as Categories of Science. In ordinary usage, "chaos" means "A condition or place of great disorder or confusion". Chaos algorithm studies the manner of systems that take the place of deterministic laws but come into sight random and changeable or we can say a dynamical system that has a sensitive dependence on its initial conditions; small changes in those conditions can lead to quite different outcomes [10].

3. Methodology of Proposed Scheme

The proposed scheme introduces a method in order to enhance the security features. The scheme presents cryptography based on chaotic, which requires few storage spaces and executes the work rapidly. The chaotic approach has many features encourage system developers to adopt chaos in encryption process to accomplish better diffusion and confusion. The proposed scheme uses pool of password in order to enhance the security, which is automated, and it minimizes user intervention. The proposed scheme consists of following levels:

3-1 Encryption Level

As mentioned above the proposed scheme is automated in its work, so the password will be generated randomly. The security is enhanced via key strength of the algorithm. In order to strengthen the keys, they should depend on randomization. There are difficulties of making the keys absolute random, the stochastic approach is based on pseudo-random number algorithm. The proposed scheme uses random key which is generated by take the digits of date denoted as (x). The input of user also is taken with mixture of digits and characters which is denoted as (y). The keys generator uses following equation in generation process:

$$\text{Key}_{n+1} = x * \text{key}_n \oplus y \bmod r \dots\dots (1)$$

$$r = \text{Key}_{n-1} \vee \text{key}_n \dots\dots(2)$$

This equation generates series of keys; the proposed scheme uses pool in order to store these keys. The proposed scheme utilizes key selection depends on length of keys and contents of keys. In contrast with traditional (static) keys the operation of generating keys in proposed scheme, which is dynamic. The key changes dynamically when the user log in which is effective way. The acquisition of key in pool is made according to rules, which are executed in short time and accomplished steady situation. The essential component of acquisition process is set of rules which controls the selection, in addition to inference rules in order to made process more accurate. Acquisition process provides an algorithm, which transforms an expert knowledge into automatic strategy of controlling. The design of acquisition process requires defining the inputs and their membership. There should be a library of chosen keys, which is defined to the process. The number of inputs is determined according to application requirements. The acquisition controller uses trapezoidal function of input memberships because of its simplicity.

The output of acquisition process is related to input which is derived from knowledge rules set. The knowledge rules acts as backbone for decision-making behavior, these rules are described as following:

- 1- The password is invalid if it is short and its contents only numbers.
- 2- The password is invalid if it is short and its contents numbers and characters.
- 3- The password is invalid if it is short and its contents only characters.
- 4- The password is invalid if it is long and its contents only numbers.
- 5- The password is invalid if it is long and its contents only characters.
- 6- The password is valid if it is long and its contents numbers and characters.

Then key is generated which concerns to chaotic cryptography utilizing Vernam cipher. It is mixing random text via One Time Pad with plain text in order to generate number sequence of pseudo random depending on chosen password to be used in encryption of selective database records. The selected password modifies according to new and old one for each process.

The encryption process is done in proposed scheme via Torus Automorphisms with some modification to appropriate the proposed scheme. The following steps a pseudo code of encryption algorithm:

STEP1: $X = R(i)$: fetch the demanded records data.

STEP2: for each x of X to separate data elements to be represented as digits of number and characters unattached.

STEP3: save x in array 2d: diffuse data elements on two-dimensional table.

STEP4: select (D) table cells with length equals to key length.

STEP5: D XOR key: perform exclusive-or operation between the key and data of selected cells.

STEP6: go to 5: restore the result of STEP5 in the database.

3-2 Decryption Level

The decryption of encrypted data is depends on the key (password). It is simple to perform when the key is known, the same algorithm is used for both encryption and decryption algorithm. Therefore, it is important to save the key but not in the same server, which holds, encrypted data, because of disclosure possibility increases simultaneously. The proposed scheme keeps the key at encrypted field transmitter as chaotic signal of noise. For decryption process, the key must be extracted from chaotic signal. The proposed system mixes the synchronization and cryptography with chaotic approach depending on exclusive-or operation.

4. Results

The proposed scheme can be analyzed using many features in order to specify the scheme robustness such as scheme analysis, encryption and decryption efficiency. The algorithm is implemented via MATLAB using Microsoft SQL server with its inner database. The range of records, which is used in experiment from 100 to 1000 in database. The experiment is implemented in computer with processor Intel® Pentium® Dual CPU T2390 @1.86GHz, 1.87 GHz, RAM: 1 GB with operating system: Windows 7, 32-bit. Performance of proposed scheme evaluates via encryption and decryption speed. Time has taken to convert plaintext into cipher text is used to specify encryption speed, while the time which is elapsed to convert cipher text into plaintext is specify decryption speed. The encryption process performs at 95 seconds for data with 106K size. While decryption process requires 98 second to decrypt 106K size of data. The proposed scheme has accuracy is 100% ability of generating key for encryption and decryption processes which is applied to all desired records in database.

Table (1) shows reduce the time between encryption process and decryption process

Type of process	size	time
encryption process	106K	95 second
decryption process	106K	98 second

5. Conclusions

1. The following points represent conclusion of proposed scheme:
2. The cryptography process (encryption and decryption) is fast, so it desirable to be adopted in such field.
3. The encryption and decryption implemented in same algorithm which facilitates design and implementation processes.
4. The security of proposed scheme depends on the key, so it must be safe as possible.
5. Generating cryptographic key is done via chaotic approach in order to provide resistant key to attacks. This feature improves the security of proposed scheme.
6. Proposed scheme uses exclusive or operation in encryption and decryption processes which decreases CPU overhead and accelerate the implementation.
7. Key generation is automatic to decreases the human intervention and improve fast generation process.

References

- [1] E. Shmueli, R. Vaisenberg, Y. Elovici, and C. Glezer, "Database encryption – an overview of contemporary challenges and design considerations," Journal of the Sigmod Record, vol. 38, no. 3, 2009.
- [2] B. Rajkumar, B. James & Goscinski. "Cloud Computing Principles and Paradigms", John Wiley & Sons, Inc., Hoboken, New Jersey USA, 2011.
- [3] R. Ravan, N. Idris, and Z. Mehrabani, "A survey on querying encrypted data for database as a service", in Proc. International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Beijing, Oct. 2013.
- [4] NIST, "Guidelines on Security and Privacy in Public Cloud Computing", December 2011, <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>, 2012-05-05
- [5] I. Sakhi, "Database security in the cloud", Försvarsmakten, Handen, Sweden, 2012.

Enhanced Color Plane Permutation for Satellite Imagery Encryption

Fadhil Hanoon Abbood Rana Saad Mohammed Intisar Abid Yousif
Computer Science Department, Education Collage, Mustansiriyah University

Abstract

Digital multimedia nowadays needs a privacy and authentication services to protect a transmitted data through a communication system and web. This paper proposed a method for a satellite imagery encryption. This method has integration selective encryption with a compression system to permute a color plane.

The proposed method is tested and compared with traditional methods that used a chaotic. The results show that the proposed method has good properties such as more secure, low cost, support direct bit-rate control and more robust to transmission errors. These properties make the proposed system suitable for real time multimedia applications.

Keywords: Satellite Imagery encryption, Color plane permutation, Selective Encryption, DCT.

تحسين التشويش للسطح اللوني لتشفير صور الأقمار الصناعية
فاضل حنون عبود رنا سعد محمد أنتصار عبد يوسف

المستخلص

الوسائط المتعددة الرقمية في الوقت الحاضر تحتاج إلى خدمات الخصوصية والتوثيق لحماية البيانات المرسلة من خلال نظام الاتصالات وشبكة الإنترنت. في هذا البحث تم اقتراح طريقة لتشفير صور الأقمار الصناعية. هذه الطريقة لديها التشفير الانتقائي المتكامل مع نظام الضغط لتشويش السطح اللوني.

تم اختبار هذه الطريقة المقترحة ومقارنتها مع الأساليب التقليدية التي تستخدم الفوضى. وأظهرت النتائج أن الطريقة المقترحة لها خصائص جيدة مثل أكثر أماناً وتكلفة منخفضة ودعم التحكم المباشر في معدل البتات ومقاومة لأخطاء الإرسال. هذه الخصائص تجعل النظام المقترح مناسب لتطبيقات الوسائط المتعددة في الوقت الحقيقي.

الكلمات المفتاحية: تشفير صور الأقمار الصناعية، تشويش السطح اللوني، التشفير الانتقائي، DCT.

1. Introduction

The standards image coding permitted the wide-ranging spread that use for applications of multimedia. Nowadays, digital documents might make distribute over the World Wide Web to a many number of customers in a cost efficient way. So a real need for more security and services to keep the provision of digital multimedia by work as both profitable for the document owner and reliable for the customer. Privacy and Authentication services for multimedia data streaming are crucial in today data dissemination through Internet.

To protect data, various encryption schemes has been proposed for image encryption, however in these schemes (total encryption schemes) all data has to be encrypted which will generally take some time, complicated calculations and high memory occupation, which makes these schemes hard to use in real time applications. In [1-6] schemes try to design a satellite image encryption.

Total encryption schemes are not necessary when we talking about most multimedia content. Given to the fact that the content is already voluminous and not all the content represents a significant importance. This paper chooses to encrypt only significant parts of the data and leave the rest to enhance a time encryption and reduce memory occupation. And also make the encryption scheme suitable in practical application given to the fact that selective crypto-systems present a simple architecture.

So the proposed method is providing method of image encryption. This method is mainly based on encrypting DCT coefficients so as not cause any changes in compression ratio. Therefore, the proposed method combines encryption process with JPEG encoding that permutes DCT blocks.

2. DCT (Discrete Cosine Transform)

The standard JPEG calls for applying the DCT to data units (Blocks) of 8×8 pixels not to the entire image because of:

- When Applying DCT on all image pixels (n×n) lead to produces better compression with many arithmetic operations, therefore. Applying DCT to all data units can be reduces the overall compression ratio but is faster.
- Many experience displays that, in a continuous-tone image, correlations between pixels are short range. Every pixel in an image has a value (color or gray) that's close to those of its near neighbors, but has nothing to do with the values of far neighbors.

The DCT can be done by the following:

$$G_{ij} = \frac{1}{4} C_i C_j \sum_{x=0}^7 \sum_{y=0}^7 p_{xy} \cos\left(\frac{(2x+1)i\pi}{16}\right) \cos\left(\frac{(2y+1)j\pi}{16}\right) \dots\dots\dots (1)$$

$$\text{Where } C_f = \begin{cases} \frac{1}{\sqrt{2}}, & f = 0, \\ 1, & f > 0, \end{cases} \text{ and } 0 \leq i, j \leq 7 \dots\dots\dots (2)$$

Where C_f is C_i, C_j and p_{xy} are the values of image component

$i, j = 0, 1, \dots, 7, x, y = 0, 1, \dots, 7$.

The JPEG decoder works by computing the inverse DCT (IDCT), using the following equation:

$$p_{xy} = \frac{1}{4} \sum_{i=0}^7 \sum_{j=0}^7 C_i C_j G_{ij} \cos\left(\frac{(2x+1)i\pi}{16}\right) \cos\left(\frac{(2y+1)j\pi}{16}\right) \dots\dots\dots (3)$$

$$\text{Where } C_f = \begin{cases} \frac{1}{\sqrt{2}}, & f = 0, \\ 1, & f > 0, \end{cases} \dots\dots\dots (4)$$

3. Color plane permutation

Blocks position of DCT under the control has been confuse of the key. So, the method of confusion founded by Space Filling Curve (SFC) pseudo-random used in order to decrease the compression ratio changing. Since the DCT coefficients are encoded depending of the previous adjacent ones in JPEG, and SFC method can be keeping the correlation between blocks in some extent. Figure (1) shows a confusion method.

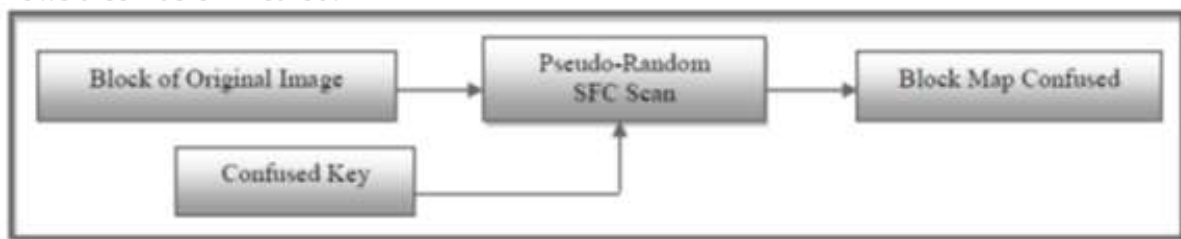


Fig. (1): Color Plane Confusion Method

3-1 Alternative Space Filling Curve Techniques

A space filling curve is a continuous map of a one-dimensional interval into a two-dimensional area (plane-filling) or a three-dimensional volume. There are different types of SFCs and each of them exhibits different locality preserving properties (also called clustering properties). Figure (2) shows several types of CFCs [7].

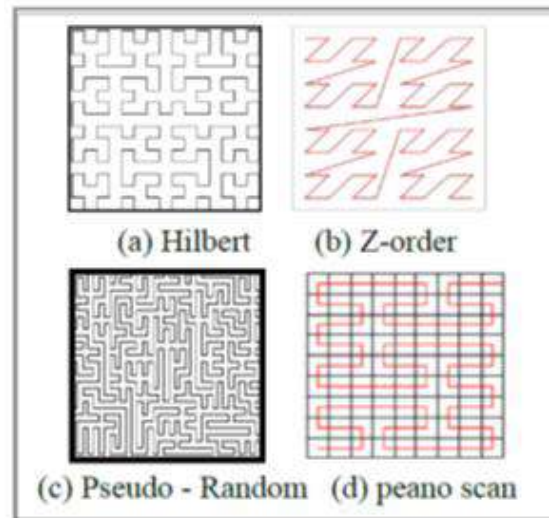


Fig. (2): Various Space-Filling Curves

1. The proposed approach of Improved Color plane permutation

Space Filling Curve (SFC) Algorithm

Input: Image matrix $I_{N \times N}$

Output: Confused matrix

1. Divide I to a set of blocks $b_i = [b_1, b_2, \dots, b_m]$.

2. Generate position array $POS[1 \dots m]$ with random sequence without repeated any number, where m is the number of blocks in image and the block size (8×8) pixels.

3. Set $i \leftarrow 1$

While ($i \leq m$)

a. Get a block number i from I

$b_i = I(\text{block } POS[i])$

b. Insert b_i into new matrix I'

$I'(\text{block } i) = b_i$

c. $i = i + 1$

The proposed method based on the idea of decomposing the image into 8×8 blocks, these blocks are transformed from the spatial domain to frequency domain by the DCT. Then, the DCT coefficients related to the higher frequencies of the image block are encrypted using the Color Plane Permutation. The general block diagram of the proposed method of selective image encryption is shown in Figure 3, which combines encryption process with DCT codec, and is composed of data encoding, parameter encryption and data decoding. The general proposed approach can be showing below.

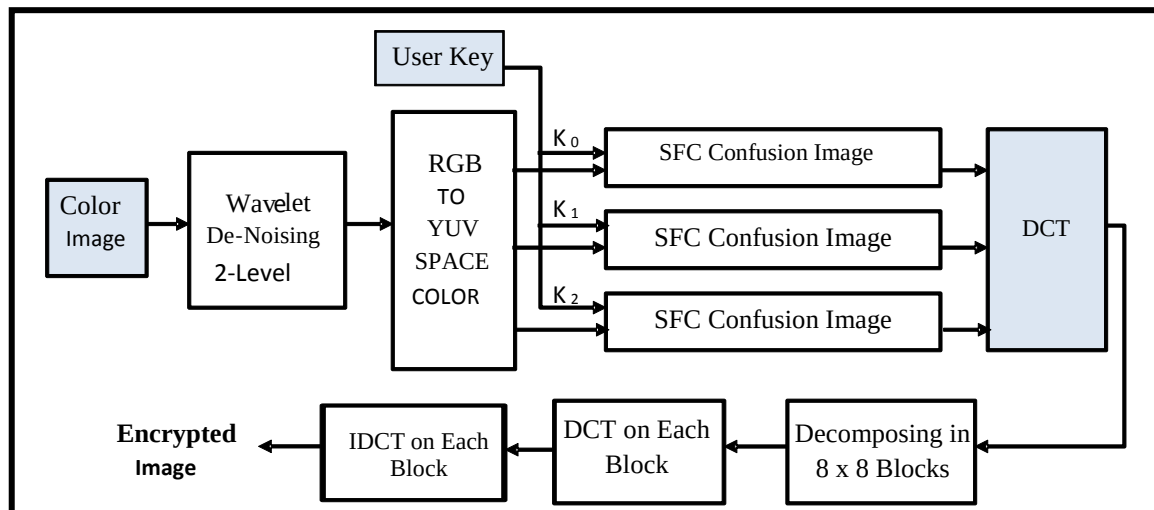


Fig. (3): The proposed Improved Color Plane Permutation based on DCT

Improved Color Plane Permutation Algorithm

Input: Image matrix $I_{N \times N}$

Output: Encrypted Image

Read color image

Input the satellite Imagery (color image) (RGB).

Image De-Noising By wavelet

De-Noising and enhancement the input image using wavelet with 2-Levels.

Convert Image Color Space

The satellite Imagery (color image) after complete de-noising process and preparing transformed from RGB into a YUV color space.

Apply SFC Confusion

This approach is to effect a Block permutation by changing the position of DCT blocks without changing the Block's value.

5. Apply DCT

To perform DCT, it must first divide the image to a block (8×8 pixels), and then apply DCT equation on each block.

Apply IDCT

2. Quality Measures and Performance of Decrypted Image

In this stage PSNR, NAE, AD, NCC, Time measures are used to show the quality of images as shown below.

1) Peak Signal to Noise Ratio (PSNR)

The small value of Peak Signal to Noise Ratio (PSNR) means that image is poor quality. PSNR is defined as follow:

$$PSNR = 10 * \log \left(\frac{(L-1)^2}{MSE} \right) \dots \dots \dots (5)$$

2) Mean Absolute Error(MAE):

The average absolute error (MAE) value means more of the image quality is poor. MAE is defined as follows:

$$MAE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N |x(i, j) - y(i, j)| \dots \dots \dots (6)$$

M, N: size of image

x (i, j): shows samples of original image.

y (i, j) shows samples of image enhancement.

i and j is the number of pixels in rows and columns trends.

3) Average Difference (AD)

It is defined as the average difference between the original and enhanced images. AD is defined as follow:

$$AD = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N [x(i, j) - y(i, j)] \dots \dots (7)$$

4) Normalized Cross – Correlation (NK)

NK is defined as follow:

$$NK = \frac{\sum_{i=1}^M \sum_{j=1}^N [x(i, j) - y(i, j)]}{\sum_{i=1}^M \sum_{j=1}^N [x(i, j) - y(i, j)]^2} \dots \dots \dots (8)$$

3. Analysis of the system

After applying these encryption methods with its steps on various images size 256×256 . The results of images (satellite image) are shown in figures (4-6). Where, image (a) is original image, (b) encrypted image Improved Color Plan Permutation (c) encrypted image using chaotic algorithm and (d) is decrypted image. The encrypted images are understood. Encrypted images of Improved

Color Plan Permutation are comparing with the encrypted images of traditional algorithm (chaotic) using some of quality measures showing in the tables (1-2) below.

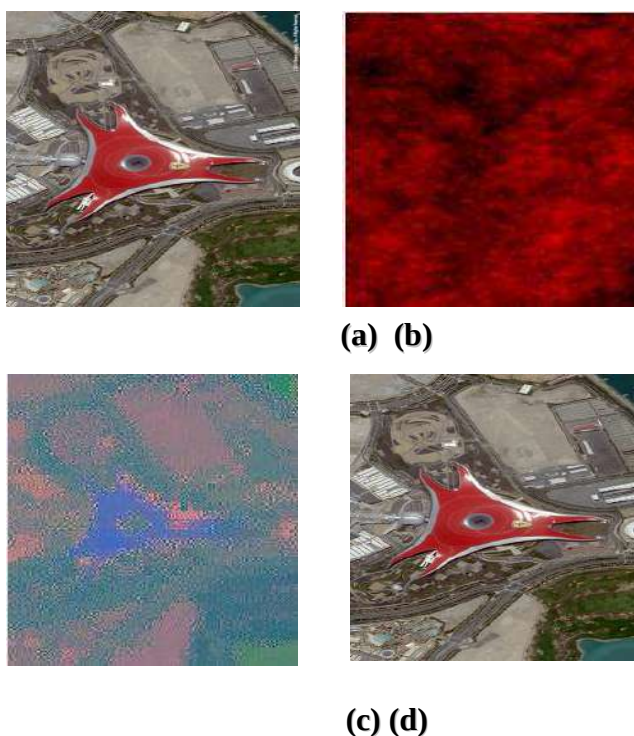


Fig. (4): (a) original image, (b) encrypted images of Color Plan Permutation, (c) encrypted images using chaotic algorithm and (d) decrypted image



Fig. (5): (a) original image, (b) encrypted images of Color Plan Permutation, (c) encrypted images using chaotic algorithm and (d) decrypted image

(a) (b)



(c) (d)

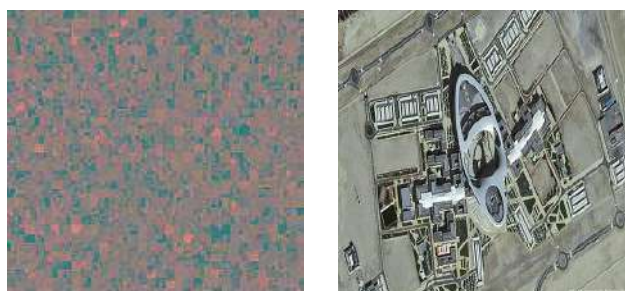


Fig. (6): (a) original image, (b) encrypted images of Improved Color Plan Permutation (c) encrypted images using chaotic algorithm and (d) decrypted image

Table (1) Quality measures of Improved Color Plan Permutation

Image	Improved Color Plan Permutation			
	PSNR	MAE	AD	NK
Image 01	77.072	0.1008	0.0384	0.9803
Image 02	72.447	0.1536	0.0133	0.9589
Image 03	75.370	0.1246	0.0111	0.9660

Table (2) Quality measures of Chaotic algorithm

Image	Chaotic algorithm			
	PSNR	NAE	AD	NK
Image 01	45.368	0.1708	0.0445	0.9803
Image 02	52.433	0.1456	0.0200	0.9589
Image 03	54.388	0.1518	0.0844	0.9660

4. Encryption Speed Test

Experiments on various satellite imagery (color images) show that the proposed method encryption is of high speed. Here, taking various color images for test, the times required for encryption are shown in Table (3). These speeds mean that the encryption using proposed method is of low cost and the scheme is of high speed. From the comparison it see that the Improved Color Plan Permutation faster than the Chaotic algorithm as seen in table (3).

Table (3) show speed test

Image	Speed Test (sec)	
	Improved Color Plan Permutation	Chaotic algorithm
Image 01	81.947	111.351
Image 02	77.672	121.658
Image 03	80.574	115.201

5. Conclusions

Nowadays, multimedia content (image, audio and video) presents a huge importance giving the fact of the rapid growth of high technologies. The rate of exchanges these types of information is growing and the need to protect it is more and more essential. Selective Image Encryption Using DCT with Improved Color Plan Permutation encryptions method has been presented in this paper. The security of the proposed approach is analyzed and compared with the results that be obtained from a traditional algorithm such as (Chaotic). The proposed system is more secure, of low cost, supports direct bit-rate control and is more robust to transmission errors. These properties make it suitable for multimedia applications with real – time operation and image transmission over a network.

References:

- [1] G. Muluaem, "**Compression and encryption for satellite images: a comparison between Squeeze cipher and spatial simulations**", Master thesis. University of Twente. 2015.
- [2] Panduranga H T, NaveenKumar S K, "**Selective image encryption for Medical and Satellite Images**". International Journal of Engineering and Technology (IJET). 2013.
- [3] Abdullah Sharaf Alghamdi, Hanif Ullah, Muhammad Usama Khan, Iftikhar Ahmad and Khalid Alnafajan, "**Satellite Image Encryption for C4I System**". International Journal of the Physical Sciences Vol. 6(17), pp. 4255-4263, 2 September, 2011.
- [4] Musheer Ahmad & Omar Farooq, "**Secure Satellite Images Transmission Scheme Based on Chaos and Discrete Wavelet Transform**". vol 169. Springer. 2011.
- [5] Bin Muhaya F., Usama M., Khan M.K, "**Modified AES Using Chaotic Key Generator for Satellite Imagery Encryption**", vol 5754. Springer. 2009.
- [6] Muhammad Usama, Muhammad Khurram Khana, Khaled Alghathbar, Changhoon Lee. "**Chaos-based secure satellite imagery cryptosystem**", ELSEVIER. 2010.
- [7] Sagan, Hans, "**Space-Filling Curves**", Springer-Verlag. 1994.

A New Algorithm for Image Encryption Based on A New Hyper Chaotic system

Asst. Prof. Dr. Sadiq A. Mehdi Hayder A. Qasim
Dept. of Computer science/ College of Education/ Mustansiriyah University
¹sadiqmehdi71@yahoo.com ²Marun_11981@yahoo.com

Abstract:

In this paper, a new image encryption algorithm using a novel hyper-chaotic system with four-dimension is introduced. The chaotic sequence generated from a new system has been used as key for image encryption, and different security analysis tests indicated that a new hyper-chaotic system has desirable chaotic characteristics like high complexity, security, large key and better performance in comparison with low dimension chaotic maps which have many disadvantage of weak security, simple structure and small key space, the new algorithm characteristics with resist to statistical attack where histogram for encrypted image is completely uniform and the values for correlation analysis are very small and close to (0), while information entropy analysis show that the result of experimental very close to theoretical value (8), the proposed algorithm also demonstrated its ability to frustrate the differential attacks where the result values for number of pixels change rate (NPCR) and unified average changing intensity (UACI) analysis within the theoretical intervals, and the key space very large which refer that the algorithm has more ability to reduce the possibility of brute-force attacks with high sensitivity to small change in key, and finally time required for encryption and decryption within real time.

Keyword: chaos, hyper-chaotic system, aperiodic, image encryption, statistical attack, key sensitivity.

خوارزمية جديدة لتشفير الصورة باستخدام نظام فوضوي مفرط جديد

أ. م. د. صادق عبد العزيز مهدي حيدر عبود قاسم

المستخلص

في هذا البحث قدمت خوارزمية جديدة لتشفير الصورة باستخدام نظام فوضوي مفرط جديد رباعي الابعاد، وقد استخدمت السلسلة الفوضوية المتولدة من النظام الفوضوي في تشفير الصورة، وأشارت التحليلات المختلفة الخاصة بالأمن والاداء الى ان النظام الفوضوي الجديد يتميز بعدة خصائص منها التعقيد العالي، الامنية، مساحة المفتاح الكبيرة، والاداء الافضل بالمقارنة مع الانظمة الفوضوية قليلة الابعاد والتي تحمل الكثير من المساوئ مثل التركيب البسيط وضعف الامنية وصغر مساحة المفتاح، الخوارزمية الجديدة تتميز بمقاومتها للتحليلات الاحصائية اذ يكون شكل المدرج التكراري للصورة المشفرة يكون موحدًا ومنظم، كما ان القيم الناتجة من تحليل الارتباط للصورة المشفرة تكون قريبة الى القيمة النظرية (0)، فيما يكون تحليل الانتروبية يقترب بشكل كبير من القيمة النظرية (8)، كذلك فان الخوارزمية المقترحة بإمكانها احباط هجمات التحليلات التفاضلية حيث تكون قيم معدل تغيير عدد النقاط الصورية (NPCR) وقيم معدل التغيير الموحد للكثافة اللونية (UACI) تكون ضمن فترات القيم النظرية المحددة وتحققها، كذلك فان مساحة المفتاح تكون كبيرة مما يؤدي الى تقليل احتمالية حصول هجمات قوية مؤثرة، فضلا عن الحساسية العالية بالنسبة للتغيير البسيط في المفتاح، واخيرا فان الزمن المطلوب للتشفير وحل التشفير يكون ضمن الوقت الحقيقي.

الكلمات المفتاحية: الفوضوية، نظام فوضوي مفرط، غير دوري، تشفير صورة، الهجمات الاحصائية، الحساسية للمفتاح.

1- Introduction

When the nonlinear dynamical systems evaluated over time with specific values of parameters and initial conditions, that evaluation can be associated with some behavior called “chaos”, the existence of fractal or attractor in phase space where the trajectories of system evolve following a specific pattern but never repeat it, all that refer to a chaotic state [1], the chaotic can be characterized with Lyapunov exponent where chaos behavior occur when there is at least one positive Lyapunov exponent [2], chaotic systems attracted much attention due to its wide application in mathematics physics, computer science and cryptography[3], chaotic system has many characteristics similar to that of cryptosystem, like mixing property, ergodicity, complex conduct,

unpredictability, sensitivity to initial conditions and parameter [4], applying chaos in cryptography algorithms can lead to many advantages like high security, better performance, high speed and less overhead, Matthews British mathematician was the first who used chaos for encryption in 1989, its encryption algorithm include used of one-dimension logistic map to generate chaotic sequence which can be used as one time pad to encrypted messages, Fridrich in 1998 was the first who proposed encryption image algorithm based chaos and referred to any encryption algorithm must composed of two stages "confusion" and "diffusion" where confusion include change or rearrange pixel positions of image while diffusion stage required modify or mask the pixel values[5]. Image in contrast with text has many different characteristics like high redundancy, bulk data capability and high correlation between adjacent pixels, all these reason make conventional encryption algorithm like DES,AES,IDEA,RSA unsuitable for encryption image and many researches proposed use of chaotic maps for encryption image due to desirable features of chaotic maps, in [6] color image encryption algorithm based hyper-chaos Chen system introduced, the proposed method include reduce the correlation among pixels of original image using Arnold map while the second steps involve generate chaotic sequence from Chen hyper-chaotic system to encryption the image pixels the outcome results of analysis tests indicate that the proposed algorithm high security, simple structure in addition to high sensitivity, in[7] a new image encryption algorithm based on hyper-chaotic Chen system constructed, the algorithm include employs an image total scrambling matrix to shuffling the image pixels position, while to disorganize the relationship between the clear-image and the cipher-image and to thwart the statistical attacks the Chen system was used,the outcome results of analysis tests indicate that the proposed algorithm have many advantages like high security, large key space and random-like conduct, in [8] presented a new hyper-chaotic system with four-dimension based on the Rabinovich system for image encryption by using higher dimension chaotic system and enhance the security, where key sequences which used to encryption image is obtained from combining chaotic sequence generated from exponential chaos map and Runge-Kutta method the outcome result of security testes refer that the new hyper-chaotic system has high security and high complexity in comparison with low-dimension chaotic systems.

2- Construction of a new hyper-chaotic system

Recently hyper-chaotic systems attracted much attention due to it is wide application in many systems like electromagnetic waves, atmospheric and viscoelastic hyper-chaotic system is characterized by the system must at least has four dimension, the number of positive Lyapunov exponent more than one, distribution of nonlinear term on equations, two equations must be have one nonlinear term respectively and Lyapunov dimension of the system is fraction, the first hyper-chaotic autonomous 4D system is proposed by Rossler in 1979 [9] in this paper a new hyper-chaotic system proposed and can be describe by the following four nonlinear differential equations:

$$\begin{aligned}\frac{dx}{dt} &= ayz - bxz - cw \\ \frac{dy}{dt} &= dx - xz - y \\ \frac{dz}{dt} &= exy - fz \\ \frac{dw}{dt} &= gxz + hzy\end{aligned}\quad \dots (1)$$

where (x, y, z, w) are the state variables of system and (a, b, c, d, e, f, g, h) are the parameters of the system and all positive real, when the values of a=18, b=3.1, c=2, d=10, e=3, f=2.6, g=5, h=13 and x(0)=0.2, y(0)=0.4, z(0)=0.6, w(0)=0.9, the system is hyper-chaotic and two Lyapunov exponents are positive, L1=0.339251, L2=0.0556285, L3=-1.21134, L4=-29.67, and the attractors are shown in Figure.1.

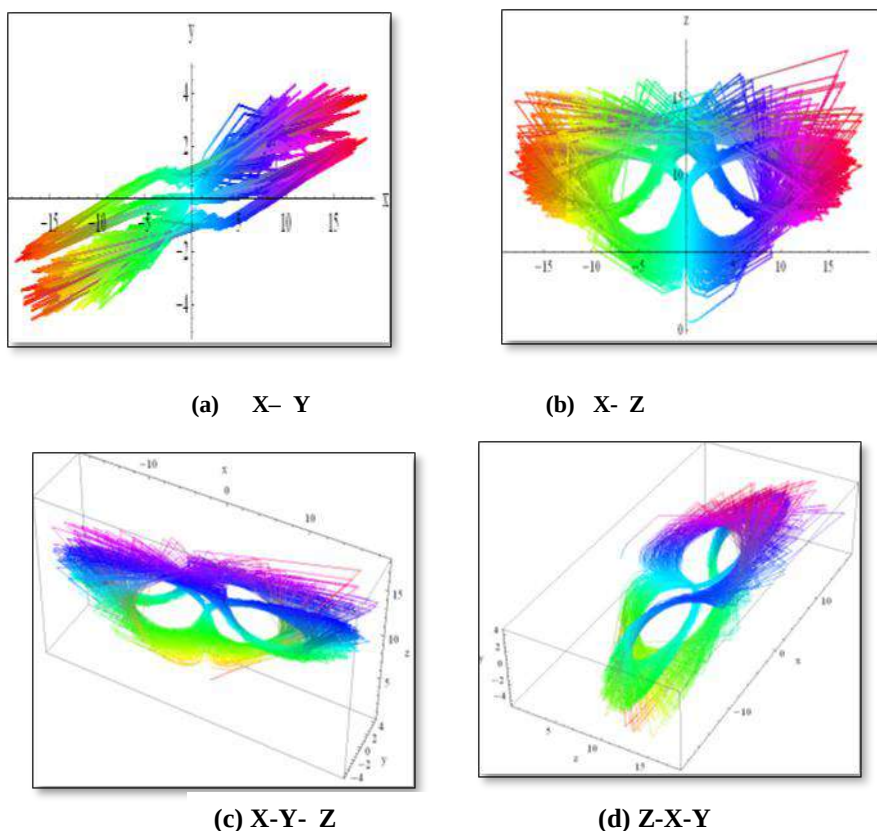


Fig. (1): phase portrait of the new hyper-chaotic attractor, (a), (b) two-dimension plan, (c), (d) three-dimension plan.

Figure.2 can show waveform analysis of hyper-chaotic system it is aperiodic and indicate that the proposed system is a chaotic system, Mathematica simulation utilized to obtain the plots that appear time versus the different states:

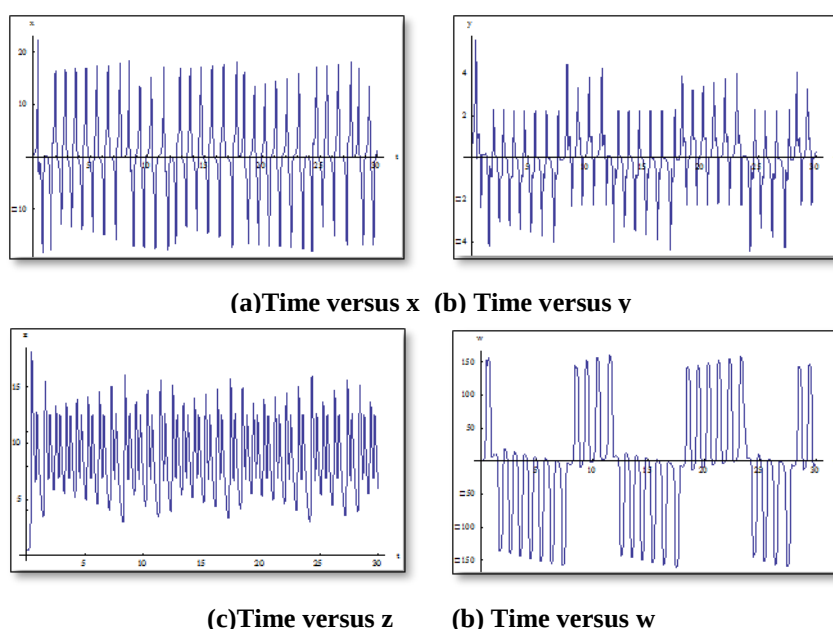


Fig. (2): waveform analysis

3-The proposed algorithm

The proposed a new image encryption algorithm characteristics with large key space, high security and high speed, the encryption algorithm include two basic operations “cconfusion” and “ddiffusion”, where in confusion stage the chaotic sequence generated from hyper-chaotic system used to scrambling the image pixel positions, while in diffusion stage the same chaotic sequence used to masking the image pixel values and the encryption process can describe as follow:

Algorithm of encryption image

Input: original image and key from a new hyper chaotic system.

Output: encrypted image.

Step1: Read the information of the original image and divide it to planes (R, G, B).

Step 2: Select the values for parameters and initial conditions.

Step3: Iterate the chaotic system (1) to generate the chaotic sequence, $\{X_i, i=1, \dots, H \times W\}$

Where H, W act respectively height and width of original image.

Step 4: Obtain vector (S) where $\{S_i, i=1, \dots, H \times W\}$, created from sort vector (X).ascending order.

Step 5: Find original location of each element $i \in S$ in vector (x), save each position in vector (IV) where $\{IV_i, i=1, \dots, H \times W\}$.

Step 6: Scrambling (R, G, B) according to (IV) vector values.

Step 7: Perform the following equation for each $i \in X$.

$$X(i) = (X(i) * 10^{15}) \text{ Mod } 65535$$

Step 8: Applying XOR operation between the plane values (R, G, B) and vector (X).

Step 9: Concatenate back (R, G, B) to create cipher image.

Step 10: Store the encrypted image, parameters and initial conditions.

The decryption process generally is the reverse of encryption process, where the Flower image (800×600) is encrypted and the result show in Figure.3.

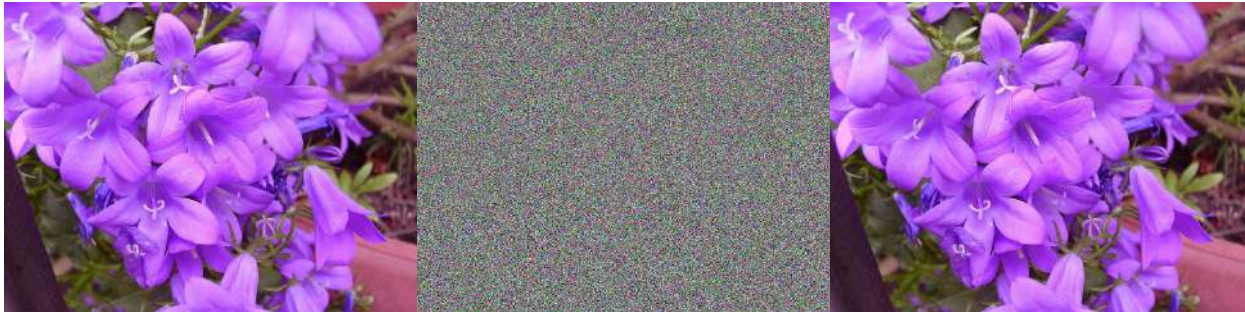


Fig. (3): (a) original Flower image, (b) cipher- image, (c) decrypted- image

4- Experiment Results

Good cryptosystem characteristic with ability of that system to resist many types of attacks like differential attack, statistical attack, brute –force attacks and cipher-text only attack, to measure the ability of proposed algorithm to withstand and frustrate the attacks many tests perform to prove its quality, more than one hundred image tested with cryptosystem and Flower image chosen as study case in this paper.

4-1 Histogram

In image pixels values distributed among many grayscale levels, where histogram is a graph that describe that distribution, for good encryption algorithm statistical similarities must be reduced between histogram of original image and encrypted image to avoid attack and histogram for each must completely different from another to ensure resist of algorithm to statistical attack, the Figure.4 show the histogram for ciphered image is completely uniform in different with that for original image.

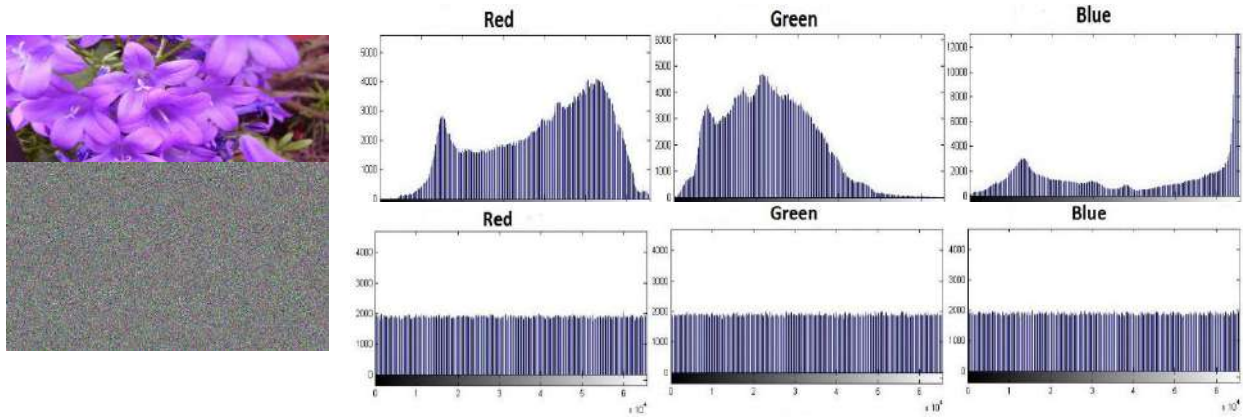


Fig. (4): histogram for rRed, gGreen, bBlue plans of original and corresponding of encrypted image.

4-2 correlation coefficient

Digital image has strong relationship among its adjacent pixels and any good encryption algorithm must be hide all characteristics of plain image, where the encrypted image must be completely different and uncorrelated, and correlation study for two adjacent pixels in (horizontal, vertical and diagonal) where the equation 5 used to that purpose.

$$D(x) = \frac{1}{N} \sum_{i=0}^N (x_i - E(x))^2, \quad \dots\dots (2)$$

$$E(x) = \frac{1}{N} \sum_{i=0}^N x_i, \quad \dots\dots (3)$$

$$\text{cov}(x, y) = \frac{1}{N} \sum_{i=0}^N (x_i - E(x))(y_i - E(y)), \quad \dots\dots (4)$$

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \quad \dots\dots (5)$$

Where (N) represent total numbers of samples and (x_i, y_i) are grayscale values of i-th pair of adjacent pixels and the Table 1 show correlation for original image and ciphered image [10].

Table (1) correlation for original “Flower” image and encrypted image.

	cHorizontal	nVertical	kDiagonal
correlation for soriginal image	00.9886	00.9891	00.9812
correlation for encrypted image	00.0005	00.0006	00.0007

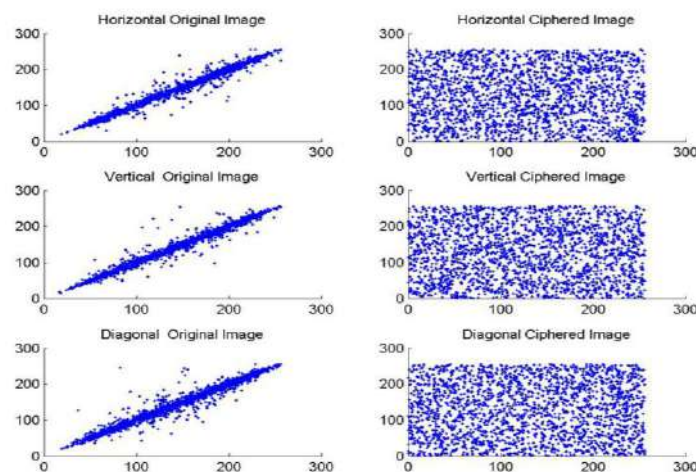


Fig. (5): correlation for two adjacent pixels horizontally, vertically and zdiagonally in original image “Flower” and its encrypted image.

From Table 1 and Figure 6, it's clearly show that correlation for the encrypted image is reduced due to high performance of the proposed encryption algorithm.

4-3 information entropy analysis

Information entropy of image describe the degree of uncertainties in an image and can be calculated from the following equation:

$$E(m) = \sum_{i=0}^{G-1} p(m_i) \log_2 \frac{1}{p(m_i)} \quad \dots (6)$$

Where entropy for encrypted image must be close to theoretical value 8 to ensure resistance of the proposed encryption algorithm to entropy attack [11].

Table (2) entropy values for plain image and ciphered image.

hImage	iImage size		rRed plane	gGreen plane	uBlue plane
Flower	800*600	Original	7.2771	7.0945	7.3285
		encrypted	7.9254	7.9148	7.9980

4-4 nNumber of Pixel Change Rate and Unified Average Change Intensity

One of the desirable characteristic of any encryption algorithm is sensitivity to plaintext, where any small change even with one pixel must be lead to completely different encrypted image with respect to encryption key, NPCR and UACR measures utilized to study the influence of change one pixel on the overall ciphered image, where NPCR can represent by the equation (7).

$$NPCR = \frac{\sum_{i,j}^{N,M} D(i,j)}{W \times H} \times 100\% \quad \dots (7)$$

NPCR is used to calculate the percentage of different pixel numbers between two encrypted images. UACI is utilized to measure the average intensity of difference between two ciphered images and expressed by the equation (8).

$$UACI = \frac{1}{W \times H} \left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255} \right] \times 100\% \quad \dots (8)$$

The result values for NPCR and UACI with in theoretical values [12] and the encryption algorithm has good resist to differential attacks [13].

Table (3) NPCR and UACI result values.

	size	nNPCR	uUACI
Flower	800×600	99.9983	33.4918

4-5 key space analysis

To frustrate the brute-force attacks the key space must be more than 2^{100} [14] and in the proposed encryption algorithm the key space calculated from parameters and initial conditions, where if the precision for each is 10^{-14} , then the key space is 10^{168} and that approximately equal 2^{550} .

4-6 sensitivity to decryption key

A secure algorithm in addition to its sensitivity to plaintext must be very sensitive to key change, where small change in key the cipher image must be completely different and to measure the sensitivity of encryption algorithm, small value up to (10^{-14}) will add to decryption key, where the value of $w(0)$ change from $w(0)=0.9$ to $w(0)=0.900000000000001$ and the oFigure 7 can show that the intruder cannot decrypted the image even with slightly difference in key and the encryption algorithm has high sensitivity to key.

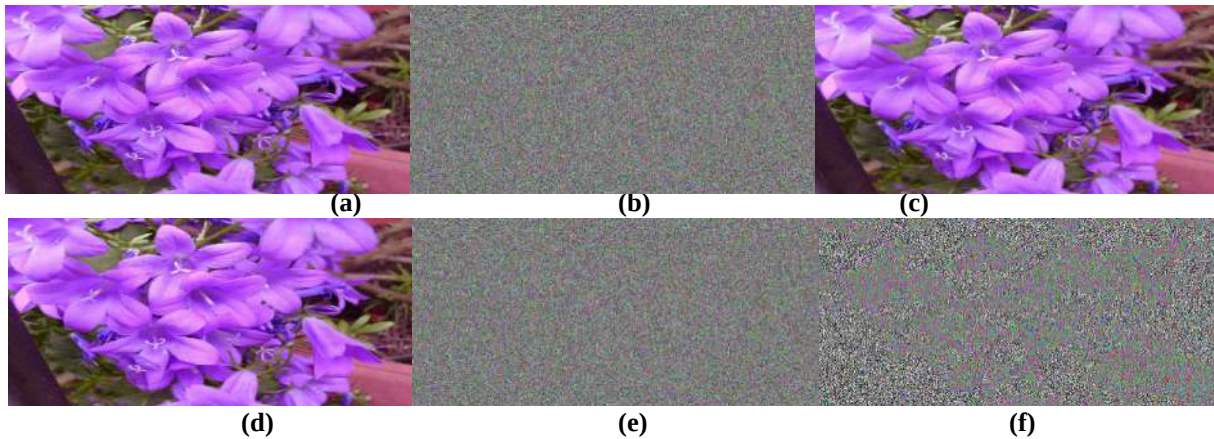


Fig. (7): (a),(d) original image “Flower”, (b),(e) ciphered image with $w(0)=0.9$, (c) Decrypted image with valid key, $w(0)=0.9$, (f) decrypted image with uncorrected key, $w(0)=0.9000000000000001$.

4-7 Efficiency Analysis

The good cryptosystem must be efficiency and appropriate for real time application where the cryptosystem implemented with Matlap13, and pc cori7, RAM 4G.

Table 4: encryption and decryption time.

Image	Size	Average Encryption time (seconds)	Average Decryption time (seconds)
Flower	800×600	0.5842	0.5968

From Table 3 the encryption algorithm has high efficiency and desirable for real time encryption application.

5- Comparison between proposed system and Rossler hype-chaotic system.

To demonstrate the high security, complexity and efficiency performance of the proposed system, the system has been compared with Rossler system using same algorithm to encrypt images and the result of tests in Table (5, 6, 7) show the efficiency of proposed system, where all tests Related to encrypted image.



City (600×410)

Table 5 show when based the proposed system in encryption algorithm the correlation values are very small and more close to zero.

Table 6 show the Entropy values for encrypted image planes are more close to eight when proposed system used.

Table (5) correlation values for Rossler hyper-chaotic system and proposed hyper-chaotic System.

Correlation for encrypted image (City)	hHorizontal	vVertical	dDiagonal
Rossler system	-00.0022	00.0018	-00.0010
Proposed system	-00.0007	00.0016	00.0010

Table (6) entropy values for Rossler hyper-Chaotic system and proposed hyper-chaotic system.

	NPSR	UACI
Rossler	99.9983	33.2550
Proposed system	99.9987	33.2333

Table (7) NPSR and UACI for Rossler hhyper-Chaotic system and proposed hhyper-chaotic system.

information Entropy for encrypted image city	Red	Green	Blue
Rossler	7.8613	7.8248	7.9974
Proposed system	7.8952	7.8381	7.9976

6. Conclusion:

A new chaotic based image encryption algorithm presented in this paper, where a new hyper-chaotic system used to shuffling image pixels and modifying its values, oFigure.1 and Figure.2 show the attractor and waveform analysis for proposed system and it is clearly display chaotic behavior, the security of encryption algorithm analysis with many tests and results show that the encryption algorithm has high resistance to statistical attacks where histogram test for encrypted image is completely uniform and correlation values for encrypted image planes (0.0005,0.0006,0.0007) is very small and close to zero, while the entropy values for encrypted image planes (7.9254, 7.9148, 7.9980) are close to theoretical value, the encryption algorithm also has high resistance to differential attack, where the values for number of changing ppxel rate and unified averaged changed intensity is pass the all theoretical intervals, the key space is very large 2^{550} and can frustrate the brute-force attack, in addition to that the encryption algorithm has good sensitivity to key change and appropriate for real time image encryption.

References

- [1] Alireza Jolfaei, Abdolrasoul Mirghadri, "Image Encryption Using Chaos and Block Cipher", Computer and Information Science, Vol, 4, No.1, 2011, p172-179.
- [2] Sadiq A. Mehdi, Abid Ali H. Alta'ai and Salim Ali ABBAS, "Analysis of A Novel Chaotic Dynamic System with ten quadratic nonlinearities", IOSR Journal of Mathematics (IOSR-JM), e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 11, Issue 2 Ver. IV (Mar - Apr. 2015), PP 40-46.
- [3] Sadiq A. Mehdi, Abid Ali H. Alta'ai and Salim Ali ABBAS, "Bifurcation and The Influence parameters On A Novel Chaotic Dynamic System", ISSN: 19948638, (2015), Volume: 7 Issue: E1 Pages: 83-92.
- [4] Sadiq A. Mehdi and Rabiha Saleem Kareem, "Using Fourth-Order Runge-Kutta Method to Solve Lü Chaotic System", American Journal of Engineering Research (AJER), e-ISSN: 2320-0847 p-ISSN: 2320-0936, (2017), Volume-6, Issue-1, pp-72-77.
- [5] J. Vahidi, M. Gorji, "The Confusion-Diffusion Image Encryption Algorithm with Dynamical Compound Chaos", Journal of mathematics and computer Science, Vol 9, (2014), p 451 – 457.
- [6] Danial Roohbakhsh, Mahdi.Yaghoobi, "Color Image Encryption using Hyper Chaos Chen", International Journal of Computer Applications (0975 – 8887) Volume 110 – No. 4, January 2015.
- [7] Tiegang Gao, Zengqiang Chen, "A new image encryption algorithm based on hyper-chaos", Physics Letters A 372 (2008) p 394–400.
- [8] Xiaojun Tong, Yang Liu, Miao Zhang, Hui Xu and Zhu Wang, "An Image Encryption Scheme Based on Hyperchaotic Rabinovich and Exponential Chaos Maps", entropy, 2015, 17, 181-196.
- [9] Jafar Biazar1, Tahereh Houlari1 and Roxana Asayesh1, "Implementation of multi-step differential transformation method for hyperchaotic Rossler system", International Journal of Applied Mathematical Research, 6 (1) (2017) 4-6.

- [10] Mintu Philip, "AN Enhanced Chaotic Image Encryption", International Journal of Computer Science, Engineering and Information Technology IJCSEIT), Vol.1, No.5, December 2011.
- [11] Ruisong Ye, Weichuang Guo, "A chaos-based image encryption scheme using multimodal skew tent maps", Journal of emerging trends in computing and information science, Vol.4, No.10, 2013.
- [12] Wu, Y., Noonan, J. P., And Agaian, S., "NPCR and UACI Randomness Tests for Image Encryption", Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), April Edition 2011, pp.31-38.
- [13] Borislav Stoyanov and Krasimir Kordov, "Image Encryption Using Chebyshev Map and Rotation Equation", Entropy 2015, Vol 17, P2117-2139.
- [14] Alvarez, G., and Li, Sh., "Some Basic Cryptographic Requirements For Chaos-Based Cryptosystems", International Journal of Bifurcation and Chaos, Vol. 16, No. 08, 2006, pp. 2129-2151.

Design System to Perform and Measures Stream Cipher Algorithms

Prof. Dr. Salim Ali Abbas Ali Jumaa Hashim

Department of Computer Science, College of Education/ Mustansiriyah University

alageeleedr.salim@yahoo.com a.hussen65@yahoo.com

Abstract:

Stream cipher algorithm is one of encryption types which has a number of good features. It is considered software-efficient because it requires simple programming instruction when it implement in software, and it consider hardware-efficient because it not require expensive hardware to implement. In this paper, we design stream cipher system, the proposed system provides the designer of stream cipher the capability of building stream cipher in new way, this new way is building stream cipher in visual manner, by providing most of stream cipher components such as LFSR, table, logical gates, and provides the possibility to link these components visually to allow date to passing among them. In addition to this new way, the proposed system also provides the possibility to building stream cipher by enter C# programming instructions of designed algorithms. The system provides the designer the capability to test keystream which produced by the designed algorithm, the test is done by apply 14 NIST statistical tests that measures the randomness proprieties and complexity of any keystream sequence. Finally, the proposed system has the ability to encrypt or decrypt any plaintext/cipher text.

Keyword: Stream Cipher, System, NIST Statistical Tests.

تصميم حزمة لبناء وتقييم خوارزميات التشفير

أ. د. سالم علي عباس علي جمعة هاشم

المستخلص

خوارزمية التشفير الانسيابي هي احد انواع التشفير التي تمتلك عدد من المزايا الجيدة، انها تعتبر ذات كفاءة عندما تنفذ برمجيا لانها تتطلب عدد قليل من التعليمات البرمجية البسيطة، وايضا تعتبر ذات كفاءة عندما تنفذ بواسطة الاجزاء المادية لانها لا تتطلب دوائر الكترونية باهظة الثمن. في هذه الورقة، تم تصميم نظام تشفير انسيابي، النظام المقترح يزود المصمم بالقابلية على بناء خوارزمية تشفير انسيابي بطريقة جديدة، وهي بناء خوارزمية التشفير الانسيابي بطريقة مرئية، من خلال تزويد المصمم بمعظم مكونات الخوارزمية مثل، LFSR الجدول، البوابات المنطقية. فضلاً عن ذلك فانه يتم تزويد المصمم بالقابلية على عمل ارتباطات بين تلك المكونات بطريقة مرئية وذلك للسماح بتبادل البيانات بينها. فضلاً عن هذه الطريقة الجديدة في بناء خوارزمية التشفير الانسيابي، فان النظام المقترح ايضا يزود المصمم بالقابلية على بناء خوارزمية التشفير الانسيابي من خلال ادخال الاوامر البرمجية للخوارزمية بلغة C#. النظام المقترح يزود المصمم بالقدرة الى اختبار المفتاح الناتج من الخوارزمية المصممة، هذا الاختبار يتم من خلال تطبيق 14 (اربعة عشر) اختبار احصائي مقامة من NIST. هذه الاختبارات تقيس الخواص العشوائية ومدى التعقيد للمفتاح لاي سلسلة من المفتاح. اخيراً، النظام المقترح يمتلك القابلية على تشفير وفك تشفير اي نص واضح/ نص مشفر.

الكلمات المفتاحية: خوارزمية التشفير الانسيابي، الاختبارات الاحصائية، نظم.

I. Introduction

As we enter the information age and the emergence of the means of digital transmission and storage of data in digital form, there was a need to develop ways to protect information from theft. [1]. Cryptography includes design and analysis a mathematical technique that provide a secure connection in the presence of a third party that seeking to disclosure of transmitted or stored information [2].

Stream cipher algorithm is one ways that used to encrypt the information and convert it into another form. Stream cipher has number of features, it is fast, and considered efficient in hardware because it is not required expensive hardware circuit. Therefore, the construction and design of stream

cipher algorithm in fast and comfortable manner is an important need for those people who specialize in building stream cipher algorithm to protect their information from theft [3].

Encryption algorithm can be classified into two types, the first type is symmetric encryption, in this type used one private key that shared between the communication parties (the sender and the recipient). The second type is asymmetric encryption, in this type used two keys, the first public and open for everyone, and the second is kept secret, and in this type one key cannot be inferred from the other keys [4]. Asymmetric encryption is slow because it's based on mathematical theories, which is impractical in applications that require live and direct processing. In symmetric encryption, there are two types of algorithms, block algorithm and stream algorithm, in Block encryption algorithm the plaintext dividing into blocks of bits. Famous Block algorithms are AES and DES [5]. Stream cipher is developed as a solution to the problems of encryption one-time pad system. In one-time pad the key must be completely random and its length is equal to the length of the message to be encrypted and uses one time, because of the impracticability of one-time pad system so stream encryption system consider acceptable solution to these problems. In the stream cipher algorithm, pseudo-random key is generated using one of pseudo-random generator [6].

Encryption in stream cipher is done by dividing the clear text into bits and then every bit is encrypted individually. Stream algorithm relies entirely on security of pseudorandom key stream. To design stream algorithm, the designer can use several components and methods, the LFSR is most popular components used in the constructing of stream algorithm [7].

II. The Proposed System

The proposed system is made up of three primary components, each component is responsible of a specific function, the first component is providing construction of stream cipher in two way, the first way is the visual way and it is new way to constructing stream cipher, the second way is construction stream cipher by enter C# programming code. The second component is responsible for evaluating (testing) the keystream sequence which produced from the first component, the evaluation process is done by apply Fourteen NIST statistical tests, these tests are measure the randomness and complexity proprieties of keystream sequence. The third and Final component is responsible for encrypt or decrypt any text by using the keystream which generated from the first component, the encryption/decryption process is done by mixing text and keystream sequence using XOR function. Fig.1 shows the structure of proposed system.

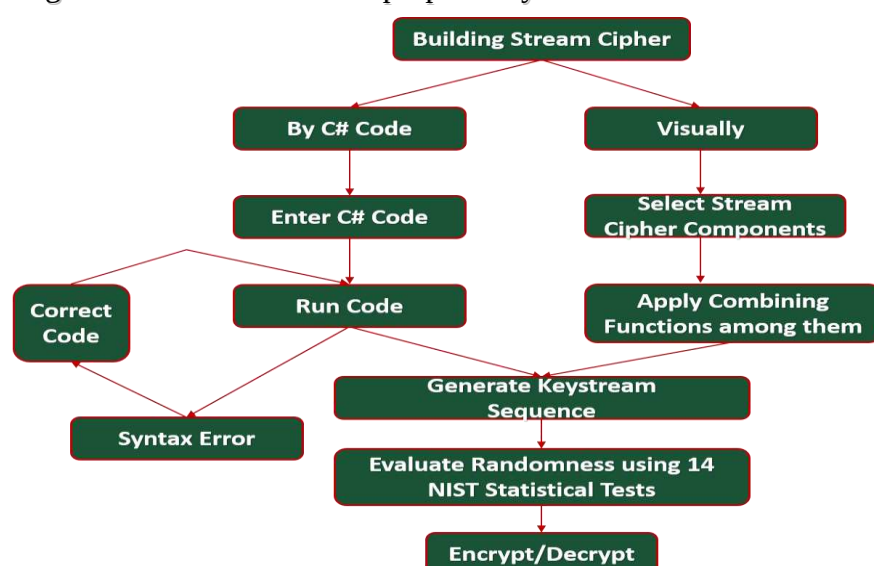


Fig.(1): Structure of the proposed system.

III. Constructing Of Stream Cipher Algorithm

As we discussed, the proposed system is capable of constructing stream cipher in two way, the first way is the visual way and it is new way in constructing stream cipher, and the second way is

building stream cipher through enter and executing C# programming code of the designed algorithm.

IV. Building Stream Cipher Visually

This method or way in building stream cipher is new way and has number of features, its reduce the total time of designing stream cipher algorithm and focus the attention of the designer on the designed algorithm, and this method works to generate the key faster and by determining any length desired by the designer. To illustrate how the proposed system provides this new ability, we take the example of building Linear feedback shift register (LFSR) in visual manner.

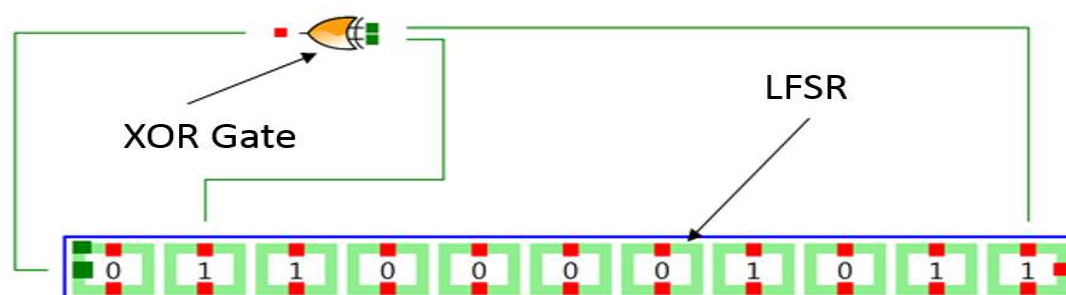


Fig. (2): Example of LFSR.

As shown in fig.2, LFSR is consists of two components, shift register and XOR combining function. Each component is consists mainly of three sub-component, which are, input sub-component (in green color), function sub-component, and output sub-component (in red color), the input is responsible for feeding new data value to function component, the function sub-component is manipulate the input data by applying a specific function such as, XOR or AND OR NOT... ets, and finally the output sub-component is responsible for transfer the new computed value to other component which connected to it.

To connected two components, the designer should click on output box of one component and then click on input box of other component, after that the connection line will appear between the connected component to imply the success of connection process as shown in fig 2.

The proposed system is providing number of stream cipher component, which are, linear feedback shift register, the logical gates such as XOR, AND, OR, JK flip flop, Inner product, police component, shrinking component, with capabilities to link these components to allowing the data to passing among them and finally generate the keystream sequence.

A. Design of the Main Interface

The main interface of proposed system is made up of four parts, tool bar, design area, stream cipher components bar, and information box.

Following is descriptions of each part:

- 1- Tools bar has tools with following functions:
 - a) Generate one bit from the designed keystream generator in each click.
 - b) Generate sequence of bits in each click, length of desired sequence enters in the textbox.
 - c) Open the window of design stream cipher algorithms using C# programming language.
 - d) Save and load designed stream cipher algorithm.
 - e) Delete any selected stream cipher components.
 - f) Text box used to enter the following:
 - 1) The length of LFSR and table components.
 - 2) To enter the content of LFSR and table. Text box also used to enter a number that represent the length of sequence to be generated from the designed keystream generator in the design area.
- 2- Design area

It is area allocated to design keystream generator visually through drag any desired components from components list and drop them on the design area,

3- Stream cipher components

It is a list of stream cipher components that used in constructed keystream generator.

4- Information box

This text box used to show information about stream cipher components that exist in design area.

B. Description of the Mechanism to Connect SCA Components

After putting all the stream cipher components on the design area in the main interface, the designer start to make connections among the components to allow of passing data among connected components. Fig.3 shown the scenario of linking two components (Comp1 and Comp2), each has one input and one output. To make connection between Output1 object that belong to comp1 and Input2 object that belong to Comp2, the designer first clicks on the Output1 of Comp1, then the designer clicks on the Input2 object of Comp2, after that the connection line will appear connecting the two components and it is imply the success of connection.

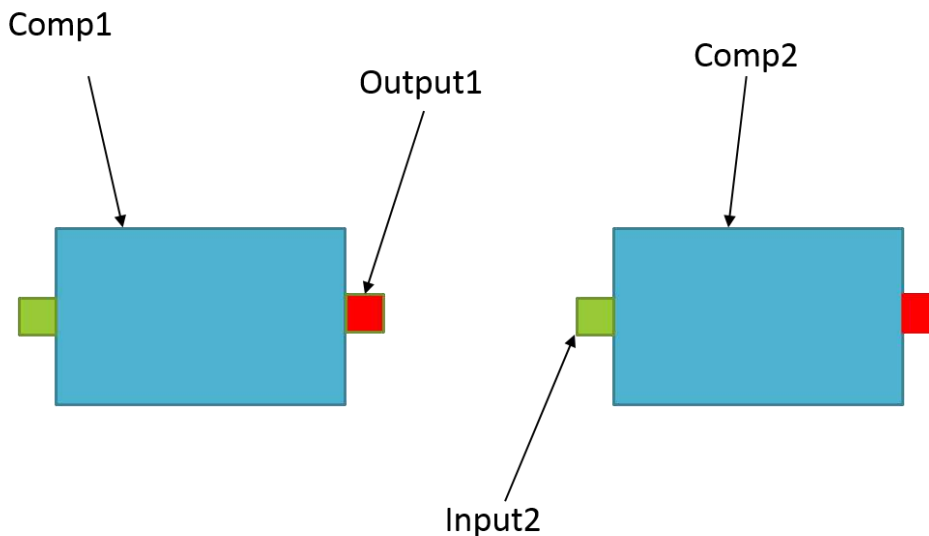


Fig. (3): Example of connecting two components

V. Build Stream Cipher Algorithms By C# Programming Language

The designer can enter the C# code of any stream cipher algorithm in C# code box or can import the C# code by click on the import button in button bar. After enter C# code, the designer has to click on the Run button in button bar to start compiling and execute of entered code. After execute the entered C# code, the output of C# code will appear in output box. Any syntax error in the entered code this will show error message in the error box.

VI. Evaluations Component

The proposed system provides fourteen statistical tests as shown in fig.4. Each test is produced value called P_value, this value if it is greater than or equal to 0.01 then the test is pass and the keystream is random, otherwise, the test is fail and the keystream is not random.

Import
Test

Nist Statistical Tests

The statistical tests	P-value	State	The statistical tests	P-value	State
Frequency test			Frequency within a Block		
Serial			Maurer's "Universal Statistical"		
Random Excursions			The Linear Complexity		
Overlapping Templates			The Approximate Entropy		
Run			The Cumulative Sums (forward)		
Tests for the Longest-Run-of-Ones in a Block			The Cumulative Sums (backward)		
The Binary Matrix Rank			The Non-overlapping Template Matching		
RandomExcursionsVariant			Discrete Fourier Transform		

Note: If the computed P-value is < 0.01, then conclude that the sequence is non-random and test fail . Otherwise, conclude that the sequence is random and test is pass.

Fig. (4): Evaluation interface

VII. Design Encryption/Decryption Interface

In the interface, there are number of buttons that perform following actions:

- 1- Import any text to encrypt it or decrypt.
- 2- Import any key file to use it in encryption/decryption process.
- 3- Clear all text in text boxes.

When the designer clicks on the encrypt button, the following actions will perform:

- 1- Convert the plain text and key stream characters to a sequence of byte.
- 2- Mix the key bytes with plaintext bytes by using XOR function, the result represents the cipher text. The cipher text stored in new array.
- 3- The new sequence that produce from mix plaintext with key stream will appear in Textbox2 in the encryption /decryption interface.

To decrypt the cipher text, the designer has to do the following

- 1- Import the cipher text file through click on import Plain/cipher text button.
- 2- Import the key stream used in produce the cipher text.
- 3- Click on the Encrypt/Decrypt button to start mixing the cipher bytes with key bytes, the result is the plaintext and will appear in the Textbox2.

VIII. Design And Evaluate Number Of Keystream Generators By Proposed System

A. Constructing and Evaluates New Stream Cipher Generator

The new designed generator is made up of following components:

- 1- Three linear feedback shift register of lengths (13, 11, 7), and each LFSR is initialize with value "ali"
- 2- Four logical gates (tow XOR, one AND, one NOT).
- 3- JK flip flop

Designed generator produced keystream of length 1000 bit which take 19 second to produced. Fig.5 is shows the new generator as built in proposed system.

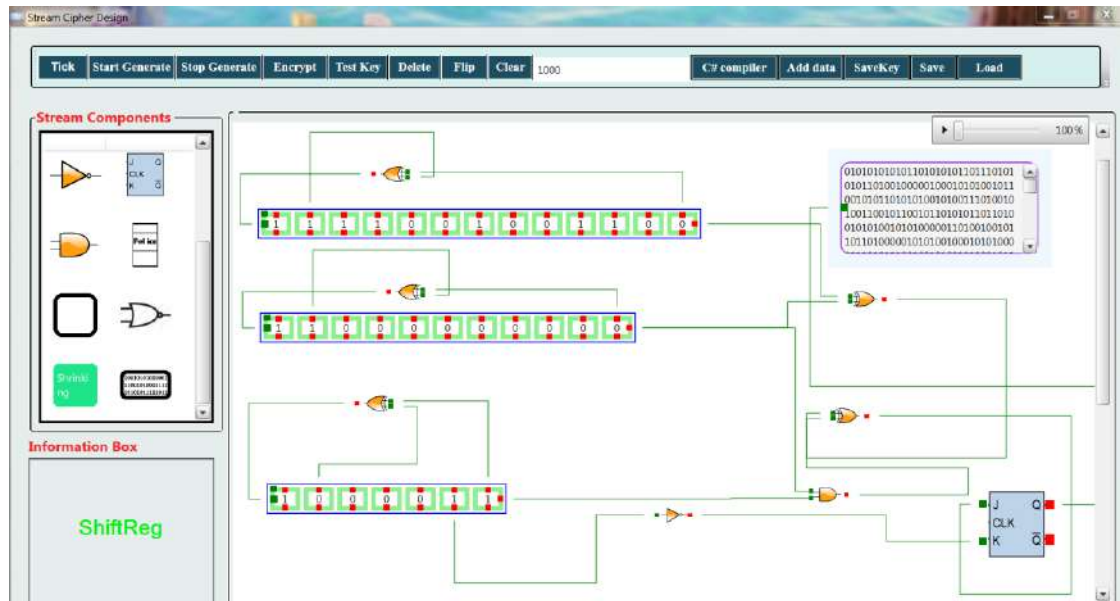


Fig. (5): Designed New Stream Cipher Generator

The designed generator is evaluated by applied 14 NIST statistical tests and fig.6 is shown the results of applying these tests.

Nist Statistical Tests					
The statistical tests	P-value	State	The statistical tests	P-value	State
Frequency test	0.38273309	Pass	Frequency within a Block	0.54482554	Pass
Serial	1.02454544	Fail	Maurer's "Universal Statistical"	0	Fail
Random Excursions	0	Fail	The Linear Complexity	0.98561031	Pass
Overlapping Templates	NaN	Fail	The Approximate Entropy	1.23765011	Fail
Run	8.95227208	Fail	The Cumulative Sums (forward)	0.74783415	Pass
Tests for the Longest-Run-of-Ones in a Block	0.09044614	Pass	The Cumulative Sums (backward)	0.21907666	Pass
The Binary Matrix Rank	0	Fail	The Non-overlapping Template Matching	0.99588272	Pass
RandomExcursionsVariant	0.45098229	Pass	Discrete Fourier Transform		

Note: If the computed P-value is < 0.01, then conclude that the sequence is non-random and test fail. Otherwise, conclude that the sequence is random and test is pass.

Fig. (6): Results of testing the new designed generator

B. Constructing and Evaluate Geffe Generator

Designed Geffe generator has following components:

- 1- Number of used LFSRs are 3; LFSRs have lengths(11,7,5), all LFSRs are initialized with (abc)
- 2- Logical gates (one XOR gate, two AND gate, one NOT gate)

Fig.7 show designed Geffe generator. After generating keystream of length 1000-bit (which taking time equal to 16 second), we evaluate the keystream and fig.8 shows the results of evaluation.

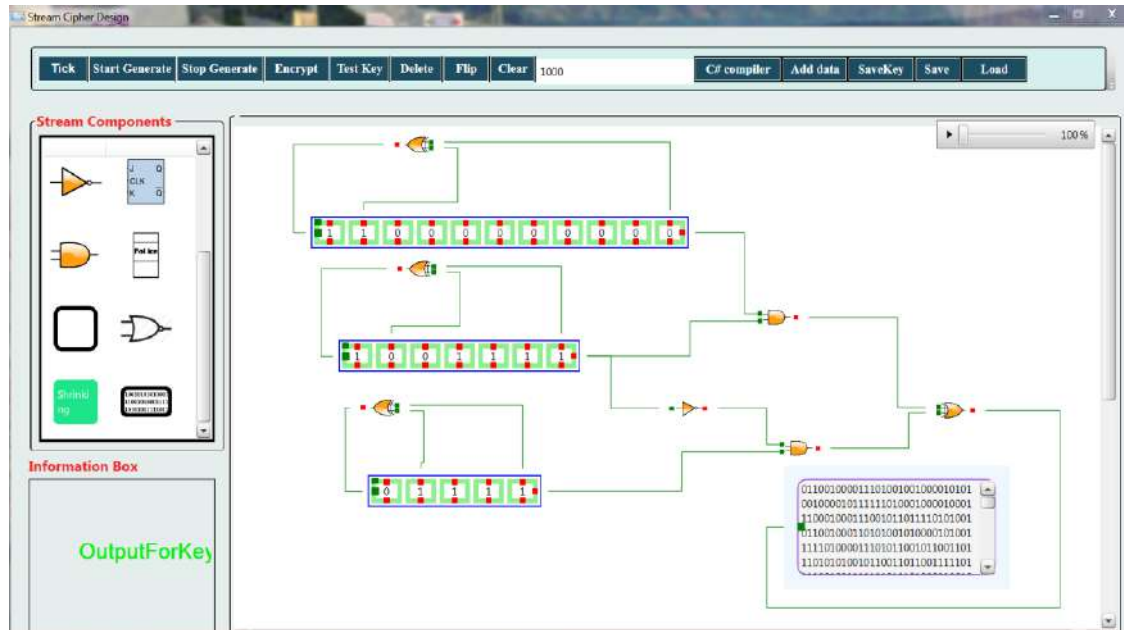


Fig. (7): Designed Geffe generator

Nist Statistical Tests					
The statistical tests	P-value	State	The statistical tests	P-value	State
Frequency test	0.22949316	Pass	Frequency within a Block	0.14558127	Pass
Serial	0.39772279	Pass	Maurer's "Universal Statistical"	0	Fail
Random Excursions	0	Fail	The Linear Complexity	4.10679460	Fail
Overlapping Templates	NaN	Fail	The Approximate Entropy	0.07893210	Pass
Run	0.60006721	Pass	The Cumulative Sums (forward)	0.21359000	Pass
Tests for the Longest-Run-of-Ones in a Block	0.09629614	Pass	The Cumulative Sums (backward)	0.16398027	Pass
The Binary Matrix Rank	0	Fail	The Non-overlapping Template Matching	0.98727193	Pass
RandomExcursionsVariant	0.49271664	Pass	Discrete Fourier Transform		

Note: If the computed P-value is < 0.01, then conclude that the sequence is non-random and test fail . Otherwise, conclude that the sequence is random and test is pass.

Fig. (8): Results of testing Geffe generator

C. RC4 Stream Cipher Algorithm

Fig.9 shows build stream cipher algorithm by the proposed system, the algorithm is RC4 and has been built by enter C# code of RC4.

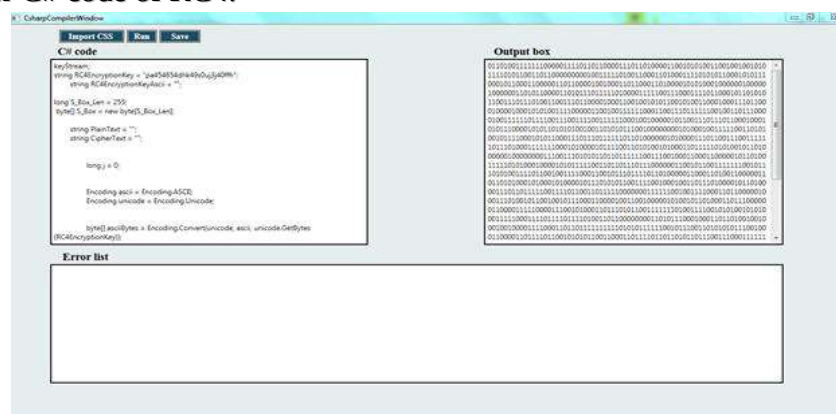


Fig. (9): The implementation of RC4

After save the key produced by the code of RC4 in text file, the key should save as binary sequence of '1' and '0'. The designed RC4 algorithm produced 2040 bits. Fig.10 shown the results of testing the keystream that produced from designed RC4 algorithm.



The statistical tests	P-value	State	The statistical tests	P-value	State
Frequency test	0.85941181	Pass	Frequency within a Block	0.04828967	Pass
Serial	0.76592833	Pass	Maurer's "Universal Statistical"	0	Fail
Random Excursions	0	Fail	The Linear Complexity	0.98560428	Pass
Overlapping Templates	0.95203973	Pass	The Approximate Entropy	0.87932927	Pass
Run	0.47906434	Pass	The Cumulative Sums (forward)	0.71509839	Pass
Tests for the Longest-Run-of-Ones in a Block	0.23090731	Pass	The Cumulative Sums (backward)	0.79746057	Pass
The Binary Matrix Rank	0.69372014	Pass	The Non-overlapping Template Matching	0.39002319	Pass
RandomExcursionsVariant	0.16512359	Pass	Discrete Fourier Transform		

Note: If the computed P-value is < 0.01, then conclude that the sequence is non-random and test fail. Otherwise, conclude that the sequence is random and test is pass.

Fig. (10): Results of testing RC4

IX. Conclusion

- 1- The proposed system provides easier and friendly tool to build unlimited number of stream cipher algorithm, either visually by use existing stream cipher components or by enter C# code.
- 2- The system provides the capability to the designer to test the keystream sequence which produced by designed algorithm, testing is done by apple 14 (fourteen) statistical tests that measures randomness and complexity proprieties of any keystream of appropriate length.
- 3- The proposed system is capable of encrypt/decrypt any text by using keystream which generated by the designed algorithm.

References

- [1] Rainer A. Rueppel, "Analysis and Design of Stream Ciphers", Berlin, Springer, 1986.
- [2] Darrel Hankerson, Alfred Menezes and Scott Vanstone, "Guide to Elliptic Curve Cryptography", New York, Springer, 2004.
- [3] Mohammad Ubaidullah Bokhari, Shadab Alam, Syed Hamid Hasan, "A Detailed Analysis of Grain family of Stream Ciphers", I. J. Computer Network and Information Security, 2014
- [4] Richard R. Brooks, "Introduction to Computer and Network Security", Boca Raton, CRC Press, 2014.
- [5] Christof Paar and Jan Pelzl, "Understanding Cryptography a Textbook for Students and Practitioners", Berlin, Springer, 2010.
- [6] M.J.B. Robshaw, "Stream Ciphers RSA Laboratories Technical Report TR-701", Redwood City, CA, RSA Laboratories, 1995.
- [7] Andreas Klein, "Stream Cipher", London, Springer, 2013.

Use PSO and IPSO in Cryptanalysis: Comparative Study

Prof. Dr. Salim Ali Abbas Riyam N. J Kadhum

Department of Computer Science, College of Education/ Mustansiriyah University

qweenr80@gmail.com alageeledr.salim@yahoo.com

Abstract:

Stream cipher is one of the hard electronic cipher systems because of high security and difficulty in breaking it. In this paper the proposed cryptanalysis system based on a Particle Swarm Optimization (PSO) with suggestions for improving the achievement of PSO, by using Simulated Annealing (SA) that is the first part of this paper. The second part represented by a comparison study for the cryptanalysis results obtained by the proposed technique, which is called Improved PSO (IPSO) with classical PSO. The cryptanalysis process includes finding the initial setting of the attacked generator using cipher text only attack with new fitness function using different ciphertext lengths and different lengths of LFSRs.

Well known stream cipher systems are attacked as case of study which are Geffe and Bruer systems.

Keyword: Stream Cipher System, Cryptanalysis, Particle Swarm Optimization, Simulated Annealing, Improved Particle Swarm Optimization.

1. Introduction

Cryptanalysis is the science of recovering the plaintext of a message without access to the key. It is a method of transforming cipher text into a plaintext without knowing the key or algorithm [1].

However the cryptanalysis of stream ciphers through soft computing techniques as Particle Swarm Optimization (PSOs), Genetic Algorithms (GAs) is still an emerging issue. GA is based on the evolutionary ideas of Natural selection and genetics [2]. GA is a good candidate for the optimal solutions to optimization and search problems. The algorithm has been successfully applied to Vertex-Cover problem [3], Maximum-Clique problem [4], Regression testing [5], N-puzzle problem [6], Traveling Salesman Problem [7].

PSO was originally developed by a social-psychologist J. Kennedy and an electrical engineer R.Eberhart in 1995 and emerged from earlier experiments with algorithms that modeled the "flocking behavior" seen in many species of birds. Where birds are attracted to a roosting area in simulations they would begin by flying around with no particular destination and in spontaneously formed flocks until one of the birds flew over the roosting area [8]. PSO has been an increasingly hot topic in the area of computational intelligence. It is yet another optimization algorithm that falls under the soft computing umbrella that covers genetic and evolutionary computing algorithms as well [9]. There are many researches has been written on using soft computing techniques to cryptanalysis different types of encryption systems some of these: A.J.Clark, in his Thesis uses various optimization heuristics in the fields of automated cryptanalysis and automated cryptographic function generation[10], M.F. Uddin in his paper focused on using of PSO in cryptanalysis of simple substitution ciphers using ciphertext only attack[11], R.R.Yako In her research, an optimization approach such as GAs is considered to improve the cryptanalysis problem[12], S. M. Hameed in her work used PSO to cryptanalysis transposition cipher, PSO used ciphertext only attack to recover the secret [13], H.A.M Al_Sharifi, in his research focused on using of PSO algorithm to cryptanalysis stream cipher using plaintext attack choosing one Linear Feedback Shift Register (LFSR) [14], B.N. Ferriman, in his Thesis focused on the RC4 algorithm and present a new approach for cryptanalysis of the cipher by attacking RC4s state register[15], Ali A. Abd in his research is considered a new approach to cryptanalysis stream cipher systems based on GA [16]. The present work explores the related work done and applicability of GAs and PSOs in a field of cryptanalysis.

In this paper the proposed technique employed for the purpose of Cryptanalysis.

To apply ciphertext only attack to cryptanalysis the Geffe and Bruer systems as a case study of stream cipher cryptosystem. This technique exploits hybridization between PSO and SA.

The rest of this paper has been organized as follows: Section 2 presents a brief overview of soft computing techniques. Section 3 presents designing cryptanalysis systems for stream cipher. Section 4 presents a comparison result of cryptanalysis system between PSO and IPSO. The last section explains the conclusion.

2. Soft Computing Techniques

2.1 Genetic Algorithm

GAs is the search heuristic that mimics the process of natural evolution [2]. It is based on the Darwin's principle of Natural selection. According to this theory the chromosomes with the best fitness function should survive and create new offspring (survival of the fittest). GAs gives useful solution to optimization and search problem. It is a rapidly growing area of Artificial Intelligence. The GAs starts with the population which is nothing but chromosomes which can be decimal or binary or even hexadecimal. The GAs operator is applied to population in order to optimize the results [17]. The new population is formed from the old population with better fitness value. The population can be crafted using the operators: Population size, Fitness Function, Selection, Crossover, Mutation. [18, 19, 20].

2.2 Particle Swarm Optimization

To build stream cipher algorithms, there are two approach. The first one is building stream cipher visually through provide the required components and provide the potentiality to link these components to generate sequence of bits.

The second is building stream cipher algorithm through C# programming language. The proposed package provides the two approaches. The following sections will discuss how provide these two approaches for constructing stream cipher algorithm in the proposed package.

Swarm Intelligent is a kind of Artificial Intelligence based on the behavior of animals living in groups and having some ability to interact with another and with the environment in which they are inserted. Every particle in the swarm acts in a distributed manner using the intelligence of its own and the group intelligence. Every particle has two features: a position and a velocity. The particles exchange the information to correct their positions and velocities by using the received information [21].

2.2.1 Basic Elements of the PSO Technique [22, 23].

The basic elements of PSO technique are briefly stated and defined as Follows:

- 1- **Particle, X^i** : It is a candidate solution represented by an m-dimensional vector, where m is the number of optimized parameters.
- 2- **Population, $\text{pop}(t)$** : It is a set of n particles at time i, i.e. $\text{pop}(i) = [X^i_1, \dots, X^i_n]^T$. The number of particles in population would be between 20 to 30.
- 3- **Swarm**: It is an unsystematic moving particles population, which Band together and at the same time every particle moves in a Unorganized direction.
- 4- **Particle velocity, V_i** : It is the speed of the moving particles which can be characterized by k-dimensional vector.
- 5- **Inertia weight, w_i** : It is a control factor used to control the effect of the preceding velocities on the present velocity.
- 6- **Individual best, p_i** : it is the composition of the particle fitness value at the present position to the best fitness value it has ever reached.
- 7- **Global best, p_g** : It is the best location obtained in all individual locations.
- 8- **Stopping criteria**: it is the terms which finish search process.

2.2.2 PSO Methods

There are several methods of PSO depending on the shape of Updated velocity equation of the particle those are:

Original PSO: Basic algorithm introduced to calculate the velocity and position of each particle and it is used to find the Optimal solution. Velocity of individual particles updated as follows:

$$V_{j+1}^i = V_j^i + c_1 r_1 (P_j^i - X_j^i) + c_2 r_2 (P_g^i - X_j^i) \quad j=1, \dots, n \dots (1)$$

with the position calculated as follows:

$$X_{j+1}^i = X_j^i + V_{j+1}^i \quad j=1, \dots, n \dots (2)$$

Where:

X_j^i : Particle position

V_j^i : Particle velocity

P_j^i : Best position found by jth particle

P_j^g : Best position found by swarm

c_1 and c_2 : are the cognitive (individual) and social, (group) learning, rates, respectively, The values of c_1 and c_2 are usually assumed to be 2.

r_1 and r_2 : are uniformly distributed random numbers in the range 0 and 1.

Inertia Weighted PSO: The inertia weighted PSO is added to decrease the velocity. Its value varies from 0.9 to 0.4. The value of the jth particle velocity can be formulated as:

$$V_{j+1}^i = w_i v_j^i + c_1 r_1 (p_j^i - x_j^i) + c_2 r_2 (p_j^g - x_j^i) \quad J=1, \dots, n, \dots (3)$$

Then the value of the inertia weight can be calculated:

$$w_i = W_{\max} - (W_{\max} - W_{\min} / i_{\max}) * I, \dots (4)$$

where:

$W_{\max}$ is the initial value of the weight.

$W_{\min}$: is the final value of the inertia weight.

$i_{\max}$: is the maximum number of iterations.

In this work, Inertia Weighted PSO type is used.

2.3 Simulated Annealing

Simulated annealing is based on the concept of annealing. In physics, the term annealing describes the process of slowly cooling a heated metal in order to attain a "minimum energy state". A heated metal is said to be in a state of "high energy". The technique merges hill-climbing with the probabilistic acceptance of non-improving moves. The search starts at some initial state $S = S_0$. There is a control parameter T known as the temperature. This starts 'high' at T_0 and is gradually lowered. At each temperature, a number of moves to new states are attempted. A candidate state is randomly selected from the neighborhood of the current state. The change in value of the cost function is calculated. If it improves the value of cost function, then a move to that state is taken; if not, then it is taken with some probability. Probabilistic acceptance is determined by generating a random value in the range (0, 1) and performing the indicated comparison. The algorithm is discussed below [24].

2.3.1 Basic Simulated Annealing

According to statistical thermodynamics, P_α , the probability of a physical system being in state α with energy E_α at temperature T satisfies the Boltzmann distribution.

where k_B is the Boltzmann's constant, T is the absolute temperature, and Z is the partition function, defined by:

$$P_\alpha = 1/Z e^{(-E_\alpha / k_B) T}, \dots (5)$$

$$Z = \sum_{\beta} e^{-(E_\beta / k_B) T}, \dots (6)$$

The summation being taken over all states β with energy E_β at temperature T . At high T , the Boltzmann distribution exhibits uniform preference for all the states, regardless of the energy. When T approaches zero, only the states with minimum energy have nonzero probability of occurrence. In SA, the constant k_B is omitted. At high T , the system ignores small changes in the energy and approaches thermal equilibrium rapidly, that is, it performs a coarse search of the space of global states and finds a good minimum. As T is lowered, the system responds to small changes in the energy, and performs a fine search in the neighborhood of the already determined minimum and finds a better minimum. At $T = 0$, any change in the system states does not lead to an increase in the energy, and thus, the system must reach equilibrium if $T = 0$. When performing SA, theoretically a global minimum is guaranteed to be reached with high probability. The artificial

thermal noise is gradually decreased in time. T is a control parameter called computational temperature, which controls the magnitude of the perturbations of the energy function $E(\mathbf{x})$. The probability of a state change is determined by the Boltzmann distribution of the energy difference of the two states:

$$P = e^{-(\Delta E / T)} \dots (7)$$

The probability of uphill moves in the energy function ($\Delta E > 0$) is large at high T , and is low at low T . SA allows uphill moves in a controlled fashion: It attempts to improve on greedy local search by occasionally taking a risk and accepting a worse solution. The algorithm of simulated annealing as following: [24].

1. Initialize the system configuration.
Randomize $\mathbf{x}(0)$.
2. Initialize T with a large value.
3. **Repeat:**
 - a. **Repeat:**
 - i. Apply random perturbations to the state
 $\mathbf{x} = \mathbf{x} + \Delta \mathbf{x}$.
 - ii. Evaluate $\Delta E(\mathbf{x}) = E(\mathbf{x} + \Delta \mathbf{x}) - E(\mathbf{x})$:
if $\Delta E(\mathbf{x}) < 0$, keep the new state;
otherwise, accept the new state with probability $P = e^{-\Delta E / T}$.
until the number of accepted transitions is below a threshold level.
 - b. Set $T = T - \Delta T$.
until T is small enough.

3- Designing Cryptanalysis Systems for Stream Cipher

In this work the soft computing techniques used as PSO and proposed technique IPSO which could be implemented and applied easily to solve various optimization problems. These techniques employed for the purpose of Cryptanalysis. We suggest main steps to designing cryptanalysis systems for stream cipher, we select the Geffe generator to be attacked. These steps of the analysis and procedure can be summarized as follows:

- Step1: select ciphertext (C_i).
- Step2: generate the key stream (K_i) from Geffe generator system.
- Step3: calculate the plaintext(P_i) as follows:
 $C_i \text{ XOR } K_i = P_i$.
- Step4: design fitness function depending on the probability of numbers of 0's in P_i
- Step5: apply soft computing techniques.
- Step6: repeat step2 until stopping criteria satisfied.

3.1 Fitness Function Calculation

The main goal of cryptanalysis is to get the key in order to obtain the plaintext. Cryptanalysis stream cipher should get the correct key to decrypt the ciphertext. Using soft computing techniques to cryptanalysis stream cipher needs fitness to determine the best new generation. In this work, new fitness function based on xoring between C_n and K_n . Cryptanalysis of stream cipher based on statistical model is used to find the Linear Feedback Shift Register (LFSRi) part of the key, i.e., the initial of the LFSRi, $i \in \{1, \dots, s\}$. Where:

C_n : cipher text digits.

K_n : the output key of Geffe generator

N : ciphertext length

Let n_0 be the number of 0's in P_i , then:

$$\text{Fitness} = P(0) = n_0 / N, \dots \dots \dots (8)$$

Here, the best fitness ≥ 0.60 , this rate considered the threshold in our work, it change according to different plaintext size.

We will attack the Geffe generator, nonlinear combining function which it consist of 3 LFSR in different Length: 3, 5, 7.

The algebraic normal form is:

$$f(x_1, x_2, x_3) = x_1x_2 \text{ XOR } x_2x_3 \text{ XOR } x_3, \dots\dots\dots(9)$$

Here, the number of ciphertext symbols is determined to perform a ciphertext-only attack on the Geffe Cipher using the correlation attack. Our conclusion from the analysis is that the pseudonoise generator's output sequence and the sequences generated by the linear feedback shift registers (LFSR) should be uncorrelated. This leads to constraints for the nonlinear combining function to be used.

3.2 Using PSO algorithm to cryptanalysis stream Cipher

In Evaluation For the initial population, the cryptanalysis process begins with randomly generated numbers between $\{-1, 1\}$ as the key size for n particles. The sequence of these numbers represents the candidate keys (particles). Randomly generates Velocity for each particle which it's bounded to some minimum and maximum values $[V_{max}, V_{min}]$ where $V_{min} = -V_{max}$ and it uses to reinforces the local search reconnoitering of the problem space. Each particle represents the candidate key and use to decrypt the ciphertext and then calculate the fitness value to determine the best particle (key). For the evaluation process, the fitness value for each particle (candidate key) must be calculated for each generation. Table 2 shows the most parameters of PSO that preferred to be used to decrypt stream cipher (see Table 2).

3.3 Using IPSO algorithm to cryptanalysis stream Cipher

In IPSO the proposed cryptanalysis system used to apply cipher text only attack to cryptanalysis the Geffe system using soft computing techniques exploded a hybridization between PSO and Simulated Annealing (SA).(see Fig.1) shows the Flow Chart of proposed system. In IPSO we will use the same parameters of classical PSO as mentioned in Table 2. The following Table 3 shows the parameters used in IPSO.(see Table 3).

4- Comparison Results Of Cryptanalysis System Between PSO AND IPSO.

4.1 Case Study 1: Attacking Geffe generator system

The following Tables 3,4, and 5 shows the results of applying proposed cryptanalysis system PSO and IPSO For Popsiz(20,100,200) and Maxiter(100,300) For TxtLen=100,40,30 characters.

The following notations are used:

Popsiz = Population size.

MaxIter= Maximum Iteration.

BF=Best Fitness.

T/sec=Time/second.

T.T/sec=Total Time/second.

Iter_Num= Iteration_Number.

Table 4 shows the results of applying PSO and IPSO for Popsiz(20,100,200) and Maxiter (100,300) For TxtLen=40 characters. (see Table 4).

Table 5 shows the results of GA, PSO and IPSO For Popsiz(20,100,200) and Maxiter(100,300) For TxtLen=30 characters (see Table 5).

4.2 Case Study 2: Attacking Bruer generator system

The following Tables 6,7, and 8 shows the results of applying proposed cryptanalysis system PSO and IPSO For Popsiz(20,100,200) and Maxiter(100,300) For TxtLen=100,40,30 characters.

Table 6 shows the results of applying PSO and IPSO for Popsiz(20,100,200) and Maxiter (100,300) For TxtLen=100 characters.(see Table 6).

Table 7 shows the results of applying PSO and IPSO for Popsiz (20,100,200) and Maxiter (100,300) For TxtLen=40 characters.(see Table 7).

Table 8 shows the results of applying PSO and IPSO for Popsiz (20,100,200) and Maxiter (100,300) For TxtLen=30 characters.(see Table 8).

Table (1) PSO parameters to attack stream cipher

Parameters	Symbol	Value
Number of particles in the swarm	Popsiz	[20-200]
Number of Key	KeyLen	[15]
Length of text	TxtLen	[10-100]
The maximum number of Iteration	MaxIter	[100-300]
The maximum of velocity	V_{max}	4
The minimum of velocity	V_{min}	$-V_{max}$
Inertia Weight	W	[0.4- 0.9]
Acceleration parameter	C_1, C_2	[0.5-2]
Random number between [0,1]	r_1, r_2	[0-1]

Table (2) IPSO parameters to attack stream cipher.

Parameters	Symbol	Value
Number of particles in the swarm	Popsiz	[20-200]
Number of Key	KeyLen	[15]
Length of text	TxtLen	[10-100]
The maximum number of Iteration	MaxIter	[100-300]
The maximum of velocity	V_{max}	4
The minimum of velocity	V_{min}	$-V_{max}$
Inertia Weight	W	[0.4- 0.9]
Acceleration parameter	C_1, C_2	[0.5-2]
Random number between [0,1]	r_1, r_2	[0-1]
Initial temperature	T	0.1

Table (3) Results of applying PSO and IPSO for Popsiz (20,100,200) and MaxIter(100,300) for TxtLen=100.

Popsiz	MaxIter	PSO				IPSO			
		BF	T/ sec	T.T/ sec	Iter_ Num	BF	T/ sec	T.T/ sec	Iter_ Num
20	100	0.6188	0.23	16.31	1	0.5657	0.35	14.70	1
	300	0.5520	0.58	47.20	1	0.5682	0.32	43.39	1
100	100	0.5656	1.21	82.32	2	0.6301	1.43	72.55	1
	300	0.5556	0.82	240.98	1	0.5669	1.45	215.47	1
200	100	0.5850	3.29	160.47	2	0.5769	2.89	144.13	1
	300	0.5760	1.58	460.32	1	0.5807	2.80	423.01	1

Table (4) results of applying PSO and IPSO for Popsiz (20,100,200) and MaxIter(100) for TxtLen=40

Popsiz	MaxIter	PSO				IPSO			
		BF	T/ sec	T.T/ sec	Iter_ Num	BF	T/ sec	T.T/ sec	Iter_ Num
20	100	0.5656	0.17	6.97	2	0.5563	0.14	6.69	1
	300	0.5875	0.18	22.41	2	0.5656	0.22	19.96	1
100	100	0.6188	0.70	32.75	2	0.5750	0.65	32.56	1
	300	0.6262	0.41	97.51	1	0.5500	0.55	98.70	1
200	100	0.6125	0.66	64.53	2	0.6188	0.22	64.46	1
	300	0.5906	1.60	463.10	1	0.5800	0.56	192.10	1

Table (5) results of applying PSO and IPSO for Popsiz (20,100,200) and MaxIter (100,300)for TxtLen=30.

Popsiz	MaxIter	PSO				IPSO			
		BF	T/ sec	T.T/ sec	Iter_ Num	BF	T/ sec	T.T/ sec	Iter_ Num
20	100	0.5708	0.06	4.20	2	0.5877	0.04	4.10	1
	300	0.5833	0.05	14.70	2	0.5669	0.10	12.22	1
100	100	0.6042	0.45	20.72	2	0.6000	0.30	22.39	2
	300	0.6083	0.10	66.30	1	0.6042	0.45	65.33	1
200	100	0.6000	0.46	43.10	1	0.6042	0.91	45.77	1
	300	0.6125	1.80	140.77	2	0.6083	1.75	138.3	2

Table (6) Results of applying PSO and IPSO for Popsiz (20,100,200) and MaxIter (100,300) for TxtLen=100.

Popsiz	MaxIter	PSO				IPSO			
		BF	T/ sec	T.T/ sec	Iter_ Num	BF	T/ sec	T.T/ sec	Iter_ Num
20	100	0.5821	0.22	20.11	1	0.5650	0.40	19.17	1
	300	0.5750	0.27	62.80	1	0.5717	0.40	60.77	2
100	100	0.5969	1.02	102.20	1	0.6000	2.11	100.1	1
	300	0.6125	2.02	317.9	2	0.6301	1.05	315.5	1
200	100	0.6301	4.01	118.5	2	0.5923	2.17	115.3	1
	300	0.6260	2.12	598.5	1	0.6250	1.99	605.3	1

Table (7) Results of applying PSO and IPSO for Popsiz (20,100,200) and MaxIter (100,300) for TxtLen=40.

Popsiz	MaxIter	PSO				IPSO			
		BF	T/ sec	T.T/ sec	Iter_ Num	BF	T/ sec	T.T/ sec	Iter_ Num
20	100	0.5821	0.22	20.11	1	0.5650	0.40	19.17	1
	300	0.5750	0.27	62.80	1	0.5717	0.40	60.77	2
100	100	0.5969	1.02	102.20	1	0.6188	2.11	100.1	1
	300	0.6188	2.02	317.9	2	0.6188	1.05	315.5	1
200	100	0.6301	4.01	118.5	2	0.5923	2.17	115.3	1
	300	0.6260	2.12	598.5	1	0.6250	1.99	605.3	1

Table (8) Results of applying PSO and IPSO for Popsiz (20,100,200) and MaxIter (100,300) for TxtLen=30.

Popsiz	MaxIter	PSO				IPSO			
		BF	T/ sec	T.T/ sec	Iter_ Num	BF	T/ sec	T.T/ sec	Iter_ Num
20	100	0.6125	0.07	5.30	1	0.5777	0.06	4.88	1
	300	0.5677	0.08	17.33	1	0.6042	0.05	16.09	1
100	100	0.6083	1.09	27.77	2	0.6000	0.56	25.66	1
	300	0.6125	1.75	87.56	2	0.6083	0.75	86.50	1
200	100	0.6000	0.87	57.86	1	0.6178	0.77	55.33	1
	300	0.6125	0.97	195.6	1	0.6000	0.87	192.4	1

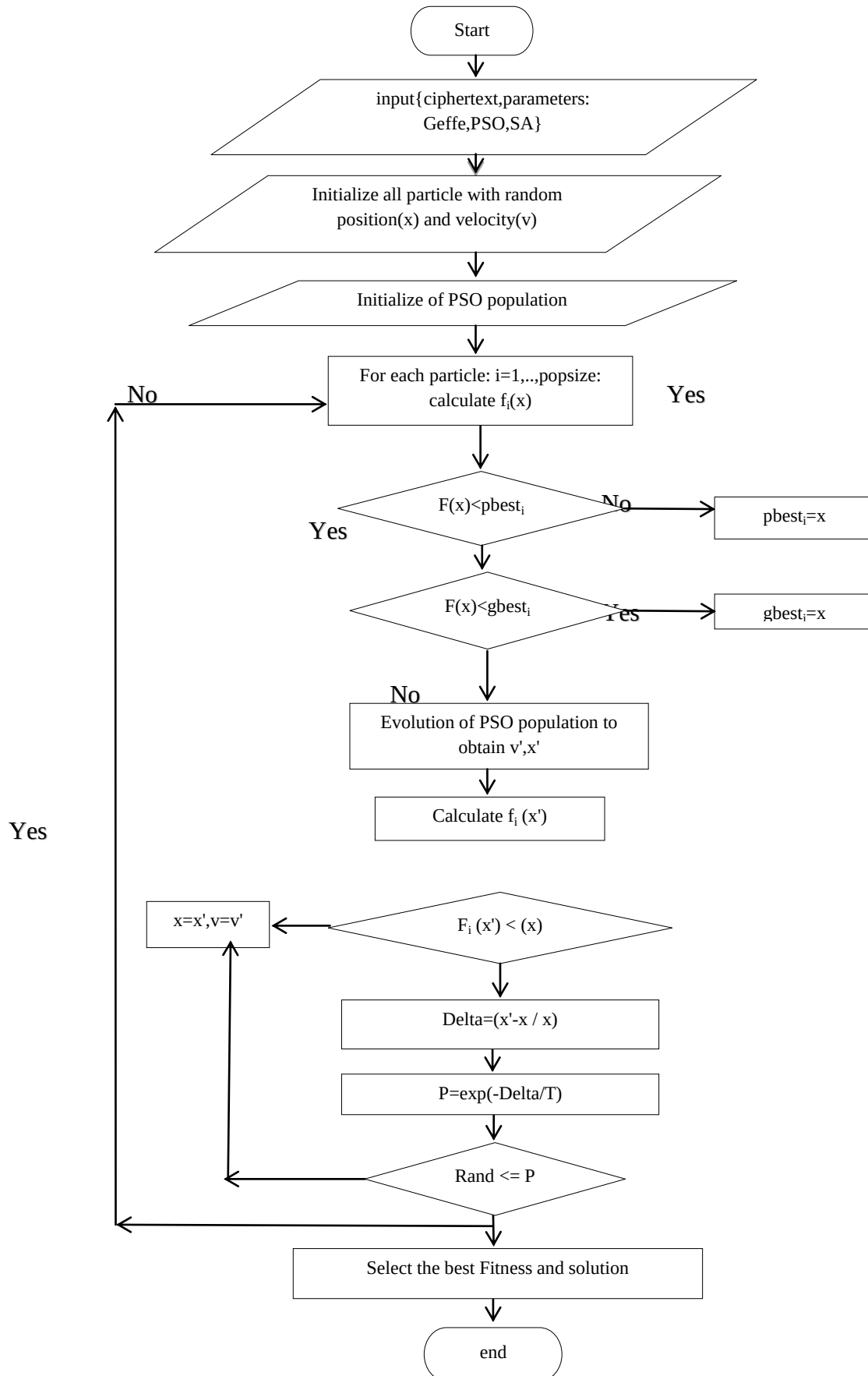


Fig.(1) Flowchart of applying IPSO to attack stream cipher.

5. Conclusions

1. Our original goal was clearly met. The Two soft computing techniques (PSO and IPSO) proved highly successful in cryptanalysis of a stream cipher systems and determining the initial setting of the attacked generators. (IPSO) to find the optimal solution for the attacked generator.
2. This work suggests a new approach which is called Improved Particle Swarm Optimization.
3. The cryptanalysis system using PSO and IPSO can find the optimal solution for text till lengths with 10 characters.
4. As shown in Tables 3, 4, 5, 6, 7 and 8 the results of applying PSO and IPSO to cryptanalysis stream cipher, we notice that 3 iterations are enough to find the best solution for both Geffe and Bruer systems for both PSO and IPSO.
5. The performance of IPSO is better than the performance of the PSO in cryptanalysis stream cipher in the term of time as shown in Tables 3, 4, 5, 6, 7 and 8.
6. As shown in Table 3 we conclude that the best results of PSO and IPSO in TxtLen=100 characters are obtained in Popsiz=100 and MaxIter=100.
7. As shown in Table 4 the best results of PSO and IPSO in TxtLen=40 characters are obtained in Popsiz=200 and MaxIter=100.
8. From a sequent 6 and 7, we conclude that Popsiz=200 and MaxIter=100 is enough to find the optimal key for the two techniques.
9. Soft computing techniques can be used as a powerful tool in generating pseudorandom sequences with good statistical properties and a high linear complexity and overcome all problems.

References

- [1] Schneier, B.1996, Applied Cryptography, Second Edition: **"Protocols, Algorithms and Source Code in C"**.
- [2] Holland, J.H.1992, Adaptation in Natural and Artificial Systems.
- [3] M.Milanovic, **"Solving the generalised vertex cover problem by Genetic Algorithm"**, Computing and Informatics,2010.
- [4] Bazgan, C.,Luchian,H.1995. **"A genetic Algorithm for maximal Clique Problem"**. In proceeding of the International Conference in Ales, France.
- [5] H. Bhasin, Manoj, **"Regression testing using Coupling and Genetic Algorithms"**, International Journal of Computer Science and Information Technologies, 2012.
- [6] H. Bhasin, N. Singla, **"Genetic based algorithm for N-Puzzle problem"**, International Journal of Computer Application,2012.
- [7] Y. Liao et al, **"Evolutionary algorithm to Traveling Salesman Problems"**, Computer & Mathematics with Applications, 2012.
- [8] Papoulis, A. **"Probability Random Variables, and Stochastic Process"**, McGraw-Hill College, 2001.
- [9] Parsopoulos K. E. and Vrahatis M. N., **"Recent Approaches to Global optimization Problems through Particle Swarm Optimization"**, Kluwer Academic Publishers, Netherlands, Natural Computing 1, pp. 235– 306, 2002.
- [10] A. J. Clark, **"Optimisation Heuristics for Cryptology"**, Information Security Research Centre Faculty of Information Technology Queensland University of Technology,1998.
- [11] M. F Uddin and Amr M. Youssef, **"Cryptanalysis of Simple Substitution Ciphers Using Particle Swarm Optimization"**. IEEE, Congress on Evolutionary Computation, Canada, 2006.
- [12] Rajaa R. Yako, **"Decrypting A Class Of Stream Cipher Using Ciphertext Only, Comparative Study"**, Master Thesis, Higher Academy for Scientific and Humanistic Studies, Department of Computer Science,2007.
- [13] Sarab M. Hameed and Dalal N. Hmood, **"particles swarm optimization for the cryptanalysis of transposition cipher "**. Journalof Al-Nahrain University, Vol.13 (4), pp.211-215, 2010.
- [14] Hussein Ali Mohammed Al_Sharifi, **"Cryptanalysis of Stream Cipher System Using Particle Swarm Optimization Algorithm "**. Journal of Kerbala University, Vol. 8 No.4 Scientific, 2010.

- [15] Benjamin Nicholas Ferriman, "**Cryptanalysis of the RC4 Stream Cipher using Evolutionary Computation Methods**", Master Thesis, University of Guelph, Guelph, Canada, 2013.
- [16] Ali A. Abd, Hameed A. Younis, and Wasan S. Awad, "**Attacking of stream Cipher Systems Using a Genetic Algorithm**". Journal of University of Thi-Qar, ISSN: 66291818, Vol. 8, Issue. 3, 2013.
- [17] Goldberg, D.E.1989. Genetic Algorithm in search, optimization and machine learning.
- [18] Goldberg, D.E et al.2000. Bayesian Optimization Algorithm, population sizing and time to convergence, University of Illinois, USA.
- [19] Melanie, M.1996. An introduction to a Genetic Algorithm: MIT press paperback edition.
- [20] Bhasin, H.2015. Algorithms: Design and Analysis.
- [21] Singiresu S. Rao "**Engineering Optimization Theory and Practice**" Book, by John Wiley & Sons, Inc.2009.
- [22] James Kennedy and Russell Eberhart "**Particle Swarm Optimization**", Book, IEEE 1995.
- [23] James Kennedy "**The Particle Swarm: Social Adaptation of Knowledge**" IEEE, 1997.
- [24] S. C. Kirkpatrick, J. D. Gelatt, and M. P. Vecchi, "**Optimization by simulated annealing**", Science, vol. 220, no. 4598, p. 671-680, 1983.

A New Image Cipher Method Based on some Statistical Properties

Dr. Anwar Abbas Hattab Maha Ali Hussian

Department of Computer Science, College of Education, Mustansiriyah University

anwarabbas76@gmail.com ali_ma2011@yahoo.com

Abstract:

Mathematical image cipher is proposed as a new method to cipher image for wireless network. This method contains three steps: first step is called variance permutation which uses variance value for each column in block which is used as a key to shift each column. Data in this block is dealt as a pixel. Second step is called key mixing, key must be generated based on Linear Feedback Shift Register (LFSR) and first pixel in first block is used as a seed to LFSR to produce random keys for whole image. Third step called mean permutation which use mean for each row in block as a key to shift each row in block. Data in this block is dealt as bit. Experiments results show strong and efficient of proposed method, tests contain histogram, correlation analysis, differential attack analysis, entropy and Peak Signal Noise Ratio (PSNR)

Keyword: Image cipher, Permutation operation, Key mixing, LFSR.

طريقة تشفير صور جديدة اعتمادا على بعض الصفات الاحصائية

المستخلص:

تشفير الصور الرياضية تقترح كطريقه جديدة لتشفير الصور للشبكات اللاسلكية. يحتوي هذا الأسلوب على ثلاث خطوات: الخطوة الأولى تسمى التباين التبادلي الذي يستخدم قيمة التباين لكل عمود في كتلة والذي يستخدم كمفتاح لتحويل كل عمود. يتم التعامل مع البيانات في هذه المجموعة كبكسل. ويسمى الخطوة الثانية خلط المفتاح، يجب أن يتم توليد المفتاح على أساس مسجل الازاحة الخطية ذات التغذية المرتدة (LFSR) اول بكسل في الكتلة الأولى تستخدم كبذرة للمسجل LFSR لإنتاج مفاتيح عشوائية للصورة كاملة. الخطوة الثالثة تسمى التبادل المتوسط الذي يستخدم متوسط لكل صف في الكتلة كمفتاح لتحويل كل صف في الكتلة. يتم التعامل مع البيانات في هذه المجموعة بصيغه البت (bit). نتائج التجارب تظهر قوة وفعالية الطريقة المقترحة، والاختبارات تحتوي على الرسم البياني، وتحليل الارتباط وتحليل التفاضلية الهجوم، الإنتروپيا ونسبة الذروة الإشارة إلى الضوضاء. الكلمات المفتاحية: تشفير الصور، عملية التبديل، خلط المفتاح، مسجل الازاحة الخطية ذات التغذية المرتدة (LFSR).

1. Introduction

Security of information like image is an important operation in wireless communication. Security of Image can be achieved by using watermarking methods or by using encryption to the images. Image watermarking techniques are used for user authentication, copyright protection, etc. Image encryption methods change original image to encrypted image to keep the image secret between employers [1]. It is most important that without decryption key no one can arrive to the plain image [2] while key management is affronting in wireless networks operating without fixed infrastructure [3]. Image communication over a mobile network requires authoritative, quick and robust secure system. The needs to complete the security needs of digital images have lead to the promotion of effective image encryption algorithms. [4, 5] Image encryption has implementations in online telecommunication, multimedia methods, medical area, military telecommunication; etc. [2]. However, the traditional cipher methods are used for text encryption which can also be used for image encryption, but it is not appropriate for two reasons. The first is that the images are larger in size than that of text. Therefore, the traditional cipher system takes more time for encrypting image data. The second problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data [6].

In this paper, a new method for image cipher is proposed in which achieves diffusion and confusion for image by permutation and key mixing operation. It is simple, rapid and less complication. Han Shuihua et al. [7] written an asymmetric image encryption method based on matrix change which is readily executed and highly active to quickly encrypt and decrypt images. Bibhudendra et al. [8] displayed an Advanced Hill encryption technique, which applies an

involuntary matrix, to encrypt images. The complication could be decreased by avoiding the process of finding reverse of the matrix during decryption. The intelligible data present in an image is due to the connections the bits, pixels and blocks in a given setting. This perceivable information could be decreased by decreasing the connection between the bits, pixels and blocks by using certain combinational permutation techniques. The permutation of pixels and blocks is good at creating higher -level security compared to bit permutation [9].

The rest of this paper is arranged as follows: Section 2 explains proposed method. Section 3 describes variance permutation, key mixing operation and key generation which are explained in section 4. Mean permutation method is explained in section 5. Performance analysis is described in section 6. Conclusion is presented in Section 7.

- **Background:**

- Mean statistic is some individual value calculated from a sample ($X_1; \dots; X_n$) (random variables), it can described as [10]:

$$E(x) = \frac{1}{n} \sum_{i=1}^n x_i \text{----- (1)}$$

- Variance statistic is described as:

$$D(x) = \frac{1}{n} \sum_{i=1}^n (x_i - E(x))^2 \text{----- (2)}$$

2. Proposed Method

New method for encryption image is proposed for wireless network, it is called mathematical image cipher because, it contains three operations or steps: first operation, variance operation based on variance value for each column used as a key to shift operation. Second operation is need generated key based on LFSR and first pixel in first block, it doesn't require any key from user but each key is deduced from mathematic prosperities for image. Key mixing uses xor operation between produced key and data block resulted from step 1, third operation is called mean permutation, which it used mean for each row as a key to shift operation for each row, proposed method makes confusion and diffusion for image in simple and fast manner. Fig (1) shows flowchart of proposed mathematical image cipher.

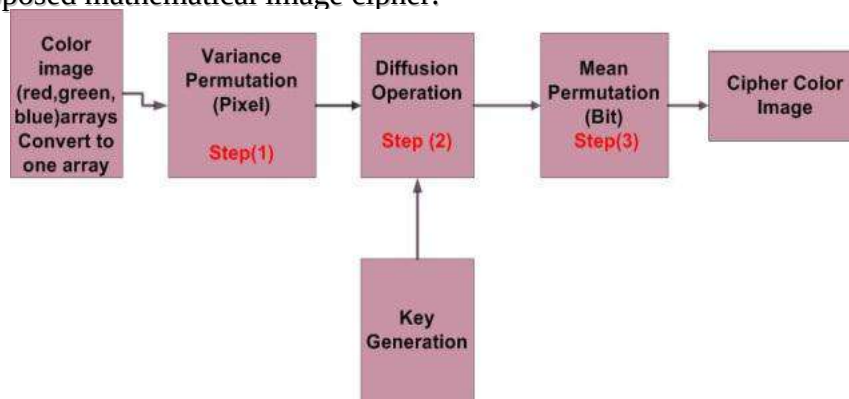


Fig. (1): Flowchart of proposed method

3. Step 1: Variance Permutation Operation

Data block in variance permutation is store in array H has size (n, m), where n and m any integer number. Variance operation performed for each column in array H. each column has specific variance value may be different from other; it is (variance value) used as a key equal to number of shift operation for each column. Variance value contents integer part and fraction part. In this step, just first number in integer part will be taken. Variance permutation flowchart is shown in Fig (2) and Algorithm (1) explains variance permutation steps.

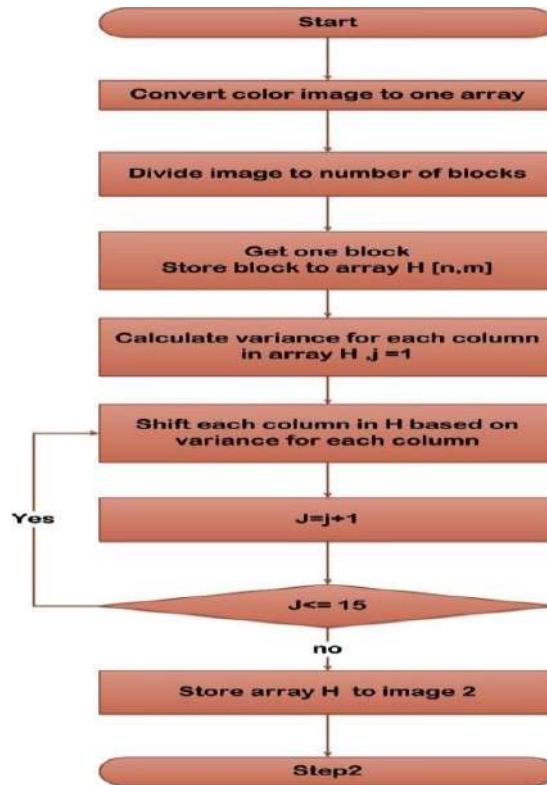


Fig. (2): Variance Permutation Flowchart

Algorithm(1):Variance Permutation Operation:

Input: block (img), iterations (itr).

Output: block. // after permutation.

Begin

1. Store block to array H (n, m).
2. Calculate variance operation for each column in the array H.
3. Get integer part from variance values without fraction part and get first number, store in array V.
4. For I=1 to itr
Shift each column, shift by using specific variance V of each column as a key.
I=I+1.
5. EndFor.
6. Send H.

END

4. Step2: Key Mixing

Input and output task are 512 bits. The data inputs are store as one-dimensional array P, described in figure (3), array (P) is X-OR with secret key. The input data and output data have the same size without any an iteration, key generation process which will be explained later and algorithm (2) using to describe XOR –operation.

a. Key Generation Method:

In mathematical image cipher, new generated key is used based on first pixel in first block and three Linear Feedback Shift registers (LFSR) are used, these explained in figure (4). LFSR1 and LFSR3 content 31 bit and have polynomial (x^3+x^{31}) , LFSR2 contains 19 bits and have polynomial $(x^1+x^2+x^5+x^{19})$, three LFSR are used to generate key which has length equal to size of image (any image used with this method). First pixel in color array has three values of red array, green array and blue array, value1 (red array) used as a seed to LFSR1. Value2 (green array) is used as a seed to LFSR2. Value3 (blue array) used as a seed to LFSR3. Plain first pixel in first block must be store in first cipher block to use in decryption operation to generate the same key again.

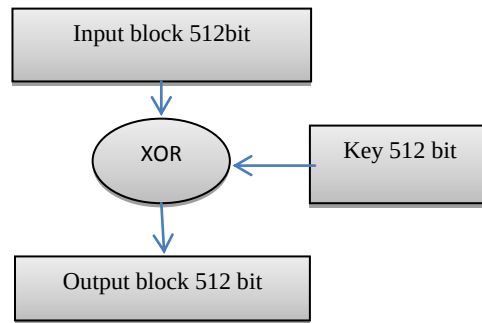


Fig. (3): XOR operation



Fig. (4): LFSR

Algorithm (2): Key Generation

Input: 3-LFSR, first pixel in image.

Output: key.

Begin:

1. Pixel 1 (red value) used as a seed to LFSR1, green value used as a seed to LFSR2, blue value used as a seed to LFSR3. I=0.
2. While (I ~ =512)
3. Perform and operation between bit (31) in LFSR1 and bit (19) in LFSR2.
4. Perform and operation between bit (31) in LFSR3 and result from step (4).
5. Shift LFSR1 bits (1-13) and shift LFSR2 bits (1-19) and LFSR3 (1-31)
6. Results from step (6) store to LFSR1 in bit (1), result (2) store to LFSR2 bit (1) and result 3 stores to LFSR3.
7. Assign result from step5 to Key array.
8. I=I+1.
9. End while

End.

Algorithm (3) XOR operation

Input: Data block, key.

Output: Data block.

Begin

1. Convert each block to vector one dimension called x.
2. Use the algorithm (2) to generate Key.
7. Perform XOR operation between Key and vector(x).

End.

5. Step 3: Mean Permutation Operation

Data block in mean permutation is stored in array H2 has size (n2, m2), where n2 and m2 any integer number. Mean operation performed for each row in array H2. Each row has specific variance value may be different from other; it is (mean value) used as a key equal to number of shift

operation for each row. Mean value contents integer part and fraction part. In this step, just first number will be taken. Mean permutation flowchart is shown in fig (5) and algorithm (3) explain variance permutation steps.

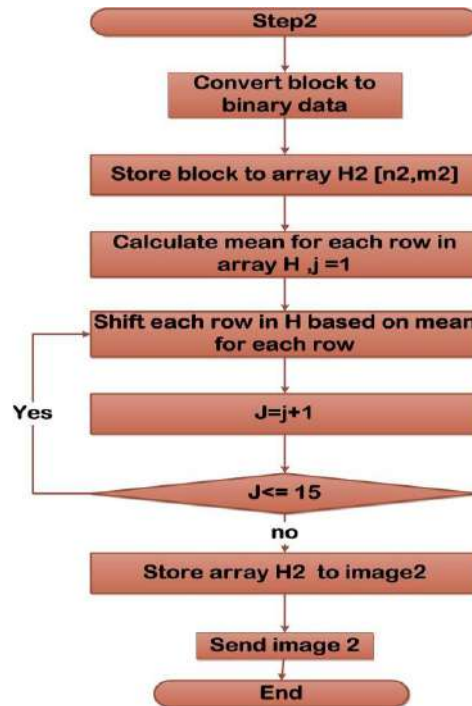


Fig. (5): Mean Permutation Flowchart

Algorithm (3): Mean Permutation Operation

Input: block (img), iterations (itr).

Output: block. // after permutation.

Begin

1. Store block to array H2 (n2, m2).
2. Calculate mean operation for each mean in the array H2.
3. Get integer part from mean values without fraction part and get first number, stored in array M.
4. For I=1 to itr
Shift each row, shift by using specific variance M of each column as the key.
I=I+1.
5. EndFor.
6. Send H.

END

6. Performance Analysis

1. Key Space Analysis:

A strong encryption algorithm should have key space large than 2^{256} to make brute –force attacked infeasible. Therefore, Mathematical Image Cipher is strong cipher method because it has key space size over than 2^{256} .

2. Statistical Analysis

Statistical tests contain many tests which can be described as following:

a. Image Histogram

Histogram explains the number of pixels in an image for any grey value in the image. Fig (6) and Fig (7) shows the histograms of original images Lena's image and Baboon image. The histogram of original images are described in a particular shape but for encrypted image has a flat histogram, hence, that mean uniform distributed for pixels. These results guarantee that the image is secured [11].

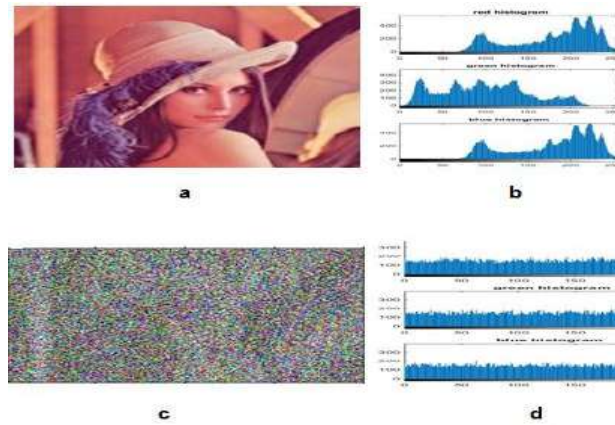


Fig.(6): a. Plain Lena image b. Plain Lena's histogram c. Lena cipher d. Lena's cipher histogram

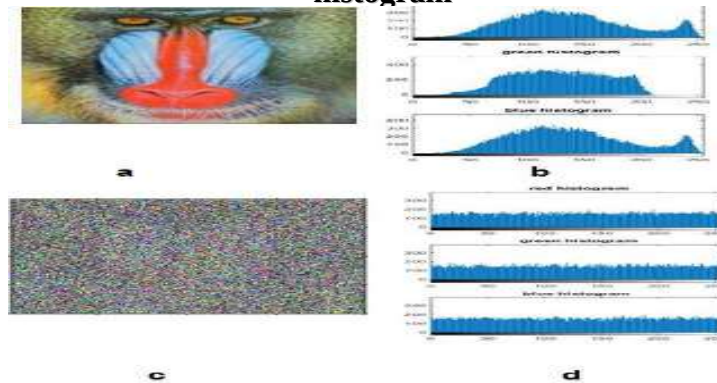


Fig. (7): a. Plain Baboon image b. Plain Baboon's histogram c. Baboon's cipher d. Baboon's cipher histogram

b. Correlation Coefficient Analysis

Correlation Coefficient Analysis is a measure of correlation between two pixels intensities of two images. The covariance (C) and the correlation coefficient H and the variables x and y are grey-scale values of pixels in equivalent pixels in different images or two adjacent pixels in the same image. The value of H is between [1, -1]. If value of H between (-1, 0) show negative relation or positive if value of H between (0, 1). Table (1) explains correlation between plain and cipher image. Table (2) explains image correlation of original and encrypted images, including horizontally, vertically, and diagonally adjacent pixels. All encrypted images are highly uncorrelated. The correlations between original images and equivalent encrypted images can be computed as following [10]:

$$C = 1/n \sum_{i=0}^n (x_i - E(x))(y_i - E(y))$$

$$H = \frac{C(x,y)}{\sqrt{D(x)D(y)}} \quad (3)$$

Where the function E(x) is expressed as:

$$E(x) = \frac{1}{n} \sum_{i=1}^n x_i, D(x) = \frac{1}{n} \sum_{i=1}^n (x_i - E(x))^2$$

Table (1) Correlation between plain and cipher

Images Names		Red Channel	Green Channel	Blue Channel
1.Baboon	R	0.0281	0.0281	0.0282
	G	0.0248	0.0433	0.0421
	B	0.0390	0.0453	0.0506
3 Lena	R	0.0749	0.0749	0.0948
	G	0.0753	0.0788	0.099
	B	0.0630	0.0569	0.0852

Table (2) Correlation coefficients between adjacent pixels for plain and cipher image

Images Names		Adjacent pixels(Correlation)			
		Image	Red Channel	Green Channel	Blue Channel
Baboon	Horizontal	P	0.9345	0.8871	0.9338
		C	8.8473e-04	-9.4454e-04	-0.0059
	Vertical	P	0.9179	0.8646	0.9258
		C	0.0048	0.0136	0.0110
	diagonal	P	0.8985	0.8256	0.8985
		C	-0.0150	0.0040	-0.0064
Lena	Horizontal	P	0.9394	0.9385	0.89751
		C	4.7235e-04	0.0064	0.0166
	Vertical	P	-0.0059	0.9705	0.9459
		C	0.0183	0.0147	0.0157
	diagonal	P	0.9132	0.9142	0.8640
		C	0.0079	0.0040	0.0054

3. Differential Analysis:

There are two scales were used for differential analysis: Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI). UACI which is the scales the average intensity of the differences between the basic and Encrypted image. Let k1, K2, whose corresponding plain images have just one pixel difference. Table (3) show NPCR and UACI for Lena and Baboon, and the NPCR of two images is defining in [12]:

$$\text{NPCR} = \left(\frac{\sum_{i,j} M(i,j)}{W \times H} \right) * 100 \text{ ----- (4)}$$

W, H represents width and high of image. And M (i, j) is defining as [12]:

$$M = \begin{cases} 1 & \text{if } k1(i,j) \neq k2(i,j) \\ 0 & \text{if } k1(i,j) = k2(i,j) \end{cases}$$

UACI define as:

$$\text{UACI} = \frac{1}{W \times H} \sum_{i,j} \left(\frac{k1(i,j) - k2(i,j)}{255} \right) * 100 \text{ --- (5)}$$

4. Image Entropy:

Image entropy is degree of uncertainties in the image. Entropy (k) can be defined as [13]:

$$\text{Entropy (k)} = \sum p(k_i) \log \frac{1}{p(k_i)} \text{----- (6)}$$

Where k_i any image, P (k_i) is the probability of k_i. Entropy (k) =8 which corresponds to an ideal value. Table (4) explains entropy of images

Table (3) NPCR, UACI for iteration=15.

Image		Itr=15
Lena	NPCR	99.432
	UACI	31.93
Baboon	NPCR	99.641
	UACI	32.91

5. Peak Signal-to-Noise Ratio (PSNR):

PSNR is used to determine encryption quality. PSNR is shown in the following Equation [14]:

$$\text{PSNR} = \left[\frac{H \times W \times 255^2}{\sum_{i=0}^{H-1} \sum_{j=0}^{W-1} (k1(i,j) - k2(i,j))^2} \right] - \text{-- (7)}$$

Here W is the width and H is the height of digital image, P (i, j) pixel estimation of the original image at matrixes k1 (i, j) and K2 (i, j) is pixel estimation of the cipher image. The great encryption algorithm must have the lower value of PSNR. Table (4) explain PSNR of images

Table (4) Entropy and PSNR for iteration=15.

Image		Itr=15
Baboon	Entropy	7.994
	PSNR	9.220
Lena	Entropy	7.992
	PSNR	8.885

7. Conclusion

In this paper new image cipher is proposed based on mathematic attributes of data, these attributes are used as seeds to generate keys for permutation or for key mixing operation, therefore, mathematic image cipher is very important for security purpose in wireless network because it simple, fast, and doesn't need to send values used as a seed to generate key because all seeds or keys are deduced from data. Experimental results show that the cipher-image histogram and entropy measured is close to the standard value. Test results explain that the proposed scheme has resistance to statistical attacks and differential analysis as NPCR and UACI. The results explain that a small change in the original image will be resulted in a small change in the ciphered image. Key space of proposed method is large enough to resist all kinds of brute force.

References

- [1] R. Kaur, E. Kanwalpreet Singh, "Comparative Analysis and Implementation of Image Encryption Algorithms", International Journal of Computer Science and Mobile Computing, Vol. 2, Issue 4, April 2013, pp. 170 – 176.
- [2] S. Dey, "SD-AI: A Cryptographic Technique to Encrypt Images", International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 26-28 June 2012, pp. 28 - 32.
- [3] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends", [http://arXiv:1505.07919v2\[cs.IT\]](http://arXiv:1505.07919v2[cs.IT]), 2016.
- [4] Borie J., Puech W., Dumas M., 2004, "Crypto-Compression System for Secure Transfer of Medical Images", 2nd International Conference on Advances in medical Signal and Information Processing (MEDSIP 2004).
- [5] J. Qayyum, M. Lal, F. Khan, and M. Imad, "SURVEY & ASSESSMENT OF WIMAX, ITS Security Threats and Their Solutions", International Journal of Video & Image Processing and Network Security, Vol. 11, No. 3, 2011, pp. 36-47.
- [6] C. Chang, M. Hwang, T. Chen, "A New Encryption Algorithm for Image Cryptosystems", The Journal of Systems and Software, Vol. 58, 2001, pp. 83 – 91.
- [7] H. Shuihua, Y. Shuangyuan, "An Asymmetric Image Encryption Based on Matrix Transformation", ECTI Transactions on Computer and Information Technology, vol. 1, no. 2, pp.126-133, 2005.
- [8] B. Acharya, S. Kumar Panigrahy, S. Kumar Patra, and G. Panda, "Image Encryption using Advanced Hill Cipher Algorithm", International Journal of Recent Trends in Engineering, vol. 1, no. 1, pp. 663-667, 2009.
- [9] A. Mitra, Y.V Subba Rao, and S.R.M Prasanna, —A "New Image Encryption Approach using Combinational Permutation Techniques", International Journal of Electrical and Computer Engineering, vol. 1, no. 2, pp.127–131, 2006.
- [10] A. Belhaj Mohamed, G. Zaibi1 and A. Kachouri, "Implementation of Rc5 and Rc6 Block Ciphers on Digital Images", 8th International Multi-Conference on Systems, Signals & Devices, 2011.
- [11] G. Hanchinamani and L. Kulakarni, "A Novel Approach for Image Encryption based on Parametric Mixing Chaotic System", International Journal of Computer Applications, Volume 96– No. 11, 2014.
- [12] V. Patidar, N.K. Pareek, G. Purohit and K. K. Sud, "A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption", Optics Communications, journal homepage: www.elsevier.com/locate/optcom, 2011.
- [13] M. Bloch and J. Barros, "Physical-Layer Security from Information Theory to Security Engineering", Cambridge University press, 2011.
- [14] J. Ahmad and F. Ahmed "Efficiency Analysis and Security Evaluation of Image Encryption Schemes", International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol: 12 No: 04, 2012.

A Novel Block Audio Encryption Algorithm Based on 2D Standard map and 2D Baker map

Dr. Ekhlās Abass Albahrani

Dr. Sawsen Abdulhadi Mahmood

Department of Computer Science, College of Education, Mustansiriyah University

akhlasabas72@gmail.com

akhlas_abas@yahoo.com

Abstract:

In this paper, novel block encryption algorithm for audio file is proposed based on two chaotic maps: 2d Standard map and 2D Baker map.. The proposed algorithm encrypts and decrypts a block size of 256 bytes. Each block is input into four transformations: First permutation, Xor adding, Substitution and Last permutation. In First and Last permutation transformations the audio block is permuted using chaotic 2D Standard map. Then the resulted block is Xored with the key block and then the resulted block is substituted using chaotic substitution S-box. This S-box is permitted one time for only even audio block by using chaotic 2D Baker map. This algorithm was performed and analyzed with audio files of varies sizes of a wave file extension. The result from key space analysis, statistical analysis, MSE (mean square error) analyses, PSNR (Peak signal to noise ratio) analyses and entropy analyses showed that the algorithm is not vulnerable to brute force attacks, statistical attacks and achieve higher level of security.

Keywords: audio encryption, chaotic maps, block cipher, chaotic S-box, 2D Standard map, 2D Baker map.

خوارزمية تشفير مقطعية جديدة للملفات الصوتية بالاعتماد على المعادلة القياسية ذات البعدين ومعادلة بيكر ذات البعدين

د. اخلاص عباس البحراني د. سوسن عبد الهادي محمود

المستخلص

في هذه البحث، خوارزمية التشفير مقطعية جديدة للملف الصوتي على أساس اثنين من معادلات الفوضى: المعادلة القياسية ذات البعدين ومعادلة بيكر ذات البعدين. الخوارزمية المقترحة تقوم بتشفير وفك تشفير مقطع بحجم 256 بايت. كل مقطع يدخل الى أربعة عمليات: عملية التبديل الأول، عملية الجمع Xor مع المفتاح، عملية التعويض واخيرا عملية التبديل الأخير. في العمليات التبادلية الأولى والأخيرة يتم تغير ترتيب مواقع مقطع الملف الصوتي الصوت باستخدام معادلة الفوضى القياسية ذات البعدين. ثم المقطع الناتج يجمع مع مقطع المفتاح باستخدام عملية Xor، ثم يتم استبدال البايت في المقطع الناتج بالبايت الموجودة في صندوق التعويض الفوضوي. ان صندوق التعويض الفوضوي تبدل مواقعه مرة واحدة فقط لمقاطع الصوت الزوجية باستخدام معادلة بيكر الفوضوية. تم تنفيذ هذه الخوارزمية وتحليلها مع ملفات صوتية بأحجام مختلفة ومع امتداد ملف الموجة. وأظهرت النتائج من تحليل الفضاء الرئيسي والتحليل الإحصائي، تحليل متوسط المسافات المتوسطة (خطأ مربع)، نسبة إشارة إلى الضوضاء وتحليل الانتروبيا أن الخوارزمية ليست عرضة لهجمات القوة الغاشمة والهجمات الإحصائية وتحقيق مستوى أعلى من الأمن.

الكلمات المفتاحية: تشفير الملفات الصوتية، معادلات الفوضى، التشفير المقطعي، صندوق التعويض الفوضوي، المعادلة القياسية ذات البعدين، معادلة بيكر ذات البعدين.

1. Introduction

The chaotic based cryptosystems have many properties that make them appropriate for multimedia encryption such as images, videos or audio data. Some of these properties are arbitrary behavior, sensitivity to control parameters and initial conditions, pseudorandomness. The method of including the key (noise) to the plain text audio is called audio cryptography encryption and while the process of taking out the original plain text back by using the same key is cryptography decryption. The audio information, which is not the same as text messages and images, has higher repetition and stronger correlation between samples. In other word, whatever audio encryption system need essential issue is that audio indicator may be holds an expansive amount from claiming contiguous specimens of comparative qualities. The solution of this problem, correlation between samples must be destroyed in encryption algorithm.

Many scholars have made efforts to investigate audio encryption algorithm but the algorithm is the best when it strikes a good balance between performance and security [1]. An encryption algorithm was proposed by Sheetal Sharma, Lucknesh Kumar [2] to encrypt audio files using RSA algorithm. In this paper, the encryption and decryption is performed by applying DFT in order to take the frequency pins of the wave audio signal. Some algorithms, such as [3], [4], [5], [6], encrypts text files and images by applying different shuffling techniques. In reference [7] the RSA algorithm was used to encrypt speech files where each word is extracted and converted into text. A chaotic audio encryption system was presented in [8] where several encryption keys are generated by using a chaotic map and used in each iteration of the encryption process. In [9] the audio encryption algorithm was implemented in five steps. These steps implement different techniques of diffusion and table substitution to the audio data to perform lossless encryption. The papers [10], [11], [12] proposed algorithm to encrypt selected parts of the audio file by using Discrete Fourier Transform [10] in order to reduce audio encryption time. Alternatively, the references [11], [12] use AES to encrypt selected blocks of the audio file at the cost of a minor decrease in the security of encrypted files. In [13] transposition technique is used to encrypt audio file.

This paper proposes new algorithm for encrypting digital audio signals by combining block cipher and chaotic maps. This algorithm will be applied to the audio data that have WAV file extension. The proposed encryption algorithm performs four transformations on each audio block based on the chaotic system.

The Section 2 of this paper presents the methodology of proposed algorithm. The proposed encryption algorithm and decryption algorithm is presented in sections 3 and 4. Analysis and results of the proposed algorithm is in section 5 while section 5 presents the conclusion.

II. Methodology

In general, the encryption algorithm encrypts and decrypts a block size of 256 byte. Each block is inputs to four transformations (First permutation, S-box substitution, Xor adding, and Last permutation). First permutation transformation permits the audio block by using standard map. Each byte in the resulted block is substituted by the byte in Dynamical Key Dependent S-box that is generated based on chaotic maps in reference [14]. Then the block is Xored with the key. The key is generated by using the pseudorandom generator discussed in reference [15]. Lastly the resulted block is permitted again.

A. Block cipher

Block cipher is an encryption/decryption algorithm where the plain text block is used to generate the cipher text block. A block of plain text bits P is encrypted to a block of cipher text bits C. the transformation is controlled by the encryption key K and it is written $EK(P)=C$ [16].

B. Chaotic system

Chaotic system has many properties that make it interesting for cryptography application. These properties are random-like behavior, sensitivity to control parameter and initial conditions, ergodicity and self-similarity [17]. Chaos sequences are created in a greatly oversimplified way by utilizing difference equations. These sequences appear absolutely arbitrary to an outer observer,, regardless of their deterministic generation, Similarly as they are sensitively dependent for starting states.

The 2-D chaotic map known as the **Standard map** is used for permutation of audio block. It is defined as [18]:

$$\begin{cases} x_{i+1} = (x_i + r_x + y_i + r_y) \bmod N, \\ y_{i+1} = (y_i + r_y + K \sin \frac{x_{i+1}N}{2\pi}) \bmod N. \end{cases} \quad (1)$$

Where K is a positive integer and the two parameters r_x and r_y both belong to range $[0.. N-1]$. The Standard map has larger key space than Cat map and Baker map which make it a good suggestion for block permutation.

The inverse Standard map is defined as [19]:

$$\begin{cases} y_i = \left(y_{i+1} - r_y - K \sin \frac{x_{i+1}N}{2\pi} \right) \bmod N \\ x_i = (x_{i+1} - r_x - y_i - r_y) \bmod N. \end{cases} \quad (2)$$

The 2-D chaotic map known as the **Baker map** is used for permutation the S-box for only even audio block. The baker map is one of the major chaotic maps which is viewed as a randomization-based tool that performs the permutation of a square block of dimensions $M \times M$ by changing the values positions based on a secret key. It allocates a value to another value position in a bijective way. The Baker map must be discretized in order to be used in encryption algorithm. The discretized Baker map is made into two versions based on different keys used in the map [20]: version A and version B.

Version A: Every part of the keys is the divisor of the image size. Take an image with $M \times M$, the key which is a series of k integers $m_1, \dots, m_k$, is selected such that each integer m_i divides M , and $m_1 + \dots + m_k = M$. The formula of version A is

$$B(x', y') = \left(\frac{M}{m_i} (x - M_i) + y \bmod \frac{M}{m_i}, \frac{m_i}{M} \left(y - y \bmod \frac{M}{m_i} \right) + M_i \right) \quad (3)$$

Where $M_i = m_1 + \dots + m_i$, the pixel (x, y) , $M_i \leq x < M_i + m_i$, and $0 \leq y < M$. For example, assume an 8×8 square matrix ($M=8$) and the secret key $K=(4,2,2)$ [19].

The chaotic randomization of this square matrix is shown in Figure 1.

C. The Substitution S-Boxes

The substitution S-box is a nonlinear transformation where every byte of the input is supplanted by an alternate byte utilizing the S-box table. Dynamical Key Dependent S-box is created by using the algorithm proposed in reference [14]. The substitution S-box is a table of 16×16 integer values (256 bytes). The S-box is generated by using two chaotic maps: 2d Logistic map and 2d Cross map. Each unique byte of input state is mapped into a new byte in the following way: the byte is divided into row value which is leftmost 4 bits and column value which is the rightmost 4 bits. These row and column values are permuted to another row and column values by using the Cat chaotic map. The byte in the new row and column is then served as S-box index in order to find a unique output byte.

The inverse substitute byte transformation is performed in the following way: the byte is searched for in the S-box table to find its row and column. These row and column values are return to their real value by using the inverse of cat map. Then the new row and column is concatenate to make the original byte.

D. The key generation method

The key for proposed algorithm is generated by using the pseudorandom number generator PRNG discussed in reference [15]. This PRNG is generated based on the Jacobian elliptic chaotic maps and Standard map. The input to this PRNG is initial parameter (x_0) and two control values (α, k) which are floating point numbers where the precision is 10^{-16} . All the keys that needed in the proposed algorithm will be generated by using this generator.

III. The proposed audio encryption algorithm

The input to proposed algorithm is an audio file and a key. The audio file is viewed as a stream of bytes. The encryption algorithm encrypts and decrypts a block size of 256 byte. The main steps of the proposed encryption algorithm are:-

- **Step1:** Inputting and reading of: -

A. Audio data.

B. The control parameters (x_0, y_0) to create the S-box.

C. The control value parameters (α, k, x_0) and for the PRNG.

These parameters numbers are floating point numbers where the precision is 10^{-16} and considered as the keys of the algorithm.

- **Setp2:** Create the substitution S-box.

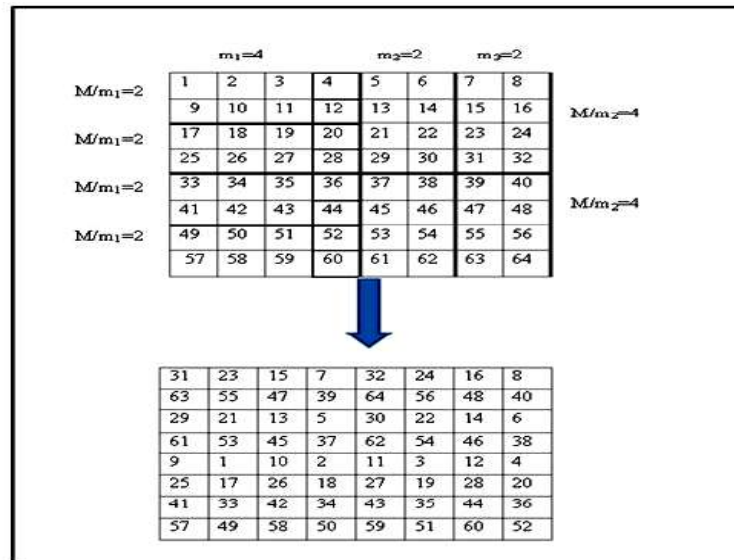


Fig. (1): chaotic permutation of an 8 X 8 matrix with a secret key (4,2,2).

• **Step3:** The original audio is divided into blocks $B_1B_2B_3B_4....B_n$, where B_i ($1 \leq i \leq n$) denotes i -th audio block with size 256 (16 x 16) bytes. When the last block is less than 256 bytes, it treats as one dimensional array B ($1 \times L$) where L is the number of bytes in this block.

- **Step4:** Repeat the following steps for all audio blocks:-

1- If block number is even then

a. Call the PRNG with its control parameters to generate the key for Baker map. The key of Baker map is sequence of t integer numbers $k_1, k_2, \dots, k_t$. Every part of the key is the divisor of the S-box size (16). The key sequence must be chosen in which each integer k_i divisible by 16 and $k_1 + \dots + k_t = 16$. The length of key sequence must be less than or equal to 16.

b. The substitution S-Box is Diffused using Baker map version A.

2- For each block do the following transformations:-

- **First Permutation transformation:** - the audio block is diffused using Standard map. The control values of Standard map is three values (r_x , r_y , k). These values will be generated by calling PRNG.

- **Substitution transformation:** - Each byte in the resulting audio block is substituted using substitution S-box. The byte substitution method in S-box is performed by using Cat map. The number of Cat map's control values is two values that will be generated by calling PRNG.

- **Xor adding transformation:-** call the PRNG to generate the key block of the same size of audio block. Each byte in the resulted audio block is Xored with the byte in the block key.

- **Last Permutation transformation:** - the resulted block is diffused also by using Standard map. In same way as in first permutation the control values of Standard map is generated by calling PRNG.

3- The resulted audio block is inserted to output encrypted audio file.

IV. Decryption algorithm

The audio decryption algorithm is reverse of audio encryption algorithm where each transformation is easily reversible. The main steps of the decryption algorithm are:-

- **Step1:** Inputting and reading of: -

A. Encrypted audio data.

B. The control parameters (x0,y0) to create the S-box.

C. The control value parameters (a, k, x_0) and for the PRNG.

These parameters numbers are floating point numbers where the precision is 10–16 and considered as the keys of the algorithm.

- **Setp2:** Create the substitution S-box.
- **Step3:** The encrypted audio is divided into blocks in the same way as in encryption algorithm
- **Step4:** Repeat the following steps for all encrypted audio blocks:-
 - 1- If block number is even, the PRNG with its control parameters is called to generate the key for Baker map. Then the substitution S-Box is Diffused using Baker map version A.
 - 2- For each block do the following transformations:-
 - **Reverse First Permutation transformation:** - Each encrypted block returns to its original position using inverse Standard map.
 - **Reverse Substitution transformation:** - Each byte in the encrypted audio block is substituted using inverse substitute S-box.
 - **Xor adding transformation:** - The reverse transformation is accomplished by XORing the encrypted audio block to the same block key. Each byte in encrypted block is Xored with the byte in the key block.
 - **Reverse Last Permutation transformation:** - Each encrypted block returns to its original position using inverse Standard map.
 3. The resulted audio block is inserted to output decrypted audio file.

V. Performance Analyzes

The encryption and decryption program implemented using Delphi7 programming language is used to run the proposed algorithm and to analyze its performance using MATLAB R2014b. The performance analysis of the proposed audio encryption algorithm is examined through a series of tests which are: -

A. Key Space Analysis

The key space for the proposed audio encryption algorithm is constructed from the control parameters that are needed for creating the substitution S-box (x_0 and y_0) and the control parameters (x_0 , α and k) that are needed for generating the key by using PRNG. These parameters are floating point numbers where each one has precision of 10^{-16} . The brute-force attack is not possible when the proposed algorithm have an extensive key space. The size a key space that is smaller than 2^{128} is not secures enough [21]. The total space of keys for the proposed algorithm is $((10^{16})^5) 2^{266}$. The encryption algorithm can resisted all types of brute-force attacks when the key space is large enough.

B. Statistical Analysis

The statistical analysis of the original audio and the encrypted audio can be considering by:

1- **Histogram analysis:** - the audio values are plotted before and after encryption to observe the effect of encryption. Figure 2(a) show a plotted of Wltvo.wav audio and Figure 2(b) show a plotted of the encrypted Wltvo.wav audio. The Wltvo.wav size is 322 KB. When comparing Figure 2 (a) to Figure 2(b), it can be seen that the encrypted audio does not give any statistically useful information about original audio and shows no Characteristics that may help an attack. These observations were the same for all tested audio files.

2- **Correlation coefficient analysis:** -The correlation, C , between two audio files, registered in two vectors X and Y , is computed as follows, where $\bar{X}$ and $\bar{Y}$ are mean values for vectors X and Y , respectively[19,22]:

$$C_{X,Y} = \frac{\sum_{i=0}^{N-1} (X_i - \bar{X}) \cdot (Y_i - \bar{Y})}{[\sum_{i=0}^{N-1} (X_i - \bar{X})^2]^{\frac{1}{2}} \cdot [\sum_{i=0}^{N-1} (Y_i - \bar{Y})^2]^{\frac{1}{2}}} \quad (4)$$

Where the mean values of A and B are:

$$\bar{X} = \sum_{i=0}^{N-1} X_i / N \text{ And } \bar{Y} = \sum_{i=0}^{N-1} Y_i / N$$

The results of correlation coefficients of 10 encrypted audio files of various sizes are shown in Table 1. Figure 3 shows the correlation for all encrypted files where encrypted audios have very small correlation values. These correlation analyses affirm that the proposed audio encryption

algorithm fulfills zero co-correlation, showing that the attacker can't get any valuable data by exploiting a statistic attack.

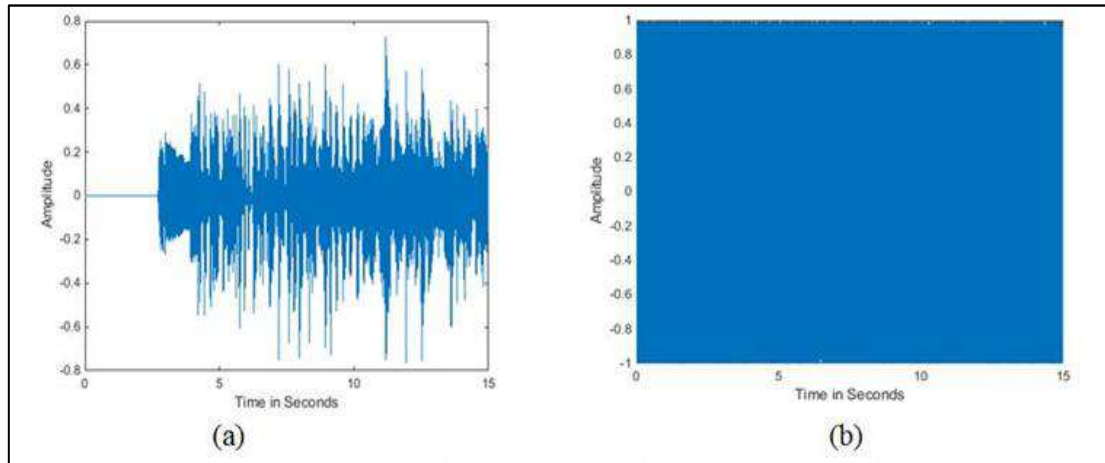


Fig. (2): plot of waveforms of (a) Original audio for Wltvo.wav. (b) Encrypted audio for Wltvo.wav.

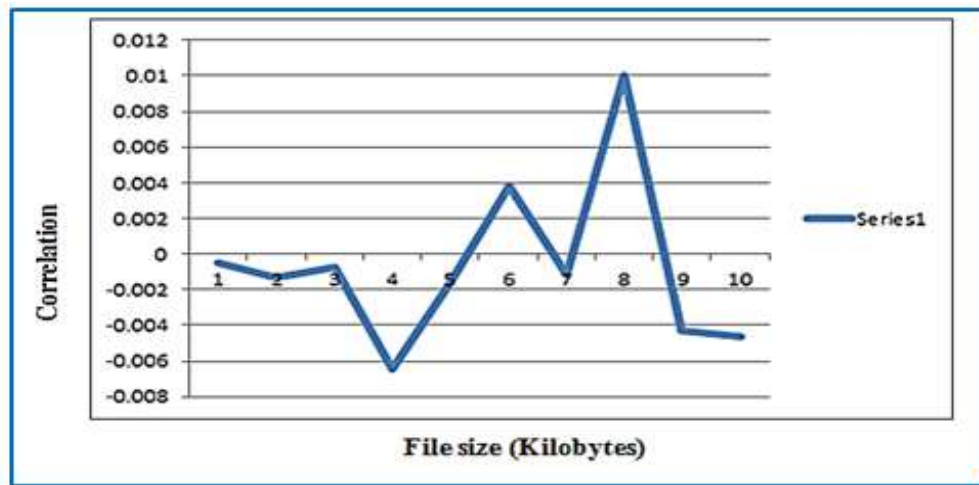


Fig. (3): Correlation coefficient of encrypted audio file.

C. Information Entropy Analysis.

Entropy is a measure of the randomness of a value and it is computed as follows [19,22]:

$$H(m) = - \sum_{i=1}^M p(m_i) \log(p(m_i)) \quad (5)$$

Where M is the maximum value of the audio data and $p(m_i)$ is the probability of the occurrence of mass function of message m_i . Higher entropy demonstrates higher resistance to statistical attacks. Table 2 shows the information entropy of 10 original and encrypted audio files. For the original audio files, the average entropy value was 3.22439 and for their encrypted files, the average entropy value was 4.57785. The entropy values indicated that when the audio files are encrypted using the proposed algorithm, their entropy values increased. This will leads to increase the randomness of values and reduced the risk of attacks.

D. Mean Square Error (MSE)

MSE is the avalanche effect measure in which the total squared lapse is discovered between the original and encrypted audios. Let two audio streams, stored in X and Y vectors, is computed as follows [19, 22]:

$$MSE = \frac{1}{N} \sum_{i=0}^L [A(i) - B(i)]^2 \quad (6)$$

If the value of MSE acquired using this equation is ≥ 30 dB (it is a logarithmic unit used to express the ratio of two values), quality difference between two audios is obvious. Table 3 shows the MSE for the all encrypted audios and it is found that all MSE values are greater or equal to 30 db which means that the difference between original and encrypted audios is evident.

E. Peak Signal-to-Noise Ratio (PSNR)

PSNR is measurement which demonstrates the adjustments in audio value qualities between the original audio and encrypted audio. It is mathematically shown in the following equation [19, 22]:

$$PSNR = 10 \log_{10} \left[\frac{M^2}{\sum_{i=0}^N (X(i) - Y(i))^2} \right] \quad (7)$$

Where $X(i)$ is the original audio vector, $Y(i)$ is the encrypted audio vector and M is the maximum audio data. PSNR values for the 10 encrypted audio files are shown in Table 3 where the average of PSNR values was 4.7929 db. Table 3 shows that the PSNR values are low which means that the encrypted audio files have a high level of noise which making them more resistant to attacks.

VI. Conclusion

A new audio encryption algorithm is proposed based on combining between chaotic maps and block ciphers. This new algorithm encrypts and decrypts the audio blocks through four transformations to increase the complexity of encryption process. In traditional block cipher, the S-box is static in the whole algorithm but in proposed algorithm the S-box is diffused in even block number. All the tested results indicates that the proposed audio algorithm is secure because of its large key space, uniform histograms, low PSNR, low correlation, high entropy and high MSR showed that the algorithm a good choice for encryption of audio data and other multimedia such as such images and videos.

Table (1) Results of correlation analysis of the proposed audio encryption algorithm.

Image name	Image Size	Correlation coefficient
Wltivo.wav	322 KB	0.001147069
A200201100.wav	9349 KB	-0.00018687
Slap.wav	42 KB	-0.00208765
Bird_caw1.wav	43 KB	-0.01522863
Africa-toto.wav	12800 KB	0.000460771
Read.wav	36 KB	0.002372778
Austinpowers.wav	53 KB	-0.00284711
Jamesbond.wav	64 KB	-0.00066150
Bugsbunny1.wav	46 KB	-0.00561513
Jelplanef16.wav	51 Kb	0.005916719

Table (2) Results of entropy analysis of the original and the corresponding encrypted audios.

Image name	Original image entropy value	Encrypted image entropy value
Wltivo.wav	2.7974	4.4838
A200201100.wav	3.9217	4.9858
Slap.wav	2.7735	4.4691
Bird_caw1.wav	2.0225	4.4489
Africa-toto.wav	4.1301	4.9885
Read.wav	3.7685	4.5012
Austinpowers.wav	2.0225	4.4694
Jamesbond.wav	3.1685	4.4525

Bugsbunny1.wav	3.5884	4.4864
Jelplane16.wav	4.0508	4.4929

Table (3) Results of MSE and PSNR of the original and the corresponding encrypted audios.

Image name	PSNR(db)	MSE
Wltivo.wav	4.7812	21794.79 =43.38 db
A200201100.wav	4.7963	21719.05 =43.36 db
Slap.wav	4.8076	21662.58 =43.35 db
Bird_caw1.wav	4.8060	21670.41 =43.35 db
Africa-toto.wav	4.7963	21718.96 =43.36 db
Read.wav	4.7675	21863.27 =43.39 db
Austinpowers.wav	4.7986	21707.56 =43.36 db
Jamesbond.wav	4.7956	21722.23 =43.36 db
Bugsbunny1.wav	4.8004	21698.47 =43.36 db
Jelplane16.wav	4.7791	21804.98 =43.38 db

References

- [1] G. Gunjan, C. Rama, "Review on Encryption Ciphers of Cryptography in Network Security". International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, no. 7, July 2012.
- [2] S. Sheetal, K. Lucknesh and S. Himanshu, "Encryption of an Audio File on Lower Frequency Band for Secure Communication". International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 7, July 2013.
- [3] J. W. Yoon and H. Kim. "An image encryption scheme with a pseudorandom permutation based on chaotic maps". Commun Nonlinear Sci Numer Simulat, vol. 15, no. 12, pp. 3998-4006, 2010.
- [4] A. Tamimi and A. Abdalla, "A double-shuffle image-encryption algorithm". Conf. Image Processing, Computer Vision, and Pattern Recognition (IPCV '12), Las Vegas, NV, USA, pp. 496-499, 2012.
- [5] A. Yahya and A. Abdalla. "A shuffle encryption algorithm using S-box". J. Comp. Science Publications, vol. 4, no. 12, pp. 999-1002, 2008.
- [6] A. Yahya and A. Abdalla. "An AES-based encryption algorithm with shuffling". Conf. Security & Management (SAM '09), Las Vegas, NV, USA, pp. 113-116, 2009.
- [7] Md. M. Rahman, T. K. Saha, and Md. A. A. Bhuiyan. "Implementation of RSA algorithm for speech data encryption and decryption". Int. J. Comput. Sc. & Netw. Secur., vol. 12, no. 3, pp. 74-82, 2012.
- [8] R. Gnanajeyaraman, K. Prasad, and Ramar "Audio encryption using higher dimensional chaotic map". Int. J. Recent Trends Eng., no. Academy Publisher, vol. 1, no. 2, pp. 103-107, 2009.
- [9] D. Sharma. "Five level cryptography in speech processing using multi hash and repositioning of speech elements," Int. J. Emerging Technol. and Adv. Eng., vol. 2, no. 5, 21-26, 2012.
- [10] S. Sharma, L. Kumar, and H. Sharma. "Encryption of an audio file on lower frequency band for secure communication," Int. J. Adv. Res. Comput. Sc. & Software Eng., 3, no. 7, 79-84, 2013.
- [11] B. Gadanayak, C. Pradhan, and U. C. Dey. "Comparative study of different encryption techniques on MP3 compression", Int. J. Comput. Appl., vol. 26, no. 3, 28-31, 2011.
- [12] B. Gadanayak, C. Pradhan, and N. Baranwal. "Secured partial MP3 encryption technique", Int. J. Comput. Sci. & Inform. Technol., vol. 2, no. 4, pp. 1584-1587, 2011.
- [13] J. Ahmad, Haviluddinb. "An audio encryption using transposition method", International Journal of Advances in Intelligent Informatics, vol. 1, no 2, pp. 98-106, July 2015.

- [14]F. J. Luma, H. S. Hilal and A. Ekhlās, “ **New Dynamical Key Dependent S-Box based on chaotic maps**”, IOSR Journal of Computer Engineering, vol. 17, no. 4, pp. 91-10, July – Aug. 2015.
- [15]F. J. Luma¹, H. S. Hilal¹ and A. Ekhlās. “**New Pseudo-Random Number Generator System Based on Jacobian Elliptic maps and Standard Map**”, IJCCCE, vol.15, no. 3, 2015.
- [16]W. Stallings. Cryptography and Network Security: Principles and Practice, 5th Edition, Prentice Hall; 2011.
- [17]P. L. Carmen and L. R. Ricardo. “**Notions of Chaotic Cryptography: Sketch of a Chaos Based Cryptosystem**”, Department of Computer Science and BIFI, University of Zaragoza, Spain.
- [18]S. Lian, J. Sun and Z. Wang. “**A Block Cipher Based on a Suitable Use of the Chaotic Standard Map**”, Chaos, Solitons and Fractals, vol. 26, pp. 117–129, 2005.
- [19]A. Ekhlās. Image Encryption Using Substitution-Permutation Network with Chaotic Mapping. Diss. University of Technology, December \ 2015.
- [20]N. Radha and M. Venkatesulu. “**A Chaotic Block Cipher for Real-Time Multimedia**”, Journal of Computer Science, vol. 8, no. 6, pp. 994-1000, 2012.
- [21]B. Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition, John Wiley & Sons; 1996.
- [22]A. Tamimi and A. Abdalla. “**An audio shuffle-encryption algorithm**”, Proceedings of the World Congress on Engineering and Computer Science, San Francisco, USA, vol. I, 2014

Data Security in Cloud Computing Architecture Based on Modified AES

Asst. Lecturer Amal Abdulbaqi Maryoosh

Department of Computer Science, College of Education, Mustansiriyah University

Abstract:

Cloud computing considered one of the most important areas of research today, because its ability to reduce costs which related with computing while increase flexibility and scalability for computing services. Using cloud computing, users store their data remotely to third party and enjoy the on-demand applications, storage and services from a shared pool of configurable computing resources, without the burden of data storage, maintenance and costs. In cloud computing people can share resources, services and information among the people through use of internet. Since we share the data through the internet, security is considered as a major issue. In Cloud computing several security issues arises like confidentiality, integrity and authentication. This paper aims to provide a secure, effective, and flexible method to ensure secured data in cloud computing by using modified Advanced Encryption Standard.

Keyword: Cloud Computing, Security, AES, Arnold Cat Map, SHA.

1. Introduction

Cloud computing is era technology that provide virtualized significant pool of computing resources. The user with cloud computing can use these resources anywhere, everywhere, on-demand and based on pay per use principle. Cloud computing has two types of models: services models (SaaS, PaaS, and IaaS), and deployment models (Public, Private, Community, and Hybrid cloud). Also the cloud computing is contains five essential characteristics (On-Demand, Broad Network Access, Rapid Elasticity, Measured Service, and Resource pooling). There are many concerns about the data security in cloud computing should be taken into account such as violation of the confidentiality and privacy of customers' data via unauthorized parties. Using cryptography is the best way to secure data in cloud computing. It becomes difficult for an intruder if the data existent in cloud is in encrypted form, as the data files or encrypted data blocks are useless for any person unless he knows the perfect method for decrypting it. In this paper I will use the modification of AES algorithm which was proposed by Ali AdulGader et al in [1] to provide data security and hash function for data authentication.

2. Related Work

Several works related to our work, which presents the security of data in cloud computing as follow:

In [2] Debajyoti Mukhopadhyay et al proposed methodology for secure uploaded file to cloud servers, this method depend on use AES algorithm and implement authentication techniques. In [3] Nikhil Gajra et al used hybrid of AES and Blowfish for encryption and used hashing for key exchange and key management. In [4] Sudhansu Ranjan Lenka and Biswaranjan Nayak used RSA algorithm to provide confidentiality and used MD5 to provide authentication for data.

3. Advanced Encryption Standard Algorithm (AES)

AES is a symmetric encryption algorithm that operate in block of data (4x4 square matrix of bytes (128 bits)) called state with key length of 128, 192, or 256 bits. The encryption and decryption operation consist of N round, where the number of rounds depends of key length (10, 12, or 14). Figure (1) show the AES algorithm architecture [5].

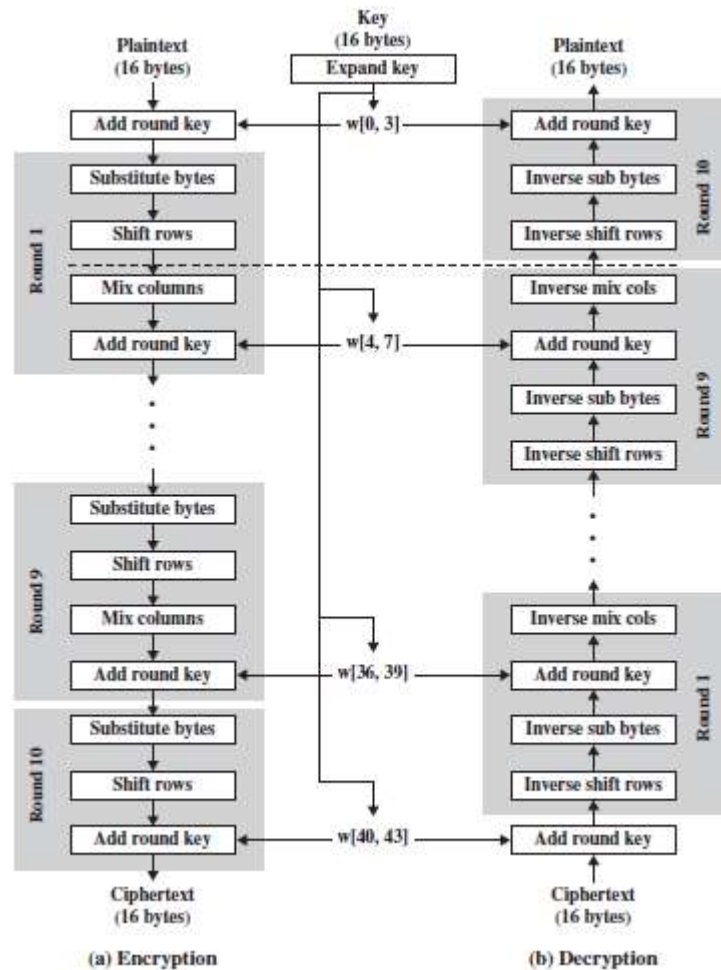


Fig. (1): Encryption and Decryption Process in AES

As shown in figure (1) AES architecture contain the following processes:

- 1- Key Expansion:** In this operation the key expansion algorithm will be used to derive key to each round from the cipher key.
- 2- Initial Round:** In this step the cipher key will combine with the state matrix using XOR operation.
- 3- Sub-Byte/ Inverse Sub-Byte:** In substitution byte operation will be working the state which resulting from the initial round. Each byte in state matrix will be replaced with S-box table. While in Inverse Sub-Byte operation the bytes in state will be replaced with InvS-box table.
- 4- Shift Rows/ Inverse Shift Rows:** Shift row operation will be applied on the state which resulting from the sub-byte step, in this step the 1st row remains without change, the 2nd row shifted one byte to the left, the 3rd row shifted two bytes to the left, the 4th row shifted three bytes to the left. In inverse shift rows only the direction of rotation will be reflected.
- 5- Mix Columns/ Inverse Mix Columns:** In this step the state that resulting from the shift row step will be multiplied with a special matrix. The inverse mixed column will be done by multiplying with another special matrix as follows:

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \quad \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}$$

Mix Column Matrix Inverse Mix Column Matrix.

6- AddRound Key: In this step the round key will added to the matrix which resulting from Mix Cloumn using XOR operation [5, 6].

4. Arnold's Cat Map Algorithm

Chaotic is a technique widely used to generate the random number, it characterized by efficiency in the processes of diffusion and permutation. Chaos is very suitable for image encryption method, there is a set of dynamic characteristics that make it suitable for chaos image encryption like: It has a high sensitivity for primary condition, natural dissimulation, and tiny movement disorder. This system's security depends on the degree of rounding between signal and random numbers that generated by secret key generator. Arnold cat map is one of chaotic map types, it used to change the pixel location in the image without deleting any information from the image or change its value [7,8]. Two-dimensional equation of Arnold's Cat Map can be written as follows:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \text{mod}(n) \dots (1)$$

Where x and y are pixel's locations, p and q are positive integers and n is a size of image.

4. Modified Advanced Encryption Standard (MAES)

This algorithm modified by Ali AdulGader et al in [1], it combination of AES in CBC mode with chaotic map system. The characteristics of this algorithm are increasing the efficiency of data encryption process and reduce the time of encryption and decryption. The modification steps in this algorithm as follow:

- 1- Gets rid from the weakness in the fixed S-box and improve the key sensitivity by implement some circular shift on the S-box based on the round keys.
- 2- Replace MixColumn step with the chaotic system to decrease the amount of calculation in AES. The used of MixColumn stage is to data diffusion in the AES algorithm that takes large computations which decelerate the work of AES. The AddRound Key and Shift Rows stages will stay without any changed.

5. Proposed Method Architecture

In this paper we want to implement a safe method to secure the images and files that we want to save them in cloud computing. The user can encrypted the images and files by using modified AES algorithm based on password and then uploaded them to cloud, also he can download any uploaded file previously. The following figure show the general diagram of the proposed system.

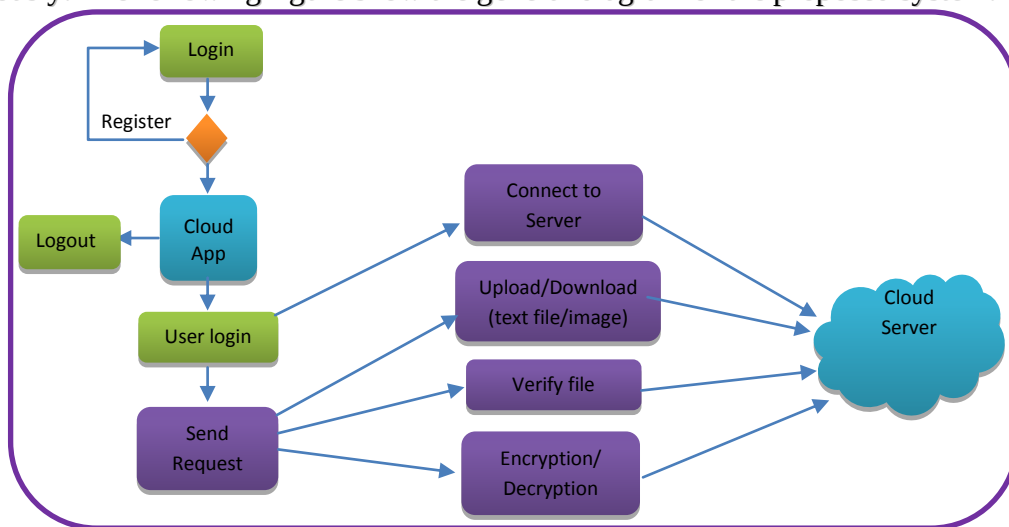


Fig. (2): General Diagram

A. Uploading Data

The following processes will explain upload data step.

- 1- The user login by enter the user name and password
 - If the user information is matching to database information then the user is authenticated, and can be establish connection with cloud service provider.
 - Else, show the message “the user not authorized”.
- 2- The user choose text file/image to be uploaded to cloud server.
- 3- In order to use the encryption service the user must enter password.
- 4- The password of user must be saved to used it for generate encryption key.
- 5- Apply encryption algorithm.
- 6- Press upload key to upload text file/image to cloud server.
- 7- The user logout from system.

When the user enter his user name and password. The system matching the user information with database, if identical then allow user to enter to the system, else show the message “the user not authorized”. The user information is encrypted using hash function before saved it in database. After the user logs on to the system, he can upload his files or images. The user files or images will encrypted before uploaded to cloud server. For file or image encryption the user must enter password, this password will used to generate encryption key and save this password to use it in decryption operation. In this paper we used Password Based Key Generation Function 2 (PBKGF2 is a pseudorandom function, in this paper we used HMAC), then send the encrypted data to cloud server. Figure (3) illustrates uploaded data steps.

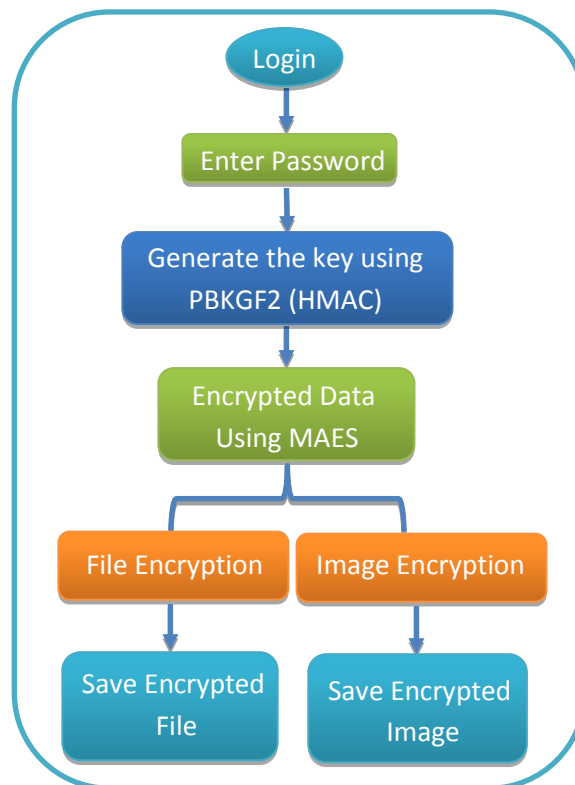


Fig. (3): Uploaded Data Processes

B. Downloading Data

The following processes will explain downloading data step.

- 1- Repeat the same first step in the process of uploading data.
- 2- The user choose the data that he want to download it.
- 3- The user enter the same password that used in encryption operation to generate the same encryption key because AES is symmetric key algorithm.
- 4- Apply decryption algorithm.
- 5- The user will get the same original data that he uploaded to cloud server.

6- The user logout from system.

Figure (4) illustrates download data steps.

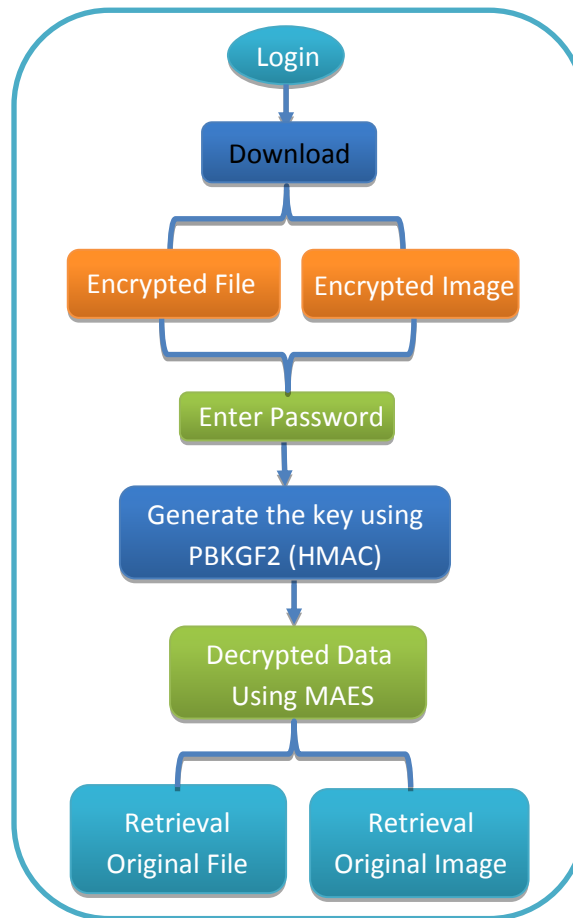


Fig. (4): Download Data Processes

6. Experimental Results

In this section, we review the results obtained when applying the proposed method. The experiment are performed on a computer with Intel Core i3 CPU 2.10 GHz, 3GB RAM with windows 7. Figure (5) show the encryption end decryption image in MAES algorithm.



Fig. (5): (a) Original image (b) Encrypted image (c) Image after decryption using MAES algorithm

6.1. Histogram Analysis

The Histogram Analysis of the three bands (red, green, blue) for original image and encrypted image are shown in Figure (6).

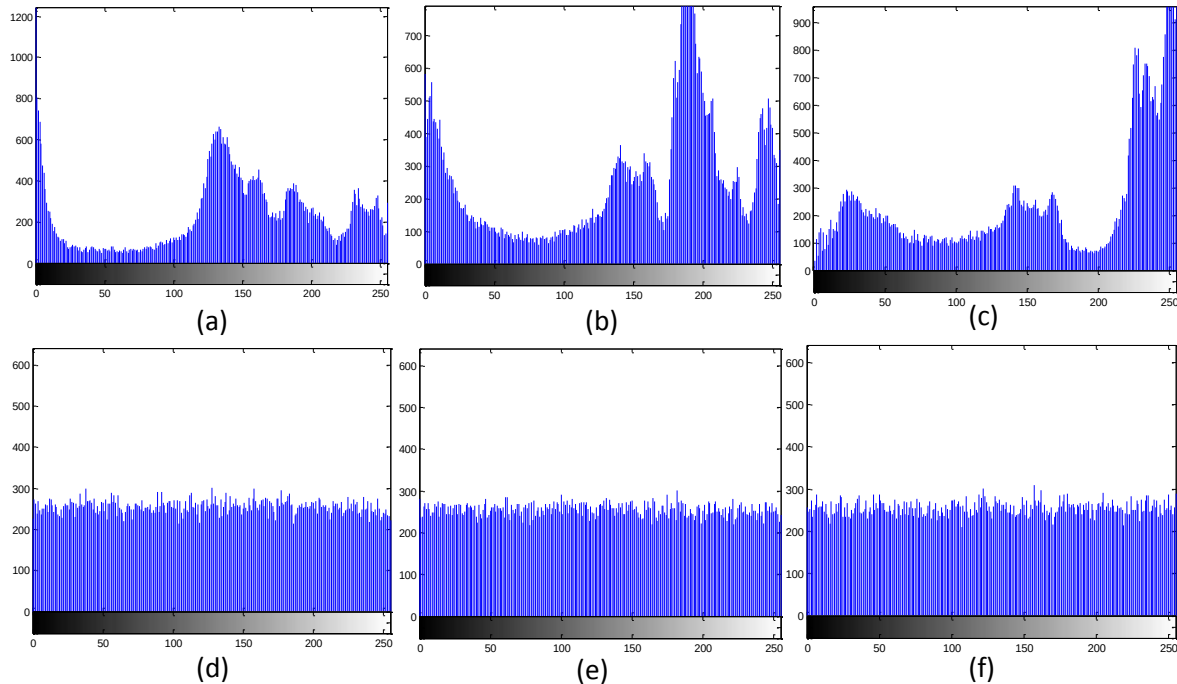


Fig. (6): The Histogram Analysis: (a), (b) and (c) are The Histogram of (Red, Green and Blue) of the Original Image, (d),(e) and (f) are The Histogram of (Red, Green and Blue) Encrypted Image by using mAES algorithm

6.2. Information Entropy

Information entropy is a quantitative measure of the randomness of a signal. Because a digital image is a type of digital signal, the entropy analysis can be used to measure the randomness of a test image. The information entropy of an image can be defined as Eq. (2), where X denotes the test image, x_i denotes the i^{th} possible value in X , and $\text{Pr}(x_i)$ is the probability of $X=x_i$, i.e. the probability of pulling a random pixel in X and its value is x_i . The maximum of $H(X)$ is achieved when X is uniformly distributed [9].

$$H(X) = -\sum_{i=1}^n p(x_i) \log_2 p(x_i) \quad \dots \dots \dots (2)$$

Table (1) shows the test results of Entropy measure for MAES scheme that compared with original AES algorithm.

Table (1) The Result of Entropy Measure for Different Images

Image	Entropy		
	Original Image	AES	mAES
Penguins 256x256	7.3568	7.9971	7.9990
Tulip 512x512	7.2069	7.9992	7.9994
Koala 1024x1024	7.8498	7.9998	7.9999

6.3. Diffusion Property Analysis

The diffusion property describes the cipher's ability of diffusing a change in a plaintext image over its corresponding ciphertext image. If a cipher is weak in diffusion, it might be vulnerable against the differential attacks. The number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI) are two most common quantitative methods to evaluate an image encryption method/algorithm/cipher for resist differential attacks [9]. The (NPCR) means the change rate of the number of pixels of the encrypted image when only one pixel of the original image changed and the (UACI) means the unified average changing intensity which gauges the average intensity of variations between the original image and encrypted image. The NPCR and UACI definition shown in Eq (3) and (4) [10]:

$$NPCR = \frac{\sum_{i,j}^{N,M} Diff(i,j)}{M \times N} \times 100\% \quad \dots\dots\dots (3)$$

$$UACI = \frac{1}{M \times N} \left[\sum_{i,j}^{N,M} \frac{C_1(i,j) - C_2(i,j)}{255} \right] \times 100\% \quad \dots\dots\dots (4)$$

In equation (3), the Diff (i, j) is determined by the initial cipher image $C_1(i, j)$ and ciphered image that is changed some grey level of the pixels $C_2(i, j)$, if $C_1(i, j) = C_2(i, j)$ then Diff (i, j) = 0, otherwise, Diff (i, j) = 1. While M and N in both equations (3) and (4) are the width and height of the image. Table 2 shows the test results of NPCR and UACI measures for MAES scheme that compared with original AES algorithm.

Table (2) Measurements of NPCR and UACI for different images.

Images	NPCR for AES	NPCR for MAES	UACI for AES	UACI for MAES
Penguins 256x256	99.6093	99.6103	33.4635	33.7115
Tulip 512x512	99.6093	99.6114	33.4635	33.8247
Koala 1024x1024	99.6067	99.6093	31.2704	33.4635

6.4. Encryption/Decryption Time Analysis

The encryption speed in this paper is analyzed by comparing the encryption and decryption time of MAES algorithm with the AES algorithm. Table 3 shows the encryption and decryption time of the algorithms for different image sizes. Table 4 shows the encryption and decryption time of different file size.

Table (3) Encryption and Decryption Time (in Second) for Different Images Size

Images	AES algorithm		MAES algorithm	
	Encryption	Decryption	Encryption	Decryption
Penguins 256x256	127.25	151.14	61.162	61.84
Tulip 512x512	504.67	542.36	231.06	223.14
Koala 1024x1024	2092.32	2125.12	1009.23	987.71

Table (4) Encryption and Decryption Time (in Second) for Different File Size

File Size	AES algorithm		MAES algorithm	
	Encryption	Decryption	Encryption	Decryption
12 KB	3.51	1.3044	1.67	0.1087
25 KB	7.3125	2.7175	3.4791	0.2264
40 KB	11.7	4.348	5.5666	0.3623

7. Conclusion

In this paper, an efficient method has been introduced to address data storage security problems in cloud computing based on the combination of chaotic map and AES algorithm. Whereas Arnold Cat map is used to construct new chaotic mask to replace mix columns transformations and improve the key sensitivity by implement some circular shift on the S-box based on the round keys. Efficiency of the method has been confirmed through above experiment results. According to these results the proposed scheme provides high key space, high key sensitivity and less time for encryption and decryption processes than original AES as well as it offers high resistance against differential and statistical attacks.

References

- [1] Ali AdulGader et al, “**Enhancement Of Aes Algorithm Based On Chaotic Maps And Shift Operation For Image Encryption**”, Journal of Theoretical and Applied Information Technology, Vol.71 No.1, January 2015.
- [2] Debajyoti Mukhopadhyay et al, “**Enhanced Security for Cloud Storage using File Encryption**”, available at <https://arxiv.org/ftp/arxiv/papers/1303/1303.7075.pdf>, accessed date: 17/7/2016.
- [3] Nikhil Gajra, Shamsuddin S. Khan and Pradnya Rane, “**Private Cloud Data Security: Secured User Authentication By Using Enhanced Hybrid Algorithms**”, International Journal of Computer Engineering and Technology (IJCET), ISSN 0976- Volume 5, Issue 8, August (2014).
- [4] Sudhansu Ranjan Lenka and Biswaranjan Nayak, “**Enhancing Data Security in Cloud Computing Using RSA Encryption and MD5 Algorithm**” International Journal of Computer Science Trends and Technology (IJCTST) – Volume 2 Issue 3, June-2014.
- [5] William Stallings, “**Cryptography and Network Security**”, principles and practice 5th edition, Pearson Education, Inc., 2011.
- [6] Salim A. Abaas and Ahmed K. Shibeeb, “**A New Approach for Video Encryption Based on Modified AES Algorithm**”, IOSR Journal of Computer Engineering, Volume 17, Issue 3, Ver. VI (May – Jun. 2015).
- [7] Pan Tian-gong and Li Da-yong, “**A Novel Image Encryption Using Arnold Cat**”, International Journal of Security and Its Applications, Vol.7 No.5, 2013.
- [8] Eko Hariyanto and Robbi Rahim, “**Arnold’s Cat Map Algorithm in Digital Image Encryption**”, International Journal of Science and Research (IJSR), Volume 5 Issue 10, October 2016.
- [9] Yue Wu et al., “**Design of Image Cipher Using Latin Squares**”, Information Sciences, January 2014.
- [10] J. Zhang, “**An Image Encryption Scheme Based on Cat Map and Hyperchaotic Lorenz System**”, IEEE International Conference on Computational Intelligence and Communication Technology, IEEE, 2015.

Proposed E-mail system based on multi-chaos maps

Assist. Prof. Dr. Haider K. Hoomod Arkan Mohammed Radi
Mustansiriyah University/ College of Education/ Computer Science Department
drhjne@gmail.com

Abstract:

Electronic mail (Email) is a set of mechanisms used that allows for users sends and receive messages by Internet. Messages exchanged between the sender and the recipient passes through many service centers and / or routers can be a real threat to the confidentiality and integrity of data and Especially if those sensitive data or military images must be encrypted and can not be read by unauthorized.

Cryptography can be providing confidentiality, authentication to content message. So, we need a safe encryption algorithm to encrypts Email messages such as algorithm Advanced Encryption Standard (AES) or DES As well as chaotic system.

The proposed E-mail system security is uses modified AES algorithm and chaotic system as key. This modification makes the proposed system more sensitivity and randomness, The execution time for both encryption and decryption of proposed system is less that original AES, And in addition to being compatible with all MailServer.

Keyword: Receiver.

أقتراح نظام بريد الكتروني يستند على خرائط فوضوية متعددة
د.م حيدر كاظم حمود اركان محمد راضي

المستخلص

البريد الالكتروني (Email) هو مجموعة من الاليات المستخدمة التي تسمح للمستخدمين بارسال الرسائل الى الآخرين. الرسائل المتبادلة بين المرسل والمستلم تمر من خلال العديد من مراكز الخدمة او الموجهات يمكن ان تمثل تهديداً حقيقياً للسرية وسلامة البيانات وخصوصاً اذا كانت تلك البيانات حساسة او صور عسكرية التي يجب ان تكون مشفرة ولا يمكن قراءتها فقط من قبل الاشخاص المخولين.

التشفير يمكن ان يوفر السرية والموثوقية لمحتويات الرسالة. لذلك نحن بحاجة الى خوارزمية تشفير امنة لتشفير رسائل البريد الالكتروني مثل خوارزمية معيار التشفير المُطَوَّر (AES) أو DES فضلاً عن الانظمة الفوضوية.

نظام البريد الالكتروني المقترح يستخدم خوارزمية AES المعدلة والانظمة الفوضوية كمفتاح. هذا التحديث يجعل النظام المقترح اكثر حساسية وعشوائية. وقت التنفيذ في كلا من التشفير وفك التشفير في النظام المقترح هو اقل من خوارزمية AES الاصلية فضلاً عن كونه متوافق مع كل خوادم البريد الالكتروني.

1- Introduction

E-mail provide to users the ease of communication With each other via the Internet and using standard protocols. [1]

The Simple Mail Transfer Protocol (SMTP) used to send the email messages. While the Internet Mail Access Protocol (IMAP) and Post Office Protocol (POP3) use to receive the email messages coming from sender's Mailbox. [2]

Sensitive data transmitted from sender's Mailbox to receiver's Mailbox over the Internet passes through many servers and/or routers. This model inherently vulnerable to eavesdropping and great threats to privacy of email. [3]

Email security contains authentication, confidentiality, integrity, non-repudiation. Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extension (S/MIME) are use to provide security services for email system but suffers from encryption low and performance weakness. [4]

Symmetrical encryption algorithm such as Advance Encryption Standard (AES) is has several important characteristics to make the contents of the email is safe against attacks [5].

Chaotic mapping has many important properties corresponding to cryptography [6]. Its randomness, sensitivity are initial conditions and control parameters. These features make chaotic systems as choice strong in constructing cryptosystems [4,7].

In this the paper focus on use both modified AES algorithm and chaotic systems (Lu and Lorenz) in design of a proposed E-mail system security.

2- Advance Encryption Standard (AES)

AES is an encryption algorithm used symmetric key and used in encrypt/decryption the contents of the message between two parties.

The data block length and key length of AES can be varied according to the requirement. Three key lengths: 128, 192, 256, whose iteration cycle number is 10, 12 and 14 round respectively, AES encryption process is shown in Figure 1. Each round consists of the following four steps: SubBytes, ShiftRows, MixColumns, AddRoundKey [8].

There are a number of benefits of AES will be relevant in provide E-mail system security as Secure, accepted Cost, Flexible, Simplest. However, these methods have some shortcomings encryption speed has a poor efficiency at a low level, If the attachments are large, it is therefore necessary to develop AES algorithm and make it more efficient in implementing encryption and decryption [28].

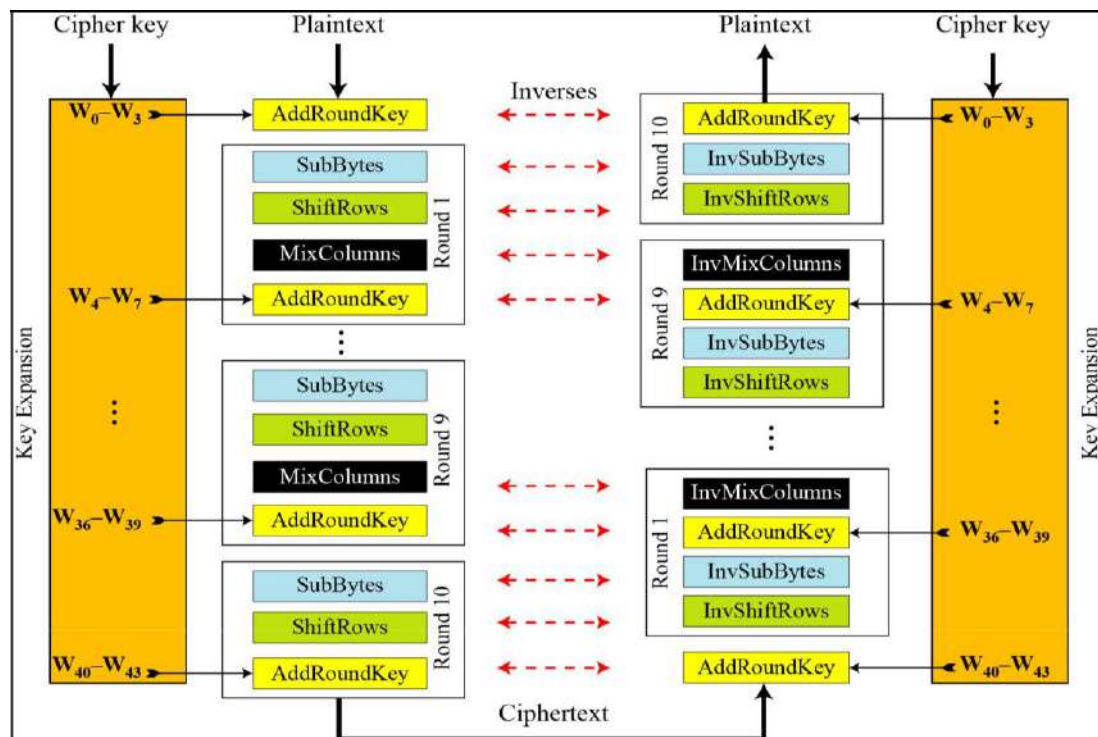


Fig. (1): AES Encryption and Decryption process

3- Chaotic Systems

Chaos Systems are nonlinear dynamical systems. Depending on the time range they are described by differential equations (discrete-time systems) or differential equations (continuous-time systems). Chaotic System is sensitive to initial condition, this means that the different initial condition produces different trajectory, the same conditions can produce the same trajectory. We need to use three-dimension chaotic system such as Lu and Lorenz are suitable to encrypt the three components of color image and In addition to text [10,11].

3-1 Lu Chaotic System

The Lu system is a three dimensions chaotic system and it is described in the following equations [12]:

$$\bar{X} = a(y - x) \quad \dots(1)$$

$$\bar{Y} = -xz + cy \quad \dots(2)$$

$$\bar{Z} = xy - bz \quad \dots(3)$$

3-2 Lorenz Chaotic System

Lorenz system is also three dimensions chaotic system and the Lorenzo system steps and its equations are described in following equations [12]

$$\bar{X} = \sigma(y - x) \quad \dots(1)$$

$$\bar{Y} = x(\rho - z) - y \quad \dots(2)$$

$$\bar{Z} = xy - \beta z \quad \dots(3)$$

4- Proposed E-mail system security:

Proposed E-mail system security consists from two part: First part is modified AES algorithm and Second part is generate key based on chaotic system. First part modified AES, is uses same the properties of encryption operations that already exist in the AES, Sub-Bytes, Shift-Rows and Add-Round-Key. but remove the Mix-Columns operation and use XOR operation and Shift feed by 2 bits instead of it, this process is shown in Fig(2). Second part Generate key, It's using the chaotic (Lu and Lorenze), The Lu system taking its initial conditions for generate three random numbers used as inputs to The three equations of Lorenz system to generate chaotic masks as the size of the image that we want to encrypt and these masks will be used to generate three block masks are used for as key to AES modify.

This modification adds more sensitivity and randomness to the system and reducing time required in both encryption and decryption for content (Text/Image) message during an exchange of messages between the sender's Mailbox and the recipient's Mailbox via the Internet using protocols (SMTP,POP3), and In addition to being compatible with all Mailserver.

5- The Proposed System Encryption and Decryption

Proposed system contains two Encryption and Decryption processes of email message:

5-1 Encryption process of email message:

In this side, First reading the plain-Image/text that we want to encrypt and second reading initial values as key that pass to chaotic systems (Lu, Lorenz) for generate key randomness is used with plain-image/text in modified AES produce cipher-Image/Text by executes encryption operations As shown in fig (2), and then XOR operation with three mask block that also generated from Lorenz system, and then send to recipient via the Internet, using protocol SMTP.

5-2 Decryption process of email message

In this side, first receives encrypted messages (Cipher-Image/text) via the Internet, using protocol POP3, and then reading initial values as key are same values that used in encryption and then pass to chaotic systems (Lu, Lorenz) for generate key randomness is used with Cipher-image/text in the modified AES for produce plain-image/text by execute decryption operations is inverse some encryption operation As shown in fig (2), and about the X-OR operation will be moved up before modified AES, that it was after modified AES.

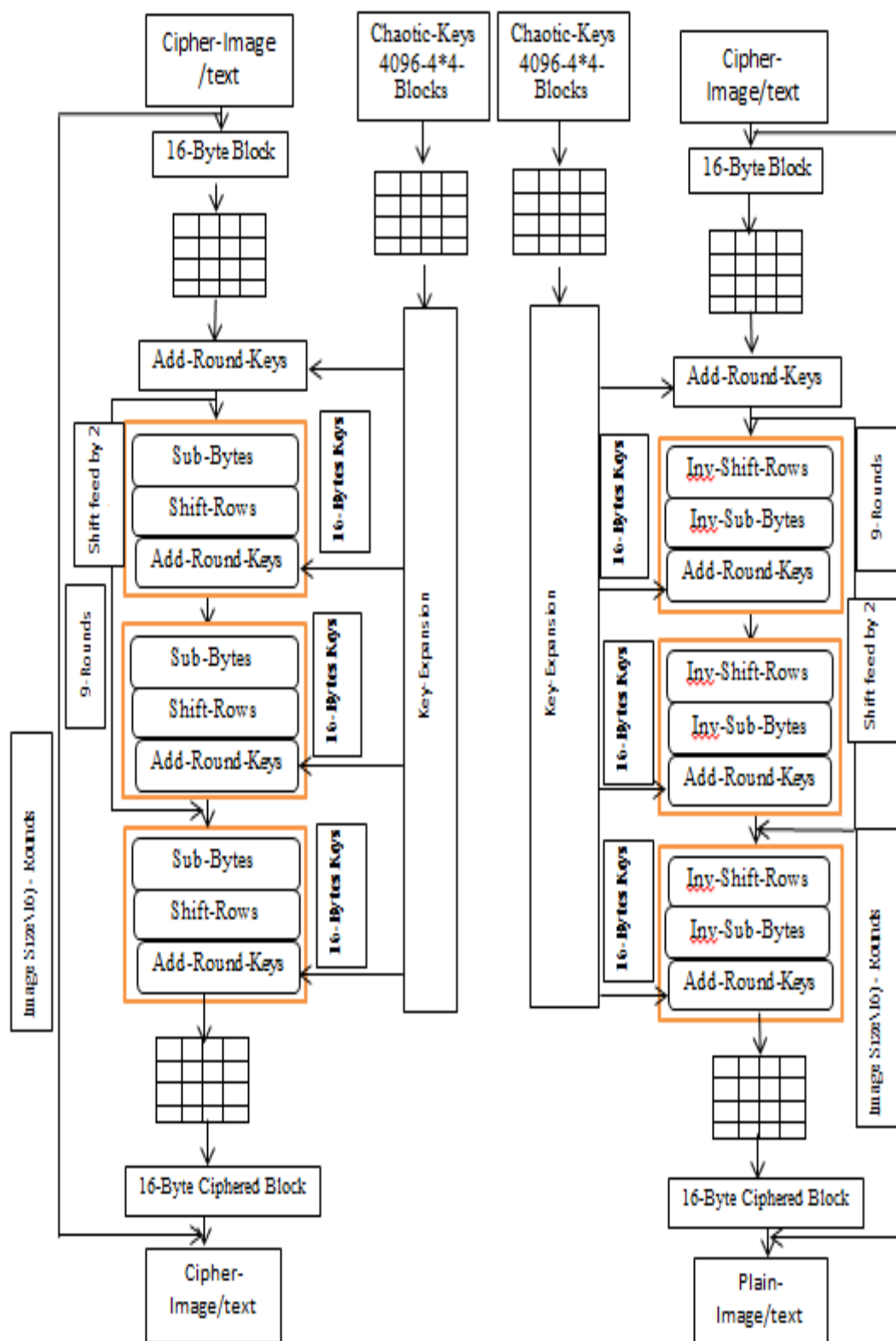


Fig.(2): Modified AES Encryption/ Decryption Process

6- Experimental Results:

Conducted on this system a series of experiments on the contents of the message (text or image) showing the efficiency of the proposed AES algorithm compared to the original AES algorithm, the main disadvantage that was resolved is a waste of time (lost) in the encryption and decryption process of original AES algorithm, which needed to a lot of time, with Large amount of data, these tests also show a sensitivity and randomness of the key that is based on chaotic (Lu, Lorenz) used in this system. Experiments on a PC with Intel Core i3 CPU M370 @ 2.40GHz, 2G RAM with Windows 7, type experiments:

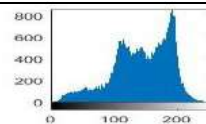
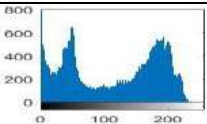
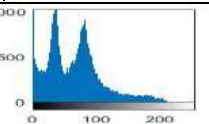
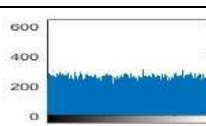
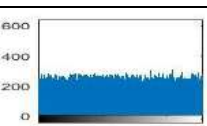
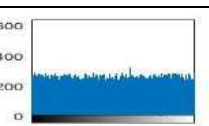
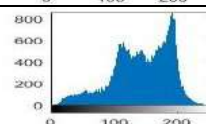
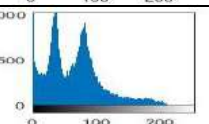
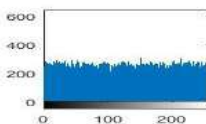
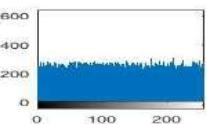
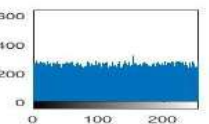
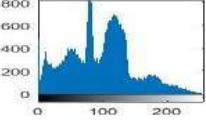
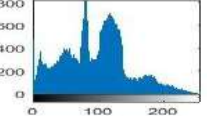
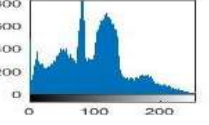
6-1 Analysis of the Key Sensitivity:

The proposed system is sensitive to the key change even if it is a slight change, for example we encrypt the contents of the message with a key (0.88), a small change in the key (0.880000000000001) and then execute operation decryption was the result the message was not decrypted.

6-2 The Histogram Analysis

The image histogram show how pixels in an image are distributed by graphing the number off pixels at each color intensity level. The Table (1) showing the histogram of the proposed system for plain and encrypted imaged.

Table (1) Histogram Analysis for the Proposed System

Image	Histogram					
		R		G		B
Original						
Encrypted						
Original						
Encrypted						
Original						
Encrypted						

6-3 Correlation Analysis:

This operation will compute the correlations between plain text/ image and encrypted text/image in proposed system, a good encryption system should give a low correlation, And this will compare between the original AES and the proposed system as shown in the Tables (2,3).

Table (2) Correlation Analysis for the Proposed System

Characters message	Correlation Analysis for body (text)	
	Proposed System	Original AES
50	-0.01391	0.00867
100	0.00225	-0.09257
250	-0.05034	5.52086

Table (3) Correlation Analysis for the Proposed System

Image		Correlation Analysis for attachment(image)					
		Proposed System			Original AES		
		R	G	B	R	G	B
1.		-0.00386	-0.00386	-0.00453	0.00501	0.00501	0.00446
2.		0.00179	0.00179	-0.00323	0.00167	7.50300	3.11918
3.		-0.00407	-0.0060	0.34690	0.00123	0.00123	0.00294

6-4 Entropy Analysis:

The entropy calculates the uncertainty association of the random values, the good encryption algorithm should give a low mutual information of the pixel values of the encrypted image, and this means that the entropy will be increased, the entropy of the proposed system is improved and gains better entropy than original AES, and the Tables (4) shows these results.

Table (4) Entropy for the Proposed System

The Entropy					50 character	100 character	250 character
	Proposed System	7.9990	7.9992	7.9992	5.70695	6.61910	7.18041
	Original AES	7.9990	7.9990	7.9972	5.76945	6.60523	7.15899

6-5 Execution Time:

The execution time for both encryption and decryption of proposed system is less that original AES, are shown in the Tables (5,6)

Table (5) Execution Time of the Proposed System (image)

Image	The Execution Times for the Proposed AES algorithm and Original AES	
	Proposed AES	Original AES
Encryption Time	20.946687	195.883332
Decryption Time	18.998631	234.801734

Table (6) Execution Time of the Proposed System (text)

Characters message	The Execution Times for the Proposed AES algorithm and Original AES			
	Proposed AES		Original AES	
	Encryption Time	Decryption Time	Encryption Time	Decryption Time
50	16.39133	15.59233	16.62481	15.60569
100	16.36625	15.50162	16.48356	15.82751
250	16.28597	15.49413	16.60452	15.95109

7- Conclusion

E-mail provides an important means of communication between users or security ministries that wish to send confidential data or military images. In this paper was proposed E-mail system secure capable of providing a high level of security for contents message and speed in encryption and decryption between two parties by Internet without the need to security networks in addition to compatible with all MailServers.

References

- [1] Gurpal Singh Chhabra, Dilpreet Singh Bajwa” **Review of E-mail System, Security Protocols and Email Forensics** ” ISSN:2249-5789, Dilpreet Singh Bajwa et al, International Journal of Computer Science & Communication Networks, Vol 5(3),201-211.
- [2] Mohammed Hassouna, Nashwa Mohamed, Bazara Barry and Eihab Bashier,” **An End-to-End Secure Mail System Based on Certificateless Cryptography in the Standard Security Model**” IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 3, March 2013 ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784
- [3] Julian Jang, Surya Nepal and John Zic “**Trusted Email Protocol: Dealing with Privacy Concerns from Malicious Email Intermediaries**” 978-1-4244-2358-3, 2008 IEEE.
- [4] Mazen Tawfik Mohammed, Alaa Eldin Rohiem, Ali El-moghazy and A. Z. Ghalwash, “**Chaotic Encryption Based PGP Protocol**”, International Journal of Computer Science and Telecommunications, Volume 4, Issue 2, February 2013.
- [5] Noura Aleisa,” **A Comparison of the 3DES and AES Encryption Standards**”, International Journal of Security and Its Applications Vol.9, No.7 (2015), pp.241-246.
- [6] Sadiq A. Mehdi, Abid Ali H. Alta’ai and Salim Ali ABBAS, “**Bifurcation and The Influence parameters On A Novel Chaotic Dynamic System**”, ISSN: 19948638,(2015), Volume: 7 Issue: E1 Pages: 83-92.
- [7] Sadiq A. Mehdi and Rabiha Saleem Kareem, “**Using Fourth-Order Runge-Kutta Method to Solve Lü Chaotic System**”, American Journal of Engineering Research (AJER), e-ISSN: 2320-0847 p-ISSN: 2320-0936, (2017), Volume-6, Issue-1, pp-72-77.
- [8] Nishtha Mathur and Rajesh Bansode,” **AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection**”, Science Direct, Procedia Computer Science 79 (2016) 1036 – 1043.
- [9] Katie Ho, Akhil Nistala, Kevin Tu,” **End-To-End Message Encryption for Tinder**”, May 11, 2016.

- [10] Qinqin Wu, Guangyi Wang and Liping Yuan, "E-mail Encryption Based on Dual Chaotic Map", 2010 International Workshop on Chaos-Fractal Theory and its Applications, 978-0-7695 4247-8/10 2010 IEEE DOI 10.1109/ IWCFTA.2010.24.
- [11] Sadiq A. Mehdi, Abid Ali H. Alta'ai and Salim Ali ABBAS, "Analysis of A Novel Chaotic Dynamic System with ten quadratic nonlinearities", IOSR Journal of Mathematics (IOSR-JM), e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 11, Issue 2 Ver. IV (Mar - Apr. 2015), PP 40-46.
- [12] G. A. Leonov, N.V. Kuznetsov" On differences and similarities in the analysis of Lorenz, Chen, and Lu systems", Applied Mathematics and Computation 256 (2015) 334–343.

Image Denoising Based on Modify Radial Basis Function Neural Network and Noise Estimation Level

Dr. Haider K. Hoomod¹

Saja Hikmat Dawood²

¹Computer Science Dept., Mustansriyah University, drhjnew@gmail.com

²Institute for Postgraduate Studies, UOITC, saja20146@gmail.com

Abstract:

Artificial neural networks (ANNs) have been applied in many areas successfully because of their ability to learn, ease of implementation and fast real-time operation. In this research, there are proposed two algorithms. The first is Modify Chaos-Radial Base Function Neural Network with noise level estimation (MCRBFNN-NLE). While the second is Radial Base Function Neural Network with noise level estimation (RBFNN-NLE). The proposed MCRBFNN modification by adding the Rossler chaos to the MRBFNN centers calculations in order to increase the learning speed and adjusted the centers selection operation efficiency. Noise level algorithm were used to image noise removal approach in order to get a good image denoising processing with high quality image visual and statistical measures. The proposed algorithm consists of three stages, firstly dividing the noisy image into 16 parts. Second stage estimate noise density and level by using the estimation technique (singular value decomposition neural network (SVD-NN) for each part in parallel. Thirdly, applying an intelligent modified denoising techniques based on (modified chaos-radial basis function neural network (MCRBFNN-NLE) or (RBFNN-NLE)) for each part in parallel and depending on noise estimation from second stage.

The results of the proposed system show that the combination of chaos MCRBFNN with noise level estimation gives acceptable PSNR and MSE with a best quality visual vision and small computational time.

Keyword: image denoising; noise level estimation; Radial Base Function network; Rossler chaos, MRBFNN.

I. Introduction

Digital image has become an integral part of daily life applications, because of its visual information, digital image use in different area of research and technology such as medical analysis like use of X-ray, MRI image, and geographical system, earth science, astronomy, space science, military application [1], digital camera, Satellite television [2].

major problems that lead to Degradation of images quality are noise and blurring, where the noise are undesirable data leads to differences in image intensity, noise can happen to images during transmission, receiving, noise caused by many factors such sensor high temperature and low lights level, etc. [1], in other hand, the blur effect I image caused by some image processing and motion of camera or objects during the capturing [3].

Denoising is essential step before further processing, there are various approaches for image denoising, such as use of Spatial Domain filtering that divide into linear filtering and nonlinear Filtering, this approach are good in term of speed but not in term of preserve edge information, another approach was engineering. To use transform domain filtering [4], for example Wavelet transform techniques that divides to other modes and filters This approach is not good in term of speed but good in term of preserve edge information [4].

For these reasons, the trend has been to use artificial intelligent techniques satisfying results on terms of noise removing and performance, such intelligent techniques are fuzzy logic, neural network, and genetic algorithm [5].

Artificial neural networks (ANNs) used in many fields successfully because their ability to learn, ease of implementation and fast real-time operation [6], using cellular neural network and radial bias function provide a good image denoising and a high-quality image from the degraded version not only in terms of visual perception but also in terms of the quality metrics [7] [8].

Xinzhong Zhu and et al, in 2009 [9], present a repair of degraded image with noise and motion bluer by applying radial basis function neural network (RBFNN). This is accomplished first by

taking away the noise using (RBFN) interpolation with variable stabilization, regulation parameters which is proportional to the sound level at each pixel. That controls two conditions in the first place cost term work, that measured the space (information and the required arrangement). The next term, is used to measure the smoothness and the connected cost. In the second step, the movement obscured image is reestablished in the view of the modernized recognizable proof of the course and length of the obscure movement. The obscured image movement is restored based on the automatic identification of the movement obscure direction. At that point, we can consequently discover its obscured length movement. That is built up as dark district appearing at particular interims in the recurrence area of the obscured image movement. Furthermore, a method (in light of thing extraction), for reestablishing nearby obscured image movement is given to illuminate the state of the terrible renovation which comes about when the worldwide obscured attributes movement are skipped for neighborhood movement obscured images. Test comes about exhibit, implements suggested technique and executes well after connected to obscured image movement. The reclamation calculation of the may give precise distinguishing proof of the corrupted model and great rebuilding comes about, even under the state of generally expansive commotion impedance.

Sander Ali Khowaja, Syed Zafi Sherhan, Muhammad Usman memon, in 2014[10], propose the using of radial basis function neural network (RBFNN) to reduce the effect of noise and blurring from the image. it is similar to multilayer perceptron (MLP) with only one difference contains single hidden layer and applying Gaussian's activation functions in the hidden layers. The RBF center selection acts as a problem that can be overcome by using orthogonal least square which is the solution of function activation, that makes orthogonal least's square method an efficient implementation with set construction of vectors of orthogonal in the spaces covered by the hidden vector unit activation for automatically selected number of neurons in a hidden layer. The results, showed that RBFNN perform better than MLP.

Mohammed Debakla, Khalifa Djemal, Mohamed Benyettou, in 2015 [11], proposed the use of radial basis function neural network (RBFNN) for medical images denoising. This is accomplished by minimization of the total variation (TV (error)) and the use of neighborhood information of center pixel as an input to the network and the output is single denoising pixel. Training of the proposed RBF network is achieved by the back propagation algorithm for determining the optimal weights and centers. These optimal parameters are obtained by minimization of an appropriate error function. In the initial step, the center values are computed by K-means clustering algorithm. They proposed a filter for reducing noise from Mammographic medical, X-Ray and MRI images to get a good visual quality with strong noise removal and more details are preserved.

II. Radial Basis Function (RBF) Neural Network

A feedforward neural network (FNN), the neurons in feed forward networks are best related to the next layer neurons. These unidirectional connections mean that the processed data will pass through one direction of the network layers. Example of it are back propagation (BP), Multilayer perceptron (MLP), radial foundation function neural network (RBFNN) [12].

A feedback (recurrent) neural network (RNN) have signal travels in bi-directional introduced loops. Values from the hidden and output layers propagating backwards to the other layer. They were powerfully operational tool but is complicated [12]. Example of it are Hopfield, Elman, Jordan, bi-directional and other networks [13]. Figure (1) shows the Topology of FNN and RNN.

A radial basis function (RBF) networks are 3-layers supervised feed forward networks which use a non-linear activation functions (commonly Gaussians) for the unhidden layers and a linear passing function for the outputs layers. The Gaussian function processes the input sets for neurons to provide a radials functions of the distances among patterns vectors and each hidden weights vectors. Each output unit implements a weighted sum of hidden gadgets' outputs.

RBFs network inherently flexible in length and topologies, makes it more powerful to different troubles. RBF networks were correctly implemented to some of visual's processing and analyses' problem, inclusive of analyses of 3D structure [12].

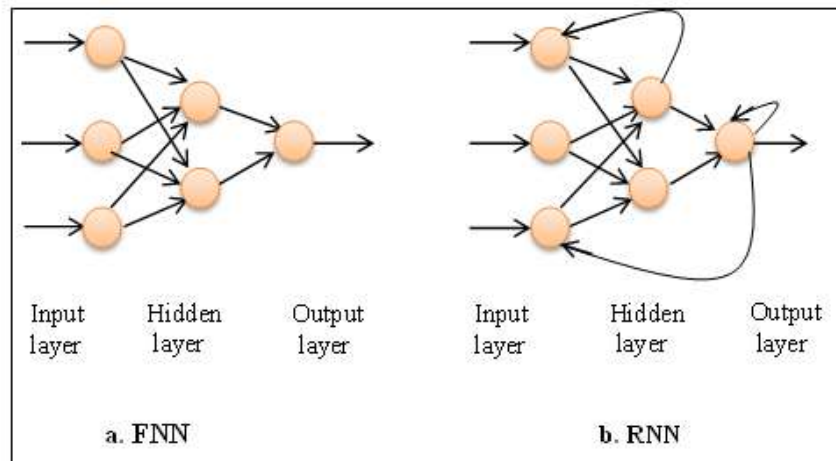


Fig. (1): Topology of simple (a) FNN (b) RNN

The input to unhidden layers are linearly combinations of weight and the inputs vectors $[x_1, x_2, \dots, x_n]^T$, while weights are pointed to unities value. The input vectors are mapped using the radials basis's functions in all unhidden nodes. The linear combination between hidden- layer and output-layer has vectors of $[y_1, y_2, \dots, y_n]^T$. Figure (2), illustrates the single output "RBFNN" structure; the network output can be received with the aid of:

$$y = f(x) = \sum_{i=1}^h w_i \phi_i(x) \dots \dots \dots (1)$$

Where: The final outputs are $f(x)$, the radials basis functions of the i^{th} unhidden nodes is $\phi_i(.)$, the hidden to output weights of the i^{th} unhidden nodes is w_i , and hidden nodes number are h .

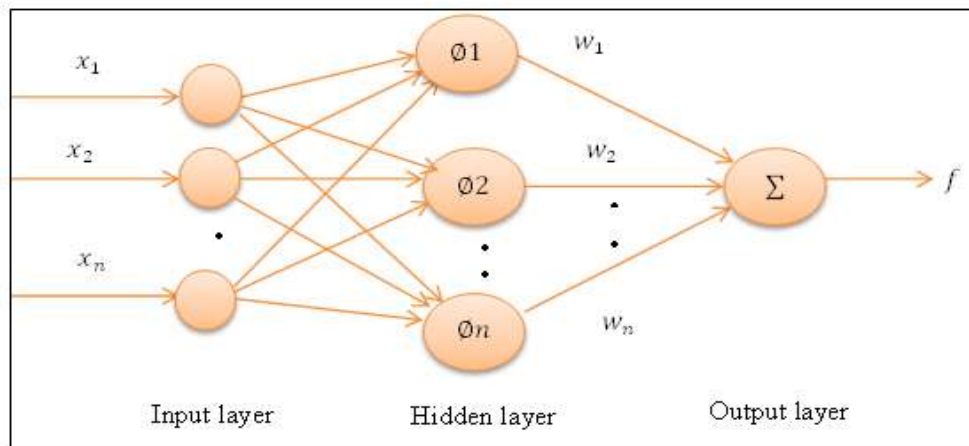


Fig. (2): Structure of single output RBFNN

A radials basis functions are multi-dimensional functions which can describe distances among given input vectors and predefined center vectors. Many radial basis function types [11], e.g. the thin plate splines $\phi(r) = r^2 \log(r)$, the Gaussians' $\phi(r) = \exp(-\xi r^2)$ and other, where ξ is a parameter [14]. A normalize Gaussian's functions usually is used as the radials basis function and is given by:

$$\phi_i(x) = \exp \left[\frac{-\|x - c_i\|^2}{2\sigma_i^2} \right] \dots \dots \dots (2)$$

where c_i and σ_i refer to the centers and spread's width of the i^{th} nodes. The parameters of an RBFNN must be initialized before training the network. The weight vector $\{w_j, j=1, 2, \dots, M\}$ could

be initialized to zeros or small random values. The initialized centers could determine, for example, by K-means cluster of number of input samples. Spread initial values σ_i could be chosen as the average of the nearest neighbor distance between the initialized centers and trained later, or fixed during the training process; this parameter is generally fixed after multiple learning experimentations.

The input to the RBFNN is the degraded image u_0 and RBFNNF output is the images compatible to the desired images u . The output of the network is formulated by:

$$u = N(u_0, w_i, c_i) \dots \dots \dots (3)$$

Where: u_0 is the noisy images representing pixel (x, y) intensity and its neighborhoods. The gray level of the output of each pixel $u_0(x, y)$ is calculated by:

$$N(x, y) = \left(\sum_{i=1}^h w_i \exp \left[\frac{-\|v_o(x, y) - c_i\|}{2\sigma_i^2} \right] \right) \dots \dots \dots (4)$$

Where $V_0(x, y)$ is the neighborhood pixels' gray level values corresponding to the pixel $u_0(x, y)$. The window's size of the neighborhood could be 3×3, 5×5, 7×7 and etc. [11]. The training process can be summarized by two steps:

The beginning, the centers of the hidden layer and weights vectors are determining, the use of handiest enter fact sets and with the aid of utilizing unsupervised training algorithm along with okay-method, decision bushes and self-organizing feature maps .

Second, the output weights (the hidden-output layer connections) are configured by using each input-output information and by using singular values decomposition (SVD) or least means squared (LMS) algorithms. Comparing to back-propagation training, both steps are highly speedy [40].

III. Singular Value Decomposition Neural Network (SVD-NN)

The structure of SVD-NN are shown in figure (3), where the result from dividing image, then elect a fix size image blocks number have minimum standard-deviation comparing with other blocks. Then blocks SVD were feed as the inputs of the neural networks, the output of training neural network is noise standard deviation (unknown noise intensity).

By using SVD-NN, and computing the singular value decomposition for each block from dividing stage and then input to BPNN input layer, the dimensions of the input-vector determines the number of the neural network input-nodes; Hidden layer nodes represent the network model's complexity, and it generally is determined by the number of input nodes. The problem complexity and the training samples; Output layer is the predicted standard deviation of noise. hidden-output layer neuron transfer function is tan-sigmoid function.

$$a = \text{tansig}(n) = \frac{2}{1 + e^{(-2 \times n)}} - 2 \dots \dots \dots (5)$$

It maps the input interval $[-\infty, +\infty]$ to the output interval $[-1, 1]$. The training algorithm of the network is using the Levenberg - Marquardt algorithm, and its main strategy is to do the linear approximation which use the model function to estimate the parameters of the vector in its neighborhood, ignoring the second order derivative term. So as to convert

The problem to linear least squares problems, which has fast convergent rate, and possesses the advantages of gradient method and Newton method [15]. Figure (3), illustrates noise estimation algorithm framework based on neural network.

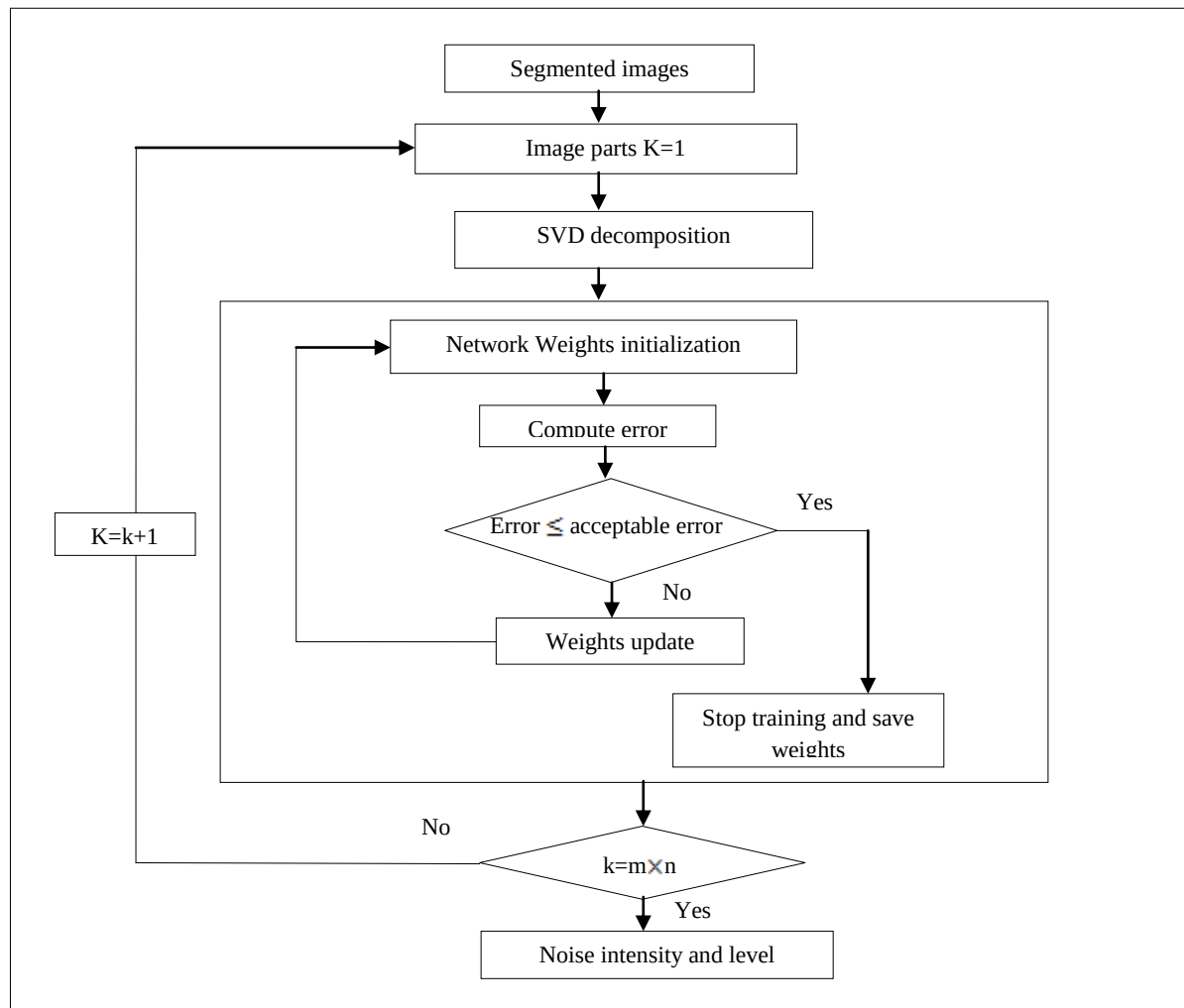


Fig. (3): Noise estimation algorithm framework based on Neural Network

IV. The Fast Image Denoising Proposed System

The goal of this proposed system is to removing or decreasing (as possible) different noise types from the colored image quickly as possible by using two approaches: first approach is Modified Chaos Radial Basis Function Neural Network (MCRBFNN) and Noise Level Estimation for Blind Denoising algorithm named MCRBFNN-NLE. The second approach is RBFNN and Noise Level Estimation for Blind Denoising algorithm named RBFNN-NLE. The noise level estimation help selecting the threshold of learning operation (in both MCRBFNN -NLE and RBFNN -NLE), also discover the noise level in each image block. If the image block has noise free, the RBFNN-NLE and MCRBFNN-NLE are neglect it and take the next block.

Estimation algorithm is choosing low rank patches from images (without high-frequency) affected by different noises (like Gaussian and salt & pepper).

The patches are select depend on the gradient and their statistical measures. The selected patches used to estimate noise levels by apply the using SVD-NN. Because the noise levels don't constantly give the better performances for non-blind denoising methods.

In this proposed system a new modify to MCRBFNN by using the chaos system. The Rossler chaos equation output were added to two position in RBFNN, first in activation function and the second location is in the output calculation equation to adjusted the input and output of the RBFNN and make it more dynamic and flexible in image denoising, this increase the MCRBFNN speed in learning and denoising operation. The Rossler chaos equations used are:

$$x(t) = -y - z(t) \dots \dots \dots (6)$$

$$y(t) = x(t) + a y(t) \dots \dots \dots (7)$$

$$z(t) = b + z(t)(x(t) - c) \dots \dots \dots (8)$$

Where (x, y, z) are the three variables that evolve in the continuous time t and (a, b, c) are three parameters [15]. In this proposed system, the RBFN network was modified to achieve the best results of denoising operation. The activation equation (2) mentioned above modified to be:

$$\phi_i(x) = \exp \left[\frac{-(\|x - c_i\| + m(IB)) - R}{2\sigma_i^2 + wm(IB)} \right] \dots \dots \dots (9)$$

Where: IB is an image block the w is the weight of the IB pixels calculated from the IB mode 3. And $m(IB)$ is the median value of IB after ordering and R is the Rossler chaos output.

Two modifications were proposed, the first is activation of the hidden layer by adding the median of the order IB ($m(IB)$) multiplied by weight (w) of IB pixels calculated from the average IB mode 3. The second modification was by adding $\sigma wm(IB)$ to the equation (1) to better optimize the output of the network. The noise level estimation are feed into RBFNN for denoising, the algorithm for that as mention in chapter (2).

$$y = f(x) = \sum_{i=1}^n w_i \phi_i(x) + \sigma wm(IB) + R \dots \dots \dots (10)$$

Where σ is the adjusted parameter with range 0 to 1. These steps illustrate proposed MCRBFNN:

Input: 16 parts (noisy image blocks ($NIBs$))

Output: denoised image

Step 1: Start

Step 2: Read the 16 parts (noisy image blocks ($NIBs$)) data

Step 3: Apply the SVD-NN algorithm to estimate the noise level estimation (NLE) value for each part in parallel.

Step 4: Check if noise estimation NLE for the first (NIB) smaller than the threshold σ , then it represent noise existence then apply steps from (4 to 9) to denoise the image. If not then apply step 7.

Step 4: Initialization of network Weights

Step 5: Applying the activation equation using equation (9)

Step 6: Calculate the output of the network by applying equation (10).

Step 7: Check if all NIBs finished then apply step (8 and 9), else repeat steps from (2 to 4) to all noisy image blocks (NIBs).

Step 8: Composed all 16 parts to produce the denoised image

Step 9: End.

Fig. 4. Shows the general proposed system block diagram. The threshold value for MCRBFNN - NLE are $\alpha = 80$, $\beta_1 = 85$, and $\beta_2 = 93$, selected according to experiments. And value of the three parameter are $a = 0.1$, $b = 0.1$, $c = 14$.

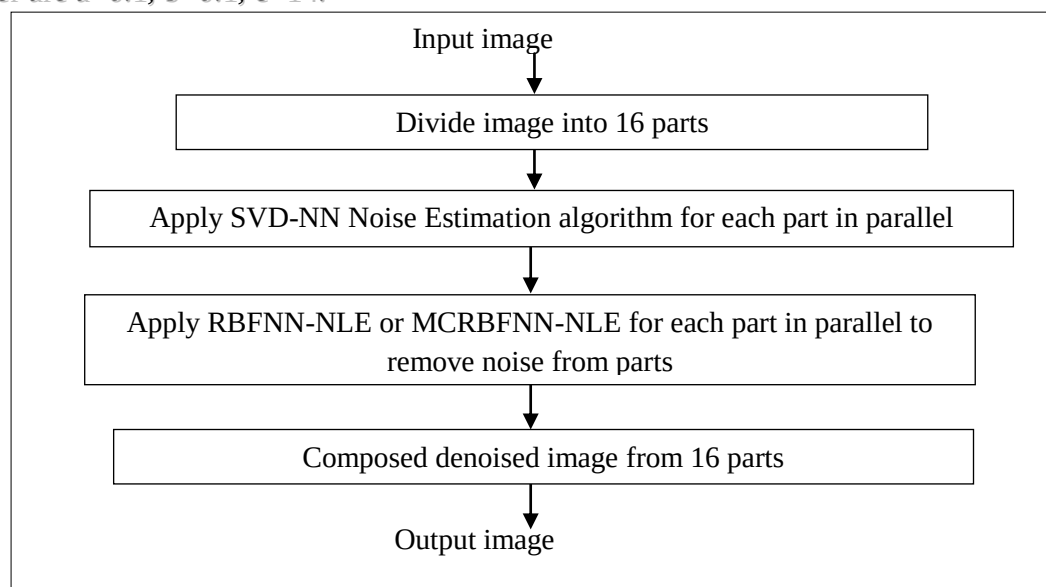


Fig. (4): The proposed system block diagram.

V. Result And Discussion

From the results, the performances of the proposed approaches (MCRBFNN-NLE and RBFNN-NLE) contain combination from artificial neural network, chaos system, and noise estimation level that have been proposed to use in this research is investigated with simulations and give a very good results for removing noise. Also, denoising is carried out for image with noise of variance types. The proposed algorithm has the best nonlinear filtering possible due to the MCRBFNN and noise estimation level, the mask replace noisy pixels depend on MCRBFNN decision (depend on a noise distribution template like salt & pepper noise distribution) and the content of the neighbor pixels values in the image part.

For quantitative measurement PSNR and MSE are used, where MSE is the cumulative square-error root between original and denoised images pixels as following:

$$total\ error = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \|x(i,j) - y(i,j)\|^2 \dots \dots \dots (11)$$

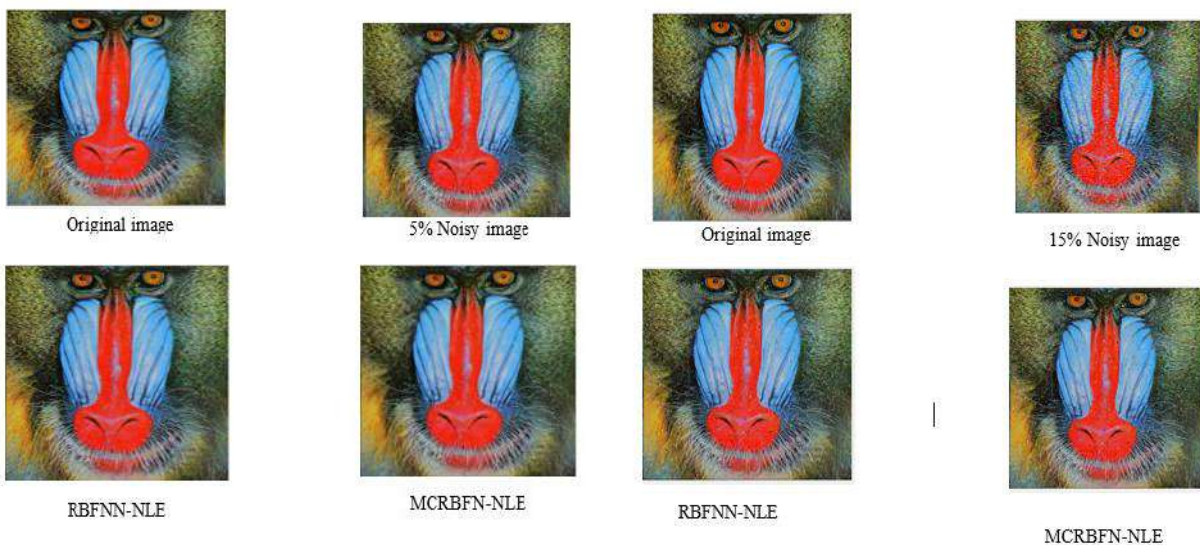
$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \|x(i,j) - y(i,j)\|^2 \dots \dots \dots (12)$$

Where $x(i,j)$ represent original image and $y(i,j)$ represent the restored (denoised image). $m \times n$ is the size of image. While the PSNR is the ratio between signal max possible power and the distorting noise power (the MSE between the origin signals and the de-noising signals) which affects the quality of its representation, and defined by:

$$PSNR = 20 \log \left(\frac{MAX_x}{\sqrt{MSE}} \right) \dots \dots \dots (13)$$

Where MAX_x is the max original image signal value. The proposed methods are implemented using some tested images sample with different noise ratio. From Fig. 5. We can note that, when the noise ratio increase (like 80% or more) the denoised image will have small noise but its acceptable vision. This remaining noise due to the heavy corrupt to the colors in noisy image and average color is not correct. But under these ratios the denoised image is better vision with high quality.

The performance of the different denoising samples with different size is compared in Tables 1 and 2. Accordingly, showing that MCRBFNN-NLE provide better result in PSNR value than RBFNN-NLE, and the MSE for the MCRBFNN-NLE is smaller than RBFNN-NLE, while the time of denoising for MCRBFNN-NLE is a little bit smaller than RBFNN-NLE. And it's clear (from results), the MCRBFNN-NLE better from the RBFNN-NLE in visual vision and statistical results.



(a) S1 with 5% noise level (b) S1 with 15% noise level



(c) S2 with 35% noise level (d) S2 with 80% noise level

Fig. (5): some proposed system results with different noise ratios. (a)S1 sample denoising results (5% salt & pepper noise). (b) S1 sample denoising results (15% salt & pepper noise). (c) S2 sample denoising results (35% salt & pepper noise). (d) S2 sample denoising results (80% salt & pepper noise).

Table (1) The Proposed System Measures (Noise 5%)

Image Sample	Image Size	MCRBFNN-NLE			RBFNN-NLE		
		MSE	PSNR (db)	Denoising Time (sec)	MSE	PSNR (db)	Denoising Time (sec)
S1	640 ×800	2.34	46.45	2.240	3.21	41.00	2.780
S2	600×500	2.22	49.56	1.932	2.78	45.10	2.041
S3	1280×800	3.43	49.70	3.670	4.10	45.30	3.900
S4	1200x1120	4.44	49.98	4.234	4.90	45.20	4.800
S5	1280 ×768	3.68	46.35	3.341	5.31	43.21	4.301
S6	600x800	2.40	47.56	1.000	3.10	43.10	1.120

Table (2) The Proposed System Measures (Noise 35%)

Image Sample	Image Size	MCRBFNN-NLE			RBFNN-NLE		
		MSE	PSNR (db)	Denoising Time (sec)	MSE	PSNR (db)	Denoising Time (sec)
S1	640 ×800	5.80	36.15	5.190	6.34	31.56	5.563
S2	600×500	9.78	35.90	3.219	10.78	33.23	3.547
S3	1280×800	13.30	34.12	5.890	15.25	31.46	6.213
S4	1200x1120	12.78	35.11	4.111	16.61	32.60	4.727
S5	1280 ×768	13.19	32.12	3.216	17.11	31.78	3.989
S6	600x800	7.98	33.67	2.871	12.22	32.32	3.320

VI. Conclusion

In this paper, we have presented two intelligent approaches for image denoising based on radial basis function neural network (RBFNN) with noise level estimation and modify Chaos- radial basis function neural network (MCRBFNN) with noise level estimation. Experimental results show that the proposed modified MCRBFNN-NLE get a best result from RBFNN-NLE in quantitative and qualitative measurement even with presence of high noise ratio due to the effects of the modifications and chaos in the learning operation and selection activations.

References

- [1] A. Pandey, Dr. K. K. Singh, "Analysis Of Noise Models In Digital Image Processing", *International Journal Of Science, Technology & Management*, Vol. 04, No. 01, May, 2015, pp. 140-144.
- [2] N. Agrawal, Dr. G. R. Sinha, "A Survey On Fuzzy Based Image Denoising Methods", *International Journal Of Engineering Research & Technology (IJERT)*, Vol. 4, No. 05, May, 2015, pp. 528-531.
- [3] J. Patil, S. Jadhav, "A Comparative Study Of Image Denoising Techniques", *International Journal Of Innovative Research In Science, Engineering And Technology*, Vol. 2, No. 3, March, 2013, pp. 787-794.
- [4] S. Kaur, E. R. Singh, "Image De-Noising Techniques: A Review Paper", *International Journal For Technological Research In Engineering*, Vol. 2, No. 8, April, 2015, pp. 1649-1653.
- [5] R. Pushpavalli and G. Sivarajde, "An Artificial Intelligent Technique For Image Enhancement", *International Journal Of Signal Processing, Image Processing And Pattern Recognition*, Vol. 6, No. 4, August, 2013, pp. 143-164.
- [6] Ş. Sağiroğlu, E. Beşdok, "A Novel Approach For Image Denoising Based Onartificial Neural Networks", *Journal Of Polytechnic*, Vol. 15, No. 2, 2012, pp. 71-86.
- [7] T. Saba, A. Rehman, G. Sulong, "An Intelligent Approach To Image Denoising", *Journal of Theoretical And Applied Information Technology*, Vol. 17, No. 1, 2005, pp. 32-36.
- [8] M. Debakla, K. Djemal And M. Rebbah, "MRI Image Denoising Approach Based On TV And Neural Network Filter", *Proceedings of 2015 International Conference On Image Processing, Production And Computer Science (ICIPCS'2015)*, Istanbul (Turkey), Vol. 3, No. 4, June 2015, Pp. 23-30.
- [9] X. Zhu, Et Al., "Noisy Motion-blurred Images Restoration Based on RBFN", *Journal of Research and Practice in Information Technology*, Vol. 41, No. 3, August 2009, pp. 195-207.
- [10] S. A. Khowaja, S. Z. S. Shah, M. U. memon, "Noise Reduction Technique For Images using Radial Basis Function Neural Networks", *Mehran University Research Journal of Engineering & Technology*, Vol. 33, No. 3, July 2014, pp. 278-285.
- [11] M. Debakla, K. Djemal, M. Benyettou, "A Novel Approach for Medical Images Noise Reduction Based RBF Neural Network Filter", *Journal of Computers*, JCP, Vol. 10, No. 2, March 2015, pp. 68-80.
- [12] J. Jiang, P. Trundle and J. Ren, "Medical ImageAnalysis with Artificial Neural Networks", *Computerized Medical Imaging and Graphics*, Vol. 34, No. 8, December 2010, pp. 617-631.
- [13] K. Suzuki, "Artificial Neural Networks Methodological Advances And Biomedical Applications", *InTech*, April 2011.
- [14] S. Pyatykh, J. Hesser, and L. Zheng, "Image Noise Level Estimation by Principal Component Analysis", *IEEE Transactions On Image Processing*, Vol. 22, No. 2, February 2013, pp. 687-699.
- [15] W. Zhiming, Y. Guobin, "Image Noise Level Estimation by Neural Networks", *International Conference on Materials Engineering and Information Technology Applications (MEITA)*, 2015, pp. 692-697.

Region of Interest Detection Using Scale Invariant Feature Transform

Dr. Ekhlas Khalaf Gbashi¹

Suha Mohammad Saleh²

University of Technology, Computer Science Dept.

¹110026@uotechnology.edu.iq

²suha74.2016@gmail.com

Abstract:

There are a lot of image processing applications which required detection, description and matching specific regions of the image which are called (ROI) in order to depend on it for making a special decision according to the application field. For this reason a lot of detection algorithms are used.

One of the main algorithms that are used to make detection and description is SIFT algorithm. The SIFT algorithm is efficient in making detection, and description of ROI because it works on large keypoints set but the main problem of SIFT algorithm is that it is required time to complete the processing of detection and description.

In the proposed system the SIFT algorithm is used to perform detection, description and matching of the ROI. In the proposed system the input image will be processed before applying the SIFT algorithm to it. The proposed system contains two stages. First stage: reducing the detail of the image by applying blurring on the image before SIFT algorithm works on it in order to make the work of the SIFT algorithm more efficiently and speed it up. The second stage: reducing the matching number with the use of the Fast Approximate nearest neighbors(FANN) matching algorithm (k-mean tree) is used to make the match SIFT algorithm work faster since the FANN algorithm will reduce the number of matching for the SIFT algorithm.

The proposed system is evaluated according to the measures that are used in detection, description and matching fields which are time and accuracy measures. The proposed system achieves (100 %) accuracy since the detection is identical. Also, the proposed system reduces the required time that SIFT algorithm needs for making the detection, description and matching of the ROI.

Keyword: invariant features, region of interest, scale invariance, image matching

اكتشاف المنطقة المهمة باستخدام خوارزمية تحويل الصورة الغير مرتبطة بمقياس

د. اخلاص خلف كباشي سها محمد صالح

المستخلص

هنالك الكثير من تطبيقات معالجة الصور التي تتطلب الكشف ووصف ومطابقة مناطق محددة من الصور تسمى (المنطقة المهمة) من اجل الاعتماد عليها لاتخاذ القرار وفقا لحقل التطبيق. لهذا السبب نستخدم العديد من خوارزميات الاكتشاف.

واحدة من الخوارزميات الرئيسية للكشف والوصف هي خوارزمية تحويل الصورة الغير مرتبطة بمقياس خوارزمية التحويل الغير مرتبطة بمقياس تكون كفوءة لكشف، و لوصف المنطقة المهمة لانها تعمل على عدد كبير من النقاط المفتاحية لكن المشكلة الرئيسية لخوارزمية التحويل الغير مرتبطة بمقياس هو انها تتطلب وقت كبير لاكمال المعالجة للكشف والوصف.

في النظام المقترح، خوارزمية التحويل الغير مرتبطة بمقياس تستخدم للكشف، والوصف، والمطابقة للمنطقة المهمة. في النظام المقترح، الصورة المدخلة ستعالج قبل تطبيق خوارزمية (التحويل الغير مرتبطة بمقياس) عليها. النظام المقترح يتضمن مرحلتين: الاولى هي تقليل التفاصيل للصورة الداخلة باستخدام متوسط الضبابية قبل تطبيق خوارزمية (التحويل الغير مرتبطة بمقياس) عليها مما يجعل خوارزمية (التحويل الغير مرتبطة بمقياس) تعمل بكفاءة وسرعة. المرحلة الثانية هي تقليل عدد نقاط المطابقة باستخدام تقنية التقريب السريع لاقرب جار (متوسط الشجرة) مما يؤدي الى السرعة في عملية المطابقة لان خوارزمية التقريب السريع لاقرب جار تقلل من نقاط المطابقة لخوارزمية (التحويل الغير مرتبط بمقياس).

لتقييم النظام المقترح تم الاعتماد على قياس الوقت والدقة للكشف والوصف والمطابقة. النظام المقترح حقق نسبة دقة 100%. وايضا في النظام المقترح تم تقليل الوقت المطلوب لخوارزمية (التحويل الغير مرتبط بمقياس) لاجراء الكشف والوصف والمطابقة. **الكلمات المفتاحية:** الصفات الثابتة، المنطقة المهمة، المقياس الثابت، مطابقة الصور.

1- Introduction

Extracting and matching properties is one of the most common issues facing the computer vision field, like object identification or structure from movement. Property detection and image matching are considered as two significant problems in computer vision, graphics, photogrammetric and the majority of images applications. Their application keeps growing in different areas daily. [1].

Object identification is the task that is concerned with finding a specific item in an image or video sequence. It is considered as an important issue facing systems of computer vision. Generally, the process of object identification has the following phases: property deduction and property matching. In computer vision, the Scale-Invariant Feature Transform (SIFT) is a method for the identification and characterization of local image properties. It offers the ability of precise object recognition with low possibility of mismatching and is easy to be matched against a large data-base of local properties. The representation of the image properties has a great effect on the results of an object identification system [2].

Regions of Interest are defined as the areas that contain user defined items of significance, and a sufficient algorithm is produced to detect such areas [3].

In this study a suggested approach that depends on the algorithm of SIFT in finding the Region of Interest in image. Moreover, in the suggested approach this algorithm has been developed for the sake of giving better results in terms of precision and speed measures.

2- Background

2.1 SIFT (Scale-invariant Feature Transform)

SIFT was introduced by David Lowe. As it is clear from its name, this algorithm's reason is transforming the image-data into SIFT coordinates related to the local properties. Lowe benefitted from the properties for the sake of executing matching procedures between distinct images of the same scenes or objects.

The extracted properties are independent of the image rotating and scaling, and they off every strong matching over a basic domain of affine distortion, three-dimensional viewpoint change, adding noise and changing in lightness. In addition, the properties are very distinctive, which means that one property might be properly matched with high degree of probability against a large property data-base.

For matching a new image, each property extracted from the new image is compared separately to the properties that are stored in the data-base. [4]

2.1.1 Feature Extraction

A set of local properties of an image is extracted from every image. Each of those properties includes a registry of it's:

- Position, or pixel location (x, y) , of the image.
- Scale, characterized by the standard deviation σ .
- Orientation, the dominating direction of the image structure in the neighborhood.
- Detailing of the image's local structure, characterized according to gradient histograms.[4]

The main steps of computation implemented for generating the group of properties are:

• **Detecting the local extrema of the scale-space**- the property positions are set as the local extrema of Difference of Gaussian pyramid. For building the pyramid of DOG the input image undergoes convolution in an iterative manner with a Gaussian kernel of $\sigma = 1.6$. The last image that was convolved undergoes down-sampling in every one of the image directions by factor equal to 2, and the convolving procedure is done again. This process is performed over and over until the down sampling is no longer possible. Every group of images of identical sizes is known as an octave. All octaves construct together the DOG pyramid that is given by a three dimensional function $L(x, y, \sigma)$. The Difference of Gaussian pyramid $D(x, y, \sigma)$ is calculated from the difference of every 2 neighboring images in DOG pyramid. The local extrema (maxima or minima) of Difference of Gaussian function are found via the comparison of every one of the pixels with its 26 adjacent pixels in the scale-space (8 neighbors in the same scale, 9 corresponding neighboring pixels in the scale above and 9 neighbors in the scale below). The searching for extrema eliminates the 1st and

the last image in every one of the octaves due to the fact that they don't have a scale above and a scale below [5].

- **Localizing the key-points**- the found local extrema are efficient nominees for keypoints. On the other hand, they should be precisely localized via fitting a three dimensional quadratic function to the scale-space local sampling point. The quadratic function is calculated with the use of a 2nd order Taylor expansion that has the origin at the sample point. Afterwards, local extrema of low contrast and such that corresponds to edges are gotten rid of due to the fact that they're of high sensitivity to noise [6].

- **Assigning the orientation**—as soon as the SIFT-property index is set, a main direction is given to every one of the features according to local image gradients. For every one of the pixels of the area surrounding the property position the gradient magnitude and direction are calculated according to:

$$M(X, Y) = \sqrt{(L(X+1, Y, \partial))x^2 + (X, Y+1, \partial) - L(X, Y-1, \partial))x^2} \dots (1)$$

$$\theta(X, Y) = \arctan((1(x, y+1, \partial)) - 1(x, y-1)) / (l(x=1, y, \partial) - l(x-, y, \partial)) \dots (2)$$

The gradient magnitudes are weighted by a Gaussian window which is of size that is dependent on the property octave. The weighted gradient magnitudes are used for establishing a direction histogram having 36 bins that cover the 360° direction range. The highest orientation histogram peak and peaks with amplitudes higher than 80% of the highest peak are utilized for the sake of creating a keypoint with this direction. Thus, there will be more than one key-point generated at the same position but with varying directions [7].

- **Descriptor of the Keypoint**- the area that is surrounding a key-point is split into 4×4 boxes. The gradient magnitudes and directions in every one of the boxes are calculated and weighted by suitable Gaussian window, and the coordinate of every one of the pixels and its gradient direction undergo rotation according to the key-points direction. Afterwards, for every one of the boxes an 8 bins direction histogram is determined. From the 16 constructed direction histograms, a 128D vector (SIFT-descriptor) is constructed. This descriptor is independent of the direction, due to the fact that it is computed according to the main direction. Lastly, for the sake of achieving the independence from variation in lighting, the descriptor undergoes normalization to unit length [6].

2.2. Mean Blurring

The main mechanism of this filter is replacing every one of the pixel values in an image with the mean ('average') value of the pixels that surround it, and that includes itself. This has the effect that eliminates pixel values that are not representative of their neighbors. This kind of filtering is typically considered as a convolution filter. Such as other kinds of convolution it is dependent on a kernel that reflects the shape and size of the neighborhood that will be sampled when computing the average. Usually a 3×3 square kernel is applied, even though kernels of larger sizes (such as 5×5) might be applied for stronger degree of smoothing. (It is important to take under consideration that a small kernel might be used repeatedly for the sake of producing a similar but not identical result as one pass with a larger kernel). Mean filtering is called Box filtering and average filtering as well. illustrate in figure(2) apply blurring.[8]

2.3. Fast approximate nearest neighbor

Nearest neighbor (NN) search is an essential issue in the area of computer vision, image retrieval, data mining, and so on. The problem can be depicted in the form:

$$X^* = \operatorname{argmin}_{X \in D} \rho(X, Q) \dots (3)$$

Where $D = \{X_1, \dots, X_n\} \subset \mathbb{R}^d$ is a dataset, Q is a query, and ρ is a distance measurement.

A simple solution to the nearest neighbor search issue is computing the distance from the query to each of the points in the data-set and return the nearest of them. This method is known as the linear searching approach and is guaranteed to find the precise NN. The computation complexity of the linear search method is $O(nd)$, where n is the size of the data-set and d is the dimensionality. This complexity might be costly for large data-sets. The issue to find the precise NN has led to developing of the approximate NN search algorithms. [9]

2.4. Random Sample Consensus Based Algorithms (RANSAC)

It is a hypothesis generating and verifying algorithm for robust property estimation. As with the RHT, RANSAC starts by randomly choosing n points from the image for generating a nominee structure defining a specific property. Afterwards, RANSAC classifies each point as either “inlier” which falls within a specific distance of the candidate structure, or “outliers” that gets eliminated. In the case where the number of inliers grows over a predetermined threshold, the inliers are utilized for re-estimating the property model. [RANSAC1]

RANSAC is an iterative algorithm that can be implemented for estimating parameters of a statistical model from a group of observed data that includes outliers. [10]

3- Test Materials of the Propose System

A set of digital images have been used as test materials to assess the performance of the propose algorithm. These images are classified into 2 groups, 18 for each type as shown in Table (1) all these test material are color image files of png type.

Table (1) Test image

No	Name of group	Number Of Samples
1	Car plate image	18
2	various image	18

4- Propos system structure

Mainly the proposed system is consisting from 4 main steps figure (1):

- Mean blurring
- Sift
- Fast approximate k-mean tree

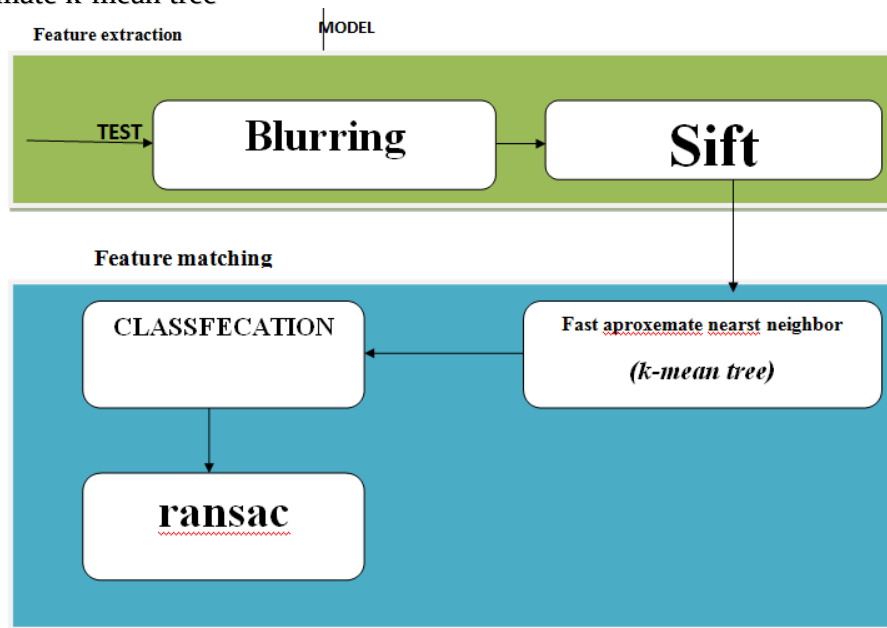


Fig. (1): Steps of proposed system

5- Implementation of the Proposed System

5.1. Blurring

In this stage applying mean blur (on model and test image) will be done to make the image look smooth or reduce detailed, as shown in figure (2).



Fig. (2): Apply mean blurring

5.2 Scale invariant feature transform

In this stage the SIFT algorithm will be implemented on the image in order to detect the ROI and provide diagnosis of the required information and provide complete description about this information. Then the extracted features will be used in the next stages.

5.3 Fast Approximate K-Means

Computing the distance from the query to each of the single points in the SIFT result keypoints and return the nearest one will lead to discard some points that considered far from group of keypoints. as shown in figure (3) and figure (4).

5.4 Ransac algorithm

This algorithm is applied to bounder the key points (final keypoints) obtained from the SIFT and then from propose algorithm, the algorithm is work by choosing points from specified image and generate candidate structure of the wanted property, in our system the points selected are the keypoints and minimum three points needed to define specific property (ROI), this algorithm can be applied to (original SIFT, propose algorithm or any image). Illustrate in figure (5).

6- Proposed System Evaluation

The system is applied on (24 picture) as a dataset and the result is discussed reference to 12 pictures as sample for each group in dataset.

Table (2) show (left column) matching result with original SIFT, (right column) matching result with propose algorithm to (car plate image).

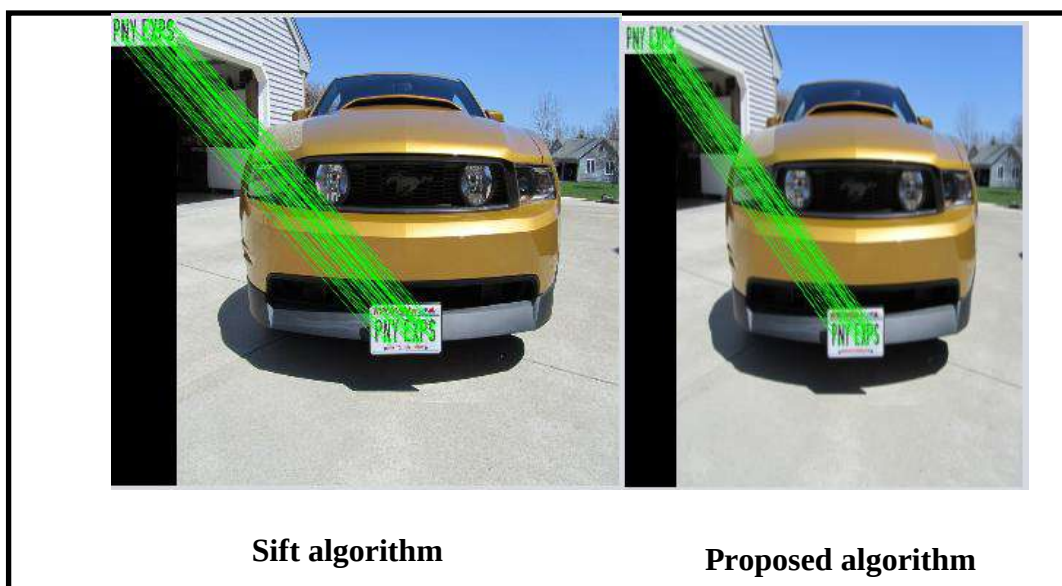
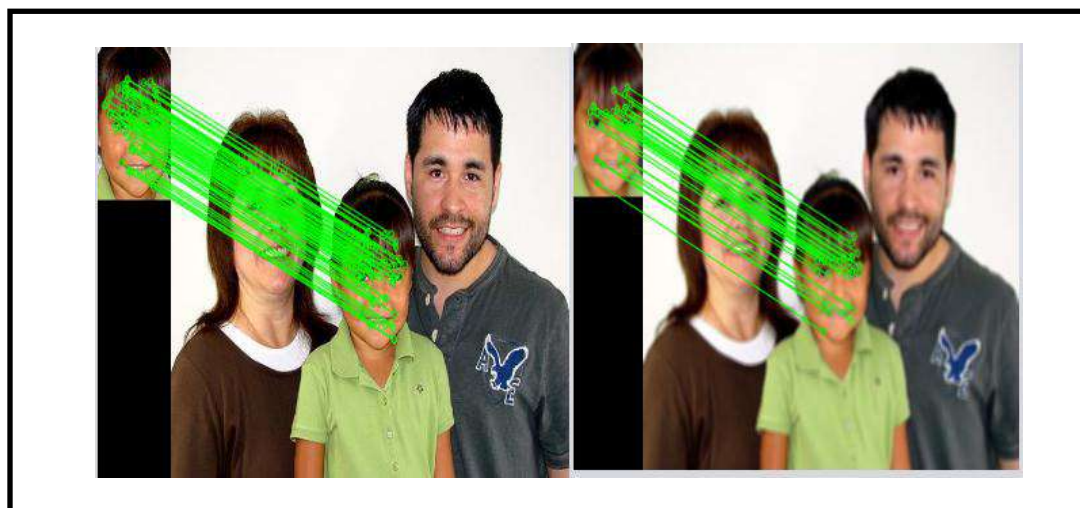


Fig. (3): Feature matching (Car plate image)



Sift Propose system
Fig. (4): Feature matching (various image)

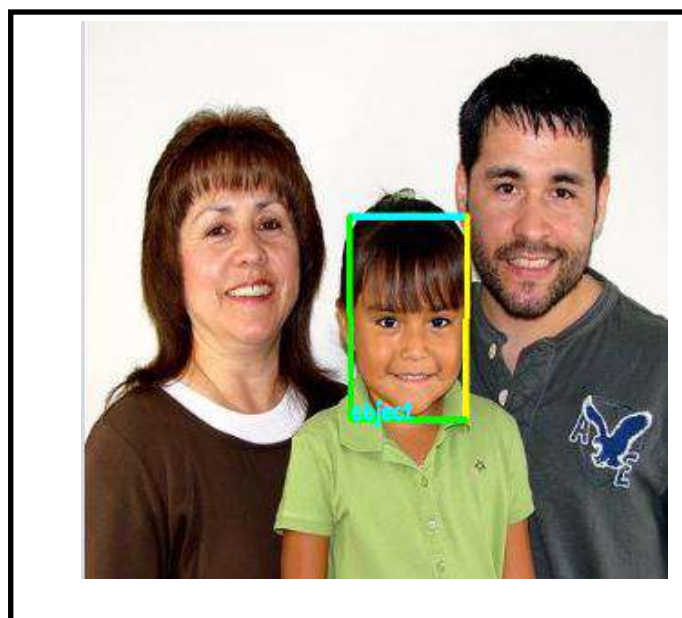


Fig.(5): boundary ROI

Table (4) show (left column) matching result with original SIFT, (right column) matching result with propose algorithm to(various image).

all the images matched and the ROI is detected and recognized.

Tables(3),(5) show Comparison the results (Number of key point,matching time) for applying the original sift and the propose algorithm to(car plate image and various image).

Table (2) Matching Car Plate Image





Image3

Image4

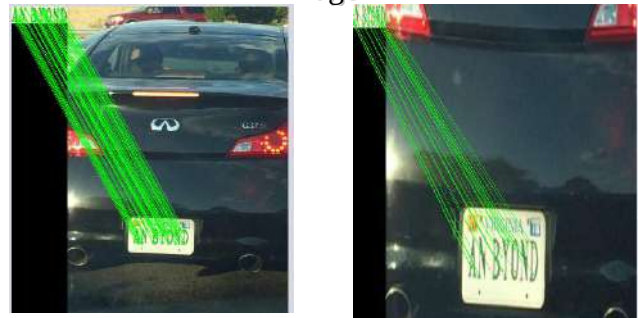


Image5

Image6

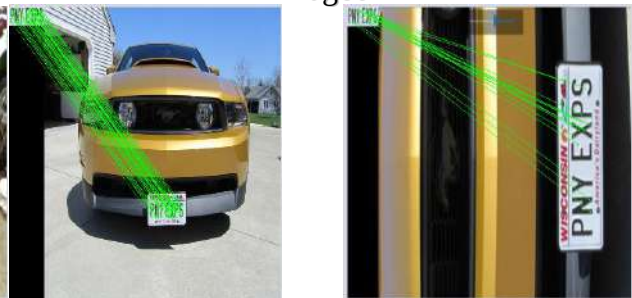


Image7

Image8

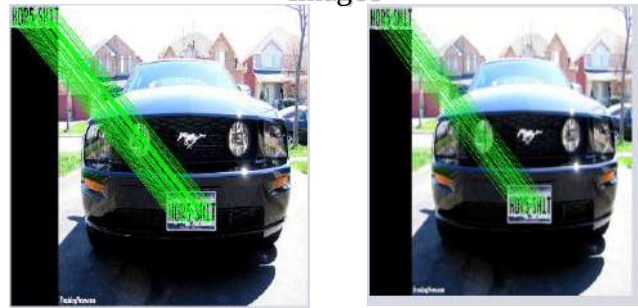


Image9

Image10



Image11

Image12

Table (3) Comparison the results (Number of key point,matching time) for applying the original sift and the propose algorithm to (car plate image).

NO image	KEY POINT OF IMAGE (sift)	KEY POINT OF IMAGE (Propose system)	Matching key point (sift)	Matching key point (Propose system)	Time (second) (sift)	Time(second) (Propose system)
1	615	262	52	23	5.692	6.385
2	1745	658	44	29	8.633	10.586
3	2992	6587	31	19	8.962	12.712
4	574	342	54	27	1.97	2.171
5	2789	922	66	25	6.21	7.041
6	2432	579	63	33	9.528	12.821
7	3560	1384	61	31	6.519	8.051
8	1109	565	73	48	6.925	7.799
9	1890	371	59	36	4.594	5.178
10	3299	1171	110	55	8.799	10.356
11	3596	1237	43	30	11.227	14.161
12	1094	395	44	16	9.729	10,677

Table (4) Matching various Image

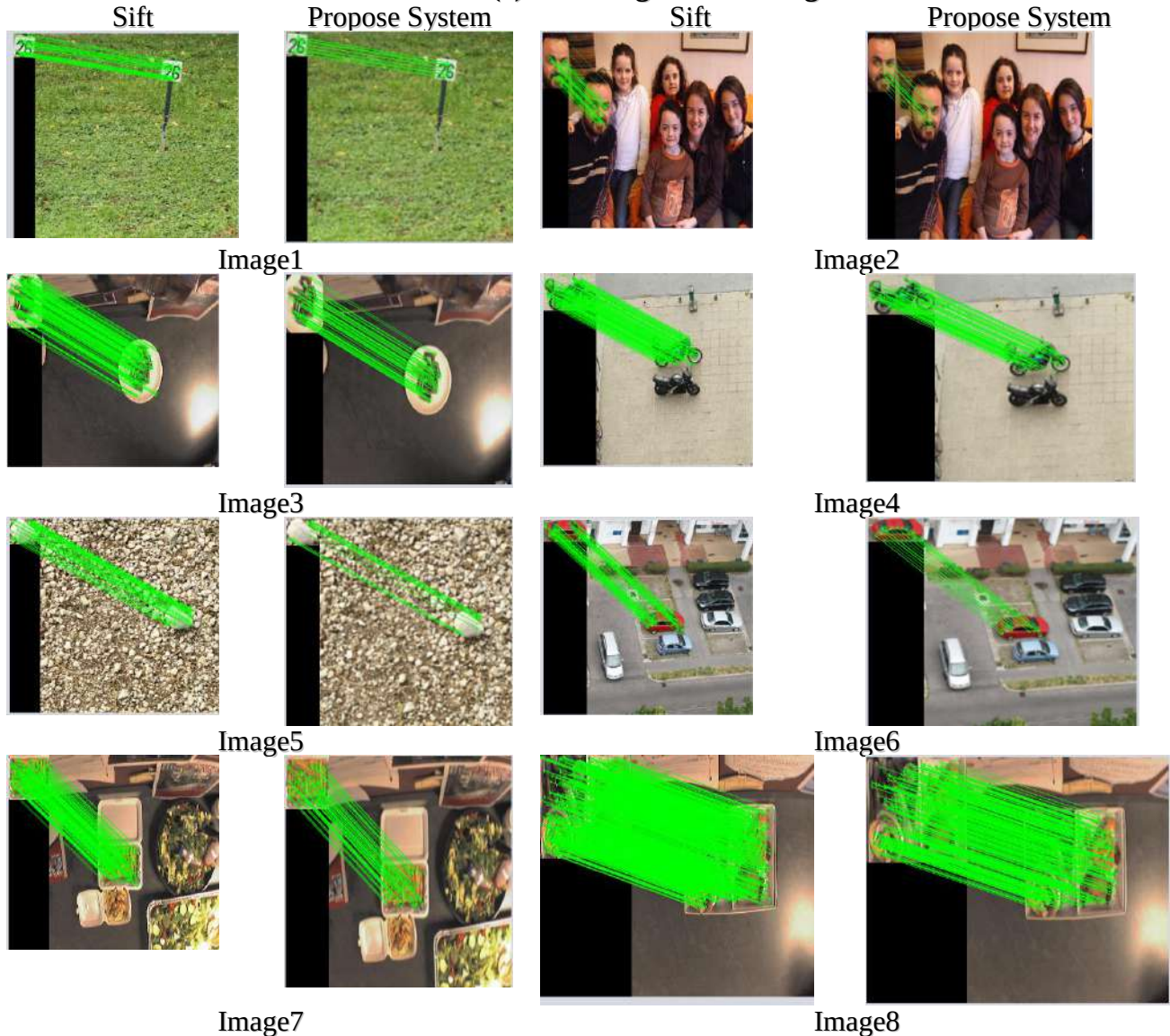




Image9



Image10

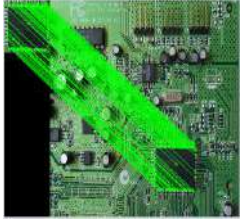
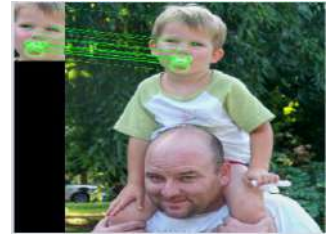
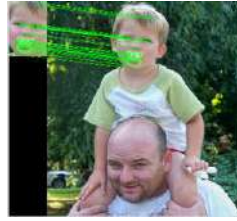


Image11

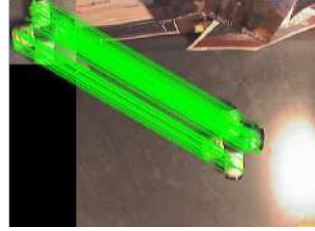


Image12

Table (5) Comparison the results (Number of key point, matching time) for applying the original sift and the propose algorithm to (various image)

NO image	KEY POINT OF IMAGE (sift)	KEY POINT OF IMAGE (Propose system)	Matching key point (sift)	Matching key point (Propose system)	Time (second) (sift)	Time(second) (Propose system)
1	5195	1752	29	16	2.819	1.696
2	2317	766	64	26	1.066	0.91
3	491	180	158	62	0.73	0.617
4	589	249	156	65	1.007	0.862
5	7131	4352	56	16	4.109	3.198
6	1509	509	51	18	2.369	1.84
7	2329	1185	207	81	3.748	3.078
8	587	297	64	29	2.245	1.809
9	2142	1221	62	29	10.656	9.509
10	5219	3665	156	25	11.874	10.386
11	5195	1752	29	16	2.819	1.696
12	2317	766	64	26	1.066	0.91

Conclusion:

- 1-The proposed system can extract many types of ROI, for this reason it can be applied on many fields that needs ROI detection, description and matching like face recognition, industry fields, etc.
- 2-The proposed system can minimize the number of keypoints and determine only the important keypoints which allow the system to make the detection, description and matching of the ROI in very quickly way.
- 3- The main problem of the SIFT algorithm is that it required time to provide the detection, description and matching of the ROI. So to avoid this problem blurring and fast approximation matching algorithm is used.

References:

- [1] K. Mikolajczyk, C. Schmid, "A Performance Evaluation Of Local Descriptors". *IEEE Trans Pattern Anal*, 27(10)1615–30, 2005.
- [2] T. Yuehua, S. Marjorie, H. Tony, X. Youming, and Ch. Xiaoxiao, " Performance Evaluation of SIFT-Based Descriptors For Object Recognition".34(8)160-39,2010.
- [3] H. Sunhyoung, "Object-Based Regions of Interest For Image Compression".67(6),34-67,2010.
- [4] D. G. Lowe "Distinctive image features from scale-invariant keypoints". *International journal of computer vision*,60(2) 91-11,2004.
- [5] P. Vinukonda, "A Study of The Scale-Invariant Feature Transform On A Parallel Pipeline". *Proc. 9th IEEE International Conference on Computer Vision*, 5-14, 2011.
- [6] W. Ouyang, F. Tombari, S. Mattoccia, D. Stefano, L. W. Cham, "Performance Evaluation of Full Search Equivalent Pattern Matching Algorithms". *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 34 (1)127-143, 2012.
- [7] D. Kim, S. Rhoand, E. Hwang, "Local Feature Base Multi-Object Recognition Scheme Forsurveillance".*Engineering Applications of Artificial Intelligence*, 25 (7), 1373–1380, 2012.
- [8] Das. Sanjib, "Study and Analysis of Digital Image Enhancement"/ (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (3), 2841-2848, 2015
- [9] D. G. Lowe, "Object Recognition From Local Scale-Invariant Features". *Computer vision, The proceedings of the seventh IEEE international conference on*. Vol. 2. IEEE, 1150-1157, 1999.
- [10] G. D. Konstantinos, "Overview of the RANSAC Algorithm". kosta@cs.yorku.ca, Version 1(2), 1-2, 2010.

A Comparative Study between BM25 and TF-IDF for Feature Extraction on Twitter

Ammar Ismael Kadhim¹, Yu-N Cheah², Baydaa Jaffar Al-Khafaji³ and Salah Talib⁴

¹Department of Computer Science College of Medicine University of Baghdad,
ammarusm70@gmail.com

²School of Computer Sciences Universiti Sains Malaysia Penang, Malaysia, Bjkh68@yahoo.com

³Computer Science Department College of Education for Pure Science/ Ibn Al-Haitham University of Baghdad, yncheah@usm.my

⁴Information Technology Center Social Protection Authority Ministry of Labour and Social affairs
salah.mymobile@yahoo.com

Abstract:

Feature extraction is to transform a text document from any format into a list of features that can be easily processed by supervised machine learning techniques. Term weighting, which calculates term (feature) values in text documents, is one of important preprocessing techniques in feature extraction. Thus, efficient feature extraction methods such as the BM25 and term frequency-inverse document frequency (TF-IDF) methods are commonly used in text classification. However, BM25 is not a single function, which is used to overly penalize very long documents. This may not represent the usefulness or significance of certain keywords, and decreases the precision of classification. This paper is a comparative study of feature weighting methods in feature extraction. Two methods were evaluated, including BM25 and TF-IDF to weight and extract the feature. We have evaluated these methods on Twitter. In this paper, TF-IDF feature extraction method is introduced, which solves the problem mentioned above. The experimental results showed that the TF-IDF outperforms BM25 with respect to the performance evaluation metrics.

Keywords: Feature extraction, supervised machine learning, term weighting, TF-IDF, BM25.

دراسة مقارنة بين TF-IDF و BM25 لاستخراج ميزة على تويتر

م.د. عمار اسماعيل كاظم ا.د. يان شياه ا.م. بيداء جعفر الخفاجي صلاح طالبالمستخلص

المستخلص:

هو استخراج ميزة تحويل مستند نص من أي تنسيق إلى قائمة بالميزات التي يمكن معالجتها بسهولة بواسطة الجهاز تحت إشراف تقنيات التعلم. مصطلح الترجيح، التي تقوم بحساب مصطلح القيم (سمة) في المستندات النصية، واحدة من تقنيات الهامة في استخراج ميزة وهكذا، ميزة كفاءة أساليب الاستخراج مثل BM25 ومصطلح الوثيقة معكوس التردد التردد (TF-IDF) من الأساليب التي تستخدم عادة في تصنيف النص مع ذلك، فان BM25 هي ليست الدالة الوحيدة التي تستخدم بافراط متعاقب في الوثائق الطويلة جداً. وهذا قد لا يمثل فائدة أو أهمية لبعض الكلمات الرئيسية ويقلل من دقة التصنيف. وهذه الورقة دراسة مقارنة لميزة الترجيح في استخراج ميزة. تم تقييم اثنين من الأساليب، بما في ذلك BM25 (TF-IDF) الوزن واستخراج ميزة وفي هذه الورقة قمنا بتقييم هذه الأساليب على تويتر، وعرض طريقة استخراج ميزة (TF-IDF) الذي يحل المشكلة المذكورة أعلاه. وأظهرت النتائج التجريبية بتفوق (TF-IDF) على BM25 فيما يتعلق بمقاييس تقييم الأداء.

1. Introduction

The increasing development of multimedia technologies, storage capacity and computational power, together with the growing and diversification of telecommunication technologies, has allowed us to receive different kinds of information supported by different kinds of media [1]. Today, a huge amount of information is available on the Internet such as those from Twitter, Facebook and LinkedIn. These information, which are stored as unstructured texts, cannot immediately be processed by computers. Therefore, specific preprocessing methods and algorithms are required in order to extract useful patterns. Text mining is generally defined as the process of extracting interesting and non-trivial features and knowledge from unstructured text documents [2].

This scenario contributed to an explosion of available information, and demanded the construction

of huge multimedia databases. In order for those databases to be useful, data should be organized and stored in such a way that the access to that information be efficient and effective. Taking into account the dimension of such databases, this is only possible with the development of automatic methods to process, organize and analyze the data.

A case in point refers to textual media, more so now that short-text communication from social media applications, such as Twitter (<http://www.twitter.com>) is heavily used as a source of communication on the Internet. It provides a platform for users to post short messages or “tweets” for followers to read on Twitter. Due to the large volume of tweets in diverse topics, the classification of tweets on Twitter [3] proves to be challenge.

In the context of the classification of tweets, feature extraction is an important step in the process of classifying text automatically and effectively. Term frequency-inverse document frequency (TF-IDF) is commonly used to weight and extract the feature. While BM25 is a ranking function used by search engines to rank matching documents according to their relevance to a given search query. This paper presents a comparative between BM25 and TF-IDF methods for feature extraction. The extracted features could represent the content of the text better and has better recognition ability. Experimental results show that the TF-IDF perform better than BM2 with respect to evaluation metrics.

2. Feature Extraction Using BM25

BM25 can be defined as a ranking function that ranks a set of text documents based on the query terms that occur in each text document, regardless of the interrelationship between the query terms within a text document. This function is not a single function, but essentially a whole family of scoring functions with marginally different components and parameters [4]. It is utilized by search engines to rank matching text documents according to their relevance to a given search query and is frequently referred to as “Okapi BM25.” The BM25 information retrieval formula function belongs to the BM family of retrieval models, which is the weight of a term t in a text document d . Given a query Q containing keywords $[q_1, q_2 \dots q_n]$, the BM25 score of the document D using Equation 1 as given by [5] is as follows:

$$BM25 = score(D, Q) = \sum_{i=1}^n IDF(q_i) \cdot \frac{f(q_i, D) \cdot (k_1 + 1)}{f(q_i, D) + k_1 \cdot (1 - b + b \cdot \frac{|D|}{avgdl})} \dots\dots\dots (1)$$

Where $f(q_i, D)$ is q_i 's TF in the document D . $|D|$ is the length of the document in terms of words. $avgdl$ is the average length of the document in the text collection from which the documents are drawn. k_1 and b are free parameters. Selection in the absence of an advanced optimization, such as k_1 in $[1.2, 2.0]$ and $b = 0.75$. $IDF(q_i)$, involves the inverse document frequency (IDF) weight of the query term q_i using Equation 2, as given by [6] as follows:

$$IDF(q_i) = \log \frac{N - n(q_i) + 0.5}{n(q_i) + 0.5} \dots\dots\dots (2)$$

Where $n(q_i)$ is the number of documents containing q_i , and N is the number of documents. Thereafter, the weights of the shortest feature results using the BM25 function can be summarized as follows:

- Step 1: Define an initial keyword set for each category of documents.
 - Step 2: Transform all documents into numerical features, and label the keyword by category ID.
 - Step 3: Calculate the IDF function for each document.
 - Step 4: Calculate the BM25 function for each document.
 - Step 5: Perform classification on the obtained numerical data and label the document with the category ID.
 - Step 6: Calculate the initial accuracy depending on the confusion matrix.
 - Step 7: Update the keyword set by adding and/or removing keywords in the current keyword set.
 - Step 8: Repeat from Step 2.
- This process is continued until the desired classification accuracy is obtained.

3. Feature Extraction Using TF-IDF Method

Feature extraction is an important step in text mining, and provides information regarding the texts such as the highest and lowest term frequency for each document. Selecting relevant features and determining how to encode them for machine learning can have a big impact on the learning machine's ability to extract a good model [7]. Term weighting can be as simple as a binary representation or as complex as a mix of terms and existing datasets.

TF-IDF is a widely known and often used weighting method, and its performance remain even comparable with novel methods. In TF-IDF term weighting, the text documents are characterized as transactions. Choosing the keyword for the feature selection process is the main preprocessing process necessary for the indexing of documents.

In this study, the TF-IDF method used to weight the terms in the term-document matrices of the evaluation dataset. A keyword may appear in different topics or categories, which leads to variability. This variability can be defined as the degree of variations in keywords according to the different categories that include this keyword. A common practice to avoid this variability or, at least, to reduce the possible impacts resulting from it, is the normalization of the TF-IDF scores for each document in the collection by using the Euclidean norm. The calculations for TF-IDF are shown in Equations (3) [8].

$$(TF - IDF)_i = (TF)_i \times (IDF)_{ij} \dots\dots\dots(3)$$

However, Equation (1) is only used in situations when $(TF) \geq 1$. Otherwise, $TF-IDF = 0$ (see Equation(4)).

$$TF - IDF = \begin{cases} TF \times IDF \geq 1 \\ 0 & \text{otherwise} \end{cases} \dots\dots\dots(4)$$

Where term frequency (TF) refers to normal weighting. It defines the weight, i , which is the frequency or the relative frequency of the word, t_i within a specific tweet, j .

Inverse document frequency (IDF) refers to global weighting. It defines the support of the word t_j with respect to the collection of tweets.

In this paper, TF-IDF term weighting is used for feature extraction.

However, prior to the assessing the term frequency, preprocessing is first carried out to remove stop words (conjunctions, pronouns, etc.), URLs, special characters, usernames, punctuations, HTML tags, etc. After preprocessing, the keywords, representing the categories for the tweets, are obtained. Then, the tweet is transformed to numerical features by counting the number of occurrences (called term frequency) of the keywords in the tweet and the keyword co-occurrences. The keywords are selected depending on a set threshold for each collection of tweets. It is important to choose the intended keywords that carry the meaning of the tweet, and reject others that do not [9]. Following this, the keywords (or features) from the individual tweets are combined.

The entire feature extraction process is listed as follows:

Step 1: Define an initial keywords set for each class of tweets.

Step 2: Transform all tweets to numerical features, and label the keyword by category ID.

Step 3: Calculate the TF-IDF

Step 4: Perform classification on the obtained numerical data and label the tweet with the category ID.

Step 5: Calculate the initial accuracy depending on the confusion matrix.

Step 6: Update the keyword set by adding and/or removing keywords in the current keyword set.

Step 7: Repeat from Step 2.

This process continues until the desired classification accuracy is obtained.

4. Experiments and Results

A small dataset of 2,196 tweets were obtained from twelve general classes: politics (210 tweets), education (180 tweets), health (200 tweets), marketing (194 tweets), music (150 tweets), news & media (170 tweets), recreation & sports (190 tweets), computers & technology (192 tweets), pets (180 tweets), food (200 tweets), family (170 tweets) and others(160 tweets); and were also filtered

based on location (via Where On Earth ID (WOEID)): New York, and Toronto. The dataset was collected using a streaming application programming interface (API) across different time intervals. This dataset was then used to train the classifier for classifying new tweets.

Since Twitter is the primary source from which the streaming API collected the tweets, each tweet in the dataset is then tagged or labeled with one of the eleven general classes. If the tweet is not related to any category, then the tweet will be classified as "other".

The data collected for New York and Toronto is shown in Figure1.

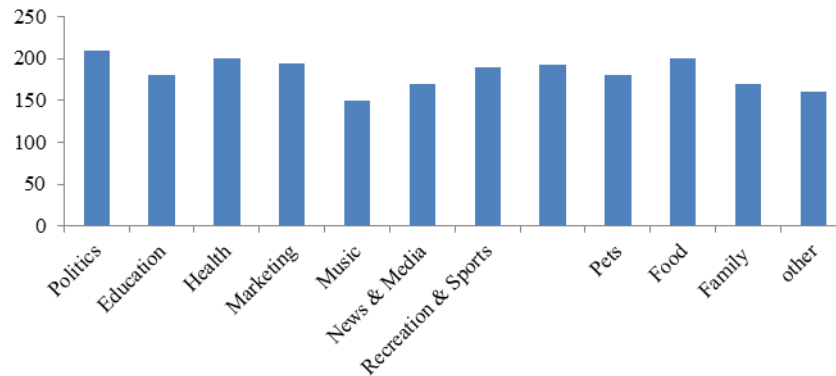


Fig. (1): The distribution of 2,196 tweets across 12 classes for New York and Toronto.

There are many metrics to assess the effectiveness of the classification. The most commonly used are accuracy, precision and recall [2].

1. Accuracy (Acc.): Is the ratio between the number of tweets which were correctly categorized and the total number of tweets.

$$Acc_i = \frac{TP_i + TN_i}{TP_i + TN_i + FP_i + FN_i} \dots\dots\dots (5)$$

where TP_i (true positives) is the number of tweets correctly identified in for a particular category, TN_i (true negatives) is the number of tweets correctly identified as not belonging to a particular category, FP_i (false positives) is the number of tweets incorrectly identified for a particular category, and FN_i (false negatives) is the number of tweets incorrectly identified as not belonging to a particular category [2].

2. Precision (P): Is the percentage of correctly categorized tweets among all tweets that were specified to the category by the classifier.

$$P_i = \frac{TP_i}{TP_i + FP_i} \dots\dots\dots (6)$$

3. Recall (R): Is the percentage of correctly categorized tweets among all tweets belonging to that category.

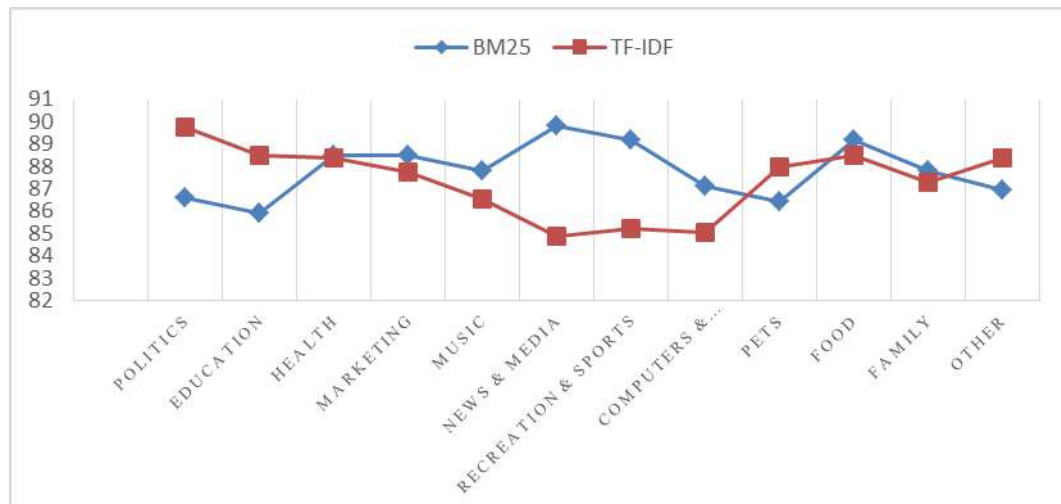
$$R_i = \frac{TP_i}{TP_i + FN_i} \dots\dots\dots (7)$$

Subsequently, another dataset of 1,200 tweets, with 100 tweets per category, was collected for testing purposes. Table 1 shows the results of the classification using the two methods, i.e. BM25 and TF-IDF. Figure 2 shows the performance comparison graph between the BM25 and TF-IDF methods with respect to the F1-measure.

Table (1) Performance of classification using BM25 and TF-IDF.

Category	BM25				TF-IDF			
	Acc.	P	R	F1	Acc.	P	R	F1
Politics	78.00	86.59	86.59	86.59	82.00	90.80	88.76	89.77
Education	77.00	86.42	85.37	85.89	80.00	88.51	88.51	88.51
Health	81.00	87.95	89.02	88.48	80.00	86.36	90.48	88.37
Marketing	81.00	86.90	90.12	88.48	79.00	87.21	88.24	87.72
Music	80.00	87.80	87.80	87.80	77.00	85.06	88.10	86.55
News & Media	82.00	90.80	88.76	89.77	75.00	85.37	84.34	84.85
Recreation & Sports	80.00	88.51	88.51	88.51	75.00	83.72	86.75	85.21
Computers & Technology	80.00	86.36	90.48	88.37	75.00	85.54	84.52	85.03
Pets	78.00	86.42	86.42	86.42	80.00	85.88	90.12	87.95
Food	82.00	89.16	89.16	89.16	81.00	90.12	86.90	88.48
Family	80.00	86.75	88.89	87.80	79.00	87.80	86.75	87.27
Other	79.00	86.42	87.50	86.96	80.00	90.48	86.36	88.37

Note: Acc. = accuracy, P = precision, and R = recall

**Fig. (2)** Comparison between BM25 and TF-IDF with respect to F1-measure.

Overall, the findings show that the maximum value of F1-measure is 89.16 using BM25. While the maximum value of F1-measure is 89.77 using TF-IDF. Moreover, The TF-IDF is more stable than BM25 for all categories based on F1-measure.

5. Conclusion

Two feature extraction methods were presented, i.e. BM25 and TF-IDF, and were evaluated based on datasets collected from Twitter. The results showed that the TF-IDF method is better than the BM25 with respect to the F1-measure. Our experimental results also reveal that feature weight methods react on the effectiveness of Twitter. Moving forward, the proposed work can be further expanded into a larger framework for text classification. This allows the inclusion of dimensionality reduction and machine learning approaches.

References

- [1] C. Macdonald, I. Ounis, **“The TREC Blogs06 collection: Creating and analysing a blog test collection,”** Department of Computer Science, University of Glasgow, Technical Report TR-2006-224, 2006.
- [2] A. T. Sadiq, S. M. Abdullah, **“Hybrid Intelligent Techniques for Text Categorization,”** International Journal of Advanced Computer Science and Information Technology (IJACSIT), vol. 2, no. 2, pp. 23-40, 2013.
- [3] J. Fiaidhi, S. Mohammed, A. Islam, S. Fong, T.-H. Kim, **“Developing a Hierarchical Multi-Label Classifier for Twitter Trending Topics,”** International Journal of u- and e- Service, Science and Technology, vol. 6, no. 3, pp. 1-12, 2013.
- [4] Lu, W., Robertson, S., & MacFarlane, A. (2005). Field-weighted XML retrieval based on BM25, 161-171, Springer.
- [5] Papineni, K. (2001). Why inverse document frequency?. The second meeting of the North American Chapter of the Association for Computational Linguistics on Language technologies, 60(5), 503-520.
- [6] S. Ramasundaram, S. P. Victor, **“Text Categorization by Backpropagation Network,”** International Journal of Computer Applications, vol. 8, no. 6, pp. 1-5, 2010.
- [7] J. Chen, H. Huang, S. Tian, Y. Qu, **“Feature selection for text classification with Naïve Bayes,”** Expert Systems with Applications, vol. 36, no. 3, pp. 5432-5435, 2009.
- [8] F. Debole, F. Sebastiani, **“Supervised term weighting for automated text categorization,”** in S. Sirmakessis (Ed.), Text mining and its applications, Springer, 2004, pp. 81-97.
- [9] F. Debole, F. Sebastiani, **“Supervised term weighting for automated text categorization,”** in S. Sirmakessis (Ed.), Text mining and its applications, Springer, 2004, pp. 81-97.

New approach to image encryption depend on substitutions operation and DNA computing

Assist. Prof. Dr. Matheel Emadaldeen Zena Mohammad Saadi
University of technology-computer science department
Dralaa_cs@yahoo.com

Abstract:

In cryptography, an S-box (substitution-box) is a basic component of symmetric key algorithms which performs substitution. In block ciphers DNA computing has prevailed in the field of cryptography. DNA cryptography uses DNA as an information transporter and gets benefit from biotechnology in order to achieve encryption. Encryption character algorithm proposed by Kang et al relying on pseudo-DNA operation, DNA encryption methods have defects such as expensive experimental equipment, complex operation and difficult to understand its biotechnology and remains cannot be effectively applied in encryption field. In this paper; a design approach for encryption image was suggested depending on substitutions operation and DNA computing in block cipher to increase more complexity when an attacker tries image retrieval. A performance analysis in measurement test between the original image and encryption image was evaluated, the values result is big to depend on no correlation for a pixel in images as equality encryption test. Other tests between plain image and clear image after decryption are good values for statistical tests as MSE is equal to zero and PSNR infinity number because no loss data or difference in this approach was found.

Keywords: color image, encryption, decryption, DNA, substitutions operation.

نهج جديد لتشفير الصور بالاعتماد على الحوسبة DNA وعمليات التبديل
أ. م. د. م. مثل عماد الدين زينه محمد سعدي

المستخلص

في التشفير، S-Box (مربع الاستبدال) هو عنصر أساسي من خوارزميات المفاتيح المتماثل الذي يؤدي إلى الاستبدال. في خوارزميات الكتلة، وعادة ما تستخدم لحجب العلاقة بين المفاتيح والنص المشفرة هي خاصية الارتباك. حوسبة الـ DNA قد تخللت في مجال التشفير. تشفير DNA استخدم DNA كحامل معلومات واستفاد من ميزة التكنولوجيا الحيوية لتحقيق التشفير. كانغ وآخرون اقترحوا خوارزمية تشفير الأحرف بالاعتماد على عملية pseudo DNA، إذ أنها استخدمت central dogma التي تنتمي إلى البيولوجيا الجزيئية لتنفيذ التشفير. ومع ذلك، فإن طرق تشفير DNA لديها مساوئ مثل معداتها التجريبية الباهظة الثمن وعملياتها المعقدة وصعوبة فهم التكنولوجيا الحيوية لها والتي لا تزال لا يمكن تطبيقها بكفاءة في مجال التشفير. في هذا البحث صمم نموذج لتشفير الصورة بالاعتماد على حوسبة DNA وعمليات متعددة في النموذج الشبكي festiel لزيادة التعقيد عندما يحاول أحد المهاجمين استرجاع الصورة. وقد تم تقييم تحليل الأداء في اختبار القياس بين الصورة الأصلية والصورة المشفرة، القيم هي كبيرة بالاعتماد على عدم وجود علاقة بين البكسل في الصورة الأصلية والمشفرة. اختبار آخر هو بين الصورة الأصلية والصورة بعد فك التشفير هي قيم جيدة لاختبار احصائي MSE مساوي للصفر و PSNR هو عدد غير منتهى بسبب عدم وجود فقدان بالبيانات أو اختلاف بهذه الطريقة.

الكلمات مفتاحية: صورة ملونة، التشفير، فك الشفرة DNA، العمليات الابدالية.

1-Intorduction

Information security is the act of defending information from any improper use and illegal access to the resources via different objectives. It has been developed over different stages through several past years. The rapid growth and huge demands indicate the need to invest into researches. Intensive research has passed through different phases in order to keep pace of the developments required over past 50 years. This included investigation of cryptographic methods, generic security of computing devices, operating systems and networks [1]. Information security objectives aim to

assure that risk can be reduced to a lowest possible percentage. The major objectives of the information security can be expressed as confidentiality, integrity, authentication, identification and availability [2]. In various areas of society, the digital images have become used on a large scale with the development of computer network technology. But due to the openness of the network, image security is exposed to serious threat by the attackers; therefore, the image encryption becomes the most effective way in order to guarantee to transmit security of images. Confusion is a measurement of the statistical characteristic of the input in correlation to the output. Basically, looking at the output should reveal little or hidden information concerning the input; briefly, the transformation should increase the complexity of the input in a way that makes the output giving a little statistical correlation to the input [3].

2-DNA Image Encryption

Of the most common methods to support the image security is encryption. There are many applications to encrypt image and video in several areas, including the multimedia systems, tele-medicine, internet communication, medical imaging, and military communication and to achieve these purposes. Researchers are constantly looking for methods of encrypting more secure [5]. Since the vast parallelism, extraordinary information intensity, and exceptional energy efficiency all are inherent in DNA molecules. DNA cryptography is a new promising field of cryptography that has become an important direction with the development of DNA computing. As it is known the DNA cryptography has many benefits in the research of DNA computing, but is not equal to the DNA computing, because there is the main difference between them. In DNA computing, the DNA technology is used to solve difficult computational problems but in DNA cryptography, several difficult biological problems are used as the security of DNA cryptosystems it can be considered as the processes of cryptography as computation but not all DNA computations relate to cryptography. In last few years, a large amount of data computational and NP problem produced with the rapid development of the technology of science and social. But DNA computer has excellent properties to process efficient parallel and mass storage capacity problem [6] [7] [8]. In digital image, it is not reasonable to use conventional encryption methods on it because a large data size and real-time requirements. Thus, a main trend is to minimize the computational requirements for secure multimedia distribution. Traditional encryption algorithms have disadvantages and they are not considered as ideal for image applications, because of the low level of efficiency when dealing with large and excessive blocks of image data. In addition, these algorithms require more power and more than the ordinary expected computation time during the performance image encryption [9] [10].

3-Chaos Theory

A chaotic system is a simple, non-linear, dynamical, and deterministic system that shows completely unpredictable behavior and appears random. Moreover, it is a deterministic system with great sensitivity to initial conditions; for example computer system can give an amazingly different result when the value of an input parameter is changed. On the other hand, in classical science, small changes in an initial value might generate small differences in the result [11] [12]. A system is called a chaotic system if it is sensitive to initial conditions, topology mix, and if periodic orbits are dense [12].

Discrete chaotic of logistic map is a simple non-linear dynamical map. The logistic map is a polynomial mapping, a complex chaotic system, the behavior of which can arise from very simple non-linear dynamical equations. The logistic map is written as [13]:

$$X_{n+1} = X_n * r * (1 - X_n) \dots \dots \dots (1)$$

Where x_n is a number between zero and one, x_0 represents the initial population, and r is a positive number between zero and four. It is highly sensitive to change in its parameter value, where a different value of the parameter will give a different map f [14].

4- New approach to image encryption depend on substitutions operation and DNA computing

In this proposal designs and implements a new structure to encrypt color image depending on different operations to increase complexity and increase the speed of traditional methods. The

proposal structure consists of many layers where the first layer replaces all pixel values with new values by using a new S-box depending on confusion principle and the second layer uses the proposed DNA operation as coding, decoding, complement, addition, subtraction and IP-Block operation. The results were good speed and active against to attack depending on different secret values. Figures (1) and (2) explain the encryption and decryption operations.

In the beginning, fetch 256 bytes from clear image depending on a confusion principle that can exchange all the bytes with new values by using substitution operation. This proposal has a new S-Box as a two dimension arrays, 16×16 having 256 values where each old byte from clear image is split to left and right as column and row numbers in new S-Box. After the locations of column and row are found, it can get new values for all bytes to replace. At the end of the replacing of all 256 bytes, the DNA operations are done (coding, addition, complement, DNA IP and decoding). But the coding DNA table operation is depending on secret map which is selected by user or static in program (number of column in DNA table). To increase the complexity, one can mix the result of clear image with output from NLFSRs. This proposal consumes more time because of the S-Box values generation and has new structure. The decryption algorithm has used a same operation but in reverse order and certain operation should use inverse as subtraction, complement and IP^{-1} that can explained in algorithms (1) and (2).

The mask generator algorithm depends on generating multi-keys from original key by using diffusion principle in feistel key generator, in the beginning input the security key as 16 bytes, the first process converts 16 bytes to 128 bits by binary process after that create 2-D array that has 16 row each row present array 1-D or vector as 128 bit, this 2-D array generated by shift and rotate to left 16 time each row has n^{th} time to get new row and put in 2-D new as binary array-Key(16,128) bits as mask key.

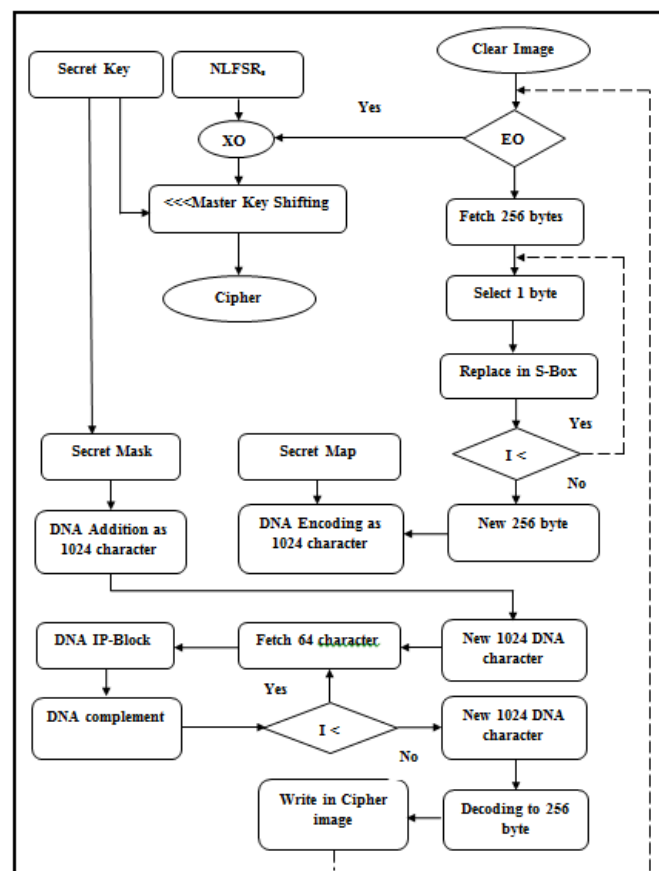


Fig. (1): Encryption Image Depending on Substitution and DNA Operation

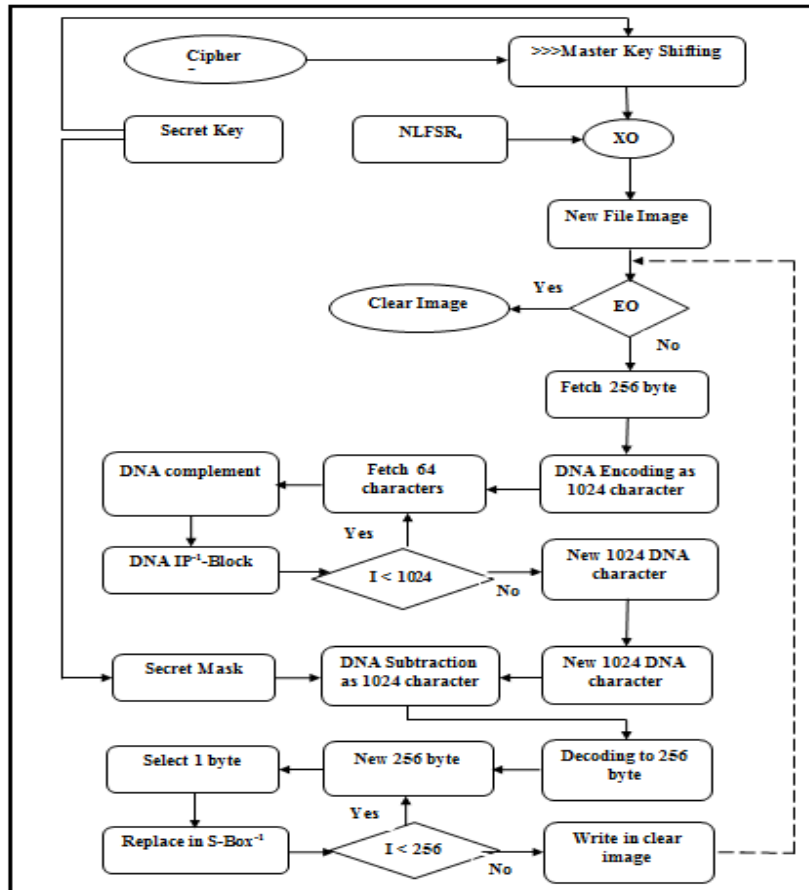


Fig. (2): Decryption Image Depending on Substitution and DNA Operation.

This algorithm illustrates encryption color image based on DNA and substitution operations.

Algorithm (1): Encryption Algorithm.

Input: Plain image, Secret Key as 16 byte.

Output: Cipher image.

Begin

C1, C2, C3, C4, C5, C6, C7, C8, C9 is strings.

Step 1: While (! EOF) do

C1=Fetch 256 Byte.

For i=1 to 256 do

C2=C2+S-Box (C1 (i)).

Next i.

C3=DNA Coding (C2, Secret Map).

C4=DNA Addition (C3, Secret Mask).

For j=1 to 1024 step + 64

C5=Mid (C4, i, 64).

C6=DNA IP-Block (C5).

C7=DNA Complement (C6).

C8=C8+ C7.

Next j.

C9=DNA Decoding (C8).

Write in cipher image (C9).

C8, C9="".

End while.

Step 2: Cipher image= Cipher image XOR NLFSR_s.

Step 3: Cipher image= Cipher image <<<(Master Key Shifting).

End.

This algorithm illustrates decryption color image based on DNA and substitution operations.

Algorithm (2): Decryption Algorithm.

Input: Cipher image.

Output: Plain image, Secret Key as 16 byte.

Begin

C1, C2, C3, C4, C5, C6, C7, C8 is strings.

Step 1: Cipher image= Cipher image >>>(Master Key Shifting).

Step 2: Cipher image= Cipher image XOR NLFSR_s.

Step 3: While (!EOF) do

C1=Fetch 256 byte.

C2=DNA Coding (C1, Secret Map).

For j=1 to 1024 step + 64

C3=Mid (C2, i, 64).

C4=DNA Complement (C3).

C5=DNA IP-Block⁻¹(C4).

C6=C6+ C5.

Next j.

C7=DNA subtraction (C6, Secret Mask).

C8=DNA Decoding (C7).

For i=1 to 256 do

C9=C9+S-Box⁻¹ (C8 (i)).

Next i

Write in cipher image (C9).

C8="".

End while.

End.

In this proposal, the design and implementation of a new idea were done to produce new S-Box to have 256 numbers. This idea that generates new S-Box was depended on multi nonlinear equation and many operations of reordering were used. This can be explained in algorithm (3)

Algorithm (3.15): New S-Box

Input: Private String as 16 byte (secret key).

Output: 16 *16 array as New S-Box.

Begin

Step 1: a=private string

For i = 1 to Len (a).

n=n+ ASCII (Mid (a, i, 1)).

Next i.

Step 2: b = Len (a).

x (0) = ASCII (Mid(a,1,1)) mod 256.

y1 (0) = (1 mod b)/ b.

y2 (0) = ((1*2) mod b)/(b+1).

v(0) = Round(((y1(0) + y2(0)) * Asc (Mid(a, 1, 1))) Mod 255.

Step 3: For i = 2 to 256

If i <= 15 Then

g = Asc(Mid(a, i, 1)) Mod 256.

Else

g = (Asc(Mid(a, (i Mod b) + 1, 1)) Xori) Mod.

End If.

y1(i - 1) = (i Mod b) / b.

y2(i - 1) = ((i * 2) Mod b) / (b + i).

v (i - 1) = Round(((v(i - 2) + y1(i - 1)*(i - x(i - 2)) + y2(i - 1)*(g- x(i - 2))) + i) Mod 256).

```

If v(i - 1) > 255 Then
  v(i - 1) = 0.
End If.
If v(i - 1) < 0 Then
  v(i - 1) = v(i - 1) + 255.
End If.
If x (i - 1) > 0 Then
  x (i - 1) = 255.
End If.
If x(i - 1) < 0 Then
  x(i - 1) = x(i - 1) + 255.
End If.
Next i.
Step 4: X=Distinct.x.
  V= Distinct.v.
Step 5:Fori =1 to 256
  xx (i)=i.
  vv (i)=i.
Nexti
Step 6: xx= Distinct for each value in x.
Step 7: vv= Distinct for each value in v.
Step 8: Fori = 0 to xx-1.
  vvv(xx(i))=vv(i).
  Next i.
Step 9: S-Box(16, 16)=vvv.
End.

```

The P-box can breakable depend on a linear attacker, so one can suggested new nonlinear P-box depending on private equation, this equation has nonlinear principle but generator sometimes many repeated numbers. So, one can execute this equation to larger size for needed P-box, the size of P-Box are 64 location, and checking the values must not repeated to insert in new P-Box. After complete building the secret map (P-Box) of reordering location in DNA input, (P-Box⁻¹) inverse map was used to decrypt or reorder the original location. This P-box has more speed comparison with traditional a P-box because in old P-box the exchanging is done bit by bit but in proposal permutation as 2 bit in each time (2 bit as one character coding A, T, C, G) used to permutation for each location in the block. In decryption algorithm used the inverse DNA P-box inversed. After merge operation between the new left and new right side put in cipher image file to get cipher image, but to more complexity, one can use the primitive and irreducible polynomials to generate big randomness string binaries, this final output string from generating XOR with cipher bytes and put in cipher image.

Each polynomial has the big degree to max period to prevent output repeated; the first and second polynomial has LFSRs, the nonlinear filter combine between two output polynomials. The explanation was introduced in equations to generate the output in new equation:

$$F_1(x): x^{16} + x^{11} + x^7 + x^5 + 1 \dots\dots\dots(2)$$

$$F_2(x): x^{13} + x^9 + x^7 + x^5 + 1 \dots\dots\dots(3)$$

Output= (f₁(x) and f₂(x)) XOR f₁(x)

The final output from pervious process, the 256 byte shifting to left by second byte from master key and so on each bytes, master key is key get from shifting key to left by first key from secret key and the result key also shifting to left by second byte for each byte in master key.

5-Time and Complexity of the Proposed Structure

In this part, one will try to find out some aspects of evaluation concerning speed, complexity and resistance against known attack as a comparative study with some block cipher system. The speed of the proposed structure and run methods is design as feistel structure to more complexity in diffusion. Then they are applied to an image with different sizes. The image has a bitmap (BMP) type and with size K that is taken and encrypted, the running time of this operation is computed.

Then the 66K, 117K, 168K, 198K, and 792K are taken and the running time of encryption and decryption of each image are calculated. Another type as JPEG, TIFF was used because it is higher resolution and lossless image can clear in tests, table (1) explains the running time evaluated.

Table (1) Encryption and Decryption Time.

Image Dimension	Image Size (K)	Encryption Time (Sec.)	Decryption Time (Sec.)
150x150	66	12	13
200x200	117	21	22
240x240	168	28	30
260x260	198	34	35
520x520	792	123	125

Also, it can be explained in figure (3) for time encryption and decryption.

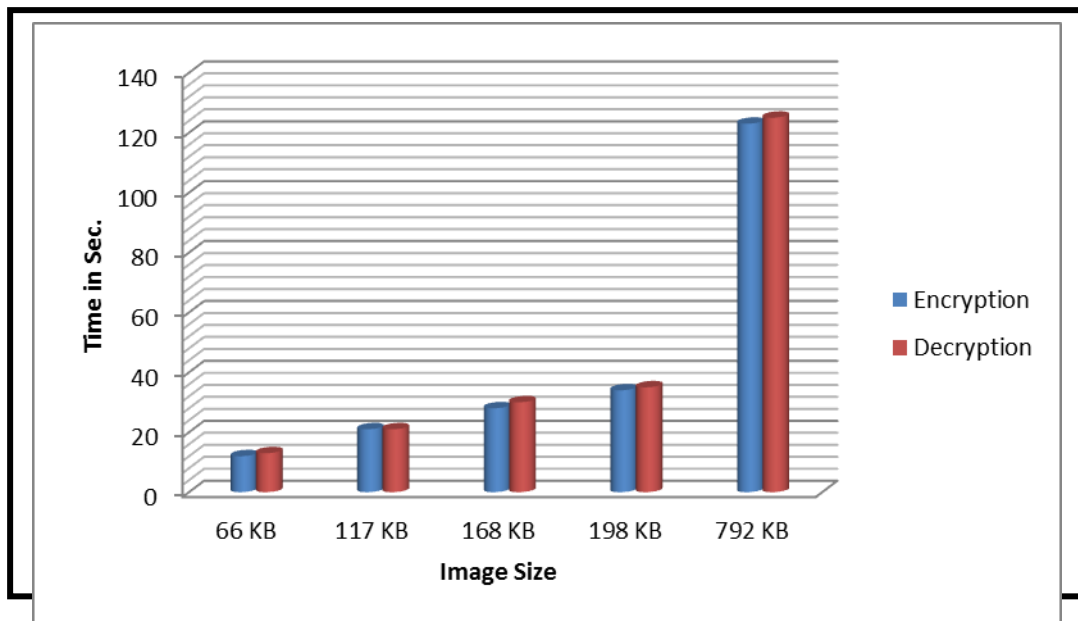


Fig. (3): Encryption and Decryption Time.

The complexity of any encryption algorithm cipher depends on key length and operations in algorithm, but in the proposed structure the complexity is computed by addition operation such as DNA operation such as (encoding, decoding, addition, subtraction, and complement), DNA permutation operation and used linear operation between encryption block (from proposed structure) and reminder key from NLFSRs system. On the other hand, the complexity of the proposed structure has depended on the complexity of feistel network and DNA computing, measurement of proposed approach structure.

6- Key Space Analysis

One of the parameters used to measure the security of an image encryption algorithm is its key space. As the key space increases, the security of encryption improves. The method describes an encryption technique that uses a color image of different size pixels. This key space is large enough to resist exhaustive attacks. The technique uses an input key size of 128-bits as (2^{128}) to breakable in brute force attack. To increase complexity, the initial condition in chaotic as $X_0=0.99$ and $\mu=3.6$ must be symmetric to generate same values and used in send and receive (encryption and decryption) and modify any values that produced other numbers as column number in DNA table.

Also, one can need same equations to generate symmetric keys for XOR operation, when modifying in equation one or two produce another output, this equation generate more bits to maximize period. With shifting operation for each 256 byte by key byte from master key is impossible retrieval clear image without key.

7- Performance Analysis

The test images have different size. The results after encrypting to plain images using the proposed algorithm are given. The diffusion characteristics include PSNR, MSE, MD, AD, NC, MEA, NAE, SC, SNR, SIM, and EQ that can explain the result in table (2).

Table (2) Compare between plain image (original) and decryption.

Image size	150*150 66.2 KB	200*200 117 KB	240*240 168 KB	260*260 198 KB	520*520 792 KB
PSNR	100 or infinity	100 or infinity	100 or infinity	100 or infinity	100 or infinity
MSE	0	0	0	0	0
AD	0	0	0	0	0
MD	0	0	0	0	0
NC	0	0	0	0	0
MEA	0	0	0	0	0
NAE	0	0	0	0	0
SC	1	1	1	1	1
SNR	100 or infinity	100 or infinity	100 or infinity	100 or infinity	100 or infinity
SIM	132.5895	121.9444	189.4609	166.9186	136.1813
Quality encryption test is between plain images and cipher images					
EQ	6853.8320	11440.1914	18300.9032	18605.5859	64812.5585

When studying the tests performance, the PSNR values for many images are infinity because MSE as zero values because no difference in pixels in plain and decryption image. PSNR is a measure of return infinity values that depend on images size that can present as 100 percentages.

The remind characteristics as equal or near from size because no modify or loss information between plain and decryption image so that the result are equal to zero. In the last one (encryption quality) it must work between the plain and cipher images to test the powerful and quality encryption, the high values produce good encryption and difference in pixels. It also depends on image size and many differences in pixels.

8-Conclusions

The proposed algorithm enhances two criteria of a standard block cipher, which are confusing and diffusion in feistel mode with DNA computing. The DNA operation such as (addition, subtraction, complement) has no more complexity because the operations are simple it. DNA permutation operation depends on the length of the string in DNA present. Also, DNA cans storage more data in the string as each two bit represented in one character. Encryption image of feistel network and DNA computing produce more complexity encryption. The secret key used to find many keys to encrypt blocks to increase quality encryption. The coding and decoding DNA consume more time. DNA permutation was used to make more difference in neighborhood pixel. When modify in one bit in secret key is done, it is affect to master key to result new master key, impossible retrieve clear image with new master key.

References

- [1] Angelo A., Cancelli G. and Barni M. , " **Watermark-Based Authentication**", Springer-Verlag Berlin Heidelberg, Vol. 282, pp. 365 -402, 2010.
- [2] Thien C. and Lin J., " **Secret Image Sharing**", Elsevier, Computers and Graphics, Vol. 26, No. 5, pp. 765-770, 2002.
- [3] Chong F. and Zhiliang Z., " **A Chaotic Image Encryption Scheme Based on Circular Bit Shift Method**", The 9th International Conference for Young Computer Scientists. (2008) 3057–3061.
- [4] Weng-Long C., Shu-Chien H. and Weicheng L., " **Fast parallel DNA-based algorithms for molecular computation: discrete logarithm**", J Supercomputing 2011; 56:129–63.
- [5] Shihua Z., Qiang Z. and Xiaopeng W., " **Image Encryption Algorithm Based on DNA Sequences for the Big Image**" , 2010 International Conference on Multimedia Information Networking and Security.
- [6] Xiao G., Lu M., Qin L. and Lai X., " **New Field of Cryptography: DNA Cryptography**", Chinese Science Bulletin, vol. 51, pp.1413-1420, 2006.
- [7] Leier A., Richter C., Banzhaf W. and Rauhe H., " **Cryptography with DNA Binary Strands**", Bio Systems, vol. 57, pp.13-22, 2000.
- [8] Heider D. and Bamekow A., " **DNA-based Watennarks Using the DNA-Crypt Algorithm**", BMC Bioinfonnatics, vol. 8, pp.176-185, 2007.
- [9] Adleman L., " **Molecular Computation of Solutions to Combinatorial problems**", Science, vol. 226, pp. 1021-024, Nov. 1994.
- [10] Cui G. and Qin L., " **Information Security Technology Based on DNA Computing**", IEEE International, China, pp. 288 – 291, April 2007.
- [11] Hung K., " **A Study on Efficient Chaotic Image Encryption Schemes** ", M.Sc. Thesis, Department of Electronic Engineering, City University of Hong Kong, September, 2007.
- [12] Maqableh M., " **Analysis and Design Security Primitives Based on Chaotic Systems for eCommerce** ", Ph.D Thesis, Durham University, School of Engineering and Computing Sciences, United Kingdom, 2012.
- [13] May R., " **Simple mathematical models with very complicated dynamics**", Nature Publishing Group, Vol. 261, pp. 459-67, 10 June 1976.
- [14] Tong X., Cui M., " **Image encryption with compound chaotic sequence cipher shifting dynamically**", Image Vision Computing, 6:843-50, 2008.

Verification Consistency Based Multi-Focus Image Fusion Using Berkeley Wavelet Transform

Iman M. G. Alwan

Computer Science Dep., College of Education for Women, Baghdad University

ainms_66@yao.comho

Abstract:

Multi-focus image fusion is the process of transferring important information and details from multiple multi-focus images into single one. In this paper, pixel-level fusion algorithm is proposed. It exploits the characteristics of Berkeley Wavelet Transform to fuse the transformed multi-focus input images. Maximum rule with modified verification consistency based on majority filter is used for detail subbands, and mean fusion algorithm for DC subband obtained from Berkeley Wavelet Transform. The proposed algorithm has been compared with wavelet transform and stationary wavelet transform based fusion algorithms. The comparative results show better results.

Keyword: Multi-focus image fusion, Berkeley Wavelet Transform (BWT), verification consistency.

دمج الصور متعددة التركيز بالاعتماد على تحقق الاتساق باستعمال تحويل موجة بيركلي
إيمان محمد جعفر علوان

المستخلص

تمثل عملية دمج الصور متعددة التركيز تحويل المعلومات المهمة والتفاصيل من الصور متعددة التركيز المتعددة الى صورة واحدة. يقدم هذا البحث خوارزمية دمج صور تعتمد على مستوى البكسل. تستثمر هذه الخوارزمية المقترحة الخصائص التي تقدمها تحويل موجة بيركلي لدمج الصور في مجالها. تم اعتماد قانون اختيار القيمة الاعلى مع تحقق الاتساق الذي تم تعديله لاعطاء نتائج أفضل بالنسبة لمعاملات التفاصيل بينما تم اعتماد خوارزمية المعدل لمعاملات التقريب. قورنت نتائج الخوارزمية مع كل من خوارزمية الدمج المعتمدة على تحويل الموجة وتحويل الموجة المستقرة وقد اظهرت النتائج تفوق الخوارزمية المقترحة.

1. Introduction

The combination of complementary information from multiple input images to construct a single image that has all information with better quality is known as image fusion. There are many applications that need to fusion process, such as medical imaging, Remote sensing, Surveillance and law enforcement, Biometry and Multimedia processing. Multi-focus image fusion merges source images acquired at varying focal lengths [1].

There are three levels where the fusion process can be implemented, pixel level, decision level, and finally feature level. The efficiency and facility of pixel-level fusion process makes it preferable and widespread. The fusion algorithms aim to produce fused image which contains all the important information of the multi-focus input images without any artifacts. Pixel level fusion algorithms are classified into spatial domain and transform domain. Computing average value of corresponding pixels from the input images is consider as the easiest image fusion technique. The disadvantage of this method is the contrast reduction. Several fusion techniques were introduced such as Ratio pyramid, Laplacian pyramid, Contrast pyramid.

In transform domain, many transforms are used in the fusion process where improved results were obtained [2]. DWT tool was used in fusion process where the input images are decomposed into approximation band and details bands. Since approximation subband represents the image without details, averaging fusion rule is used to combine coefficients of the approximation subbands. Maximum fusion rule in which coefficient with maximum value is chosen from the corresponding band of the detail subbands is used since these bands represent edges and details. IDWT is implemented to get the fused image. In [3, 4] Discrete Cosine Transform and Discrete Complex

Wavelet Transform are used in fusion process with different fusion rules such as weighted average. In [5], Stationary Wavelet Transform is invested in fusion process by using extended spatial frequency. In [6] curvelet transform with mean and PCA fusion rule is used, while [7] uses contourlet transform with different fusion rules such as entropy, mean and standard deviation. In this paper, Berkeley Wavelet Transform (BWT) is used in multi-focus image fusion. It is a wavelet transform with triadic two dimension. The Berkeley wavelets are localized in space, tuned in spatial frequency and orientation. Hence it forms a set that is approximately scale invariant [8]. The fusion rules which used in this proposed algorithm depends on the characteristics of the BWT coefficients. Maximum rule with modified verification consistency is used for details subbands and mean fusion rule for DC subband. The rest of the paper is organized as follow: section two, explain the Berkeley Wavelet Transform, section three demonstrate the fusion process, section four is for the experimental results and finally section five for conclusion.

2- The Berkeley Wavelet Transform

Berkeley Wavelet Transform (BWT) simulates the physiology characteristics of the receptive fields of neurons in mammalian primary visual cortex (V1) because it has the same properties in choosing base with them. They are spatially localized, oriented and frequency bandpass [8].

BWT transform is constituted by eight mother wavelets, in four pairs. Each pair has a different direction: 0, 45, 90 and 135. Within each pair, one wavelet is odd symmetric, the other is even symmetric. The Berkeley wavelet transform (BWT), is a two-dimensional triadic wavelet transform. The Berkeley wavelets are localized in space, tuned in spatial frequency and Orientation. Hence it forms a set that is approximately scale invariant. BWT is a complete, orthonormal basis and hence it is inexpensive to compute, manipulate and invert. These properties of BWT make useful in the situations where computational power or experimental data are limited Translation and scaling of the whole set (plus a single constant term) of wavelet results in a complete, orthonormal basis in two dimensions. For applying the BWT, the input image must be square and also the side length should be a power of three. Figure (1) represents the output decomposition of the BWT for image. There are 9 bands, each one represents certain orientation of wavelets pair as in [9]:

[90-odd 135-odd 45-even]
[90-even 135-even 45-odd]
[DC 0-even 0 -odd]

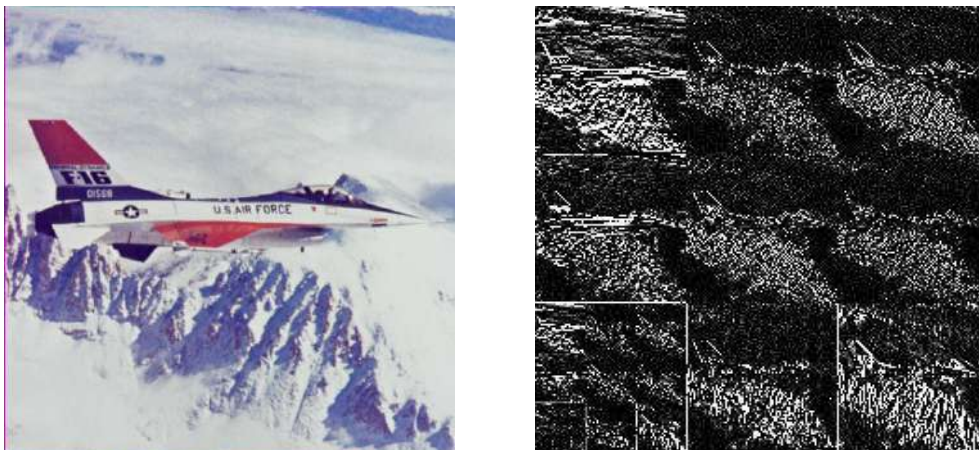


Fig. (1): BWT for Plane image

3- The Fusion Process

The main point of multi-focus image fusion is to determine best focus parts in the input images to be combined to produce quite focused images through particular fusion rules. In transform domain, in which input images are decomposed into low band frequencies and high band frequencies, different fusion rules are followed. The window-based fusion rules usually consider the neighboring pixels in making decision choice, so they are superior to conventional pixel-based fusion rules [5].

In this algorithm, mean fusion rule is executed for DC bands of the transformed input images to acquire the fused DC band as in equation (1).

$$C_{dcf} = (C_{dcx} + C_{dcy})/2 \quad \dots (1)$$

Where, C_{dcx} , C_{dcy} represent the DC band coefficients of images X, Y to be fused.

C_{dcf} the resultant fused coefficients for image F.

The fusion of the details bands is implemented by applying maximum fusion rule.

In order to eliminate the noise, blurring effect that may come from fusion process, the window-based consistency verification procedure through applying majority filter which is proposed by [9] is followed. In this step, a small window which is 3×3 size centered at the current coefficient position. The rule is that if the center fused coefficient after applying maximum fusion rule comes from image X, while the majority of the surrounding coefficients come from image Y, then the center coefficient is altered to come from Y, the same thing for image Y. To execute this endeavor, a binary decision map followed by majority filter are used. Then a new binary decision map is utilized to get the fused coefficients of the details bands. The process is explained as follows for input images X, Y, and the fused image F. $w \times w$ is the applied window, C_x , C_y , C_f represent the transformed coefficients of X, Y input images and fused image respectively. p represents the decomposed detail eight bands [10].

$$C'_x = \max_{w \in W}(|C_x(p, w)|) \quad \dots (2)$$

$$C'_y = \max_{w \in W}(|C_y(p, w)|) \quad \dots (3)$$

$$m_x(p) = \begin{cases} 1, & C'_x > C'_y \\ 0, & otherwise \end{cases} \quad \dots (4)$$

$$m_y(p) = \begin{cases} 1, & C'_y > C'_x \\ 0, & otherwise \end{cases} \quad \dots (5)$$

$$Dm_x(p) = \begin{cases} 1, & \sum m_x(p) > w^2/2 \\ 0, & otherwise \end{cases} \quad \dots (6)$$

$$Dm_y(p) = 1 - Dm_x(p) \quad \dots (7)$$

$$C_f(p) = Dm_x(p)C_x(p) - Dm_y(p)C_y(p) \quad \dots (8)$$

The steps of the proposed algorithm are as follows:

Input: image X, image Y, where they are multi-focused.

Output: image F, the fused image.

1- Resize input images to $(3^n \times 3^n)$ where n is integer number.

2- Implement BWT for images X, Y.

3- For DC band of both transformed images apply mean fusion rule to get the fused DC band as in equation (1).

4- For eight detail bands apply equations (2-8) to obtain fused detail sub bands.

The size of $w \times w$ is equal to 3×3 . The decision map which resulted from equation (6) is modified in this proposed algorithm to get best results. Instead of using value $w^2/2$ [9], $(w^2 - 2)$ is used to overcome the blurring effect which may result from fusing process.

5- Implement inverse BWT to obtain the fused image F.

6- End

4- The Experimental Results:

Experiments are executed on multi-focus color images of size 243×243 since Berkeley Wavelet Transform is a triadic wavelet transform. To evaluate the proposed algorithm, the obtained results are compared with wavelet and stationary wavelet based image fusion algorithms. Figure (2), shows the test color images that obtained from [11] and the resultant fused ones. To evaluate the fused image quality, four quality criterions are used. They are: Standard Deviation (SD) which reflects the spread in data, Average Gradient (AG) measures the degree of clarity and sharpness, Spatial Frequency (SF) measures the overall information level in the regions, and Entropy (E) which estimates the amount of information present in the image.

These criterions are used because no reference images are available. Equations (9-12) represent these evaluation criterions [12].

$$SD = \sqrt{\frac{\sum_{i=1}^m \sum_{j=1}^n (f(i,j) - \bar{f})^2}{mn}} \quad \dots (9)$$

$$AG = \frac{\sum_i \sum_j ((f_{i,j} - f_{i+1,j})^2 + (f_{i,j} - f_{i,j+1})^2)^{1/2}}{m \times n} \quad \dots (10)$$

$$SF = \sqrt{RF^2 + CF^2} \quad \dots (11)$$

$$RF = \sqrt{\frac{\sum_i \sum_j (f(i,j) - f(i,j-1))^2}{mn}} \quad \dots (11-1)$$

$$CF = \sqrt{\frac{\sum_i \sum_j (f(i,j) - f(i-1,j))^2}{mn}} \quad \dots (11-2)$$

Where $f(i,j)$ represents intensity of fused pixel at i, j position, m , and n are the image size.

$$Entropy = - \sum_{f=0}^{255} pf(f) \log_2 pf(f) \quad \dots (12)$$

Where $pf(f)$ is the probability of intensity value f in image F .

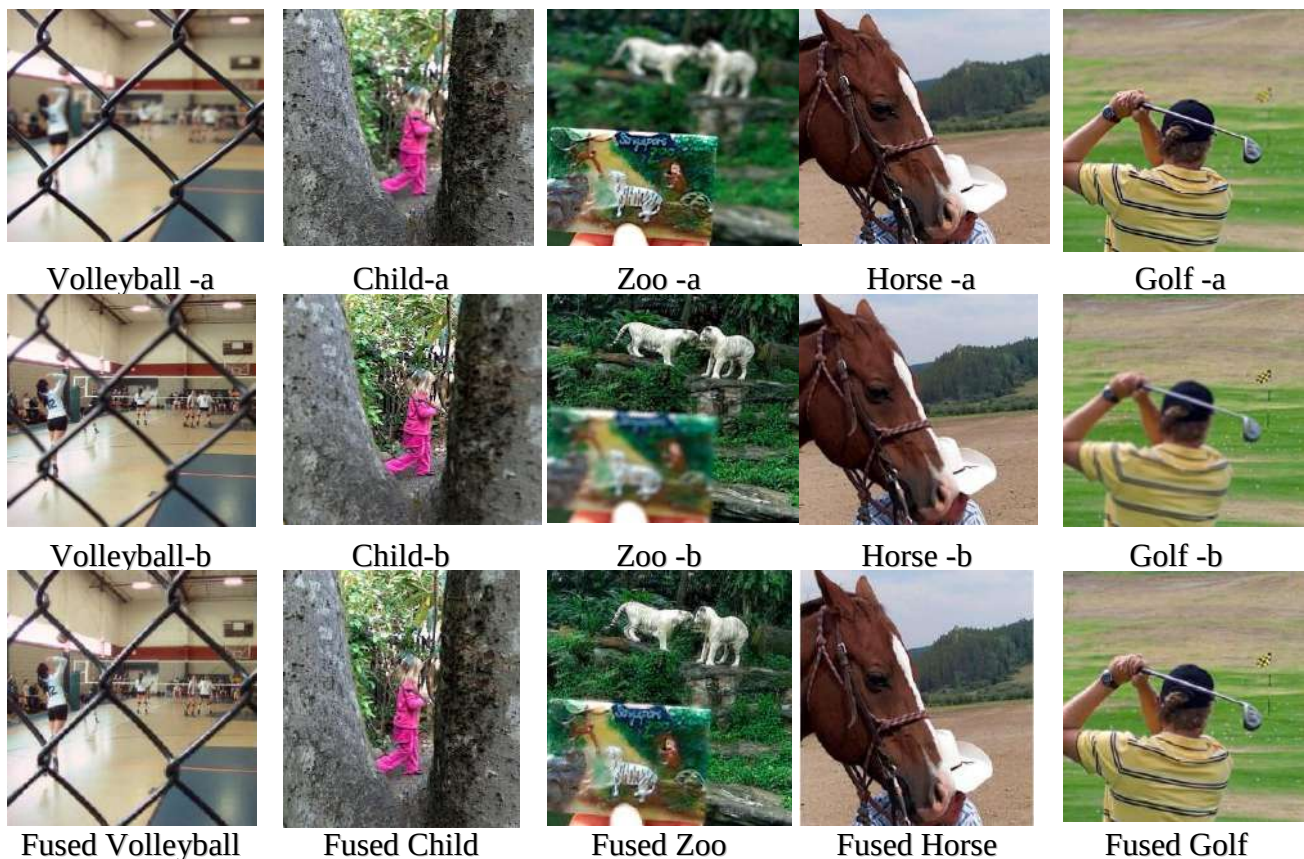


Fig. (2): Test color images and the resulted fused images.

Table (1) represents the values of the evaluation criterion for the test images as well as the evaluation criterion for the two other comparable methods: wavelet transform and stationary wavelet transform fusion algorithms. From the results one can notice that, the results of the proposed algorithm are better than other methods except the value of entropy for volleyball and zoo images where the value of WT is greater in few hundredth.

To evaluate the proposed algorithm in terms of Peak-Signal-to-Noise-Ratio, five test reference color images are used. 5x5 average filter is used to blur right and left side of the test images respectively. Figure (3) represents the test images and blurred ones that made artificially. Table (2) represent PSNR for the test images of Figure (3) for the proposed algorithm and the other comparative algorithms. The results show that the PSNR of the proposed method outperform the other algorithms except for Fruit image in SWT based algorithm which is of largest value.



Fig. (3) Test color images made artificially

Table (1) Results of evaluation criteria for test images

Volleyball	SD	<i>AG</i>	SF	E
Proposed	61.8219	15.1955	24.4373	7.7577
WT	61.3332	14.4709	22.7293	7.7581
SWT	61.2732	13.9853	22.0995	7.7554
Child				
Proposed	48.7882	25.9622	33.2092	7.5456
WT	48.3837	24.8762	31.7264	7.5388

SWT	48.3491	24.6276	31.4468	7.5376
Zoo				
Proposed	62.4024	22.0678	28.6988	7.4926
WT	61.5671	20.1986	25.9368	7.4936
SWT	61.4902	19.5761	25.1997	7.4927
Horse				
Proposed	65.7636	11.7724	19.9628	7.5729
WT	65.7044	11.6522	19.6976	7.5727
SWT	65.7018	11.5708	19.6185	7.5719
Golf				
Proposed	42.9783	12.6544	20.8385	7.2604
WT	42.4375	11.7180	18.9748	7.2428
SWT	42.3831	11.4503	18.6003	7.2418

Table (2) PSNR (dB) of the proposed algorithm and other comparable ones

Test images	Boy	Fruit	Clock	Monument	Plane
proposed	42.19	40.02	41.07	40.65	39.11
WT	40.95	39.78	38.91	38.10	38.43
SWT	41.40	40.33	39.58	39.18	38.86

5- Conclusion

In this paper, a multi-focus image fusion algorithm is proposed. It depends on using a new kind of wavelet transforms named Berkeley Wavelet Transform (BWT). It is a two-dimensional triadic wavelet transform, localized in space, tuned in spatial frequency and Orientation. The fusion process depends on using average fusion rule for DC bands of the transformed multi-focus input images and maximum rule with consistency verification for the detail subbands. The proposed algorithm is compared with wavelet based and stationary wavelet based image fusion. The results of the proposed algorithm are better than other comparative ones.

References

- [1] S. Banerjee, V. N. Gangapure, A. S. Chowdhury, "Multispectral Multifocus Image Fusion with Guided Steerable Frequency and Improved Saliency", ICVGIP '14, December 14-18, 2014, Bangalore, India.
- [2] D.P. Bavirisetti, R. Dhuli., "Multi-focus image fusion using multi-scale image decomposition and saliency detection", Ain Shams Eng J., (2016), <http://dx.doi.org/10.1016/j.asej.2016.06.011>.
- [3] V.P.S. Naidu, "Discrete Cosine Transform based Image Fusion Techniques", Journal of Communication, Navigation and Signal Processing, 1(1)35-54,2012.
- [4] P. Hill , N. Canagarajah, D. Bull, "Image fusion using complex wavelets," in Proc. 13th Brit. Mach. Vision Conf., Cardiff, U.K., 487-496, 2002.
- [5] P. Borwonwatanadelok, W. Rattanapitak, S. Udomhunsakul, " Multi-Focus Image Fusion based on Stationary Wavelet Transform and extended Spatial Frequency Measurement", International Conference on Electronic Computer Technology, IEEE, 77-81, 2009.
- [6] G.M. Taher, M.E. Waheed, G. El Taweel, "New Approach for Image Fusion Based on Curvelet Approach", (IJACSA) International Journal of Advanced Computer Science and Applications, 5(7) 67-73, 2014.
- [7] V.T. Manu, P. Simon, " A Novel Statistical Fusion Rule for Image Fusion and Its Comparison in Non-Subsampled Contourlet Transform Domain and Wavelet Domain", The International Journal of Multimedia & Its Applications (IJMA), 4(2)69=87,2102.
- [8] B. Willmore, R.J. Prenger, M. C-K. Wu, J.L. Gallant, "The Berkeley Wavelet Transform: A biologically-inspired orthogonal wavelet transform", Neural Computation Journal, 20(6) 1537-1564, 2008.

- [9] H. Li, B. Manjunath, S. Mitra “**Multisensor image fusion using the wavelet transform**” Graph Models Image Process, 57(3) 235–45,1995.
- [10] Y.Yang, S. Huang, J. Gao, Z. Qian, ”**Multi-focus Image Fusion Using an Effective Discrete Wavelet Transform Based Algorithm**”, Measurement Science Review, 14(2)102-108, 2014.
- [11] <http://mansournejati.ece.iut.ac.ir/content/lytro-multi-focus-dataset>.
- [12] B.K. Shreyamsha Kumar, “**Multifocus and Multispectral Image Fusion based on Pixel Significance using Discrete Cosine Harmonic Wavelet Transform**”, Signal, Image and Video Processing, 2012, DOI: 10.1007/s11760-012-0361-x.

التعرف على الوجوه

Review of Face Recognition Methods

أ.م. د رحاب فليح حسن سري رحيم عيدان

الجامعة التكنولوجية / علوم الحاسوب

Sura_19852001@yahoo.com, surorh@yahoo.com

المستخلص

التعرف على الوجوه (face recognition) احد المهام التي يؤديها الانسان بشكل روتيني، دون ادراكه لعدد المرات التي يقوم بها بتنفيذ ذلك، وهي احدى الخصائص البايومترية التي حاول الانسان محاكاتها عن طريق برامج وتطبيقات الحاسوب أو الهواتف الذكية من خلال الاستفادة من القدرة والاداء العالي في تنفيذها اليا، وهو واحد من اكثر المجالات التي شغلت الباحثين على مدى السنوات الماضية وحتى الان اولت الابحاث اهتماما كبيرا في التعرف على الوجه للاستفادة منها على الاصعدة الامنية والاجتماعية للحد من عمليات التزوير، التعرف على الاطفال المفقودين، وتعزيز الامن والمراقبة، واستخدامها في الشبكات الاجتماعية (فيسبوك، تويتر)، والمطارات وامكن عامه، والمصارف. ولما يتميز به هذا النظام من مزايا عن الانظمة البايومترية الاخرى.

هذه الورقة تقدم ادبيات هذا الموضوع بشكل مبسط ليستطيع الباحث الالمام بالموضوع. قسمت الورقة الى جزئين ركزت بالجزء الاول على المقاييس الحيوية بشكل عام والتطبيقات والوظائف والية عملها بشكل عام والمقارنة بين انواع المقاييس المختلفة لان نظام التعرف على الوجه هو احد انواع هذه المقاييس. ثم تناول الجزء الاخر التعرف على هيكليته النظام والطرق المستخدمة في كل خطوة بدءا من مرحلة الكشف واستخلاص الخصائص وصولا الى عملية التعرف والتحديات التي تواجهها كل مرحلة فيها والتقنيات الشائعة.

الكلمات المفتاحية: التعرف على الوجوه، كشف الوجوه، المقاييس الحيوية.

1. مقدمة:

نظام التعرف على الوجوه هو احد التطبيقات التي تبنى من اجل التعرف على الاشخاص وكشف هويتهم من خلال صوره أو مقطع فيديو، فالهدف هو خلق نظام يحاكي القدرة البشرية في التعرف على الوجوه. العديد من الدراسات قدمت لغرض تحسين قدرة الحاسوب وايجاد الطريقة الامثل للتعرف على الوجوه منذ خمسينيات القرن الماضي وحتى الان ولايزال التعرف على الوجوه يشغل اهتمام الباحثين في مجالات (علم النفس، الاعصاب، معالجة الصور، الرؤية الحاسوبية، التعرف على الأنماط، التعلم الآلي، الشبكات العصبية،.. الخ). من أوائل الابحاث التي تناولت موضوع التعرف على الوجوه بعلم النفس والاعصاب حاولت فهم ومعرفة كيف يقوم الانسان بهذه المهمة وكيف تتم بشكل تلقائي للبحث عن التصميم الملمه، من المهم أن نفهم كيف يمكننا القيام بهذه المهمة، كيف يمكننا تصور البشر، هذه جاءت مرافقة إلى قضايا أخرى مثل تفسير الوجوه، والعواطف أو تصور لإيماءات الوجه (Bruner and Tagiuri, 1954)^[1]، العديد من التساؤلات طرحت لفهم هل هذه المعرفة تفيد لاستنتاج نظام يطبق للتعرف على الوجوه اليا^[2].

اولى المحاولات لعمل نظام تعرف آلي كانت في الستينات وحتى بداية السبعينات باستخدام المعلومات الهندسية (Woodrow W. Bledsoe)، خلال عامي (1965، 1964) قام (Bledsoe) مع (Helen Chan, Charles Bisson) باستخدام الحاسوب للتعرف على الوجوه بتمويل من وكالة الاستخبارات لذلك لم ينشر منه الا القليل، تم استخدام قاعدة بيانات كبيرة للصور ووصف (Bledsoe) العديد من الصعوبات الي واجهتم منها (تعبيرات الوجه، تغير زاوية دوران وميل الرأس، الشيوخوخة، الاضاءة، .. الخ) ان عملية مطابقة الانماط لصورتين بزاوية دوران مختلفة ستكون غير دقيقة حتى وان كانت الصورتان لنفس الشخص (Bledsoe, 1966). تطلب العمل وضع (landmarks) لتحديد الملامح الرئيسة (كالأنف، العيون، اذان، الفم) على الصور وتم حساب (Relative distances) النقاط المرجعية المشتركة (common reference point) ومقارنتها مع (data reference). وقد وصف هذا المشروع (man-machine) لأن الإنسان يستخرج الإحداثيات لمجموعة من features من

الصور، واستخدمت بعد ذلك بواسطة الكمبيوتر للتعرف. باستخدام حاسوب الرسم اللوحي (GRAFACON أو RAND TABLET)، فإن operator يستخرج الإحداثيات من feature مثل مركز البؤبؤ، والزوايا الداخلية للعيون، الزاوية الخارجية للعيون، وشعر مقمة الرأس، الى آخره. من هذه الإحداثيات تم حسابها قائمة (20 distances) مثل عرض الفم وعرض بؤبؤ العين. هذه operators يمكنها معالجة حوالي 40 صورة في الساعة. عند بناء قاعدة البيانات، ارتبط اسم الشخص في الصورة مع قائمة المسافات المحسوبة والمخزنة في جهاز الكمبيوتر. في مرحلة التعرف تتم مقارنة مجموعة المسافات مع المسافة المقابلة لكل صورة، تنتج المسافة بين الصورة و قاعدة البيانات المسجلة، ويتم إرجاع النتيجة الاقرب. صمم (Bledsoe) نظام semi-automatic system.

في عام 1971 تقريبا (Harmon, Goldstein) استخدم (21 subjective markers) لأتمته التعرف مثل: لون الشعر، سمك الشفاه، والمشكلة هنا القياسات والمواقع تحسب يدوياً. بعض الدراسات المبكرة شملت العمل على تعبيرات الوجه (Darwin, 1972). حاول (Elschanger, Fischler, 1973) قياس الملامح المتشابهة تلقائياً باستخدام خوارزمية local template (matching) لإيجاد وقياس ملامح الوجه ووجدوا ان هذه الملامح لا تحتوي على بيانات كافية ومتساوية لتمثيل وجوه البالغين. بعض الباحثين حاولوا تحديد الوجه كمجموعه من (geometric parameters) وتم تنفيذ بعض تقنيات تمييز الانماط بالاعتماد على هذه المعايير. واول من وضع نظام الي بالكامل للتعرف على الوجه هو (Kenade, 1973) الذي استخدم أساليب معالجة الصور البسيطة لاستخراج vector من (16 facial parameters) تلقائياً واستخدم قاعدة بيانات لعشرين شخصا بمعدل صورتين لكل شخص حيث استخدم واحده كمرجع والاخرى للاختبار وحقق نسبة تعرف 45-75%.

ذكر (Eigen faces) لأول مره في معالجة الصور والتي اصبحت التقنية السائدة في اغلب البحوث فيما بعد، خلال فترة الثمانيات طبق كل من (Kirby, sirovich) مبدء تحليل المكونات الأساسية (PCA) وتقنيات الجبر الخطي القياسية للتعرف على الوجه. كان هدفهم لتمثيل صورة في بعد أقل، دون أن تفقد الكثير من المعلومات، كانت اول طريقة مقبولة على نطاق واسع وحتى يومنا هذا لا تستخدم فقط كطريقة مرجعية لمقارنة الطرق الجديدة وانما كقاعدة للكثير من الطرق التي اشتقت من الفكرة الاساسية لها. شهدت فترة التسعينيات اعتراف واسع النطاق للنهج eigenface المذكور كأساس الحالة من الادبيات والتطبيقات الصناعية الأولى. قدم (Turk and Alex Pentland, 1992) من معهد ماساتشوستس للتكنولوجيا وهو العمل الذي يستخدم eigenfaces للتعرف. وكانت الخوارزمية قادرة على تحديد وتعقب وتصنيف رأس الشخص المعني، تم اختبار الطريقة باستخدام قاعدة بيانات مؤلفة من 2500 صورة وتحت ظروف مختلفة بثلاث وضعيات (لدوران الرأس، والاضاءة، والحجم) لسته عشر شخصا حيث كانت نسبة تعرف (96%, 85%, 64%).

في 2001 تم الاستفادة من مراقبة الصور ومقارنتها بقاعدة بيانات رقمية في لعبة Super Bow في ولاية فلوريدا، وقد اثارت اهتمام الجمهور والاعلام، مما زاد الطلب لاستغلال التكنولوجيا لدعم الحاجات الوطنية. ولا تزال الدراسات مستمرة لتقديم خوارزميات وتحسين طرق لتحقيق افضل اداء واعلى نسبة.

2. نبذة تاريخية عن القياسات الحيوية:

قبل الخوض في تفاصيل التعرف على الوجوه التي هي احدى القياسات الحيوية الشائعة ومعرفة التقنيات المستخدمة في ذلك لابد من تقديم نبذة عن اساسيات القياسات الحيوية لغرض تكوين معرفة عامة عن كل المقاييس البايومترية المستخدمة اليا في أنظمة التعرف، سنوضح في هذا الجزء خصائصها وعملها والايجابيات والسلبيات لكل منها ولابد من الإشارة ان كل أنظمة التعرف تحتاج الى قواعد بيانات خاصة بها.

القياسات الحيوية (Biometric authentication, or simply biometrics) هو علم إثبات الهوية والتحقق من الاشخاص استناداً إلى استخدام القياسات الحيوية للجسد (physiological biometrics) مثل (القزحية، شبكية العين، بصمة الاصبع، الوجه، هندسة اليد، الحمض النووي، بصمة القدم، الوريد، بصمة الكف، الأنسجة، شكل الأذن) والسلوكية للفرد (المشية، التوقيع،

ضربة المفتاح (على لوحة المفاتيح)، التعرف على الصوت) نظرا لتمييز الاشخاص في هذه الخصائص عن بعضهم البعض فاذا تم التعرف عليهم سيتم التعامل معهم بثقة وسيصبح بإمكانهم استخدام كافة الموارد والامتيازات المتاحة. يرجع تاريخ استخدام هذا العلم منذ ايام البابليون (500 ق.م) الذين استخدموا بصمات الاصابع في التعاملات التجارية والمصريون القدامى كانوا يستخدمون اوصاف الوجه للتجار لغرض تمييزهم والتعرف عليهم وتدوين المعلومات الخاصة بهم اما التجار الصينيون الاوائل استخدموا البصمات وكذلك الاباء استخدموا بصمات اليد والاقدام لتمييز بين ابنائهم^[3]، وفي الكهوف القديمة وجد بصمات اليدين قبل (3000عام)، ومنذ ذلك الوقت بدأ هذا العلم بالتطور وتدرج من الطرق التقليدية مثلا (كاستخدام كلمة السر، بطاقة الهوية) التي ممكن تخمينها أو الحصول عليها الى محاولة محاكاتها لنظم آليه تستخدم لتمييز الاشخاص البيا. ان استخدام هذه المقاييس في أنظمة التعرف على الاشخاص بدلا من الانظمة التقليدية هو لتعزيز السلامة العامة والامن القومي بما في ذلك تحديد المطلوبين للأجهزة الامنية والكشف عنهم، وتنظيم الدخول للاماكن، توفير مراقبة الوصول للمعلومات للحد من الغش وتحسين الخدمات الاجتماعية والطبية وتنفيذ التعاملات التجارية، توجد العديد من التطبيقات التي تستخدم هذه الانظمة ويمكن تصنيفها الى ثلاث مجاميع^[4] موضحة بالجدول (1).

ان استخدام احد هذه السمات (الجسدية والسلوكية) غير كافية لإنجاز عملية التحقق كما في انظمة (unibiometric) التي تستخدم ميزة واحدة (مصدر واحد للبيانات الحيوية) والتي تكون غير كافية لتلبية عدد من متطلبات النظام بما في ذلك مطابقة الأداء التي تفرضها العديد من التطبيقات المصادقة على نطاق واسع. نظم Multibiometric تسعى إلى الحد من بعض العقبات التي تواجهها أنظمة unibiometric لتعزيز الأدلة المقدمة من المصادر البيومترية المتعددة اذ ان (multibiometric system) يتم الحصول فيها على عدة بيانات بيومترية (قبول اثنين أو اكثر من المدخلات الحيوية) في نفس الوقت بدلا من ميزة واحدة لنقدم نتائج تحديد أكثر موثوقية لنظام التحقق من الهوية وبيانات أكثر امنية وفي حالة فشل احدى العينات ممكن ان نعتمد على الاخرى، وهذا يمثل حاجة ملحة في الانظمة التي تتطلب دقة عالية ونظم توثيق على نطاق واسع مثل (عبور الحدود، قاعدة بيانات عسكرية)، أن متطلبات التخزين، والوقت اللازم للتجهيز والمتطلبات الحسابية لنظام Multibiometric يمكن أن يكون أعلى بكثير. ومن المعوقات التي تواجه النظم البايومترية كثيرة كالتقدم بالعمر، البيئة، المرض، الاجهاد، عوامل اجتماعية وثقافية أو دينية.

جدول (1) تطبيقات المقاييس الحيوية^[4]

Forensic تطبيقات الطب الشرعي (applications)	تطبيقات الحكومية (Government applications)	التطبيقات التجارية (Commercial applications)
- التعرف على الجثث - التحقيق الجنائي - اثبات النسب - الاطفال المفقودين	- بطاقة الهوية الوطنية - أجازه السوق، تسجيل الناخبين - عبور الحدود، فحص الجوازات في المطار. - ادارة شؤون السجناء - الضمان الاجتماعي والرعاية الاجتماعية	- اجهزة الصراف الالي (ATM)، استخدام البطاقة الائتمانية. - مراقبة الدخول للاماكن، تسجيل الدخول الى الحاسوب. - الهاتف المحمول - التجارة الالكترونية، الانترنت، البطاقة الذكية، التعاملات المصرفية. - ادارة السجلات الطبية، التعلم عن بعد

2. 1 وظائف القياسات الحيوية:

تنقسم الى قسمين:

- **التحقق (Verification):** تستخدم للتأكد من هوية الشخص المدعي تسجيله بالنظام بمقارنة البيانات البيومترية المكتسبة مع القالب (template) المخزن مسبقاً في قاعدة بيانات النظام، المطابقة تكون (one to one)، تعطى صوره البيانات للنظام والنظام يخبرنا اذا التخمين صح أو خطأ، الأشخاص الذين يحاولون الحصول على اذن الدخول هما فئتان اما (Clients) الدخول باستخدام الهوية الخاصة بهم، أو (Imposters) الذين يحاولون الوصول للنظام باستخدام هوية مزوره معروفه للنظام ولكن لا ينتمون اليها. أن الهدف هو منع اشخاص اخرين من استخدام نفس الهوية.
- **كشف الهوية (Identification):** يتعرف النظام على الشخص من خلال البحث في القوالب المخزنة لكافة المستخدمين في قاعدة البيانات لغرض مطابقة العينة، وبالتالي النظام يجري مقارنة بطريقة (one to many) ليبين هوية الشخص أو يفشل إذا كان من غير المسجلين في قاعدة بيانات النظام. النظام يخبرنا الهوية الأكثر احتمالاً من هو أو من هي. يستخدم في التطبيقات التي لا تتطلب تفاعل المستخدم، أي تطبيقات المراقبة.

2.2 عمل أنظمة القياسات الحيوية: نظم القياسات الحيوية هو أساساً نظام تمييز أنماط الذي يكتسب البيانات البيومترية من

الشخص، ويستخرج مجموعة السمات البارزة من البيانات، ويقارن هذه المجموعة من الميزات مع مجموعة الميزات المخزنة في

قاعدة البيانات، وينفذ العمل بناء على نتيجة المقارنة. توجد اربع وحدات رئيسية بشكل عام لعمل نظم القياسات الحيوية:

1. **Sensor module:** يتطلب قارئ أو ماسح ضوئي أو كاميرا للحصول على البيانات البيومترية الخام للفرد (سلوكية أو جسمية) يجب ان يكون الجهاز ملائم للمواصفات المطلوبة لان البيانات تتأثر بالخصائص التكنولوجية.
2. **Quality assessment and feature extraction module:** تقييم جودة البيانات التي تم الحصول عليها من جهاز الاستشعار لتحديد مدى ملائمتها للمعالجة ويتم اخضاع البيانات الى خوارزمية لغرض تحسين جودة البيانات واحياناً تكون نوعية البيانات غير جيدة لذلك يطلب من المستخدم اعادة تقديم البيانات البيومترية مره اخرى. ثم تتم معالجة البيانات البيومترية ومجموعة الميزات البارزة التمييزية المستخرجة لتمثيل السمة الأساسية (underlying trait).
3. **Matching and decision-making module:** مقارنة feature المستخرجة مع القوالب templates المخزنة لتوليد نتائج المطابقة. ويتم ايجاز صنع القرار الذي يستخدم نتائج المطابقة اما للتحقق من هوية المدعي أو تصنيف هويات المسجلين من اجل تحديد الشخص.
4. **System database module:** تعمل قاعدة البيانات كمستودع للمعلومات البيومترية. أثناء عملية التسجيل، مجموعة الميزات المستخرجة من نموذج البايومتري الخام (template) والمخزنة في قاعدة البيانات ربما مع بعض المعلومات ببيوغرافية (مثل الاسم ورقم التعريف الشخصي (PIN)، العنوان، إلخ) الذي يتصف به المستخدم.

2. 3 خصائص المقاييس الحيوية:

- المقاييس البيومترية لها عدة خصائص يتم استخدامها في تطبيقات مختلفة وكل واحد من هذه المقاييس لها ايجابيات وسلبيات وان استخدام واحد منها لتطبيق معين يعتمد على مجموعه من القضايا الى جانب ادائها. حددت [5] (Jain A.K., 1999) سبعة عوامل التي تحدد مدى ملائمتها للخصائص الجسدية أو سلوكية لاستخدامها في التطبيق البيومتري. وفيما يلي الخصائص:
1. **Universality** الشمولية: وهي معيار اساسي يجب ان يمتلك هذه السمة (trait) كل شخص له حق الوصول للتطبيق ولا يقتصر وجودها عند فئة معينة من الاشخاص.
 2. **Uniqueness** تفرّد: السمة المعطاة يجب ان تكون مختلفة للأفراد حتى بين التوائم ولا يمكن استنساخها.
 3. **Permanence** دائمة: يجب ان تكون السمات البيومترية ثابتة لا تتأثر بتقدم العمر بشكل كبير لأنها ستكون غير مفيدة فيما يخص خوارزمية المطابقة.

4. **Measurability** قابلة للقياس: يجب أن تكون البيانات الخام المكتسبة قابلة للمعالجة لاستخراج مجموعة ميزات (feature) تمثلها بصورة جيدة، وينبغي أن يكون من الممكن اكتساب ورقمته السمات البايومترية باستخدام الأجهزة المناسبة التي لا تسبب إزعاج للأفراد.

5. **Performance** الاداء: دقة التعرف والمصادر المطلوبة لتحقيق الدقة يجب ان تلبي متطلبات التطبيق.

6. **Acceptability** إمكانية القبول: يجب ان يكون الاشخاص في المجتمع المقصود مستعدين لتقديم السمة البايومترية للنظام للاستفادة من التطبيق.

7. **Circumvention** التحايل: هذا يشير الى تقليد السمة البايومترية اثناء دخول المستخدم الحقيقي الى النظام و اخذ نسخة منها (الاصابع المزيفة، قناع الوجه، تسجيل الصوت، نسخة من التوقيع، ..الخ) على سبيل المثال يمكن الحصول على البصمة من تعامل المستخدم مع الأجهزة كالهاتف أو الاماكن التي يذهب اليها وباستخدام تقنيات بسيطة يمكن الحصول على صورة من بصمة الإصبع واستنساخها تمكنوا من التحايل والوصول بنجاح للأجهزة. هذا يعني ان السمات المستخدمة يجب ان تتوافق مع المتطلبات الامنية للتطبيق.

جدول (2) مقارنة بين القياسات الحيوية^[6]

ت	القياسات الحيوية	تاريخ	الايجابيات	السلبيات
1.	بصمة الاصبع Fingerprint	الستينات	- سهولة الاستخدام والتتصيب عادة - تكلفة منخفضة - سرعة عالية لعملية التحقق - يتطلب معدات غير مكلفة - هي المقياس الأكثر تفضيلاً - الدقة عالية - تستهلك ذاكرة قليلة	- صعوبة التعرف على البصمة نتيجة العمل كحرفيين أو كيميائيين - يمكن التحايل على النظام - يتطلب اتصال مباشر مع الجهاز مما يسبب إزعاج البعض، وكذلك يكون وسط ناقل للجراثيم
2.	القرنية Iris	1949 استخدمت رسومات الحدة للتعرف الشخصي سجلت بوضوح في كتاب (جيمس دوجارت) - طورت كنظام في التسعينات	- لا يتطلب اتصال جسدي مع الجهاز - عملية التعرف عالية السرعة والدقة - ثابتة ولا تتغير مدى العمر - حجم القالب صغير لذلك عملية التحقق تستغرق من (2-5 ثواني) - لا يؤثر ارتداء العدسات اللاصقة أو النظارات على عملية التعرف	- أجهزة المسح الضوئي لها تكون تكلفتها عالية - تكون مزعجة وصعبة للضبط لاختلاف قامات الأشخاص - تتأثر الدقة بتغيرات الإضاءة - الأشعة تحت الحمراء تسبب إزعاجات لمرضى السكري - قد يندفع الماسح الضوئي بالصورة عالية الجودة - يتطلب وضعية مناسبة لغرض اخذ البيانات
3.	الوجه face	الستينات	- سهولة الاستخدام - غير تدخلية لا تتطلب اتصال مباشر من قبل الأشخاص - يمكن استخدامها في الاماكن العامة - تصلح للمراقبة	- تتأثر عملية التعرف بعدة عوامل (وقفه الشخص من الكامير، تعابير الوجه، الإضاءة، النظارات، الشعر الطويل، الشيخوخة، حجب الوجه وجود نقاب أو استخدام كاميرات) أثناء الحصول على الصورة - دقة الصور - مكلفه، ومعقده نوعا ما

4.	اليدين Hand geometry	• في السبعينات	• بسيطة • سهلة الاستخدام	• غير دقيقة جدا • مناسبة للبالغين وليس الاطفال • تتطلب اتصال جسدي • تتأثر في الحالات المرضية للعظام والمفاصل
5.	النقر على لوحة المفاتيح Keystroke	• بدء الاهتمام بها في منتصف القرن 19 اثناء الحرب العالمية الثانية، يمكن لمستخدمي التلغراف تحديد بعضهم البعض	• لا تتطلب اجهزة خاصة • يمكن الحصول على المعلومات بشكل سري • سريع وامن • غير مكلفه	• الايقاع على لوحة المفاتيح يتأثر (المرض، الكحول، تغيير اللوحة) • ايقاع الكتابة قابل للتغير خلال اليوم.
6.	المشي Gait	• قدم مقترح Murray في الدراسات النفسية 1967،	• غير تدخله اي لا تحتاج اتصال مباشر بالجهاز لاختذ المعلومات كما في بعض المقاييس الاخرى • صعب اخفاؤها أو سرقتها • يمكن استخدامها للكشف عن الاضطرابات الصحية من خلال التغير في نمط المشي • تفيد في عمليات المراقبة، يمكن معرفة هوية الشخص دون علمه	• تؤثر عدة عوامل على عملية التعرف منها (طبيعة الارض، نوع الملابس والاحذية، تعاطي المخدرات والكحول، التغير بالوزن، الامراض) • قد لا تكون موثوقة • غير جيدة في الاماكن المفتوحة على عكس المغلقة • تؤثر الزاوية التي تم التقاط الصورة فيها
7.	التوقيع Signature	• الثمانينات	• مقبول على نطاق واسع • غير تدخلية	• العوامل التي تؤثر عليه (المرض، التقليد، الظروف العاطفية والمادية). • متغير بمرور الوقت.
8.	الصوت Voice	• الخمسينات	• سهل التنفيذ • اسرع من بعض المقاييس الاخرى • يساعد ذوي الاحتياجات الخاصة • لا يتطلب تدريب للمستخدمين • معالجة الاخطاء الاملائية بشكل اسرع	• الصدى وتداخل الاصوات في البيئة المحيطة • تغيره مع التقدم بالعمر • سهولة التقليد أو اخذ نسخة مسجلة • يتأثر الصوت بالمرض • مكلفة

3. نظام التعرف على الوجوه: ان بناء نظام للتعرف على الاشخاص من خلال الوجه تلقائيا بدلا من الانظمة الاخرى الواردة اعلاه نظرا لما يتمتع به هذا المقياس من سهولة الاستخدام ولا يتطلب تعاون من قبل الاشخاص مما يجعله مفيد جدا للمراقبة، اذ يتم الحصول على المعلومات من خلال النقاط صورة أو اطار (frame) لمقطع فيديو من كاميرا رقمية، ان هذه الصور اما تكون ثنائية أو ثلاثية الابعاد (7) حسب متطلبات التطبيق والغرض المستخدم لأجله، ان الانظمة الثنائية الابعاد تكون دقتها منخفضة بسبب التغيرات في الاضاءة والاختلاف في التعبيرات واختلاف وضعية الوقفة امام الكاميرا، ومن اجل التغلب على هذه التحديات تم استخدام الصور الثلاثية الابعاد في انظمة التعرف نتيجة للتطور في تقنيات الماسح الضوئي الثلاثي الابعاد، مع ذلك هناك تحديات لهذا النظام فالمشكلة الرئيسية هي التكلفة العالية لهذه الاجهزة وللتغلب على هذه المشكلة قدم الباحثون طرق لدمج

الطريقتين والوصول الى نتائج من شأنها الاستغناء عن هذه الاجهزة. ان انظمة التعرف على الوجه كنظام بايومتري اما ان تعمل في احد الوضعين أو كلاهما: التحقق (verification): يقارن صورته الوجه المستفسر عنه مع الوجه المسجل للتحقق من صحة هوية الشخص (المدعي)، أو الكشف عن الهوية (Identification): مقارنة الوجه المستفسر عنه مع كل الوجوه الموجودة في قاعده البيانات المخزنة لكشف الهوية). هناك عدة امور تؤخذ بنظر الاعتبار عند تصميم النظام منها:

■ **تعاون المستخدم:** يمكن تقسيم تطبيقات التعرف الى الوجه الى فئتين اعتمادا على تعاون المستخدم:

○ **Cooperative التعاوني:** في هذا النوع من التطبيقات يكون المستخدم متعاون اي يعرض الوجه بطريقه ملائمة (العيون تكون مفتوحة، تعابير الوجه طبيعية، الوقفة مناسبة لزاوية الكاميرا) للنظام ليمنح وصول أو امتياز خاص. مثال على ذلك جواز السفر الالكتروني، التحكم بالوصول، تسجيل الدخول للحاسوب.

○ **Noncooperative غير متعاون:** اي ان المستخدم لا يدرك ان النظام يقوم باستخدام بيانات الوجه والتعرف عليه من مسافه، كما في تطبيقات مراقبة الفيديو ولغرض امني تتم بشكل سري دون علم الشخص ان النظام يتتبعه ليتحقق من بيناته.

■ **المسافة:** ويقصد بها بعد المستخدم من الكاميرا ان بعض تطبيقات التعرف على الوجه تصنف من ناحية المسافة الى: near-distance (تستخدم غالبا في التطبيقات cooperative) تتم من مسافة قريبة حيث يمكن للكاميرا التقاط صور عالية الدقة واكثر وضوح كما في انظمة تسجيل الدخول سواء للاماكن أو الحاسوب، أما في الانظمة التي تتطلب امنية وسرية وعدم التعاون كما في انظمة المراقبة هناك حاجة للتعرف على الوجه من مسافه بعيدة (FRAD)، ويستخدم في ذلك نوعان من الكاميرا: stationary cameras عالية الوضوح و Active-Vision Systems تغطي مساحة واسعة مع دقة منخفضة للصور. ان نظام التعرف على الوجه من مسافة FRAD (Face Recognition at a Distance) (شكل 1)) يواجه نوعان من الصعوبات الرئيسية أولا: الحصول على صور الوجه من مسافة بعيدة، ثانيا: التعرف على الشخص على الرغم من العيوب (مثل جودة الصور منخفضة، عدم وضوح الصورة الملتقطة Out of Focus بسبب بعد المسافة للوجه عن الكاميرا، التداخل Interlace تداخل اطارات الفيديو بسبب الحركة السريعة للوجوه فتظهر في مواقع مختلفة، Motion blur بسبب حركة الاجسام بسرعة أو اهتزاز الكاميرا) في البيانات التي تم التقاطها. ويستخدم هذا النظام في العديد من التطبيقات التجارية، والامنية منها:

- **Access control:** فتح الأبواب عندما يقترب الأشخاص.
- **Watch-list recognition:** اصدار تنبيه عند كشف شخص مشير للاهتمام (ارهابيين، مجرمين، موظفين غير مخولين).
- **White-list recognition:** اصدار تنبيه كلما تم الكشف عن شخص غير مصرح له الدخول
- **Rerecognition:** التعرف على الاشخاص بواسطة كاميرا مراقبه تلقائيه وتتبعهم.
- **Event logging:** اختيار افضل صورته لكل شخص يدخل المنطقة
- **Marketing:** فهم انشطة وسلوك العملاء.



شكل (1) تبين عملية التعرف على الوجه من مسافه بعيدة وفي الهواء الطلق، نوع الكاميرا المستخدمة (PTZ camera) [15]

■ مصدر المعلومات: نوع الجهاز المستخدم لالتقاط الصور:

○ كاميرا مراقبة (اما ثابتة يتم تنصيبها في مكان مناسب لمراقبة مشاهد معين، أو متحركة: تكون لها قابلية الدوران والتكبير والتصغير تكون عملية في المراقبة والملاحقة) أو كاميرا رقمية لالتقاط صورة أو مقطع فيديو.

○ باستخدام الأشعة تحت الحمراء infra-red: تستخدم للكشف والتعرف على الوجوه وهي طريقة فعالة للتغلب على التغيرات في الإضاءة، هذه الأشعة تكشف الأوردة والانسجة وهيكال الوجه وهي فريدة كبصمات الاصابع. التحديات التي تواجه هذا النوع: كلفة عالية لأجهزة الاستشعار الحرارية، الدقة منخفضة وارتفاع مستوى الضوضاء في الصور، لا توجد قاعدة بيانات متاحة على نطاق واسع للصور بالأشعة تحت الحمراء، ارتداء النظارات ممكن يحجب جزءا من الوجه بسبب انعكاس الأشعة على الزجاج، هذه الأشعة حساسة للتغيرات في درجة الحرارة.

○ شبكة كاميرات: Camera Network يتم التقاط صور متعددة في وضعيات مختلفة ومن زوايا مختلفة في لحظة زمنية معينة لغرض الاستفادة وتكامل المعلومات كما موضح بالشكل (2). يجب معرفه كيف تستغل هذه المعلومات في لحظة زمنية لتتبع افضل صوره وجه. الاستفادة من المعلومات التي تم جمعها من الكاميرات، يجب ان تكون الطريقة قادره على معالجة الاختلافات pose، اخذ البيانات الاقرب مسافة ووضح دقه.



شكل (2) عده صور ملتقطة بواسطه كاميرات متعددة بمختلف الوضعيات [4]

■ بيئة النظام: تصميم النظام أو عمل تطبيق على الهاتف أو على الحاسوب

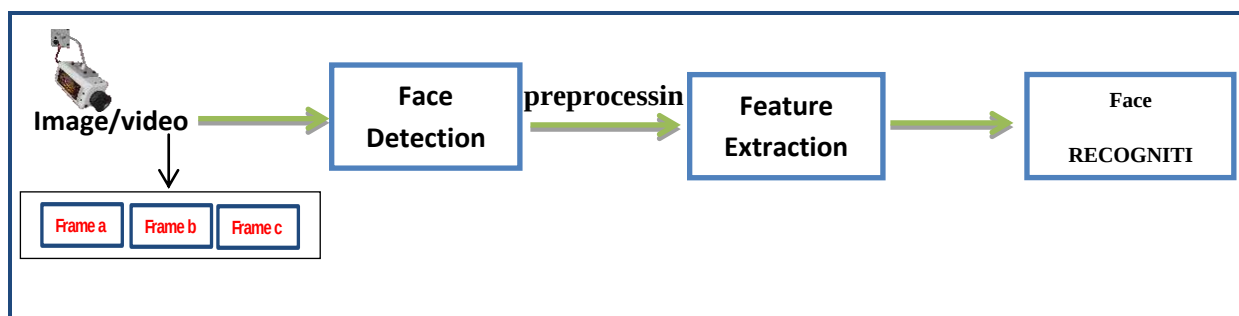
■ الغرض من النظام: مراقبة، أمنية، تسجيل دخول.

■ قاعدة البيانات: ماهي قاعدة البيانات التي ستطبق عليها الدراسة، اذ ان هناك العديد من قواعد البيانات المتوفرة على شبكة الانترنت (جدول رقم (3)). وتشمل هذه القواعد مجموعه من الاشخاص بلقطات مختلفة تحت ظروف مختلفة (منها: عوامل داخلية Intrinsic factors وعوامل خارجية Extrinsic factors)، وان اداء انظمة التعرف على الوجه يعتمد بشكل كبير على مجموعه العوامل هذه، تتضمن العوامل الداخلية التغيرات التي تحدث للخصائص الجسدية اما متعلقة بالشخص نفسه Intrapersonal factors (التغيرات بمظهر الوجه نتيجة: التقدم بالعمر age، اختلاف تعبيرات الوجه facial expression، facial paraphernalia (شعر الوجه، النظارات، مستحضرات التجميل)) أو بين الاشخاص Interpersonal factors اي اختلاف مظهر الوجه في خصائص يشترك بها الاشخاص من نفس الجنس أو العرق. العوامل الخارجية تشمل التغيرات التي تحدث بمظهر الوجه نتيجة اختلاف الإضاءة، الوقفة اتجاه الكاميرا pose، الحجم scale (اي صوره الوجه قد تبدو بأحجام مختلفة داخل المشهد)، ضوضاء، الدقة، تركيز الكاميرا. أو بناء قاعده بيانات حسب الدراسة التي يقوم بها الباحث.

جدول (3) يوضح بعض قواعد البيانات المتوفرة على الانترنت

Face databases	Resources
Caltech Faces	http://www.vision.caltech.edu/html-files/archive.html
CASIA-3D FaceV1	http://biometrics.idealtest.org/dbDetailForUser.do?id=8
Face Recognition Data, (faces94, faces95, faces96, grimace)	http://cswww.essex.ac.uk/mv/allfaces/index.html
Face Video Database	http://vdb.kyb.tuebingen.mpg.de/
FERET database	http://www.itl.nist.gov/iad/humanid/feret/
Georgia Tech face database	http://www.anefian.com/research/face_reco.htm
Large Age-Gap Face Verification	http://www.ivl.disco.unimib.it/activities/large-age-gap-face-verification/
SCface database	https://link.springer.com/article/10.1007%2Fs11042-009-0417-2
SoF Dataset	https://sites.google.com/view/sof-dataset
UT Dallas database	http://www.utdallas.edu/dept/bbs/FACULTY/PAGES/otoole/database.htm
XM2TVS database	http://www.ee.surrey.ac.uk/Research/VSSP/xm2vtsdb/
Yale face database	http://cvc.cs.yale.edu/cvc/projects/yalefaces/yalefaces.html
Yale face database B	http://vision.ucsd.edu/~leekc/ExtYaleDatabase/Yale%20Face%20Database.htm

3. 1 هيكلية النظام: يتكون نظام التعرف على الوجوه بشكل عام من الخطوات الموضحة بالشكل رقم (3) .



شكل (3) يوضح المخطط العام لنظام التعرف على الوجه

▪ **Face Detection:** اول مرحلة من مراحل النظام الآلي للتعرف على الوجه، ويقصد بها عملية استخلاص منطقة الوجه من الخلفية، سواء كانت صورة أو مقطع فيديو من خلال التتبع والملاحقة، اذ يتم تحديد الوجوه واستخراجها من المشهد، تتضمن هذه المرحلة أمرين مهمين:

- هل هناك وجوه أشخاص بالمشهد؟
- أين تقع هذه الوجوه ؟

تطبق قواعد لتصنيف الانماط الى فئتين اما وجه أو غير وجه، بعد كشف الوجه ستكون مخرجات هذه المرحلة هي (patches) التي تستخدم مباشرة في المرحلة اللاحقة. عملية كشف الوجه تتأثر بعدة عوامل حتى وان كانت الصورة مأخوذة لنفس الشخص (rotation, brightness, size,.. etc.) لذلك نحتاج الى معالجة Preprocessing لغرض تعزيز عملية Feature

Extraction والحصول على نتائج قوية، اما في الوقت الحالي بعض تطبيقات التعرف على الوجه لا تحتاج الى هذه الخطوة لان في بعض الحالات صور الوجه تكون مخزنة في قاعدة بيانات.

هناك العديد من طرق كشف الوجه، لا يوجد تصنيف عالمي لتصنيف الخوارزميات لكن البعض يصنفها اعتمادا على عدة سيناريوهات (بيئة متحكم فيها من ناحية الاضاءة وهنا تستخدم تقنيات بسيطة للكشف عن الحافة، الصور الملونة حيث يتم الكشف عن الوجوه على اساس لون البشرة، كشف الوجه في الفيديو آنياً)، لخص الباحثين طرق كشف الوجه الى اربع فئات:

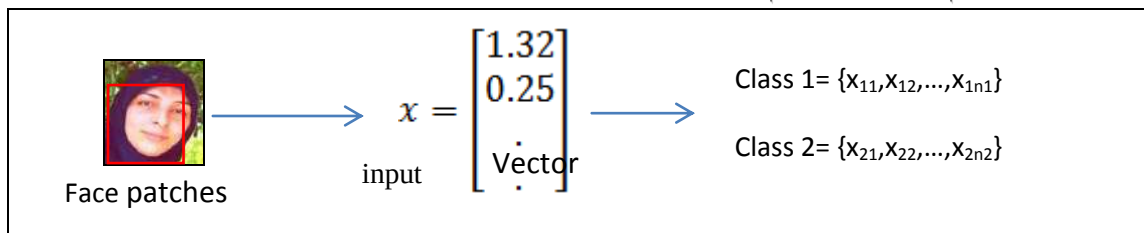
1. **Knowledge-based methods** (الطرق المستندة على المعرفة): تستخدم مجموعة من القواعد لوصف ملامح الوجه والعلاقة فيما بينهم باستخدام المسافات النسبية ومواقع الملامح. بنيت هذه القواعد من المعرفة الإنسانية بديهية لمكونات الوجه على سبيل المثال الوجه دائما يحتوي على عينين وانف وفم حيث ان العينين تقع على خط مستقيم واحد ومركز العينين والفم والانف يشكل مثلث.

2. **Feature invariant approaches**: تهدف هذه الخوارزميات البحث عن الميزات الهيكلية حتى في حالة اختلاف (pose) الوقفة بالنسبة للكاميرا، أو ظروف الاضاءة)، واستخدامها لتحديد الوجه، وصممت اساسا لتحديد موقع الوجه

3. **Template matching methods** طرق مطابقة القالب: تبني قالب واحد أو أكثر من قالب (نماذج) لوصف ملامح الوجه. العلاقة بين الصورة المدخلة ونموذج بناء تمكن من التمييز اذا يوجد وجه ام لا. هذه الطريقة بسيطة وسهلة التنفيذ لكن نتيجة التعرف تعتمد على حجم القالب للصورة، الاتجاه والوقفة بالنسبة لزاوية الكاميرا، والشكل.

4. **Appearance-based methods**: تستخدم التحليل الاحصائي وتقنيات التعلم الالي لاستخراج الميزات الأكثر صلة للوجه وغير الوجه. وهي طريقة ناجحة وتصمم اساسا للكشف الوجه.

▪ **Feature Extraction**: ان (feature) هي مرادف (input variable) أو (attribute)، وهي معاملات تحسب باستخدام معادلات رياضية أو احصائية، استخراج الميزات يتضمن تقليل كمية المصادر المتطلبة لوصف مجموعه كبيره من البيانات وذلك لان تحليل مثل هذه المجاميع يتطلب ذاكرة اكبر ويستغرق وقتا اطول في المعالجة، فالغرض منها الحصول على بيانات اكثر دقة وبسيط شكل لوصف البيانات الاصلية واهمال البيانات الغير ضرورية، ان تحليل مشكلة استخراج الميزات تتضمن خطوتين: بناء الميزة واختيار الميزة، بناء الميزات هي احدى الخطوات الرئيسية لتحليل البيانات وتعد شرطا لنجاح اي احصاءات لاحقه أو عملية تعلم، اما عملية اختيار ميزة دون اخرى لتقليل البيانات ومتطلبات الخزن وزيادة سرعة الخوارزمية وتوفير البيانات للاستفادة منها فيما بعد وتحسين الاداء وفهم البيانات وكيف تم توليدها.



شكل (4) يوضح عملية الكشف واستخلاص الميزات.

تستخدم (patches) المستخلصة من الصورة بعد عملية (Face Detection) لتمييز الوجه كما موضح بالشكل (4). وبعد هذه المرحلة (Face patches) تحول الى: (vector) مع بعد ثابت، ومجموعة (fiducial points)، هذا (feature vector) الناتج من هذه العملية يطابق مع (classes) مجموعة صور الوجوه للأشخاص المسجلين في قاعدة البيانات. المعوقات التي تواجهها في هذه المرحلة هي عدد البكسلات المكونة للصورة يمكن ان يكون كبير جدا مما يؤثر على بناء النظام، اختلاف الكاميرا المستخدمة لالتقاط الصورة من ناحية المحاذاة والاضاءة وتعبيرات الوجه. يمكن تمييز ثلاث أنواع من طرق استخراج الميزات:

1. **generic methods**: هذه الطرق تستند على الحواف، الخطوط، المنحنيات.

2. feature-template-based methods: تستخدم للكشف عن ملامح الوجه.

3. structural matching methods: تأخذ بنظر الاعتبار القيود الهندسية على الميزات.

▪ **Face recognition**: هذه الخطوة تعمل بعد عملية كشف الوجه للصورة المدخلة واستخراج الميزات لها ثم تحديده من خلال المقارنة مع قاعدة الوجوه المخزنة التي تم بنائها لكل شخص مع خصائصه في قاعدة البيانات، اختلف الباحثون في تقسيم تقنيات التعرف على الوجوه بسبب تنوع الطرق وتداخلها مع بعضها في كثير من الاحيان من اجل تحسين الاداء والتغلب على المشاكل الموجودة في كل تقنية، منها صنفت وفق دراسات علم النفس حول كيف يستخدم البشر السمات في التعرف أو تصنف حسب الطريقة التي يجمع بها البيانات، أو تصنيف التقنيات حسب Face (Image-Based Face Recognition), (Video-Based Recognition):

أولاً. Image-Based Face Recognition:

1. **Feature-based approaches**: أو (Local-based methods) في هذه الطريقة اول عملية تجري على صورة الوجه المدخلة هي تحديد واستخراج ملامح الوجه المميزة (أنف، عينيّين، فم) بالإضافة الى العلامات المرجعية (fiducial marks)، واحتساب (geometric relationships) بين هذه النقاط المرجعية وبالتالي تقلل الصورة المدخلة الى vector من الميزات الهندسية.

- المحاسن: الميزة الرئيسية لهذه الطرق يتم استخراج الميزات أولاً، من حيث المبدأ قوية نسبياً للتغيرات المواقع في الصورة المدخلة
- المساوئ: صعوبة الكشف عن الميزات تلقائياً.

2. **Holistic matching methods**: تسمى ايضاً (appearance-based approaches) هذه الطريقة تستخدم كامل الوجه كمدخلات خام، بدلاً من التركيز على الملامح الرئيسية من الوجه، تقسم هذه الطرق الى مجموعتين:

▪ **Statistical**: صوره الوجه تمثل كمصفوفه من البكسلات (high-dimensional)، الهدف هو اختيار وتطبيق الاداة الاحصائية المناسبة لاستخراج وتحليل (manifold)، هذه الادوات تحدد منطقة الوجه ضمن مساحة الصورة واستخراجها، وبهذا فان الانماط التي تنتمي لصنف معين ستتقارب في مواقعها وبالتالي ممكن تحديد اصنافها واختيارها كسمات، العديد من هذه الطرق لا تستخدم وحدها وانما يتم التعديل عليها من قبل الباحثين للحصول على نتائج افضل.

▪ **AI approaches**: هذه الطريقة تستخدم تقنيات تعلم الآلة والشبكات العصبونية لتمييز الوجوه.

ان الميزة الرئيسية لهذا النهج (Holistic) هو التركيز على مناطق محدده أو النقاط المثيرة للاهتمام وبالتالي لا تلغي اي من معلومات الصورة، ومع ذلك هذه الميزة تشكل عائقاً كبيراً لان اغلب هذه الطرق تفترض ان كل بكسل له نفس الدرجة من الاهمية مما يجعل هذه التقنيات مكلفة حسابياً وتتطلب درجة عالية من الترابط بين صور الاختبار والتدريب كما انها غير فعاله في حالة اختلاف الموضع (pose) بالنسبة للكاميرا والتغيرات بالإضاءة. العديد من الخوارزميات اجريت عليها تحسينات للتغلب على هذه المشاكل.

3. **Hybrid method**: يستخدم كلا النهجين (holistic, local features) كما يستخدمها نظام الرؤية البشري، تشمل العوامل الرئيسية التي تؤثر في أداء النهج الهجين كيفية تحديد السمات التي يجب أن تكون مجتمعة وكيفية الجمع بينها، وذلك للحفاظ على مزاياها وتجنب عيوبها في نفس الوقت. وعلى الرغم من البحوث الكثيرة والافكار التي طرحت لاتزال هناك مشاكل لم تحل. مكونات نظام هجين، يجب أن تكون دقيقة ومتنوعة. هذه الطرق لديها القدرة على تقديم أداء أفضل من الأساليب (holistic) أو (local features)، حيث يمكن الاستفادة منها لمعلومات أكثر تفصيلاً.

ثانياً. Face Recognition from Video Sequences:

يعتبر الفيديو من المصادر الغنية بالمعلومات، والتحدي الرئيسي هو كيفية استغلال هذه المعلومات للوجه والجسم التي يوفرها المقطع كاختلاف في (الإضاءة، الإيماءات، الحركات، التعبيرات،...) واستخدامها في التعرف. النقاط المعلومات يتم اما باستخدام (single camera) كاميرا واحده مثبتة في جهة معينة أو باستخدام (camera networks) التي توفر صور متعددة بأوضاع

مختلفة في لحظة زمنية معينة وتسمح بتكامل المعلومات من مختلف زوايا النظر. ان نظام التعرف على الوجه المستند على الفيديو يتكون من ثلاث مراحل رئيسية كما موضح بالشكل:

- **detecting the face**: كشف الوجه ضمن اطار الفيديو
- **tracking**: تتبع أو ملاحقة الوجه، الرأس أو سمات معينة في الفيديو، حيث ينفذ باستخدام مختلف الطرق يمكن تصنيفها الى: 2D/3D dimensional, head tracking.
- **recognizing**: يشمل التعرف والتي يمكن ان تستخدم الطرق السابق ذكرها في (still images)، احد التطبيقات الرئيسية هي المراقبة وتستخدم المعلومات من الفيديو لغرض امني، التحكم بالوصول، امن المعلومات، ان استخدام التعرف على الوجه على اساس الفيديو يكون أفضل من (still images). ان استخدام هذا النهج يوفر عدة مزايا منها:
- النظام يوفر كمية هائلة من البيانات تمكن من اختيار افضل اطار يحتوي على الصورة المناسبة وتجاهل الصور الاقل وضوحا.
- يوفر تسلسل زمني مما يتيح تصنيف المعلومات يمكن جمعها من عدة اطراري وبالتالي يحسن من اداء التعرف.
- يسمح الفيديو بتتبع صور الوجه تحت ظروف مختلفة مثل اختلاف التعبيرات، تنوع الوقفة بالنسبة للكاميرا (pos)، كلها يمكن الحصول عليها من مقطع الفيديو وبالتالي تحسين الاداء.
- توفر (Dynamic schemes) امكانية كشف وجه في مشهد افضل من (static)، حيث ان هذه المخططات تستخدم الحركة لاقتطاع والكشف عن الوجه لشخص يتحرك.
- اما المساوئ:

- low quality images: الصورة ممكن ان تكون ذات جوده منخفضه ويمكن تحسينها باختيار تقنيات فائقة الدقة.
- cluttered backgrounds: الخلفية ممكن تكون مشوشه أو وجود اكثر من وجه في المشهد الواحد مما يتطلب معالجة اكثر.
- Face images are small: حجم الصورة قد يكون اصغر بكثير من الحجم المطلوب من قبل النظام المستخدم، وتكون اصعب في التعرف وتؤثر على دقة الوجه المستقطع.

3. 2 المقاييس المعتمدة:

ان تنوع خوارزميات التعرف على الوجوه اظهر الحاجة الى ايجاد طرق ومقاييس تستخدم لتقييم اداء هذه الخوارزميات مما اسهم في تطويرها بشكل افضل، وان اداء خوارزمية أو نظام في ظروف معينة أفضل من غيرها وكذلك الانظمة التجارية، كما ان هذه المقاييس بينت ان نسبة التعرف على الرجال اسهل من النساء، ان هذا التقييم عمل من قبل معهد الوطني للمعايير والتكنولوجيا في 1994, 1995, 1996 ويعرف بروتوكول (FRVT) Face Recognition Vendor Test، وينص على كيفية اجراء التقييم وحساب النتائج. ومن هذه البروتوكولات المعتمدة:

- The FRVT 2000: ويتألف من جزئين: اختبار اداء التعرف الذي يقيم التكنولوجيا ويهدف لمقارنة التقنيات المتنافسة لاداء التعرف على الوجوه، واختبار قابلية استخدام المنتج وفحص استخدام خصائص اداء نظام التحكم.
- FRVT 2002 protocol: صمم للتقييمات البايومترية بشكل عام وليس فقط لتقييم خوارزميات التعرف على الوجه.
- FRVT 2006: الهدف منه هو قياس تقدم انظمة وخوارزميات التعرف على الوجه التجارية، ويقيم اداء للصور العالية الدقة.

4. الاستنتاجات:

تم تقديم نظام التعرف على الوجوه كأحد المقاييس البايومترية المستخدمة لتحقيق من هوية الافراد سواء كان بعلمهم لتسجيل الدخول أو بدون علمهم كما في عمليات المراقبة، وان الاعتماد على هذا المقياس لتصميم نظام كفوء قادر على كشف وتمييز الاشخاص من خلال التقنيات التي تم استعراضها في كل مرحلة بشكل عام، وادراج ثلاث مراحل رئيسية لهيكلية النظام بشكل عام (الكشف، واستخلاص الصفات، التعرف) لانها اساسية في تصميمه، وهناك عمليات اخرى تجرى داخل كل مرحلة لتحسين نتائجها وازالة تأثير العوامل التي تعيق اداء النظام بشكل كفوء.

ان النتائج التي تم الحصول عليها من مرحلة الكشف تطبق عليها معالجة اولية لغرض ضبط الصورة ومحاذاتها وازالة تأثيرات التي تشوه نتائج المرحلة. اما في عملية استخراج الميزات لابد من الاخذ بنظر الاعتبار الزمن المستهلك في الحساب واستهلاك الذاكرة، لأنها تؤثر على مرحلة التعرف واختيار الخوارزمية التي تتلائم مع مدخلات النظام (صورة، أو فيديو).

ان الغرض من هذه الدراسة اعطاء فكرة عامة عن موضوع التعرف على الوجوه بشكل عام ليسهل على الباحث والمهتم في هذا الحقل الالمام بالمفاهيم الاساسية ويكون على دراية بمتطلباته، والاستفادة من المعلومات الواردة اعلاه والتي تم جمعها من أهم الاوراق البحثية والكتب المصدرة. للاستفادة من هذه التقنية في التطبيقات التي تخدم الوطن وخصوصا القضايا الامنية، اذ اقترح تصميم نظام يستفاد من معلومات البطاقة الوطنية بالاعتماد على تقنية التعرف على الوجوه ويستخدم في نقاط التفتيش بدلا من الطريقة الروتينية المتبعة بالتعرف على الاشخاص، وهذا سيعزز الامن ويكشف التزوير ويحد من انتقال المجرمين بين المحافظات، والتعرف على المخطوفين والمفقودين، التعرف على الاشخاص في الحوادث المرورية والوصول الى ذوبهم من خلال قاعدة البيانات بشكل أسرع. معرفة السجل الطبي وتقديم الرعاية اللازمة للمصابين. هذا النظام سيسهل عمل الكوادر الامنية ويحد من الوقت والجهد الضائع.

المصادر

- [1] Bruner, Jerome S., and Renato Tagiuri. "The perception of people. In", Handbook of Social Psychology, vol. II. (Lindzey, G., ed.). (1954)
- [2] De Carrera, Proyecto Fin, and Ion Marques. "Face recognition algorithms", Master's thesis in Computer Science, Universidad Euskal Herriko. 2010
- [3] J. Berry, The history and development of fingerprinting, in H. C. Lee and R. E. Gaensslen (eds) Advances in Fingerprinting Technology. CRC Press, Florida, 1994, pp. 1-38
- [4] Ross, Arun A., Karthik Nandakumar, and Anil Jain. Handbook of multibiometrics. Vol. 6. Springer Science & Business Media, 2006.
- [5] Jain A.K., B. R.. Personal Identification in Networked Society, vNorwell, Mass. Kluwer Academic Publisher. (1999)
- [6] Saini, Rupinder, and Narinder Rana. "Comparison of various biometric methods", International Journal of Advances in Science and Technology (IJAST) 2.1 (2014)
- [7] Zhao, Wenyi, et al. "Face recognition: A literature survey." ACM computing surveys (CSUR) 35.4 (2003): 399-458.
- [8] Jafri, Rabia, and Hamid R. Arabnia. "A survey of face recognition techniques", Jips 5.2 (2009): 41-68.
- [9] Bruce, Vicki, and Andy Young. "Understanding face recognition", British journal of psychology 77.3 (1986): 305-327.
- [10] De Carrera, Proyecto Fin, and Ion Marques. "Face recognition algorithms", Master's thesis in Computer Science, Universidad Euskal Herriko (2010).
- [11] Wayman, James, et al. An introduction to biometric authentication systems. Springer London, 2005.
- [12] J. Berry, The history and development of fingerprinting, in H. C. Lee and R. E. Gaensslen (eds) Advances in Fingerprinting Technology. CRC Press, Florida, 1994, pp. 1-38
- [13] Guyon, Isabelle, and André Elisseeff. "An introduction to feature extraction", Feature extraction. Springer Berlin Heidelberg, 2006. 1-25.
- [14] I.A. Kakadiaris, G. Passalis, G. Toderici, E. Efraty, P. Perakis, D. Chu, S. Shah, and T. Theoharis, "Handbook of Face Recognition", Second Edition, Springer, 2011
- [15] Tan, Xiaoyang, et al. "Face recognition from a single image per person: A survey", Pattern recognition 39.9 (2006): 1725-1745.
- [16] Ao, Meng, et al. "Face recognition at a distance: system issues", Handbook of Remote Biometrics. Springer London, 2009. 155-167.

Detection Citrus Aurantium Musty Using First Order Statistics Feature

Assistant Prof. Amel H. Abbas Marwa A. Shamel

Computer Science, College of Science, Mustansiriyah University

dr.amelhussein2017@uomustansiriyah.edu.iq mi9437911@gmail.com

Abstract:

Texture is an important characteristic for analysis of many type of image because it gives us information about the spatial arrangement of the color or intensities in an image or selected region of an image. In this paper used to distinguish between different types of fruit to distinguish fruit (Citrus Aurantium) to recognize between fresh fruits (fruit is not infected with mold) and musty fruit first order statistics from gray level histogram it used to calculate for each (mean, variance, Skewness, kurtosis, entropy and energy), computed of the measurement of texture for both the fresh and musty for the fruit. Used a three sample of Citrus aurantium. The samples used after extract the region of interest, size (301*301) from each fruit (Fresh, Musty and Mixed between fresh and musty) from the results, in this paper observed value for each the mean, variance and skewness features is the better than the energy and entropy features because differences varying small.

Keywords: texture feature, first order statistics from gray level histogram, Citrus Aurantium M

الكشف عن النارج المتعفن باستخدام الميزات الإحصائية ذي الرتبة الاولى

أ. م. د. أمل حسين عباس مروة أبراهيم شامل

المستخلص

الملس هو السمة الهامة لتحليل العديد من نوع صورة لأنه يعطينا معلومات عن الترتيب المكاني من لون أو شدة في صورة أو المنطقة المحددة من الصورة هذه البحث تستخدم للتمييز بين أنواع مختلفة من الفاكهة للتمييز بين الفواكه (النارج) للتمييز بين الفواكه الطازجة (الفواكه غير مصابة بالعفن) والفواكه المتعفنة. باستخدام الميزات الإحصائية ذي الرتبة الاولى تستخدم لحساب كل من (المتوسط التباين، الانحراف، الكون، الطاقة) هذه الابعاد حسبت لكل من الطازجة والمتعفنة والخليط. استخدمنا ثلاثة عينات من الفواكه (النارج) استخرجنا من كل عينة ثلاثة مناطق كل منها من حجم (301*301) من كل الطازجة والمتعفنة والخليط فيما بينهما.

من النتائج لاحظنا ان كل من قيم المتوسط والتباين والانحراف هي افضل من الكون والطاقة لان لاختلافات متفاوتة بنسبه صغيرة في كل منهما الطاقة والكون.

1. Introduction

Fruits and vegetables provide health benefits and are important for the prevention of illnesses. The U.S. Department of Agriculture recommends filling half of your plate with fruits and vegetables at each meal. Fruits contain a variety of nutrients including vitamins, minerals and antioxidants. Eating the recommended amount of fruits in day can reduce the risk of chronic diseases. Is consider Prevention of Disease, Eating produce can cut your risk of cardiovascular disease, stroke and type 2 diabetes and protect against various forms of cancer. The USDA states that fruits high in fiber can reduce chances of developing coronary heart disease. Eating potassium-rich foods such as bananas and potatoes can help reduce blood pressure, decrease bone loss and prevent development of kidney stones [1]. Prevention is a more effective strategy than is treatment of chronic diseases. Functional foods that contain significant amounts of bioactive components may provide desirable health benefits beyond basic nutrition and play important roles in the prevention of chronic diseases. Consider the bitter orange an excellent source of health-promoting compounds due to the balanced mixture of minerals and antioxidants including vitamins C [2]. Image analysis technique based on the texture plays an important role in the fruit that contains the discovery of a musty or any other

type of disease. the purposes of texture description is to derive some measurements that can be used to classify a particular texture, consider using texture to analyze forests in remotely sensed images. texture is not limited to being relevant in the images analysis being solves problems wide range of applied recognition, segmentation, and synthesis problems, but also it provides a key to understand basic mechanisms that underlie human visual perception[3].texture analysis has a rich history in image processing and computer vision.image well usually contain sample of more than samples of more than one texture [4].texture for a feature to be us, it should produce the same value for images of the same Mode image capture, while giving us the results of different values of the image in a position to capture other different. Texture features provide a critical source of information for various recognition tasks. Among the many type of feature that can be extracted from texture image, one is the faced with the problem of selecting those features that carry the most information about the image [5]. These features contain important information about the structural arrangement of surfaces and their relationship to the surrounding environment. Simplest texture features can achieve by calculated statistical features, like (mean, variance, Skewness, kurtosis, entropy and energy), from gray level histogram [3].there are two method that can be used to calculate the texture feature of image. One is statistical texture; the other is structure analysis [6]. Statistical methods characterize texture by the statistical distribution of the image intensity. Spatial distribution of gray values is one of the defining qualities of texture. Statistical methods analyze the spatial distribution of gray values, by computing local features at each point in the image, and deriving a set of statistics from the distributions of the local features [7]. A class of simple image properties. That can be used for texture analysis are the first-order statistics of local property values, i.e., the means, variances etc. In particular, a class of local properties based on absolute differences between pairs of gray levels or average gray levels has performed well; for example in the comparative studies of Weszka *et al.*[8]. The texture of an image region is determined by the way the gray levels are distributed over the pixels in the region [9]. Is the type first order statistics of image intensities characterizing the statistical properties of an image? The first order statistic represents a 1-D probability distribution, the features is calculated from first order can be used to characterize and recognize an image or sub image [5].

2. Materials And Methods

The purpose of this work is the distinctions between fruit have quality and fruits poor quality by extracting features texture. The used three samples RGB and each sample we took from them three ROI(region of interest) of information each sample(JPG, 301x301,Size8,unite Class).in this paper is done using MATLAB software version R2015a.

2.1. Image Capture

In this paper is used three sample of fruit We use the same one of the fruit were segmentation three regain (fresh, mixture and musty). Has been capture by camera type (Mobile galaxy) Resolution (13 Mika pixels).

2.2. Preprocess

This paper is aim the preprocessing to classification image based the extracted texture feature from digital image RGB, to differentiate between Citrus Aurantium Musty and fresh. method is Start by input digital image RGB and selection three region of interest (ROI) of equal size from different tissue in the in the original input image, after selection three region convert to gray scale image, the sub image in gray is calculated statistics features used method fist order statistics from gray level histogram.

3. Statistical Feature Of Texture

3.1. First Order Statistical Features

Texture analysis based on statistical properties of the intensity histogram is a frequently used approach [3]. This kind of texture are analyzed studying the statistical properties of the intensity values of pixels [3]. Histogram based approach to texture analysis is based on the intensity value concentrations on all or part of an image represented as a histogram[10]. after preprocessing, the

sub image was calculated its statistical features by 6 descriptors which are (mean, variance, Skewness, kurtosis, entropy and energy).

The first-order histogram $P(I)$ is defined as:

$$p(I) = \frac{\text{number of pixels with gray level } I}{\text{total number of pixels in region}} \dots \dots \dots (1)$$

Based on the definition of $P(I)$,

Where g is the number of possible gray levels. $\sum$ is sigma(used for the summation operator.

the most frequently used mean(μ) are Variance (σ), Skewness ($m3$), Kurtosis($m4$), Entropy(h) and Energy (E), given by (3), (4), (5), (6) and (7) respectively. The Variance is a measure of the histogram width that measures the deviation of gray levels from the Mean. Skewness is a measure of the degree of histogram asymmetry around the Mean and Kurtosis is a measure of the histogram sharpness.[12].

- Mean: given the probability distribution of intensities in an image [5].

Expression for mean:

$$\mu = \frac{\sum_{i=0}^{g-1} i p(i)}{\sum_{i=0}^{g-1} p(i)} = \frac{\sum_{i=0}^{g-1} i p(i)}{n} = \sum_{i=0}^{g-1} i p(i). \dots (2) [5][7][9][11].$$

- Variance: a more credible feature

Expression for variance:

$$\sigma = \sum_{i=0}^{g-1} (i - \mu)^2 p(i). \dots (3) [5][7][9][11].$$

- Skewness: are the Texel intensities usually darker/lighter than average

$$m3 = \sum_{i=0}^{g-1} (i - \mu)^3 p(i). \dots (4) [5][7][9][11].$$

- Kurtosis: which shows the degree of similarity of a distribution to a normal.

Expression for kurtosis

$$m4 = \sum_{i=0}^{g-1} (i - \mu)^4 p(i) \dots (5) [5][7][9][11].$$

- Entropy: Histogram uniformity measure,

Expression for entropy:

$$h = \sum_{i=0}^{g-1} p(i) \log_2 p(i) \dots (6) [5][7][9][11].$$

- Energy: how much intensity variation is there in the region.

Expression for energy

$$E = \sum_{i=0}^{g-1} [p(i)]^2 \dots (7) [5][7][9][11].$$

4. Result And Discussion

The purpose in this paper to distinguish between Citrus Aurantium with high quality and poor quality, the recognition system was used to recognition fresh fruits(Citrus Aurantium) and fruits with mold(Citrus Aurantium).to perform the work of this system the first step is the process of obtaining images followed by analysis images and finally get the required outputs view figure (1) shows the performance of the system, The process of input the image and selecting three ROI(region of interest) for each sample of the Citrus Aurantium and the size 301 * 301 for each (fresh, mix between fresh and musty,musty). The converted in to the gray scale then Calculated the first order statistical of each ROI for each of the three samples of the then (mean, variance, Skewness, kurtosis, entropy and energy)features from the result in table(1) observed the Skewness that appear negative value in case the musty Citrus Aurantium help to the recognition.

5. Conclusion

First Order Statistical Features can be extracted many texture features. In this work, an evaluation of calculated for each (mean, variance, Skewness, kurtosis, entropy and energy) for gray level images, that computed of the measurement of texture for each the fresh, mixture and musty. The six measurements commonly used to recognition between fresh and musty. The results indicate that the best feature can be used to recognize among them is theses skewness, followed by each of the mean and variance.

6. Future Works

This method statistical features is not Effective. There is used to The use of statistical methods is not very high efficiency, the propose in the future work to use method structure analysis (gray-level co-occurrence matrix (GLCM) for detect the fresh fruit and the musty to give high performance efficiency.

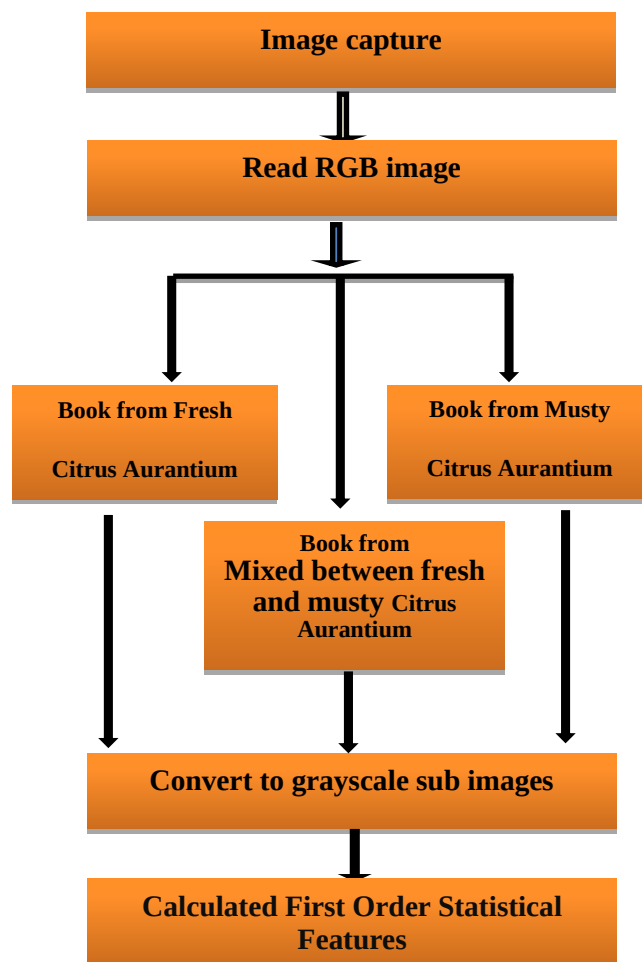


Fig. (1): Block diagram of implemented system

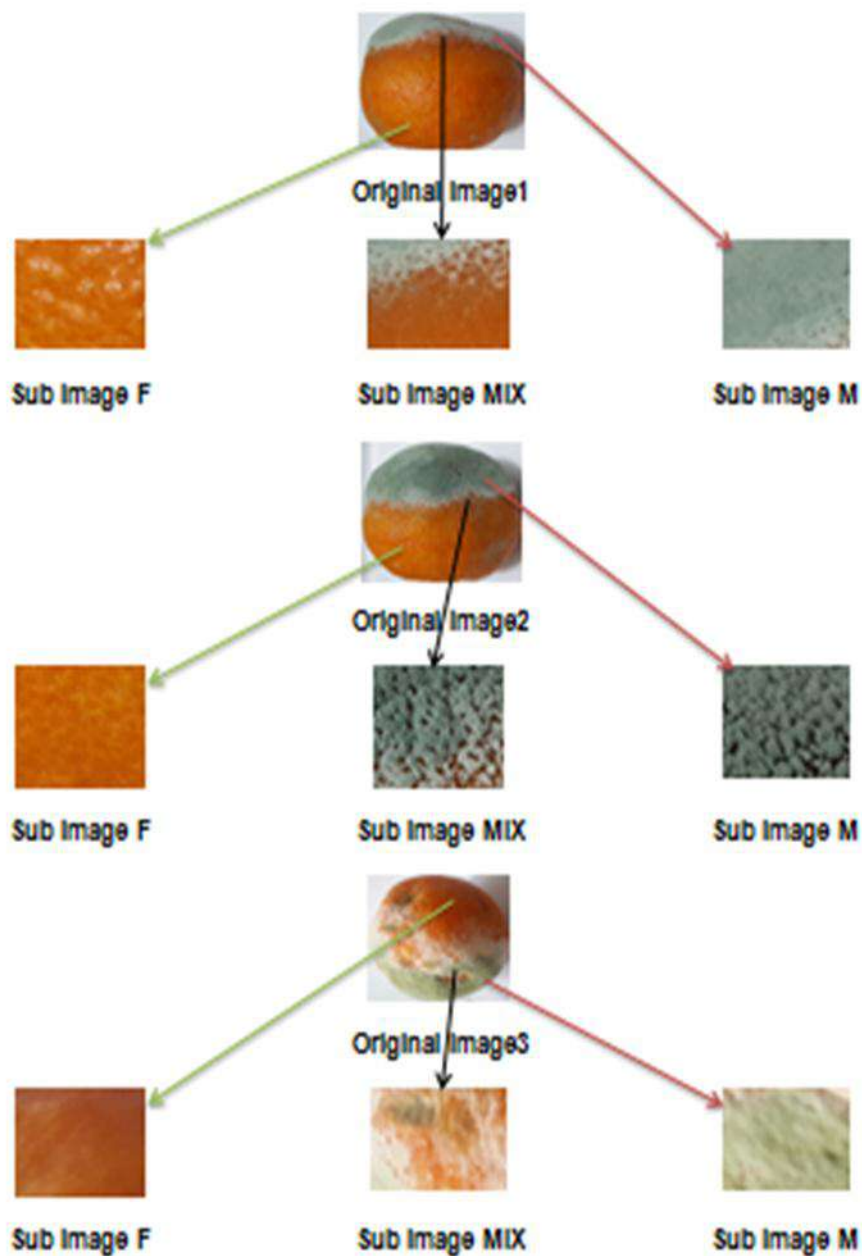
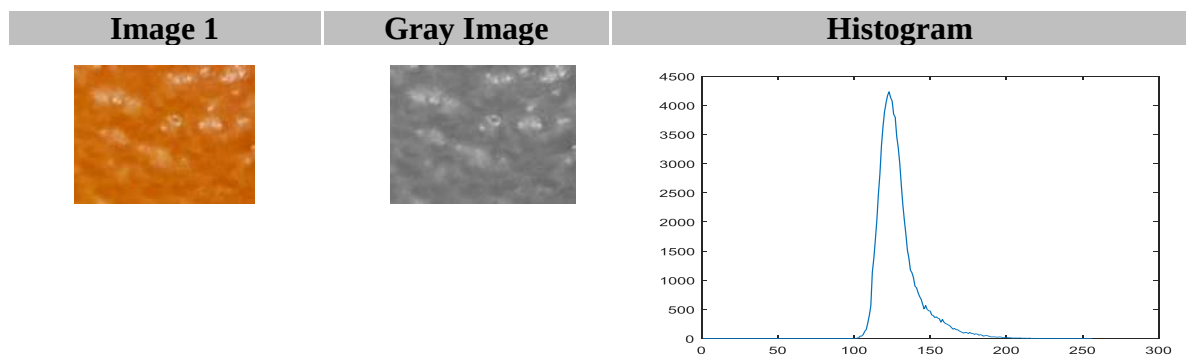


Fig.(2):Three selected regain of(Fresh, Mixture And Musty) from three sample



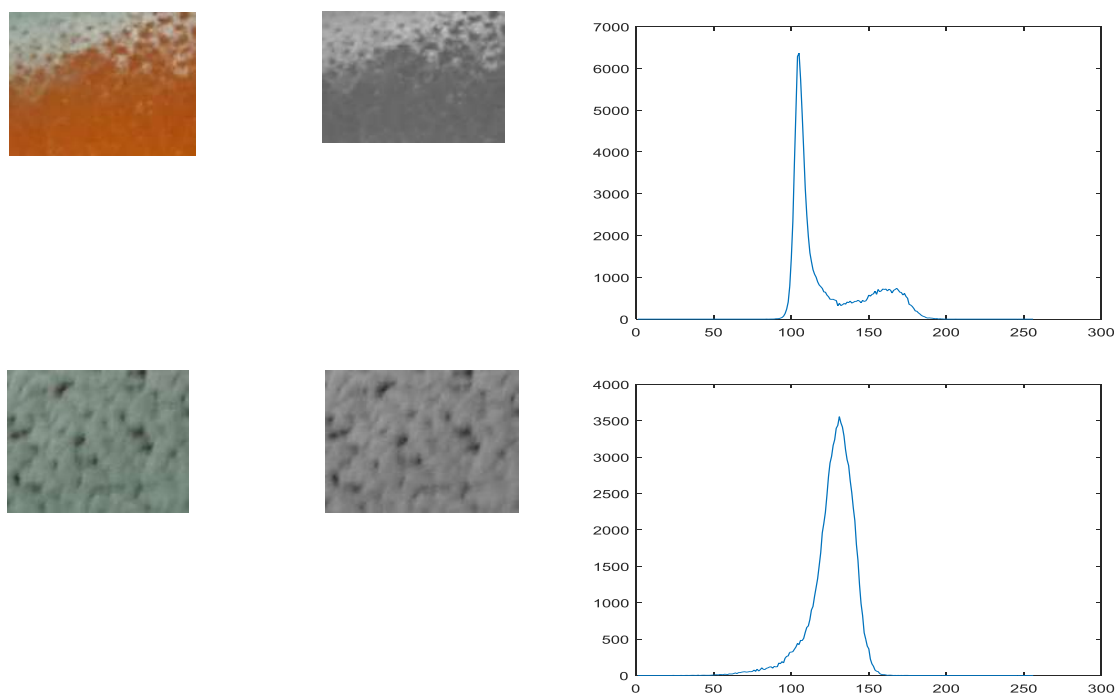
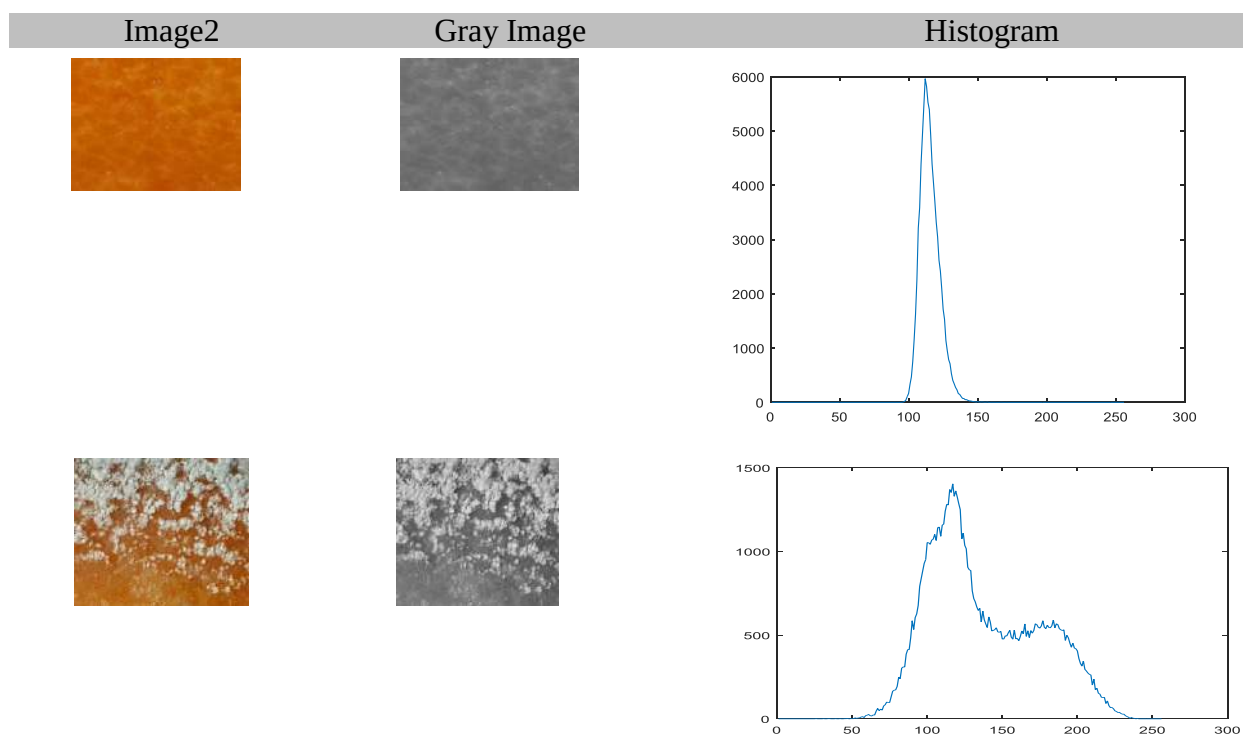


Fig. (3): Results Implementation For Each Sub Image



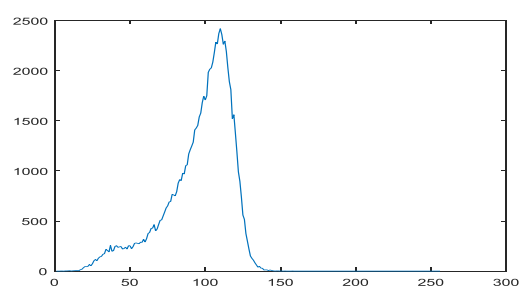
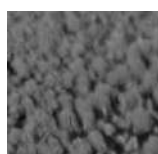


Image3

Gray Scale

Histogram

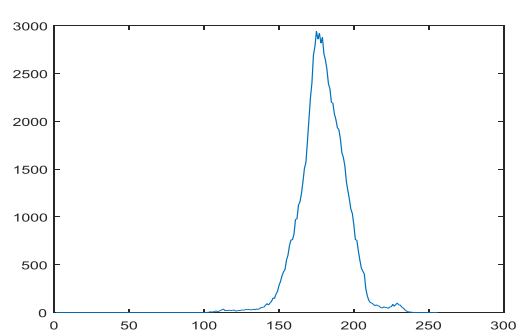
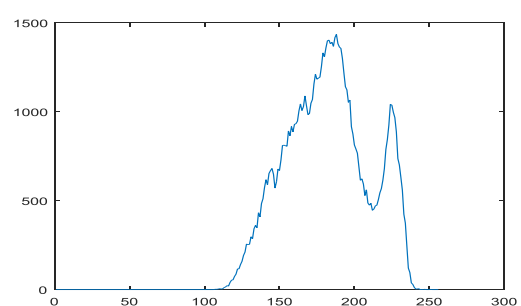
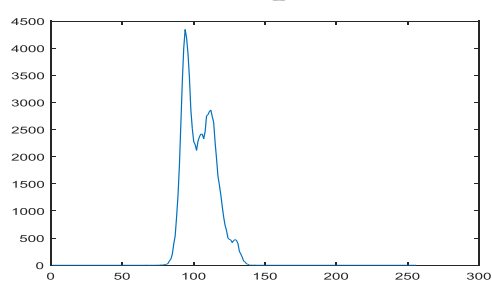
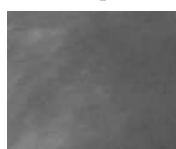


Fig.(4): Implementation for each sub image

Table (1) Show the result for calculated first order statistics

	Image1			Image2			Image3		
	Sub Image F	Sub image MIX	Sub Image M	Sub Image H	Sub Image MIX	Sub Image M	Sub Image F	Sub Image MIX	Sub Image M
Mean	2.8949	3.5228	6.4764	3.4830	5.1598	5.7807	4.9527	5.1736	5.5328
Variance	0.8444	2.7988	0.6183	0.5675	1.9250	1.4546	1.3202	2.3828	0.8309
Skeness	1.4917	0.9050	-1.2841	0.6558	0.4409	-0.9988	0.0639	0.0639	-0.1760
Kurtosis	6.6141	2.4405	6.9061	3.9730	2.3026	3.6663	2.3645	2.3645	4.1818
Energy	0.3681	0.2495	0.5324	0.3939	0.2171	0.2698	0.1775	0.1775	0.3262
Entropy	1.1904	1.5790	0.9061	1.1056	1.6621	1.4841	1.4881	1.8184	1.3106

References

- [1] [Centers for Disease Control and Prevention: Fruit and Vegetable Benefits.](#)
- [2] [Fruit and Vegetable Benefits.](#)
- [3] F. H. Mahmood¹, W. A. Abbas, "Texture Features Analysis using Gray Level Co-occurrence Matrix for Abnormality Detection in Chest CT Images, *Iraqi Journal of Science*, 2016, Vol. 57, No.1A, pp: 279-288", 2016.
- [4] M.S.Nixon and A.S.Aguado, "Feature Extraction & Image Processing For Computer Vision", 3d, UK 84 Theobald's Road, London WC1X 8RR, UK, 2012,.
- [5] A.A.Goshtasby, "Image Registration", Springer London Dordrecht Heidelberg New York, ISSN 2191-6586, ISBN 978-1-4471-2457-3, 2012.
- [6] B. Pratap , N. Agarwal, S.Joshi p&S. Gupta, " Global Journal of Computer Science and Technology: C Software & Data Engineering", vol 14 Issue 5 V.1.0, 2014.
- [7] S.S.elvarajah¹ and S.R. Kodituwakku, "Analysis and Comparison of Texture Features for Content Based Image Retrieval", *International Journal of Latest Trends in Computing (E-ISSN: 2045-5364)* 108 Volume 2, Issue 1, March, 2012.
- [8] Weszka, J., C. Dyer, and A. Rosenfeld, "A Comparative Study of Texture Measures for Terrain Classification", *IEEE Trans. Systems, Man, and Cybernetics* pp.269-285, 6, 1976.
- [9] N. Aggarwal, R. K. Agrawal, "First and Second Order Statistics Features for Classification of Magnetic Resonance Brain Images", *Journal of Signal and Information Processing*,, 3, 146-153, 2012.
- [10] S. Hailemichael, "Imaging Techniques to Identify and Classify Normal and Defective Tomatoes", 2014.
- [11] P.Ngian, "Vegetables Recognition Based On Texture Feature", online open access (full text), 2011.
- [12] Namita Aggarwal, R. K. Agrawal, "First and Second Order Statistics Features for Classification of Magnetic Resonance Brain Images", *Journal of Signal and Information Processing*, pp, 146-153, 2012.

Edge Detection of Ear Image Based on Canny Method

Prof. Dr. Jamila Harbi S.¹

Sara Salman²

Mustansiriyah University, College of Science, Dept. Computer Science

¹dr.jameelahharbi@gmail.com

²sarah.salman.q93@gmail.com

Abstract:

Biometrics refers to the recognition of individuals based on their physiological or behavioural characteristics. The human ear is a new feature in biometric which has various advantages over other features that makes it a good candidate for passive person identification. In this paper, an ear edge detection algorithm is proposed which uses canny method to detect the region of interest. The proposed algorithm pre-processes the ear image before the segmentation phase. The pre-processing step involves enhancing the image's brightness by converting it to Hue saturation value (HSV) system. Skin segmentation by Hue saturation value(HSV) and separation things of the unwanted and get the ear. Canny edge detector performs better than all other edge detectors on various aspects such as it is adaptive in nature, performs better for noisy image, gives sharp edges, low probability of detecting false edges.

Keyword: Biometrics, Ear recognition, Preprocessing, Skin Segmentation, Edge Detection.

اكتشاف حافات صورة الاذن بالاعتماد على طريقة كاني

ساره سلمان

أ. د. جميلة حربي

المستخلص

القياسات الحيوية تشير إلى تمييز الأفراد على أساس الخصائص الفسيولوجية أو السلوكية. الأذن البشرية هي ميزة جديدة في القياسات الحيوية التي لديها مزايا مختلفة تميزها عن بقية القياسات الحيوية مما يجعلها مرشح جيد لتحديد هوية الشخص. في هذا البحث تم اقتراح خوارزمية الكشف عن حافة الأذن الذي يستخدم طريقة كاني للكشف عن منطقة الاذن. الخوارزمية المقترحة تتطلب منا معالجة صورة الأذن قبل مرحلة التجزئة. تتضمن خطوة المعالجة المسبقة تحسين سطوع الصورة وتحويلها إلى نظام قيمة تشبع اللون. تجزئة الجلد عن طريق قيمة تشبع اللون وفصل الأشياء غير المرغوب فيها والحصول على الأذن. كاني حافة كشف ينفذ أفضل من جميع أجهزة الكشف عن حافة أخرى على جوانب مختلفة مثل أنها قابلة للتكيف في الطبيعة، ينفذ بشكل أفضل لصورة ضوضاء، ويعطي حواف حادة، واحتمال منخفض للكشف عن حواف كاذبة.

الكلمات المفتاحية: القياسات الحيوية، التعرف على الأذن، المعالجة المسبقة، تجزئة الجلد، كشف الحافة.

1-Introduction

Ear recognition is a good and reliable biometrics for human verification and identification [1]. The structure of the ear is fairly stable and robust to changes in facial expressions or aging [2]. The human ear is considered one of the best features for passive identification, and may become an invaluable tool used in security for highly sensitive areas. The ear has desirable properties such as shape, universality, uniqueness and permanence [3]. It is now widely accepted that the shape and appearance of the ear is unique to each individual and comparatively fixed during the lifetime. No one can prove the uniqueness of the ear; numerous studies provide empirical supporting evidence. According to reports, the variation over time in a human ear is most noticeable during the period from four months to eight years old and over 70 years old. The ear growth between four months to eight years old is approximately linear, and after that it is constant until around 70 when it increases again. Whilst there are some small changes that take place in the ear structure, these are restricted to the ear lobe and are not linear. Such stability and predictable changes make ear biometrics an exciting realm for future research. Commonly, the acquisition of ear images and facial images are very similar, meaning that the former can potentially be used in the same situations [4].

2-Related Work

A complete human recognition system using 3D ear biometrics has been presented in [5]. The system consists of 3D ear detection, 3D ear identification, and 3D ear verification. Multiple geometrical feature extraction (such as shape, Euclidian distances of side of a triangle and angles of a triangle as a feature vector) of ear based method to identify a person using ear biometrics has been proposed. A study presented in [6] proposed a multimodal biometric system for fingerprint and ear biometrics. SIFT descriptor based feature sets extracted from fingerprint and ear are fused. Two approaches to detect ear from 2D side face images has been presented in [7]. The first approach was edge detection based method and the second was template matching method. The experimental results showed the effectiveness of these methods, but both methods fail, if side face is oriented with some angle. A robust method for 2D ear recognition using color SIFT features has been proposed in [8]. Firstly, SIFT algorithm originally performed on the intensity channel to the RGB color channels to maximize the robustness of the SIFT feature descriptor. Secondly, a feature matching algorithm for ear recognition is proposed by fusion of the features extracted from the different color channels. A completely automated approach for the robust segmentation of curved region of interest using morphological operators and Fourier descriptors using 2D ear imaging was presented in [9]. Paper conducted a survey of some of the unimodal biometrics that are either currently in use across a range of environments or those still in limited use or under development, or still in the research realm. In this paper propose an ear edge detection algorithm is proposed which uses canny method to detect the interest region.

3-The Proposed Method

The proposed method consists of five main stages namely: preprocessing image, color model conversion, skin segmentation, find skin and edge detection as shown in Figure (1). A detailed explanation of each stage is given in the next subsections.

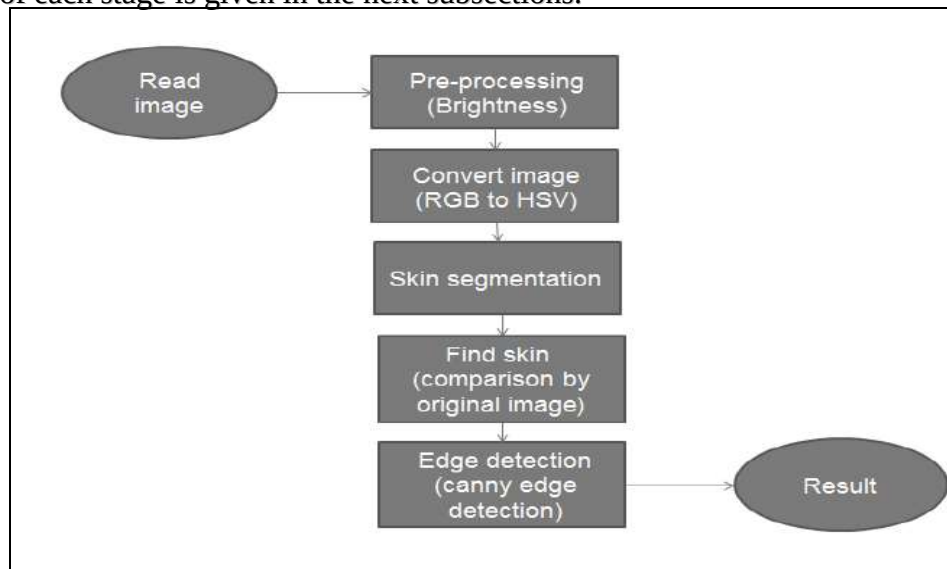


Fig.(1): The main steps of the proposed technique

3.1 Preprocessing Image Stage

Preprocessing image has for the purpose of improving the image and give the best results because some of the images may hide the details of the real noise and duplicates of pixels is necessary. In the proposed technique the preprocessing is used of the way to improve image brightness for the purpose of showing the image detail well, because sometimes it is the process of capturing the image is taken it is appropriate or inappropriate to the circumstances that the brightness of images is increase in relative terms between 0 and 255. Brightness modification of an image defined as:

$$\left. \begin{aligned} R_1 &= R_1 + \text{Brightness} \\ G_1 &= G_1 + \text{Brightness} \\ B_1 &= B_1 + \text{Brightness} \end{aligned} \right\} \dots \dots \dots (1)$$

3.2 Color Model Conversion Stage

HSV stands for the three components are: Hue, Saturation and Value components. The value represents intensity of a color, which is decoupled from the color information in the represented image [10]. The hue and saturation components are intimately related to the way human eye perceives. The transformation equations (2,3,4) for RGB to HSV color model conversion are shown:

$$V = \max (R, G, B) \dots \dots \dots (2)$$

$$S = \frac{\max - \min (R, G, B)}{\max}, \text{ if } \max > 0 \dots \dots \dots (3)$$

$$H = \begin{cases} \frac{(G_1 - B_1)}{\max - \min}, & \text{if } \max = R \\ 2 + \frac{(B_1 - R_1)}{\max - \min}, & \text{if } \max = G \\ 4 + \frac{(R_1 - G_1)}{\max - \min}, & \text{if } \max = B \end{cases} \dots \dots \dots (4)$$

3.3 Skin Segmentation Stage

The third step of the proposed technique is skin segmentation which aims to detect skin regions in an image to reduce the search space for the ear. In this paper propose skin segmentation by HSV and for the purpose to get on the ear because there are details in the picture that does not need it. Remove maximum number of non-face pixel from the image in order to narrow focus to remove predominantly skin-color region. Skin Segmentation to eliminate all non-skin pixels from the image. After image color conversion applied, HSV is used to detect skin segmentation. The skin color has value 1 if the skin region and the other have value 0.

3.4 Find Skin Stage

For reducing the noisy pixels that may appear after Skin segmentation, median filter is applied. The median is just the middle value after ascending all the values of the pixels in the neighborhood; the median has half the value in the neighborhood. After applying median filter the resulted image became bluer image.

The smooth image is completed and separated skin separated from other skin only. The comparison of original image with each color skin image, if we have skin pixel then give it one value otherwise is zero.

3.5 Edge Detection Stage

The edges are detected from the input image using the Canny method. First of all the color image is converted to gray scale image so that we can apply edge detection algorithm. The Canny method finds edges by looking for local maxima of the gradient of intensity image. The gradient is calculated using the derivative of a Gaussian filter. The method uses two thresholds, to detect strong and weak edges and includes the weak edges in the output only if they are connected to strong edges. This method is therefore less likely than the others to be fooled by noise, and more likely to detect true weak edges. The edges of ear have definitely been detected in extracted region which has higher probability to contain ear. The flowchart in figure (2) is summarized canny edge detection algorithm.

4-Experimental Results

The experimental results are obtained from our proposed Ear Detection Technique:

1-Preprocessing Image stage: The enhancement processing applied on the color image as shown in Figure (3).

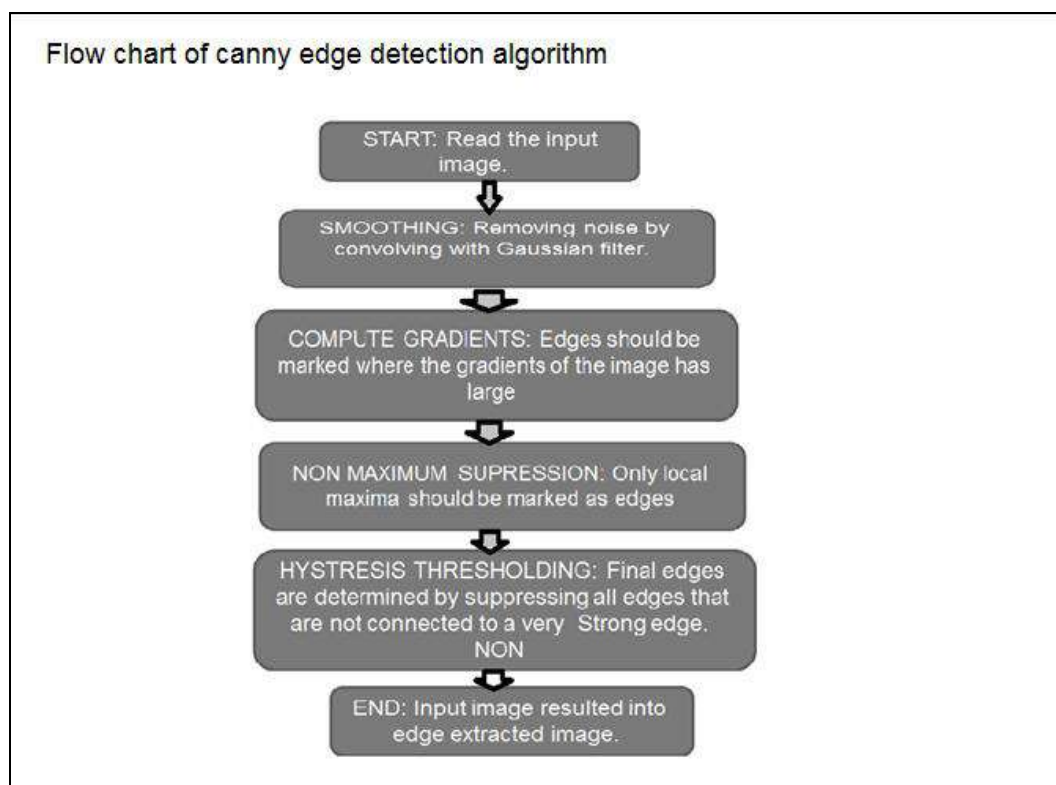


Fig. (2): Canny edge detection algorithm as:

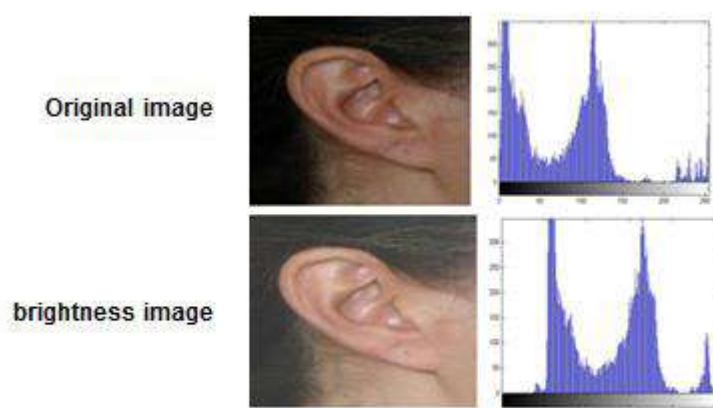


Fig. (3): The output of pre-processing stage

2- Color Model Conversion stage: The results of conversion color image model to HSV model as shown in Figure (4).

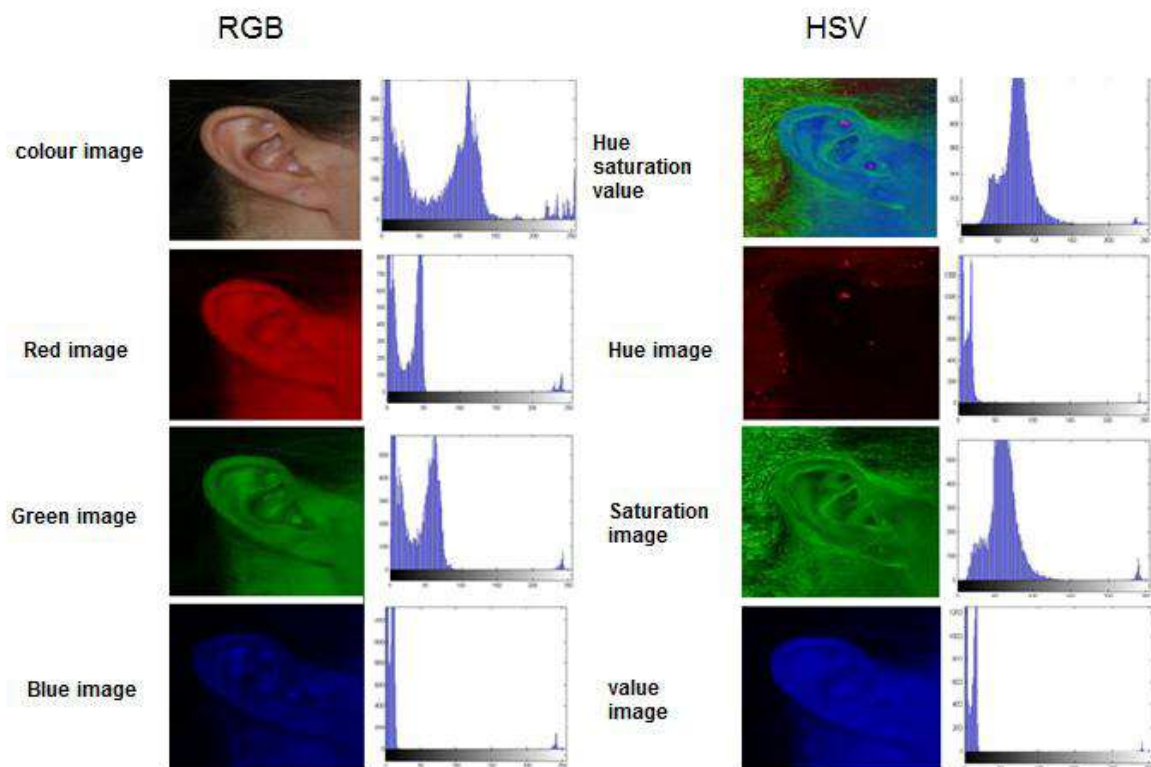


Fig. (4): Conversion RGB image to HSV image

3- Skin Segmentation stage: The skin segmentation of HSV ear image as shown in Figure(5).

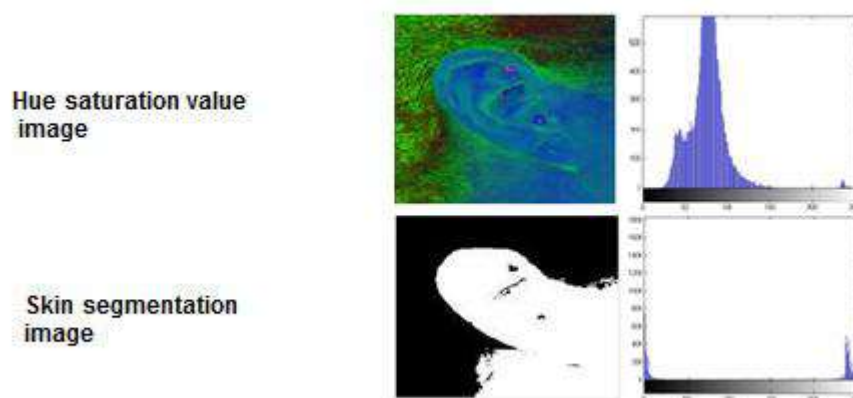


Fig. (5): The output of skin segmentation stage

4- Find Skin stage: skin segmentation image comparison of original image with each color skin image see figure (6)

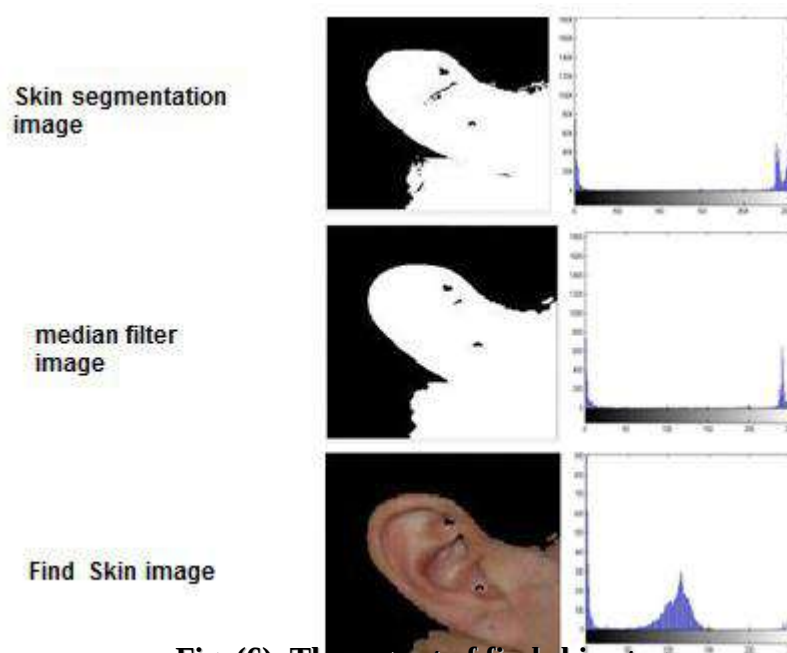


Fig. (6): The output of find skin stage

5- Edge Detection stage: The edge detection is significantly reducing the amount of data in an image and preserves the structural properties for further image processing as shown in Figure(7)

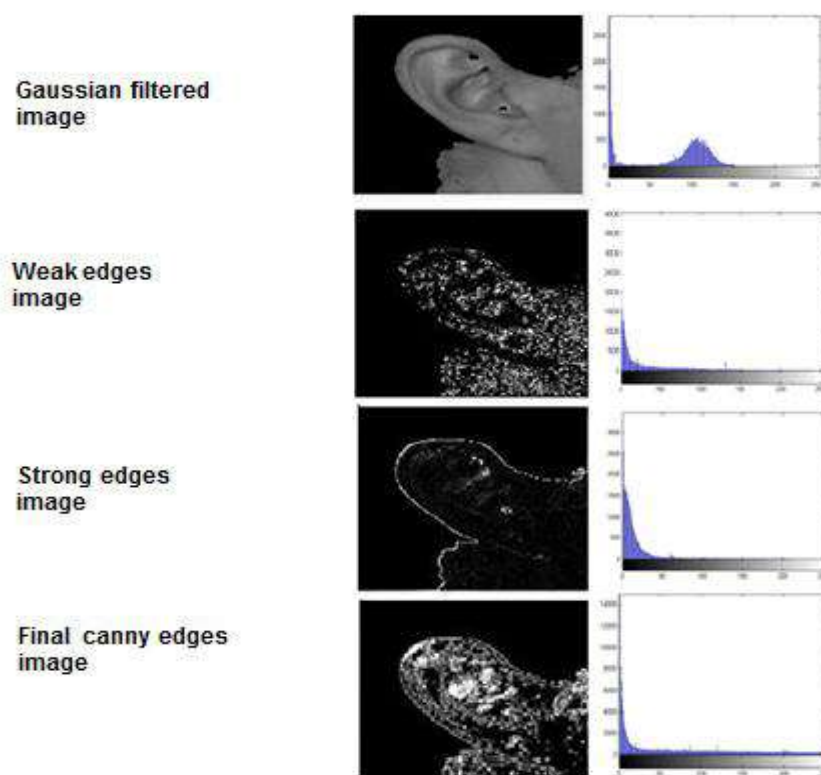


Fig. (7): The output of edge detection stage

5-Conclusions

In this paper introduced edge detection of the ear using Canny edge detection method. To perform the process of the image segmentation, we need to preprocessing image get on enhanced image by brightness, and give better results to find the details of the image. The conversion color image model to HSV, because HSV model is a unique method of color classification, similar to human mode and its results are more powerful for different lighting. Skin segmentation by HSV and separation things of the unwanted such as hair and earing other than that and get the ear which isolated the skin from non-skin. Canny method is an excellent way to calculate all the weak and powerful edges, so we have seen that canny edge detector gives better result as compared to others with some positive points. It is less sensitive to noise, adaptive in nature, resolved the problem of streaking, provides good localization and detects sharper edges as compared to others., in the future help us in our work which will help us in finding the region of interest by adopting the edges of the image.

References

- [1] B. Bhanu and H. Chen., " **Human Ear Recognition by computer**", Springer, 2008.
- [2] A. Iannerelli, " **Ear Identification**", Forensic Identification Series, Paramount PublishingCompany, Fremont, Calif, 1989,USA.
- [3] Chen, H., B. Bhanu," **Human Ear Detection From 3D Side Face Range Images**", Computational Imaging and Vision. 2007.
- [4] Kumar, V.K., B. Srinivasan, " **Ear Biometrics in Human Identification System**". I.J. Information Technology and Computer Science, 2012.
- [5] Chen, H. & Bhanu, B, " **Human Ear Recognition in 3D**". IEEE Transactions on Pattern Analysis and Machine Intelligence, 2007.
- [6] Kisku, D.R., Gupta, P. & Sing, J.K." **Level Fusion of Biometrics Cues: Human Identification with Doddington's Caricature**", Communications in Computer and Information Science. Springer: Warsaw,2009.
- [7] Chauhan, N. C, " **Edge Detection and Template Matching Approaches for Human Ear Detection**". International Conference on Intelligent Systems and Data Processing (ICISD). Special Issue published by International Journal of Computer Applications, 2011.
- [8] Zhou, J., Cadavid, S. & Abdel-Mottaleb, M," **Exploiting color SIFT features for 2D ear recognition**". 18th IEEE International Conference on Image Processing ,2011.
- [9] Kumar, A. & Wu, C., " **Automated human identification using ear imaging**". Pattern Recognition, 2012.
- [10] Patil, Neelamma K., Ravi M. Yadahalli, and Jagadeesh Pujari. " **Comparison between HSV and YCbCr color model color-texture based classification of the food grains**." International Journal of Computer Applications, 2011.

Vertex Neighborhood Detection Based on Connectivity Information

Sawsen Abdulhadi Mahmood Amal Abbas Kadhim

Lamyaa Mohammed Kadhim Sally Ali Abdu Lateef

Computer Science Dep., Collage of Education, Mustansiriyah University

sawsenhadi@gmail.com

Abstract:

In 3D image analysis, a 3D surface vertex by itself does not offer rich geometry information; it only represents a location in the 3D space. To be more informative, a detection of vertex position relative to other points that fall within its local neighborhood must be achieved. In this paper, a vertex neighborhood detection algorithm of 3D mesh image is presented based on connectivity information only. To validate the performance of the propose algorithm, we used 3D mesh image samples taken from GAVADB database. The experimental results provide an accurate determining for vertex neighbors number compared to the classic approach (Euclidean Distance).

Keyword: 3D mesh, neighborhood, local shape descriptor.

تحديد جوار الرأس اعتمادا على معلومات الاتصال

سوسن عبد الهادي محمود، أمل عباس كاظم، لمياء محمد كاظم، سالي علي عبد اللطيف

المستخلص

في انظمة تحليل الصور ثلاثية الابعاد، النقطة أو الرأس ثلاثي الابعاد على السطح لوحده لا يوفر المعلومات الهندسية، هو يمثل موقعه في الفضاء الثلاثي. لكي يكون مصدر وافي للمعلومات، يجب ان يتم تحديد موقع الرأس نسبة الى مجموعة النقاط التي تقع في جواره. في هذا البحث يتم عرض خوارزمية لتحديد نقاط الجوار للرأس الثلاثي في الصورة 3D الشبكة (mesh) اعتمادا على معلومات الاتصال فقط. ولغرض التحقق من أداء الطريقة المقترحة، قمنا باستخدام عينات من صور ثلاثية الابعاد مأخوذة من قاعدة البيانات (GAVADB). وقد اظهرت النتائج التجارب دقة في تحديد عدد جوار الرأس مقارنة بالطريقة التقليدية Euclidean distance.

الكلمات المفتاحية: الشبكة 3D، الجوار، واصف الشكل المحلي.

1. Introduction

The preprocessing phase is usually aims to improve the quality of 3D images. Since preprocessing operation has a great influence on the extracted feature quality, it leads to degrade or support the effectiveness of system performance [1]. The neighborhood determining of each vertex in 3D images is considered as essential step of preprocessing operations in 3d images analysis and recognition systems. The neighbor points in [2] are determined according to the interpolation scheme to form each vertex valid neighbors. Boundary points are initially determined by a sweep through the range image, row by row, to find the first and last valid 3-D point. This process is repeated until no additional points are created. The neighbor points in [3] were defined by the 8-nearest neighbors (i.e., within the 3×3 window) of the current point. The process of neighborhood detection process is applied on a set of vertices, which is included within a local neighborhood, see Figure (1). In order to locate this local neighborhood, the classic approaches followed a simple procedure requires a distance metric and a threshold. This procedure involves the following concept; all the points whose distance to a specific point is less than a predefined threshold are included in the local neighborhood for this point. The common approaches that are utilized to detect the neighborhood of 3D point are based on two main methods:

Euclidean distance: which represents the traditional distance D_{Ec} between two given points in R^3 . Let $p_1 = (x_1, y_1, z_1)$, $p_2 = (x_2, y_2, z_2)$ two 3D points, then D_{Ec} between p_1 and p_2 is given by the following Equation:

$$D_{Ec} = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2 + (z_2 - z_1)^2} \dots \dots \dots (1)$$

Geodesic distance: calculates the distance between any two given points in R^3 according to shortest path between these two points [4]. In the presented work in [5] the vertex neighbors were fixed with size to 25 mm in geodesic distance (based on observations of the curvatures decomposition) which is more appropriate in such computations because it takes into account the image surface shape. Recall that geodesic distance between point A and B is defined as sum of Euclidean distances between points in the shortest path between points A and B on the underlying surface. The neighbors of vertex were determined in [6] based on using nearest neighbor interpolation scheme. Therefore, in order to reduce the computation time, an innovative approach to detect the neighborhood for each vertex in the surface mesh will be stated and described in this paper.

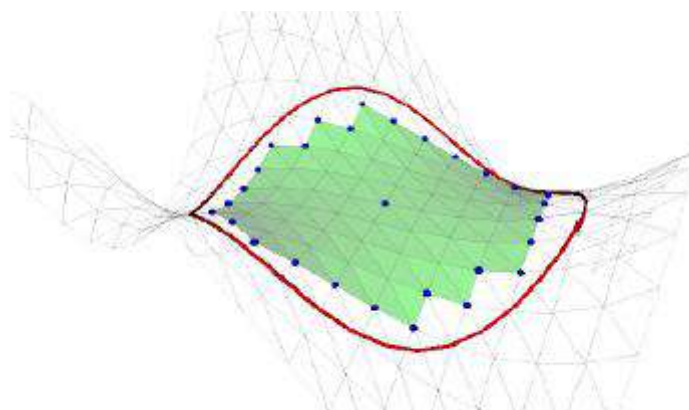


Fig. (1): Neighborhood of 3D point represented by computing Euclidian desistance

In this paper, detailed description and implementation technique of the preprocessing operations required for preparing and neighbor determining of 3D image are introduced.

2. Reading Data Files

The initial step of the preprocessing step includes reading data files of 3D database available which have the format (.wrl, mesh). Then, the readable data points (vertices and faces) are arranged in a suitable data structure within a general data structure of the proposed system. Each vertex v_i in the constructed data structure relates with n_f faces that surround v_i . Meanwhile, a 3D viewer application for mesh file format visualization is designed and implemented using C++ programming language and OpenGL graphic library, in order to facilitate following up and gaining solution to unsolved problems associated with the proposed approach. Also provides a suitable environment to visualize and analyze 3D extracted interesting regions from the acquired meshes. Figure (2) displays examples of facial scans visualized using the 3D viewer program. The designed 3D viewer application is characterized by the following properties:

- Reading data files with a mesh data format and an unstructured point cloud data format.
- Its applicability to Apply zooming in and zooming out 3D transformations over the viewed data points. A predefined scale factor is utilized at each scaling operation.
- The designed application also has the ability to apply 3D rotation transformation (around yaw axis) over the viewed data points. This transformation is applied with assistance of the keys ← and →, which performs the rotation transform to the left and right sides respectively.

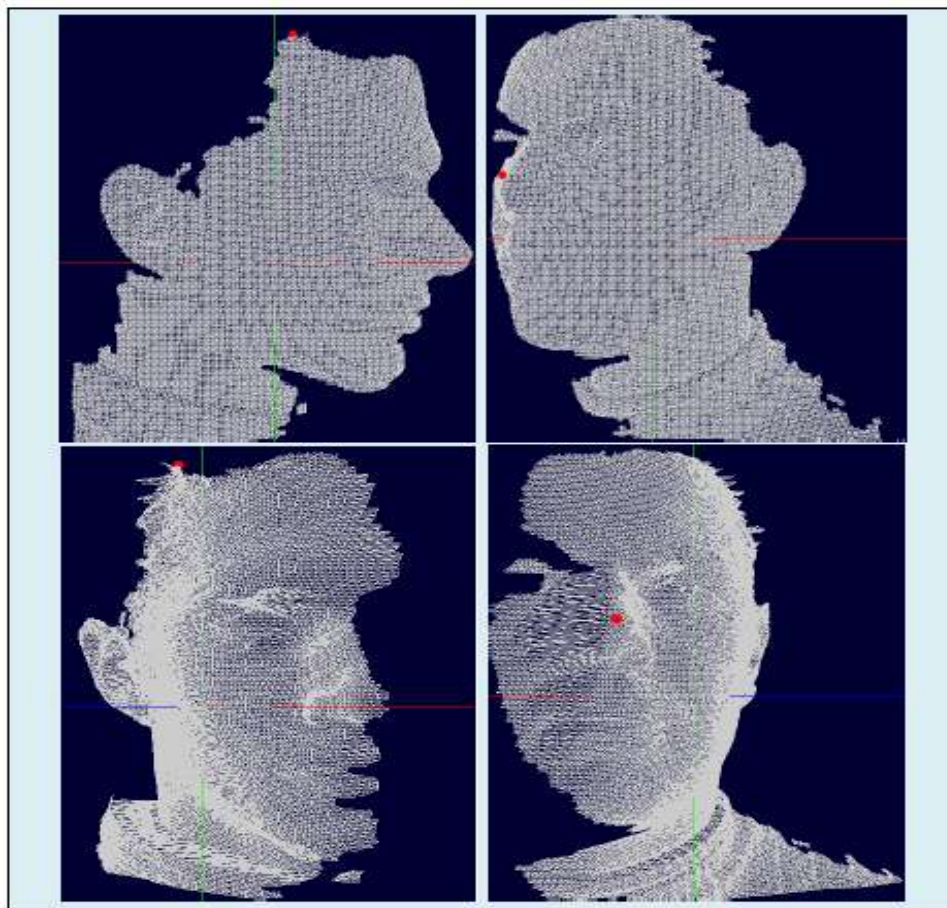


Fig. (2): Examples of 3D data files are displayed using the 3D viewer program: the top row represents two facial meshes for different subjects under different poses, the second row represents the same rotated facial meshes using the proposed 3D viewer.

3. Neighborhood Detection Algorithm

The second essential step in the preprocessing operations is represented by determining the neighboring vertices for each vertex in the acquired mesh and having knowledge of vertex localization relative to other vertices that localized and scattered within its local neighborhood. Additionally, the quantitative description of local surface shape needs to be detected in a manner which is invariant to the image scan pose with regard to 3D camera location. It is obvious that the accurate determination of vertex local neighborhoods has a great influence on local shape descriptor computation for this vertex. In this work, an innovative approach for neighbors defining is proposed, which is based only on connectivity information of mesh polygons namely VND-CI.

The proposed VND-CI method implies an exploitation of triangular faces that surround each vertex in order to detect K-ring neighborhood for this vertex, as shown in Figure 3. The classic method that used for detecting vertex neighbors is mainly based on using geodesic distance or Euclidean distance measure. As observed, computing geodesic distances or Euclidean distances between all points and over a surface mesh is computationally expensive. In general, each identified neighborhood is extremely generic. It includes three main elements:

- The vertices that formulate the neighborhood.
- The faces that contain neighborhood vertices.
- The threshold value used for defining the neighborhood border.

The main steps of VND-CI method are described in method 3.1, which involves an exploring the connectivity information of any vertex v_i through reading data file phase. The input to this method is list of polygonal faces nf . The connectivity information of each vertex v_i represented by a set of triangular faces surrounding it and the vertices that constitute each triangular face. Then, for each

vertex v_i , a gathering process for all vertices that share the same faces and surrounds the vertex v_i is performed. An ignoring of the repeatable vertices is taking in consideration. The main contributions of VND-CI method could be summarized via the following reported observations:

- To avoid the common computationally expensive approaches, which are based on geodesic distance or Euclidian distance computation for each mesh vertex.
- To have knowledge about vertex localization with respect to other vertices that are scattered within its local neighborhood.
- Speed up the processing time throughout the whole system via utilization of faces and their vertices only.
- To provide flexible size of the extracted interested regions in the 3D image.
- Facilitate the calculation process for local shape descriptors.
- Facilitate the computation of the normal vector for each vertex in the 3D image.

Method 3.2 Neighbours Detection Method VND-CI

Input: Set of triangular faces nf

Output: Vertex Neighbours

Initialize $i \leftarrow 0$

Initialize $j \leftarrow 0$

for each f_i in nf do

$f_i.Buf_FaceIndexes = \text{Read vertices of } f_i$

 for each v_j in $f_i.Buf_FaceIndexes[j]$ do

 if ($\neg \text{find}(v_j, \text{Neighbor}[v_j])$)

$v_j.Neighbor = v_j$

$j \leftarrow j+1$

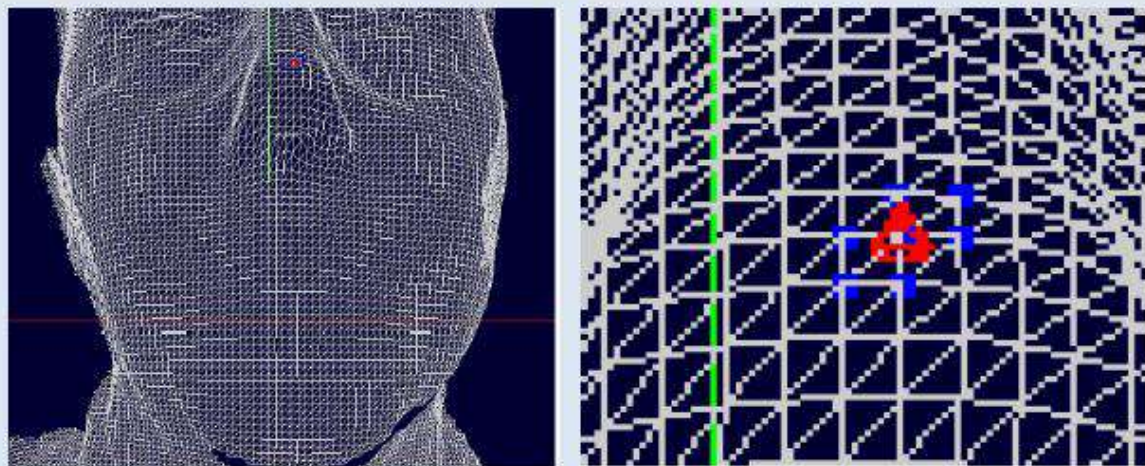
 end

 end

$j=0$

$i=i+1$

end



(a)

(b)

Fig. (3): One –Ring Neighborhood Determining approach of mesh vertices: (a) sample of detected Node tip (red color) and its neighbor (blue color), (b) same sample with zooming over nose tip patch

4. Experimental Results

As stated in section 3., a new method called Vertex Neighborhood Detection Based Connectivity Information VND-CI was presented to determine the K-ring neighborhood for each vertex in the acquired 3D mesh image. In order to evaluate the performance of the VND-CI neighboring detection approach, an experiment was carried out over 80 facial scans with different poses taken in arbitrary way from GAVADB databases. The reported results denoted that VND-CI method specifies lower time computation vs. the classic method, as shown in Table (1)

Table (1): Comparative results between neighbouring detection based VND-CI method and Euclidian distance measure.

Image Type	Average mesh size (vertex)	Computation time using Euclidian Distance (sec)	Computation time using VND-CI method (sec)
Frontal images	13643	7.8	0.308
Partial images	16184	11.46	0.35
Complexity	----	$O(n^2)$	$O(n)$

5. Discussion

As mentioned previously in section 3., the classic method to determine the neighbors of mesh vertex v_i is; by using geodesic distance or Euclidian distance to compute the distance between vertex v_i and each vertex in the mesh. Then, collecting all the vertices that lie within predefined radius sphere for the purpose of identifying the neighbors of vertex v_i . The computation time in this case will be $O(n^2)$ (expensive computationally), since n is the number of vertices in the acquired mesh. Regarding VND-CI method based neighbors detection process, there is no need to calculate the distance between vertex v_i and all the vertices in the 3D mesh image due to taking the advantage of connectivity information of v_i only. Consequently, a great drop in computation time is yielded; $O(n)$. Furthermore, the reported computation time in Table 4.1 corresponds to the computation time of two main preprocess operations; reading data file and determining neighbors for each vertex in the readable data points. As shown in Table 4.1, the experimental results provide an accurate determining for vertex neighbors number compared to the classic approach.

References

- [1] N. Alyüz, B. Gökberk and L. Akarun, “**Regional Registration for Expression Resistant 3D Face Recognition**”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 5, NO. 3, Sep. 2010.
- [2] T. C. Faltemier, K. W. Bowyer, and P. J. Flynn, “**A region ensemble for 3D face recognition**,” IEEE Trans. Inf. Forensics Security, vol. 3, no. 1, pp. 62–73, Mar. 2008.
- [3] Chua, C., Jarvis, R.: Point signatures: a new representation for 3D object recognition. Int. J.Comput. Vis. 25(1), pp. (63–85), 1997.
- [4] R. Kimmel and J. A. Sethian, “**Computing Geodesic Paths on Manifolds**”, In Proc. Natl. Acad. Sci. USA, Vol. 95, pp. 8431 – 8435, July 1998.
- [5] Szeptycki, P., Ardabilian, M., & Chen, L., “**A coarse-to-fine curvature analysis-based rotation invariant 3D face landmarking**”. International conference on biometrics: theory, applications and systems, pp. (32–37), 2009.
- [6] Xin Fan, Qi Jia, Kang Huyan, Xianfeng Gu, Zhongxuan Luo, “**3D facial landmark localization using texture regression via conformal mapping**” Pattern Recognition Letters, ELSEVER, pp. (1-8), 2016.

Fuzzy - Lagrange Techniques With Slantlet Transform For Image De-blurring

Ahmed Othman Khalaf Waleed Rasheed Humood Shaimaa Khudhair Salih
Mustansiriyah University/ Educational College/ Computer Science Department
ahmedokha@yahoo.com waleedsoft2000@yahoo.com shaimaaash@yahoo.com

Abstract:

"This work introduces an image de-blurring method which combines both the slantlet transform method, soft thresholding and mathematical method (Lagrange polynomial interpolation method) and uses fuzzy level control to compare between results to choose the best and suppress blur effect, the key idea of the proposed system is to split the image into low-frequency image and high-frequency image using slantlet transform, and apply proposed fuzzy Lagrange filter regularization-based sharpening."

"The proposed system was designed using the principles and theory of the Lagrange polynomial interpolation to estimate the pixels values replaced in the center window of the filter. The effects of the neighborhood's window pixels on the center pixel will be calculated by Lagrange, the replacing operation of the pixels will be controlled by adaptation technique like Fuzzy rules. The fuzzy rules were used to adjust the replacing operation or adjust the pixels value to get the adaptive sharpening operation. This operation will be applied to the image resulting from the slantlet transform."

Keyword: Image de-blurring, weighted-median, Lagrange method, Slantlet Transform, Fuzzy rules.

تقنيات المنطق المضرب ونظريه لاكرانج الرياضية مع تحويل سلانليت لإزالة غواش الصورة
م.م. احمد عثمان خلف م.م. وليد رشيد حمود م.م. شيماء خضير صالح

المستخلص

هذا العمل يقدم طريقة لتقليل الغواش والتي تجمع طريقة تحويل سلانليت وحد العتبة الناعم وطريقة رياضية (طريقة توليد لاكرانج متعدد الحدود) وباستخدام مستوى السيطرة المضرب للمقارنة بين النتائج لأختيار الأفضل والتي تقوم بقمع تأثير الغواش، المبدأ الرئيسي من النظام المقترح هي تجزئة الصورة الى ترددات عالية للصورة وترددات واطئة باستخدام تحويل سلانليت وتطبيق مقترح مرشح منظم لاكرانج المضرب مبني على الحدة.

النظام المقترح صمم باستخدام مفاهيم ونظريات توليد لاكرانج متعدد الحدود لتخمين قيم عناصر الصورة التي توضع في مركز نافذة المرشح. تأثيرات عناصر الصورة المجاورة لمركز نافذة الصورة سوف تحسب بواسطة لاكرانج. عملية تبديل عناصر الصورة سوف يتم السيطرة عليها من خلال تقنية قابلة للتكيف مثل قوانين المنطق المضرب، قوانين المنطق المضرب سوف تستخدم لتنظيم عملية التبديل أو لضبط قيمة عنصر الصورة للحصول على عملية حدة متكيفة. هذه العملية سوف تطبق على الصورة الناتجة من تحويل سلانليت.

الكلمات المفتاحية: إزالة الغواش، تحويل سلانليت، توليد لاكرانج متعدد الحدود، مستوى السيطرة المضرب.

1. Introduction

"Since our eyes gather more information than any of our other sense organs, and since the visual cortex seems to dominate the brain, images play a central role in our existence [1]. With the advantage of computers, and their ever-increasing role in managing the many activities of everyday life, the representation and processing of images in digital form have acquired great importance. The representation of images plays central roles in computer graphics, especially in image synthesis, processing, and analysis [1]."

"With the rapid development of computerized scientific instruments come a wide variety of interesting problems for data analysis and signal processing. In fields ranging from extra galactic astronomy to molecular spectroscopy to medical imaging to synthetic aperture radar imaging to

computer vision, one must recover a signal, curve, image, spectrum or density from incomplete, indirect and noisy data [2].

Image De-blurring

The de-blurring method developed relies on the facts that natural images have sparse leading edges and Edges of the blurred image are lesser sparse than that of the de-blurred images as the edges of the blurred images occupy a larger area due to blurring. So, a prior which tend to make the edges sparser will tend to make the images sharper also. The assumption that edges are sparser in natural sharp images may be an oversimplification of the problem but the results obtained on this analysis are promising.

The prior should be adjusted and the cost function should be altered such that initial iteration which estimate the lower frequency components of the image are regularized with bigger weight whereas later iterations which corresponds to higher frequency components should be regularized with smaller weights. This adjustment ensures noise suppression at the same time allows for better sparseness.

The Slantlet Transform

“The Slantlet Transform (SLT) is an orthogonal discrete wavelet transform (DWT) with two zero moments and with improved time localization. It also retains the basic characteristic of the usual filter bank such as octave band characteristic, a scale dilation factor of two and efficient implementation. However, the SLT is based on the principle of designing different filters for different scales unlike iterated filter bank approaches for the DWT [3].”

The discrete wavelet transform (DWT) is usually carried out by filter bank iteration, however, for a fixed number of zero moments, this does not yield a discrete-time basis that is optimal with respect to time localization. The basis, is not based on filter bank iteration, instead different filters are used for each scale. For coarse scales, the support of the discrete-time basis function approaches $2/3$ that of the corresponding functions obtained by filter bank iteration. This slantlet basis is piecewise linear and retains the octave-band characteristic [4].

“For the two-channel case, the shortest filters for which the filter bank is orthogonal and having K zero moments are the well-known filters described by Daubechies. For $K=2$ zero moments, those filters $H(z)$ and $F(z)$ and are of length 4. For this system, designated $D2$, the iterated filters in figure (3.6) are length 10 and 4. without the constraint that the filters are products, an orthogonal filter bank with $K=2$ zero moments can be obtained where the filter lengths are 8 and 4, as shown in Figure (1), side by side with the iterated $D2$ system. That reduction of two samples grows with the number of stages. [5].”

Weighted Median Filter [6]

“Weighted-Median filter used in spatial domain to add blur to image, then the proposed system implemented on those Images. The basic idea is to give higher weight to some samples, according to their position with respect to the center of the window.” The following steps explain the implementation of Weighted Median filter:

1. Each sample is given a weight according to its spatial position in the window.
2. Weights are defined by a weighting mask
3. Weighted samples are ordered as usually
4. The weighted median is the sample in the ordered array such that neither all smaller samples nor all higher samples can cumulate more than 50% of weights.
5. If weights are integers, they specify how many times a sample is replicated in the ordered array.

The following is a Numerical example for the weighted median filter.

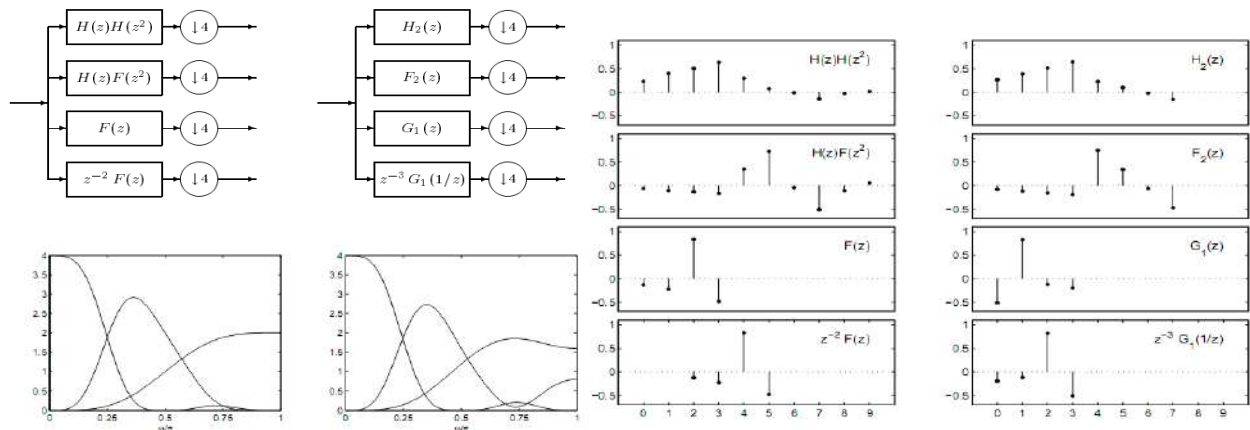
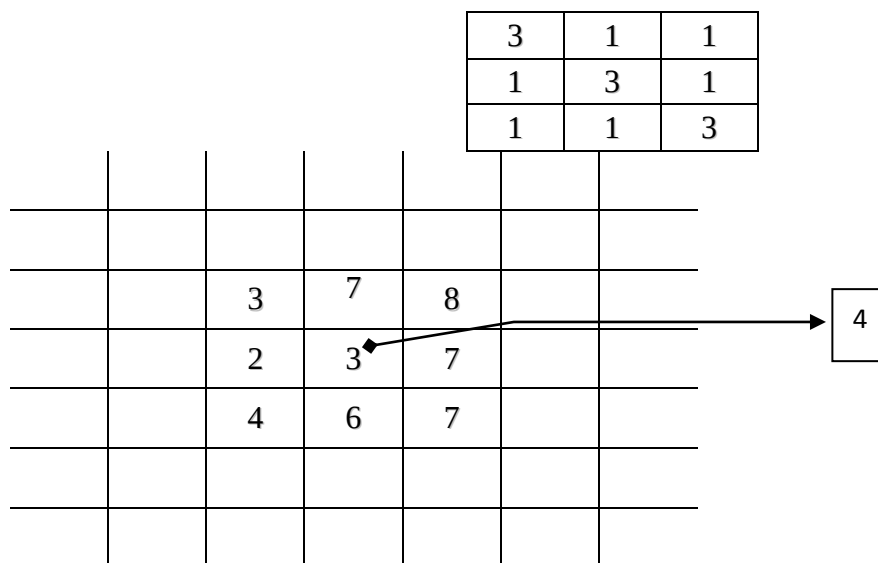


Fig. (1): comparison of iterated D2 filter bank (left-hand side) and Slantlet filter bank (right hand-side).



3,3,3,7,8,2,3,3,3,7,4,6,7,7,7

After ascending sort

2,3,3,3,3,3,3,4,6,7,7,7,7,8

Fig. (2): Example for the weighted median filter

The Lagrange Interpolation Polynomial⁷⁷

“The problem of constructing a continuously defined function from given discrete data is unavoidable whenever one wishes to manipulate the data in a way that requires information not included explicitly in the data. The relatively easiest and in many applications often most desired approach to solve the problem is interpolation, where an approximating function is constructed in such a way as to agree perfectly with the usually unknown original function at the given measurement points. In the practical application of the finite calculus of the problem of interpolation is the following: given the values of the function for a finite set of arguments, to determine the value of the function for some intermediate argument [7].”

Lagrange Interpolation

“Consider the function $f: [x_0, x_n] \rightarrow \mathbb{R}$ given by the following table of values:”

x_k	x_0	x_1	$\dots$	x_n
$f(x_k)$	$f(x_0)$	$f(x_1)$	$\dots$	$f(x_n)$

x_k is called *interpolation nodes*, which are not necessarily equally distanced from each other. One seeks to find a polynomial $P(x)$ of degree n that approximates the function $f(x)$ in the interpolation nodes, i.e. [8].

$f(x_k) = P(x_k)$; $k = 0, 1, 2, \dots, n$.

The Lagrange interpolation method finds such a polynomial without solving the system.

“Theorem: Lagrange Interpolating Polynomial [7].”

“The Lagrange interpolating polynomial is the polynomial of degree n that passes through $(n + 1)$ points $y_0 = f(x_0)$, $y_1 = f(x_1)$,... $y_n = f(x_n)$. Let: ”

$$P(x) = \sum_{j=0}^n P_j(x) \quad \text{..... (1)}$$

where

$$P_j(x) = y_j \prod_{k=0, k \neq j}^n \frac{x - x_k}{x_j - x_k}. \quad \text{..... (2)}$$

written explicitly:

$$P(x) = \frac{(x-x_1)(x-x_2)\dots(x-x_n)}{(x_0-x_1)(x_0-x_2)\dots(x_0-x_n)}y_0 + \frac{(x-x_0)(x-x_2)\dots(x-x_n)}{(x_1-x_0)(x_1-x_2)\dots(x_1-x_n)}y_1 + \dots + \frac{(x-x_0)(x-x_1)\dots(x-x_{n-1})}{(x_n-x_0)(x_n-x_1)\dots(x_n-x_{n-1})}y_n. \quad \text{..... (3)}$$

Lagrange interpolating polynomials are implemented in *mathematics* as Interpolating Polynomials [data, var]. For the case $n = 4$, i.e. interpolation through five points, one has:

$$P(x) = \frac{(x-x_1)(x-x_2)(x-x_3)(x-x_4)}{(x_0-x_1)(x_0-x_2)(x_0-x_3)(x_0-x_4)}y_0 + \frac{(x-x_0)(x-x_2)(x-x_3)(x-x_4)}{(x_1-x_0)(x_1-x_2)(x_1-x_3)(x_1-x_4)}y_1 + \frac{(x-x_0)(x-x_1)(x-x_3)(x-x_4)}{(x_2-x_0)(x_2-x_1)(x_2-x_3)(x_2-x_4)}y_2 + \frac{(x-x_0)(x-x_1)(x-x_2)(x-x_4)}{(x_3-x_0)(x_3-x_1)(x_3-x_2)(x_3-x_4)}y_3 + \frac{(x-x_0)(x-x_1)(x-x_2)(x-x_3)}{(x_4-x_0)(x_4-x_1)(x_4-x_2)(x_4-x_3)}y_4 \quad \text{..... (4)}$$

and

$$P'(x) = \frac{(x-x_2)(x-x_3)(x-x_4) + (x-x_1)(x-x_3)(x-x_4) + (x-x_1)(x-x_2)(x-x_4) + (x-x_1)(x-x_2)(x-x_3)}{(x_0-x_1)(x_0-x_2)(x_0-x_3)(x_0-x_4)}y_0 + \frac{(x-x_2)(x-x_3)(x-x_4) + (x-x_0)(x-x_3)(x-x_4) + (x-x_0)(x-x_2)(x-x_4) + (x-x_0)(x-x_2)(x-x_3)}{(x_1-x_0)(x_1-x_2)(x_1-x_3)(x_1-x_4)}y_1 + \frac{(x-x_1)(x-x_3)(x-x_4) + (x-x_0)(x-x_3)(x-x_4) + (x-x_0)(x-x_1)(x-x_4) + (x-x_0)(x-x_1)(x-x_3)}{(x_2-x_0)(x_2-x_1)(x_2-x_3)(x_2-x_4)}y_2 + \frac{(x-x_1)(x-x_2)(x-x_4) + (x-x_0)(x-x_2)(x-x_4) + (x-x_0)(x-x_1)(x-x_4) + (x-x_0)(x-x_1)(x-x_3)}{(x_3-x_0)(x_3-x_1)(x_3-x_2)(x_3-x_4)}y_3 + \frac{(x-x_1)(x-x_2)(x-x_3) + (x-x_0)(x-x_2)(x-x_3) + (x-x_0)(x-x_1)(x-x_3) + (x-x_0)(x-x_1)(x-x_2)}{(x_4-x_0)(x_4-x_1)(x_4-x_2)(x_4-x_3)}y_4$$

Note that the function $P(x)$ passes through the points (x_i, y_i) , i.e. $P(x_i) = y_i$.

For Examples: The Lagrange interpolating polynomial is given by [8].

$$f_n(x) = \sum_{i=0}^n L_i(x) f(x_i) \quad \text{..... (5)}$$

where n in $f_n(x)$ stands for the n^{th} order polynomial that approximates the function $y = f(x)$ given at $n+1$ data points as $(x_0, y_0), (x_1, y_1), \dots, (x_{n-1}, y_{n-1}), (x_n, y_n)$, and

$$L_i(x) = \prod_{\substack{j=0 \\ j \neq i}}^n \frac{x - x_j}{x_i - x_j} \quad \text{..... (6)}$$

$L_i(x)$ is a weighting function that includes a product of $n-1$ terms with terms of $j = i$

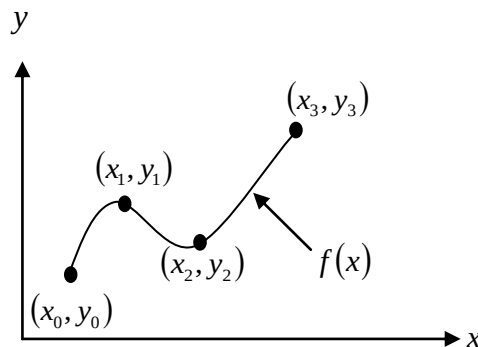


Fig. (3): Interpolation of Discrete Data.

Let $Y = F(x)$ such that $y_0 = f(x_0), y_1 = f(x_1), y_2 = f(x_2), \dots, y_n = f(x_n)$, then to estimate value of $f(x)$ we use:[11]

x	x_0	x_1	x_2	...	x_n
F(x)	y_0	y_1	y_2	...	y_n

$$F(x^*) = \sum_{j=0}^n f(x_j) \prod_{\substack{i=0 \\ i \neq j}}^n \frac{(x^* - x_i)}{(x_j - x_i)} \quad \text{..... (7)}$$

Example: By Lagrange formula, find the value of $f(3)$ and $f(5)$ from the table.

X	0	1	2	4
F(x)	1	1	2	5

Solution:

$$\begin{aligned} F(3) &= \sum_{j=0}^3 f(x_j) \prod_{\substack{i=0 \\ i \neq j}}^3 \frac{(3 - x_i)}{(x_j - x_i)} \\ &= f(x_0) \frac{(3 - x_1)(3 - x_2)(3 - x_3)}{(x_0 - x_1)(x_0 - x_2)(x_0 - x_3)} + f(x_1) \frac{(3 - x_0)(3 - x_2)(3 - x_3)}{(x_1 - x_0)(x_1 - x_2)(x_1 - x_3)} + \\ &\quad f(x_2) \frac{(3 - x_0)(3 - x_1)(3 - x_3)}{(x_2 - x_0)(x_2 - x_1)(x_2 - x_3)} + f(x_3) \frac{(3 - x_0)(3 - x_1)(3 - x_2)}{(x_3 - x_0)(x_3 - x_1)(x_3 - x_2)} \end{aligned}$$

$$F(3) = 3.5$$

So by the same way one has $F(5)=6$.

Fuzzy System

“Fuzzy logic is a rule-based decision process that seeks to solve problems where the system is difficult to model and where ambiguity or vagueness is abundant between two extremes. Fuzzy logic allows the system to be defined by logic equations rather than complex differential equations and comes from a thinking that identifies and takes advantage of the grayness between the two extremes. Fuzzy logic systems are composed of fuzzy subsets and fuzzy rules. The fuzzy subsets represent different subsets of the input and output variables. The fuzzy rules relate the input variables to the output variables via the subsets. Given a set of fuzzy rules, the system can compensate quickly and efficiently. Though the Western world did not initially accept fuzzy logic and fuzzy ideas, today fuzzy logic is applied in many systems.”

“There are many benefits in using fuzzy logic. Fuzzy logic is conceptually easy to understand and has a natural approach [9]. Fuzzy logic is flexible and can be easily added to and adjusted. It is very tolerant of imprecise data and can model complex nonlinear functions with little complexity. It can also be mixed with conventional control techniques. There are three major components of a fuzzy system: fuzzy sets, fuzzy rules, and fuzzy numbers”.

To further see how fuzzy sets contain smaller sets and so forth, consider an off-road vehicle. An off road vehicle is a smaller set of vehicles. Every off-road vehicle is a vehicle, but not every vehicle is an off-road vehicle. The question is raised: when is a vehicle an off-road vehicle? Once again it is a matter of degree. An off-road truck with raised suspension stands for an even smaller set of vehicles, a subset of off-road vehicles. These fuzzy sets combined with fuzzy rules build a fuzzy system. Fuzzy sets can be created out of anything.

2. Related Work

Khalid Ali Hussien in (2011) [10]

- The Lagrange interpolation method was used in a new neural network learning by develops the weighting calculation in the back propagation training. This proposed developing decrease the learning time with best classification operation results. Also, the Langrage interpolation polynomial was used to process the image pixels and remove the noise of image. This interpolation gives the effective processing in removing the noise and error in the image layers. One of the advantages of this method is reduce the noise to minimum value by replacing the noisy pixels (detected by Lagrange Back propagation Neural Network LBPNN) by results calculated by the Lagrange interpolation with high speed processing and best RMSE results.

Adarsh Nagaraja in (2010) [11]

- The method only makes weak assumptions about the blurring filter and is able to undo a wide variety of blurring degradations. To overcome the ill-posedness of the blind image deblurring problem, the method includes a learning technique which initially focuses on the main edges of the image and gradually takes details into account. A new image prior, which includes a new edge detector, is used.

3. The Proposed System

“Degradations are usually unavoidable and come in many forms with noise and blur as the most studied. Blurs render images useless since it makes image understanding difficult or impossible. Due to the wealth of information that images contain, researches have been attempting to remove blurs for decades. This process is known as image restoration or reconstruction.”

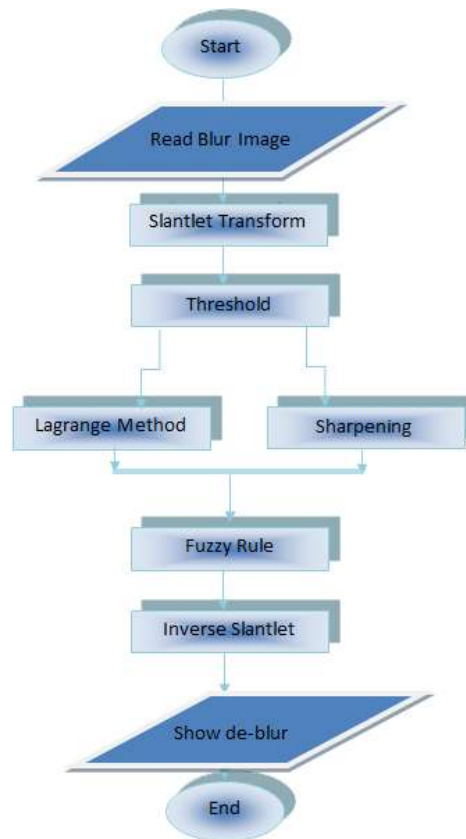


Fig. (4): The Block Diagram of the Proposed System

Thresholding is a simple non-linear technique, which operates on one slantlet coefficient at a time. In its most basic form, each coefficient is threshold by comparing it against threshold, if the coefficient is smaller than or equal to threshold, set to zero; otherwise it is kept or modified. Replacing the small noisy coefficients by zero and inverse slantlet transform on the result may lead to reconstruction with the essential signal characteristics and with less noise.

“In this proposed method, a threshold estimation techniques for image de-blurring are presented which are sub-band dependent i.e. the parameters for computing the threshold are estimate from the observed data, one for each sub-band. The aim of this work is to implement a de-blurring method that can remove the image blur by using the slantlet transform and thresholding techniques by applying weighted median in spatial domain to help in the image reconstruction and by using Lagrange method and fuzzy rules.”

The proposed method depends on estimating blur in the image of types (BMP, JPEG, and TIFF) file format, then calculating the appropriate threshold to remove the coefficient of slantlet filter using the slantlet decomposition technique.

The first step is to input the blurry image and choose threshold rule (Visushrink) and apply weighted median in spatial domain by multiplying mask [3*3] with small windows from image array (convolution).

“The second step is to call Slantlet transform function in order to represent important information on four sub-bands in frequency domain to features extraction then perform the threshold type equation to eliminate noise signal less than the threshold value (Thv) and shrink the signal greater than threshold value (Thv).”

The third steep is to call the Lagrange method and sharpening techniques and compare the results that come from both methods by using the fuzzy rules that decide finally the best result and use it and then apply the inverse Slantlet transform and show the processed image.

Finally, compute and display the objective criteria (Peak Signal-to-Noise Ratio, Signal-to-Noise Ratio, and Root Mean Square Error) as unbiased criteria in order to compare with other methods of de-blurring image.. Algorithm 3.1 describes the steps of proposed method.

Algorithm 1: proposed method steps.

Input: Blurry image

Output: De-blurring image

Step 1: Start

Step 2: Read blur image.

Step 3: Apply slantlet transform.

Step 4: Apply threshold selection rule method (Visushrink).

Step 5: Apply Lagrange method and sharpening techniques simultaneously.

Step 6: Apply fuzzy rules to choose the best result.

Step 7: Apply Inverse slantlet transform.

Step 8: Compute PSNR, SNR and ERMS.

Step 9: Display de-blurring image.

Step 10: End.

Images results of BMP files as objective criteria using Visushrink method with hard thresholding type are better than soft threshold, CPU time in hard threshold is almost shorter than CPU time in soft threshold and for PSNR the image which was blurred by using median filter with soft and hard threshold get the best result from the other. Table (1) represents the PSNR, SNR, and ERMS of BMP files by soft and hard threshold type with using Visushrink.



Fig. (5): Lena Original Image



(a)



(b)



(c)

Fig. (6) Represents lena.bmp in (a) Blurred Image with Mean Filter (b) Blurred Image with Median Filter (c) Blurred Image with Weighted Median Filter



(a- after de-blur)



(b- after de-blur)



(c- after de-blur)

Fig. (7) Represents lena.bmp After De-blurring by Using Soft Threshold with VisuShrink



(a- after de-blur)



(b- after de-blur)



(c- after de-blur)

Fig. (8) Represents lena.bmp After De-blurring by Using Hard Threshold with VisuShrink

4. Result Discussion

The method of image de-blurring using slantlet transform and Lagrange with fuzzy rule in this work has yielded the following conclusions:

1. By using slantlet transform instead of special methods the process speed increases.
2. Lagrange method with slantlet transform is used to estimate the blur value nearest to neighborhood values of it. It makes the method more accurate with speed increase.
3. The fuzzy rule is used to achieve comparison to choose the best and most suitable value to replace it instead of the blur value, making the reconstructed image as good as possible based on objective criteria.
4. Images results of de-blurring BMP files by using soft threshold type are better than those of hard thresholding type based on objective criteria.

Table (1) Show Results of the PSNR, SNR, ERMS, CPU Time After Blurring Lena.BMP Image by Different Filters with Soft and Hard Threshold with VisuShrink.

Threshold Types	Blur Type	PSNR	SNR	ERMS	CPU Time
Soft Threshold With VisuShrink	Mean Filter	48.0156	35.4677	3.0480	2.5896
	Median Filter	51.5569	53.0761	2.0275	2.8704
	Weighted Median Filter	49.9554	44.2175	2.4380	2.0280
Hard Threshold With VisuShrink	Mean Filter	53.6944	68.4251	1.5852	2.6832
	Median Filter	57.6817	107.6605	1.0016	2.0280
	Weighted Median Filter	56.1296	90.2523	1.1976	2.2308

5. Conclusions and Suggestions for Future Work

5.1 Conclusions

The method of image de-blurring using slantlet transform and Lagrange with fuzzy rule in this work has yielded the following conclusions:

1. By using slantlet transform instead of special methods the process speed increases.
2. Lagrange interpolation calculation was used with a Slantlet transform and fuzzy technique to de-blurring images with a full blurring or partial blurring.
3. Fuzzy rules more effect in the partial blurred image with good RMSE values.

5.2 Suggestions for Future Work

The future works suggestions related to this thesis are demonstrated in the following recommendations.

1. Use Lagrange with neural network or genetic algorithm instead of Lagrange with fuzzy.
2. Apply the algorithm that is implemented in this work to the moving images (video films). In this case, care must be taken to synchronize frames to ensure correct display of the video film frames and the speed of the process is efficient.
3. Develop a modified version of the slantlet transform like multi-slantlet transform in order to increase the speed of the process.

References

- [1]. Bates, R. H. T., and McDonnell, M. J., **"Image Restoration Reconstruction"**, Clarendon Press-Oxford, 1986.
- [2]. Gomes, J., and Velho, L., **"Image Processing for Computer Graphics"**, Springer-Verlag New York, Inc., 1997.
- [3]. Donoho, D. L., **"Nonlinear Wavelets Methods for Recovery of Signals, Densities, and Spectra from Indirect and Noisy Data"**, In Ingrid Daubechies editor, Different perspectives on wavelets, I, PP. 173-205, American Math. Society, providence, 1993.
- [4]. G. Panda, P. K. Dash, A. K. Pradhan, and S. K. Meher, **"Data Compression of Power Quality Events Using the Slantlet Transform"**. IEEE. Transaction on Power Delivery, vol. 17, NO. 2, April 2002.
- [5]. Ivan W. Selesnick, **"Discrete Wavelet Transform Of Approximation Order 2 With Improved Time-Localization-The Slantlet Transform"**, Polytechnic University, Electrical Engineering, 6 Metrotech Center Brooklyn, NY 11201-3840.
- [6]. Ivan W. Selenick, **"The Slantlet Transform"**, IEEE TRANCTIONS ON SIGNAL PROCESSING, VOL. 47, NO. 5, MAY 1999.
- [7] Gonzalo R. Arce¹, Jan Bacca¹, and José L. Paredes², **"Nonlinear Filtering for Image Analysis and Enhancement"**, ¹University of Delaware; ²Universidad de Los Andes.
- [8]. Denis, D., **"Depth from Blur, Combining Image De-blurring and Depth Estimation"**, submitted on July 24, 2009.
- [9]. **"Fuzzy Logic Toolbox"** available at <http://www.mathworks.com/access/helpdesk/help/toolbox/fuzzy/fuzzy.shtml>
- [10]. Khalid, A. H., **"The Lagrange Interpolation Polynomial for Neural Network Learning"**. IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.3, March 2011.
- [11] Adarsh, N., **"Blind and Semi-Blind De-blurring of Natural Images"**, on Image Processing, IEEE Transactions. (Vol. 19, Issue:1), www.cs.ucf.edu/~adarsh/blindDeconv_v2.pdf, Jan. 2010.

The K-SVD Algorithm for Image Denoising Depending on Weighted Median Filter with Slantlet Transform

Ahmed Othman Khalaf Waleed Rasheed Humood Shaimaa Khudhair Salih
Mustansiriyah University/ Educational College/ Computer Science Department
ahmedokha@yahoo.com waleedsoft2000@yahoo.com shaimaaash@yahoo.com

Abstract:

"The digital images include undetermined degree of noise. Image denoising algorithm try to remove this noise from the image. In theory, the resulting de-noised image will not include any noise. Denoising of natural images influenced by Salt& Pepper noise by Slantlet transformation techniques is very operative because of its capability to capture the energy of a signal in small number energy transform values".

"In this paper, mean pixel energy for each windows of noisy image will calculate by using the Energy Estimation operation then store in a dictionary. Noisy image decomposed using Slantlet transform and then applied K-SVD algorithm noise removal. In the same time, the Weighted Median Filter is also applied to the de-noised image for noise removal. Finally, the de-noised image get from the comparison between (Weighted Median with K-SVD algorithm) outputs and select the appropriate pixels depend on the energy value stored on the dictionary. From the experimental results, the suggest technique can effectively remove a single Salt& Pepper noise while curing the image information in good health with less blur and demonstrate its better fidelity criteria (PSNR and E_{RMS}) after apply proposed pixel rule selection compared with results of Weighted Median and K-SVD algorithm."

Keyword: Image, Denoising, Slantlet, Image demising, K-SVD.

خوارزمية كي - اس في دي لإزالة ضوضاء الصورة بالاعتماد على مرشح المتوسط المرجح و تحويل سلانليت

م.م. احمد عثمان خلف م.م. وليد رشيد حمود م.م. شيماء خضير صالح

المستخلص

الصورة الرقمية تشمل درجة غير محددة من الضوضاء. خوارزمية ازالة الضوضاء من الصورة تحاول رفع الضوضاء من الصورة. نظرياً، عملية رفع الضوضاء من الصورة لن يتضمن اي ضجيج. أزاله الضوضاء من الصور الطبيعية المتأثرة بضوضاء رشة الملح والفلفل عن طريق تقنيات تحويل سلانليت فعالة جدا بسبب قدرة النقاط الاشارة من قيم تحويل الاشارة للقيم الصغيرة. في هذا البحث، معدل طاقة البكسل لكل نافذة الصورة المصابة بالضوضاء ستحسب باستخدام عملية تقدير الطاقة ثم تخزين في القاموس، الصورة المصابة بالضوضاء سوف تحلل باستخدام تحويل سلانليت وبعد ذلك يتم تطبيق خوارزمية كي - اس في دي، في نفس الوقت، مرشح المتوسط المرجح يتم تطبيقه لرفع الضوضاء من الصورة المصابة بالضوضاء، أخيراً، الصورة المرفوع منها الضوضاء تأتي من المقارنة بين نتائج (خوارزمية كي - اس في دي ومرشح المتوسط المرجح) واختيار البكسلات الملائمة يعتمد على قيم الطاقة المخزنة في القاموس. من النتائج العملية، الطريقة المقترحة يمكن ان تزيل بشكل كفوء ضوضاء الملح والفلفل بينما تبقى معلومات الصورة باقل درجة من التشويه وتعرض معايير الدقة (نسبة ذروة الاشارة- للضوضاء، وجذر القيمة العظمى للخطأ) بعد تطبيق قاعدة اختيار القيمة والمقارنة مع نتائج (خوارزمية كي - اس في دي ومرشح المتوسط المرجح).

الكلمات المفتاحية: الصورة، ازالة الضوضاء، تحويل سلانليت، اصل الصورة.

1. Introduction

The first encounter with digital image denoising were in the region of relating to astronomy imaging and space exploration. Digital Images included were frequently subject to noise of one from or other. set an example, the region of relating to astronomy imaging degradation problem is in many cases be distinct by poisson noise, That is signal-dependent and hold its roots in the photon-counting statistics included with low light sources [1]. And another kind of noise is

Salt&Pepper noise. Fail pixel elements in the camera sensors, defect memory locations, or timing errors causes the salt-and-pepper type noise show up in the image as dots infect the image.

“The denoising purposes is to cutoff the noise section of the signal and to rebuilt signal while retaining as much as possible the significant signal features [2].

De-noising of natural images damaged by Salt&Pepper by use Transform techniques is very efficient, the case is its ability to capture the energy of a signal in small amount of energy transform values. Unprocessed, it states that the Slantlet transform return a large number of small coefficients so that a small number of large coefficients. variational method is very famous and powerful for image restoration since the complete variation. Anyway, the results that receives with total variation could be over-smoothed and the image details like textures could be removed simultaneously with noise[3]”.

Proposed Salt&Pepper noise removal method is to use Slantlet Transform with K-SVD Algorithm. A Weighted Median filter with mean energy window also used in pixel selection rule to obtained denoised image result with a good fidelity evaluation criteria for noisy colored Image.

The Slantlet Transform

Slantlet Transform (SLT) is consider an orthogonal discrete wavelet transform (DWT) with two zero moments, improved time localization. Also retains the basic specialty of the usual filter bank like octave band characteristic, a scale dilation factor of two and effective implementation. However, the SLT is based on the fundament of designing different filters for different scales not the same of iterated filter bank approaches for the DWT [4].

“Discrete wavelet transform (DWT) is often carried out with filter bank iteration, though, for a fixed number of zero moments, this does not income a discrete-time basis that is optimal with consideration to time localization. The concepts, is not based on filter bank iteration, therefor different filters are used for each scale. For coarse scales, the support of the discrete-time basis function technique 2/3 that of the corresponding functions included by filter bank iteration. This Slantlet concepts is piecewise linear and feedback the octave-band characteristic [5], Figure 1 shows the filter bank of slantlet transformation.”

Every filter bank has a scale dilation factor of two and supply a multiresolution decomposition. Slantlet filters are piecewise linear. There is no tree structure for Slantlet can be efficiently implemented such as an iterated DWT filter bank. Therefore, computational entanglement of the Slantlet are like the order as of the DWT, but Slantlet transform award better presentation in denoising and compression of the signal [6]

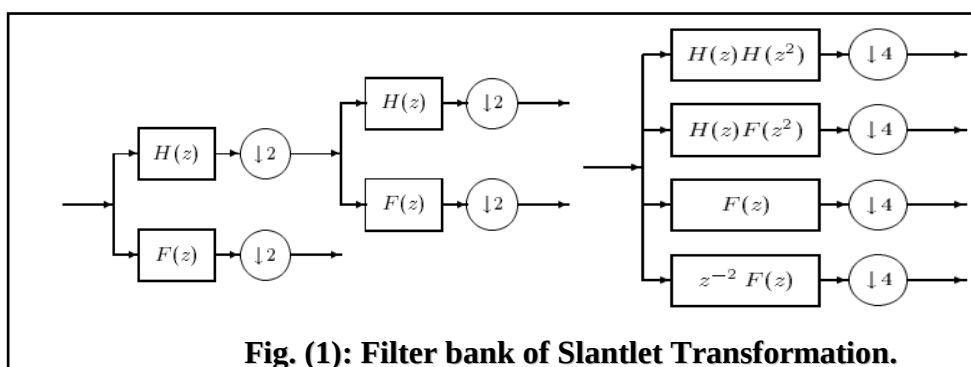


Fig. (1): Filter bank of Slantlet Transformation.

Denoising using K-SVD [7]

“In this part we discuss the implementation of the K-SVD algorithm to denoising of images. Before that can be addressed, we discuss how the method can be scaled up to address image denoising of arbitrary sizes. From the theory it is obvious that if the signal vectors have a high dimensionality, the size of the dictionary needs to be large for a stable acceptable reconstruction. This may not be the most suitable thing to do as the computational complexity scales up with the size of the vectors and the number of atoms in the dictionary. To address this issue the authors propose to break up the noisy image into patches and treat the vectorized version of each patch as

signals, thereby restricting the dimensionality of each atom in the dictionary. However, the size of the patch has to be chosen such that it encodes enough details of the underlying signal.”

It is also natural to select these patches to be overlapping in nature in order to reduce blocking artifacts that might result at the boundaries. Dealing with patches as signals, the K-SVD algorithm can be effectively scaled to denoise large images.

Application of the method to denoising necessitates posing the problem of denoising first.

For a given image, which can now be thought of as a set of signals Y , the denoising problem can be stated as the ill-posed problem of finding a set of patches Z which are related by

$$Y = Z + \eta \dots \dots (1)$$

where η is assumed to be the noise which corrupts the patches. The noise over the entire image is assumed to be zero mean Gaussian noise. In order to find the denoised image patches Z , we define an optimization problem akin.

The cost function let us to minimize the error for there stored image and the input noisy one, under the assumption that each patch in the input image can be described as a sparse linear collection of patches in the dictionary D . Ideally, for denoising the first term should be rewritten as $\|Z - Y\|_2^2 < C\sigma^2$ where C is a constant and σ^2 is the variance of the noise. This term is included incorporated into the cost

function in the choice of the parameter which will depend of the noise variance. The best form solution to this cost function is given by

$$\hat{Z} = \frac{(\lambda Y + \sum_i R_i^T D x_i)}{(\lambda I + \sum_i R_i^T R_i)} \dots \dots (2)$$

The solution to this problem thus involves averaging of overlapping patches behind each patch has been sparse coded beside with a weighted sum of the original noisy patch. Each pixel in a patch is hence a weighted linear combination of different pixels, the weights being derived from the sparse coding.

Since the patches are overlapping, the final value of each pixel is thus an average of all representations obtained from sparse coding stage.

Denoising by Weighted Median Filter

Weighted-Median filter is used in spatial domain to remove noise with minimum blur in image denoising.

The weighted median does “less filtering” than the ordinary median and is suitable when the noise is not too severe.[8]

It has the advantages of being easy to understand and extensible to image sharpening applications. [8]

The basic idea when using weighted-median filter is to give higher weight to some samples according to their position with respect to the center of the window, Each sample will supply with a weight to its attune spatial position in the window. Therefore, Weights are defined by a weighting mask and Weighted samples are organized in an ascending order.

The weighted median approach is the sample in the organized array such that neither all smaller samples nor all higher samples can accruing more than 50% of weights.

If weights are combining, they determine how many times a sample is iterated in the ordered array.

2. Proposed Image Denoising

The methodology of the proposed system for image denoising has six steps as shown in figure 2.

1. Calculate mean window energy of noisy image and stored as energy value in dictionary.
2. Transform the noisy image to orthogonal domain by using the Slantlet transform.
3. Apply K-SVD algorithm
4. Perform inverse Slantlet transform to obtain the K-SVD denoised image.
5. Apply Weighted Median filter (described in section 4) for noisy detail removal for noisy image.
6. Apply pixel selection rule to obtained the final denoised image.

The pixel selection rule suggested to select the best pixel from the result of K-SVD denoised Image output and Weighted Median denoised Image output, the selection based the energy window dictionary values that calculate in the first step of proposed system (energy estimation step). The rule of this step is (for each window of image):

$$P_{DI}(i) = \begin{cases} P_{K-SVD} & P_{K-SVD} \geq E_{dic} \\ P_{WM} & P_{WM} \geq E_{dic} \end{cases} \dots (3)$$

Where $P_{DI}(i)$ is the pixel of denoised image and $i=1,2,3,\dots,N$ the size of window.

P_{K-SVD} is the pixel of the K-SVD image output,

P_{WM} is the pixel of the Weighted Median image output,

E_{dic} is the mean pixel energy stored in dictionary calculate in step 1.

This step increase the accuracy of the output denoised Image and give the best estimation criteria.

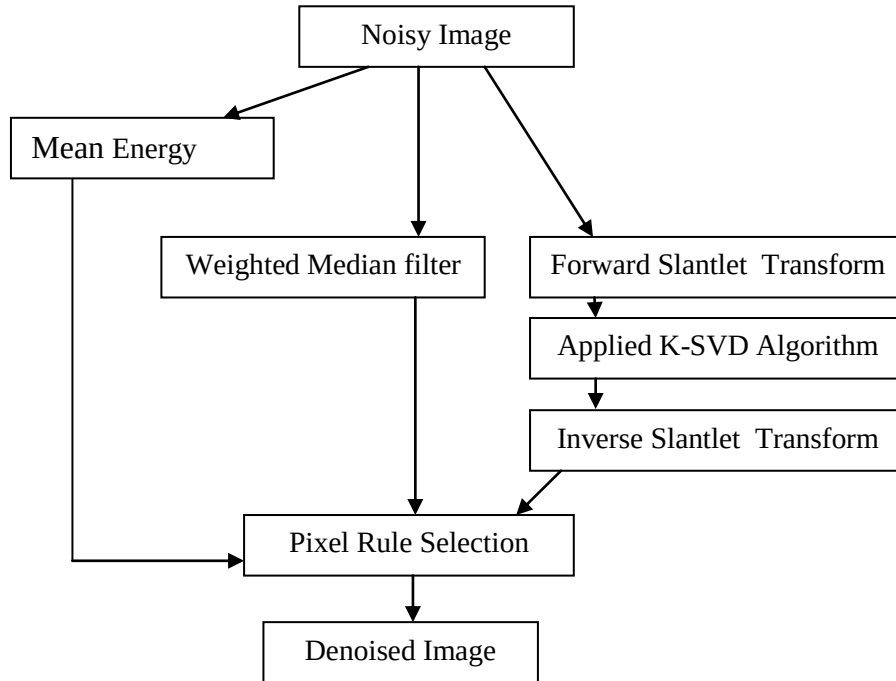


Fig. (2): Proposed Image Denoising System

The Denoising Algorithm(K-SVD): [3]

“The K-SVD algorithm building by using upon sparse representations, the outline review the major mathematical ideas of the K-SVD denoising algorithm. Let $g, f \in \mathbb{R}^{S1 \times S2}$ be the $S1 \times S2$ the size of noise in image and the clean images, respectively. To simplify notations, in this work always use the lowercase letters such as $g \in \mathbb{R}^{S1 \times S2}$ to acting a column vector by stacking the columns of the matrix g . Identical to the maximum a-posteriori probability (MAP) estimator and an assumption that all small image packaging can be sporadic implemented as a linear cluster of a redundant learned dictionary. The following steps for the K-SVD algorithm “.

- Select atoms from input.
- Atoms can be patches from the image.
- Patches are overlapping.
- Replace unused atom with minimally represented signal.
- Identify signals that use k-th atom (non zero entries in rows of X). Deselect k-th atom from dictionary.
- Find coding error matrix of these signals.
- Minimize this error matrix with rank-1 approximate from SVD The above steps are repeated until the path can be sparsely represent for entire image.

Fidelity Criteria [9]

In the proposed system evaluated criteria used to quality measurement like the Peak Signal to Noise ratio (PSNR)simultaneously with Root mean square Error using the following formulae,

$$MSE = \frac{1}{N * M} \sum_{r=0}^{M-1} \sum_{c=0}^{N-1} [x(r,c) - \hat{x}(r,c)]^2 \quad \dots\dots(4)$$

$$E_{RMS} = \sqrt{MSE} = \sqrt{\frac{1}{N * M} \sum_{r=0}^{M-1} \sum_{c=0}^{N-1} [x(r,c) - \hat{x}(r,c)]^2} \quad \dots\dots(5)$$

$$PSNR = 10 \log_{10} (255^2 / MSE) \text{ (db)} \quad \dots\dots(6)$$

3. Results and Discussions

The proposed system are implemented on image as sample with degree (15% and 35%) of Salt & Pepper noise.

After study, analysis and compare among results concluded some points about objective criteria explain in the following points:

1-images results as objective criteria (PSNR and E_{RMS}) after perform pixel rule selection greater than results with Weighted Median.

2-“images results as objective criteria (PSNR and E_{RMS}) after perform pixel rule selection greater than results with K-SVD Algorithm.”

“The tests were done using a window of size 5X5. The results here are 5X5 neighborhood window size are shown in table 1.”

Table (1) proposed System Experiments Result of 5X5 Neighborhood Window Size

Original image	Noisy image corrupted by 35% Salt&Pepper noise	After Weighted Median	After K-SVD&SLT	Denoised image
				
		PSNR=32.304 E_{RMS} =16.5805	PSNR=27.4102 E_{RMS} =19.3421	PSNR=34.031 E_{RMS} =13.5823
Original image	Noisy image corrupted by 15% Salt&Peppernoise	After Weighted Median	After K-SVD&SLT	Denoised image
				
		PSNR=38.2369 E_{RMS} =8.0263	PSNR=32.4923 E_{RMS} =15.3472	PSNR=41.5675 E_{RMS} =10.5624

4. Conclusions

In this paper, the image denoising using Slantlet transform is resolve with K-SVD algorithm and Weighted Median filter. Experimental results show the blur in the denoised image results after result pixel rule selection is less than from the Weighted Median and K-SVD Algorithm. Also, images results as objective criteria(PSNR and E_{RMS}) after perform pixel rule selection better than results with Weighted Median and K-SVD algorithm because the pixel rule selection use the relation of energy with a best pixel in selected window(from the results of Weighted Median and K-SVD algorithm)depend on the stored energy value in the (energy estimation dictionary). The selection between results of Weighted Median and K-SVD algorithm will done by compare between them with the mean energy of the neighborhood window of image.

References

- [1] Burrus, C. S., Goperath, R.A. and Gue, H., "**Introduction to wavelet and wavelet transform**", A primer Upper Saddle, NJ(U.S.A.), Prantice Hall, Inc., 1998.
- [2] Nagaraj B Patil, V M Viswanatha, Dr. Sanjay Pande M B, " **Slant Transformation as Atoolfor Pre-Processing in Image Processing**", International Journal of Scientific & Engineering Research Volume 2, 4, April-2011.
- [3] Shajun Nisha and KotherMohideen,"**A Novel Approach for Image Mixed Noise Reduction Using Wavelet Method**", IJARCSSE, ISSN: 2277 128X, Volume 3, Issue 11, November 2013
- [4] G. Panda, P. K. Dash, A. K. Pradhan, and S. K. Meher,"**Data Compression of Power Quality Events Using the Slantlet Transform**". IEEE. Transaction on Power Delivery, vol. 17, NO. 2, April 2002.
- [5] Ivan W. Selesnick, "**Discrete Wavelet Transform of Approximation Order 2 with Improved Time-Localization-The Slantlet Transform**", Polytechnic University, Electrical Engineering, 6 Metrotech Center Brooklyn, NY 11201-3840.
- [6] Pratt W. K., Chen W., and Welch L. R., "**Slant Transform Image Coding**", IEEE Transactions on Communications, Vol. com-22, No. 8, 1974, pp.1075-1093,2005.
- [7] Priyam Chatterjee and Peyman Milanfar, "**Denoising using the K-SVD Method**", EE 264-Image Processing and Reconstruction, Spring 2007.
- [8] Gonzalo R. Arce, Jan Bacca, and José L. Paredes, "**The Essential Guide to Image Processing**", ISBN: 978-0-12-374457-9, Elsevier Inc., 2009.
- [9] Al-saleh, I.K.I, "**Image Denoising Using Wavelet Transform**". M.Sc. thesis, college of Eng., Univ. of Baghdad, June 2001.

Impact of Computer Applications in Construction Industry of Iraq

Dr. Hassan Issa Abdul-Kareem

Lecturer, Civil Engineering Department, Engineering Faculty, Mustansiriyah University

hassan.issa78@uomustansiriyah.edu.iq

Abstract:

The need for work development in construction industry raised where there are many activities in different project levels performed by numerous parties. The work development satisfied by using professional computer applications. This research aims to study the impact of these applications in Iraq construction industry. The positive impact represented in a number of information technology benefits have been adopted from a previous study to be tested in a number of construction institutes of Iraq through a questionnaire. The target respondents were the engineers and construction managers in construction companies and projects. About 150 questionnaire forms were distributed and 102 were received, but only 100 of them were completed. The method which have been used to analyses the data were descriptive Statistic (DS). The results of this study showed that the impact of computer applications illustrated in increasing and Improving Competitive Advantages, Work Flexibility, Work Relationships and Information Quality while it can Reduce Working Time.

Keywords: computer application; computer benefits; construction industry.

تأثير التطبيقات الحاسوبية على الصناعة الإنشائية في العراق

حسن عيسى عبد الكريم

المستخلص

إن الحاجة إلى تطوير العمل في صناعة البناء والتشييد برزت، إذ هناك العديد من الأنشطة في مختلف مستويات المشروع التي تؤدي بواسطة العديد من الأطراف. تطوير العمل يتحقق باستخدام تطبيقات الحاسوب المتخصصة. يهدف هذا البحث إلى دراسة تأثير هذه التطبيقات في صناعة البناء والتشييد في العراق. وقد تم اعتماد التأثير الإيجابي المتمثل في عدد من فوائد تكنولوجيا المعلومات التي تم تبنيها من دراسة سابقة ويتم اختبارها في عدد من مؤسسات البناء في العراق من خلال استبيان. وكان المستجيبون المستهدفون هم المهندسون ومديرو البناء في شركات البناء والمشاريع. وتم توزيع حوالي 150 استمارة استبيان واستلام 102 استمارة، ولكن لم يتم إكمال سوى 100 منها. وكانت الطريقة التي استخدمت لتحليل البيانات طريقة الإحصاء الوصفي. وأظهرت نتائج هذه الدراسة أن تأثير تطبيقات الحاسوب تتمثل في زيادة وتحسين المزايا التنافسية، مرونة العمل، علاقات العمل وجودة المعلومات في حين أن استخدام الحاسوب يمكن تقليل وقت العمل.

1- Introduction

The effect of computer applications presents the changes occurred in terms of the required work enhancements on the current situation. The management support is essential to realize computer applications effect on construction work. Management impact illustrated in a serial of activities in planning, training and review. This impact will have a long time impression presented in enhancing parties relationships, increasing work control, developing a connection bridges between suppliers and customers, activate electronic business [1]. Recognition the impact of computer applications varies between short time to long time depending on the type of application [2]. Also, it varies between tangible effect on productivity and intangible effect on performance [3].

This study conducted in a number of Iraqi construction industry institutes among many professional engineers and managers involved in user team of computer applications. The term impact translated as benefits where it considered the positive impact on the work. The benefits of computer applications represented in Information Technology benefits, so this study will adopt the observed benefits of IT in the previous studies.

2- Computer applications

Human-Computer interaction started since many decades and developed rapidly depending on the needs and to make the work in different industries and marketing more easy and accurate. Understanding the progress of Human-Computer interaction depends on assessing the potential for future visions and advances which could make the aspects of visions contributes in working prototype and evolution of design and applications. These visions and interaction between human and computer could be translated through a hardware engine which is more powerful than the expensive systems designed and used by the pioneers.

Construction companies spend a lot of money in business computers to maintain the main working interests. To justify these expenses, the management should focus on the benefits of these applications and its future output. Many applications in marketing and different industries sectors, especially construction industry, have been monitored and tested by previous studies such as [4]. The common construction industry applications are the basic usage of Microsoft office, integrated design (CAD/CAM), specialized software, integrated design, project planning and cost estimating [4]. Also, there is an application related to the wireless network [5] and hiding information by securing message allows covert transmission of information over an over the communications channel [6]. In addition to a new direct-connected intelligent home gateway between two different wireless communication technologies. At the same manner, the resources of a novel concept of Cloud computing are virtualized, dynamically extended and provided as a service on the Internet [7].

3- Impact of Computer applications

There are a number of references argued and investigated the positive impact (benefits) of computer applications in construction work such as [8] and [9] and so on. In this research, the benefits of information technology (the main representation of computer applications in construction industry) have been adopted from [10], [11] and [12] table 1 shows the description of these benefits and their clusters.

Table (1) Summary of Computer Applications Benefits in Construction Companies Grouped in Clusters [12]

Description of Benefits	Cluster of Benefits
Attaining client expectations. Improving client satisfaction. Improving focus on client requirements. Improving service.	Client Satisfaction
Reducing marketing costs. Reducing work transaction costs. Reducing operating costs. Reducing labor costs. Reducing staff requirements. Reducing training costs. Increasing ability to provide instant price quotations of procurements to clients. Improving finance transaction methods. Achieving greater integration with other work functions. Increasing profit margins. Strategic cost savings.	Cost Reduction
Providing better information to management. Improving data management data. Improving full life-cycle information management. Improving contract administration. Improving quality of decision-making in design and construction. Reducing project risk efficiently. Minimizing business risk. Reducing technology risks in design and construction. Enhanced inventory management.	Improving Management

Increasing the strategic competitive advantage. Keeping up with competitors.	Competitiveness Advantages
Increasing work operations efficiency. Reducing number of redundant tasks. Exchanging ideas and viewpoints among project team members. Improving process of developing project information. Increasing ability to handle complex projects. Increasing project value. Improving work productivity. Improving quality of output in management, design and construction. Achieving substantial reduction or elimination of rework. Improving planning process by simplifying updating process.	Improving Business Success Criteria
Improving ability to respond to changing conditions. Faster response to client enquiries. Faster response to project requirements and problems. Increasing responsiveness of senior management to business problems. Faster response to supplier quotations. Faster response in arranging urgent meetings for construction projects.	Increasing Response Rate
Increasing work flexibility. Improving organizational and process flexibility. Improving integration between different business functions.	Increasing Work Flexibility
Increasing market share. Achieving strategic intelligence of new markets. Realizing market leadership.	Increasing Market Share
Increasing quality of information. Reducing paperwork. Improving information availability. Increasing ability of exchanging data and information. Facilitating the process of getting meaningful information. Increasing ability to handle enquiries. Reducing storage requirements. Improving delivery scheduling of procurement. Reducing loss of project information. Improving recording process of staff skills. Improving external access to records of procurement. Improving communication between management stakeholders. Enabling data collaboration between parties in entire work without re-entry. Improving integration in design process. Improving ability of referring back to data. Reducing impact of mistakes. Getting more relevant and reliable data	Improving Information Quality
Improving growth and success. Providing space and capacity for business growth. Satisfying requirements for new technology. Promoting proactive culture.	Improving Organizational Growth
Improving teamwork. Improving ability to develop technical skills and select appropriate staff. Improving employee relations within office.	Improving Work Relationships
Reducing time required to collect construction tenders. Reduced time of preparing cost plans. Reducing overall procurement cycle time. Reducing invoicing time. Reducing lead times for design. Reducing project-planning time. Reducing project duration time. Increasing service delivery. Reducing communication time. Reducing time through greater transparency (fewer objections). Reducing work evaluation time	Reducing Working Time

4- Questionnaire survey

The benefits have been tested in a number of construction institutes in Iraq through a questionnaire. The target respondents were engineers and managers. About 150 questionnaire forms were distributed and 102 were received, but only 100 of them were completed. The method which have been used to analyses the data were descriptive Statistic (DS) to describe the characteristic of the sample and check the variables underlying the statistical techniques that used to address research questions [13].

5- Questionnaire results

The background information of the respondents is presented in Table 2. The most respondents were engineers (40%) and 31% managing directors. More than half of the respondents (55%) degree holders and about half of the respondents (49%) individuals with more than ten years of experience in construction.

Table (2) Background information of the respondents

Variable	Frequency (n=100)	Percentage (Total=100%)
Occupation		
Engineer	40	40
Managing Director	31	31
Project Manager	29	29
Education level		
Diploma	29	29
Bachelor	55	55
Post graduated	16	16
Experience		
<5	20	20
5 -10	31	31
>10	49	49

The results of benefits obtain according to Likert scale quantification, with 1.00=strongly disagree to 5.00=strongly agree. The considered agree-disagree levels are shown in Table 3.

Table (3) Considered Agree-Disagree Level Results from Likert Scale Quantification

Likert Scale	Agree Level
1.00 - 1.50	Strongly Disagree
1.51 - 2.50	Disagree
2.51 - 3.50	Neither Agree nor Disagree
3.51 - 4.50	Agree
4.51 - 5.00	Strongly Agree

From figure 1 which shows the mean values of benefits, the impact of computer applications illustrated in increasing and Improving Competitive Advantages, Work Flexibility, Information Quality and Work Relationships while it can Reduce Working Time where the means are (4.3, 4.3, 4.3, 4.1 and 4.3) respectively. The respondents didn't agree that using computers satisfy Client, Reduce Cost, Improve Management and Business Success Criteria. The means of these items were (2.5, 2.5, 2.4 and 2.09) respectively. On the other hand, the respondents neither agree nor disagree with Increasing and Improving Response Rate, Market Share and Organizational Growth where the means are (3.2, 3.2 and 3.1) respectively.

The comparison of these results with the findings of [10], [11] and [12], it is clear that the Malaysian industry recognized Improving in Management and in Business Success Criteria while it is not in Iraq. However, the benefits recognized in Malaysia are more than in Iraq where the works are big and the computer usage is wide.

6- Conclusion

The impact of using computer applications represented in increasing and Improving Competitive Advantages, Work Flexibility, Work Relationships and Information Quality while it can Reduce Working Time. While the other observed benefits as a positive impact in a number of construction industry institutes did not recognized by this study which conducted in Iraq. However, this modest impact could be justified by considering that the type and size of most projects in Iraq were small and limited national projects, so this could effect on the recognized tangible benefits and impact when the necessity and need for the technology are dwindling.

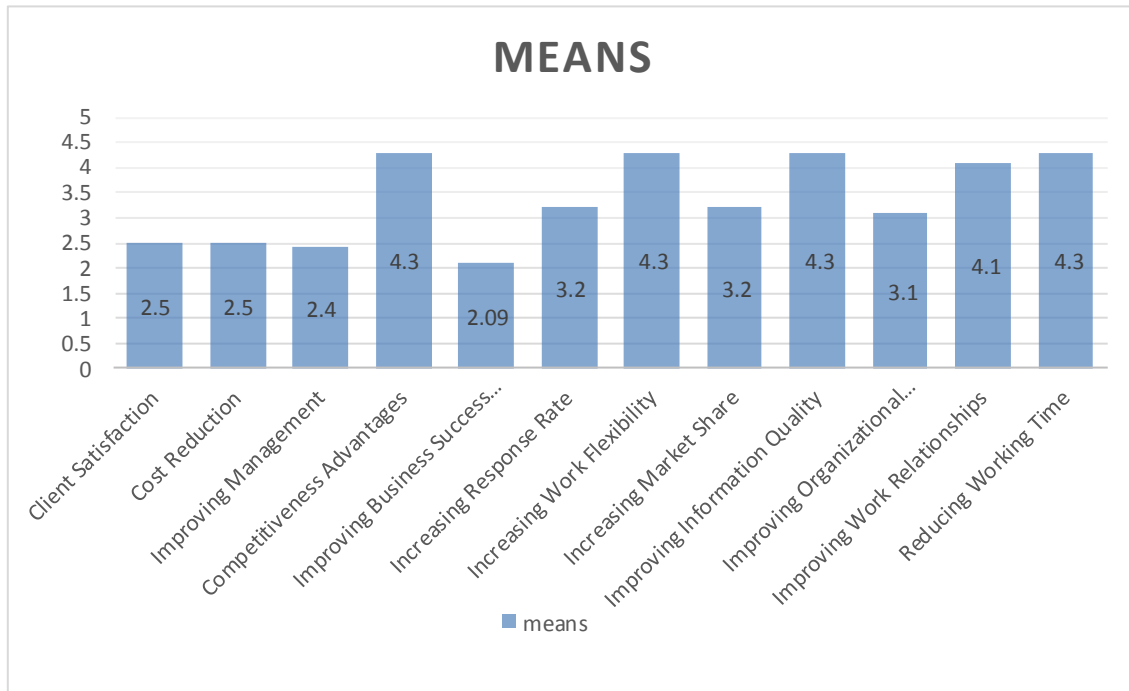


Fig. (1) The mean values of computer application benefits in Iraq

References

1. Lucas, H. C. Jr. (2000). *Information technology for management*, 7th edition. USA: McGraw-Hill Companies, Inc.
2. Peppard, J., Ward, J., & Daniel, E. (2007). Managing the Realization of Business Benefits from IT Investments. *MIS Quarterly Executive*, 6(1), 1-11.
3. Andresen, J., Baldwin, A., Betts, M., Carter, C., Hamilton, A., Stokes, E. & Thorpe, T. (2000). "A Framework for Measuring IT Innovation Benefits". *Journal of Information Technology in Construction (ITcon)*, 5, 57-72.
4. Yusuf, S., & Osman, O. (2008). "An evaluation of the use of Information Technology in the Malaysian construction industry". *proceeding of ICoPM*. University of Malaya, Kuala Lumpur, 710-718.
5. Tyagi, S.S. & Chauhan, R. K. (2010). "Performance Analysis of Proactive and Reactive Routing Protocols for Ad hoc Networks". *International Journal of Computer Applications*, 1 (14).
6. Kumar, A. & Pooja, Km. (2010). "Steganography- A Data Hiding Technique". *International Journal of Computer Applications*, 9 (7).
7. Omar, S., Mohammed, A. & Mohsine, E. (2012). "OpenStack: Toward an Open-source Solution for Cloud Computing". *International Journal of Computer Applications*, 55(3).
8. Love, P. E. D., Irani, Z., & Edwards, D. J. (2004). "Industry-centric benchmarking of information technology benefits, costs and risks for small-to-medium sized enterprises in construction". *Journal Automation in Construction*, 13(4), 507– 524.
9. Eadie, R., Perera, S., & Heaney, G. (2010). Identification of e-procurement drivers and barriers for UK construction organisations and ranking of these from the perspective of quantity surveyors, *ITcon*, 15, 23-43.
10. Abdul-kareem, H. I., Abu Bakar, A. H., & Abbas, M. (2009). "Perception of work problems and related roles of IT among selected professionals in construction in Malaysia". *International Journal of Management Perspectives (IJMP)*, 1(3), 72-92.
11. Abdul-kareem, H. I., & Abu Bakar, A. H. (2011). "Identifying IT benefits for Malaysian Construction Companies". *Journal of Information Technology in Construction (ITcon)*, 16, 477-492
12. Abdul-kareem, H. I. (2015). *A Process Framework for Managing IT Benefits in Construction Companies*. LAP LAMBERT OmniScriptum GmbH & Co. KG Saarbrücken, Deutschland/ Germany.
13. Pallant, J. (2001). *SPSS survival manual: a step by step guide to data analysis using SPSS for Windows, (Version 10)*. Buckingham: Open University Press.

An Efficient Data Reduction Technique for Image By Using Multiwavelet and Run Length Encoder

Elham Fadel Aqeel

Mustansiriyah University/ College of Education/ Computer Department

albeatyali9@gmail.com

Abstract:

Image compression techniques are consider to be effective tools to reduce transmission bandwidth and the transmission cost of the image information or storage memory requirements.

In this paper two image compression algorithms have been, the first one is multiwavelet method that is based on wavelet transform (WT) consider an effective tool, which represent an effective way in reducing lass important high wavelet. Second technique Run length encoding (RLC) consider also an effective tool. Finally, a new method (hybrid (HWT_RUN) is designed by coding technique low wavelet band with (HWT) and high wavelet with (RLC).Which on the best result showed that best the compression ratio (CR) with best quality (PSNR). This project executed by using mat lab language.

Keyword: Haar Wavelet Transform, Run-Length Encoding.

طريقة كفاءة لاختزال البيانات في الصورة الرقمية باستخدام متعدد التحويل المويجي وطريقة طول الترميز (RLC)
الهام فاضل عقيل

المستخلص

طريقة كفاءة لاختزال البيانات في الصورة الرقمية باستخدام متعدد التحويل المويجي وطريقة طول الترميز المطورة (RUN). تعتبر تقنيات ضغط الصورة كأداة فعالة لتقليل عرض حزمة الارسال او كلفة الخزن في الذاكرة.

في هذا البحث تم اعتماد تقنيتين لضغط الصور. اولا تقنية متعدد التحويل المويجي (IWT) التي تعتمد على التحويل المويجي (WT) التي تعتبر طريقة فعالة لتشفير العناصر ذات الترددات العالية الناتجة من تطبيق التحويل المويجي على الصورة. والثانية خوارزمية تشفير الترميز (RLC) التي تعتبر ايضا من الطرق الفعالة، واخيرا تم تصميم خوارزمية الهجينة (Hybrid) اذ يتم تشفير العناصر ذات التردد العالي باستخدام (IWT) والعناصر ذات التردد الواطئ بطريقة خوارزمية (RLC) للصورة. وبينت النتائج افضل نسبة ضغط (CR) مع الاحتفاظ بكفاءة الصورة. من تطبيق الطريقة الهجينة مع جودة عالية. تم تصميم هذا البحث بلغة ماتلاب.

الكلمات المفتاحية: ضغط الصورة، التحويل المويجي

1-Introduction

Data Compression is the branch of data reduction science of representing information in a compact form. It is used to reduce the number of bits required to represent an image or a video sequence. A Compression algorithm takes an input X and generates compressed information that requires fewer bits. The Decompression algorithm operates on the compressed information to generate the reconstruction Y. Based on the reconstruction Y, the compression algorithms are broadly classified into two categories, namely Lossy and Lossless compression Algorithms [1].

2- Compression Techniques

2.1 Lossless compression

These techniques, involve no loss of information. The Original information can be recovered exactly from the compressed data. It is used for applications that cannot tolerate any difference between the original and the reconstructed data.

2.2 Lossy compression

It involves some loss of information. The data that have been compressed using lossy techniques generally cannot be recovered or reconstructed exactly. It results in higher compression ratios at the expense of distortion in reconstruction. Compression Techniques can be applied directly toward the images or to the transformed image information (transformed domain). The Transform techniques are well suited for image compression. Here the image is decomposed or transformed into components that are then coded according to the individual characteristics. The transform should possess high-level compaction property, so as to achieve high compression ratios. The Performance of a Compression method can be evaluated in a number of ways: the relative complexity of the technique, Memory requirement for implementation, Speed of the Technique on a machine, the amount of compression, and the distortion rate in the reconstructed image.

Compression Ratio (CR): It is the ratio of the number of bits required to represent the image before compression to the number of bits required to represent the image after compression.

Data Rate: it is defined as the average number of bits required to represent a single sample. It is specified in term of bits per pixel (Bpp).

Distortion: the difference between the original and reconstructed image is called as distortion. It is denoted using

Mean Square Error (MSE) in db.

$$MSE = 10 \log_{10} \left[\frac{1}{N \times N} \sum_{i=0}^{N \times N} (X_i - Y_i)^2 \right] \dots (1)$$

3- Discrete Wavelet Transforms (DWT)

An image signal can be analyzed by passing it through an analysis filter bank followed by a decimation operation. This analysis filter bank, which consists of a low pass and a high pass filter at each decomposition stage, is commonly used in image compression [2]. When a signal passes through these filters, it is split into two bands. The low pass filter, which corresponds to an averaging operation, extracts the coarse information of the signal. The high pass filter, which corresponds to a differencing operation, extracts the detail information of the signal. The output of the filtering operation is then decimated by two. A two dimensional transform can be accomplished by performing two separate one-dimensional transforms. First, the image is filtering along the x dimension and decimated by two. Then, it is followed by filtering the sub-image along the y-dimension and decimated by two. Finally, we have split the image into four bands denoted by LL, LH, HL and HH after one – level decomposition. Further decomposition can be achieved by acting upon the LL subband successively and the resultant Image is split into multiple bands as shown in figure (1).

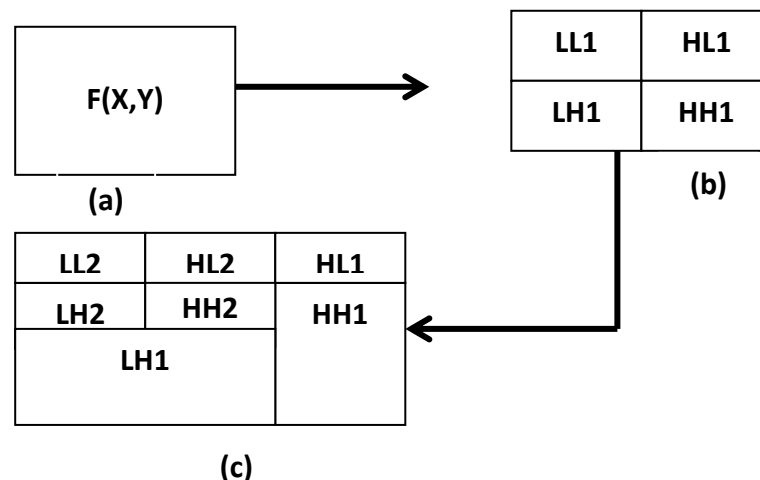


Fig. (1): Two Dimension Discrete Wavelet Transform

In mathematical term [3], the average operation or low pass filtering is the inner product between the signal and the scaling function (ϕ) as shown in eq. (2) below. Whereas the differencing operation or high pass filtering is the inner product between the signal and the wavelet function (ψ) as shown in eq. (3) below [4].

Average coefficients,

$$C_j(K) = \langle f(t), \phi_{j,k}(t) \rangle = \int f(t) \phi_{j,k}(t) dt \dots \dots \dots (2)$$

Detail coefficients,

$$d_j(k) = \langle f(t), \psi_{j,k}(t) \rangle = \int f(t) \psi_{j,k}(t) dt \dots (3)$$

The scaling function or the low pass filter is defined as

$$\phi_{j,k}(t) = 2^{j/2} \phi(2^j t - k) \dots (4)$$

The wavelet function or the high filter is defined as

$$\psi_{j,k}(t) = 2^{j/2} \psi(2^j t - k) \dots (5)$$

Where, j : denotes the scaling index.

K : denotes the translation index.

3-1 Haar wavelet Transform

The Haar wavelet is the simplest wavelet. The Haar transform consists of taking average and difference. Consider two number a and b , neighboring samples of a sequence, a and b have some correlation (hopefully) of which we'd like to take advantage. Simple linear transform can be used to replace a and b by their average and difference d [5].

$$S = (a+b)/2 \quad d = (a-b)/2$$

The aim is to reduce the number of bits required for d , which will be the case if a and b are highly correlated. This computation can be reversed to recover a and b :

$$a = s + d \quad b = s - d$$

This is the idea behind the Haar wavelet. Now consider the following discrete- time signal.

(64 2 3 61 60 6 7 57)

For the first step, the average can be taken of each pair of components in the original string and place the results in the first four positions of our new sting. the remaining four numbers are the differences of the first element in each pair and its corresponding average.

Therefore, the result of the first step contains four averages and four detail coefficients it is shown below.

(33 32 33 32 31 -29 27 -25)

Then if the same method apply to the first four components of our new sting resulting in two new averages and their corresponding detail coefficients. The remaining four detail coefficients are simply carried directly down our previous step, and the result for step tow is as follows.

[32.5 32.5 0.5 0.5 31 -29 27 -25]

Performing the same average and differencing to the remaining pair of averages completes step there.

The results of applying the wavelets transform is a set of coefficients of which most have very small amplitudes and only few have significant values. In order to get compressions, map the set of wavelet transform coefficients to a new set of discrete values. This process of mapping from a continuous set of real values to a set of discrete values is called quantization [6].

4-Run length encoding (RLC)

Run length encoding (RLC) is perhaps the simplest compression technique in common use. RLE algorithms are lossless, and work by searching for runs of bits, bytes, or pixel of the same value, and encoding the length and value of the run. As such, RLE achieves best results with images containing large areas of contiguous color, and especially monochrome images. Complex color images, such as photographs, do not compress well – in some cases, RLE can actually increase the file size. There is a number of RLE variants in common use, which are encountered in the TIFF,

PCX and BMP graphics formats [7]. Run-length encoding represents a string by replacing each subsequence of consecutive identical characters with (char, length). The string 11112222333111 would have representation (1,4) (2,4) (3,3) (1,3). Then compress each (char, length) as a unit using say, human coding. Clearly, this technique works best when the characters repeat often. one such situation is in fax transmission, which contains alternating long sequences of 1s and 0 s. the distribution of code words is taken over many documents to compute the optimal human code. [8].

5- Algorithm of proposed system

In this section, we introduce a new algorithm to compression based of two techniques, one is Haar method and second is Run Length coding (RLC).

5-1 Proposed Haar Wavelet

Here we use Haar wavelet transform, and block edge coding (BEC) techniques. coding process is performed as follows:-

5-1-1 Algorithm of the coding and decoding Haar Wavelet stages

1- input image (Img)

2- perform WT (2-level) for original image (get 7-subimages) see Figure (3), get transform image (I)

3- Round integer the values of sub –image (1), and store it with (8-bits per element).

4- Put threshold values (5, 10,..., 25) to discard high pass coefficients (in order to determine exits edge or not).

5- Block edges code (BCE) that is used to code sub –image

Coefficients (2-6), this is performed as follows:-

i- Divide the sub-image into non-overlapping blocks

ii- Detrrmine, if the block contain edges or not through use threshold value (above threshold value consider edge other not edge).

iii-If it does not contain edges then store code (zero) and move to the next block.

- Else for each point in block save two values:

One to save the position of the (x,y), and the second value to represent the quantization value of this edge by using:

$$q(r,c) = (ql * (I(r,c) + K)) / 255$$

Where

$I(r,c)$ = Ttransform image (sub-image coefficient (2-6))

ql = maximum quantization value.

K = constant and in this work we take

K=128.)

6- Ignoring transform coefficients in sub_image (7).

While the decoding process performed, by using the following steps:

1- Read first part from coded data file to reconstruct the low frequency band.

2- Perform inverse the block edge code to reconstruct the high frequency band as follows:-

a- Read code, if (code=0) then full the block (8*8) by zeros.

b- If (code = 0) then

- L = code (represent the location of the edge point in the block (i.e. (x,y))

- Read next value (i.e. g(x,y))

- Dequantization the g (x,y) using:

$$I(x,y) = (255 * (g(x,y)_k)) / ql$$

3- Put Zeros in sub-image (7).

4- Apply the inverse WT (IWT) to reconstruct the image again.

1	2
3	4

1	2	5
3	4	
6		7

(a) One level DWT (b) Two level DWT

Fig. (2): Two – level Haar Wavelet transform

Compression ratio (CR) is the ratio between the sizes of compressed data to the size of uncompressed data.

CR = size of Compressed Data / size of uncompressed data

5-2 Steps Run Length Coding (RLC) algorithms:-

5-2-1 Proposed Run Length Coding.

- 1- Read the image.
- 2- Get the height N and the width M for the image
- 3- Create an array, let it M ain (N,M),
- 4- Convert the image to the main array, M ain (N,M)
- 5- Let X = M ain (0, 0), M ain (0,0) is the first element in an array. let th = 10, th: the threshold,
- 6- For th = 10, TH: the threshold
- 7- For I = 0 to n-1
- 8- For j = 0 to m-1
- 9- If X-main (I,j) <= TH then
Let C = C+1
- Else
Let X = Main (I,J) and C =0
- 10- end

5-3 Hybrid Haar Wavelet Transform (HWT_ RLC) Coding Technique

The coding steps are as the following:-

- 1- Take the original image
- 2- To get in matrix from of images is read using "imread" command.
- 3- Haar Wavelet Transform applied to the matrices.
- 4- Hard thresholding is adopted on the output.
- 5- Run Length Coding is applied.
- 6- Compression ratio is calculated.

Here for the input haar wavelet transform is applied. The transform image will be in two halves containing the approximated data and the detail coefficients. Hard thresholding is applied to the transformed image. Hard Thresholding is used for high degree of compression. Here threshold values say is set. Then the detail coefficient in the transformed data whose magnitude is less then equal to € is set to zero, this will increase the number of zeros in the transformed matrix. Thus the level of compression is increase. After thresholding the values are encoding by using entropy coding. One such entropy coding is RUN Length Encoding (RLE). First the value are converted into single dimensional array. Lastly compression ratio is calculated between output RLE and original image.

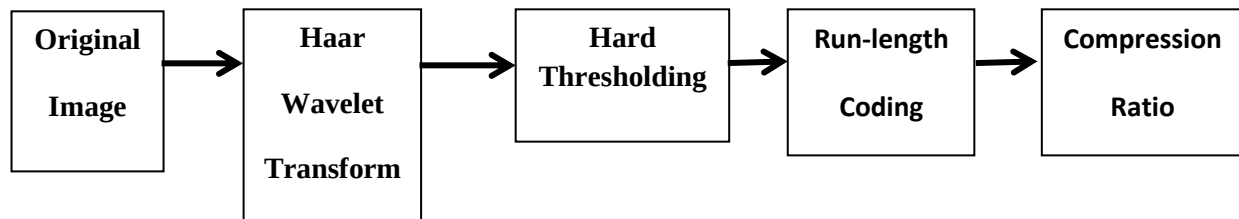


Fig. (3): Proposed Model Block Diagram

6-Results and Discussion

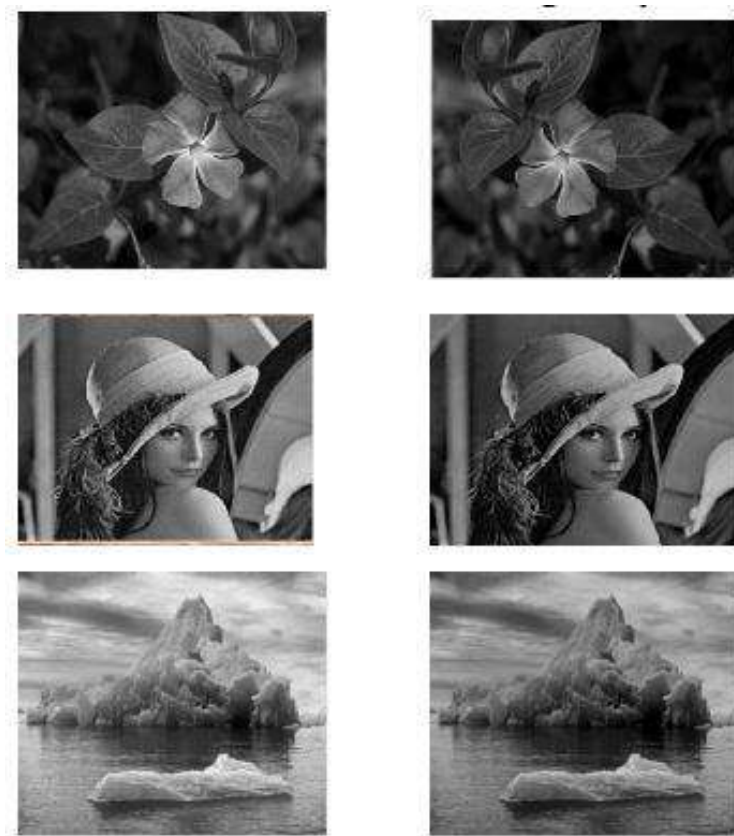
In this section, we shall discuss the results obtain by implanting the Haar wavelet, Run Length coding and hybrid Haar wavelet transform (HWT) Run Length coding (RLC). Techniques, to get high compression ratio image (Lana). Figure (3, 4, 5) shows the image used in this study.

6-1 Results of Haar Wavelet Transform

Table (1) illustrates the results of coding performance, and utilizing block (8*8). As it is clear.

Table (1) Results Haar wavelets transform

Test image	Size image	Threshold	Block size	PSNR	Compression ratio
Lena	256*256	5	8*8	35.252	3.3
		10	8*8	31.71	5.7
		25	8*8	26.78	12.5
Rose	256*256	5	8*8	34.10	4.3
		10	8*8	31.52	8.2
		25	8*8	28.60	13.7



Original Image

Compression Image by Haar wavelet transforms (HWT)

6-2 Results of Run Length Coding

Table (2) illustrates the results of coding Run Length Coding performance.

Table (2) Results Run Length Coding

Test image	Original Size	Threshold Value	New size (KB) Using RLC	Compression ratio
Lena	170	10	31	5.48:1
Rose	127	10	62	3.6:1
Ice	226	10	211	3.55:1



Original Image

Compression Image by Haar wavelet Transform (HWT) & Run-length coding

6-3 Hybrid Haar Wavelet Transform (HWT) and Length Coding (RLC)

Table (1) illustrates the results of coding performance, and utilizing block (8*8). As it is clear.

Table (3) Results of Hybrid (HWT-RLC)

Test image	Size image	Block size	Threshold Value	PSNR	Compression ratio
Lenna	256*256	8*8	10	39%	49%
Rose	256*256	8*8	10	49%	32%
Ice	256*256	8*8	10	32%	34%

7- Conclusion

Here we compress image by using HWT and RLC. Both compression methods used here are simple, computationally less complex and also more efficient in aspect of time performance. And it presents quality measurement of the image which is compressed. in further research, the trade –off between threshold ϵ values and quality of image will be studied. The performance can be further improved by using other wavelet transform such as orthogonal wavelet.

References

- [1] K. Rajakakumar and T.Arivoli, " **IMWT Coding using Lossy Image compression Techniques for Satellite Images**", ARPJ Journal of Engineering and Applied Sciences, VOL 10,no 9, May 2015.
- [2] Sheila Horan, " **Data Compression Statistic and Implication** ",New Mexico State University, 2000.
- [3] Choo Li Tan, " **Still Image Compression Using Wavelet Transform**", Thesis, The University of Queensland 's School of Information Technology and Electrical Engineering, 2001.
- [4] Panrong Xiao, " **Image Compression by Wavelet Transform**", MSC. Thesis, East Tennessee state University, Department of Computer and Information Sciences, 2001.
- [5] K. N. Ngan, K.S. Leong and H. Singh, " **Adaptive cosine transform coding of image in perceptual domain** ", IEEE Trans. On Assp, vol.37, no.11, November 1989.
- [6] Jessica, F. (12 February 2002), " **Algorithms for Massive Data Sets Context-based Compression**", CS493, 1:1-3, www.docstoc.com/docs/54164044/Run-Lengh-ncoding.
- [7] Andrew B. Watson, " **Image Compression Using the Discrete Cosine Transform**", Mathematica Journal, 4(1), 1994, p. 81-88.
- [8] Radomir S. Stankovi, Bogdan J. Falkowski, " **The Haar wavelet transform: its status and achievements**" Computers and Electrical Engineering 29 (2003) 25-44.

Image Dehazing using modified fast visibility restoration with HSV color space

Hazim G. Daway¹ Hana H. Kreem² Haitham S. Chyed³ Dhuha A. Abdulabbas¹

¹Department of physics/ College of Science/ Mustansiriyah University

²Department of physics/ College of Education/ Mustansiriyah University

³Department of computer/ College of Education/ Mustansiriyah University

Abstract:

The research aims to dehazing image using Modified Fast Visibility Restoration (MFVR) algorithm developed based on the transform HSV and sigmoid function taking into consideration Histogram Equalization (HE) and Multi Scale Retinex with Color Restoration (MSRCR) algorithm to show the efficiency of this algorithm was compared with the algorithms Single Image Haze-removed (SIH), FVR and MSRCR, the results showed the proposed method efficiency good improvement.

Keywords: image enhancement visibility restoration, sigmoid function.

1. Introduction:

The atmosphere reacts to light due to the composition of the atmosphere under stable conditions, contains a variety of different molecules and small suspended particles called aerosols [1]. One of the common problems is an Aerial Imaging degraded by these particles. Aerosols are extremely fine solids or liquids particles suspended in the atmosphere with very low fall speed. Their size generally lies between 10–2 and 100 μm . Furthermore, fog, haze, dust, smoke, drizzle, rain and snow are examples of aerosols[2]. The light reflected from the object and ambient light in the medium, referred to as the airlight [3]. Which, should have propagated in straight lines is actually scattered and replaced by previously scattered light. As a result, this airlight are absorbed and scattered by Aerosols in the medium before reaches the camera [3]. This interaction produces a wide variety due to particulate matter may significantly attenuate the transmitted signal (visibility) [4]. Visibility characterizes the transparency of the atmosphere as estimated by a human observer. It is measured by the runway visual range (RVR) [2]. When the scene has a poor visibility condition this limit the range and effectiveness of imaging systems because of image lose contrast and color fidelity. Image enhancement operations such as Retinex algorithm [5] and histogram equalization [6] is significant to provide better interpretability or perception of information in images for viewers, or to improve the input for other image processing techniques. In this paper, a novel enhancement approach, associates modified Fast Visibility Restoration method with sigmoid function is used for improving the quality of Aerial poor images.

2. Image Enhancement Operations

A. Single image haze removal algorithm

It depends on dark channel prior algorithm as follow [7]:

- Input color image c_i , $i=1,2,3$ (red,green,blue), with size $h*w$, window size=15.
- Compute the dark channel prior:

$$J^{\text{dark}}(x) = \min_{c \in \{r,g,b\}} (\min_{y \in \Omega(x)} (J^c(y))) \quad \dots\dots\dots (1)$$

$J^{\text{dark}}(x)$: the dark channel of J .

J^c : is a color channel of J .

$\Omega(x)$: is a local patch centered at X .

- Compute (estimating) the transmission map:

$$t(x) = 1 - \omega \cdot \min_c (\min_{y \in \Omega(x)} \left(\frac{I^c(y)}{A^c} \right)) \quad \dots\dots\dots (2)$$

$w = 0.95$, $A^c = 160/255$

d. Conducted soft matting to refine transmission map by $t(x)$, they minimize the following cost function:

$$E(x) = t^T L t + \lambda (t - \tilde{t})^T (t - \tilde{t}) \quad \dots\dots\dots (3)$$

L = is the matting laplacian matrix by levin.

λ : regularization parameter.

e. the (i,j) element of matrix L is defined as:

$$\sum_k \mathbb{1}_{(i,j) \in w_k} (\delta_{ij} - \frac{1}{|w_k|} (1 + (I_i - \mu_k)^T (\sum_k + \frac{\varepsilon}{|w_k|} U_3)^{-1} (I_i - \mu_k))) \quad \dots\dots\dots (4)$$

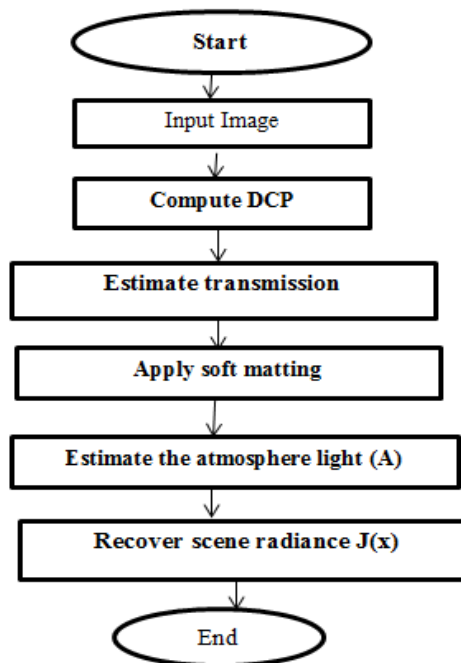
The optimal t can be obtained by solving the following sparse linear system:

$$(L + \lambda U)t = \lambda \tilde{t} \quad \dots\dots\dots (5)$$

f. compute recovering the scene radiance by:

$$J(x) = \frac{I(x) - A}{\max(t(x), t_s)} + A \quad \dots\dots\dots (6)$$

$t_s = 0.1$



B. Fig.(1): shown Block diagram of SIH Algorithm

C. Multi scale retinex with color restoration algorithm

The multi scale retinex (MSR) is explained from single-scale retinex (SSR) we have [8, 9]:

$$R_i(x, y, c) = \log[I_i(x, y)] - \log[F(x, y, c) \otimes I_i(x, y)] \quad \dots\dots\dots (7)$$

Where $R_i(x, y, c)$ the output of channel i ($i \in R, G, B$) at position x, y, c is the Gaussian shaped surrounding space constant, $I_i(x, y)$ is the image value for channel i and symbol $\otimes$ denoted convolution. $F(x, y, c)$ Gaussian surrounds function that is calculated by [8]:

$$F(x, y, c) = (k) \exp\left(\frac{-(x^2 - y^2)}{c^2}\right) \quad \dots\dots\dots (8)$$

k is determined by [9]:

$$\iint F(x, y, c) dx dy = 1 \quad \dots\dots\dots (9)$$

The MSR output is then simply a weighted sum of the outputs of several different SSR output where:

$$R_{MSR}(x, y, w, c) = \sum_{n=1}^N W_n R_i(x, y, c_n) \quad \dots\dots\dots (10)$$

Where, N is the number of scales, $R_i(x, y, c_n)$ the i 'th component of the n 'th scale, $R_{MSR}(x, y, W, c)$ the i 'th spectral component of the MSR output and W_n the weight associated with the n 'th scale. And we insist that $(\sum W_n = 1)$. The result of the above processing will have both negative and positive RGB values, and the histogram will typically have large tails. Thus a final gain-offset is applied as mentioned in [9] and discussed in more detail below. This processing can cause image colors to go towards gray, and thus an additional processing step is proposed in [8]:

$$R' = R_{MSR} \cdot I_i'(x, y, c) \quad \dots\dots\dots (11)$$

Where I' given by

$$I_i'(x, y, a) = \log\left[1 + a \frac{I_i(x, y)}{\sum_{i=1}^3 I_i(x, y)}\right] \quad \dots\dots\dots (12)$$

Where we have taken the liberty to use $\log(1+x)$ in place of $\log(x)$ to ensure a positive result. In [9] a value of 125 is suggested for (a) second. And the final step is gain-offset by 0.35 and 056 respectively [10]. In this work we used $(w_1=w_2=w_3=1/3)$ and $(c_1=250, c_2=120, c_3=80)$ [9]. This algorithm done by using following steps:

a. Input color image $I_i(x, y)$, $i = r, g, b$.

b. Calculate Gaussian surrounds function:

$$F(x, y, c_n) = (k) \exp\left(\frac{-(x^2 - y^2)}{c_n^2}\right)$$

c. Where k is normalization constant, c_n , $n=3$, $\{c_1=250, c_2=120, c_3=80\}$.

d. Compute SSR from; $R_i(x, y, c) = \log[I_i(x, y)] - \log[F(x, y, c_n) \otimes I_i(x, y)]$

e. Compute MSR from $R_{MSR}(x, y, w, c) = \sum_{n=1}^N W_n R_i(x, y, c_n)$

Where, $N=3$, $\{w_1=w_2=w_3=1/3\}$.

f. Calculate MSR with color restoration by:

$$I_i'(x, y, a, b) = b \log\left[1 + a \frac{I_i(x, y)}{\sum_{i=1}^3 I_i(x, y)}\right]$$

Where, $b=100$, $a=125$.

g. Output image is gotten form gain offset by;

$$I_{pi}(x, y) = 0.35(I_i'(x, y, a, b) + 0.56)$$

D. Fast Visibility Restoration Algorithm

A fast visibility restoration algorithm [11, 12] used to remove hazy from the image. The color image c_i , $i=1,2,3$ (red, green, blue), with size $h \times w$, window size $SV = 11$, percentage of restoration $p = 0.95$ and $g f = 1.3$. Compute the white balance given by:

$$C_{wi} = \frac{c_i}{c_{ti}} \quad \dots\dots\dots (13)$$

Where

$$C_{ti} = \frac{c_{mti}}{c_{mtm}} \quad \dots\dots\dots (14)$$

Also

$$C_{mti} = \left(\frac{c_{mi}}{c_{mm}} \right) \quad \dots\dots\dots (15)$$

and

$$C_{mtm} = \frac{c_{mt1} + c_{mt2} + c_{mts}}{3} \quad \dots\dots\dots (16)$$

$$C_{mm} = \frac{c_{m1} + c_{m2} + c_{m3}}{3} \quad \dots\dots\dots (17)$$

And c_{mi} is the median filter for three component r,g,b. Compute photometric bound by using:

$$pb = \min(C_{w1}, C_{w2}, C_{w3}) \quad \dots\dots\dots (18)$$

Compute the saturation bound by:

- i. Finding median filter for photometric bound window size SV to get pb_{md} .
- ii. Finding the absolute difference between pb and pb_{md} .

$$gd = \text{abs}(pb - pb_{md}) \quad \dots\dots\dots (19)$$

Then, Compute the median filter for gd using by window size SV to get pb_{md} . The saturation bound by finding the absolute difference between gd and gd_{md}

$$sb = \text{abs}(gd - gd_{md}) \quad \dots\dots\dots (20)$$

Finding the inferred atmospheric veil by:

$$v = p * \max(\min(pb, sb)) \quad \dots\dots\dots (21)$$

After that, compute the Restoration by using inverse koschmieder law:

$$ft = \frac{1}{(1-v)} \quad \dots\dots\dots (22)$$

For Restore original light colors by:

$$r_{ti} = r_i * c_{ti} \quad \dots\dots\dots (23)$$

Where

$$r_i = (c_{wi} - v) * ft \quad \dots\dots\dots (24)$$

To get gamma correction by:

$$i. lo = \ln(pbo(n, m) + \frac{1}{510}) \quad \dots\dots\dots (25)$$

Where

$$pbo = \text{mean}(c_{w1}, c_{w2}, c_{w3}) \quad \dots\dots\dots (26)$$

$$ii.l_r = \ln(r_m(n, m) + \frac{1}{510}) \quad \dots\dots\dots (27)$$

Where $\left(\frac{2}{3}\right)h \leq n \leq h$, $1 \leq m \leq w$

$$r_m = \frac{r_1 + r_2 + r_3}{3} \quad \dots\dots\dots (28)$$

iii. Finding:

$$ui = rti^{powe} * \exp (mo - mr * powe) \quad \dots\dots\dots (29)$$

$$mo = \text{mean} (lo) , \quad mr = \text{mean} (lr)$$

$$so = \text{std} (lo) , \quad sr = \text{std} (lr)$$

And

$$Powe = gf * \frac{so}{sr} \quad \dots\dots\dots (30)$$

Finally, the restoration image given by:

$$crsi = \frac{ui}{1 + \left(1 - \frac{1}{umi}\right)ui} \quad \dots\dots\dots (31)$$

$$umi = \max(ui)$$

E. Modified fast visibility restoration algorithm

This novel modified approach bases on an algorithm (FVR). In this algorithm is transforming color image from basic RGB color space to HSV color space, the forward transform is given by equation:

$$V = \max\{R, G, B\} \quad \dots\dots\dots (32)$$

$$S = \frac{\max - \min}{\max} \quad \dots\dots\dots (33)$$

$$H = \begin{cases} \frac{G-B}{6(\max - \min)} \\ \frac{1}{6} \left(2 + \frac{B-R}{\max - \min}\right) \\ \frac{1}{6} \left(4 + \frac{R-G}{\max - \min}\right) \end{cases} \quad \dots\dots\dots (34)$$

Where $\max = \max\{R, G, B\}$ and $\min = \min\{R, G, B\}$. All three components V , S , and H are in the range $[0, 1]$

And using sigmoid function as illustrate in figure 2 below:

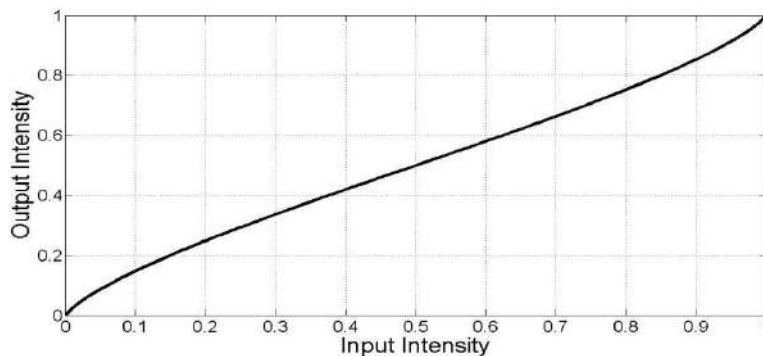


Fig. (2): sigmoid function

The advantage of this method gives restore additional data in color and non-color components. in the non-color components (lightness). Increasing sigmoid function:

$$y = \frac{1}{(1 + \left[\frac{(1-a)(1-I)}{aI} \right]^b)} \quad \dots (35)$$

By improving lightness, especially after applied histogram equalization (HE), and to keep lightness information. Then we take average after applied FVR on the color components unchanged. Then we combine those components and apply the reverse transform from HSV back to RGB is given by [13]:

$$[R, G, B] = [V, V, V] \quad \text{if } S = 0 \quad \dots (36)$$

If the saturation is not zero, then the RGB components are given:

$$[R, G, B] = \begin{cases} [V, K, M] & \text{if } 0 \leq H < 1/6 \\ [N, V, M] & \text{if } 1/6 \leq H < 2/6 \\ [M, V, K] & \text{if } 2/6 \leq H < 3/6 \\ [M, N, V] & \text{if } 3/6 \leq H < 4/6 \\ [K, M, V] & \text{if } 4/6 \leq H < 5/6 \\ [V, M, N] & \text{if } 5/6 \leq H < 1 \end{cases} \quad \dots (37)$$

Where M , N , and K are defined as:

$$M = V(1 - S) \quad \dots (38)$$

$$N = V(1 - SF) \quad \dots (39)$$

$$K = V(1 - S(1 - F)) \quad \dots (40)$$

And

$$F = 6H - V \quad \dots (41)$$

To get Image restored as in the following scheme:

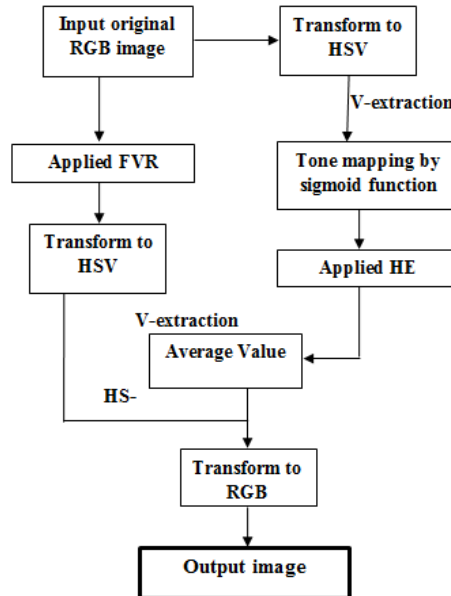


Fig. (3): Block diagram of MFVR

This done by the following steps:

- Input color image $C(x,y,i)$, $i=1,2,3$ (red,green, blue) components, and Applied FVR on image C to get C_{FVR} .
- Transform color image C_{FVR} from RGB color space to HSV and estimation V_{FVR} component and HS_{FVR} components.
- Go to step 1 and transform C from RGB color space to HSV and estimation V component.

- d. Transform lightness component by using sigmoid function getting V_s .
- e. Apply HE on V_s to get V_{SHE} then Computing average component V_{ave} for (V_{SHE}, V_{FVR}) .
- f. Collection component V_{ave} and HS_{FVR} and then applied inverse transformation to basic RGB color space to getting output image.

g.

3. Results and Discussion:

Four methods have been implemented and tested (SIH,MSRCR,FVR and the proposed approach MFVR)simulation experiment have been conducted on popular test figures(4,5,6 and 7) with type Jpg,and size 600×400 pixels.by using Matlap software program and simulate the proposed method which based on sigmoid function and association of different method together we get some result which help as to find the advantages of these methods and techniques on poor visibility aerial images.

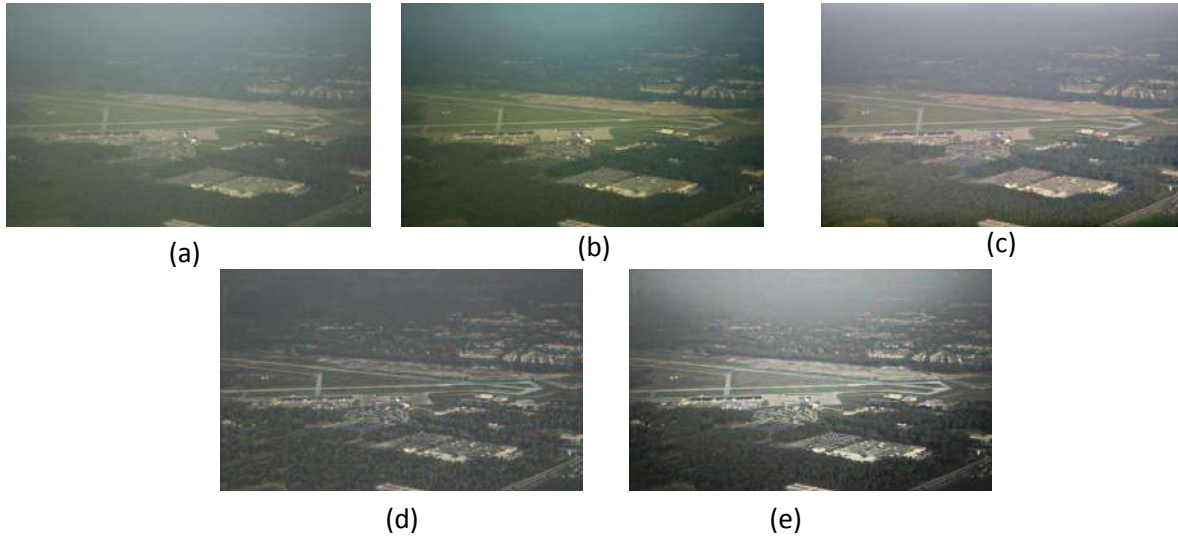


Fig.(4):from left to right ; (a) the original image, (b) the SIH image, (c) the MSRCR image, (d) the FVR image (e) the MFVR image.

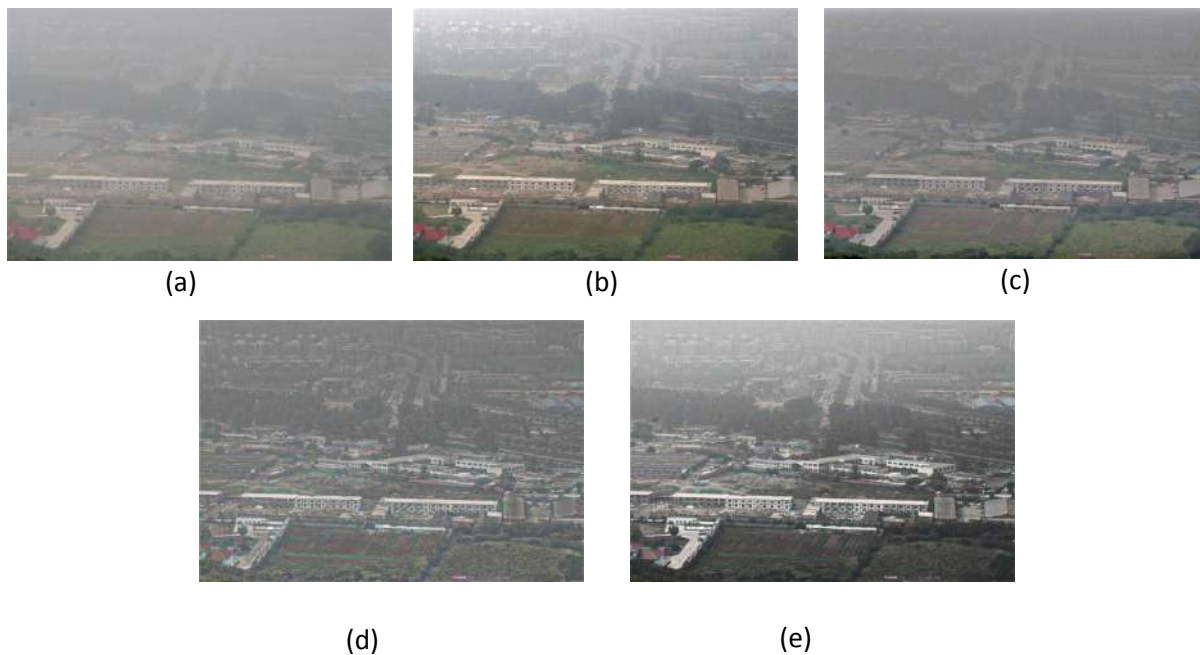


Fig.(5): From left to right; (a) the original image, (b) the SIH image, (c) the MSRCR image, (d) the FVR image,(e) the MFVR image.

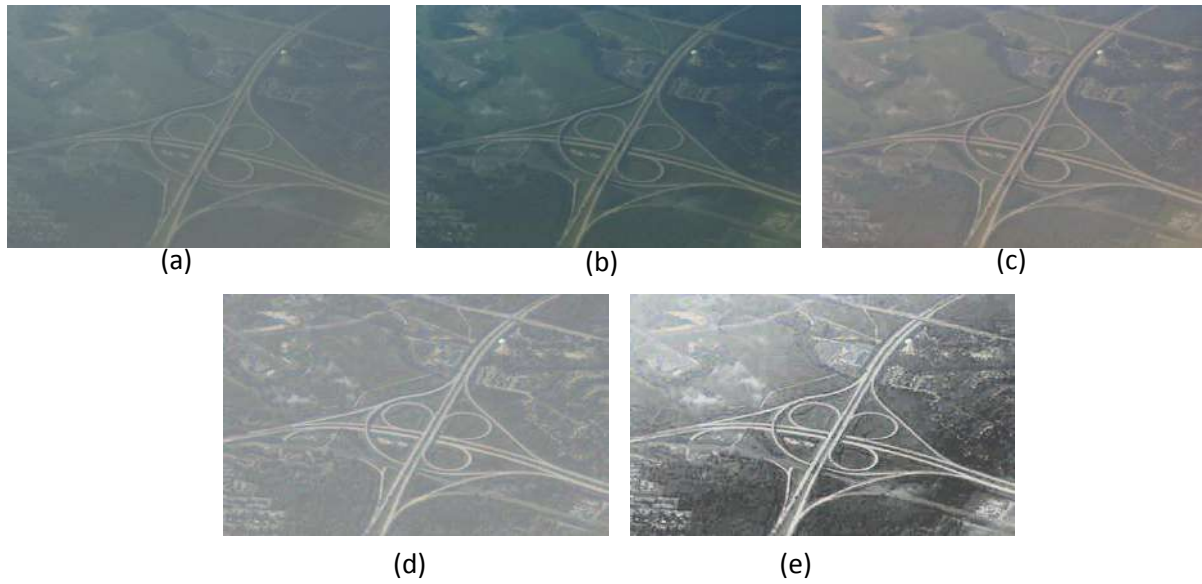


Fig. (6): From left to right; (a) the original image, (b) the SIH image, (c) the MSRCR image, (d) the FVR images (e) the MFVR image.

The figures (4, 5, 6 and 7) illustrated the restoration image for groups (b,c,d and e) from these figures the best algorithm is MFVR because the enhances lightness and contrast, and follows SIH and follows MSRCR but the negative of the MSRCR algorithm is halo effect. Furthermore, from the images restoration by using FVR, the lightness enhancement is not good due to low distribution of lightness, finally from these result it is clear that the proposed method yields the best appearance.

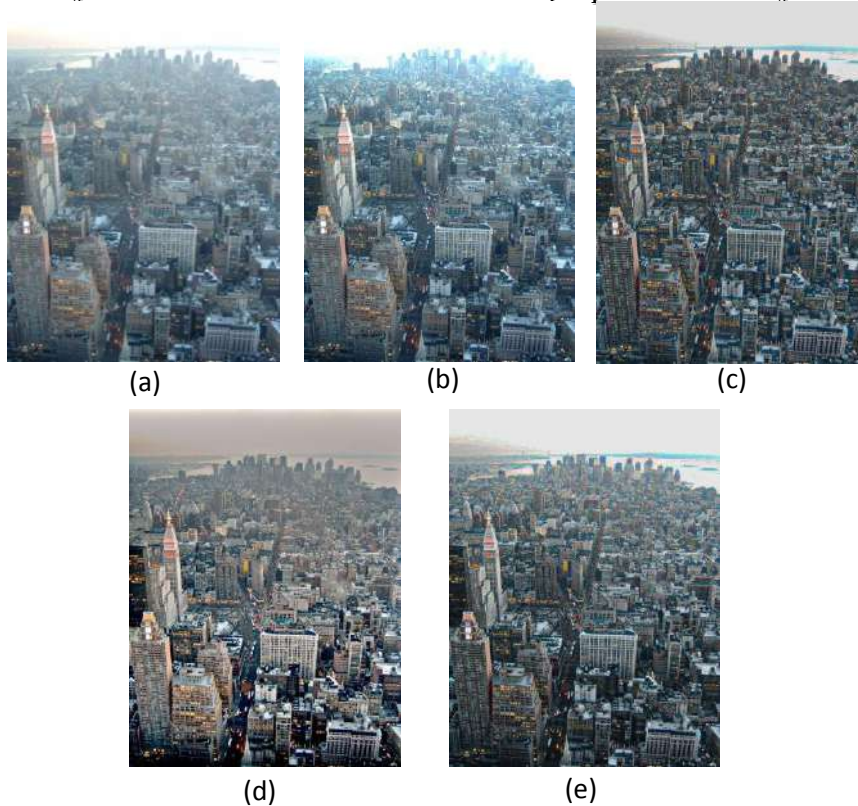


Fig. (7): From left to right; (a) the original image, (b) the SIH image, (c) the MSRCR image, (d) the FVR images (e) the MFVR image.

Thus, this novel technique used as an effective contributory in the environmental studie.in addition to it improve the images taken by the airplanes under different atmospheric conditions; it can improve the underwater images of poor visibility.

4. Conclusion

The proposed algorithm (MFVR) characterized by the flexibility, simplicity and It succeeded in retrieving the missing details of by processing of color and lighting components separately. While the FVR algorithm did not improve the colors well. Also, SIH and MSRCR algorithms didn't success to improve the lightening of the color images as halos appeared. The proposed method (MFVR) was enabled to improve both lightness and contrast in the poor visibility Aerial images, provides better visual representation and edge information, Comparing to the other methods (SIH, MSRCR and FVR).

References

- [1] James, S. Aber, Irene Marzolf, Johannes B. Ries, Small-Format Aerial Photography, First edition, Elsevier, 2010.
- [2] Rianl, Murphy, Robertd. Morrison, Introduction to Environmental Forensics, Third edition, Elsevier, 2015.
- [3] Jacobs, I. S. and C. P. Bean, 1963. Fine particles, Thin Films and Exchange Anisotropy, in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, pp: 271-350.
- [4] Srinivasan, R., D. Sridharan, 2010. "**The Climate Effects on Line of Sight (LOS) in FSO Communication**", IEEE International Conference on Computational Intelligence and Computing Research.
- [5] Wang Hao, Ming He, HuiGe, Cheng-jin, Wang Qing, Wei Gao, 2011. "**Retinex-Like Method for Image Enhancement in Poor Visibility Conditions**", Procedia Engineering, (15): 2798-2803.
- [6] Rafael, C., Gonzalez, Richard E. Woods, Digital Image Processing, 2011. Third edition, Pearson Education.
- [7] Z. Wang and Y. Feng, "**Fast single haze image enhancement**", Elsevier, Computers and Electrical Engineering, Vol. 40, Issue 3, P 785–795, 2014.
- [8] D. Jabson, Z. Rahman, and G.A. Woodell, "**A multi-scale retinex for bridging the gap between color images and the human observation of scenes**", IEEE Trans. Image Process. 6, pp. 965-976, July 1997.
- [9] D. J. Jobson, Z. Rahman, and G. A. Woodell, "**Properties and performance of a center/surround retinex**", IEEE Trans. on Image Processing 6, pp. 451–462, March 1996.
- [10] K. Barnard and B. Funt, "**Analysis and Improvement of Multi-Scale Retinex**" In Proceedings of the IS&T/SID Fifth Color Imaging Conference: Color Science, Systems and Applications, Scottsdale, Arizona, pp. 221-226, 1997.
- [11] Hauti `ere, N., J.-P. Tarel, J. Lavenant and D. Aubert, 2006. Automatic Fog Detection and Estimation of Visibility Distance Through use of an Onboard Camera, Machine Vision and Applications, 17(1): 8-20
- [12] Jean-Philippe Tarel, Nicolas Hautière, "**Fast visibility restoration from a single color or gray level image**", IEEE 12th International Conference on Computer Vision, P 2201 – 2208, 2009.
- [13] Marc Ebner, "**Color Constancy**", John Wiley & Sons, 2007.

تحسين إضاءة وتباين الصورة الطبية بواسطة معادلات عددية

أ. د. زياد محمد عبود م. م. فلاح عابر بيده

الجامعة المستنصرية/ كلية التربية

المستخلص

تم في هذا البحث، وضع معادلة من معادلاتي القوة واللوغاريتم لتحسين الإضاءة والتباين لصور طبية، وكذلك تم إنشاء مرشحين (3×3) من حل المعادلتين بواسطة طريقة نيوتن-رافسون، واستخدمها في تحسين الإضاءة والتباين لتلك الصور. تم استخراج معاملات جودة الصورة ومقارنتها مع معاملات جودة الصورة لنفس الصور والتي تم معالجتها بواسطة مرشح المعدل، وتبين انه الطريقة المقترحة أعطت نتائج افضل.

الكلمات المفتاحية: معالجة الصور، تحسين التباين والإضاءة، صور طبية، معاملات جودة الصورة.

Enhancement the brightness and contrast of the image medical by numerical equations

Prof. Dr. Ziad M. Abood Falah A. Bida

Abstract:

In this research, an equation of power and logarithm equations was create to improve the illumination and contrast of medical images, and three (3×3) candidates were created from the Newton-Raafson equation solution and used to improve the illumination and contrast of these images.

Image quality coefficients were extracted and compared with image quality coefficients for the same images, which were processed by the modified filter, and showed that the proposed method gave better results.

Keywords: image processing, contrast and lighting improvement, medical images, image quality coefficients.

1. المقدمة:

ازداد استخدام الصور الرقمية في السنوات الأخيرة نظراً لتوافر التكنولوجيا والمعدات التي جعلت عملية التعامل مع الصور من الأمور الممكنة، فالكاميرات التقليدية تعتمد أساساً فيزيائياً يتحكم المستخدم بنسبة الإضاءة الداخلة إلى العدسة عن طريق التحكم بكميتها وبتجاه الضوء، أما الكاميرا الرقمية فلا تتطلب سوى دراية بسيطة من قبل المستخدم، ومبدأ عملها يعتمد على تحويل الضوء إلى شحنات كهربائية، وتحويل الصورة إلى سلسلة من الأرقام الثنائية (الأصفر والاحاد) لتمثل النقاط التي تكون الصورة. [1]

وان التطور الهائل في التقنية الحاسوبية، والتقدم الكبير في مجال التسجيل الرقمي للصور ساعداً على ظهور الأجهزة التي تسمح بالحصول على الصور دون معالجة كيميائية. وقد أثارت بعض المزايا التي يوفرها التصوير الرقمي مثل: ثبات جودة الصورة بغض النظر عن طول فترة التخزين، وعدد مرات النسخ، وإمكانية المعالجة بالحاسوب، اهتمام العديد من العاملين في المجالات الطبية، وجذبتهم إلى مجال التصوير الرقمي. [2]

إن الفرز البسيط بمساعدة الحاسوب (Computer-Aided Simple Triage-CAST) هي أساليب، أو أنظمة حاسوبية تُساعد الأطباء في التفسير الأولي، وتصنيف الصور الطبية، والفرز البسيط بمساعدة الحاسوب هو فئة فرعية من برامج التشخيص بمساعدة الحاسوب (Computer-Aided Detection Diagnosis-CAD). إذ تقوم أنظمة برامج "الفرز البسيط بمساعدة الحاسوب" بالفرز (التصنيف) المبدئي للتقائي الكامل لدراسات التصوير الطبي التشخيصية. وقد تم إعداد "الفرز البسيط بمساعدة الحاسوب" أساساً للحالات المهمة في التصوير التشخيصي، التي يكون مطلوباً فيها التشخيص السريع للحالات الحرجة التي تُهدد حياة الفرد، على عكس التشخيص بمساعدة الحاسوب التقليدي، الذي يُستخدم أساساً للكشف عن الأورام الخبيثة، يتعامل "الفرز

البسيط بمساعدة الحاسوب" مع الحالات الخطيرة التي تُهدد حياة الفرد، عندما يكون التشخيص الفوري حرجاً في التعامل مع الحالة. في حين يمثل الهدف الأساسي من التشخيص بمساعدة الحاسوب التقليدي في تحسين الدقة التشخيصية للمستخدم [3]. ومع التطور السريع في المجال الطبي، أصبح ما يعرف بـ (الطبيب الإلكتروني) واقعاً يمكن الوثوق به بدرجة عالية وعامل مهم في الكشف عن كثير من الأمراض، وتشخيصها بشكل مبكر مما يساعد على الشفاء المبكر أو حتى تجنب كثير من هذه الأمراض لاسيما الأمراض السرطانية منها. ويتنامى دور هذه الأنظمة مع التقدم الكبير في طرائق التصوير الطبي باستخدام الحاسوب التي تنتج كميات هائلة من المعطيات التي تحتاج لمن يفسرها، ويستخلص منها معلومات تشخيص الأمراض بشكل سريع وفعال [4].

2- الجانب النظري:

1-2 أساسيات الصورة الرقمية Basic Concept of Digital Image

يدرك الإنسان ما حوله من مشاهد أو صور بوساطة العين إذ تستلم الصورة بشكل مجموعة من الطاقة الضوئية الموزعة بترتيب معين وإن هذه الصور تسمى صوراً ضوئية Optical Image والتي تمثل معلوماتها بشكل إشارات كهربائية تماثلية Analog Form، وعند التعامل معها بالحاسوب فلا بد من تحويلها إلى شكل رقمي Digital Form أو مقطع Discrete Form قبل إجراء أي معالجة حاسوبية عليها وهذا يتم بعملية الرقمنة Digitalization وفي كل من أحداثي الحيز والاتساع، وتدعى رقمنة الحيز بالتقسيم (التجزئة) Sampling ورقمنة الاتساع بالتكميم Quantization ففي الصور الملونة فإن عملية التكميم تتم باختيار مجموعة من الألوان التي تمثل السلسلة اللونية للصورة [5]. أن عملية التقسيم تعني تجزئة الصورة إلى عناصر صغيرة كل عنصر يدعى بكسل ومن ثم تكتم قيم هذه العناصر بأخذ معدل الشدة لكل عنصر وتمثيله بعدد صحيح محدد ضمن الفترة (L_{min}, L_{max}) الصورة الناتجة من عملية التقسيم تسمى بالصورة الرقمية وهي عبارة عن مصفوفة ثنائية الأبعاد مرتبة بشكل أعمدة وصفوف وكل عنصر من عناصر هذه المصفوفة يسمى بالكسل.

أن تحليلية الشدة تشير إلى اصغر تغيير قابل للتمييز في المستوى الرمادي، يكون عادة عدد المستويات عدد صحيح L يمثل بالعلاقة الآتية [6]:

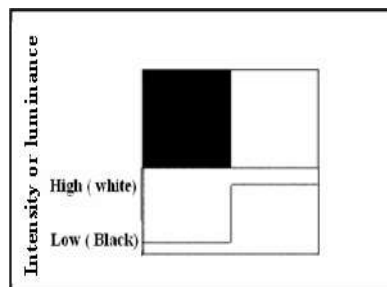
$$L = 2^n \quad \dots (1)$$

اذ n عدد صحيح يمثل عدد المراتب الثنائية لتمثيل المستوى الرمادي، ان العدد الأكثر شيوعاً لتمثيل المستوى الشدة هو 8 bit أي $L = 2^8 = 256$ وهناك بعض التطبيقات تستخدم $n = 12\text{bit}$ أو $n = 16\text{bit}$ ان تمييز تفاصيل الصورة سوف يكون محكوماً $(n \times M \times N)$ اذ ان $(N \times M)$ هي التحليلية الحيزية و n عدد البت لتمثيل كل مستوي من المستويات الرمادية، فالصورة ذات التحليلية العالية هي الصورة التي تمتلك عدد عناصر $(N \times M)$ كبيراً ومستويات التدرج الرمادي L لها عالٍ وكلما كانت هذه الأعداد صغيرة قلت الوضوحية وضعفت عملية تمييز تفاصيل الصورة [7][8].

2-2 الإضاءة Lightness

تعتبر الإضاءة عنصراً شديداً الأهمية في المعالجة اللونية. ان الضوء الداخل للعين هو نتيجة لشدة الإضاءة ومعامل انعكاس المشهد لأي طول موجي [13]. يتأثر الإحساس اللوني في العين اذا حصلت تغيرات في لون المشهد نتيجة تغير في شدة الإضاءة، فعند الانتقال من غرفة مضاءة بضوء صناعي إلى ضوء الشمس يقوم الجهاز العصبي البصري البشري بالتعويض التلقائي لتغير شدة الإضاءة بخلاف آلة التصوير الكاميرا التي لا تقوم بمثل هذا التعويض ويكون للتغيرات الحاصلة في شدة الإضاءة تأثير شديد على قيم اللونية لعنصر الصورة للحزم اللونية RGB [14].

الإضاءة تشير إلى الإضاءة العالية Lightness او العتمة Darkness في كل الصورة، يمتلك اللون الاسود شدة واطئة المصطلح الصحيح يسمى النصوع Luminance ويمتلك اللون الأبيض شدة عالية او نصوعاً عالياً الشكل (1) يبين طريقة تمثيل الحافة بشكل تخطيطي يلاحظ من الشكل ان الجانب الأيسر واطئ النصوع ثم يتصاعد ليكون عالي النصوع من الجانب الأيمن.



الشكل (1): طريقة تمثيل الحافة [12]

طريقة نيوتن-رافسون (The Newton-Raphson Method):

هي طريقة عددية فعالة لإيجاد جذور تابع حقيقي. لذلك تعتبر مثلاً لخوارزميات إيجاد الجذور يمكن استخدامها لإيجاد الحدود العليا والحدود الدنيا لمثل هذه التوابع، عن طريق إيجاد جذور المشتقة الأولى للتابع، في هذه الطريقة يفترض أن المسألة المراد حلها تكون على الصورة: [18]

$$f(x)=0$$

اذ ان x هو المتغير الذي يحقق المعادلة $0=f(x)$ وبشرط اتصال الدالة عند هذا الجذر على الأقل. على ذلك يمكن البحث عن جذر قريب من x وليكن x_n وتعويضه في طريقة نيوتن الموضحة في المعادلة (2) لإيجاد قيمة أكثر دقة ولتكن x_{n+1} :

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)} \dots\dots\dots (2)$$

إذ إن $f(x_n)$ تمثل الدالة و $f'(x_n)$ مشتقة الدالة.

4- أحصائيات جودة الصورة:

تم تطبيق إحصائيات الأنثية لقياس جودة الصورة المطبقة عليها مرشحات الدراسة الحالي، وهي:

a - معدل مربع الخطأ (MSE):

يعرف بأنه الخطأ التربيعي التراكمي بين الصورة الناتجة والصورة الأصلية، ويحسب من العلاقة الآتية:

$$MSE = \frac{1}{MN} \sum_{y=1}^N \sum_{x=1}^M [I_1(x, y) - I_2(x, y)]^2 \dots\dots\dots (3)$$

اذ أن $I_1(x, y)$: عنصر الصورة الأصلية في الموقع (x, y) . [15]

$I_2(x, y)$: عنصر الصورة المطلوب حساب MSE لها في الموقع (x, y) .

M, N عدد العناصر المراد حساب معدل مربع الخطأ لها قد تمثل حجم الصورة ككل أو حجم جزء من الصورة.

b- مقياس قيمة ذروة نسبة الضوضاء إلى الإشارة (PSNR):

ذروة نسبة الإشارة إلى الضوضاء، وتعني النسبة لأعلى قيمة، وأوطأ قيمة للإشارة إلى الضوضاء: [16]

$$PSNR = 10 \log \left(\frac{(L-1)^2}{MSE} \right) \dots (4)$$

إذ ان: L هو عدد المستويات الرمادية ويقاس PSNR بوحدة (dB) decibel

c- جذر مربع الخطأ (RMSE):

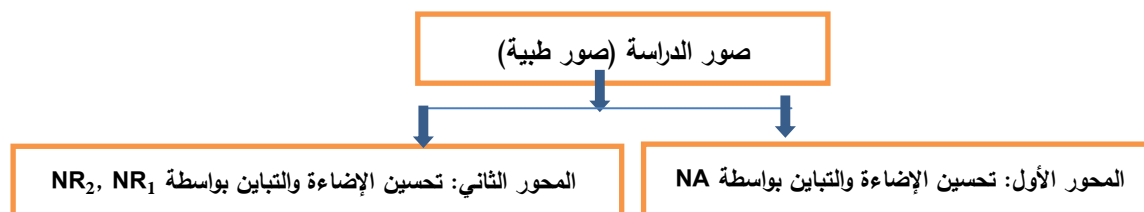
ويعرف بأنه الجذر التربيعي لمعدل مربع الخطأ MSE فكما كانت قيمتها قليلة أي أقل خطأ تكون أقرب إلى الأصلية. [17]

$$RMSE = \sqrt{\frac{1}{MN} \sum_{y=1}^N \sum_{x=1}^M [I_1(x, y) - I_2(x, y)]^2} \dots (5)$$

3- الجانب العملي:

3-1 المحاور التي تم اعتمادها في الدراسة:

يبين الشكل (2) مخطط للمحاور التي اعتمدت في الدراسة الحالية، والتي من خلالها تم بناء المرشحات وتطبيقها على صور الدراسة.



الشكل (2): مخطط محاور الدراسة الحالية

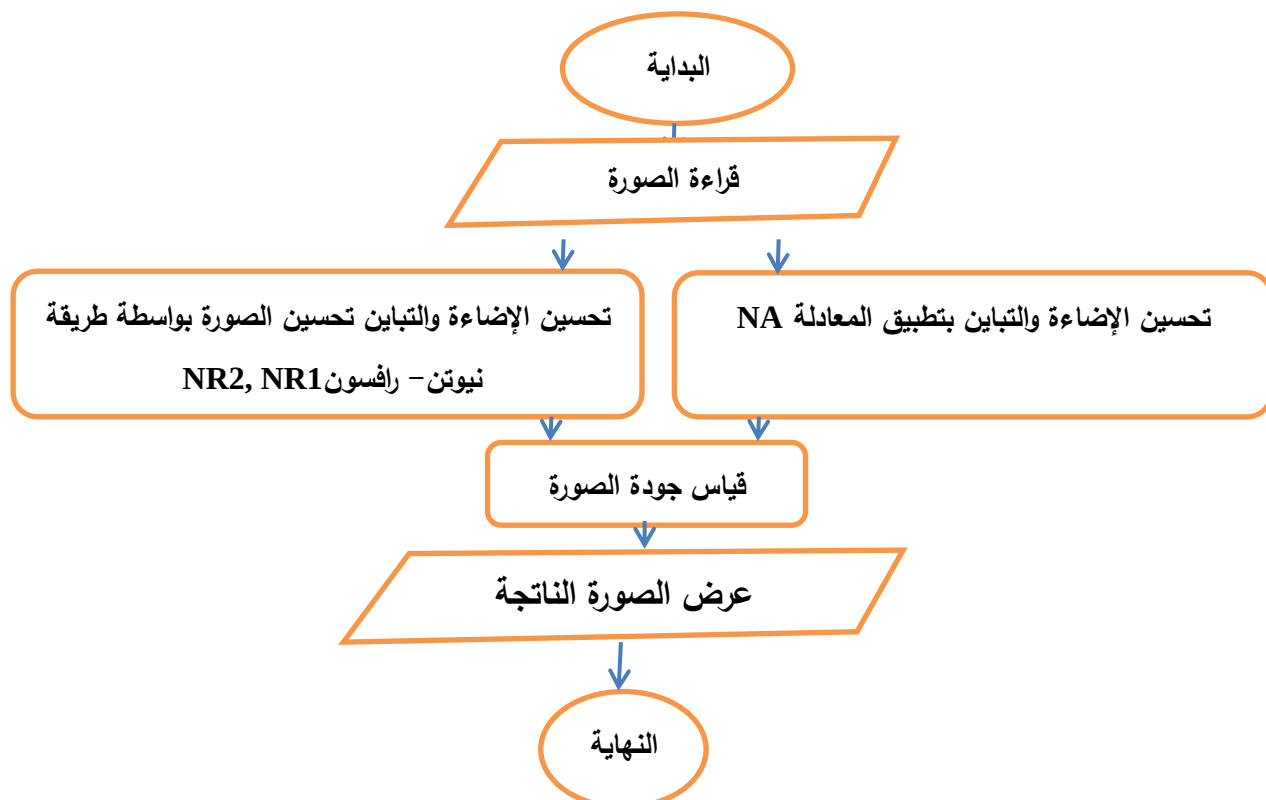
الجدول (1) يضم الطرق والمعادلات التي تم وضعها ضمن محاور الدراسة.

الجدول (1)

المحور	الطريقة	الترميز	العلاقة الرياضية
المحور الأول	1- تحسين الإضاءة والتباين	NA	$s = c/2[\log(1+r) + (r)^g]$
المحور الثاني	2- تحسين الإضاءة والتباين بواسطة طريقة نيوتن - رافسون	NR1 NR2	$1 - f(X) = X - \cos(X)$ $2 - f(X) = X \exp(X) - 1$

3-2 خوارزمية العمل:

الشكل (3) يبين لخطوات العمل الحالي.



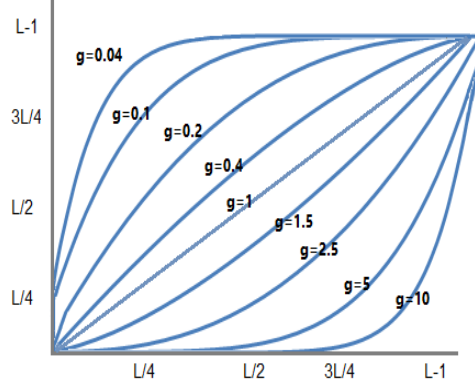
الشكل (3): مخطط يوضح خوارزمية الدراسة الحالية

4- النتائج والمناقشة:

4-1 نتائج المحور الأول: تحسين إضاءة وتباين الصورة بواسطة المعادلة NA:

بتعويض قيم الشدة (r) للصورة والتي تتراوح قيمتها بين (0-255) في المعادلة NA في الجدول (1) نحصل على قيمة الشدة الخارجة للصورة المحسنة s لقيم مختلفة من g والتي تساوي (0.04, 0.1, 0.2, 0.4, 0.67, 1, 1.5, 2.5, 5, 10) وبثبوت قيمة ($c=1$).

يمثل الشكل (4) العلاقة بين شدة الصورة الداخلة (r) وشدة الصورة المحسنة (s) والتي تم حسابها من المعادلة NA.

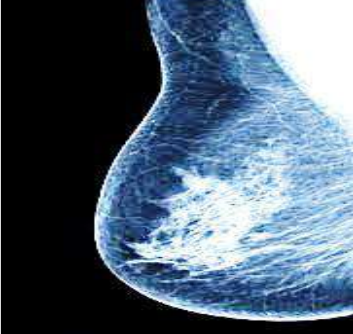
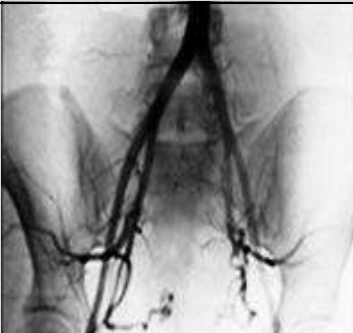
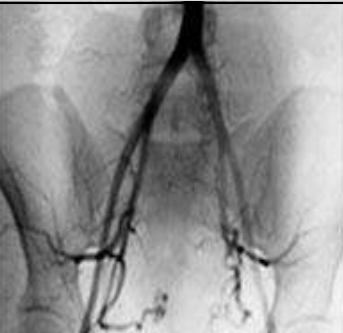


الشكل (4): يمثل العلاقة بين شدة الصورة الداخلة (r) وشدة الصورة المحسنة (s) حسب المعادلة NA

الجدول (2) يمثل الصور قبل المعالجة وبعد تحسين أضاعتها وتباينها بواسطة المعادلة NA.

الجدول (2) الصور قبل المعالجة وبعد تحسين أضاعتها وتباينها

ت	تقنيات التصوير	الصورة قبل المعالجة	الصورة بعد المعالجة
1	الأشعة السينية x-Ray $g = 0.2$		
2	التصوير بالرنين المغناطيسي Magnetic Resonance MRI Imaging $g = 0.4$		

		التصوير بواسطة الموجات الفوق صوتية Ultrasound (D) $g = 0.2$	3
		التصوير الشعاعي للثدي Mammography $g = 0.04$	4
		التصوير المقطعي Computed Tomography (CT) Scan $g = 0.2$	5
		تصوير الأوردة والشرابين والأشعة التداخلية Angiography and Interventional $g = 0.4$	6
		التصوير بأجهزة التنظير Fluoroscopy $g = 0.04$	7

4-2 نتائج المحور الثاني: تحسين الصورة بواسطة طريقة نيوتن-رافسون:

تصبح معادلة نيوتن-رافسون (2) كالآتي: [18]

$$C_j = C_i - \frac{f(C_i)}{f'(C_i)} \dots \dots \dots (6)$$

C_i = البكسل المركزي (Central pixel).

C_j = البكسل المجاور للبكسل المركزي C_i (Neighboring pixel of C_i).

وحل المعادلة الآتية وتكوين المرشح NR1 على أساس حساب المسافة بين البكسل وجيرانه.

$$f(C_i) = i - \cos(i), f'(C_i) = 1 + \sin(i) \dots \dots \dots (7)$$

إذ تم استخدام هذه المسافة لتحسين قيمة البكسل غير المرغوب فيه لإزالة الضوضاء وتحسين مظهر الصورة.

وبنفس الطريقة أعلاه نحل المعادلة الآتية ومشتقتها في المعادلة (6) نحصل على المرشح NR2.

$$f(C_i) = i \exp(i) - 1, f'(C_i) = i \exp(i) + 1 \dots \dots \dots (8)$$

وبتعويض المعادلات (7) في معادلة نيوتن-رافسون (6) وتعويض عن قيمة البكسل المركزي ($C_i = x=1$) ومنها نجد قيمة

البكسل المجاور C_j للبكسل المركزي وبعدها نعتبر البكسل المجاور الذي حصلنا عليه هو البكسل المركزي وبنفس الطريقة نجد

له البكسل المجاور نضع النتائج في مصفوفة (3*3) ونحصل على المرشح NR1 والموضحة بالجدول (3).

وبنفس الطريقة السابقة نحل معادلة (8) ونحصل على المرشح NR2 والموضحة بالجدول (3).

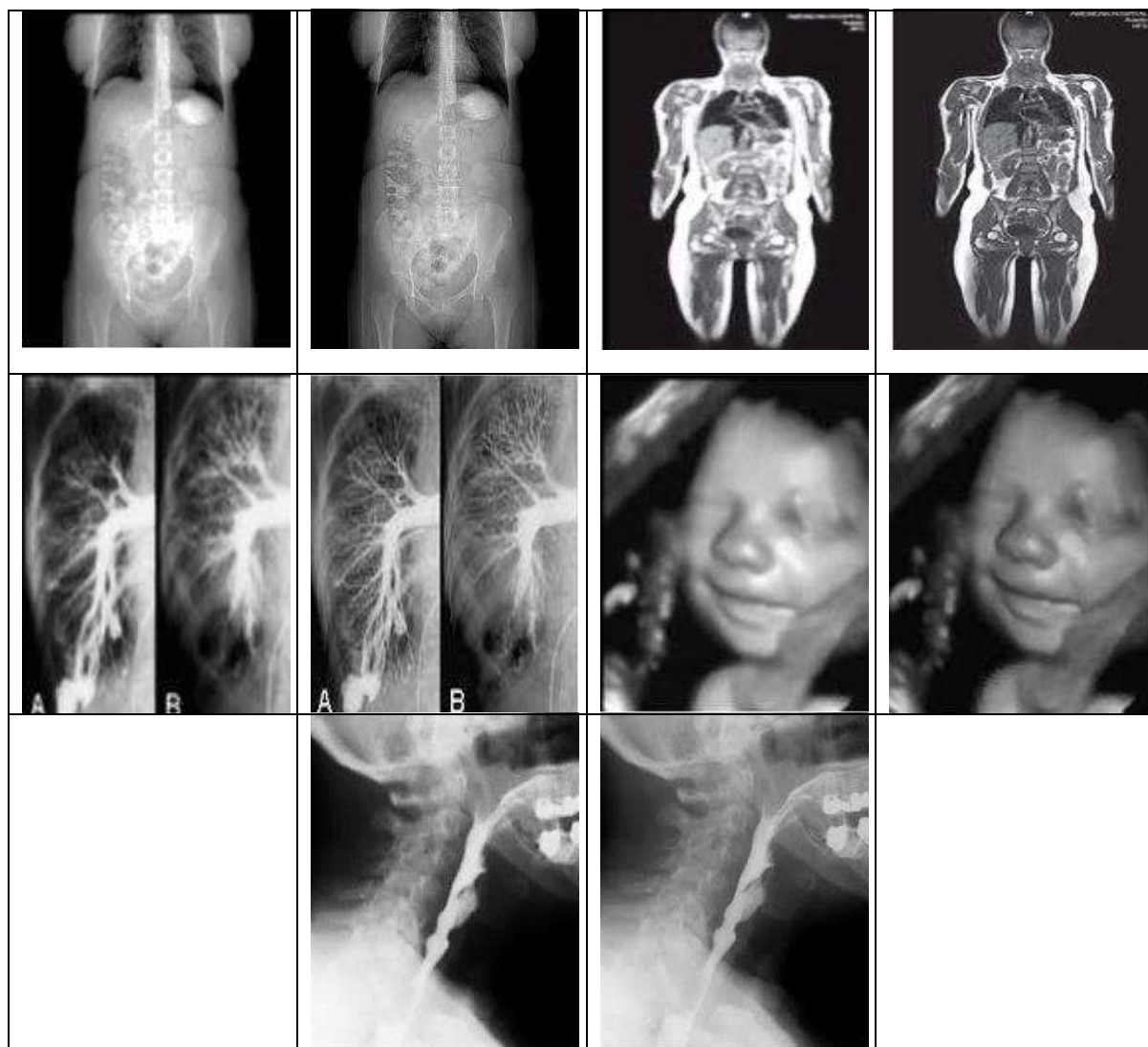
الجدول (3) المرشحات الناتجة من حل المعادلات (7) و (8) باستخدام طريقة نيوتن-رافسون

رقم المعادلة	رمز المرشح	الصيغة الرياضية للمعادلة	(3x3) مرشح المعادلة		
1	NR1	$f(x) = x - \cos(x)$	0.739112891	0.750363868	0.739112891
			0.750363868	1	0.750363868
			0.739112891	0.750363868	0.739112891
2	NR2	$f(x) = x \exp(x) - 1$	0.893514757	0.683939721	0.893514757
			0.683939721	1	0.683939721
			0.893514757	0.683939721	0.893514757

استخدم المرشح NR1 المعادلة (1) لتحسين صور الدراسة، وتم الحصول على النتائج في الجدول (4).

الجدول (4) نتائج تطبيق المرشح NR1 على صور الدراسة ونتائج تحسينها

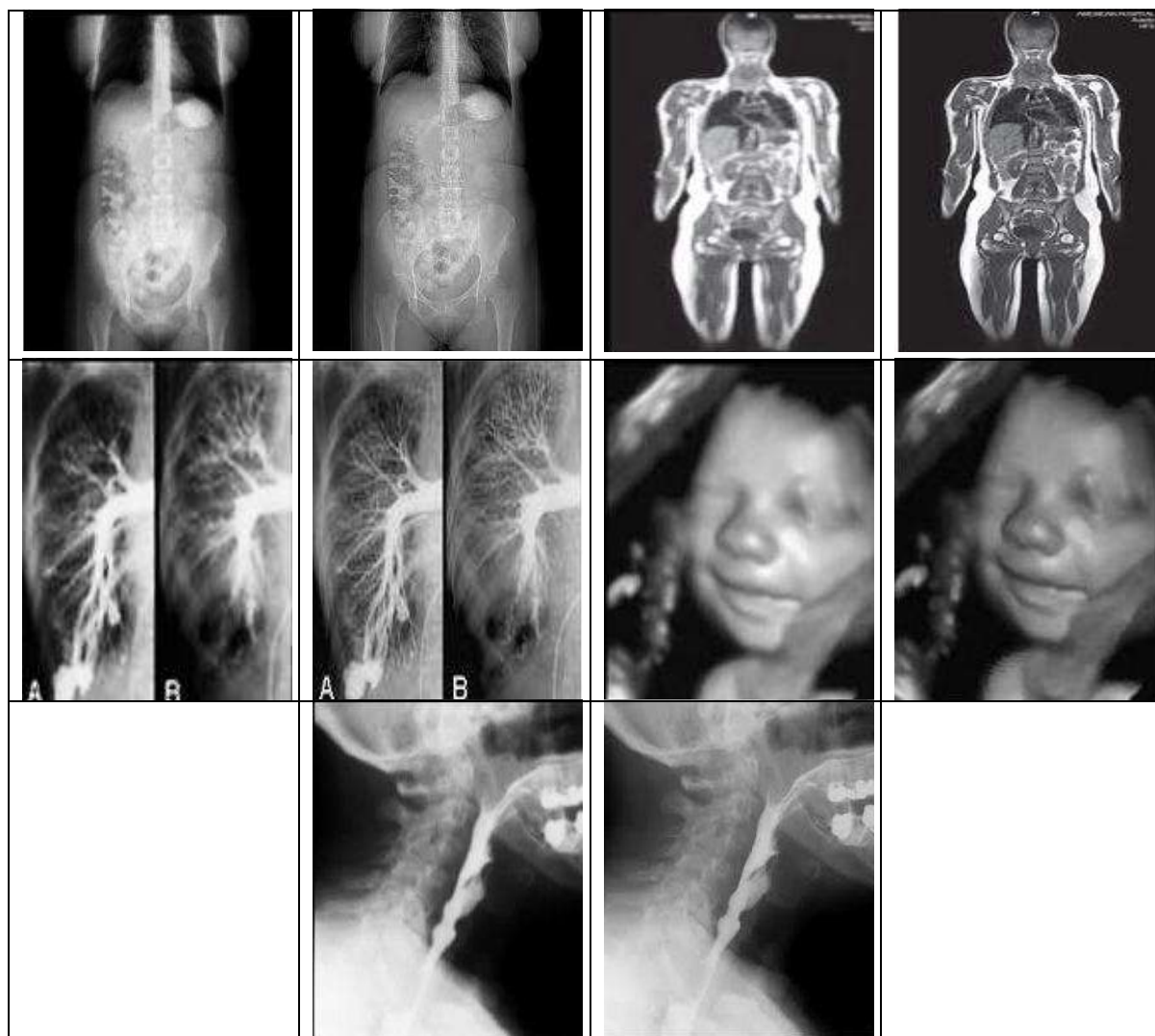
الصورة الأصلية	الصورة بعد التحسين	الصورة الأصلية	الصورة بعد التحسين
			



تم استخدام المرشح NR2 لتحسين الصور الدراسة، وتم الحصول على النتائج في الجدول (5).

الجدول (5) نتائج تطبيق المرشح NR2 على الصور ونتائج تحسينها

الصورة الأصلية	الصورة بعد التحسين	الصورة الأصلية	الصورة بعد التحسين



3-4 النتائج الإحصائية:

يمثل الجدول (6) قيم PSNR و MSE و RMSE للصور التي تم تحسين الإضاءة والتباين لها بواسطة المعادلة NA.

الجدول (6) قيم PSNR و MSE و RMSE للصور المحسنة بواسطة المعادلة NA

الاحصائيات			ت	تقنية التصوير
PSNR	MSE	RMSE		
86.5979	3.3580772	1.8325057	1	x-ray
90.3054	2.7898659	1.6702892	2	MRI
93.7578	2.3475531	1.5321727	3	Ultrasound
22.3856	83.261274	9.1247616	4	Mammography
57.1775	14.619972	3.8236072	5	CT
52.1751	18.774669	4.3329746	6	Angiography and Interventional
68.94	8.1194592	2.8494665	7	Fluoroscopy

يمثل الجدول (7) قيم PSNR و MSE و RMSE للمرشح (3x3) NR1، ومقارنتها مع قيم المرشح المعدل (Average 3x3).

الجدول (7) قيم PSNR و MSE و RMSE للمرشح (3x3) NR1 والمرشح المعدل (Average 3x3)

المرشح (3x3) NR1			المرشح (Average 3x3)			ت	تقنية التصوير
PSNR	MSE	RMSE	PSNR	MSE	RMSE		
61.5742	11.7347	3.4256	52.8255	18.1739	4.26309	1	x-ray
58.1337	13.9374	3.73328	57.4334	14.4341	3.799224	2	MRI
46.8922	24.4505	4.94475	47.064	24.2414	4.92356	3	Ultrasound
39.5413	35.3111	5.94231	29.5622	58.1574	7.626102	4	Mammography
49.7342	21.2117	4.60561	45.175	26.6426	5.161652	5	CT
46.596	24.8153	4.98150	40.6903	33.3396	5.774053	6	Angiography and Interventional
47.3682	23.8755	4.88625	36.4432	41.2274	6.420858	7	Fluoroscopy

يمثل الجدول (8) قيم PSNR و MSE و RMSE للمرشح (3x3) NR2، ومقارنتها مع قيم المرشح المعدل (Average 3x3).

الجدول (8) قيم PSNR و MSE و RMSE للمرشح (3x3) NR2 والمرشح المعدل (Average 3x3)

المرشح (3x3) NR2			المرشح (Average 3x3)			ت	تقنية التصوير
PSNR	MSE	RMSE	PSNR	MSE	RMSE		
61.5978	11.7209	3.42358	53.0837	17.94082	4.23566	1	x-ray
58.0399	14.002957	3.742053	59.2769	13.16311	3.6281	2	MRI
46.7332	24.645727	4.964446	38.1385	37.87679	6.15441	3	Ultrasound
35.510	43.196676	6.572418	34.0326	46.50843	6.81970	4	Mammography
49.9624	20.971063	4.579417	38.413	37.36048	6.11232	5	CT
46.3847	25.078942	5.007888	35.2177	43.83263	6.62062	6	Angiography and Interventional
46.7637	24.608171	4.960662	55.6862	15.75178	3.96885	7	Fluoroscopy

4-4 المناقشة:

أظهرت النتائج الإحصائية لكل من PSNR و MSE و RMSE كفاءة المعادلة المستحدثة NA في تحسين الاضاءة والتباين للصور الطبية وخصوصا للصور المقطعية (Computed Tomography Scan) (CT) وصور الأوردة والشرابين (Angiography and Interventional) وصور الأشعة التنظيرية (Fluoroscopy) كما أظهرت النتائج الإحصائية كفاءة المعادلات المستحدثة NR1 و NR2 في تحسين الاضاءة والتباين لصور تقنيات التصوير المقطعي Computed Tomography Scan) (CT) وتصوير الأوردة والشرابين والأشعة التداخلية (Angiography and Interventional) والتصوير بأجهزة التنظير (Fluoroscopy) بالمقارنة مع النتائج الإحصائية لتحسين الاضاءة والتباين لنفس الصور بواسطة المرشح المعدل (Average).

References

- [1] Kotropoulos C. and Pitas I. "Nonlinear model based image video processing and analysis", A Wiley- Interscience publication, John Wiley & Sons, Inc, USA, 2001.
- [2] إبراهيم الفضيلات، "التصوير الضوئي التقليدي والرقمي"، ط3، مرجع شامل في النظرية والتطبيق، عمان، الاردن، 2002.
- [3] Goldenberg R., Peled N., "Computer-aided simple triage", Int. J Compute Assist Radial Surg., 6(5):705-11, Sep, 2011.
- [4] Taylor P., Wilson R., Johnston K., Potts H., "The impact of the discovery of computer-aided claims over the sensitivity and specificity of mammography", 10- 70, (6) 9, 2005.
- [5] Paul M., "Computer Processing of Remotely Sensed Image: An Introduction", John Wiley and Sons, (1987).

- [6]Huang T., "**Picture Processing and Digital Filtering**", New York Verlay bbelin, (1979).
- [7]Eugene H., "**Optics**", 3rd edition Addison Longman, Inc., chapter (5 and 6), (1998).
- [8]Rafael C., Richard E., "**Digital Image Processing**", 3rd edition, 2008.
- [9]Vliet L., "**A Non Linear Laplace Operator as edge detection in noisy Image**", New York Computer Graphics, (1989).
- [10] Harry C., "**Monochrome Digital Image Enhancement**", IEEE, Computer Society, New York, the Optical Society of America vol. 15,(1985).
- [11] Sony S., and Horne J, "**The Color Image Processing Hand Book**", International Thomson, (1998).
- [12] Scott E., "**Computer Vision and Image Processing**", prentice Hall, (1998).
- [13] Nezamzbad M. and Berns R., "The Effect of Image Size on the Color appearance of Image reproduction using Colorimetrically Calibrated LCD and DLP displays", J. Soc.Inf. DISP. 14 (9), PP.773, (2006).
- [14] Wendell B. and Farrell J., "**Convert in Scanner RGB to Tristimulus XYZ**", Proceeding. SPIE, (1993).
- [15] Gonzalez, R. C., and Wintz, P., "**Digital Image Processing**", 2nd ed., Addison-Wesley Publication Company, 1987.
- [16] Mahadevaswamy H. R., "**New Approaches to Image Compression**", Ph.D. thesis, Regional Engineering College, university of Calicut, December, 2000.
- [17] Sati Satish K., "**An Introduction to Image Compression**", [http://www. debugmode. com/imagecmp](http://www.debugmode.com/imagecmp), 22, Oct, 2000.
- [18] J. M. McDonough, "**Computational Numerical Analysis**", University of Kentucky Lexington, KY 40506 (2007).

Color Image Enhancement For The Objects Immersed in Turbid Water Using Adaptive Retinex Algorithm Based on Gamma Correction

Fatima I. Abbas¹ Ali Abid D. Al – Zuky²
Hazim G. Dway² Radhi Sh. Al-Taweel¹

¹Department of Physics, College of Education, AL-Mustansiriyah University, Iraq.

²Department of Physics, College of Science, AL-Mustansiriyah University, Baghdad, Iraq

fatma11113333@yahoo.com Al-zuky@yahoo.com

hazimdo@yahoo.com drradhi55@yahoo.com

Abstract:

The objects in the underwater images are not clearly visible due to low contrast and scattering of light and the large degradation present in the water environment which leads to lose its original color and details. The Retinex (R) is an image enhancement algorithm that improves the brightness, contrast and sharpness of an image. In this paper, could be proposed a new image enhancement algorithm dependent on the Retinex (R) algorithm using Gamma correction, called adaptive Retinex (AR) Algorithm. From the result has been see the (AR) has best result from the (R) for enhancement color image of the objects immersed.

Keyword: Image color, Image Enhancement, Retinex, Adaptive Retinex, GAMMA Correction, Median Filter.

تحسين الصور الملونة للأجسام المغمورة في الماء العكر باستخدام خوارزمية رتينكس المطورة بالاعتماد على تصحيح كاما فاطمة اسماعيل عباس، علي عبد داود الزكي، حازم كاطع دوي، راضي شدهان حمودي الطويل

المستخلص

صور الأجسام تحت الماء غير واضحة للعيان بسبب التباين المنخفض نتيجة التشتت الكبير للضوء ووجود تشوهات في البيئة المائية مما يؤدي الى حصول ضعف في وضوحية الصورة ووهن في تفاصيل الصورة كذلك لونها الأصلي. ان خوارزمية رتينكس (R) تعمل على تحسين مستوى السطوع والتباين والشدة من الصورة. في هذا البحث أقترحنا خوارزمية جديدة لتحسين الصورة تعتمد خوارزمية رتينكس (R) باستخدام تصحيح كاما، تدعى خوارزمية رتينكس المطورة (AR). تبين ان نتائج خوارزمية (AR) افضل من نتائج خوارزمية (R) لتحسين الصور الملونة للأجسام المغمورة.

الكلمات المفتاحية: صور ملونة، تحسين الصور، رتينكس، رتينكس المعدلة، تصحيح كاما، مرشح المتوسط.

1. Intrduction

Enhancement techniques for the capture images for the objects immersed in water provide a way to improving the object identification in underwater environment. There is lot of research started for the improvement of image quality, but limited work has been done in the area of underwater images, because in underwater environment image get blurred due to poor visibility conditions and effects like (absorption, reflection, bending, and scattering) of light etc. These are the important factor which causes the degradation of underwater images [1]. Another well-known problem concerning the underwater images is related to the density of the water in the sea which is considered 800 times denser medium than air. Therefore, when light rays moves from the air to the water, it is partly reflected reverse and at the same time partly enters the water. The total light amount that enters the water also starts reducing start it goes deeper in the sea. Similarly, the water molecules also absorb certain amount of light. As a result, the underwater images are getting dim as the deepness increases. Not only the quantity of light rays is reduce when it goes deeper but also colors drop off one by one depending on the wavelength of the colors[1].

When taking a picture of an underwater object from outside the water container, waves on the surface cause distortion. If series of pictures are taken at various times, different distortions will be seen in each picture. The image seen by the camera is distorted by refraction as a function of both the angle of the water surface normal at the point of refraction and the amplitude of the water

waves. If the water is perfectly flat (i.e., there are no waves), there will be no distortion due to refraction. However, if the surface of the water is being disturbed by waves, the nature of the image distortion becomes considerably more complex,[2]. Color images provide more and richer information for visual perception than that of the gray images. Color image enhancement plays an important role in digital image processing. The purpose of image enhancement is to get good appearance images and highlight the useful information. During poor illumination conditions, the images appear darker or with low contrast. Such low contrast images need to be enhanced, [3].

The images with good lightness and contrast are a strong requirement in good vision, and remote sensing. The analysis of such images by measuring the quality is very important for this applications [4].

The related literature concerning underwater image processing and enhancement techniques as follows:

1. Kashif Iqbal, et.al. in 2007, [5] they proposed an approach based on slide stretching. The objective of this approach is twofold. Firstly, the contrast stretching of RGB bands to equalize the colour contrast in images. Secondly, the saturation and intensity stretching of HSI is used to increase the true colour and solve the problem of lighting.
2. Chiang, J.Y., et.al. in 2012, [6] the WCID They can effectively restore image color and remove haze. However, the salt ratio and amount of suspended particles in ocean water varies with time, location, and season, making accurate estimation of the rate of energy attenuation problematic. In addition, it is presumed that artificial light sources produce spherically radiating light different to surface light sources generally used in underwater photography; therefore the value of luminance is also difficult to estimate accurately.
3. Pulung Nurtantio, et.al. in 2013, [7] they using a new method of pre-processing of true-color imagery taken under water based on the Contrast Limited Adaptive Histogram image Equalization (CLAHE) algorithm. They explained the preprocessing step of underwater image registration using image enhancement framework.
4. Also, Nabeel Mubarak Mirza et.al., in 2014, [8] they proposed a new image enhancement algorithm dependent on the Modified Multi Scale Retinex Algorithm with Color Restoration (MMSRCR). This technique is using the lightness component in YIQ color space that is transformed by the Sigmoid Function. The results have been compared MSRCR, Histogram Equalization (HE), Adaptive Integrated Neighborhood Dependent Approach (AINDANE) algorithms. Where they developed and suggested two methods to assess the level of enhancement; the first dependent on segmentation of image for lightness component in YIQ color space called Minimum Distance Classifier (MDC). The second dependent on edge regions for lightness component in RGB basic color space called Quality Factor (QF).
5. Bhanudas Sandbhor, et.al, In 2015, [9] They discuss causes of underwater image distortion and various underwater image processing techniques. Also discuss limitations of various underwater image enhancement techniques. Also take an overview of WCID algorithm which is best among other underwater image enhancement techniques.

2. Enhancement Method and Gamma Correction

Some of contrast and lightness enhancement algorithms are used to enhance color images from any type of distortion (such as noise, color shift, inverse transform for any operation and lightness change), such as Histogram Equalization, Multi Scale Retinex algorithm and AINDANE algorithm. In this paper introduced famous method called Multi Scale Retinex algorithm, a new image enhancement algorithm dependent on the Retinex (R) algorithm using Gamma correction, called adaptive Retinex (AR) Algorithm,[8].

Gamma color correction is the name of a nonlinear operation used to code and decode luminance or tristimulus values in video or still image systems. Gamma correction is, in the simplest cases, defined by the following power-law expression,[10]:

$$I_o = KI_i^{\gamma} \quad (1)$$

Where K is a constant and the input I_i and output I_o values are non-negative real values; in the common case of $K = 1$, inputs and outputs are typically in the range $(0 - 1)$. A gamma value $\gamma < 1$ is sometimes called an encoding gamma, and the process of encoding with this compressive power-law nonlinearity is called gamma compression; conversely a gamma value $\gamma > 1$ is called a decoding gamma and the application of the expansive power-law nonlinearity is called gamma expansion,[10]. Fig.(1), the pixel values range from 0.0 representing pure black, to 1.0, which represents pure white. As the figure shows. Gamma values greater than 1.0 lighten an image and a gamma equal to 1.0 produces no effect on an image,[10].

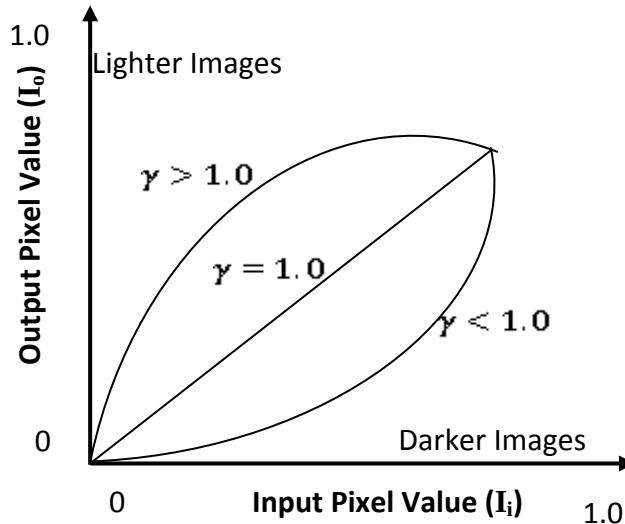


Fig.(1): Gamma Curves

3. Median Filter

Often desirable to be able to perform some kind of noise reduction on an image or signal. The median filter is a nonlinear digital filtering technique, often used to remove noise. The Median Filter is performed by taking the magnitude of all of the vectors within a mask and sorted according to the magnitudes. The pixel with the median magnitude is then used to replace the pixel studied. The pixel with the median magnitude is then used to replace the pixel studied. The median of a set is more robust with respect to the presence of noise. The median filter is given by, [11]:

$$I_o = \text{Median Filter}(I_1, \dots, I_n) = \text{Median value}(I_m) \quad (2)$$

Where n is Natural number greater than 1.0, $I_m \in$ median pixel value in processing window.

4. The Mean of Locally (μ, σ) Model Quality Assessment Measure

The image quality assessment is important process to determining the level of enhancement, in this section will be present developed method to assess the quality of underwater color image based on changing in the depth of target (object) in the water. In NASA Langley research center [4] concluded heuristics to measure quality of the image, proposed the idea that good visual representations seem to be based upon some combinations of high regional visual lightness and contrast. To compute the regional parameters, where have been divided the image into non overlapping blocks that are 50×50 pixels. For each block, the mean ($\bar{I}$) and a standard deviation ($\bar{\sigma}$) are computed in then taking the mean of them $\bar{\bar{I}}$ and $\bar{\bar{\sigma}}$ as shown in Fig.(2). If the points tend to visual optimal region the image has higher quality of lightness and contrast, whereas if $\bar{\sigma}$ (without $\bar{\bar{I}}$) is increased, it makes image having insufficient lightness, but if $\bar{\bar{I}}$ (without $\bar{\bar{\sigma}}$) is increased it makes insufficient contrast in the image.

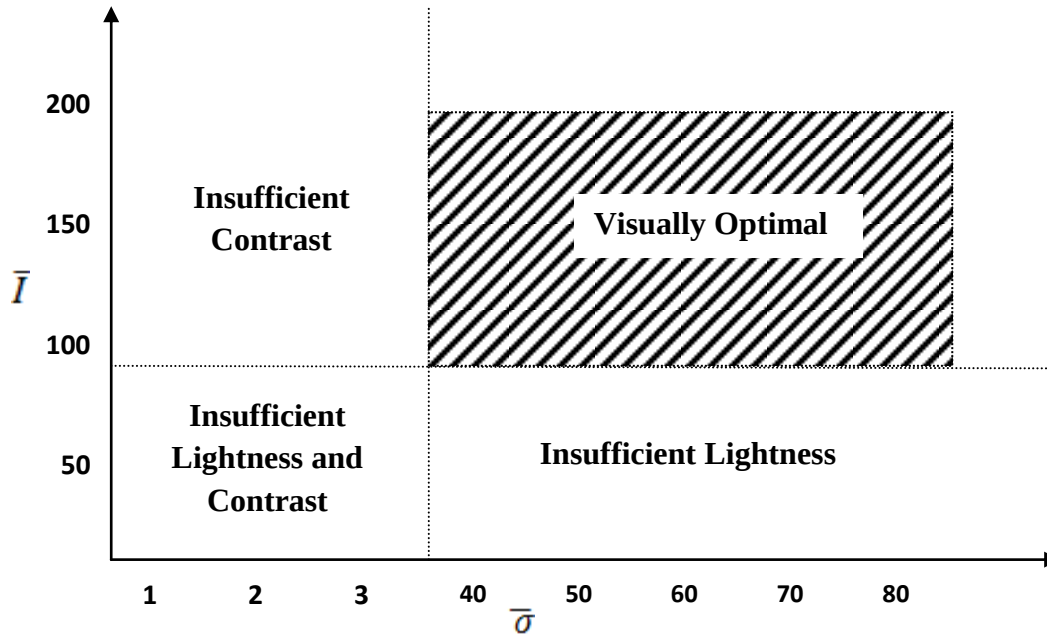


Fig. (2): Image quality description in the mean of locally mean and standard deviation of image model.

5. Retinex (R) Algorithm

The Multi-Scale Retinex (MSR) is explained from Single-Scale Retinex (SSR) have been [12]:

$$I_o(x, y, c) = \log[I_i(x, y)] - \log[F(x, y, c) \otimes I_i(x, y)] \quad \dots(3)$$

Where $I_o(x, y, c)$ the output of channel i ($i \in R, G, B$) at position x, y , c is the Gaussian shaped surrounding space constant, $I_i(x, y)$ is the image value for channel i and symbol $\otimes$ denoted convolution. $F(x, y, c)$ Gaussian surrounds function that is calculated by, [13]:

$$F(x, y, c) = k e^{-\left[\frac{(x^2 - y^2)}{c^2}\right]} \quad \dots(4)$$

k is determined by [14]:

$$k = \iint F(x, y, c) dx dy = 1 \quad \dots(5)$$

The MSR output is then simply a weighted sum of the outputs of several different SSR output where [14]:

$$I_{MSR}(x, y, w, c) = \sum_{n=1}^N W_n I_o(x, y, c_n) \quad \dots(6)$$

Where N is the number of scales, $I_o(x, y, c_n)$ the i 'th component of the n 'th scale, $I_{MSR}(x, y, w, c_n)$ the i 'th spectral component of the MSR output and W_n the weight associated with the n 'th scale. Hence can be insist that ($\sum W_n = 1$). The result of the above processing will have both negative and positive RGB values, and the histogram will typically have large tails. Thus a final gain-offset is applied as mentioned and discussed in more detail below. This processing can cause image colors to go towards gray, and thus an additional processing step is proposed in [13]:

$$R = I_{MSR} \cdot L(x, y, c) \quad \dots(7)$$

Where L given by

$$L(x, y, a) = b \log \left[1 + a \frac{I_i(x, y)}{\sum_{i=1}^3 I_i(x, y)} \right] \quad \dots(8)$$

Where have taken the liberty to use $\log(1+x)$ in place of $\log(x)$ to ensure a positive result. The values of $a=125$ and $b=100$ are suggested for a specific test image.

$$I_{pi}(x, y) = 0.35 (L(x, y, a, b) + 0.56) \quad \dots(9)$$

The final step is gain-offset by 0.35 and 0.56 respectively, I_{pi} is output image,[15]. In this work have been used ($w_1=w_2=w_3=1/3$) and ($c_1=250, c_2=80, c_3=15$) [12]. The Algorithm(1) describe steps of the program sequence.

Algorithm (1) Retinex (R) algorithm, [4]

Input: color image $I_i(x, y)$, $i = r, g, b$.

Step1: Calculate Gaussian surrounds function from Eq.(4), where k is normalization constant, $c_n, n=3, \{c_1=250, c_2=80, c_3=15\}$.

Step2: Compute SSR ($I_o(x, y, c)$) from Eq.(3).

Step3: Compute MSR ($I_{MSR}(x, y, w, c)$) from Eq.(6), Where $N=3, \{w_1=w_2=w_3=1/3\}$.

Step4: Calculate MSR with color restoration by Eq.(8), Where, $b=100, a=125$.

Output: image $I_{pi}(x, y)$ is gotten from gain offset by Eq.(9):

6. The Practical Work

In this study, have been selected group color ball in a bowl, putted in the bottom of basin dimensions (80, 37, 50)cm Fig.(3), which is consisting of (red, green, blue, yellow, white and black). Camera is placed in fix place at the top of the basin. Heights(H) of water in basin was changed level (10, 20, 30, 40 and 50) cm in each case added tea bags(Lipton-2.0 gram Fig.(4)) into the water to get the turbid (darkness) so that vision is quite clear, and cannot see the object underwater clearly, so the capture of this object not clear or not good. Long a ruler used to determine the height(H) of the water. Images were taken by using camera (Sony DSC -TX10), format with size (640×243 pixel), after that these images are processed by program bulleted in Mat lab.



Fig. (3): Basin of water, fix camera above and below the object(target)



Fig. (4): Tea Bag

The suggested algorithm consists of two stages: in first stage Adaptive Retinex (AR) algorithm method applied then lightness component in YIQ color space is transformed using sigmoid function, and Gamma correction is applied on Y component and in the second stage inverse color transform RGB enhancement algorithm is applied. The proposed algorithm is abbreviated as Automatic Color Contrast Enhancement (AR) Algorithm. The model of proposed method is shown in Fig.(5).

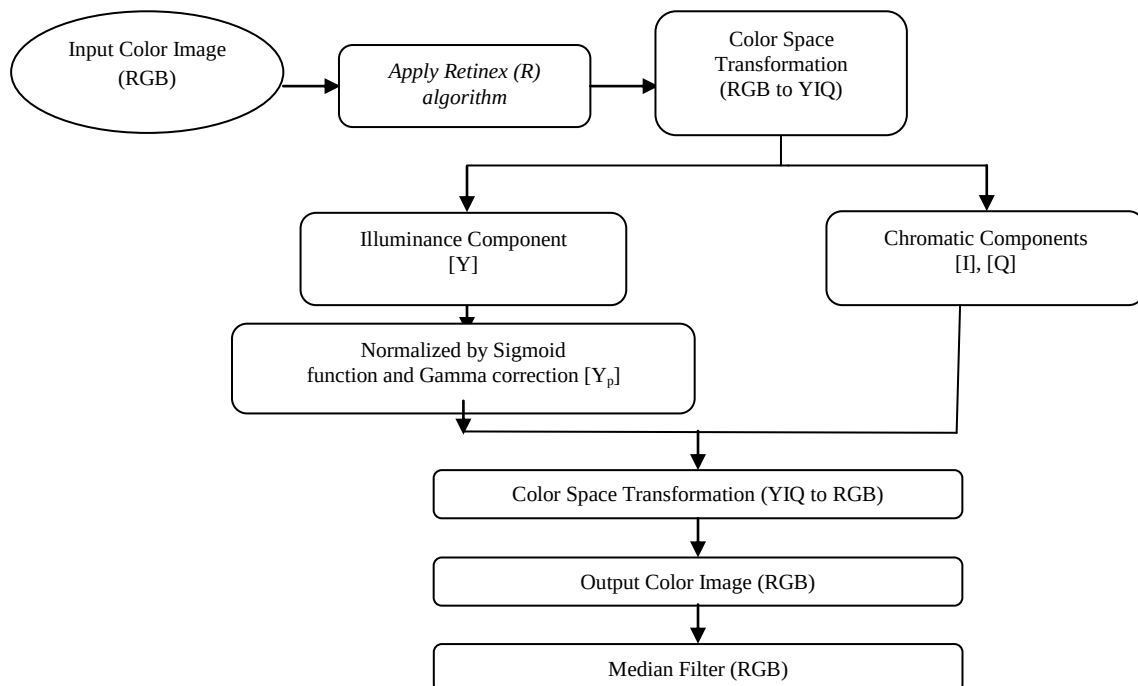


Fig.(5) Block diagram of Adaptive Retinex (AR) algorithm

7- Adaptive Retinex Algorithm (AR).

First step in this algorithm is Input color image $C(x, y)$, then apply Retinex (R) from the algorithm(1), note that the last step in algorithm(1) $[I_{pi}(x, y) = 0.35 (L(x, y, a, b) + 0.56)]$, has been adaptive in this study where underwent the principle of trial and error, so that could get the best improvement when have been changed the values to $[I_{pi}(x, y) = 0.1 (L(x, y, a, b) + 0.3)]$.

The second step transform color image from basic RGB color space to YIQ color space, the forward transform is given by Eq.(10),[16]:

$$\begin{aligned} y &= 0.299r + 0.587g + 0.114b \\ i &= 0.596r - 0.275g - 0.321b \\ q &= 0.212r - 0.523g - 0.311b \end{aligned} \quad (10)$$

Where, y is lightness component, i,q are chromatic components. Consider $I(x, y) = y = 0.299r + 0.587g + 0.114b$, then the normalized Intensity is given by:

$$I_n(x, y) = \frac{I(x, y)}{255} \quad (11)$$

Where, I_n is the normalized lightness value.

The third step is transformed normalized lightness value by using sigmoid function EQ(12) and Gamma correction by using lightness component y_t in color space that is given by Eq.(13),[17]:

$$S_n = \frac{1}{1 + \sqrt{\frac{1-I_n}{I_n}}} \quad \dots (12)$$

$$y_t = [S_n]^\gamma \quad \dots (13)$$

Optimization parameter in this study is γ gamma correction parameter, can be used value ($\gamma=0.5, 0.6, 0.7, \dots, 1.3$), and find the best gamma value. Fig.(6) shows the relationship between input lightness in versus output lightness S_n .

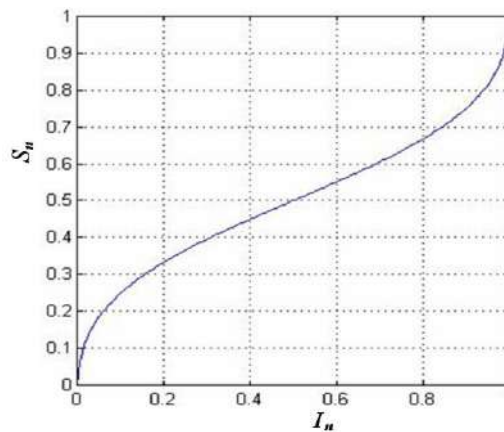


Fig.(6):Relationship between input lightness versus output lightness[16]

Then used the inverse transformation from YIQ to RGB color space

$$D_{YIQ \text{ to } RGB} = \begin{bmatrix} 1 & 0.956 & 0.621 \\ 1 & -0.272 & -0.647 \\ 1 & -1.060 & 1.703 \end{bmatrix} \quad (14)$$

Calculated in Y_pIQ that is given by [16]:

$$\left. \begin{aligned} r_p &= y_p + 0.956i + 0.621q \\ g_p &= y_p - 0.272i - 0.647q \\ b_p &= y_p - 1.106i + 1.703q \end{aligned} \right\} \quad \dots (15)$$

Finally the Retinex (R) had been applied on new component in Eq.(15), then determine median filter by Eq.(2) for the output image in RGB color component. Algorithm (2) explain the steps of sequence of adaptive Retinex (AR) enhancement, in which the work was divided into several steps, during each step includes a simplified explanation of this work.

Algorithm (2) The adaptive Retinex algorithm

Input: color image $C_i(x, y)$, $i = r, g, b$.

Step1: Apply Retinex (R) algorithm(1), depending principle of trial and error, and changed the last step in Retinex logarithm to $[I_{pi}(x, y) = 0.1 (L(x, y, a, b) + 0.3)]$.

Step2: Transform color image $C_i(x, y)$ from RGB space to YIQ space and estimated lightness component $Y(x, y)$.

Step3: Normalize the lightness component Eq.(13), (Where $\gamma = 0.5, 0.6, 0.7, \dots, 1.3$), to get best gamma correction to get y_t .

Step4: Transform color image $Y(x, y)$ from YIQ space to RGB space.

Output: The image result from components, r', g', b' .

Calculated median filter for the transform image RGB from Eq.(2) to get final enhancement image.

8- Results and Discussions

In this study have been optimize to get the best segmond function and Gamma correction based on YIQ space, Retinex algorithm of enhancement the Turbid image by adding tea Material (tea effect (n_t), where n_t is number of tea bags). New way to control intensity of light and color for the purpose of get better quality data in poor visibility environments or in general turbid images. The images which captures have been illustrated in Fig.(7), showing increased image distortion by increase the number of tea bags added, and increases with height(H) of water. It has been found for each heights(H) of water, Gamma values are used ($\gamma = 0.5, 0.6, \dots, \text{and } 1.3$) is the best Gamma is ($\gamma = 0.9$).

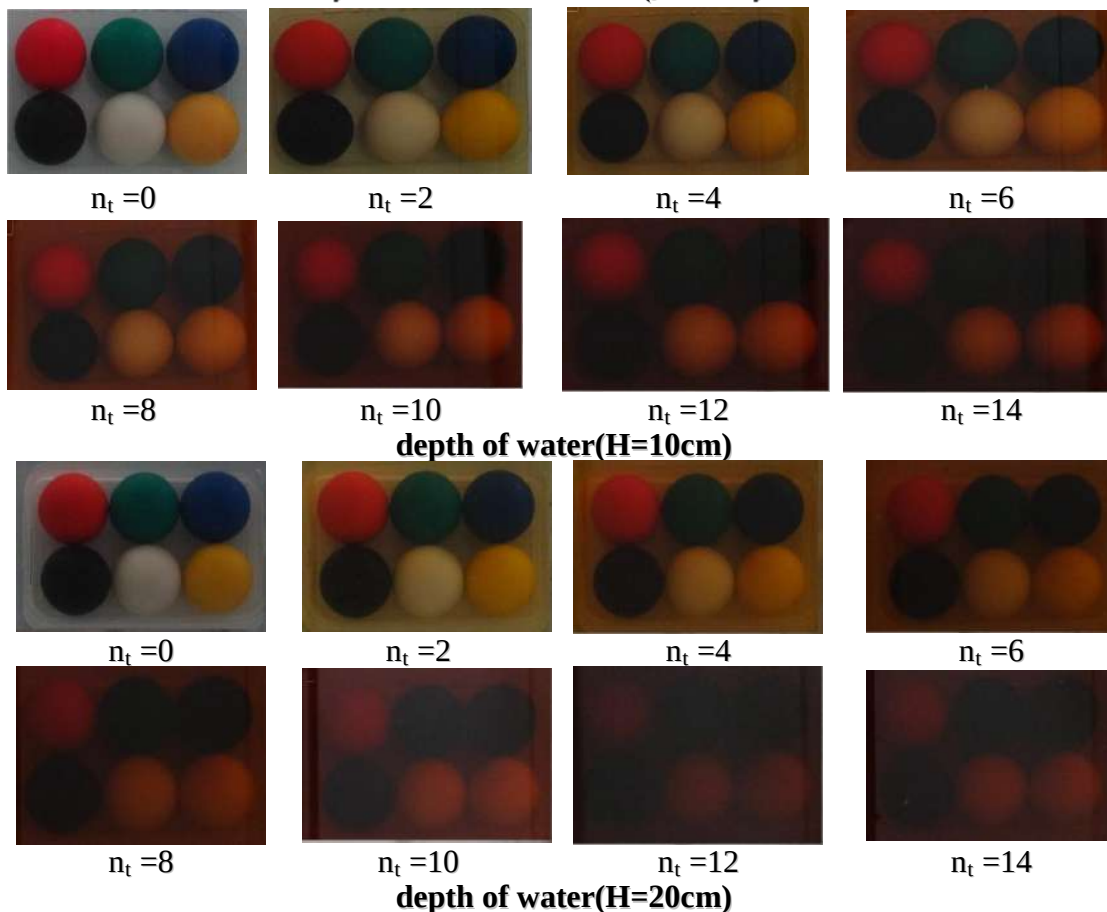
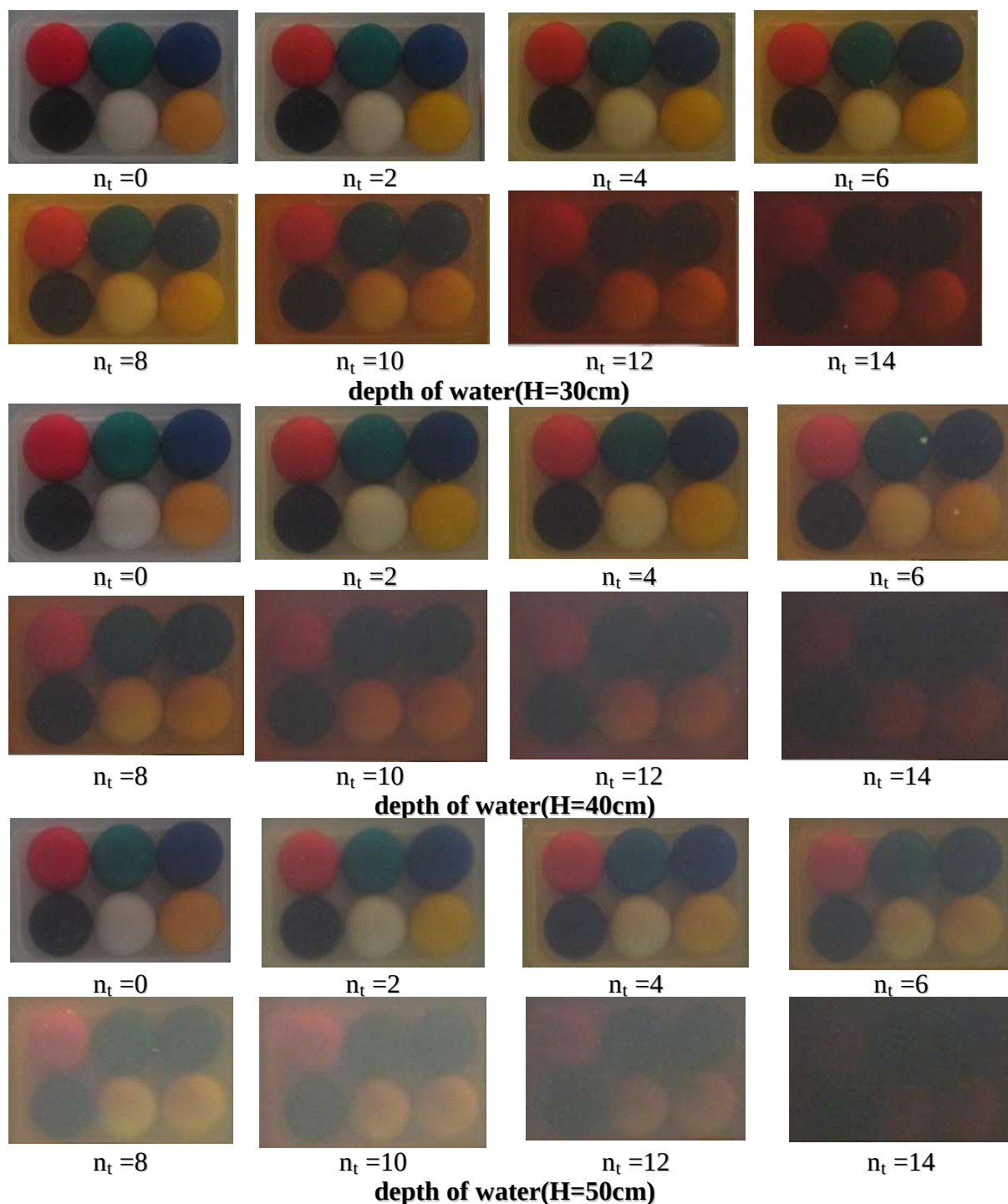
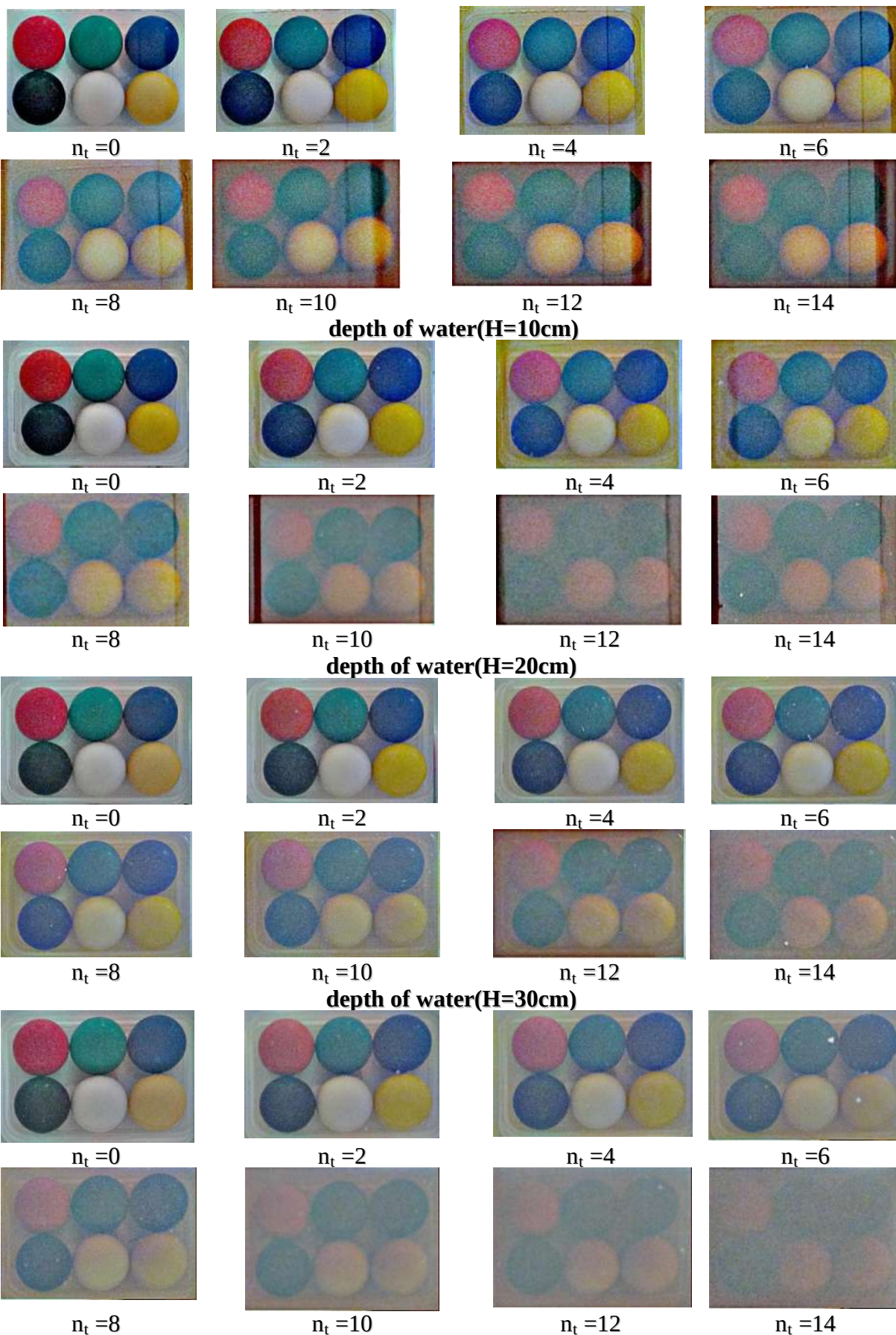


Fig.(7): The Captured images written underneath number of tea bags added(n_t),and different depth(H),Gamma=0.9



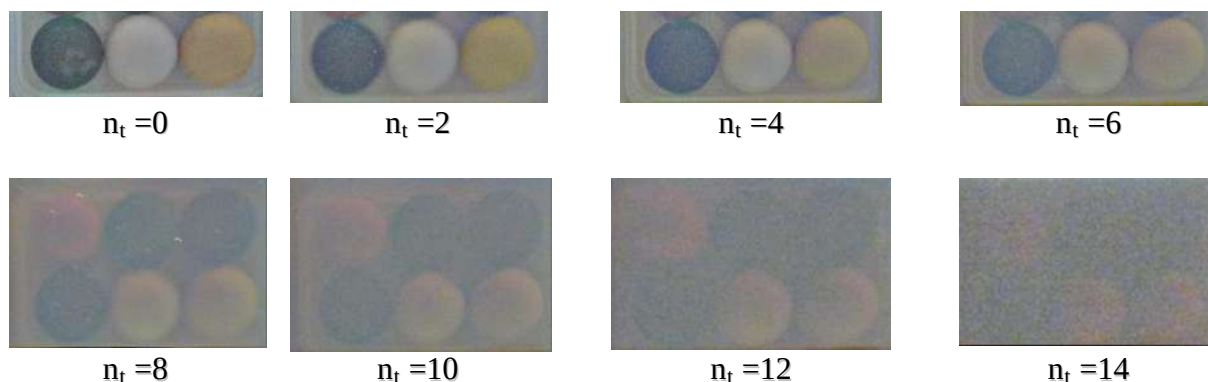
Continue Fig.(7): The Captured images written underneath number of tea bags added(n_t), and different depth(H), Gamma=0.9

The following images shows us the improvement using the Retinex(R) method at the same Gamma value contain simple improvement, and addition some noise. As noted in these images contain the contrast more than lighting, as shown in fig.(8).



depth of water(H=40cm)

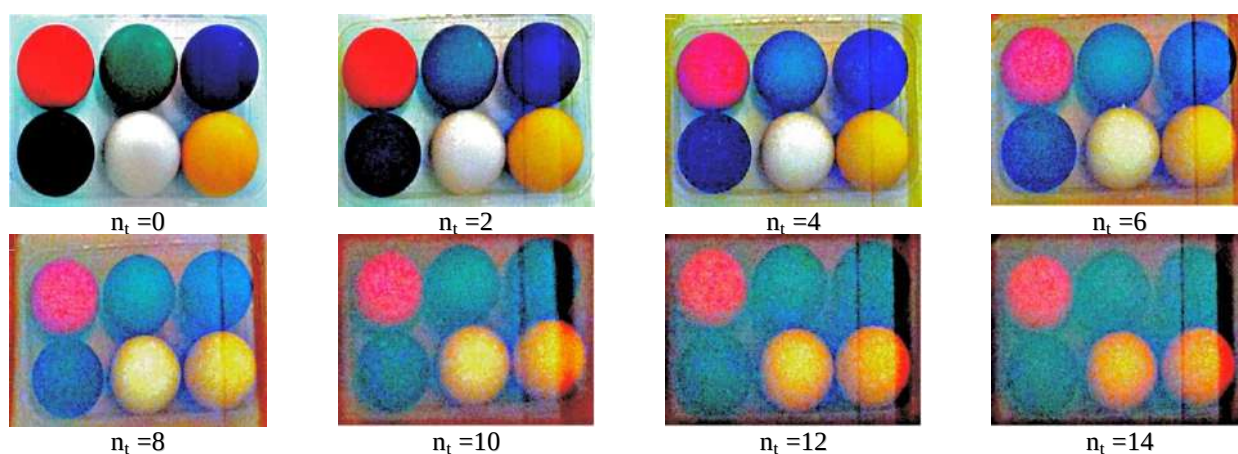
fig.(8): Enhanced images by using Retinex(R) written underneath number of tea bags added(n_t), and different depth(H),Gamma=0.9,



depth of water(H=50cm)

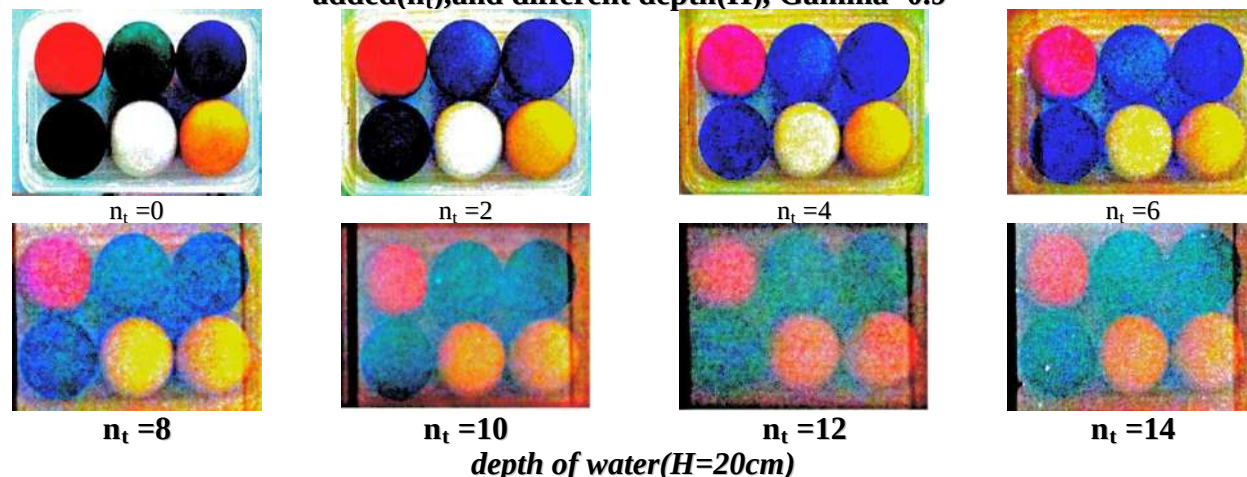
Continue fig.(8): Enhanced images by using Retinex(R) written underneath number of tea bags added(n_t), and different depth(H),Gamma=0.9

In the new method Adaptive Retinex (AR),have been surpassed defects in the Retinex method (R), Well Gamma in all cases images, and got lighting and high-contrast images, as shown in fig.(9).

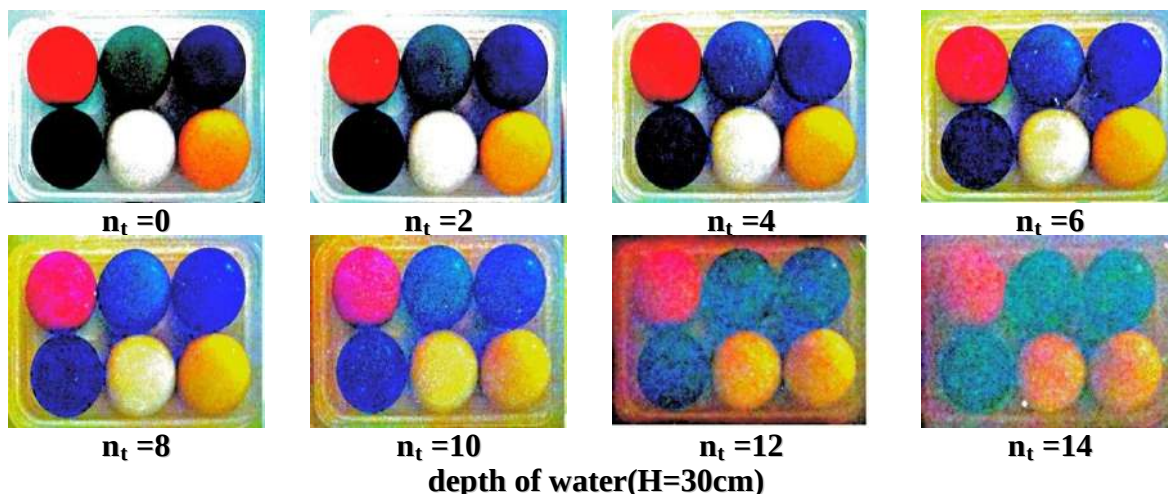


depth of water(H=10cm)

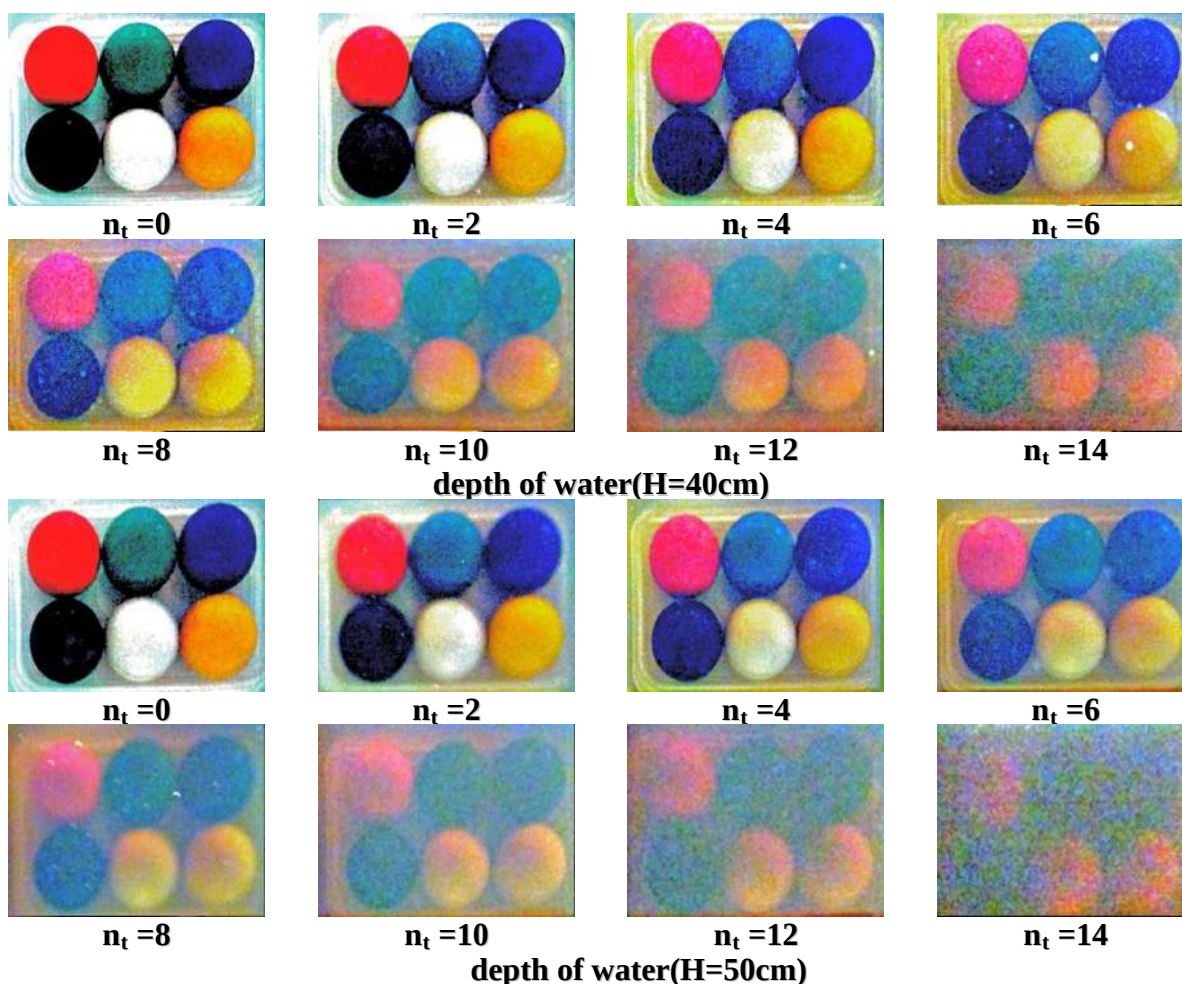
Fig.(9): Enhanced images by using (AR) images written underneath number of tea bags added(n_t),and different depth(H), Gamma=0.9



depth of water(H=20cm)



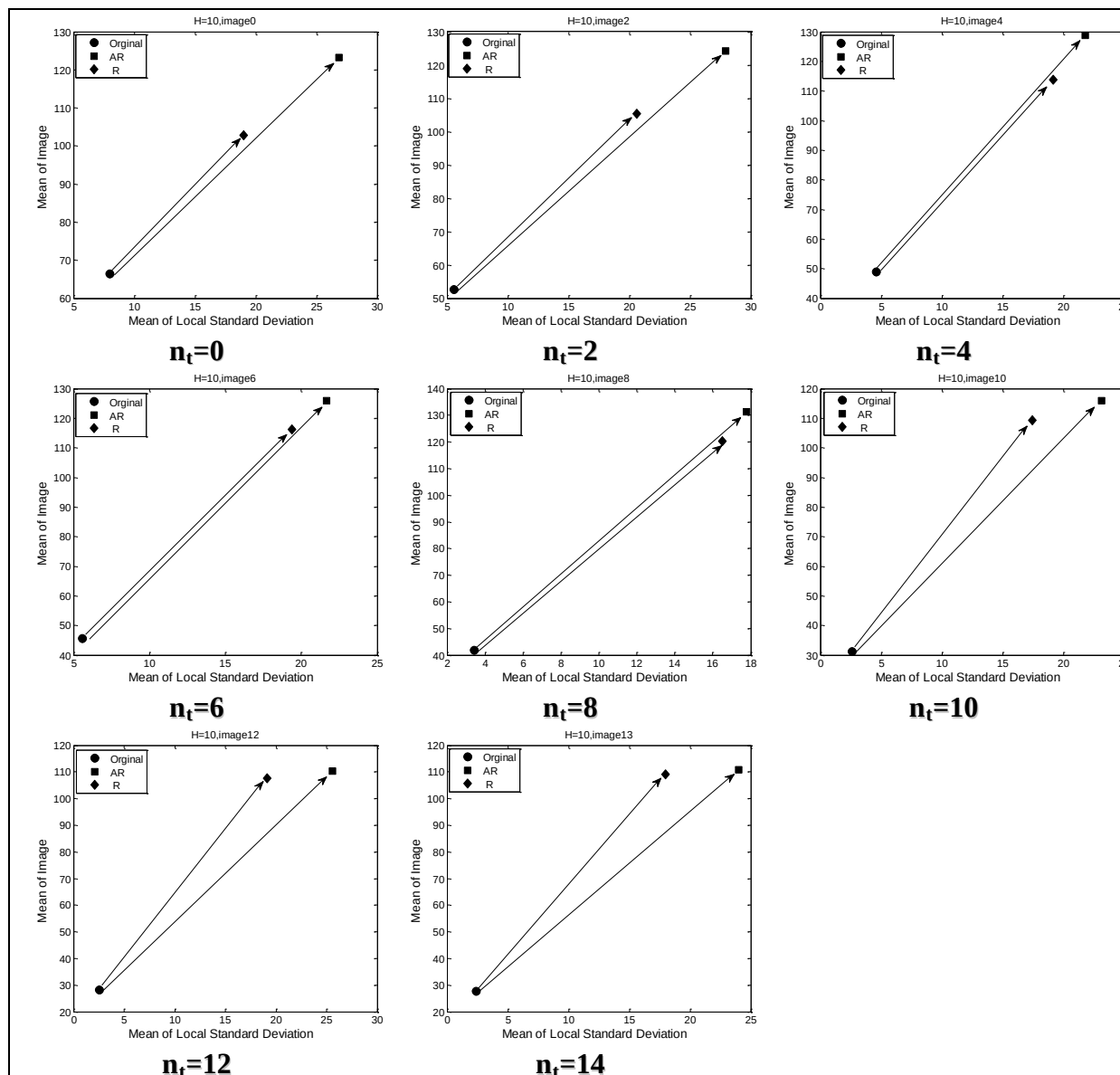
Continue Fig.(9): Enhanced images by using (AR) images written underneath number of tea bags added(n_t),and different depth(H), Gamma=0.9



Continue fig.(9): Enhanced images by using (AR) images written underneath number of tea bags added(n_t),and different depth(H), Gamma=0.9

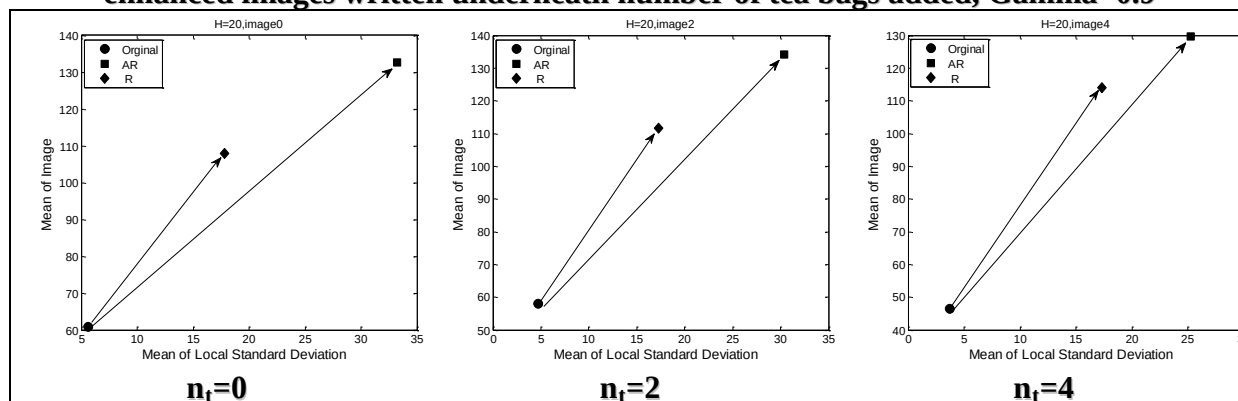
In comparison the results of suggested method (AR)with the Retinex method (R) the Relationship between mean of local standard deviations and mean of original and enhanced images in the fig.(10), noted that from shapes drawn, were able to confining, image values in the middle between

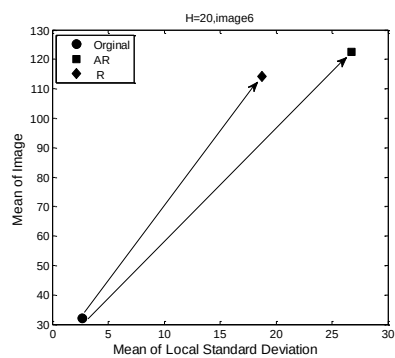
the brightness and contrast region, which represents a good vision region, the suggested method gave us a very good and highly efficient results.



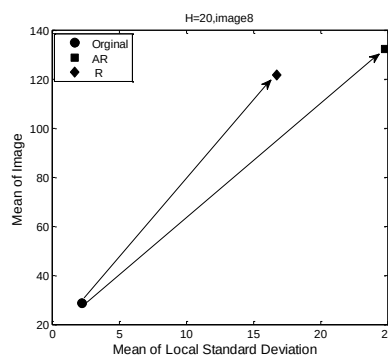
depth of water(H=10cm)

Fig.(10): Relationship between mean of local standard deviations and mean of original and enhanced images written underneath number of tea bags added, Gamma=0.9

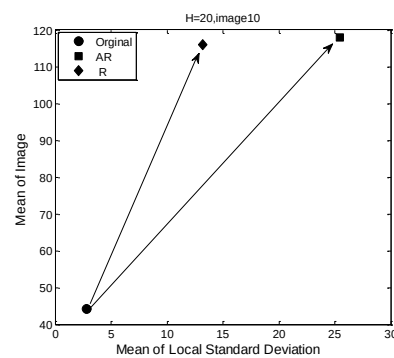




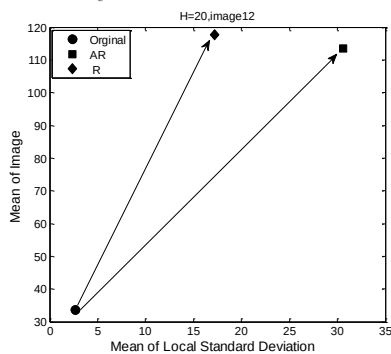
$n_t=6$



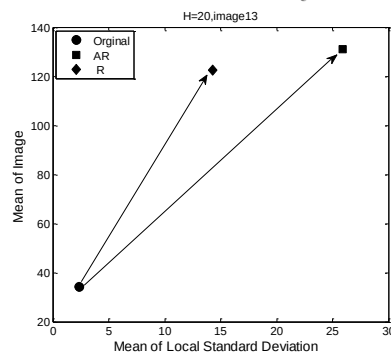
$n_t=8$



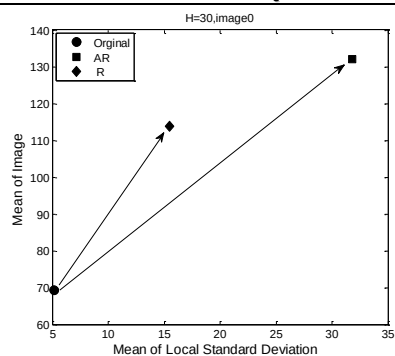
$n_t=10$



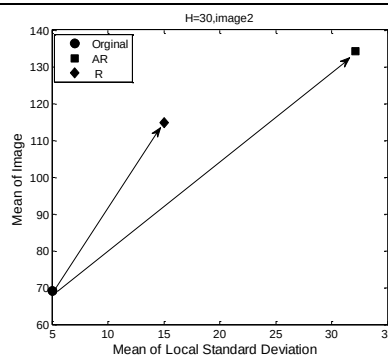
$n_t=12$



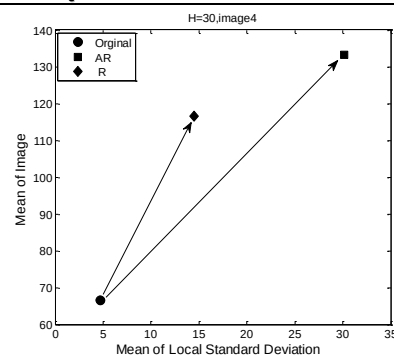
$n_t=14$



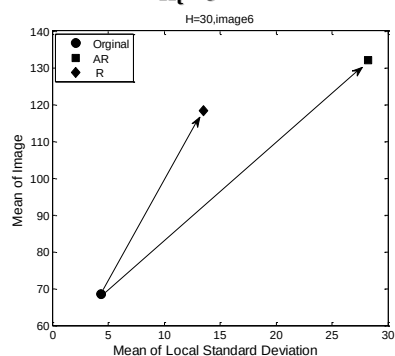
$n_t=0$



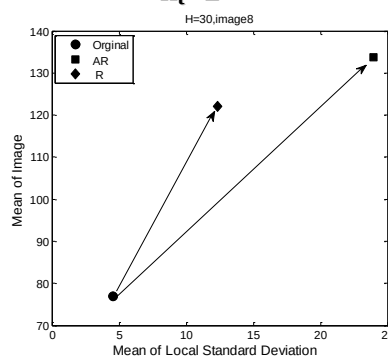
$n_t=2$



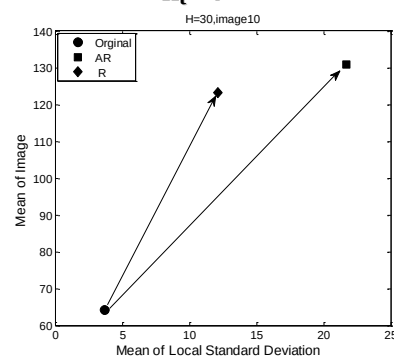
$n_t=4$



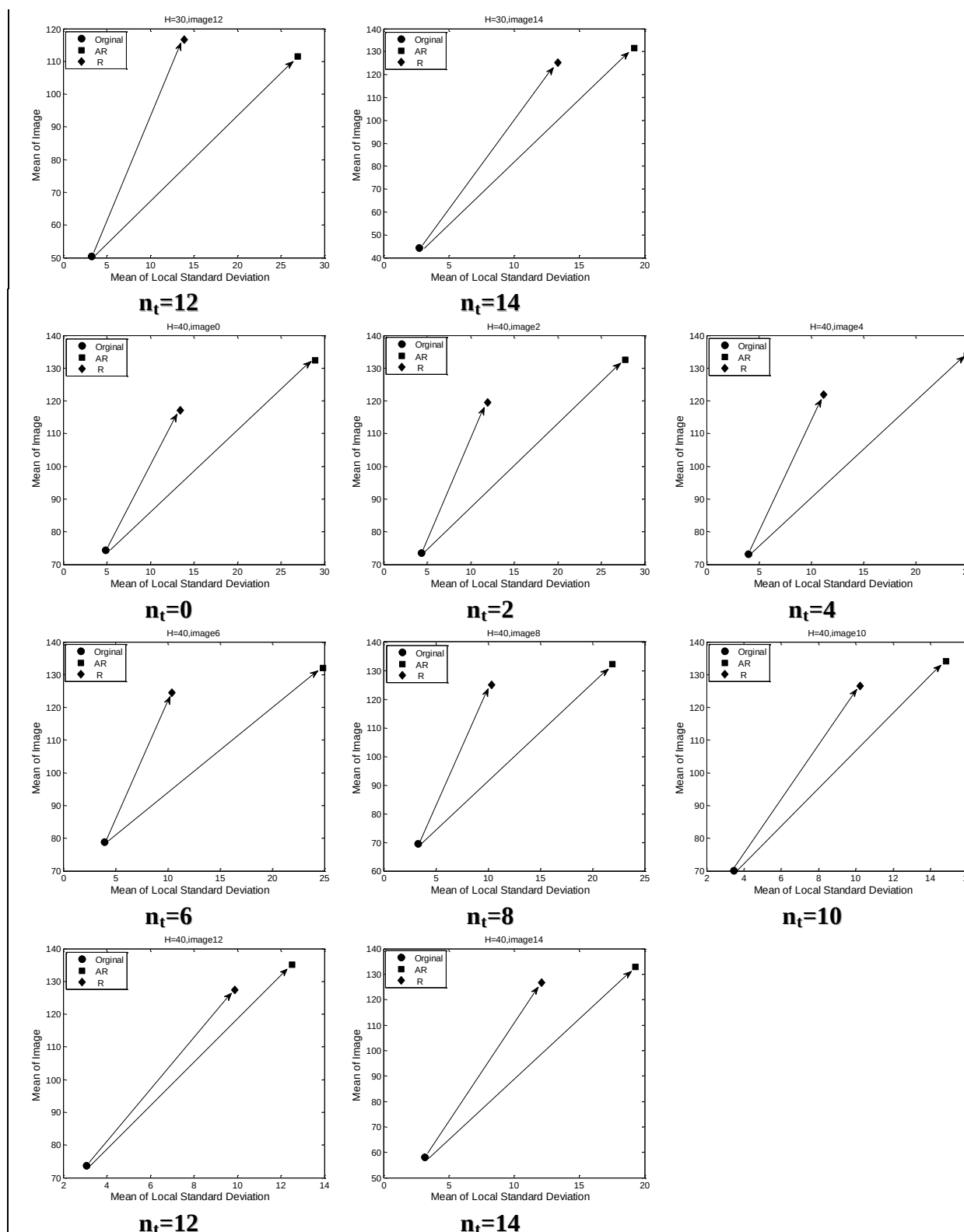
$n_t=6$



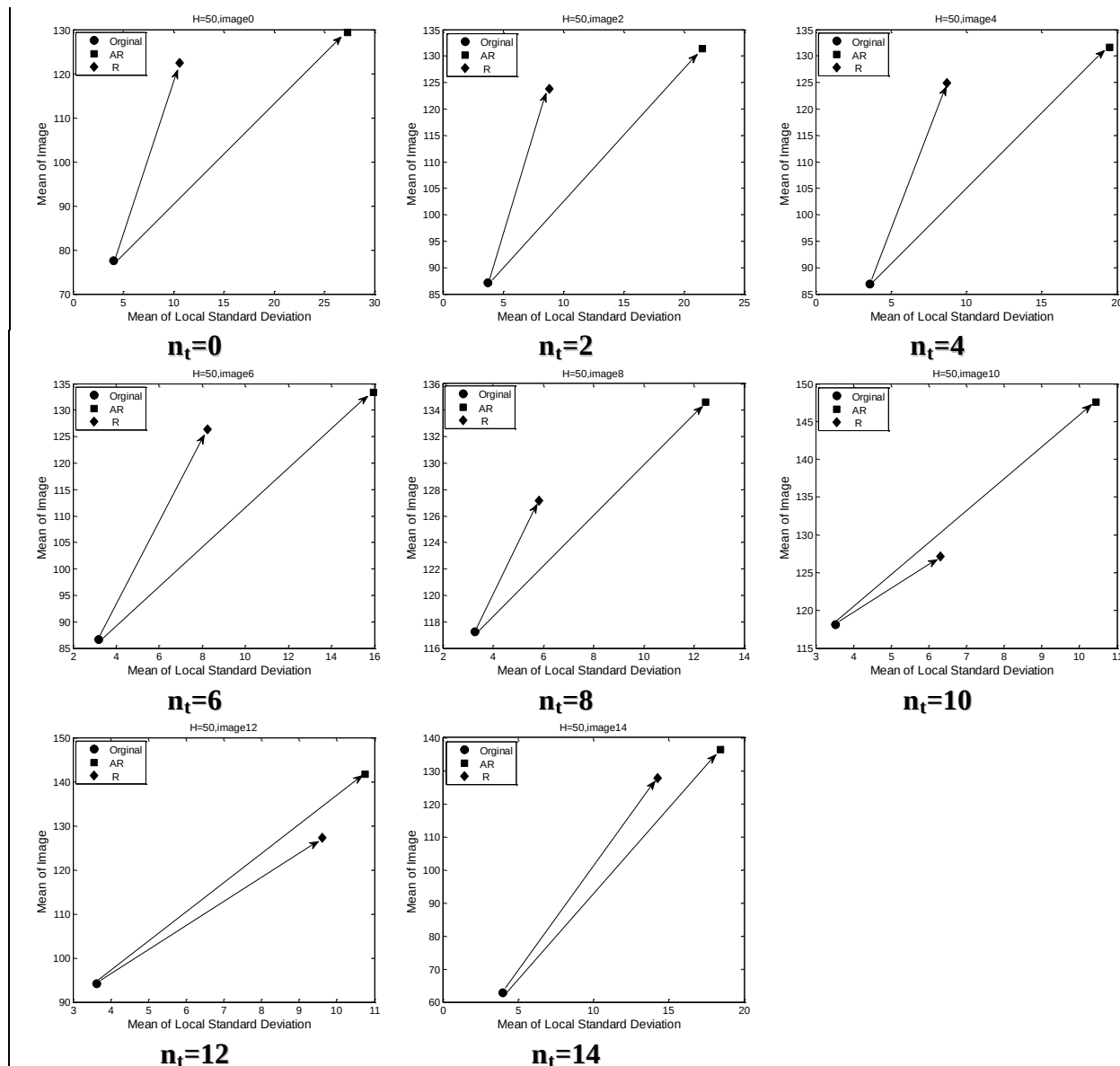
$n_t=8$



$n_t=10$



depth of water($H=40\text{cm}$)
Continue fig.(10): Relationship between mean of local standard deviations and mean of original and enhanced images written underneath number of tea bags added, $\text{Gamma}=0.9$,



depth of water(H=50cm)

Continue fig.(10): Relationship between mean of local standard deviations and mean of original and enhanced images written underneath number of tea bags added, Gamma=0.9,

7. Conclusion

Results proved through comparison between for both Retinex (R) and Adaptive Retinex (AR) methods, that the user modification (AR) is the best because, the possibility of to get the improvement and the achievement of the desired brightness and contrast of images darkness(turbid) within a good vision region for improvement all the pictures and all cases. The effectiveness of Retinex (R) algorithm for underwater image colors and this is a good indicator at process improving the image of dim lighting. The Retinex Adaptive (AR) has ability to restore and achieve a balance in colors, increase the lightness, resolution and contrast strongly in image exquisitely. The mean of locally (μ, σ) model is a good method to determine the quality of images low lightness level(dark or turbid). The points of (AR) tend to visual optimal region. The suggested method, showed that the (AR) enhancement method was improve the visibility of underwater images effectively, especially in all water deep.

References

- [1] S. S. Thakare et. al., "**Comparative Analysis of Various Underwater Image Enhancement Techniques**", April- 2014.
- [2] L. K. Chouthmol, et. al., "**Enhancement of Underwater Images by Image Fusion Using Wavelet Decomposition**", International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882, Volume 3, Issue 4, July 2014.
- [3] A. K. Vishwakarma et. al., "**Color Image Enhancement Techniques: A Critical Review**", Indian Journal of Computer Science and Engineering (IJCSE), ISSN: 0976-5166 Vol. 3 No. 1 Feb - Mar 2012.
- [4] H. G. Dway Al-Khuzai, "**Enhancement of Color Images Captured at Different Lightening Conditions**", ph. Thesis, 2011.
- [5] K. Iqbal, et.al., "**Underwater Image Enhancement Using an Integrated Colour Model**", 2007.
- [6] J. Y. Chiang, et.al., "**Underwater Image Enhancement: Using Wavelength Compensation and Image Dehazing (WCID)**", 2012, Taiwan.
- [7] P. Nurtantio, et.al., "**Underwater Image Enhancement Using Adaptive Filtering For Enhanced Sift-Based Image Matching**", 2013.
- [8] N. M. Mirza, et.al., "**Underwater Images Quality Assessment Based on the Minimum Distance Classifier (MDC) and Quality Factor Algorithms**", 2014.
- [9] B. Sandbhor, et.al, "**A Review on Underwater Image Enhancement Techniques**", IJARCSSE (2015).
- [10] J. Chen, et.al, "**Handbook of Visual Display Technology**", ISBN: 978-3-642-35947-7 (Online), 2015.
- [11] S. Kumar, et.al, "**Performance Comparison of Median and Wiener Filter in Image Denoising** ", International Journal of Computer Applications (0975 – 8887) Volume 12– No.4, November 2010.
- [12] S. J. Xie, et.al, "**Intensity Variation Normalization for Finger Vein Recognition Using Guided Filter Based Singe Scale Retinex**", *Sensors* (2015).
- [13] D. J. Jabson, et.al, "**A multi-scale retinex for bridging the gap between color images and the human observation of scenes**", *IEEE Trans. Image Processing*, (1997).
- [14] D. J. Jobson, et.al, "**Properties and performance of a center/surround retinex**", *IEEE Trans. on Image Processing*, (1996).
- [15] K. Barnard et.al., "**Analysis and Improvement of Multi-Scale Retinex**", In *Proceedings of the IS&T/SID Fifth Color Imaging Conference: Color Science, Systems and Applications*, Scottsdale, Arizona, (1997).
- [16] S. Lal, et.al., "**Automatic Method for Contrast Enhancement of Natural Color Images**", *J Electr Eng Technol*; 10(1): 30-40, 2015.
- [17] M. Gupta, et. al., "**On Controlling Light Transport in Poor Visibility Environments**", *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2008.

Modification CB (Center-to-Boundary) Filter to Remove Noises in Color Images Based on Parallel Hybrid Algorithm

Khalid Ali Hussein¹ Abed Ali H. Altaee² Haider K. Hoomod³

^{1,3}Department of computer/ Mustansiriyah University/ Baghdad –Iraq

²Department of Mathematics/ Mustansiriyah University/ Baghdad –Iraq

kah682001@yahoo.com

Abstract:

Noise Removal approach is one of the topics image enhancement. In this paper, new proposed modified filter worked on removing noise depending on the parallel hybrid algorithm to find roots of nonlinear equations, were discussed. Parallel hybrid algorithm is used to obtain two correct positive real roots of single nonlinear equations of the fourth degree to form masks for the CB filter. The results of our modification filter will be comparing with results of the original filter.

Keyword: Numerical Algorithms, Hybrid Algorithm, Finding Roots, Image Enhancement, Imaged Processing.

تعديل المرشح CB لازالة الضوضاء من صورة ملونة بالاستناد الى الخوارزمية الهجينة المتوازية

خالد علي حسين عبد علي الطائي حيدر كاظم حمود

المستخلص

نهج ازالة الضوضاء هو أحد مواضيع تحسين الصور. في هذه الورقة، تم اقتراح فلتر معدل يعمل على ازالة الضوضاء بالاستناد الى خوارزمية هجينة معدلة لايجاد جذور المعادلات اللاخطية. أن الخوارزمية الهجينة تستخدم لايجاد جذرين حقيقيين موجبين لمعادلة لاخطية من الدرجة الرابعة لتشكيل اقنعة للفلتر المعدل. النتائج التي حصلنا عليها من الفلتر المعدل تم مناقشتها ومقارنتها مع الفلتر الاصلي.

1. Introduction

Imaged enhancement is then processed of applying techniques to facilitate the development off a solution to a computer imaging problems. Applications like scientific, industrial, and military can improve its view by denoising, emphasize and sharpen image feature. In addition image enhancement methods are used to make images look better. [1]

Numerical analysis is a very important branch of computer science that deals with the study of algorithms that use numerical approximation in mathematical analysis. It involves the study of methods of computing numerical data. It has its applications in all fields of engineering and the sciences [2].

The algorithms in that study uses in several applications like as, uses bisection method in electrical engineering [3], and implemented on an electrical circuit element, also uses in image processing to adaptive filters, like as [4] using Newton-raphson method to improve two novel algorithms CB (Center-to-Boundary) and BB (Boundary-to-Boundary) filters.

In this paper, we introduce modification of CB filter based on parallel hybrid algorithm to find real correct roots used to constructed masks to this filter from a lot of polynomial equations.

2. CBs (Centers – to o- Boundary) Filter. [4]

Inn CBs filtered; pixels area scanned from Centers too boundary's too calculated the distanced between themes buy using Newton-Raphson formulas. They Newton-Raphson method is a powerfully techniques forms solved equations numerically. The Newton-Raphson formulas it's based own they equations (1) ask given bellow:

$$x_j = x_i - [f(x_i) / df(x_i)] \dots\dots (1)$$

Where: $f(x_i) = x^2 - x - 1$; $df(x_i) = 2x - 1$; x_i = central pixel

x_j = neighboring pixel of x_i

Explain method: let $f(x) = x^2 - x - 1$, $df(x) = 2x - 1$ and apply Newton-Raphson method to find two iterative.

First iterative: $x_j = x_i - [f(x_i) / df(x_i)] = 1 - [-1 / 1] = 2$

Second iterative: $x_j = x_i - [f(x_i) / df(x_i)] = 2 - [1 / 3] = 1.67$

The first iterative (2) fills the locations a_{12} , a_{21} , a_{23} and a_{32} , while the second iterative (1.67) fills the locations a_{11} , a_{13} , a_{31} , a_{33} as shown in figure (1).

1.67	2	1.67
2	1	2
1.67	2	1.67

Fig. (1): (3x3) mask of CB filter

3. Root-finding Algorithm

The root-finding problem is one of the most important computational problems. It rises in a wide variety of practical applications in mathematics, physics, chemistry, biosciences, engineering, etc. As a matter of fact, determination of any unknown appearing implicitly in scientific or engineering formulas gives rise to a root-finding problem. A root-finding algorithm is a numerical method to finding a value x such that $f(x)=0$, for given function f . Numerical root-finding methods use iteration, producing a sequence of numbers that hopefully converge towards a limit (the so-called "fixed point") which is a root. The first values of this series are initial guesses. The method computes subsequent values based on the old ones and the function f . [2]

3.1 Parallel Hybrid algorithm. [5, 6]

This algorithm compute the roots of nonlinear equations $f(x)=0$, by propose hybrid algorithm between the Bisection algorithm and Newton-Raphson algorithm. It's take a first approximation by apply two times the Bisection method and complete a correct approximation by use the Newton-Raphson method, and convert it to parallelism by distributed the first approximation in k^{th} intervals for k^{th} cores with finding images of intervals ends in parallel, also the results comes from first parallel algorithm enter in the second parallel approximation by finding $f(x)$ & $df(x)$ in k^{th} intervals in parallelism.

Given f , df , $a[k]$, $b[k]$ and δ (tolerance)

Step 1: do in parallel for four roots

Step 2: for $i=1$ to 2

Step 3: $x_i = (a[k] + b[k]) / 2$

Step 4: compute $f(x_i)$ and $f(a[k])$ in parallel

Step 5: If $f(x_i) = 0$ or $f(x_i) < \delta$, then step 15

Step 6: If $f(a) * f(x_i) < 0$, then $b[k] = x_i$

Step 7: Else $a[k] = x_i$

Step 8: end for

Step 9: for $i = 1$ to n

Step 10: do in parallel compute $f(x_i)$ and $df(x_i)$

Step 11: $x = x_i - f(x_i) / df(x_i)$

Step 12: If $f(x_i) < \delta$, then go to step 15

Step 13: $x_i = x$

Step 14: end for

Step 15: stop iteration.

4. Proposed Modified CB (Center to Boundary) Filter

Krishan and others in [4] presented CB (center to boundary) filter, this section proposed a modified CB (center to boundary) filter by using two equations as form $f(x) = ax^4 + bx^3 + cx^2 + dx + e$ (Quartic Function):

$$1x^4 - 4x^3 + 2.9x^2 + 2.5x - 2 = 0 \dots\dots\dots (3)$$

$$x^4 + 3x^3 - 5x^2 - 2x - 1 = 0 \dots\dots\dots (4)$$

By applying the **Parallel Hybrid Method** to find the real positive correct roots of these equations, then pick from eq. (3) the root $x_1 = 1.4251$, and from eq.(4) the root $x_2 = 1.5037$, construct the 3x3 mask table (1), as follows, we set in $a_{22} = 1$, and fill the positions in mask a_{11} , a_{13} , a_{31} , a_{33} by the

correct root from the eq.(4) $x_1 = 1.4251$, fill the positions of mask table (1), a_{12} , a_{21} , a_{23} , a_{32} by the correct root from the eq.(4) $x_2 = 1.5037$, similarly construct three masks like as table (2).

Table (1) 3×3 Mask for Modified Filter

1.4251	1.5037	1.4251
1.5037	1	1.5037
1.4251	1.5037	1.4251

Table (2) Masks Yield from Parallel Hybrid Method

No. of Mask	The mathematical formula of the equation	3×3 mask		
1	$x^4 - 4x^3 + 2.9x^2 + 2.5x - 2 = 0$ $x^4 + 3x^3 - 5x^2 - 2x - 1 = 0$	1.4251	1.5037	1.4251
		1.5037	1	1.5037
		1.4251	1.5037	1.4251
2	$x^4 - 4x^3 + 2.9x^2 + 2.5x - 2 = 0$ $x^4 - 4x^3 + 2.8x^2 + 2.6x - 1.9 = 0$	2.6661	2.7062	2.6661
		2.7062	1	2.7062
		2.6661	2.7062	2.6661
3	$x^4 + 4x^3 + 3x^2 - 5x + 1 = 0$ $x^4 + 4x^3 - 3x^2 - 5x + 1 = 0$	0.5791	1.2267	0.5791
		1.2267	1	1.2267
		0.5791	1.2267	0.5791

Table (3) Modified CB Values of PSNR, MSE, RMSE and SNR with Noise Ratio 5%

Images	Mask NO.	CB filter				Modify CB filter			
		PSNR	MSE	RMSE	SNR	PSNR	MSE	RMSE	SNR
Image 1	1	44.277	24.533	4.053	24.556	49.864	9.492	3.080	29.854
	2	=	=	=	=	51.279	7.387	2.717	30.943
	3	=	=	=	=	38.789	67.496	8.215	21.335
Image 2	1	38.088	76.421	8.741	23.278	40.530	49.586	7.041	24.157
	2	=	=	=	=	40.642	48.608	6.972	24.243
	3	=	=	=	=	33.642	167.95	12.959	19.858
Image 3	1	34.715	116.33	10.786	22.796	37.176	89.814	9.477	23.919
	2	=	=	=	=	37.122	90.685	9.522	23.878
	3	=	=	=	=	31.193	259.14	16.098	19.317
Image 4	1	39.380	60.787	7.796	24.636	42.294	36.278	6.023	26.878
	2	=	=	=	=	42.483	34.084	4.923	27.023
	3	=	=	=	=	34.166	153.06	12.372	20.626
Image 5	1	44.549	24.332	4.932	27.081	46.994	14.780	3.972	28.962
	2	=	=	=	=	47.116	14.442	3.929	29.056
	3	=	=	=	=	38.262	74.093	8.607	22.245
Image 6	1	43.594	28.819	4.368	24.836	44.938	19.025	4.361	26.639
	2	=	=	=	=	44.756	19.649	4.432	26.499
	3	=	=	=	=	39.192	62.848	7.927	21.450

Table (4) Modified CB Values of PSNR, MSE, RMSE and SNR with Noise Ratio 15%

Images	Mask No.	CB filter				Modify CB filter			
		PSNR	MSE	RMSE	SNR	PSNR	MSE	RMSE	SNR
Image 1	1	43.707	28.247	4.314	24.118	49.639	9.878	3.142	29.681
	2	=	=	=	=	50.855	7.963	2.822	30.616
	3	=	=	=	=	36.413	102.81	10.139	19.507
Image	1	37.892	79.124	8.895	23.127	40.475	50.067	7.075	24.115

2	2	=	=	=	=	40.582	49.128	7.009	24.197
	3	=	=	=	=	32.200	216.82	14.725	18.749
Image 3	1	34.452	121.88	11.040	22.593	37.147	90.271	9.501	23.897
	2	=	=	=	=	37.104	90.964	9.537	23.864
	3	=	=	=	=	29.794	332.01	18.221	18.241
Image 4	1	39.030	64.678	8.042	24.367	42.241	36.620	6.051	26.837
	2	=	=	=	=	42.418	34.491	4.957	26.973
	3	=	=	=	=	32.469	206.75	14.379	19.320
Image 5	1	43.608	28.743	4.361	26.358	46.865	16.146	4.018	28.862
	2	=	=	=	=	46.994	14.779	3.972	28.962
	3	=	=	=	=	34.803	114.53	10.702	20.354
Image 6	1	43.137	31.248	4.590	24.484	44.858	19.298	4.393	26.577
	2	=	=	=	=	44.693	19.868	4.457	26.451
	3	=	=	=	=	37.253	88.595	9.412	19.958

Table (5) Modified CB Values of PSNR, MSE, RMSE and SNR with Noise Ratio 35%

Images	No. of mask	CB filter				Modify CB filter			
		PSNR	MSE	RMSE	SNR	PSNR	MSE	RMSE	SNR
Image 1	1	24.295	334.73	18.295	20.317	29.128	106.25	10.308	24.470
	2	=	=	=	=	29.635	91.285	9.554	24.020
	3	=	=	=	=	19.796	173.62	13.176	14.360
Image 2	1	22.217	84.113	18.421	19.051	23.895	50.892	7.133	20.870
	2	=	=	=	=	23.961	49.894	7.063	20.941
	3	=	=	=	=	17.754	319.89	17.885	14.217
Image 3	1	20.695	132.64	11.517	18.522	21.932	91.594	9.570	19.862
	2	=	=	=	=	21.910	92.189	9.601	19.838
	3	=	=	=	=	16.472	376.32	19.399	13.947
Image 4	1	22.702	72.728	8.528	19.881	24.895	37.723	6.141	22.257
	2	=	=	=	=	24.988	36.697	6.057	22.357
	3	=	=	=	=	17.835	312.21	17.669	14.608
Image 5	1	24.973	36.854	6.070	21.065	27.570	169.425	13.016	23.878
	2	=	=	=	=	27.718	162.03	12.729	24.039
	3	=	=	=	=	19.441	193.07	13.895	14.072
Image 6	1	24.077	34.728	4.977	19.919	27.047	198.126	14.075	22.053
	2	=	=	=	=	26.970	202.70	14.237	21.970
	3	=	=	=	=	20.489	141.078	11.877	14.948

Imaged 1	Imaged 2
	
Imaged 3	Imaged 4
	
Imaged 5	Imaged 6
	

Fig. (2): The Tested Images

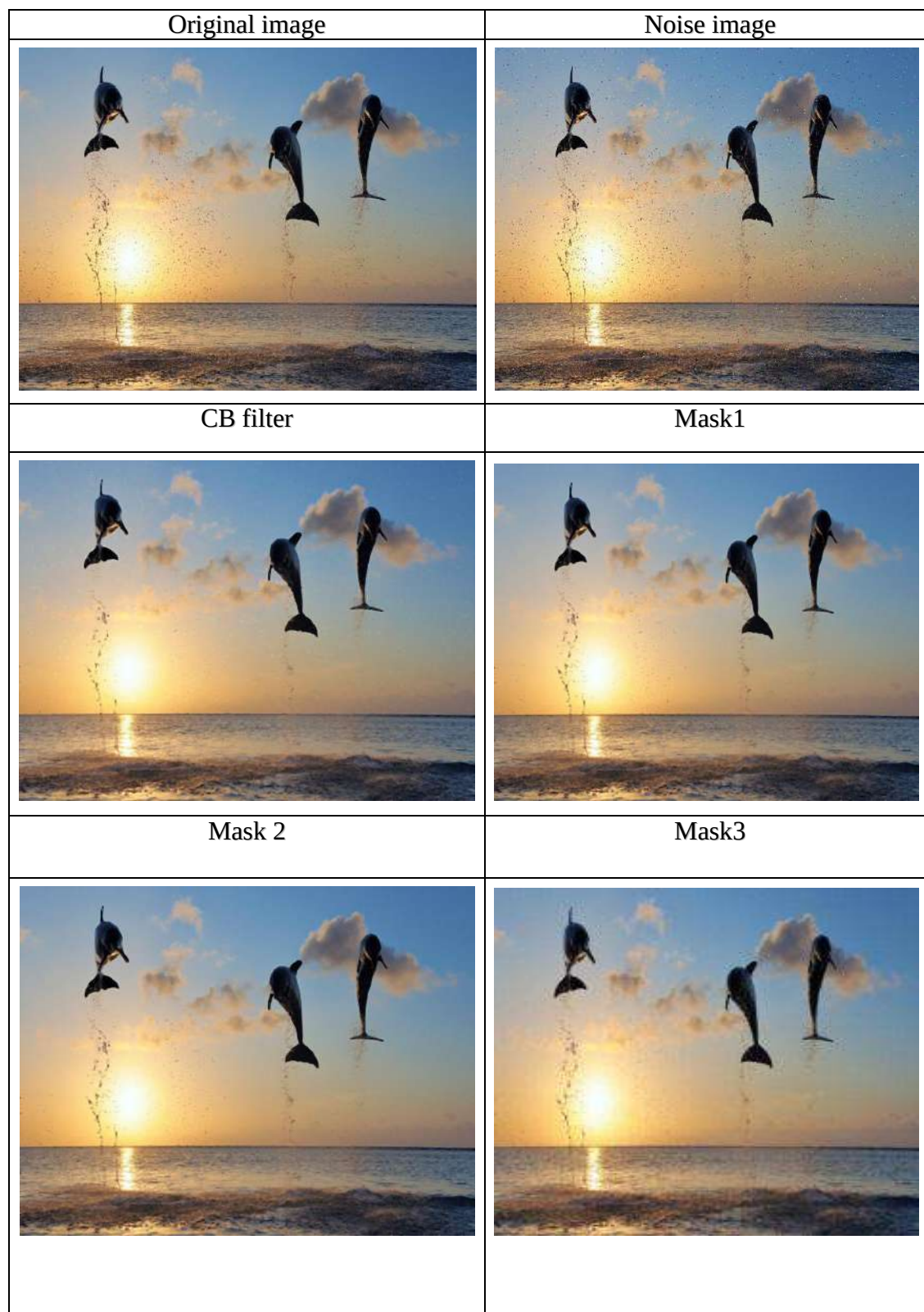


Fig. (3): The Images Denoising 5% Ratio of Image (3)



Fig. (4): The Images Denoising 15% Ratio of Image (3)

Original image	Noise image
	
CB filter	Mask1
	
Mask2	Mask3
	

Fig. (5): The Images Denoising 35% Ratio of Image (3)

V. Results and Discussions

In testing, modified CB filter uses more than 100 colors images and case study from 6 images in three stages of noises 5%, 15% and 35% of salt and pepper noise, from tables (2), (3) and (4) for values of PSNR, MSE, RMSE and SNR we get the following results:

- The researchers prove in [4] the results off novel CBs filtered area much better thanes they averages (mean) filter, because the MSEs values off CBs filters are less than averages filters and the PSNRs values off CBs filters are much higher thanes averages filters that its necessary for goods enhanced imaged.
- The mask (1) and mask (2) used in proposed Modify CB filter show that they are better than CB filter for good enhanced images, the PSNR values of modify CB filter is higher than novel CB filter, and they MSE values off modify CBs filters less thank CB filtered.

References

- [1] Gonzalez R.C. and Woods R. E., "**Digital image processing**", second edition, Includes bibliographical references ISBN 0-201-18075-8, 2002.
- [2] R.L. Burden, J.D. Faires, Numerical Analysis, 9th Edition, Brooks/Cole, 2011.
- [3] S. E. Umbauch, "**Computer Vision and Image Processing and A Practical Approach Using CVIP Tools**", Prentice Hall PTR, Upper Saddle River, NJ 07458, June 1999.
- [4] Krishan K.L., Shivali, Rajiv K., "**Image Enhancement Using Filtering Techniques**", International Journal on Computer Science and Engineering (IJCSE), Vol.4, No. 1, PP. 14-20, 2012
- [5] Khalid A. Hussein, Abid Ali H. Alta'ai, Haider K. Homood, "**A New Approach to Find Roots of Nonlinear Equations by Hybrid Algorithm to Bisection and Newton-Raphson Algorithms**", Iraqi Journal of Information Technology, ISSN:1994-8638, vol. 7 No.1,2015.
- [6] Khalid A. Hussein, Abid Ali H. Alta'ai, Haider K. Homood, "**Parallel Hybrid Algorithm of Bisection and Newton-Raphson Methods to Find Non-Linear Equations Roots**", IOSR Journal of Mathematics (IOSR-JM), e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 11, Issue 4 Ver. II (Jul - Aug. 2015), PP 32-36.

Iris Recognition Based on fusion of Multi-features

Rafid. E. Haleot kawther. T. Saleh Raniah Ali Mustafa Haitham S. Chyad
Computer Science Dept., College of Education, University of Mustansiriyah
rafidalkenany@yahoo.com, kawtherthabt@uomustansiriyah.edu.iq
Raniah Ali Mustafa, hchyad88@yahoo.com

Abstract:

The iris recognition system is topic to a comparatively biometric advanced technology. Numerous usages might rely on this propose system, such that commercial, personal security. This system can equipping appropriate for high security environments. Experimental results show that the algorithm is effective and adjusts with the environment, e.g. it doing well even for inconstant illumination, interpenetrate of eyelashes and eyelids, and disfigured iris images. This paper presents the development and implementation of Iris recognition system based on feature-level fusion. Gabor wavelet transform and 2D discrete cosine transform used in stage of feature extraction and Fusion. Probabilistic Neural Network (PNN) is used in the classification stage. The proposed approach is tested on a CASIA eye image database of version 4.0. Experimental results show that our approach offer best detection accuracy for fusion of Multi-feature is much better than the performance of Iris recognition using only one type of feature. The maximum success of 99.8% recognition has been achieved.

Keywords: Iris recognition, feature Fusion, Gabor wavelet transform, 2D discrete cosine transform, Probabilistic Neural Network (PNN).

1. Introduction

Iris recognition system is a well-known of the most unassailable systems for identity of individuals [1]. Compared with other biometrics systems; iris recognition system is a relatively novel biometric system and attain better results like retina, voice, fingerprint face e.t.c. [2]. Fundamental iris recognition procedures comprise mainly four phases:

- Image acquisition: catching an eye picture take from camera that has a high resolution specifications.
- Image preprocesses (IP): noise removal, normalization and Localization of eye image.
- Feature extraction (FE): to extract the most distinguished characteristic from iris.
- Matching: using an iris template to compare in the dataset verification

Notice fig-1 shown Block diagram of iris recognition system. Iris feature extraction (IFE) is utilized for extracting roughly distinguish characteristic in images iris. t is a specific form of dimensionality reducing and comprises roughly of the information of an iris image in the database original. The feature is extracted feature coefficient and then is encoded for comparison among templates can be done correctly and easily.

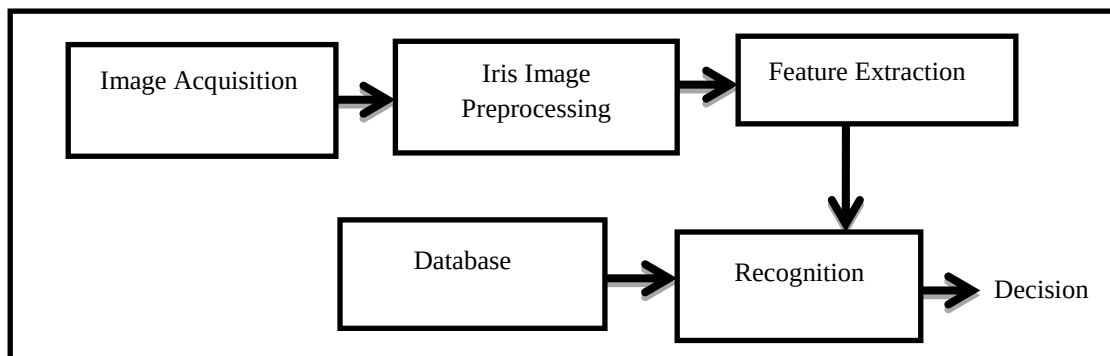


Fig.(1): Iris recognition system

Feature extraction (FE) extractor the roughly distinguished characteristics existing in an image. It equipping each global and local information of iris image. Distinguished iris texture information should be extractor and encoded to have true comparisons among iris image templates. Complication of feature extraction effectiveness the complication of program and handling speed of iris recognition system.

2. Related Works

A summarized of several journals/articles, supplying information concerning various feature extraction technicality in iris recognition system is offered presently.

1- Yong Zhang and Yan Wo [3], [2015] has suggested a novel technique for iris features extraction. He presented a novel technique for iris feature extraction. Through utilizing 2D and 1D log Gabor filter. 2D Gabor filter extractor stage information as 2D and 1D log Gabor filter extractor stage information as 1D. Hamming distance is utilized for the matching of feature vector. He ae well suggested Fisher's linear discriminate (FLD) to estimate weights of gathering. IITD database is utilized for immediate experiences which has 224 subjects, every subjects comprises 10 images. Upon experience, this technique products satisfying results as precision was 98.921 which is best than 2D and 1D log-Gabor filter single.

2- Charles O Ukpai [4], [2015] has offered a new method for iris feature extraction. It is rely on base texture pattern and double tree composite wavelet transform. The base orientation of the iris texture utilizing base ingredient analysis is calculated and an angle of base orientation is gained. After that composite wavelet filter are constructed which are located in the orientation of base orientation and opposite orientation image is decomposed into 12 sub band utilize double tree composite wavelet transform. The highest recognition rate of 98.86 % has been accomplished by the applied algorithm.

3- In his paper [Tze Wang [5], 2010] has utilized Haar wavelet decomposition manner to analysis the pattern of iris. The suggestd iris recognition system has two major module that are feature extraction and iris matching. Haar wavelet transform is selection for computational plainness in feature extraction. To product conformable coefficients, iris images are filtered utilize high pass filter and low pass filter for four times. The matching distance algorithm utilize is hamming distance and database is of CASIA. The recognition rate of 98.45% is accomplished utilizing this algorithm.

4- [Kshamaraj Gulmire and Sanjay Ganorkar [6], 2012] suggested the paper "Iris recognition using Gabor wavelet for feature extraction in iris recognition system". The two dimensional Gabor filter was structure and the image was filtered. The stage information created from the filter was encoded into 2048 bits. It is found to be convenient for texture impersonation. The iris database utilized in this research is CASIA iris database. The hamming distance is utilized for matching purpose.

5- In this paper [Amir and Hamid] [7] has progressing an iris feature extraction manner rely on Contourlet transform. The substantial geometrical portion of iris is taken into consideration and decomposed into a set of orientation sub bands. The sub-band with texture information are apprehend in various direction at differents scales to decrease the orientation of feature vector. It extracts only important bit and information from normalized iris image. The matching of iris template is done by hamming distance. The suggested algorithm has accuracy level of 94.2%.

6- [J. Daugman [1], 2004] utilized Gabor filter for extracting features of iris images which have various sets of frequencies and different directions that can be utilized for extracting helpful information from iris images. He demodulated the result produced by convolving the Gabor filter by phase quantization in order to decrease the amount of data that was produced. A biometric template was formed by quantizing stage information into four levels. The number of bits utilized for compares was 2048.

In this paper, we propose a feature-level fusion, consisting of two types of features: Gabor wavelet transform, 2D discrete cosine transform.

3. Dataset

To acquisition an eye image this is requirement to treat taking an obvious and perfect image with the assist of digital camera with high resolution. Here we utilize the database CASIA eye image of version 4.0 has been employed for enforcement our assignments because this set of images comprises a good details to extract features and don't contain shining reflexions [8].

4. Research Methodology

Iris recognition system (IRS) comprised of diverse sub-systems that are feature extraction (FE), matching, localization and normalization of features template as be seen in Fig-2. The aim of analyses and to increase the rise system achievement, the original iris image requirements to be pre-processed. The contain preprocessing of the following stages normalization and localization of iris images. In addition also comprises the elimination of undesirable noise existing in the system. One of the most significant pre-processing stages is to insulate the current iris portion of digital image in demand to eliminate each irrelevant portion. After that normalization is utilized in demand to have stable dimensions of iris images.

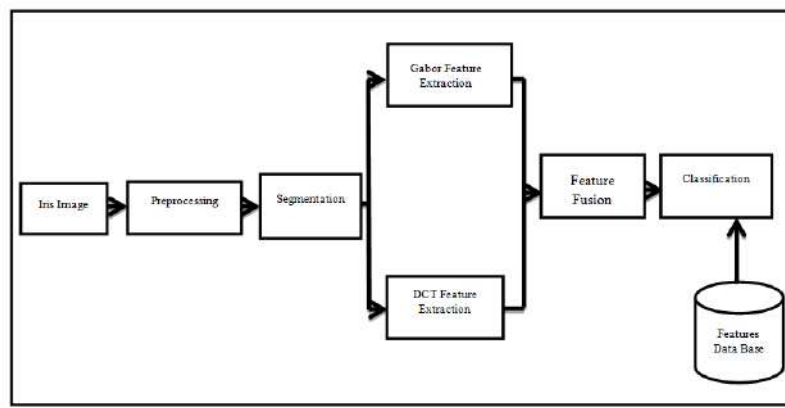


Fig.(2): Purposed methodology steps

4.1 Iris Localization

One of the most significant stages in iris recognition system is Iris localization. It is utilized for determination the internal and external confines of iris. An eye consists of pupil, sclera and iris. Sclera is white in color and is out of iris. Pupil is inner iris and its size variations due to density of illumination decline on it. Iris comprises texture information, so there is demand to localise the pupil and iris. Several specifics of iris portion like its size, location and shape should be recognized for feature extraction technicality to be utilized efficiently. To attain desirable results for circular, localization Hough transform is utilized. Hough transform [2] is eligible to define the parameter of simple geometric objects like circles and lines existing in image. The radius of iris and pupil and center coordinates can be readily found through utilizing circular Hough transform. The manner suggested through Wilde-et-al [9], an edge map as offering in Fig-3 is gained merely through thresholding the image density gradients magnitude.

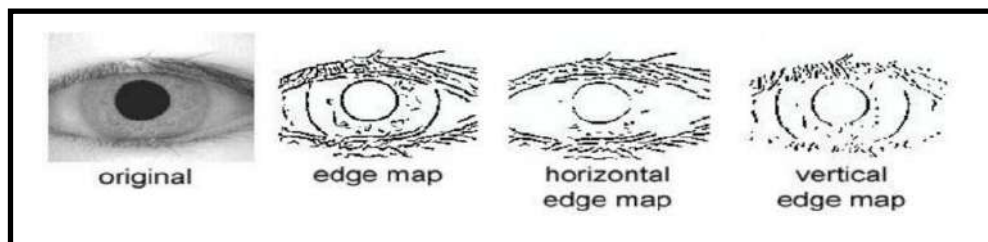


Fig. (3): Iris localization

4.2 Normalization

Normalization indicates to the transmutation of image from Polar Coordinates to Cartesian Coordinates. On having succeeded localise the iris image, the following stage is to convert the iris region of eye image in demand to have constant dimensions which is illustrate in Fig-4. The constant dimension iris image permits the feature extraction procedure to match the two iris images. There might be the dimensional discrepancies due to stretching of pupil from variable level of lighting [10, 11]. Another reason of dimensional inconsistency comprises camera rotation, alter image distance, rotation of eye inside the eye socket and head tilt. Thus normalization procedure is requirement to product same fixed dimensions so that two images of same iris beneath alter condition will have characteristics features at the same spatial locations.

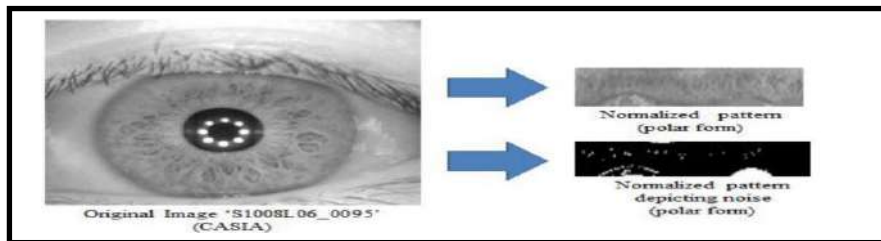


Fig. (4): Normalization process on CASIA database image

There are some algorithms for normalization but here Daugman Rubber Sheet Model [1] has been offered which is illustrating in Fig-5. The homogeneous rubber sheet model which was inventive through Daugman remaps every points inner iris into a couple of polar coordinates (r, θ) where r indicates for (u, 1) and θ indicates for (u,z).

$$I(x(r, \theta), y(r, \theta)) \rightarrow I(r, \theta) \dots\dots\dots(1)$$

With x_p

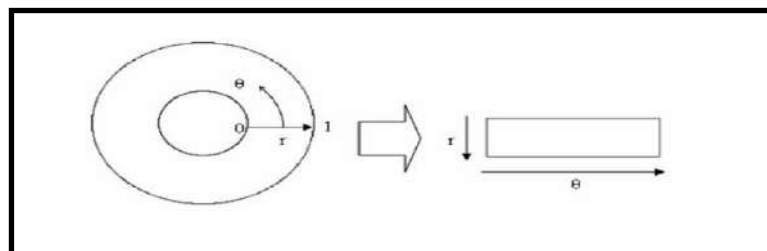


Fig. (5): Daugman's rubber sheet model

The reference point taken is the position of pupil and the radial vector push through iris region. A number of data point has been chosen along every radial line which has been depict as radial resolution. The total number of radial lines which are going about the iris region is depicted as angular resolution.

4.3 Feature extraction

4.3.1 Gabor wavelet transform feature

Gabor filters are utilized for extract the characteristic of iris images. 2D Gabor functions were suggested through Daugmann [12] to model the spatial gathering properties (of the receptive fields) of simple cells in the visible peel. They are vastly utilized in psychophysics, neuroscience, computer vision, and image processing. Visualize Gabor functions, utilize a Gabor filter for extraction and edge detection of texture features, emulate complex and simple cells (visible peel), emulate non-classical receptive field surround suppression or inhibition and utilize it for object contour exposure, and illustrate certain visible conception influences

The iris feature extraction utilized two dimension Gabor function is illustrate equation:

$$g(x, y) = -\frac{k^2}{\sigma^2} \exp\left(-\frac{kx^2}{2\sigma^2}\right) [\exp(ik \cdot x) - \exp\left(-\frac{\sigma^2}{2}\right)] \dots\dots\dots(2)$$

Where (x, y) is the spatial domain variables, k is the wave-factor that defines the range and direction of Gabor function, $\frac{k^2}{\sigma^2}$ factor covers all spatial frequency bands by means of equal energy, $\frac{\sigma^2}{2}$ subtract the DC component of Gabor filter.

The value of σ is π for the image of resolution 256 X 256. Eighteen different Gabor filter represents excellent texture information of image with three spatial frequencies ($k = \pi/4, \pi/8, \pi/16$) and six orientations from 00 to 1800. In this experiment the value of $\sigma = \pi$ and $k = \pi/4, \pi/8, \pi/16$ and the center frequency is at the origin.

Also we do weighted value calculation after feature extraction. It gives the highest weighted values for the system. The highest energy frequency in spatial domain has highest weighted value and all the highest weighted values are extracted from input images [13].

The Gabor function for the specified values of the parameters "wavelength", "orientation", "phase offset", "aspect ratio", and "bandwidth" will be calculated and displayed as an intensity map image in the output window. (Light and dark gray colors correspond to positive and negative function values, respectively.) The image in the output window has the same size as the input image.

The training data set obtained using Gabor Filter kernel by changing various parameters of Gabor function such as Wavelength, orientation, rotation angle are shown in fig 6 below.

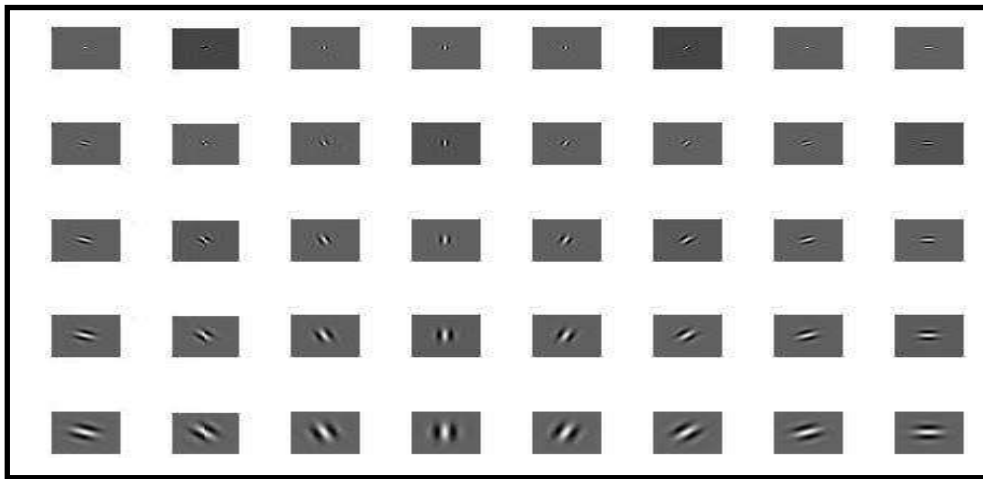


Fig. (6): Gabor Filter Kernel with different wavelength, orientation, and angle

4.3.2 Feature extraction by employing 2D DCT

One of the most significant stages in authentication of biometric system is feature extraction biometric system. It is the procedure of extracting feature of desirable images from a large gathering to be utilized in classification and selection assignment. Feature extraction (FE) extractor the roughly distinguished characteristics existing in an image. Distinguish iris texture information should be extracted and then encoded to have true comparisons among iris images templates. Complication of feature extraction influences the complication of program and processing speed of iris recognition system. In this paper feature extraction has been done by 2D-DCT. The discrete Cosine Transform (DCT) can be depict as a restricted sequence of data points which are in terms of gathering of cosine functions oscillating at various frequencies. such as another transforms, it as well attempts to de-correlate a offered signal. After being de-correlated, the transform coefficient is encoded independently in such a way that there is no damage in compression effectiveness. The DCT coefficients are reflection of the different frequency components which are present in it. The coefficient at the first place of the DCT refers to the DC component of the signal which is its lowest frequency and most of the time, it carries the maximum of the relevant information present in the input signal. The higher frequencies are represented by the coefficients present at the end and these generally represent the finer details about the original signal. The remaining coefficients carry other levels of information of the input signal given by:

$$x(r, \theta) = (1 - r)x_p(\theta) + rx_1(\theta) \dots \dots \dots (3)$$

$$y(r, \theta) = (1 - r)y_p(\theta) + ry_1(\theta) \dots \dots \dots (4)$$

$$F(u, v) = \alpha(u)\alpha(v) = \sum_{x=0}^{n-1} \sum_{y=0}^{n-1} \cos \left[\frac{\pi u}{2N} (2x + 1) \right] \cos \left[\frac{\pi v}{2M} (2y + 1) \right] f(x, y) \dots (5)$$

Where

$$\alpha(u)\alpha(v) = \begin{cases} \sqrt{\frac{1}{N}} & \text{for } u, v \neq 0 \\ \sqrt{\frac{2}{N}} & \text{for } u, v = 0 \end{cases} \dots \dots \dots (6)$$

Where $f(x, y)$ is the intensity of pixel at coordinates (x, y) , u varies from 0 to $M-1$ and v varies from 0 to $N-1$, where $M-1$ and v varies from $N-1$ where $(M \times N)$ is the size of image. Here the system gets a normalized image which has fixed dimensions. First DCT is applied on entire normalized image in order to extract features. DCT when applied to an image all the low frequency components gets accumulated towards the top corner of DCT spectrum. These low frequency components corresponds to the main distinguishable features of the iris while the high frequency components correspond to the finer details of the iris. The low frequency components are sufficient in recognition based applications and that is why the components which reside on top left corner of the spectrum are extracted and remaining is discarded. Fig-7 shows image transformation from spatial domain to frequency domain. Working from left to right, top to bottom, DCT is applied to each block. Each block is compressed through quantization. The obtained DCT coefficients are then binaries to form the templates of the images. For binary bits, the value of positive coefficients is assumed one and negative coefficients are discarded. Templates are compared under same nominal size, position, orientation and illumination conditions. The feature vector contains all the low to mid frequency DCT coefficients, having the maximum variance [14].

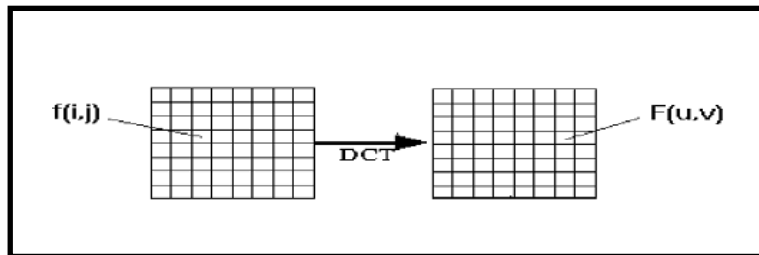


Fig. (7): Image transformation from spatial domain to frequency domain

5. Iris Classification by Probabilistic Neural Network (PNN)

This paradigm of neural network (NN) is a type of radial base network, it is appropriate for classification troubles, it is rely on Bayes classification rule (BCR) for decision operation, as well rely on Parzen window (PW) which evaluation the probability density function (PDF) for every denomination rely on training samples [15, 16].

In 1990, this neural model was introduced by Donald Specht who showed that the Bayes Parzen classifier could be detached into a massive number of simple procedures completed as a multilayer model and every one of these procedure units can be run separately in parallel way [17].

The execution of this neural model in subject identification attributes with decreased complication, it has rapid training speed, and it can readily append novel pattern neurons to pattern layer. Unluckily the PNN demands huge memory due the patterns nodes in pattern layer are equal to every number of training samples, that ordinary rely on the specimen magnitude and basically reasons rise network magnitude [18].

6. Experiment results:

The experiments have been done using MATLAB 7. To covers all conditions of Iris recognition system, the experimental results have been performed on a dataset acquired by (CASIA eye image database of version 4.0). The recognition rate of Iris recognition using fusion of Gabor wavelet transform and 2D discrete cosine features is 99.8%. Comparison of this approach has been made

with other existing algorithms of feature extraction in iris recognition system. Table-1 shows the comparison of recognition rate of various algorithm and our approach.

Table (1) Recognition rate of (visible, near-infrared, fusion visible near-infrared) by Gabor wavelet transform feature

Researcher	Algorithm	Year	Recognition rate (in percentage)
Mohd. Tariq [14]	Gabor wavelet transform	2013	99
A. Kumar [15]	2D DCT	2016	99.4
Proposed method	fusion of Gabor wavelet transform and 2D discrete cosine	2017	99.8

7. Conclusion

In this paper, we proposed to use enhancement method fusion of (Gabor wavelet transform feature and DCT feature) as the feature extracted for Iris recognition. The obtained fused feature vectors are fed up into Probabilistic Neural Network (PNN) for classification. Experiments carried out on (CASIA eye image database of version 4.0). The implementation has been done exclusively using Matlab and its image processing toolbox. The experimental results show this approach of fusion multi feature (Gabor wavelet transform feature and DCT feature) can be used to automatically identify the Iris more effective than used one feature alone. The maximum success of 99.8% recognition has been achieved.

References:

- [1] Daugman, "How iris recognition works," IEEE Transactions on Circuits and Systems for Video Technology". Vol. 14, No. 1, pp. 21-30, January 2004.
- [2] Daugman, "High confidence visual recognition of persons by a test of statistical independence," IEEE transactions on Pattern Analysis and Machine Intelligence, Vol. 15, No. II, pp. 1148-1161, 1993.
- [3] Yong Zhang, yan wo, "A fusion iris feature extraction based on linear discriminant". IEEE Proceedings of the 2013 International Conference on Machine Learning and Cybernetics, Tianjin, 14-17 July, pp 5-9, 2013.
- [4] Charles O Ukpai, Prof. S.S Dlay, Dr. Wl. Woo, "Iris feature extraction using principally rotated complex wavelet filter". IEEE International Conference on Computer Vision and Image Analysis Applications, Print ISBN: 978-1-4799-7185-5, 2015.
- [5] Tze Weng Ng, Thien Lang Tay, SiakWang Khor, "Iris recognition using rapid haar wavelet decomposition". IEEE 2nd international conference on signal processing system, 5-7, vol.1, Issue 6, pp. 234-238, July 2010.
- [6] Kshamaraj Gulmire, Sanjay Ganorkar, "Iris Recognition Using Gabor Wavelet". International Journal of Engineering Research & Technology (IJERT) Vol. 1, Issue 5, pp. 1-5, July –2012.
- [7] Amir Azizi, Hamid Reza Pourreza, "Efficient iris recognition through improvement of feature extraction and subset selection", International journal of computer science and information security, Vol.2, No.1, pp. 6-16, 2009.
- [8] CASIA-Database. <http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp>.
- [9] Mahmoud Elgamal, Nasser Al- Biqami, "An efficient feature extraction method for iris recognition based on wavelet transformation". International journal of computer and information technology, Vol.02, Issue 03, pp. 445-450, 2013.
- [10] R. Wildes, J. Asmuth, G. Green, S. Hsu, R. Kolczynski, J. Matey, S. McBride, "A system for automated iris recognition". Proceedings IEEE Workshop on Applications of Computer Vision, Sarasota, FL, pp. 121-128, 1994.
- [11] W. Boles, B. Boashash, "A human identification technique using images of the iris and wavelet transform". IEEE Transactions on Signal Processing, Vol. 46, No. 4, pp. 1185-1188, 1998.

- [12] J.G. Daugman: "**Uncertainty relations for resolution in space, spatial frequency, and orientation optimized by two-dimensional visual cortical filters**", Journal of the Optical Society of America A, 1985, vol. 2, pp. 1160-1169.
- [13] Vijayalaxmi, P.Sudhakar, Sreehari, "**Neural Network Approach for eye detection**", The Second International Conference on Computer Science, Engineering and Applications (CCSEA-2012), May 26-27, Delhi, India, Proceedings Volume Editors: David C. Wyld, Jan Zizka, Dhinakaran Nagamalai ISBN: 978-1-921987-03-8,(2012).
- [14] A. Kumar, A. Potnis and A. Pratap,"**Iris recognition and feature extraction in iris recognition System by employing 2D DCT**", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056, Volume: 03 Issue: 12 Dec -2016.
- [15] S. Meshoul and M. Batouche, "**Combining Fisher Discriminant Analysis and Probabilistic Neural Network for Effective On-Line Signature Recognition**", 10th International Conference on Information Science, Signal Processing and their Applications (ISSPA), IEEE, in 2010.
- [16] N. B. Nimbhorkar and S. J. Alaspurkar, "**Probabilistic Neural Network in Solving Various Pattern Classification Problems**", IJCSNS International Journal of Computer Science and Network Security, vol.14 No.3, in March 2014.
- [17] H. M. and B., I., "**A probabilistic Neural Network Approach for Modeling and Classification of Bacterial Growth/no-Growth Data**", Journal of Microbiological Methods, pp 217– 226, in 2002.
- [18] W. S. Lim and Rao M.V.C., "**A New Method of Reducing Network Complexity in Probabilistic Neural Network for Target Identification**", IEICE Electronics Express, Vol.1, No.17, 534-539, Faculty of Engineering & Technology, Multimedia University, in December 2004.

Enhancement Human Face Recognition based on fusing of Infrared and visible Images

Ziad M. Abood Ghada S. Karam Rafid. E. Haleot

Mustansiriyah University/ College of Education

dr.ziadmabood@yahoo.com, ghadask@yahoo.com, rafidalkenany@yahoo.com

Abstract:

Biometrics offers a promising alternative to classical forms of identification, such as card IDs, which are not embedded into one's physical property. Face recognition (FR) become one of the research hottest topics, since it is the natural technique of identification and is perfectly unobtrusive, the Infrared Spectrum is used in human Face recognition, due to its relative insensitive to variations in face appearance caused by ambient light changes. This paper proposes an accurate, and fast approach for detection and recognition facial features based on feature-level fusion where the infrared (IR) and visible face images are fused to achieve feature integration in the recognition process and to improve final FR system performance. Gabor wavelet transform is used in feature extraction stage for extracting features. Support Vector Machine (SVM) are used in the classification stage. The proposed approach tested on a Carl Face Database (Visual/ Infrared) images. Experimental results shows a significant performance improvements in recognition accuracy for fusion of two different spectrums of Visual and Infrared datasets than the performance of face recognition using visible images. The maximum success of 94.5% recognition has been achieved.

Keywords: Face recognition, Infrared image, image Fusion, Gabor wavelet transform, SVM.

تحسين التعرف على الوجه البشري اعتماداً على دمج صور الأشعة تحت الحمراء وصور مرئية

المستخلص:

تقدم القياسات الحيوية بديلاً عن لأشكال الكلاسيكية لتحديد الهوية، مثل معرفات البطاقات الشخصية، والتي لا تكون جزءاً لا يتجزأ من الملكية المادية للشخص. وأصبح التعرف على الوجه واحدة من أهم المواضيع، إذ يعد هو تقنية لتحديد هوية الأشخاص. ويستخدم الطيف الأشعة تحت الحمراء للتعرف على وجه الإنسان. وتقتصر هذه الورقة طريقة سريعة للكشف عن ميزات الوجه والتعرف عليه على أساس (دمج) المميزات للوجه من خلال دمج الأشعة تحت الحمراء (IR) وصور الوجه المرئية. استخدم تحويل كابور المويجي في مرحلة استخراج الميزات، واستخدم دعم ناقلات آلة (SVM) في مرحلة التصنيف. تم اختبار الطريقة المقترحة على قاعدة بيانات (صور مرئية/ الأشعة تحت الحمراء). أظهرت النتائج التجريبية تحسينات كبيرة في الأداء في دقة التعرف على الوجه نتيجة دمج اثنين من مجموعات البيانات المرئية والأشعة تحت الحمراء بالمقارنة بالتعرف على الوجه باستخدام صور مرئية وقد تم تحقيق دقة بالتعرف تصل الى 94.5%.

الكلمات المفتاحية: التعرف على الوجه، صورة الأشعة تحت الحمراء، دمج صورة، تحويل كابور المويجي، SVM.

1. Introduction

Progress in computer vision and sensor technology has made it possible to acquire various types of information, such as two-dimensional (2D) data at different wavelengths, [1,4]. Since each type of sensor provides different features under various environmental conditions, the performance of an application depends highly on selecting a sensor or multi-sensor combination. Therefore, the selection of appropriate sensors has become one of the most significant factors for high-performance vision systems. Most of the early computer vision applications were based on visible (RGB) sensors, since a visible image represents what humans perceive visually [1, 6]. The range of wavelengths correspond to a frequency is approximately at the range 380 nm to 700 nm. Images also contain texture information, which is one of the most important types of information for object detection, tracking and classification [7, 8]. However, since visible sensor images are strongly

distorted by changes in illumination, the performance of visible-sensor-based systems also depends highly on illumination conditions. The wavelength range of near-infrared (IR) and thermal-IR sensors are from 0.7 to 1 μm and from 8 to 14 μm , respectively. Although these wavelengths are not perceived by the human visual system, IR images contain distinctive features, such as thermal radiation emitted by objects. Furthermore, compared to visible sensor images, infrared images are more invariant to visible illumination changes [9,10]. However, neither near-IR nor thermal-IR images include color (RGB) information. In addition, thermal-IR images do not contain texture information and can be affected by ambient temperature. As explained above, each sensor provides different information and has advantages and disadvantages in different environments. Therefore, to design more flexible and robust systems, the selection of sensors for a specific application is a very important problem.

In this paper, we propose a fusion-spectrum sensor system, consisting of two types of sensors: visible and Infrared by using Feature Level Fusion.

2. Related Works

The process of thermal face recognition has been attracted many researchers during the last decades, Kong et al. [11] presented registration fusion of visible and thermal IR image data. Huang, et al. [12] proposed an Extend Local Binary Pattern method for Near IR face recognition. They designed a device including PC, camera, an active NIR lighting, and an optical sensor. Akhloufi et al. [13] presented an approach for face recognition in the IR spectrum using a network of physiological features. Their technique extracts the unique face print, which represents medial axis regions of isotherms extracted from IR face images. They used a distance transform to achieve an invariant matching during face recognition steps. George et al.[14] investigated two different fusion schemes, the first one is pixel based and operates in the wavelet domain, while the second schemes is feature based and operates in Eigen space domain. Deepali H. shah et al. [15] presented a novel approach to face recognition using modifies principal component analysis method and uses support vector machine SVM classifier with constant hyper plane. Irfan Riaz et al.[16]examined new detection scheme for thermal images using transform histogram features and SVM their results exhibits better detection accuracy by reducing the training and testing time. Sofiah Radzi et al. [17] presented multi scale framework of thermal face detection using HOG method and SVM based on two different spectrum training sets.

3. Fused Images

Image fusion is a combination of two or more images to improve visual perception or feature extraction. Visible images are formed by reflection in the visible spectrum while Infrared images are created from Infrared radiation [18]. Fusion of both Infrared and visual images will generate a new fused image that will store the information of both Infrared and visual face. So, the resulted fused image is more informative than any of the individual image. In face recognition, visual images sometimes are found to be more helpful than Infrared images. Where IR information becomes less reliable due to various environmental (i.e. temperature changes), physical (lack of sleep) and physiological conditions (i.e. fears, stress) again, Infrared images are best to detect liveliness. Infrared imagery is invariant to change in ambient illumination, and provides a capability for identification under all lighting conditions including complete darkness. So, we can apply the concept of fusion in face recognition to get better result of person recognition. In face recognition three types of fusion methods can be used [19, 20]:

• Feature Level Fusion:

The role of feature-level fusion is to establish boundaries in feature space and separate patterns belonging to different classes. Thus two main issues are involved: the feature detection and the use of distance metrics for clustering.

• Decision Level Fusion:

Decision level fusion is generally based on a joint declaration of multiple single source results to achieve an improved classification or event detection. At the decision level, prior knowledge and domain specific information can also be incorporated.

• Pixel / Data Level Fusion:

Pixel-data level fusion is the combination of the raw data from multiple source images into a single image. It combines information into a single image from a set of images source using pixel, feature or decision level techniques.

4. Gabor wavelet transform feature

For extracting the feature of visible and Infrared images, we applied the Gabor filters are in our approach. Two-dimensional Gabor functions were proposed by Daugmann [21] to model the spatial summation properties (of the receptive fields) of simple cells in the visual cortex. They are widely used in image processing, computer vision, neuroscience and psychophysics. Visualize Gabor functions, use a Gabor filter for edge detection and extraction of texture features, simulate simple and complex cells (visual cortex), simulate non-classical receptive field inhibition or surround suppression and use it for object contour detection, and explain certain visual perception effects.

The general 2D Gabor function for facial feature extraction

$$g(x, y) = -\frac{k^2}{\sigma^2} \exp\left(-\frac{kx^2}{2\sigma^2}\right) \left[\exp(ik \cdot x) - \exp\left(-\frac{\sigma^2}{2}\right)\right]$$

Where (x, y) is the spatial domain variables, k is the wave-factor that defines the range and direction of Gabor function, $\frac{k^2}{\sigma^2}$ factor covers all spatial frequency bands by means of equal energy, $\frac{\sigma^2}{2}$ subtract the DC component of Gabor filter.

The value of σ is π for the image of resolution 256 X 256. Eighteen different Gabor filter represents excellent texture information of image with three spatial frequencies ($k = \pi/4, \pi/8, \pi/16$) and six orientations from 00 to 1800. In this experiment the value of $\sigma = \pi$ and $k = \pi/4, \pi/8, \pi/16$ and the center frequency is at the origin. Also we do weighted value calculation after feature extraction. It gives the highest weighted values for the system. The highest energy frequency in spatial domain has highest weighted value and all the highest weighted values are extracted from input images [22].

The Gabor function for the specified values of the parameters "wavelength", "orientation", "phase offset", "aspect ratio", and "bandwidth" will be calculated and displayed as an intensity map image in the output window. (Light and dark gray colors correspond to positive and negative function values, respectively.) The image in the output window has the same size as the input image.

The training data set obtained using Gabor Filter kernel by changing various parameters of Gabor function such as Wavelength, orientation, rotation angle are shown in figure 1 below.

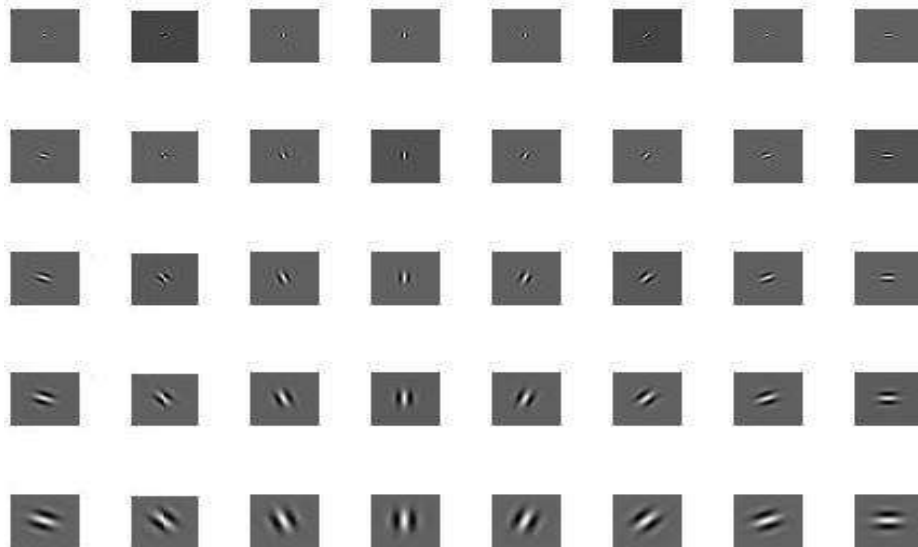


Figure 1: Gabor Filter Kernel with different wavelength, orientation, and angle [22]

5. Image Classification by SVM

All classification algorithms typically based on the assumption the data in question holds one or more features, each of this features belongs to one of several distinct classes [23, 24]. Support Vector Machine is a pattern classification method, is a set of related supervised learning methods that analyze data and recognize patterns, used for classification and regression analysis. This method aims to separate two data sets with maximum distance between them. The training of a classification SVM involves the fitting of a hyper plane such that separates the largest possible fraction of points of the same class on the same side, while maximizing the distance from either class to the hyperplane. This method separates two data sets by searching for an optimal separating hyperplane (OSH) between them. [25, 26, 27].

The training of a classification SVM involves the fitting of a hyperplane such that the largest margin is formed between 2 classes of vectors while minimizing the effects of classification errors (figure 2).

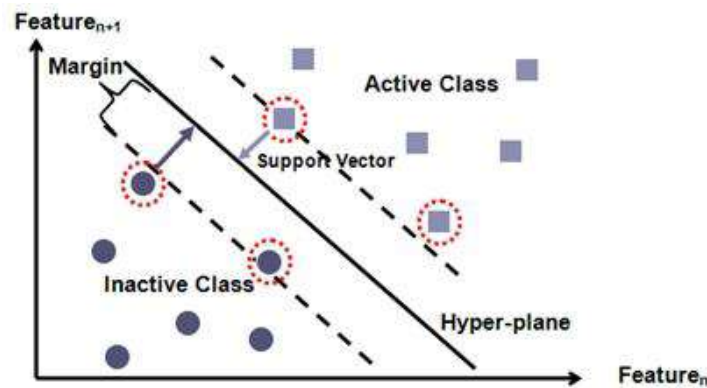


Figure 2. Maximum separation hyperplane [26].

6. Dataset

We used a Carl dataset, the visible images (in the band of 400 -700nm) and near-infrared images (in the band of 0.7–1.4 μ m), The face images are a BMP 24 bit/pixel and The visible images 640 $\times$ 480 pixels, and the resolution of near-infrared images is 640 $\times$ 480 pixels figure 3.



Figure (3) two spectral face image for each person in dataset

Additionally, the distance between the face of the user and the tripod that holds the sensors is 135cm. Each user has been recorded in four different acquisition sessions performed between November of 2009 and January 2010. In this sense, distinctive changes in the haircut and/or facial hair of some subjects may be appreciated. The acquisitions have been done in the whole day from 9 AM to 5 PM, because it was getting dark after 5 PM. The average time required for the full acquisition process of a skilled user has been 10 minutes, being 15 minutes for a non-skilled one. The whole set of users were acquired in two days per session.

A different facial expressions have been collected (smiling/non smiling, open-closed and blinking eyes...etc). In order to reduce the correlation between consecutive acquisitions of the same session, between a couple of snapshots the user is asked to stand up make a loop to the room, including one step which corresponds to the portion of the room close to the blackboard, and sit down again. It is

worth to mention that thermal camera was able to detect a temperature increase due to this additional physical exercise figures [4-5-6].



Figure (4) visible image for some persons in the dataset



Figure 5 Near-infrared images for some persons in the dataset

Final database consists of 41 people (32 males, 9 females) shown in Table (1). Each individual contributed in four acquisition sessions and in each sessions 15 image under three image sensors. This implies a total of: $41 \times 4 \times 15 \times 2 = 4920$ images.

Table (1) data set for visible and NIR

Image spectral	Image format	Image size (pixels)	Number of person	Number of session	Number of image in each session
Visible (400 nm-700nm)	BMP 24 bit/pixel	640×480	41	4	15
near-infrared (0.7 μm –1μm)		640×480			
			Total image: 41x4x15x2= 4920 image		

7. Proposed method:

In The proposed Face Recognition System (FRS) the following steps of methods are used: feature extraction, feature fused, and classification. The architecture of the overall system is shown in Figure 6.

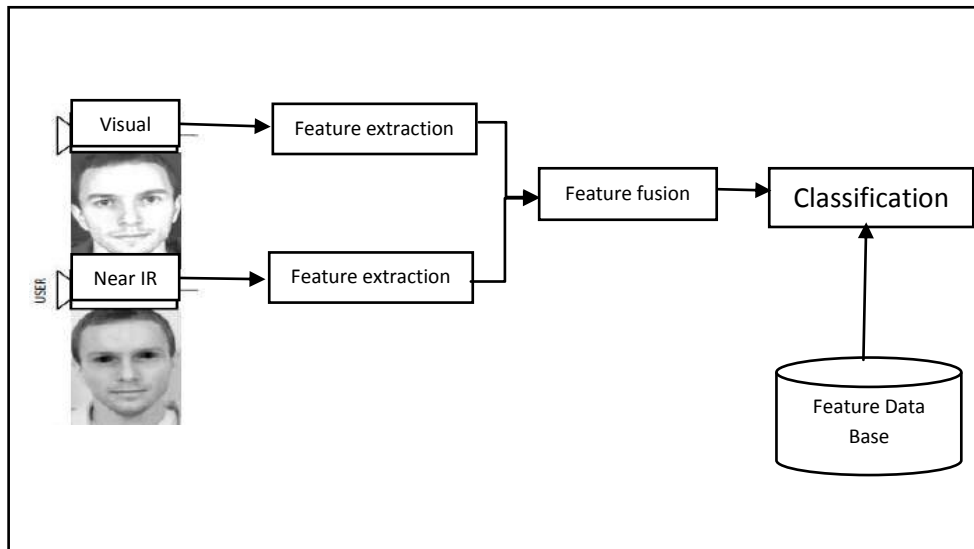


Figure 6: Overall purposed processing system. Multi-sensor fusion at feature level.

8. Experiment results:

All the experiments have been done using MATLAB 7. To covers all conditions of human face recognition, the experimental results have been performed on a dataset acquired by Carl Database consists of 41 people (32 males, 9 females) the database contains images in the near-infrared and the images in the visible spectrum. We test the performance of the established face recognition system: first it is tested on the training set (1230 images) and then on testing set (3690 images). The recognition rate of (visible, near-infrared, fusion Visible and near-infrared) by Gabor filter feature is shown in Table 2 and Figure 8. The system performance reaches 94.5% over the selected range of test data in the fusion visible, near-infrared images.

Table (2) Recognition rate of (visible, near-infrared, fusion visible near-infrared) by Gabor wavelet transform feature

Image spectral	Recognition Rate
visible	88.6%
near-infrared	86.4%
fusion Visible, Near IR	94.5%

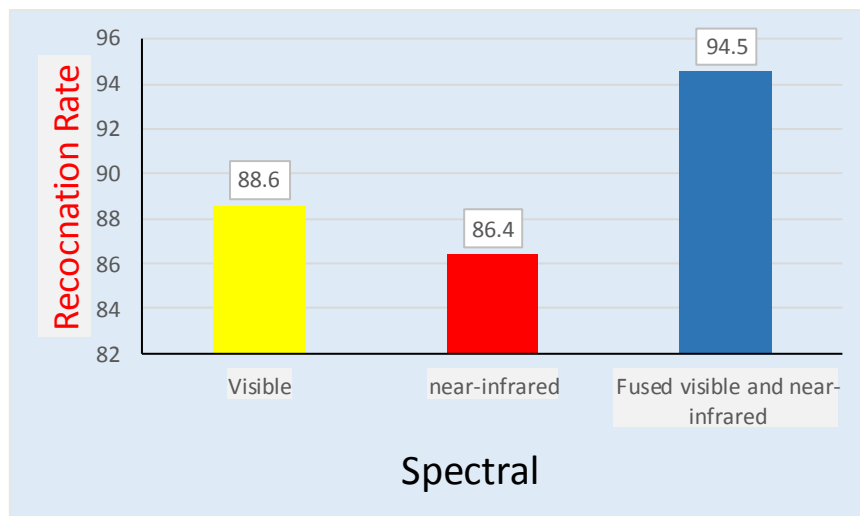


Fig. 8. Recognition rate of (visible, near-infrared, fusion visible near-infrared) by Gabor wavelet transform feature

9. Conclusion

In this paper, we proposed enhancement method for face recognition based on fusion of multispectral images using Gabor wavelet transform feature as the feature extracted for face recognition. The obtained fused feature vectors are fed up into Support Vector Machine (SVM) classifier for classification. Experiments carried out on (Carl Face) Database that both visual images, infrared images are investigated. The implementation has been done exclusively using Matlab and its image processing toolbox. The experimental results show this approach of fusion multi spectrum (visible-near infrared) can be used to automatically identify the faces more effective than used alone of visual image faces or infrared image. The maximum success of 94.5% recognition has been achieved.

References:

1. Ukimura, O. Image Fusion; InTech: Rijeka, Croatia, 2011.
2. Thomas, C. Sensor Fusion and its Applications; Sciyo: Vienna, Austria, 2011.
3. Kolb, A.; Barth, E.; Koch, R.; Larsen, R. Time-of-Flight Sensors in Computer Graphics; Eurographics Star Report; Munich, Germany, 2009.
4. Lange, R. 3D Time-of-Flight Distance Measurement with Custom Solid-State Image Sensors in CMOS/CCD-Technology. Ph.D. Dissertation, University Siegen, Siegen, Germany, 2000.
5. Wilfried, E. An Introduction to Sensor Fusion; Research Report 47/2001; Vienna University of Technology: Vienna, Austria, 2001.
6. Andrea, F.; Nappi, A.M.; Riccio, D.; Sabatino, G. 2D and 3D face recognition: A survey. *Pattern Recogn. Lett.* 2007, 28, 1885–1906.
7. Zhong, Y.; Jain, A.K. Object localization using color, texture and shape. *Pattern Recognit.* 2000, 33, 671–684.
8. Mirmehdi, M.; Maria, P. Segmentation of color textures. *IEEE Trans. Pattern Anal. Mach. Intell* 2000, 22, 142–159.
9. Stan, Z.; Li, R.; Chu, S.; Liao, S.; Zhang, L. Illumination invariant face recognition using near-infrared images. *IEEE Trans. PAMI* 2007, 29, 627–639.
10. Chang, H.; Koschan, A.; Abidi, M.; Kong, S.G.; Won, C.H. Multispectral Visible and Infrared Imaging for Face Recognition. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, Anchorage, AK, USA, 23–28 June, 2008; pp. 1–6.
11. S. G. Kong, J. Heo, F. Boughorbel, Y. Zheng, B. R. Abidi, A. oschan, M. Yi, M. A. Abidi, Multiscale fusion of visible and thermal IR images For illumination-invariant face recognition, *International Journal of Computer Vision*, Vol. 71 (2), 215–233, 2007.
12. Di Huang, Yunhong Wang, and Yiding Wang, A Robust Method for Near Infrared Face Recognition Based on Extended Local Binary Pattern, *ISVC 2007, Part II, LNCS 4842*, pp. 437–446, 2007.
13. A. Moulay, B. Abdelhakim, Infrared face recognition Using Distance Transforms, *Proc. of World Academy of Science, Engineering, and Technology*, vol. 30, July, 2008.
14. George Bebis, Aglika Gyaourova, Saurabh Singh, Ioannis Pavlidis, Face recognition by fusing thermal infrared and visible imagery, *Image and Vision Computing*, vol. 24, pp. 727–742, 2006.
15. Deepali H. Shah, J. S. Shah, A Novel Approach to Face Recognition using Split PCA, *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, vol. 4, Issue 3, May-June 2015.
16. Irfan Riaz., Jingchun Piao., Hyunchul Shin. Human detection by using centrist features for thermal images, *IADIS International Journal on Computer Science and Information Systems* Vol. 8, No. 2, pp. 1–11.
17. Sofiah Radzi, Kamarul Hawari Ghazali, Sabira Khatun, Zuwairie Ibrahim, Multiscale Thermal Face Detection Using Histogram Oriented Gradients, *Proceeding of the International Conference on Artificial Intelligence in Computer Science and ICT (AICS 2013)* 25 -26 November 2013, Langkawi, Malaysia. pp. 201–216.
18. D. M. Bulanon, T. F. Burks, V. Alchanatis, Image fusion of visible and thermal images for fruit detection, *Biosystems engineering*, vol. 103, 2009, pp. 12–22.

19. George Bebis a, Aglika Gyaourova a, Saurabh Singh a, Ioannis Pavlidis by Face recognition by fusing thermal infrared and visible imagery, Image and Vision Computing 24 (2006), pp.727–742.
20. M. Saquib Sarfraz, Rainer Stiefelbogen, Deep Perceptual Mapping for Thermal to Visible Face Recognition, In Proceedings British Machine Vision Conference (BMVC) 2015, Swansea, UK, September 2015 (Best Industry Paper Award) pp. 1-11.
21. J.G. Daugman: Uncertainty relations for resolution in space, spatial frequency, and orientation optimized by two-dimensional visual cortical filters, Journal of the Optical Society of America A, 1985, vol. 2, pp. 1160-1169.
22. Vijayalaxmi, P. Sudhakar, S., “Neural Network Approach for eye detection”, 2nd International Conference on Computer Science, Engineering and Applications (CCSEA-2012), 26-27 May, Delhi, India, Proceedings Volume Editors: David C. Wyld, Jan Zizka, Dhinaharan Nagamalai ISBN: 978-1-921987-03-8,(2012)
23. Michael Teutsch, Thomas Muller, Marco Huber, and Jürgen Beyerer, Low Resolution Person Detection with a Moving Thermal Infrared Camera by Hot Spot Classification, CVPRW 14 Proceedings of the 2014 IEEE Conference on Computer Vision and Pattern Recognition Workshops, pp. 209-216.
24. Ergun Gumus et. al., Evaluation of Face Recognition Techniques Using PCA, wavelets and SVM, An international journal: Expert Systems with Applications 37 (2010) 6404–6408, Elsevier publication.
25. G. Dai and C. Zhou, Face Recognition Using Support Vector Machines with the Robust Feature, in Proceedings of IEEE Workshop on Robot and Human Interactive Communication, 2003, pp.49-53.
26. Deepali H. Shah, J. S. Shah, A Novel Approach to Face Recognition using Split PCA, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), vol. 4, Issue 3, May-June 2015.
27. Hui-Ming Huang, He-Sheng Liu, Guo-Ping Liu, Face Recognition Using Pyramid Histogram of Oriented Gradients and SVM, Advances in information Sciences and Service Sciences (AISS),V.4, N.18, Oct 2012, pp.1-8.

Categorization Quranic Text Using NB algorithm

Geehan Sabah Hassan¹

Faris Mahdi Alwan²

¹Assistant Lecturer in Natural Language Processing, Quality Assurance & Academic performance Department, University of Baghdad (UOB), gee.fah@gmail.com

²Operations Research/ Reliability and Maintenance, Statistics Department, College of Administration and Economics, University of Baghdad (UOB), faris.or@gmail.com

Abstract:

This essay discusses two methods: the first one Arabic text classification (TC) and a second developing Arabic-English Machine Translation system. The research objectives are, to formulate a Naive Bayes (NB) algorithm for the automatic and suitable classification of any Holy Quran Tafseer segment; to identify relevant categories of Holy Quran Tafseer in the form of number classes; and to retrieve, Tafseer of verses of the Holy Quran in English language. This research has been designed to classify different verses in the Holy Quran. The result shows the outperform of TC using the NB algorithm is a good algorithm for categorization Tafseer of Holy Quran.

Keywords: Text Classification (TC), Naive Bayes (NB) algorithm.

1. Introduction

TC is a process of labeling natural language texts with one or several categories from a predefined set. TC is a supervised learning where the set of categories and examples of documents belonging to those categories is given. As a research area, TC appeared in the 1960s, but became a major field of information science only 15 years ago. Applications of TC, which includes document indexing with controlled vocabulary, filtering of irrelevant information, web page categorization, email management, and detection of text genre among others. Text categorization techniques are necessary nowadays when most information is produced and stored digitally [1].

Business and personal correspondence, scientific and entertaining articles, conference proceedings, and patient data are a few examples of electronic text collections. The advent of the World Wide Web (WWW) a massive repository of text information which required automatic means of efficient and effective storage and retrieval system that can be provided through TC [2]. Such a system comprises different types of approaches that help solve many real world problems such as K-Nearest Neighbor, Rocchio's algorithm, Decision Trees, Naïve Bayes algorithm, Back propagation Network, and Support Vector Machines. Each approach implements text categorization techniques to achieve its goal [3].

2. Background

Categorization is classifying data to improve effectiveness and efficiency. TC is one of the most widely used and significant methods of supervised learning in data mining. Let $(d_j, c_i) \in D \times C$, where D is the set of documents and $C = \{c_1, c_2, \dots, c_{|C|}\}$ is a predefined set of categories. The main mission of TC is to allocate a Boolean value to every pair in D [4] [5].

Figure 1 shows that, various categories are found in the document domain D and set C . D includes three different types of documents, namely '#', '\$' and '@' after categorization. Every document is categorized in its own category.

The following observations are worth considering:

- The categories are only symbolic labels. They are supposedly obtainable to assist in building the classifier. This observation implies that "text" forms the category label.
- The predication of documents to categories, is generally, achieved on the basis on the meaning of words in documents, and not on metadata. Document categorization should underlie only on subjective knowledge and not on exogenous knowledge [6].

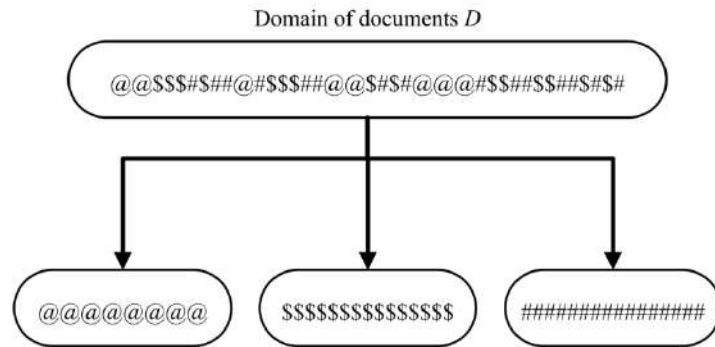


Fig. (1): Pictorial of representation of Categorization

Figure 2 shows the general structure of a categorization system. The first stage is preprocessing and provides the document for the classification process. Text are normalized the text by tags, and stop words are removed. Words in the documents are then listed and indexed. The vocabulary is extracted, and phrases and terms may be recognized. Word stemming is optionally performed. Finally, a discriminating algorithm is invoked to distinguish between categories [7].

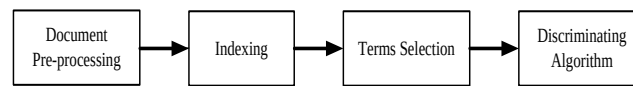


Fig. (2): Categorization steps

3. Methodology

This research comprises three phases. The first phase is pre-processing and modeling involves normalization, term extraction, stemming, and using the dictionary to convert Arabic words to English words after using inverted index, dimensionality reduction and weighing terms (TF*IDF). The second phase addresses how to Naive Bayes algorithm to derive the solution applied to the Tafseer Holy Quran. The third phase evaluates the performance of the categorization model by using the precision and recall values.

3.1 Classifier Learning Algorithms

A text classifier for $c_i \in C$ is generated automatically by a general inductive process. This process is conducted by monitoring the properties of the document sets before classification according to c_i or c_i which obtain the properties of a new hidden document wherein c_i must belong. With the goal of building classifiers for C , a document set S is needed such that the value of $\Phi(d_i, c_i)$ is well known for every $(d_i, c_i) \in \Omega \times C$ the experimental results of the TC show that S is generally divided into two separate sets, namely, T_r (training set) and T_e (test set)[8]. The training data set (T_r) indicates the record collection already known in class labels. (T_r) is used for building the categorization model and is applied to the testing data set. The test data set (T_e) indicates the record collection known in class labels. However, when given as an input to build categorization models, accurate class labels should be returned to the records. (T_e) would help identify the accuracy of the model [9].

Figure 3 explains how to build a categorization model to solve categorization problems. Different learner methods are implemented in TC. Several of these methods create binary-valued classifiers in the form of $\hat{\Phi}: D \times C \rightarrow \{T, F\}$ By contrast; other learner methods create real-valued functions in the form $CSV: D \times C \rightarrow [0,1]$ where, CSV is stands for categorization status value. When dealing with categorization problems, a set of thresholds τ_i need to be determined to allow the conversion of real-valued CSVs into final binary decisions [8]. In different applications, the methods noticeably perform a real-valued function that can be useful when thresholds are not required.

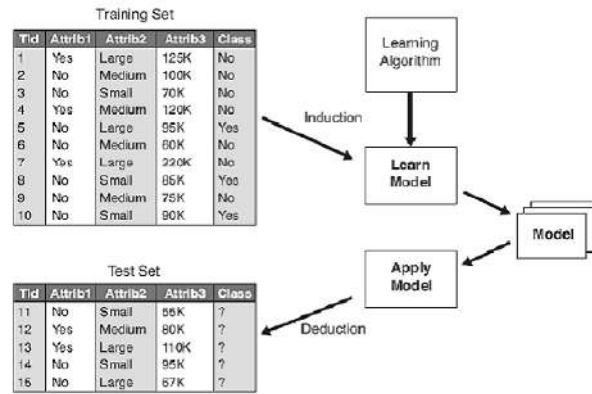


Fig. (3): General approach for building a categorization model

The training efficiency (viz, the average time required to build a classifier $\hat{\Phi}_i$ from a corpus Ω), classification efficiency (viz, average time required to classify a document through $\hat{\Phi}_i$) and effectiveness (viz, the correctness of the average of $\hat{\Phi}_i$ s behavior of classification) are all legitimate procedures of learner success.

3.2 Naive Bayes Algorithm

A Naive Bayesian (NB) is an easy algorithm that uses common statistical modeling strategy [7]. Depending on how the Bayes' theorem was used for Bayesian statistics as:

$$P(C_i|D_i) = \frac{P(D_j|C_i)P(C_i)}{P(D_j)} \quad 5$$

This strategy estimates the class-conditional probability, by assuming that the attributes are equally important and conditionally independent. In this manner, the existence or non-attendance of a certain feature is assumed to be actually independent of the existence or non-attendance of every other feature. The Naive Bayes classifier is defectively performed with increased correlation of the features [10].

3.3 Implementation

The implementation detail of the proposed method using the NB algorithm containing three phases. First phase: Database that included Document Pre-processing containing several methods; Second phase: NB algorithm implementation; and Third phase: Precision and Recall values evaluate the performance of the categorization model.

The database of this research consisting of 1000 (verses) of the Holy Quran and data was divided into two text document sets (training and testing). The training set is (800) verses and for testing set (200) verses. We choose only seven categories of Tafseer texts shown in the table 1.

Table (1) Categories in this research for Holy Quran Tafseer

Arabic Main Categories	English Translation
الزواج	Marriage
الارث	Inheritance
الصلاة	Pray
الزكاة	Almsgiving
بر الوالدين	Honouring parents
الحلال	Halal
الجهاد	Jihad

The all training data in this phase in Arabic language and containing the label (verses) text, label). The process of preprocessing data includes tokenization, stop word list, normalization, stemming and dictionary. After the pre-processing phase, all stemming words will be matched with the dictionary and convert words from the Arabic language to the Malay language. Figure 4 shows the example for stemming algorithm and dictionary.

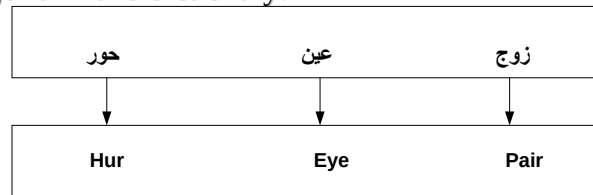


Fig. (4): The example for stemming (verses) and dictionary

The next step is to generate the weighting terms by using (TF*IDF). (TF*IDF) method put document vector in the feature space this end step in the training phase of NB algorithm. Table 2 shows the training data set collected in this study. There is a certain number of documents, which located in this class.

Table (2) Training data set collection

Category	Total Documents
Marriage	139
Inheritance	100
Pray	129
Almsgiving	114
Honouring parents	90
Halal	110
Jihad	118

A new document given the categorization model must predict the correct category label based on previous training. TF*IDF calculations helps to create document vectors in feature space. Then the cosine similarity between the test document and specific training documents are calculated.

4. Results

The effectiveness of the categorization depends on the NB algorithm or the accuracy of the results obtained after the implementation of NB algorithm and calculating the precision and recall are computed based on the following equation:

$$Precision = \frac{a}{(a+b)} \quad (5)$$

$$Recall = \frac{a}{(a+c)} \quad (6)$$

$$Fallout = \frac{b}{(b+d)} \quad (7)$$

$$Error\ rate = \frac{(b+c)}{(a+b+c+d)} \quad (8)$$

$$Precision = \frac{tp}{tp+fp} \quad (5)$$

And

$$Recall = \frac{tp}{tp+fn} \quad (6)$$

where a is a number of documents that both the human and the computer classify as positive examples, b is number of documents that the human classifies as negative examples but the computer classifies as positive examples, c is number of documents that the human classifies as positive example but the computer classifies as negative examples, d is number of documents that

both the human and the computer classify as negative documents, and $(a + b + c + d)$ represent total number of test documents(n).

Table 3 shows precision, recall, fallout, and error rate for every category.

Table (3) Precision and recall value of NB.

Category	Precision	Recall	Fallout	Error rate
Marriage	1	0.67	0.8	0.95
Inheritance	1	1	1	0.98
Pray	0.84	0.84	0.84	0.96
Almsgiving	0.8	0.68	0.71	0.77
Honouring parents	0.68	0.68	0.68	0.76
Halal	0.99	0.99	0.99	0.96
Jihad	1	1	1	0.94

5. Conclusions and Future Work

Classification of the Holly Quran is unlike typical classification. First, this is since we are dealing with a sacred script and hence classification should be context sensitive. Further, there is a need to understand existed and possible classifications for Quran verses. One of the popular Quran text classifications is to classify verses into: (Meccan or Medinan). Other possible classifications that can give deeper understanding of context or semantics should be thoroughly investigated in future research related to the Holly Quran. In this study, we described the design and successful implementation of a new text classification suitable for classifying different Ayah (verses) of the Holy Quran using the NB algorithm and there search deals a limited number of text files in the training set and test set. Increase the number of these files in both sets to extend conclusions it has schemes in the future. On the other hand, the number of classes (characters) it will be increased. That means our future studies will include larger datasets and a larger number of classes.

References

- [1] Kiritchenko, S. (2005), "Hierarchical text categorization and its application to bioinformatics", Retrieved from
- [2] Abdullah, S. Sadiq, D. (2014), "Hybrid Intelligent Techniques for Text Categorization", International Journal of ..., 2(2), 23–40.
- [3] Baharudin, B., Lee, L. H., & Khan, K. (2010), "A Review of Machine Learning Algorithms for Text-Documents Classification", Journal of Advances in Information Technology, 1(1), 4–20.
- [4] Sebastiani, F. (2005). Text categorization, 109–129.
- [5] Jiang, S., Pang, G., Wu, M., & Kuang, L. (2012), "An improved K-nearest-neighbor algorithm for text categorization", Expert Systems with Applications, 39(1), 1503–1509. doi:10.1016/j.eswa.2011.08.040
- [6] Baharudin, B., Lee, L. H., & Khan, K. (2010), "A Review of Machine Learning Algorithms for Text-Documents Classification", Journal of Advances in Information Technology, 1(1), 4–20. doi:10.4304/jait.1.1.4-20
- [7] Fall, C. J., & Benzineb, K. (2002). Literature survey: Issues to be considered in the automatic classification of patents. World Intellectual Property Organization, 29.
- [8] Sonka, Milan, Vaclav Hlavac, R. B. (2014), "Image processing, analysis, and machine vision".
- [9] Bishop, C. M., & Nasrabadi, N. M. (2006), "Pattern Recognition and Machine Learning", (Vol. 1). Springer New York.
- [10] Pawar, P., & Gawande, S. (2012), "A comparative study on different types of approaches to text categorization". International Journal of Machine. Retrieved from http://fit.hcmup.edu.vn/~haits/Conferences/ICMLC 2011/rp080_vol.4-C01020-R001.pdf

New Facial Imprint Detection Algorithm Based on Ycber Model and Ant Colony

Dina Riadh Alshibani

Samar Amil Kassir

Mustansiriya University, College of Science, Computer Science Dept.

dinashibani@uomustansiriya.edu.iq samarkassir@yahoo.com

Abstract:

In this research, new efficient algorithm for human imprint detection is presented; this algorithm relies on utilizing swarm Ant Colony Algorithm (ACO) in detecting phase; First, the skin area of the face is detected using YC_bC_r model, and then range rules is derived and applied for localizing face clip; Median filter is used to reduce the noise; Face clip is extracted. Gaussian filter is applied on face clip for smoothing aim; then the clip is converted to gray scale and finally Ant Colony algorithm is applied to obtaining the facial imprint. The presented algorithm tested on data set comprises of (30) of human face pictures; different skin colors, the lighting and background is not the same in all pictures. Upon examinations; presented algorithm has achieved excellent results for extracting facial imprint.

Keyword: YC_bC_r Color Model, Gaussian filter, Ant Colony algorithm.

1-Introduction

In the last years, face and facial expression identification have attracted much attention though they have been studied for more than 20 years by psychophysicists, neuroscientists, and engineers [1]. Numerous research demonstrations and commercial applications have been developed from these efforts. A first phase of any face processing system is detecting the locations in pictures where faces are present. However, face detection from a single picture is a challenging task because of variability in scale, location, orientation, and pose (frontal, profile), facial expression, occlusion, and lighting conditions also change the overall appearance of faces [2]. The main idea in this research is facial imprint detection based on utilizing Ant Colony algorithm as an edge detection algorithm; the essential trait of ACO algorithm is the combination of a priori information about the organizational chart of a promising solution with a posteriori information about the structure of previously obtained good solutions [3]. The remaining of this research as follows: in Part 2 some of the essential concepts used in this research will be explained along these lines fragments; Part 3 explains the presented algorithm. Part 4 the work outcomes; Part 5 final notes are given.

2-Related Work

In [1] the aim of edge detection, enthused from Ant algorithm, is fulfilled by Ant (ACO). For the determination of threshold computation, a novel technique of Fisher ratio (F-ratio) is used. The achievement of the work done is verified visually with the assistance of test pictures and empirically verified on the basis of many statistical factors of comparison. In [4] (ACO) algorithm is introduced to tackle the picture edge detection problem. A pheromone matrix is established to characterize the edge information presented at each pixel of the picture, according to the movements of a number of ants which are dispatched to move on the image. Investigational consequences are delivered to fix the superior performance of the presented algorithm.

3-Methodologies

A set of filters and techniques used in this research for convert face picture to other color model, detect the skin area, smoothing the face details and convert it to gray scale, for detecting the facial imprint. These techniques are explained in the next sections:

3-1 YC_bC_r Model

YC_bC_r Color Model represents color as brightness and two color difference signals, while RGB represents color as red, green and blue. In YC_bC_r , the Y is the brightness (luma), C_b is blue minus luma (B-Y) and C_r is red minus luma (R-Y); it is an encoded nonlinear RGB signal. Color is represented by luma [5], constructed as a weighted sum of the RGB values, and two color

difference values C_r and C_b that are formed by subtracting luma from RGB red and blue components. The conversion can be explained as equations below:

$$Y = 0.299R + 0.587G + 0.114B \quad \dots (1)$$

$$C_b = 128 - 0.168736R - 0.331264G + 0.5B \quad \dots (2)$$

$$C_r = 128 + 0.5R - 0.418688G - 0.081312B \quad \dots (3)$$

The transformation simplicity and explicit separation of luminance and chrominance components makes this model attractive for skin color modeling [6], [7].

3-2 Median Filter

Spatial filtering is usually done for noise removal; among the most commonly used filters is median filter. This type of filter is nonlinear, characterizing by reduce the noise with saving sharp and precise details exist in picture [8].

3-3 Gaussian Filter

It is a 2D convolution operator. The form of filter clarified as follow:

$$f(x, y) = \frac{1}{2\pi\sigma^2} \exp\left(-\frac{x^2+y^2}{2\sigma^2}\right) \quad \dots (4)$$

Where x, y are the distance from the origin in the horizontal and vertical axis and σ is the standard deviation of the Gaussian distribution. There are two aims from exploiting this kind of filter; first aim is for de noise and the second for blurring [9].

3-4 Gray-scale Image

The brightness value is the only constituent of gray scale image, each pixel value characterized by 8 bits [0 – 255]. To determine the gray value from the colored image, the following formula is utilized [10]:

$$G(x, y) = \text{Threshold}\left(\frac{R+G+B}{255}\right) \quad \dots (5)$$

Where $G(x, y)$ is the gray value; the red, green, and blue color components represented by R, G, B respectively.

3-5 Ant Colony Optimization

ACO is a meta-heuristic population founded approach for discovery optimal solutions [3] as explain in ACO_MetaHeuristic algorithm. The basis of ACO is the food researching behaviors of real ants. While walking from their nest to the food source and vice versa as shown in Figure (1), ants deposit on the way a kind of substance called pheromone in which its concentration becomes weaker with elapse of time due to evaporation. Pheromone is exploited to exchange information about which route should be followed. The more of ants traces given route, the stronger the pheromone concentration and thus more attractive this track becomes [11], [12] and [13].

ACO_MetaHeuristic algorithm

```
while(not_stop condition)
    generate Solutions()
    daemonActions()
    pheromoneUpdate()
end while
end algorithm
```

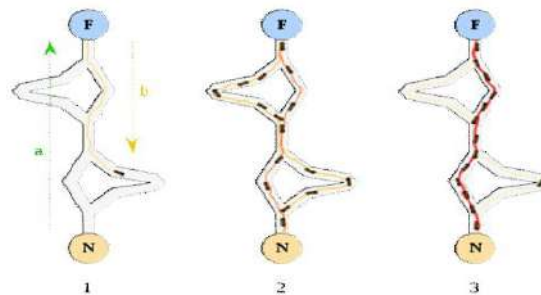


Fig. (1): Ants follow a route between Nest and Food

The motion of ants from a pixel to another pixel is probabilistically dictated by the transition probabilities. All pixels of the image are initialized with small value of pheromone.

4-Presented Algorithm

The framework of detecting human facial imprint algorithm is consists of the following steps and as shown in Figure (2):

Step 1: Read a RGB face image m of size $(N \times N)$, where N and N are rows and columns of the image respectively.

Step 2: m_{YCbCr} is gained by calculating YCbCr value for each pixel as explained in section (3.1) to m .

Step 3: m_{Skin} is obtained by applying range rule on m_{YCbCr} as explained in section (3.2).

Step 4: $m_{De-noise}$ is obtained by applying median filter on m_{Skin} as explained in section (3.3).

Step 5: m_L is obtained by applying research algorithm to $m_{De-noise}$ as clarified in section (3.4).

Step 6: m_{Clip} is obtained by applying Clipping step to m_L as explain in section (3.5).

Step 7: m_{Smooth} is gained by applying Gaussian filter to m_{Clip} as explained in section (3.6).

Step 8: m_{Gray} is gained by converting the m_{Smooth} to gray scale image as clarified in section (3.7).

Step 9: $m_{Faceimprint}$ is gained by applying ACO on the m_{Gray} resulted from step 8 as explained in section (3.8) which represents the final output of the presented algorithm.

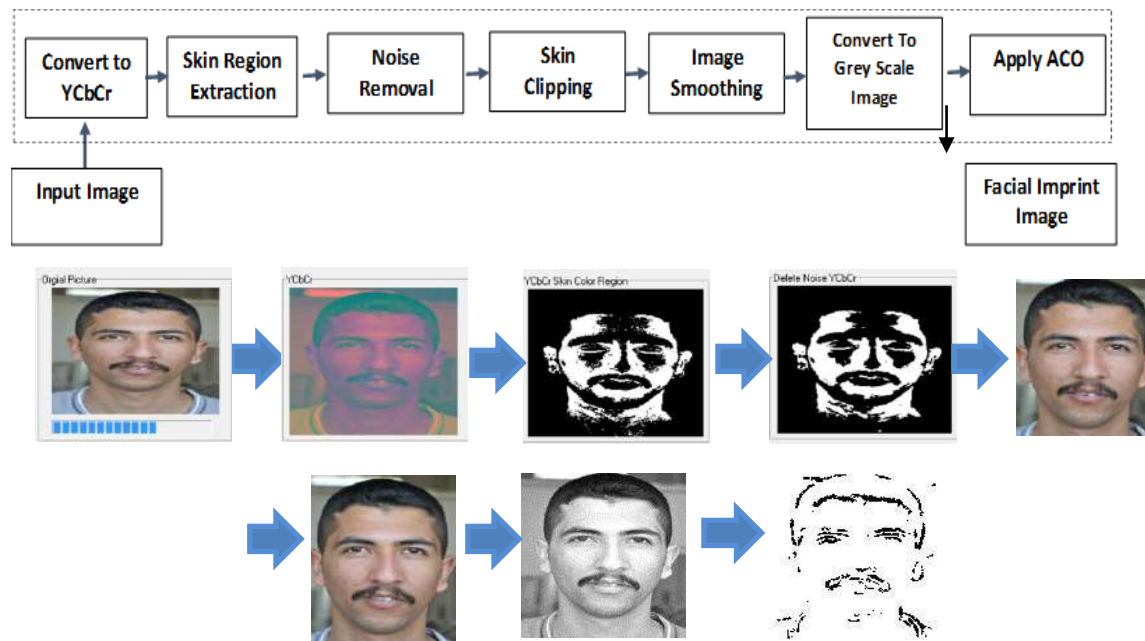


Fig. (2): The outcomes of Presented algorithm steps

4-1Concert to $YCbCr$ Color Model Step

In this step, the color face picture converts to $YCbCr$ model as explain in section (2.1). The Figure below shows the result of converting process.

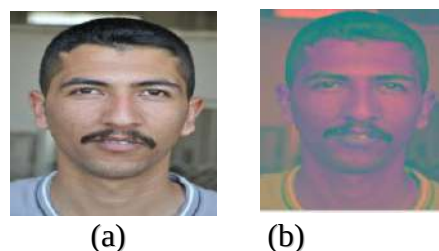


Fig. (3): Convert color face picture to $YCbCr$ Color Model: (a) face picture in RGB color model (b) after converting face picture to $YCbCr$ color model

4-2 Skin Area Detection Step

The detection process of skin area depend on the observation that the $YCbCr$ sub model is a strong distinguish of skin color, 4 range rules was formulated from it, The range rules are derived for intensity values between (0 - 255) for each of Y, C_b and C_r bands as presented in Figure (4).

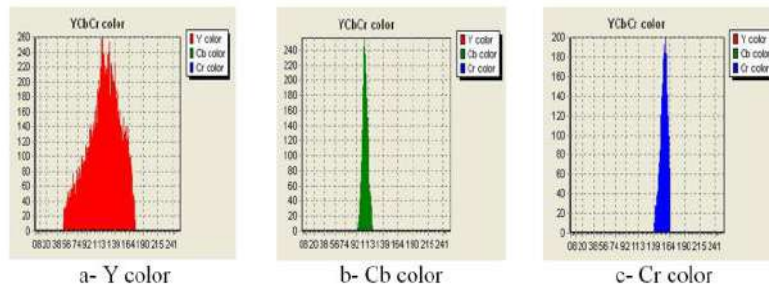


Fig. (4): Distribution of sub model Y, C_b , C_r

The 4 range rules as below:

$$\begin{aligned} &(Y > 50) \text{ and } (Y < 175) \text{ and} \\ &(C_b > 90) \text{ and } (C_b < 120) \text{ and} \\ &(C_r > 140) \text{ and } (C_r < 165) \text{ and} \\ &(C_r > C_b) \text{ and } (C_r - C_b > 15) \end{aligned} \quad \dots (6)$$

Then, each pixel that achieves range rule as Eq. 6 is classified as a skin pixel.

The result of this step is binary picture; the white color representing skin area and black color representing non skin area; also noisy pixel, as clarified in Figure (5).

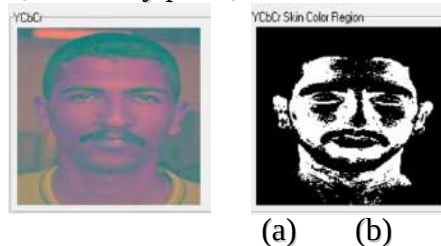


Fig. (5): Skin area detection process:
(a) face picture in $YCbCr$ color model (b) After skin area detection

4-3 Remove Noise Step

Medium filter is applied in this step for reducing the noise pixels. the size of filter which is applied equal (3×3), and is applied three times to get best outcome as shown in figure below.

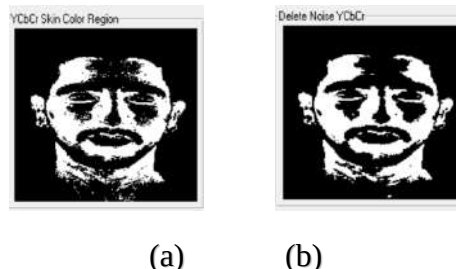


Fig. (6): Skin area de noise:
(a) before de noise (b) After de noise

4-4 Localization Face Area Step

The goal of this step is localizing and extracting face area from face picture. The location of skin area is localized based on checking the values of x and y-coordinates; the minimum and maximum

x values represent the left and right margins, while minimum and maximum y values represent the top and bottom margins, respectively and as shown in Figure (7).

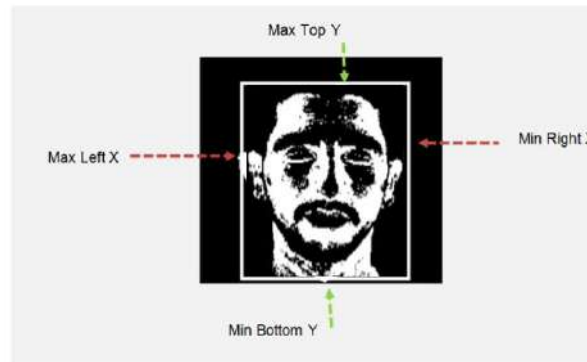


Fig. (7): localization skin area

4-5 Clipping Step

Face area is clipping in this step, without unnecessary parts like right ear, left ear, neck and Palate as shown in Figure (8). The result is necessary to determine the required face clip in color model.



Fig. (8): Face clipping step

4-6 Image Smoothing Step

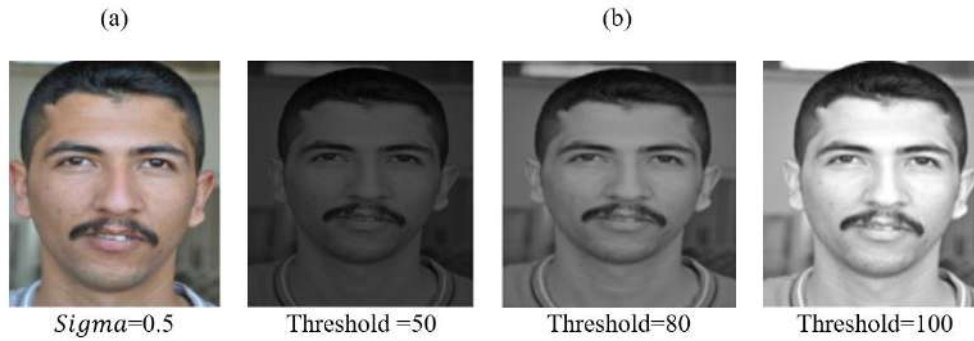
Gaussian filter as expressed in Eq. 1 is utilized in this step of presented algorithm. The goal of this step is to obtain better edge extraction outcomes. Figure (9) explains application of filter with mask size (3×3), (5×5) and (7×7) and sigma values (0.5, 1, and 1.5). The sigma equal to (0.5) has been selected in this research.



Fig. (9): Explains the applying of Gaussian filter with different sigma values

4-7 Convert to Gray Scale Step

In this step of presented algorithm; Eq. 2 has been applied; the proper threshold value is (50) assessed after trying different threshold values to the image resulted from smoothing step. Figure (10) below explains the outcomes of applying different threshold value.



(a) face picture after Gaussian filter (b) face pictures after converting to Gray-Scale

4-8Ant Colony Optimization for Edge Detection

In ACO algorithm for edge detection, ants move through a research space, the graph which consists of nodes and edges. The pixels in the digital image can be considered as the nodes of a graph. The steps of ACO algorithm is as follow:

Step 1: initialization process

Completely N ants are arbitrarily allocated on an image **img** with a size of $n1 \times n2$, each pixel of which can be viewed as a node. The first value of each component of the pheromone matrix $\mathbf{m}$ (0) is set to be a constant **minit**.

Step 2: construction process

At the n construction-stage, one ant is arbitrarily chosen from the total A ants, and this ant will consecutively move on the image for l movement- strides. This ant moves from the node (l, m) to its neighboring node (i, j) according to a move likelihood is defined as this equation:

$$P_{(l,m),(i,j)}^{(n)} = \frac{(t_{i,j}^{(n-1)})^\alpha (\eta_{i,j})^\beta}{\sum_{(i,j) \in \Omega(l,m)} (t_{i,j}^{(n-1)})^\alpha (\eta_{i,j})^\beta} \quad \dots (7)$$

Where m $(n-1)$ i, j is the pheromone amount of the node (i, j) , $\Omega(l, m)$ are the neighborhood nodes of the node (l, m) , $\eta_{i,j}$ represents the heuristic information at the node (i, j) . The constants α and β represent the influence of the pheromone matrix and the heuristic matrix, respectively.

Step 3: update process

The presented algorithm apply (2) updates processes for updating the pheromone matrix.

1. The first update is applied after the movement of each ant within each construction-step. Each element of the pheromone matrix is updated as this equation:

$$T_{i,j}^{(N-1)} = \begin{cases} (1-p) \cdot T_{i,j}^{(n-1)} + p \Delta_{i,j}^{(k)} & \text{if } (i,j) \text{ is visited by the current } A - \text{th ant} \\ T_{i,j}^{(n-1)} & \text{otherwise} \end{cases} \quad \dots (8)$$

Where p is defined in (2), $\Delta(k) i, j$ is specified by the heuristic matrix; that is, $\Delta(k) i, j = \eta_{i,j}$.

2. The second update is applied after the movement of all ants within each construction-step as this equation:

$$T^{(n)} = (1 - \rho) \cdot T^{(n-1)} + \rho \cdot T^{(0)} \quad \dots (9)$$

Step 4: Decision Process

In this stage, a binary choice is made at each pixel position to determine whether it is edge or not, by applying a threshold T on the last pheromone matrix $\mathbf{m}$ (N). In this work, the above-mentioned T is presented to be adaptively computed based on the process developed in [9]. The whole process of the ACO is as follow:

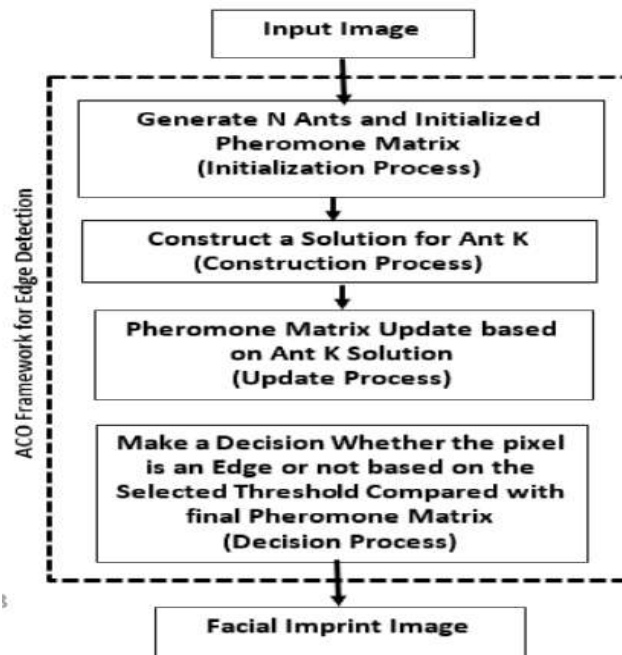


Fig. (11): the Layout of ACO algorithm

5-Experimental Results

The dataset that are used for training and testing the presented algorithm collected from 30 volunteers consist of different samples; 10 samples for each person, the images were taken with varying pose, orientation (tilting and rotation about to 30 degrees in two directions left and right), and expressions (surprise, sadness, look up/down and smiling/non-smiling). Not all images are taken with the same background; the face is in frontal position. The picture is read as BMP 24 bit. As shown in Fig. (7), in experiments the presented algorithm has attained high edge detection rates. This work has demonstrated that the effect of factors (smoothing degree, lightness) actually a practical solution to generate accurately facial imprint from face picture that can be used for farther processing extraction feature and recognition aim.



Fig. (12): the outcomes of presented algorithm

6- Conclusions

The conclusion have been derived from the examinations outcomes; for face detection phase based on YC_bC_r color model leads to higher detection rate. The presented algorithm for localizing and extracting face clip is shows best result; even though there are the variant of pose, orientation and expression. The outcomes of the showed examinations on data set pictures show that the best attained edge detection rate happens by applying ACO algorithm on face picture when using the values of factors window size of Gaussian filter equivalent (3×3) and its sigma (0.5), threshold of gray scale equivalent (50). The modeling of pheromone depositing by ants in their research for paths to food sources led in the development of algorithm to obtain the facial imprint.

References

- [1] Prashant Kumar Mohanty, "On Edge Detection of Images Using Ant Colony Optimization and Fisher Ratio", Department of Electronics and Communication Engineering National Institute of Technology Rourkela Rourkela- 769008, India in 2012.
- [2] Ningthoujam Sunita Devi, Prof. K. Hemachandran, "Automatic Face Recognition System Using Pattern Recognition Techniques: Survey", International Journal of Computer Applications Volume 83 No 5, December 2013.
- [3] Dr. Mafaz Mohsin Khalil Al-Anezi, Omar Nazar Bader, Zainab Mohammad Abdullah and Ayad Imad Atallah "Intrusion Detection and Classification Using Ant Colony Optimization Algorithm", Iraqi Journal of Statistical Sciences, the 6th Scientific Conference of the College of Computer Sciences & Mathematics in Oct. 2013.
- [4] P. Thukaram and S.J.Saritha, "Image Edge Detection Using Improved Ant Colony Optimization Algorithm", JNTUACEP, INDIA, International Journal of Research in Computer and Communication Technology, Vol 2, Issue 11, November- 2013.
- [5] Chris Solomon and Toby Breckon "Fundamentals of Digital Image Processing", Physical Sciences, University of Kent, Canterbury, UK, in 2011.
- [6] PHUNG, S. L., BOUZERDOUM, A., AND CHAI, D. "A novel skin color model in YC_bC_r color space and its application to human face detection", In IEEE International Conference on Image Processing (ICIP'2002), vol. 1, 289–292. In 2002.
- [7] V. Vezhnevets, V. Sazonov and A. Andreeva "A Survey on Pixel-Based Skin Color Detection Techniques", Graphics and Media Laboratory, Faculty of Computational Mathematics and Cybernetics, Moscow State University, Moscow, Russia in 2003.
- [8] Wilhelm Burger, Mark J. Burge, "Principles of Digital Image Processing", Fundamental Techniques, Springer, in 2009.
- [9] Chris Solomon and Toby Breckon, "Fundamentals of Digital Image Processing", Physical Sciences, University of Kent, Canterbury, UK, in 2011.
- [10] Gonzalez R., Woods R. "Digital Image Processing", Second Edition, Prentice Hall, in 2002.
- [11] Manish T, Dr. D Murugan and Ganesh Kumar "Hybrid Edge Detection Using Canny and Ant Colony Optimization", Manonmaniam Sundaranar University, Tamilnadu, Communications in Information Science and Management Engineering, Vol. 3 Iss. 8, PP. 402-405, in Aug. 2013.
- [12] Rabia Jafri, Hamid R. Arabnia, "A Survey of Face Recognition Techniques", Journal of Information Processing Systems, Vol. 5, No.2, in June 2009.
- [13] ANNA VERONICA C. and CARLOS M. OPPUS "Ant Colony Optimization for Image Edge Detection", Department of Electronics and Communications Engineering Ateneo de Manila University, in 2008.

Modify Multi-Connect Architecture (MMCA) Associative Memory

Rusul Hussein Hasan¹

Emad I Abdul Kareem²

¹College of Law, Baghdad University, Iraq, Baghdad.

²College of education in Computer Science, Mustansiriyah University, Iraq, Baghdad.

rshs97@yahoo.com

mmimad72@yahoo.com

Abstract:

Associative memory is a data collectively stored in the form of a memory or weight matrix, which is used to generate output that corresponds to a given input, can be either auto-associative or hetero-associative memory. Multi-Connect Architecture (MCA) neural network model for auto-association and optimization tasks. A Modify Multi-Connect Architecture (MMCA) has been suggested to improve the MCA neural network by modifying the net architecture, learning and convergence processes, and this modification is to increase the performance of associative memory neural network. This research will propose modifying multi connect architecture associative memory to improve the efficiency of Multi-Connect Architecture in order to decrease the network size and weight size. In addition to increase the ability for noise robust as well as speed up its learning and convergence process. The results proved that the Modify Multi-Connect Architecture net can learn and recognize unlimited patterns in varying sizes with the acceptable percentage noise.

Keywords: Neural Network, Associative Memory, Hopfield Neural Network, Pattern Recognition.

تعديل الهندسة المعمارية متعددة الاتصال

عماد عيسى عبد الكريم

رسل حسين حسن

المستخلص

الذاكرة التجمعية هي البيانات المخزنة بشكل جماعي في شكل ذاكرة أو مصفوفة ، والتي يستخدم لتوليد مخرج الذي مع مدخلات المعطاه، يمكن أن تكون إما ذاكرة auto-associative او ذاكرة hetero-associative. متعدد الاتصال العمارة (MCA) هو نموذج الشبكة العصبية للمهام التنظيم الذاتي والتحسين. وقد اقترح تعديل الهندسة المعمارية متعددة الاتصال (MMCA) لتحسين الشبكة العصبية MCA عن طريق تعديل معمارية الشبكة والتعلم وعمليات التقارب، وهذا التعديل هو لزيادة أداء الشبكة العصبية الذاكرة التجمعية. هذا البحث سوف يقترح تعديل متعددة ربط العمارة الذاكرة النقابي لتحسين كفاءة الهندسة المعمارية متعددة الاتصال من أجل تقليل حجم الشبكة وحجم الاوزان. بالإضافة إلى زيادة القدرة قابليتها على تقبل الضوضاء قوية وكذلك تسريع عملية التعلم والتقارب. وأثبتت النتائج أن الشبكة تعديل متعدد الاتصال الهندسة المعمارية يمكن أن تتعلم تميز أنماط غير محدودة في أحجام مختلفة مع نسب مختلفة من الضوضاء.

الكلمات المفتاحية: الشبكات العصبية، الذاكرة الترابطية، شبكة الهوبفيلد، تمييز الانماط.

1- Introduction

One of the neural networks that are used for optimization task and auto-association is a Hopfield neural network (HNN). HNN has many limitations, which are effected in its performance. Firstly, patterns number that can be accurately recalled and stored is severely limited, the second problem, there is possibility for return stored pattern with inverse values, the third problem is ratio of mistake and missing data in unknown pattern is limited, the Fourth problem is correlation which is happens when unknown pattern share many bits with another pattern, the fifth problem is it is clear desirable to reach global minimum rather than setting down at a local minimum as it can happen while using the energy function and the sixth problem it is impossible to return stored pattern when enter it to HNN with scaling or shifting. [1]

To avoid most Hopfield limitation using MCA, but the scaling and shifting problem cannot void it. In additional, the efficient learning, convergence process and smaller size of network.

This paper present to improve MCA efficiency by decrease weight, size and network size. In additional to speed up its learning phase and convergence phase as well as, increase ability for noise robust. Like to HNN and MCA, the MMCA neural network is a single layer that is, using auto-association task which is working two phases (i.e., Learning phase and convergence phase). The experiments illustrated promising results when MMCA offers high efficiency to distinguish high noise rate in patterns with different size comparing with MCA and HNN.

2- Related Work

Anyway, MCA is improving in auto associative memory, this paper shows related work for auto-associative memory modification.

Abbiss and et al. Present procedure of implementation NN which is depended on HNN, which is used various code schemes and there are two elements consists in the networks, while that consisting of more complex neurons were able of representational connection. [2]

Dotseniko and et al. The present theory of mean filed, that is similar to HNN but has modified interactions. Interactions modification it has been achieved by a special thermal noise recurring procedure. Result links had an intermediate form between pseudo inverse and Hebb-like learning rules. Obtainable replica symmetric free energy of model. [3]

Lee and Sheu described analysis on locations of HNN local minima, also presented improve architecture of the network to remove such local minima. Specially, introduced another amplifier at processor neurons to give correct condition. This HNN modification has been implemented to analog to digital construction converter with optimal solution. [4]

Li described augmented Lagrange Hopfield (ALH), which is new method to modify HNN in both solution quality and convergence process in solving combinatorial optimization, that is used ALH, which combines both penalty method and Lagrange method to effectively solve dilemma. [5]

Cavalieri and Russo present fuzzy-logic depended algorithm to automatically determine the coefficients, which limited intervention of required human. In additional, define the rules of fuzzy logic, which is reproduced acquired manual experience when determining HNN coefficients in applications number. [6]

Zeng and Martinez present, relaxation rate to control relaxation process to improve the performance of HNN. The analysis suggested that relaxation process had important impact on solution quality. To control the relaxation process introduced relaxation rate to acquired better quality solutions. [7]

Gimenez-Martinez present procedure for recurrent neural network implementing depended on well-known HNN adapting. Recurrent neural network shown as complete graph, in additional, learning mechanism is depended on law of Hebb's, but with very important difference. Thus, weight that is dynamics control of network is happened by graph of coloring. [8]

Garcia and Morenos present new insight to HNN training by using theory of kernel, which is drawn from work on their related algorithms and learning machines of kernel. Therefore, the kernel "trick" is used to define included pattern of memory to feature vectors of memory, which allow network training to be carried out in feature space without explicitly representing it. Improve performance of network by introduction of kernel theory in network training phase. [9]

Bauk and et al. Present, the inverse polarized diode replaced with capacitor with large capacity to shift, anyway, parameters of HNN analysis from linear differential equation field to exponential transcendental equation field, solvable analytically by method called linear approximation depended on the STFT (special Trans function theory). Also present on other paper, HNN modification, which is allowed to description behavioral by transcendental exponential equation system solvable analytically by special Trans function theory. [10, 11]

Wu and coworkers present modification version to modified HNN by using sequential algorithm depended on continuous state change. In additional, maximal energy descent in update rule. [12]

Dehghan and et al. described, applied finite various techniques of equation of Helmholtz- on this property to minimize energy functions. Additional, correlation and mathematical representation between modified HNN and finite techniques of equation of Helmholtz. [13]

A.H. Muhammad Amin and et al. proposed novel distributed single cycle learning algorithm depended on concept of associative memory called Distributed Hierarchical Graph Neuron (DHGN), which is used to improve and extend improved version of Graph Neuron (GN) algorithm. The Graph Neuron (GN) algorithm is real-time recognition scheme and scalable, which is used in pattern recognition scheme in mobile network. [14]

Emad Issa and et al. proposed method to improve HNN by modified architecture of network, learning phase and convergence phase, called Multi-connect architecture (MCA). This modification is avoid most of HNN limitations that leads to increase the performance of HNN. [15]

The DHGN and MCA have the same goal is to improve the Hopfield neural network by modifying architecture of the network, learning phase and convergence phase. While the other related work used improve HNN for specially purpose.

3- Associative Memory

Associative Memory (AM) believe that memory of human is saved in form of complex interconnection between different nodes. In artificial neural network (ANN) simulating AM, the data are collective saved in form of weight matrix or memory, to generate output pattern that matched to given input pattern. That process is indicate to storing or learning the desired patterns, while recall process or retrieval process is indicate to generate of output pattern [16]. Figure (1) illustrated AM system performing in block diagram, that associative mapping for input vector (x) to output vector (v) as shown in Equation (1).

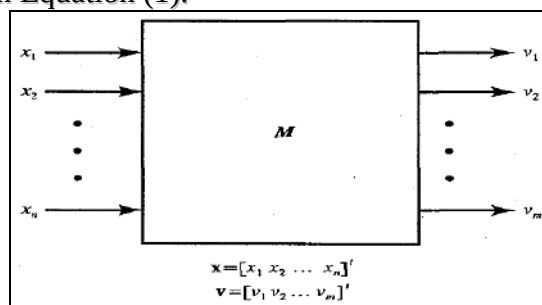


Fig. (1): Block Diagram of AM.

$$v=M[x] \quad \dots (1)$$

The AM system offer map vector x into vector v , in space of input and space of output, respectively, by transformation. The operator M indicate to nonlinear matrix-type operator; that has various meaning for each memory form. Which are defines a practical model that needs to be carefully outlined for each kind of memory. The operator M include time variable for dynamic memories. In the memory output, v will be available at a later time when the input is applied [17].

AM can be implemented in any hetero-associative or auto-associative applications. Mathematically, AM is map from space of input into space of output. In general, as shown in Figure (2) the dimensions of input and output spaces are various in hetero-associative memory. While, input and output spaces of auto-associative memory are similar, as shown in Figure (3). [1] [17]

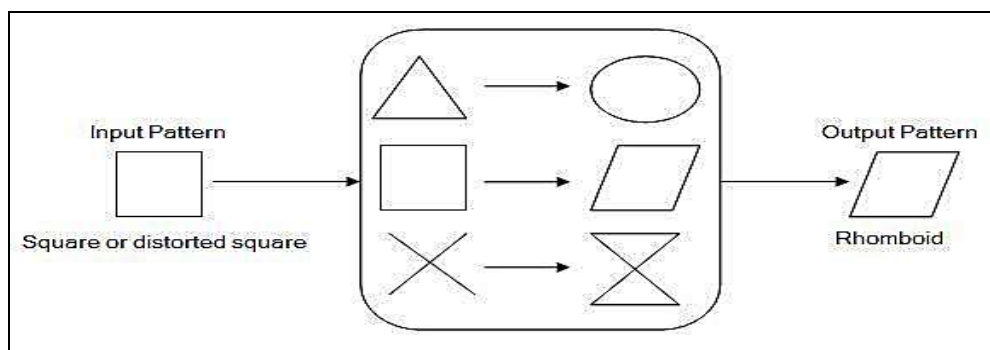


Fig. (2): Hetero-association Memory.

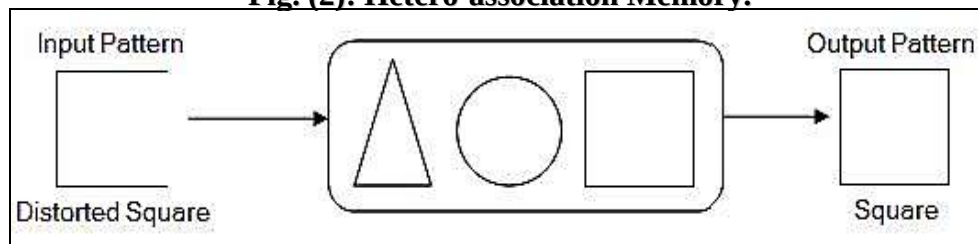


Fig. (3): Auto-association Memory.

Multi Connect Architecture (MCA) is the one of the auto-associative memory neural networks, which is presented in the next section.

3-1 Multi Connect Architecture (MCA) Associative Memory [15, 18]

MCA is one of NN models that present in this research, which is improve HNN by modifying network architecture, learning process and convergence process. In general, MCA is single layer, that is use auto-association task which is work in two phases (i.e., learning phase and convergence phase). MCA was developed depended on two principles, the first principles is, use smallest size of network rather than based on length pattern size. The second principles is, avoid learning similar parts many times in learning process which is performed to limited parts of pattern only.

The number of neurons in Hopfield network (Hopfield network size) based on length of pattern used by Hopfield (i.e., the pattern with length (100) requires Hopfield network of size (100)). Therefore, MCA is modified HNN, According to the first principle, divided pattern to set of vector with length three (i.e., the network size will be only three). Thus, MCA network will deal with part of pattern instead of entire pattern as one vector.

The smallest size of network lead to benefit working, as well as multiple connections among three nodes. The new architecture of MCA lead to avoid learning same vectors many times. The cause for choose vector length is shortest odd length of vector is three. Which is need due to vector majority description (vmd: is sum each elements of vectors is be negative and positive), which is paly role to overcoming HNN problem. In the next subsection explain MCA architecture.

3-1-1 MCA Architecture

Like HNN, each neuron is connect to all other neuron but not to itself. These connections between neurons represent weight for each vector. The number of connections between neurons is four, although the number of vectors is eight, which based on fact each pair of orthogonal vectors has the same weight. All connection weights is symmetric, thus, weight from neuron j into neuron i is same as that from neuron i into neuron j; therefore, $w_{ji} = w_{ij}$ and $w_{ii} = 0$. The network architecture leads into assumed threshold is zero.

The information of MCA network does not flow in single direction that is possible for signal to flow of neuron back to itself during other neurons. Thus, there is recurrent because neurons may be used repeatedly to process information or network feedback. This is to contrast with feed forward network as illustrate in Figure (4).

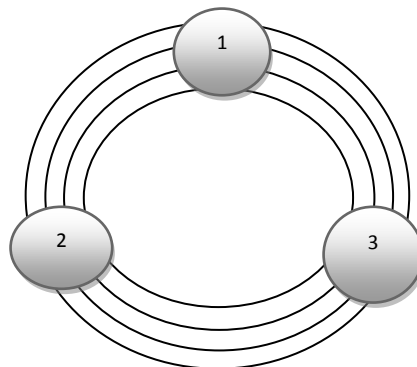


Fig. (4): MCA network.

3-1-2 MCA Algorithms

After explain the new architecture for MCA, it is important to view algorithms for the network (i.e., learning phase and convergence phase).

(a) Learning phase

Through the implementation learning phase, MCA is able to distinguish all required bipolar vectors in pattern. Thus, the input of learning phase is set for patterns that considered as training patterns for MCA. The output of learning phase are in two parts, firstly is set of weights for all vectors of patterns (Named: save vector weight (svw)). Secondly is set of vectors that are the majority

description for all vectors of pattern (Named: save majority description (smd)), which are stored in a lookup table. Figure (5) shows algorithm for MCA.

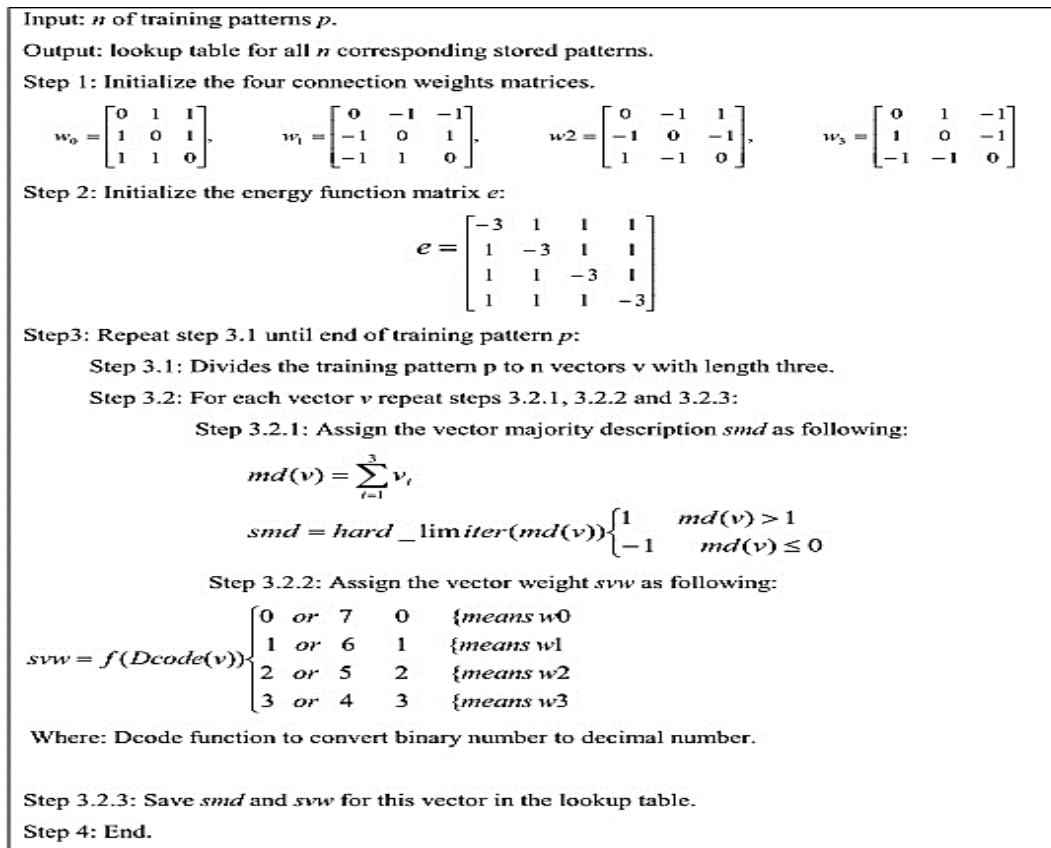


Fig. (5): MCA Algorithm for Learning Phase.

(b) Convergence Phase

Four weights and energy function matrices are initialized in convergence phase as shown in Figure (6).

4- Proposed Modify Multi Connect Architecture (MMCA) Associative Memory

Similar to the MCA, in MMCA each pattern will be divided to set of vectors, each vectors with two elements (i.e., the network size is two). The smallest size of network leads to benefit working. Like HNN and MCA, each neuron of MMCA is connecting to all other neuron but not to itself. These connections between neurons represent weight for each vector. The number of connections between neurons is two, although the number of vectors is four, which based on fact each pair of orthogonal vectors has the same weight. All connection weights is symmetric, thus, weight from neuron j into neuron i is same as that from neuron i into neuron j ; therefore, $w_{ji} = w_{ij}$ and $w_{ii} = 0$. The network architecture leads into assumed threshold is zero. As shown in Figure (7).

MMCA used to improve MCA efficiency by decrease weight size and network size. In additional to speed up its learning phase and convergence phase as well as, increase ability for noise robust.

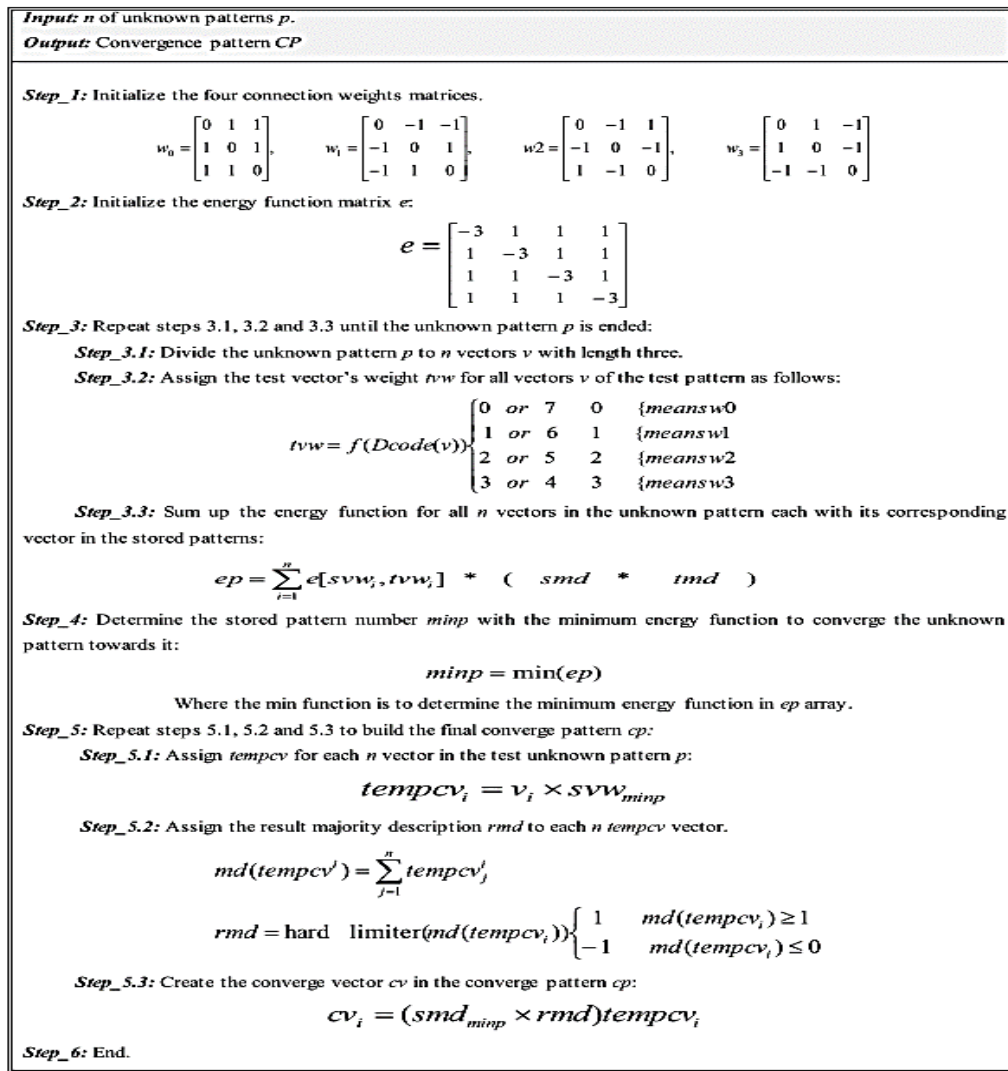


Fig. (6): MCA Algorithm for Convergence Phase.

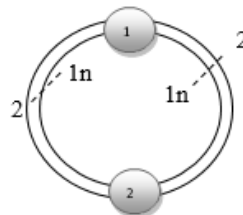


Fig. (7): MMCA Network.

(a) Learning Phase

A modification learning phase for MMCA based on learning phase for MCA, which is need to creates a symmetric weight ($t_{ij} = t_{ji}$) for training patterns without diagonal zero because that lead to oscillations in case. As illustrate in Figure (8).

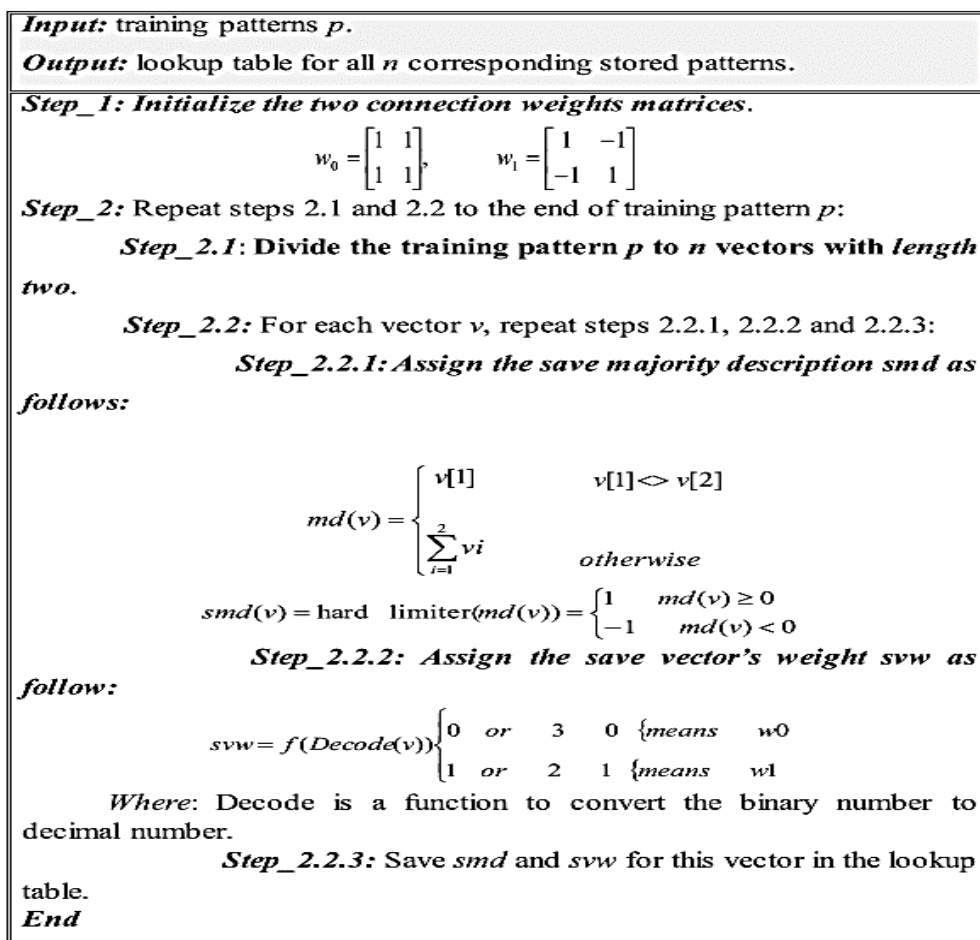


Fig. (8): MCA Algorithm for Learning Phase.

(b) Convergence Phase

Based on MCA convergence algorithm and similar to learning algorithm for MMCA, all two weights and energy function matrices are initialized and unknown pattern will be divided to set vectors with length two as shown in Figure (9).

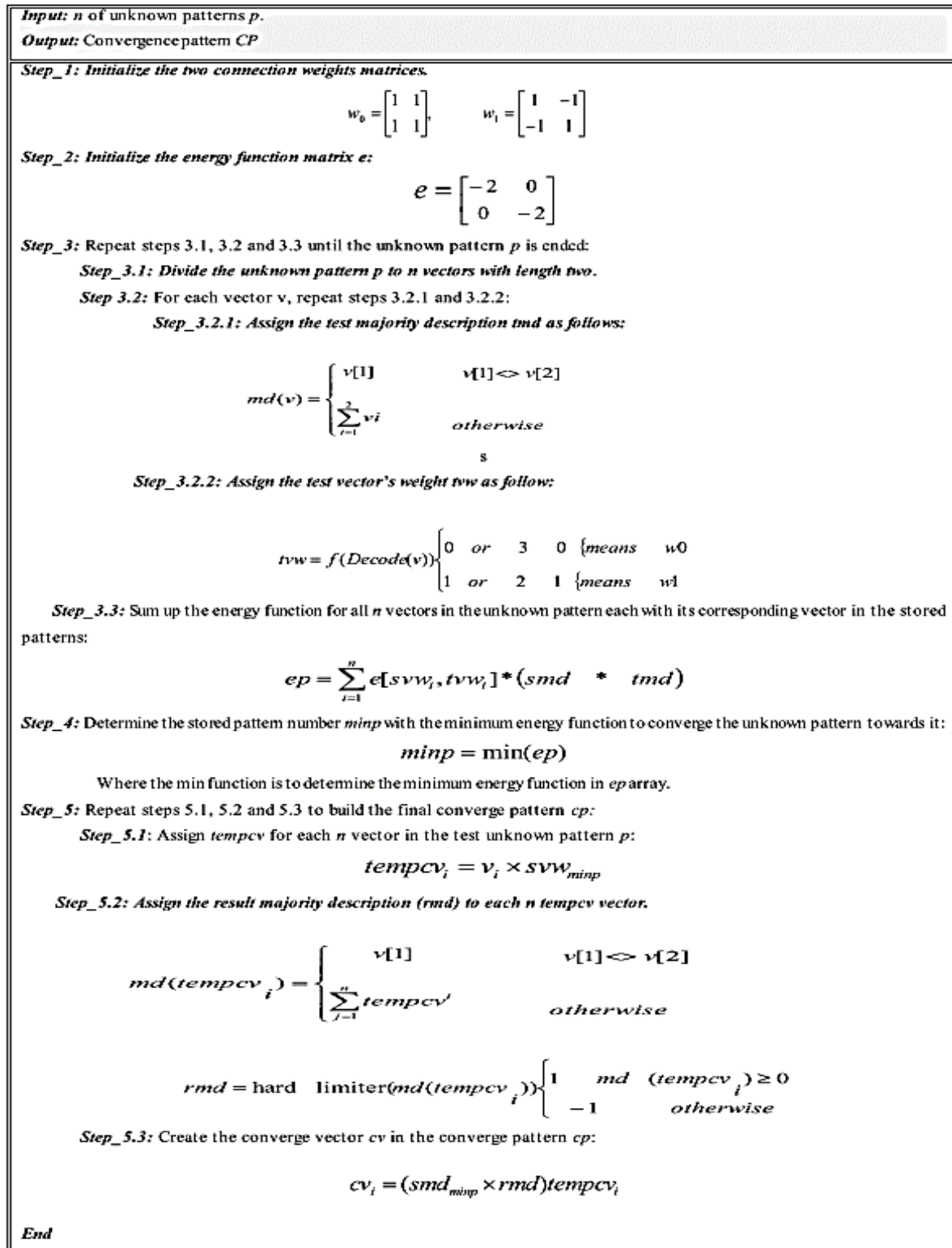


Fig. (9): MCA Algorithm for Convergence Phase.

5 -Result Evaluations of MMCA

There are three experiments to evaluate MMCA present in this section. Which applied to HNN, MCA and MMCA to allow comparison. The experiments measured efficiency of MMCA and compared with HNN and MCA, which is depended on analysing noise rate (mistake or missing pixels), the smallest network size and large number of training patterns.

5-1 Number of Stored Patterns

This experiment measured the number of stored pattern in networks, for HNN MCA and MMCA, this measure was depended on learn maximum number of patterns, this process was stopped when the networks completely failed to distinguished all stored patterns. This experiment based on alphabetical letters patterns without noise and size 10 x 10 as shown in Figure (10).

Number of Stored Patterns	Hopfield Network						MCA Network						MMCA Network					
	A	B	C	D	E	F	A	B	C	D	E	F	A	B	C	D	E	F
1	A						A						A					
2	A	B					A	B					A	B				
3	A	B	C				A	B	C				A	B	C			
4	A	B	C	D			A	B	C	D			A	B	C	D		
5	A	B	C	D	E		A	B	C	D	E		A	B	C	D	E	
6	A	B	C	D	E	F	A	B	C	D	E	F	A	B	C	D	E	F

Fig. (10): HNN, MCA and MMCA learning on six alphabetical English letters with converge patterns for all of them.

As shown in Figure (10), the learning phase occurred progressively begin from pattern one to six. To make sure there are three networks (i.e., HNN, MCA and MMCA) were able to recovery patterns until all or one of them arrive state of complete failure. HNN start to distinguish some patterns when number of patterns that had been learned was four. And when number of patterns became six HNN complete failure to return pattern.

5-2 Results Analysis and Discussion

When number of stored patterns increased that lead to decreased convergence rate of HNN, due correlation problem. In previous experiment the convergence rate was failure when the number of stored patterns become four and complete failure when the number of stored patterns become six. While the convergence rate of MCA and MMCA was 100% until number of stored patterns increased into 6 as shown in Figure (11).

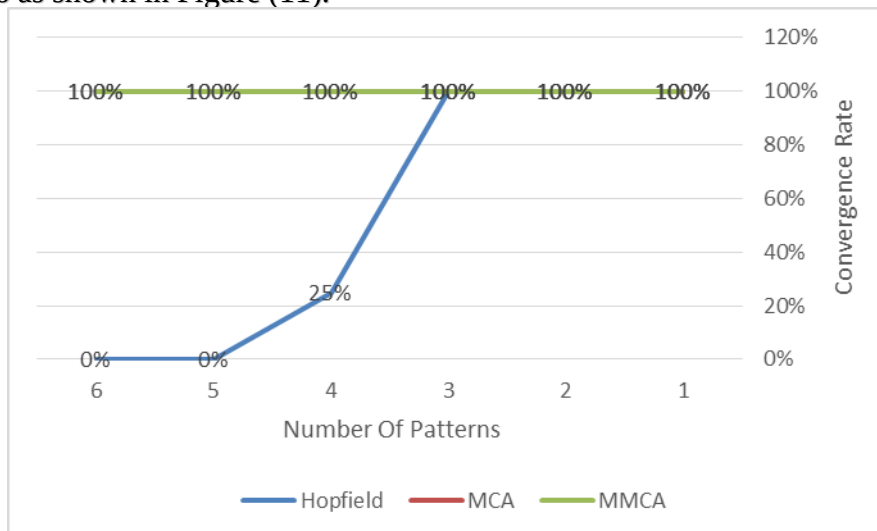


Fig. (11): Comparison between HNN, MCA and MMCA network for number of stored patterns.

In the previous experiment the stored pattern size was 10×10 . Therefore, the size of HNN was 100 neurons, which is depends on size of pattern. While the size of MCA and MMCA was kept at three and two neurons respectively.

5-3 Noise Rates

Depended on previous experiment, HNN kept efficiency at 100% until number of stored patterns was three (See Figure (10)) with 0% noise. Therefore, in this experiment, HNN, MCA and MMCA learned on three patterns with size 10×10 . In additional, this experiment have three tests, for each test having three patterns (i.e., A, B and C) with different random noise. The convergence process was applied with the networks by testing patterns with random noise ranging from 10% to 90% (See appendix A (A1, A2, A3)), which is illustrate response of the networks when the same patterns had learned previously were showed with various noise ranging from 10% to 90%

5-4 Results Analysis and Discussion

HNN efficiency was 100% until noise rate became 40%. While MCA and MMCA efficiency was 100% until noise rate became 50% and 60% respectively. Then the networks failed to recognize some stored pattern until noise rate became 90%. As shown in Figure (12) comparison between results for the networks.

In additional, HNN return any stored pattern with reserve color (i.e., white pixels became black pixels and vice versa). In MCA and MMCA, this phenomenon was not happened.

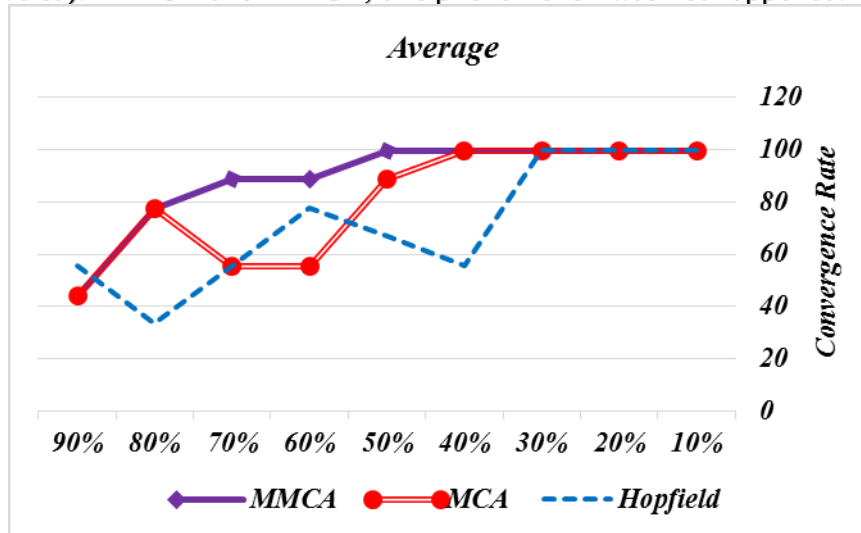


Fig. (12): Comparison Result between HNN, MCA and MMCA with various noise rates.

MMCA efficiency was 100% until noise rate become 60%. MMCA deal pattern as vector with length two, with small pattern there was possibility for random noise operation to change at least one pixel in all vectors of pattern. Thus, MMCA may not have distinguished pattern because its convergence phase based on these vectors.

5-5 Different Patterns Sizes with Different Noise Rates

177 patterns were presented with different noise ratios and different sizes of the networks as unknown patterns to determine rates of the convergence show in this experiment, This experiment, between MCA and MMCA networks because MCA and MMCA net can learn and recognize unlimited patterns with different sizes, unlike HNN is learn and recognize limited patterns (See Figure (10)).

5-6 Results Analysis and Discussion

Convergence rate of MCA and MMCA was more efficient when pattern size increased as illustrated in Figures 13 and 14.

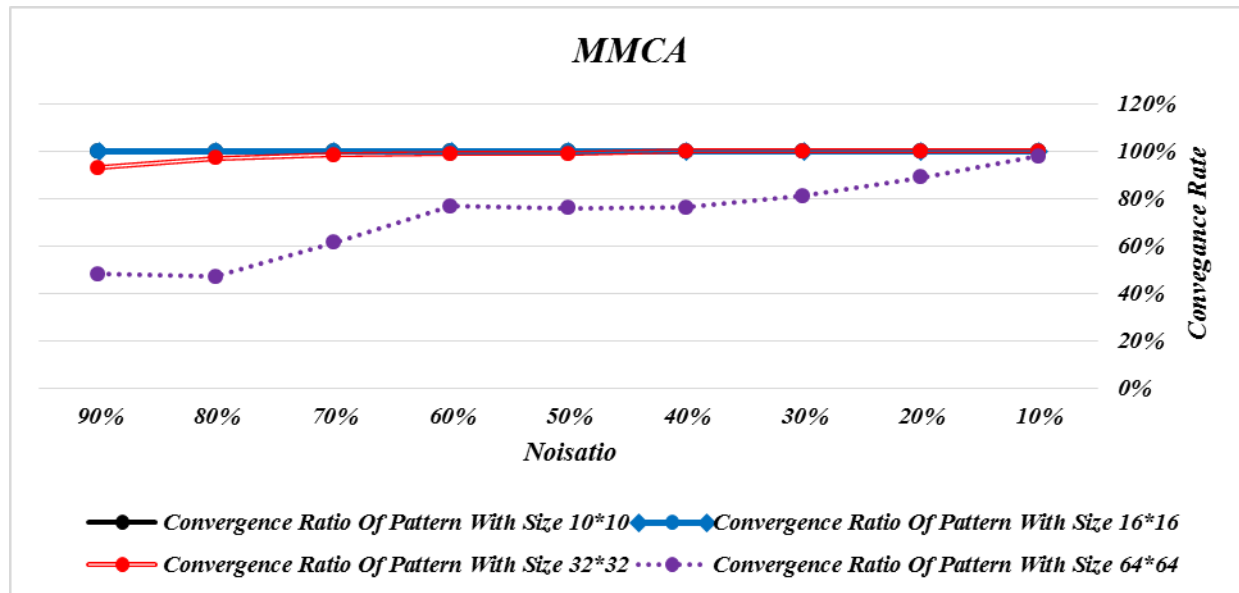


Fig. (13): Comparison between the 4 tests of 177 various noise rates and various patterns size for MMCA.

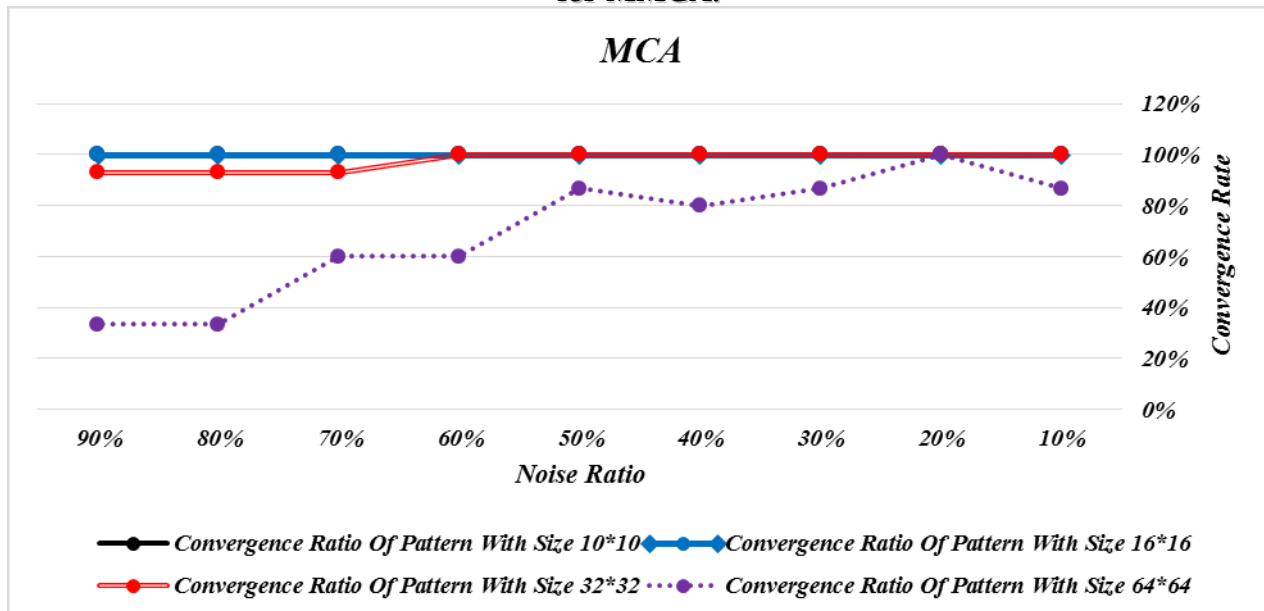


Fig. (14): Comparison between the 4 tests of 177 various noise rates and various patterns size for MCA.

MCA and MMCA efficiency was 100% with pattern size 32*32 and 64*64, with small patterns there was possibility for random noise operation to change at least one pixel in all these vectors. Because the convergence algorithm based on these vectors, MCA and MMCA may not have distinguished pattern. Thus, without or with noise, MCA and MMCA are efficient with large patterns size.

6- Comparison among the MMCA, MCA, (Distributed Hierarchical Graph Neuron and Hopfield

The algorithm described in DHGN (Distributed Hierarchical Graph Neuron) is single cycle learning algorithm depended on concept of associative memory [14].

This experiment was depended on allowable percentage of noise (i.e., compare pixel by pixel). Although this comparison, algorithms HNN, MCA, MMCA and DHGN are used five patterns in the

learning phase with noise rate 20% and size it 5x7 pixels. The efficiency comparison among HNN, MCA, MMCA and DHGN algorithms on characteristic patterns as shown in Figure (15).

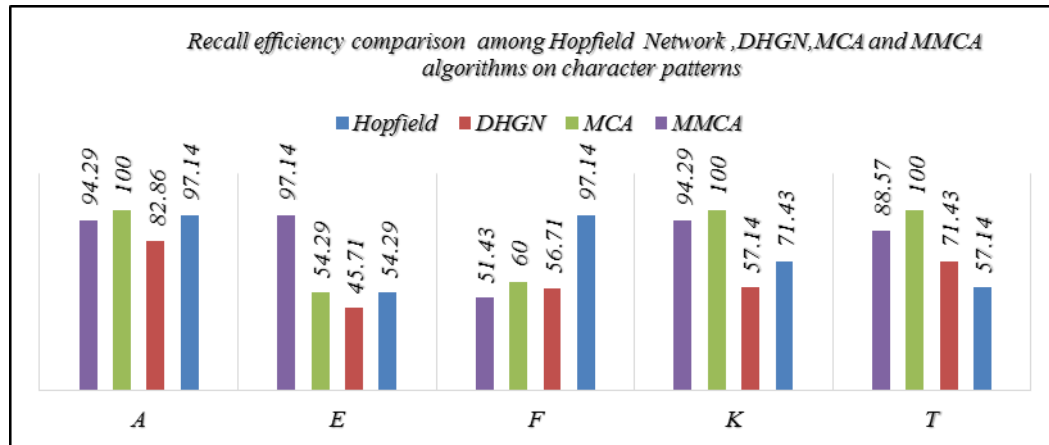


Fig. (15): The efficiency comparison among HNN, MCA, MMCA and DHGN algorithms on characteristic patterns.

7- Conclusion

This paper present to improve MCA efficiency by decrease weight size and network size. In additional to speed up its learning phase and convergence phase as well as, increase ability for noise robust. In addition, to increase ability for noise rate at 60%. And for architecture improved the MMCA size is still fixed (but with two nodes) with any size of pattern. This size of network caused that size of learning weigh matrix becomes smaller (two matrices with size 2*2). For learning process modification kept net reached unlimited stored pattern, i.e. MMCA still efficient even when the number of stored patterns increases. In additional, MMCA still kept MCA ability to avoid the Hopfield limitation which are converge rate, capacity, local minimum, correlation problem, and retrieving stored pattern with inverse pixels. In additional MMCA still failed to distinguish any stored patterns if shifting and scaling.

References

- [1] Faustt, L., "Fundamental of Neural Networks Architecture", Algorithms and Application Prentice Hall, 1994.
- [2] Abbiss, J.B., B.J. Brames, and M.A. Fiddy, "Superresolution Algorithms for A Modified Hopfield Neural Network. IEEE Transactions on Signal Processing", 1991. 39(7): p. 1516-1523.
- [3] Dotsenko, V. S., N. D. Yarunin, and E. A. Dorotheyev, "Statistical-Mechanics of Hopfield-Like Neural Networks with Modified Interactions". Journal of Physics a-Mathematical and General, 1991. 24(10): p. 2419-2429.
- [4] Lee, B.W. and B.J. Sheu, "Modified Hopfield Neural Networks For Retrievin0g The Optimal Solution". IEEE Transactions on Neural Networks, 1991. 2(1): p. 137-142.
- [5] Li, S.Z., "Improving convergence and solution quality of Hopfield-type neural networks with augmented Lagrange multipliers". IEEE Transactions on Neural Networks, 1996. 7(6): p. 1507-1516.
- [6] Cavalieri, S. and M. Russo, "Improving Hopfield neural network performance by fuzzy logic-based coefficient tuning". Neurocomputing, 1998. 18(1-3): p. 107-126.
- [7] Zeng, X.C. and T.R. Martinez, "improving the performance of the Hopfield network by using relaxation rate". Artificial Neural Nets and Genetic Algorithms, 1999: p.67-72.
- [8] Gimenez-Martinez, V., "A modified Hopfield auto-associative memory with improved capacity". IEEE Transactions on Neural Networks, 2000. 11(4): p. 867-878.

- [9] Garcia, C. and J.A. Moreno, "The Hopfield associative memory network: Improving performance with the kernel "trick". Advances in Artificial Intelligence", - Iberamia 2004, 2004. 3315: p. 871-880.
- [10] Bauk, S.I., S.M. Perovich, and IEEE. "Computing the modified Hopfield network parameters by STFT". In International Conference on Computer as a Tool (EUROCON 2005). 2005. Belgrade, SERBIA MONTENEG: IEEE. Multi-Connect Architecture (MCA) Associative Memory: A Modified Hopfield Neural Network 307
- [11] Bauk, S.I., S.M. Perovich, and A. Lompar. "The linear approximation method to the modified Hopfield neural network parameters analysis". In 7th International Conference on Adaptive and Natural Computing Algorithms (ICANNGA). 2005. Coimbra, PORTUGAL: pringer-Verlag Wien.
- [12] Wu, Y.D., and et al. "An improved algorithm for image restoration based on modified Hopfield neural network". in 4th International Conference on Machine Learning and Cybernetics. 2005. Canton, PEOPLES R CHINA: IEEE.
- [13] Dehghan, M., M. Nourian, and M.B. Menhaj, "Numerical Solution of Helmholtz Equation by the Modified Hopfield Finite Difference Techniques". Numerical Methods for Partial Differential Equations, 2009. 25(3): p. 637-656.
- [14] A.H. Muhamad Amin, et al., "Analysis of Pattern Recognition Algorithms using Associative Memory Approach: A Comparative Study between the Hopfield Network and Distributed Hierarchical Graph Neuron (DHGN)". IEEE 8th International Conference on Computer and Information Technology Workshops, 2008.
- [15] Emad I Abdul Kareem, et al., "Multi Connect Architecture (MCA) Associative Memory: A Modified Hopfield Neural Network". Intelligent Automation and Soft Computing, Vol. 18, No. 3, pp. 291-308, 2012.
- [16] Kishan Mehrotra, C.K.M.a.S.R., "Elements of Artificial Neural Networks". Bradford Books, Complex Adaptive Systems, New York, USA, 1996.
- [17] Zurada, J.M., "Introduction to Artificial Neural System". PWS Publishing Co., Boston, MA, USA, 1999.
- [18] Emad I. Abdul Kareem, Aman Jantan, "MCA: A Developed Associative Memory Using Multi-Connect Architecture", International Journal of Intelligent Information Processing, Volume 2, Number 1, March 2011.

Appendix A

Random Noise Rate	Test 1			Test 2			Test 3		
	A	B	C	A	B	C	A	B	C
10%	A	B	C	A	B	C	A	B	C
20%	A	B	C	A	B	C	A	B	C
30%	A	B	C	A	B	C	A	B	C
40%	EE	EE	C	A	B	C	EE	EE	C
50%	EE	EE	EE	A	B	C	A	B	C
60%	A	B	C	A	B	C	A	EE	EE
70%	EE	EE	C	A	EE	C	A	B	EE
80%	EE	B	C	EE	EE	EE	EE	A	EE
90%	A	EE	C	A	EE	EE	A	EE	EE

Fig. (A1): Traditional Hopfield net learned three alphabetical English letters (A, B and C) with it's converge patterns.

Random Noise Rate	Test 1			Test 2			Test3		
	A	B	C	A	B	C	A	B	C
10%	A	B	C	A	B	C	A	B	C
20%	A	B	C	A	B	C	A	B	C
30%	A	B	C	A	B	C	A	B	C
40%	A	B	C	A	B	C	A	B	C
50%	A	C	C	A	B	C	A	B	C
60%	B	B	C	A	B	A	A	A	B
70%	B	A	C	B	A	C	A	B	C
80%	A	B	C	B	B	C	A	B	A
90%	B	C	C	A	B	B	B	B	A

Fig. (A2): MCA net leaned just three alphabetical English letters (A, B and C) with its convergence patterns.

Random Noise Rate	Test1			Test2			Test3		
	A	B	C	A	B	C	A	B	C
10%	A	B	C	A	B	C	A	B	C
20%	A	B	C	A	B	C	A	B	C
30%	A	B	C	A	B	C	A	B	C
40%	A	B	C	A	B	C	A	B	C
50%	A	B	C	A	B	C	A	B	C
60%	A	B	C	A	B	C	A	B	C
70%	A	B	C	A	B	C	A	B	C
80%	A	B	C	A	B	C	A	B	C
90%	A	C	B	A	C	C	A	A	B

Fig. (A3). MMCA net leaned just three alphabetical English letters (A, B and C) with its convergence patterns.

Must Frequency Frequent Pattern-Tree Algorithm for Mining Association Rules

Enas Mohammed Hussien Media Noaman Solagh

Computer Science Dept. Education College, Mustansiriyah Uni., Baghdad, Iraq

enas.seead38@yahoo.com

media_nouman@yahoo.com

Abstract:

Data mining is very become important at the present time, especially with the increase in the area of information is huge, so it was necessary to use data mining to contain them and using them, one of the data mining techniques are association rules and using the Pattern Growth method kind enhancer for the apriori. The pattern growth method depends on fp-tree structure , this paper presents modify of fp-tree algorithm called Must Frequency FP-Tree by using must frequent item in fp-tree so final nodes for conditional tree less than the original fp-tree. When applied the MFFP-tree using banking data set shows that the MFFP-TREE method is efficient and scalable for mining both long and short frequent patterns, and is about an order of magnitude faster than the FP-tree and using less than memory space.

Keywords: frequent pattern mining, association mining, algorithm, performance improvements, data structure

1. Introduction

Association rule mining represents one of the most important and well techniques in the data mining field, was first introduced by A grawal et al. Its main objective is to extract interesting correlations or associations among sets of items in transaction databases. Due to their importance in information systems, association rules are widely used in various areas such as market, finance, telecommunication networks. A priori algorithm [1] is one of the most significant approaches to find association rules from datasets. This algorithm generates association rules from so-called frequent itemsets that are itemsets that satisfy a statistical measure, called minimum support (minsup). This minsupport is the core of any association rule algorithm, and it is used to distinguish between frequent and unfrequentitemsets, essentially to limit the number of generated association rules. While the minsup allows to reach this objective, using only one minsup value for all items of a given database is problematic. In fact, with only one minsup value, an association rule mining algorithm assumes that all items (or attributes) of a dataset have the same frequency[2]. One of the currently fastest and most popular algorithms for frequent item set mining is the FP-growth algorithm [8]. It is based on a prefix tree representation of the given database of transactions (called an FP-tree), which can save considerable amounts of memory for storing the transactions. The basic idea of the FP-growth algorithm can be described as a recursive elimination scheme: in a preprocessing step delete all items from the transactions that are not frequent individually, i.e., do not appear in a user-specified minimum number of transactions. Then select all transactions that contain the least frequent item (least frequent among those that are frequent) and delete this item from them. Recourse to process the obtained reduced (also known as projected database, remembering that the item sets found in the recursion share the deleted item as a prefix. On return, remove the processed item also from the database of all transactions and start over, i.e., process the second frequent item etc. In these processing steps the prefix tree, which is enhanced by links between the branches, is exploited to quickly find the transactions containing a given item and also to remove this item from the transactions after it has been processed.[3]. Similar to several other algorithms for frequent item set mining, like, for example, Apriori or Eclat, FP-growth preprocesses the transaction database as follows: in an initial scan the frequencies of the items (support of single element item sets) are determined. All infrequent items—that is, all items that appear in fewer transactions than a user-specified minimum number—are discarded from the transactions, since, obviously, they can never be part of a frequent item set. In addition, the items in each transaction are sorted, so that they are in descending order w.r.t. their frequency in the database. Although the algorithm does not depend on this specific order, experiments showed that it leads to much shorter

execution times than a random order. An ascending order leads to a particularly slow operation in my experiments, performing even worse than a random order [3] [6].

2. Related works

- **In 2014, MS-FP-Growth**, In this study suggested a new way to find association rules and through the application of a set of tests based on monitoring the difference between increasing and decreasing the minsup value, The main objective of these algorithms is to produce interesting knowledge from low level to high level. In this context, they propose to introduce the multi-support approach in the FP-Growth algorithm, This variant is applied in three cases, In the first case, we increase the minsup value from one level to another, In the second case, we decrease the minsup value between levels, In the last and third case, we vary the minsup value randomly increasing and decreasing The aim of this section is to study the impact of multi-supports on number of Association Rules (AR) generated [7].

- **In 2010, SLP-Growth Algorithm**, this paper proposes a scalable trie-based algorithm named SLP-Growth. This algorithm generates the significant patterns using interval support and determines its correlation. Experiments with the real datasets show that the SLP-algorithm can discover highly positive correlated and significant of least association. Indeed, it also outperforms the fast FP-Growth algorithm up to two times, thus verifying its efficiency , By definition, least item is an itemset whose rarely found in the database but still can produce interesting and potentially valuable ARs. These rules are very important in discovering rarely occurring but significantly important, such as air pollution detection, critical fault detections, network intrusions, etc, highly correlated least ARs are referred to the itemsets that its frequency does not satisfy a minimum support but are very highly correlated. ARs are classified as highly correlated if it is positive correlation and in the same time fulfils a minimum degree of predefined correlation, a new algorithm named Significant Least Pattern Growth (SLP-Growth) to extract these ARs is proposed. The proposed algorithm imposes interval support to capture all least itemsets family first before continuing to construct a significant least pattern tree (SLP-Tree). The correlation technique for finding relationship between itemset is also embedded to this algorithm [9].

- **In 2006, fast algorithm**, develop a method that reduce candidate generation and test and utilize some novel data structures to reduce the cost in frequent pattern mining because most time consuming operation in this discovery process is the computation of the frequency of the occurrences of interesting subset of items (called candidates) in the database of transactions, A fast algorithm has been proposed for solving this problem. Our algorithm use the "TreeMap" which is a structure in Java language. Also we present "Arraylist" technique that greatly reduces the need to traverse the database [10].

- **In 2002, Top Down FP-Growth**, In this paper, we propose an efficient algorithm, called TD-FP-Growth (the shorthand for Top-Down FP-Growth), to mine frequent patterns. TD-FP-Growth searches the FP-tree in the top-down order, as opposed to the bottom-up order of previously proposed FP-Growth. The advantage of the top-down search is not generating conditional pattern bases and sub-FP-trees, thus, saving substantial amount of time and space. We extend TD-FP-Growth to mine association rules by applying two new pruning strategies: one is to push multiple minimum supports and the other is to push the minimum confidence. Experiments show that these algorithms and strategies are highly effective in reducing the search space.

3. Frame work

Apriori-like algorithms expensively handle a great number of candidates. Additionally, it repeated scanning of the database is tedious. Therefore, Han et al. developed an efficient FP-tree based method, FP-growth, for mining frequent itemsets without generating candidates; this approach scans the database only twice [7, 8].

3.1 FP-growth

First discovers all frequent 1-itemsets and then establishes a compact tree structure, called an FP-tree (frequent-pattern tree). The FP-tree is a prefix-tree structure that stores information about each frequent 1-itemset, in which the items are arranged in order of decreasing support value. Then, the mining process is transformed to mine the fp-tree.

Consider the example in Table 1 and $\text{minSup} = 30\%$, The mining process begins from the bottom of the header table, and moves toward the top the process of generating the conditional FP-tree terminates will No more frequent itemsets can be generated in this conditional fp-tree. In table 2 consider mining process.

Table (2) Mining rules

Items	conditional pattern base	conditional fp-tree
A1	{(:8)}	{() A1}
C1	{(A1,:7),(,:7),(,:7)}	{() C1}
I1	{(A1,C1,:7),(C1,G,:7),(,:7)}	{() I1}
L1	{(A1,C1,I1,:6),(I1,K2,:6),(,:6),(J2,:6)}	{() L1}
F1	{(A1,C1,I1,L1,:5),(C1,G,I1,K2,J2,:5),(I1,K2,L1,:5),(L1,:5),(J2,L1,:5)}	{() F1}
M1	{(A1,C1,I1,L1,F1,:5),(C1,G,K2,J2,:5),(C1,G,I1,K2,J2,F1,:5),(I1,K2,L1,F1,:5)}	{() M1}
N1	{(A1,C1,I1,L1,F1,M1,:5),(C1,G,K2,J2,M1,:5),(J2,L1,F1,:5),(,:5)}	{() N1}
O1	{(A1,C1,I1,L1,F1,M1,N1,:5),(C1,G,K2,J2,M1,N1,:5),(J2,L1,F1,N1,:5),(N1,:5)}	{(N1:20,) O1}
P1	{(A1,C1,I1,L1,F1,M1,N1,O1,:5),(C1,G,K2,J2,M1,N1,O1,:5),(J2,L1,F1,N1,O1,:5),(N1,O1,:5)}	{(N1:20,O1:20,) P1}
J1	{(A1,C1,I1,L1,F1,M1,N1,O1,P1,:3),(I1,K2,L1,F1,M1,:3),(L1,F1,:3)}	{(L1:9,F1:9,) J1}
G	{(C1,:7),(C1,:7)}	{(C1:14,) G}
K2	{(C1,G,:7),(C1,G,I1,:7),(I1,:7)}	{() K2}
J2	{(C1,G,K2,:6),(C1,G,I1,K2,:6),(,:6)}	{() J2}
F2	{(C1,G,K2,J2,M1,N1,O1,P1,:4),(,:4),(N1,O1,P1,:4)}	{() F2}
L2	{(C1,G,K2,J2,M1,N1,O1,P1,F2,:3),(C1,G,I1,K2,J2,F1,M1,:3),(F2,:3)}	{() L2}
N2	{(C1,G,I1,K2,J2,F1,M1,L2,:3),(I1,K2,L1,F1,M1,J1,:3),(F2,L2,:3)}	{() N2}
P2	{(C1,G,I1,K2,J2,F1,M1,L2,N2,:3),(I1,K2,L1,F1,M1,J1,N2,:3),(L1,F1,J1,M3,:3)}	{(F1:9,) P2}
M3	{(L1,F1,J1,:3),(N1,O1,P1,F2,:3)}	{() M3}

3.2 MFFP-growth algorithm: The tree structure of the MFFP-growth (MFFP-tree) can be considered as extracting the sub tree MF (MF denotes the most frequent 1-itemset) from the FP-tree. Other sub trees of the root are merged with the MF sub tree. Additionally, the MF node becomes the root of the MFFP-tree. Therefore, the nodes in the MFFP-tree are fewer than those of the fp-tree. Counter of the MFFP-tree record the same information as the FP-tree; pattern-growth algorithm can be applied to generate all frequent itemsets. An NFP-tree can be constructed as follows:

Algorithm 1 (NFP-tree construction)

Input: (1) DB: a transaction database, and (2) min Sup: minimum support threshold

Output: NFP-tree

Procedure:

- 1.Scan DB once. Store all the frequent 1-itemsets F and their individual support values.
2. Sort F in order of decreasing support value to generate a list of frequent 1-itemsets L.
- 3.Select the most frequent 1-itemset (MF) to generate the root node of the NFP-tree, labeled MF.
- 4.For each transaction $T \subset DB$, perform the following:
- 5.Select the frequent 1-itemsets in T and sort them in order of L. Let the frequent itemsets list in T be $\{p_1, p_2, \dots, p_n\}$
- 6.If $p_1 == MF$, call function Insert_node(p_2 , root); else call function Insert_node(p_1 , root).

The pseudo code of the function Insert_node(p, N) is as follows.

Function Insert_node(p, N)

```

1. if p1 == MF {
2.   for each child Chof N {
3.     if exist N' ∈ Chs such that N'.label == p {
4.       N'.counter[0]++;
5.       Insert_node(pi+1, N'); }
6.   else {
7.     create a new node N';
8.     N'.counter[0] = 1;
9.     Insert_node(pi+1, N'); } }
10.  else {
11.   for each child Chof N {
12.     if exist N' ∈ Chs such that N'.label == p {
13.       N'.counter[0]++;
14.       Insert_node(pi+1, N'); }
15.   else {
16.     create a new node N';
17.     N'.counter[0] = 1;
18.     Insert_node(pi+1, N'); } }

```

Example 2: Consider the same transaction database as in Table 1 with min Sup = 30%. First, MFFP-growth scans the database to discover all frequent 1-itemsets, and then sorts these 1-itemsets. The order is the most frequent 1-itemset MF. The process of the first scan of the database is identical to that associated with FP-growth. Therefore, the sorted frequent 1-itemsets in each transaction are listed in the last column of Table 1. Then, MFFP-growth stores the entire frequent 1-itemsets of each transaction in an MFFP-tree structure. The root of the NFP-tree is created first and stores the support value of MF. Next, MFFP-growth scans the database second time. The first transaction is used to establish the first branches of MFFP-tree. For mining process generating conditional MFFP-tree, the process of generating the conditional MFFP-tree terminates when no more association items to generate. see table 3 and figure 2.

4. Experimental Results

The performance of MFFP-growth is compared with that of FP-growth is more efficient approach for mining frequent itemsets, based on most frequent. Memory space for MFF-tree in GB less than memory space for FP-tree. Test this algorithm on 30%, 50% minsup, using for coded visual .net, and the dataset is real dataset from UCI machine learning. I use bank marketing dataset after preprocessing dataset. Full dataset 1500 records in fig. 2. show computational performance of mining the bank marketing dataset between FP-growth and MFFP-growth.

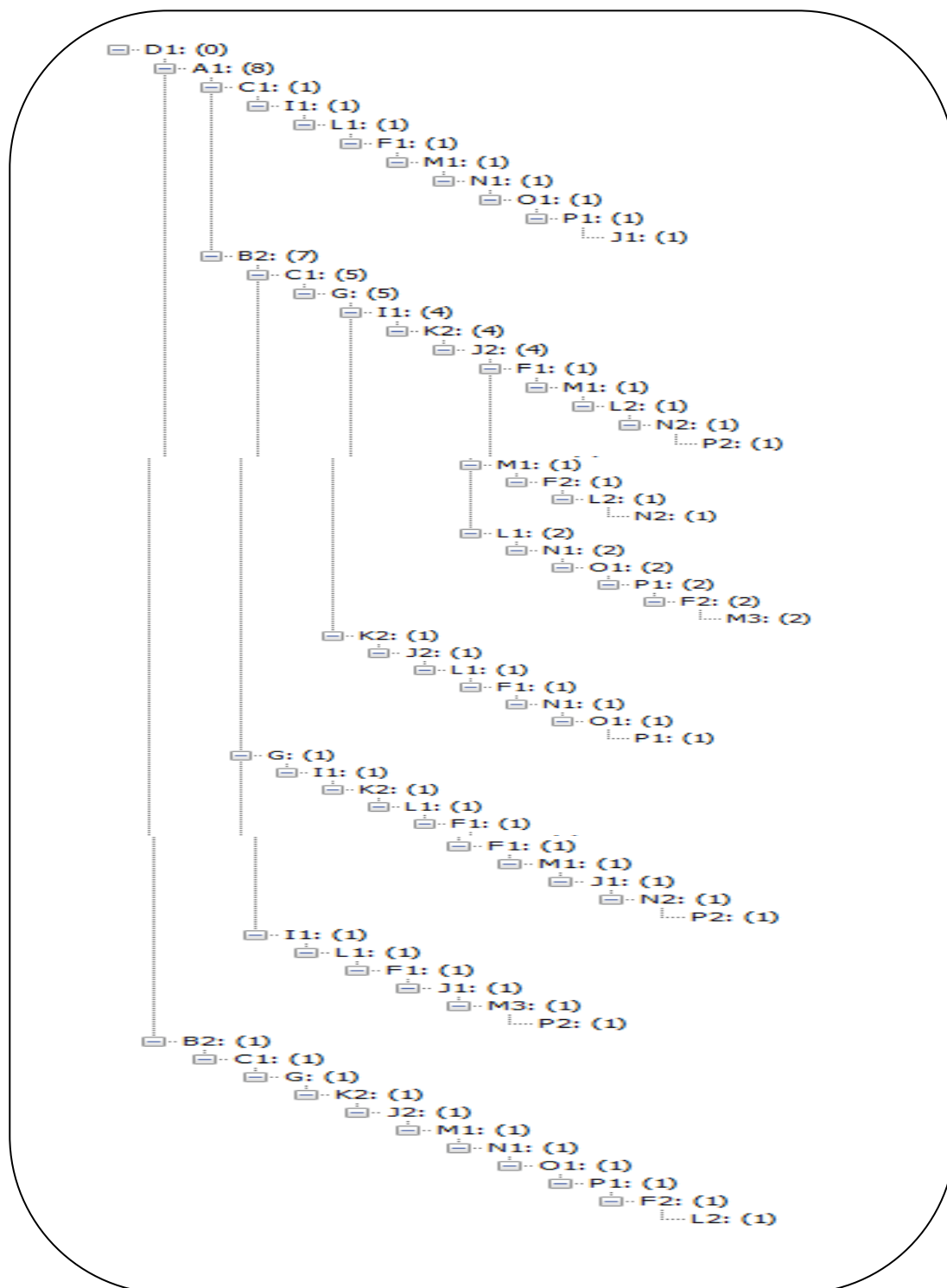


Fig. (2): Mining MFFP-tree

Table (3) Mining rules

Items	conditional pattern base	conditional fp-tree
C1	{(:7),(7),(7)}	{() C1
I1	{(C1,:7),(C1,G,:7),(7)}	{() I1
L1	{(C1,I1,:6),(I1,K2,:6),(6),(J2,:6)}	{() L1
F1	{(C1,I1,L1,:5),(C1,G,I1,K2,J2,:5),(I1,K2,L1,:5),(L1,:5),(J2,L1,:5)}	{() F1
M1	{(C1,I1,L1,F1,:5),(C1,G,K2,J2,:5),(C1,G,I1,K2,J2,F1,:5),(I1,K2,L1,F1,:5)}	{() M1
N1	{(C1,I1,L1,F1,M1,:5),(C1,G,K2,J2,M1,:5),(J2,L1,F1,:5),(5)}	{() N1
O1	{(C1,I1,L1,F1,M1,N1,:5),(C1,G,K2,J2,M1,N1,:5),(J2,L1,F1,N1,:5),(N1,:5)}	{(N1:20,) O1
P1	{(C1,I1,L1,F1,M1,N1,O1,:5),(C1,G,K2,J2,M1,N1,O1,:5),(J2,L1,F1,N1,O1,:5),(N1,O1,:5)}	{(N1:20,O1:20,) P1
J1	{(C1,I1,L1,F1,M1,N1,O1,P1,:3),(I1,K2,L1,F1,M1,:3),(L1,F1,:3)}	{(L1:9,F1:9,) J1
G	{(C1,:7),(C1,:7)}	{(C1:14,) G
K2	{(C1,G,:7),(C1,G,I1,:7),(I1,:7)}	{() K2
J2	{(C1,G,K2,:6),(C1,G,I1,K2,:6),(6)}	{() J2
2	{(C1,G,K2,J2,M1,N1,O1,P1,:4),(4),(N1,O1,P1,:4)}	{() F2
L2	{(C1,G,K2,J2,M1,N1,O1,P1,F2,:3),(C1,G,I1,K2,J2,F1,M1,:3),(F2,:3)}	{() L2
N2	{(C1,G,I1,K2,J2,F1,M1,L2,:3),(I1,K2,L1,F1,M1,J1,:3),(F2,L2,:3)}	{() N2
P2	{(C1,G,I1,K2,J2,F1,M1,L2,N2,:3),(I1,K2,L1,F1,M1,J1,N2,:3),(L1,F1,J1,M3,:3)}	{(F1:9,) P2
M3	{(L1,F1,J1,:3),(N1,O1,P1,F2,:3)}	{() M3

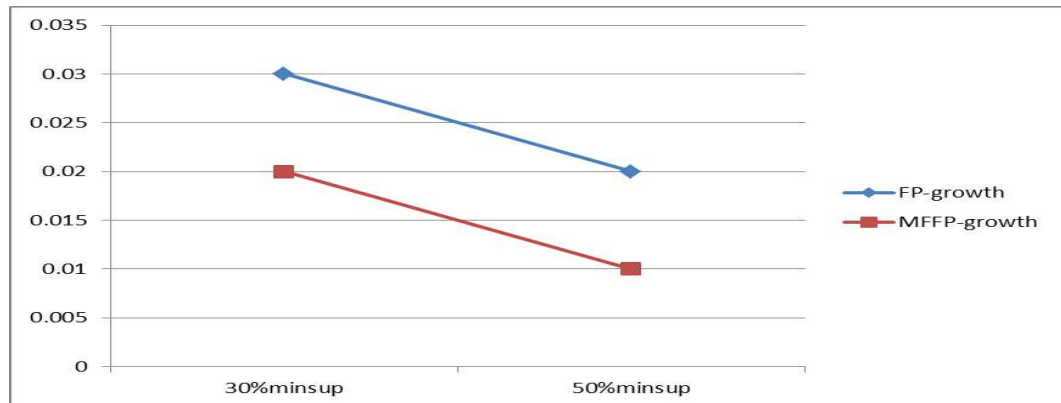


Fig.(3) dataset in table1

In fig.4.show the computational performance based on several interval supports. For same dataset, use full dataset.

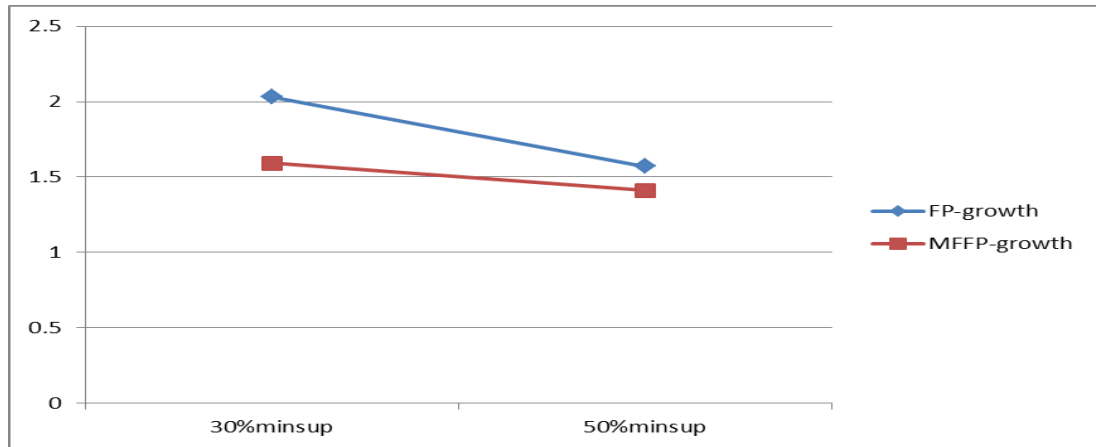


Fig.(3): full dataset

4. Conclusions

Mining frequent itemsets in a transaction database is critical for mining association rules. This research suggested a new method to performance FP-tree efficiency in two dimension effect:

- reducing the memory space of FP-tree
- reducing the time of execution tree
- Applies a smaller tree to discover frequent itemsets faster.

5. Recommendations

We recommend replacing the tree structure by graph structure and using another algorithm to find the pattern set like as forest FP-tree.

References

- [1] Rakesh Kumar Soni¹, Prof. Neetesh Gupta², Prof. Amit Sinhal³, "An FP-Growth Approach to Mining Association Rules ", IJCSMC, Vol. 2, Issue. 2, February 2013, pg.1 – 5
- [2] Wiem Taktak¹ and Yahya Slimani², "MS-FP-Growth: A multi-support Version of FP-Growth Algorithm", International Journal of Hybrid Information Technology, 2014
- [3] Christian Borgelt, "An Implementation of the FPgrowth algorithm"
- [4] S. Lin and X. Huang, "A Parallel Algorithm for Mining Association Rules Based on FP-tree", CSEE 2011, Part IV, CCIS 217
- [5] Zailani Abdullah¹, Tutut Herawan², and Mustafa Mat Deris³, "Mining Significant Least Association Rules Using Fast SLP-Growth Algorithm", AST/UCMA/ISA/ACN 2010
- [6] Jian Hu^{1,2} and Xiang Yang-Li^{1,2}, "A Fast Parallel Association Rules Mining Algorithm Based on FP-Forest", ISSN 2008, Part II, LNCS 5264
- [7] M. H. Margahny and A. Shakour, "Fast Algorithm For Mining association Rules", Journal of Engineering Sciences, Assiut University, Vol. 34, No. 1, pp. 79-87, January 2006
- [8] Yu-Chiang Li and Chin-Chen Chang, "A New FP-Tree Algorithm for Mining Frequent Itemsets", AWCC 2004, LNCS 3309, pp. 266, 2004–
- [9] Ke Wang, Liu Tang, Jiawei Han, and Junqiang Liu, "Top Down FP-Growth for Association Rule Mining", PAKDD 2002, LNAI 2336.

Stream Data Classification Using Various Mining Algorithms

Enas Mohammed Hussein Hind Raad Ibrahim

Computer Science Dept. Education College, Mustansiriyah Univ., Baghdad, Iraq

enas.seead38@yahoo.com hindraad81@gmail.com

Abstract:

Advances in hardware technology have driven to the increasing popularity of data stream. Streaming data are potentially endless sequence of incoming data at high speed that evolve over time, so that does not permit to permanently conserve them in memory. Consequently traditional data mining algorithms incompetent of treating data stream and yields for the demand of stream data algorithms that appropriate to these characteristics, stream data mining algorithms are classified essentially in classification, clustering, and pattern mining. This paper is only converging on classification techniques. The target of this paper is to assess different classification techniques in three different datasets. Classifiers like Hoeffding tree algorithm and naïve Bayes (NB) are applied to these datasets in order to classify it, some Performance evaluation metrics like accuracy, sensitivity are compared and analysed.

Keywords: stream data classification, naïve Bayes, hoeffding tree algorithm incremental learning.

1- Introduction

Data mining is technique of analyzing data from different sources and summarizing it into fruitful information. [1]. There is number of algorithm for mining a data that do not fit in main memory. But this algorithm only tested on few million examples. But currently every day record millions of transactions, millions of calls connect by telecommunications companies, large banks process millions of ATM and credit card operations, and popular Web sites log millions of hits. So create a massive amount of data. In many cases, these large volumes of data can be mined for interesting and relevant information in a wide variety of applications. The process of taking knowledge from this continuous and rapid data is called streaming data mining. Streaming data require interpret in one pass because it's impervious to store [2]. When the volume of the underlying data is very large, it leads to a number of computational and mining challenges: (1) with increasing volume of the data, it is no longer possible to process the data efficiently by using multiple passes. Rather one can process a data item at most once. Therefore, stream mining algorithms typically need to be designed so that the algorithms work with one pass of the data. (2) In most cases, there is an inherent temporal component to the stream mining process. This is because the data may evolve over time. This behaviour of data streams is referred to as temporal locality. Therefore, a straight forward adaptation of one-pass mining algorithms may not be an efficient solution to the task. Stream mining algorithms need to be carefully designed with a clear focus on the evolution of the underlying data [3].

2- Issue In Stream Mining

The first issue is limited computation resources: in many applications, the computation power and memory at hand does not measure up to the massive amount of data in the input stream. For example, in a single day, Google serviced more than 150 million searches; Walmart executed 20 million sales transactions; and Telstra generated 15 million call records. However, traditional data mining algorithms make the assumption that the resources available will always match the amount of data they process. This assumption does not hold in data stream mining. Stream mining algorithms shall learn fast and consume little memory resources. And the another characteristic of data streams is that data is no longer a snapshot, but rather a continuous stream. This means that the concept underlying the data may change over time. For effective decision making, stream mining must be adaptive to concept change. For example, when customer purchasing patterns change, marketing strategies based on out-dated transaction data must be modified in order to reflect current customer needs [4]. So continuous stream of information has challenged our storage, computation and communication capabilities in computing systems. And for effective processing of stream data,

new data structure, techniques, and algorithms are needed. Because we do not have finite amount of space to store stream data, we often trade-off between accuracy and storage [5].

3- Stream Data Classification Algorithms

In data stream scenarios, the classification ability of a stream classification model generally decreases with time because of the concept evolving reality. For example, in data streams, a classification model c_N built at time stamp N may classify its synchronous data chunk DN accurately, but its accuracy on incoming data chunk $DN+1$ may deteriorate significantly. This is because that data distributions in $DN+1$ may be significantly different from the training samples collected at time stamp N [4]. Accordingly, There are number of algorithm for classification. Following are listed some algorithm and approaches for classification of data stream based on the data mining tasks.

- Hoeffding tree algorithm that is based on decision tree.
- GEMM and FOCUS algorithm and that mining task is decision tree and frequent item set.
- OLIN algorithm uses info-fuzzy techniques for building a tree-like classification model.
- VFDT (Very Fast Decision Tree) and CVFDT (Concept-Adapting Very Fast Decision Tree) algorithm works on decision tree task.
- A Classifier ensemble Approach [7].

3-1 Related Works

Classification is the process of predicting the class label of unknown data instances based on model constructed from training examples. Classification is a process of analysis of data. Classification is a benefit to the streaming data. It is very necessary to classify the streaming data. Classification has more applications that are artifice detection, retailing, analytical modeling, manufacturing and medical analysis [7].

Various classification algorithms for streaming data have been devised from time to time in the last decade. Each algorithm has its own capabilities and key focus to avert stream data challenges [4].

- **Domingos and Hulten** proposed the **Very Fast Decision Tree (VFDT)** an anytime system that builds decision trees using constant memory and constant time per example. VFDT is an incremental algorithm; it can incorporate tens of thousands of examples as they arrive. It uses Hoeffding bounds to guarantee that its output is asymptotically nearly identical to that of a conventional learner. Also require a single scan of the stream data [8].

- **Hulten, Spencer and Domingo's** offered **Concept adapting Very Fast Decision Tree(CVFDT)** Incremental algorithms, it is an amended version of VFDT, title Concept Adaptive Very Fast Decision Tree learner (CVFDT). CVFDT is eligible to conform to concept-drift in the data flow, mounting reciprocal sub-trees at each node of the decision tree, substitute the existing sub-tree with the reciprocal whenever the ultimate turn into more delicate. This is completed by safeguarding sufficient statistics on a time-window animated during the data influx [9]. CVFDT persistent observes the fineness of fresh data and modulate those that are no longer valid. Whenever novel data reach, CVFDT incrementing counts for fresh data and decrements counts for ancient data in the window. The algorithm then waits for more instances and if the new instances confirm that the new (sub) tree learned is of higher quality than the original, the original is replaced [10].

- **Frederic Stahl, Mohamed MedhatGaber and Manuel Martin Salvador** presented a recent data stream classifier development is e-Rules. A modernistic rule based adaptive classifier for data streams, based on an incubating collection of Rules. E-Rules deduce a set of rules that is permanently fateful and convenient to changes in the data stream by appending new and eliminating musty rules [11].

- **W. Nick Street and Yong Seog Kim** gave a method takes the advantages of plentiful data building separate classifiers on sequential chunks of data (block) independently. These classifiers are combined into a fixed size of ensemble using a heuristic replacement strategy (based on their expected classification accuracy on the test data). Building a committee of classifiers that combine the results of many classifiers. The result is an algorithm for large scale or streaming data that classified as well as single tree build on all data requires more memory space [12].

In this paper we will introduce some classification algorithm of streaming data mining such as Hoeffding Tree algorithm and Naïve Bayes algorithm. Hoeffding Tree algorithm is Decision Tree based algorithm. The Naive Bayes algorithm is conditional probability based. This paper has focused on a critical issue arising in decision tree construction on streaming data i.e., time efficiency, memory space and accuracy measurement. Which includes the time processing, it means the total time required for constructing decision tree, memory space and the classification accuracy.

3.1.1 Hoeffding Tree

Hoeffding algorithm is a decision tree learning algorithm and an effective way of classification of data points. In Hoeffding tree algorithm, classification of different problems must be defined. Classification problems area collection of training examples of the form (p, q) , where p is a vector of s attributed and q is a discrete class label and aim is to produce a model of the form $q=f(a)$. Such that the function $f(a)$ predicts the classes' j for future examples I with higher accuracy [13]. It consist of the test node, root node and the leaf nodes, where each leaf node denotes prediction of class. In our case major requirement is the classification of streaming data in a single pass. Data streams are to be read in less amount of time for classification. Hoeffding algorithm combines the data into a tree while the model is being built incrementally, even at that time we can use to classify data.

Hoeffding Tree Algorithm:

1. Hoeffding is a Tree with a root node
2. for all training data do
3. Sort example into leaf l using Hoeffding Tree
4. Update abundant statistics in l
5. Increment ml
6. If $ml \bmod M \min = 0$ and e.g. at l not of same Class then
7. Calculate $g(V_i)$ for each attribute factor
8. Let V_a be attribute with highest attribute g
9. Let V_b be attribute with second-highest attribute g
10. Compute hoeffding bound $\epsilon = \sqrt{(R^2 \ln(1/\delta))/2n}$
11. If $V_a \neq V_0$ and $(g(V_a) - g(V_b)) > \epsilon$ or $\epsilon < t$ then
12. Replace l with an internal node that splits on V_a
13. for all branches do
14. Insert a new leaf with initialized sufficient statistics
15. End for
16. End if
17. End if
18. End for

3.1.2 Naive Bayes

Naive Bayes classifier is a probabilistic classifier. It is also called as simple Bayes and Independence Bayes classifier. It is based on Bayes Theorem [14]. It has ability to solve diagnostic and predictive problems. Bayesian Classification provides a useful perspective for understanding and evaluating many learning algorithms. It calculates explicit probabilities for hypothesis and it is robust to noise in input data

Let us assume,

$P(H|X)$ =Posterior probability

$P(H)$ = Prior probability

$P(X|H)$ =Posterior probability of X conditioned on H .

$P(X)$ = prior probability of X .

Formula for Bayes theorem is:

$$P(H|X) = P(X|H) * P(H) / P(X)$$

4- Proposed system

The total system architecture is designed to support a data mining-based approach As shown in Figure 1, the architecture consists of dataset, classifiers and -decision parameters.

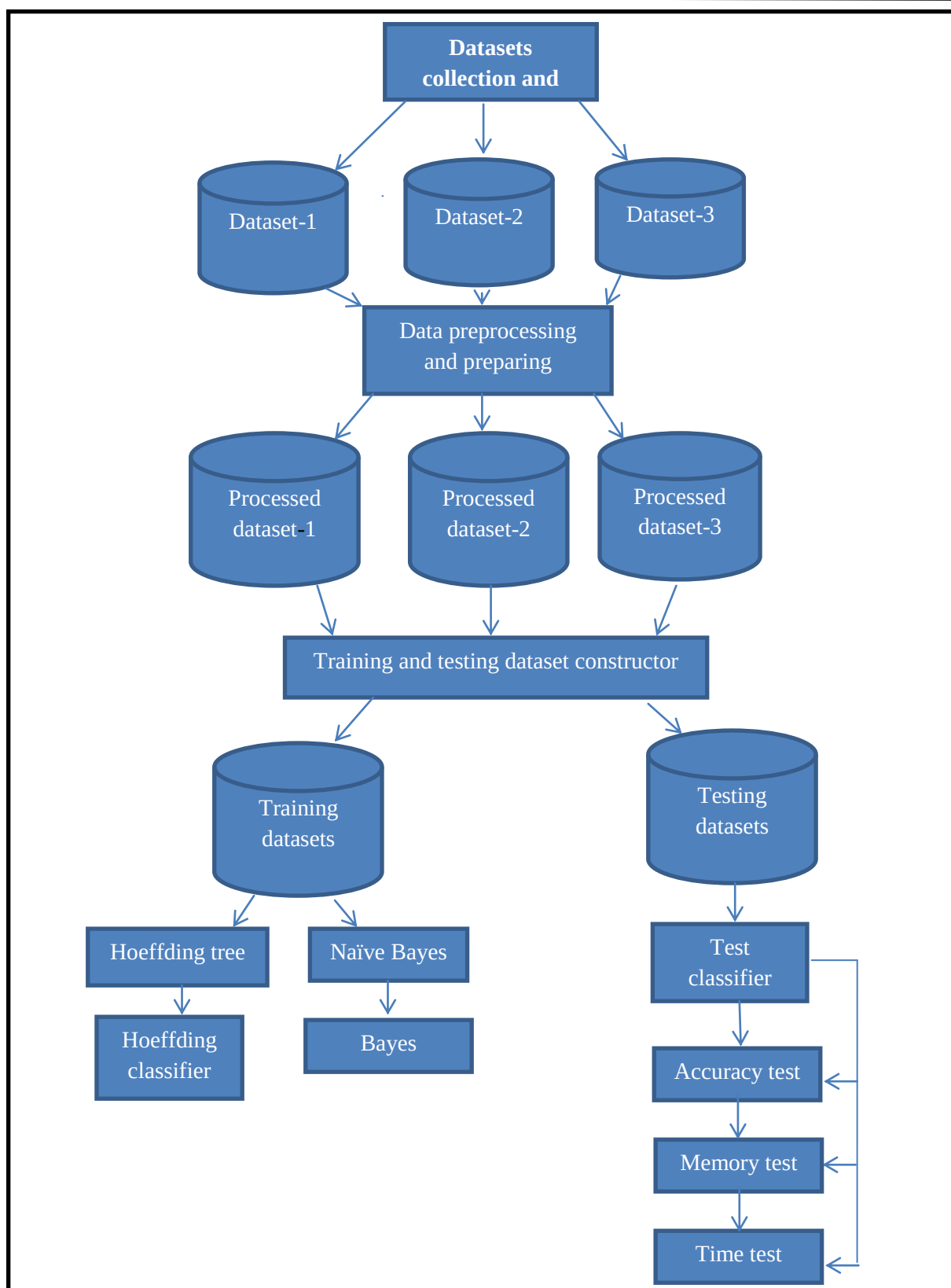


Fig. (1): System Architecture

First the datasets were collected from several sources, and then divided into three different medical datasets, preprocessing is an significant step to make these data prepare and be ready to apply data mining algorithms, then separating it into training and testing dataset, the algorithms are carried out and the two models were induced the first one Hoeffding classifier model and Bayes classifier is the

second one. The two models were tested according to a standard measures which are the classification accuracy, execution time.

Dataset Used

Dataset is a collection of set of information which is comprised of separate elements. Here we gathered the three datasets from different sources, the first dataset which are hypertensive dataset, we obtained it directly from the hospital (collected manually), and heart disease and diabetes dataset are obtained from UCI repositories. The datasets then preprocessed to be ready to apply the two algorithms. We focused on an important attributes like cholesterol, serum triglyceride, serum low density lipoprotein, serum high density lipoprotein, serum very low density lipoprotein. Which are considered a very significant indicator to decide if the person is sick or healthy? There are three various datasets sizes in our dataset between (10000-100000) instances. This dataset used for classifying each instance as sick or healthy.

5- Experimental Results

We developed an application in visual basic language, the application is carried out with several steps. So accordingly, evaluation of results will be shown and accuracy and time has been considered for measuring the overall performance.

1. Accuracy

It means that how much our system is accurate enough to classify between normal and anomalous behavior. It is calculated as,

$$A = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

Where,

- TP – is the True Positives which mean positive cases are correctly identified.
- TN – is the True Negatives which mean positive cases are incorrectly identified.
- FP – is the False Positives which mean negative cases are incorrectly identified as positive.
- FN – is the False Negatives which mean positive cases are incorrectly identified as negative.

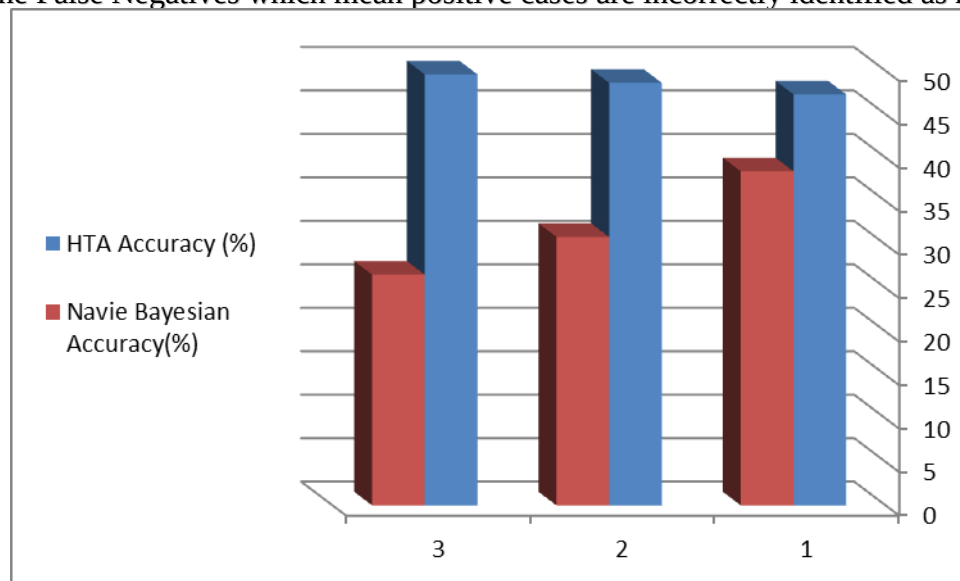


Fig. (2): MHTA vs. Naïve Bayesian for Accuracy in dataset-1

Figure 2 shows the result of classifiers on hypertensive dataset. From the graph it clear that Hoeffding tree algorithm gives 51% and naïve Bayes classifier gives 37% And taking more time than Hoeffding tree algorithm.

2. Time to Build

It is the time required to build the model. It is calculated in seconds. Experimental results show that Hoeffding tree is taking much less time as compared to Naive Bayes.

6- Conclusion

In this paper, we have used classification techniques to make a comparison between two classification algorithms which are Hoeffding tree algorithm is a streaming decision tree induction, the name is derived from the Hoeffding bound that is used in the tree induction. And naïve Bayesian is conditional probability based classifier. Result analysis on real dataset using these classifiers, we obtained that Hoeffding Tree classifier is the best than naïve Bayesian according to execution time and classification accuracy. Whereas naïve Bayesian classifier is not compatible to use with huge dataset, it is proper to use with large or moderate dataset.

References

- [1] Shabiashabir khan, M. A. Peer, S. M. K. Quadri, "**Comparative Study of Streaming Data Mining techniques**", International conference on computing for sustainable Global Development, 2014.
- [2] Albert Bifet, Geoff Holmes, Richard Kirkby and Bernhard Pfahringer (may 2011) Data Stream Mining A Practical Approach.
- [3] Dariusz Brzezinski (2010), Mining Data Streams With Concept Drift, Poznan University of Technology.
- [4] Aggarwal, C., Han, J., Wang, J., and Yu, P.S., (2004): On Demand Classification of Data Streams. In Proceedings of 2004 International Conference on Knowledge Discovery and Data Mining (KDD '04).
- [5] Agrawal, C.C. (2007). Data Streams: Models and Algorithms. Springer.
- [6] A . Bifet , "**Pitfalls In Benchmarking Data Stream Classification And How To Avoid Them**" machine learning and knowledge discovery in databases, pp.465-479. Springer BerlineHedileberg (2013).
- [7] J. Han, M. Kamber and J. pie, "**data mining concepts and techniques**", 3rd edition, Morgan Kaufmann, (2011).
- [8] Domingo's, P. and Hulten, G., (2000): Mining High-Speed Data Streams. In Proceedings of the Association for Computing MachinerySixth International Conference on Knowledge Discovery and Data Mining.
- [9] Aggarwal, C., Han, J., Wang, J., and Yu, P. S., (2004): On Demand Classification of Data Streams. In Proceedings of 2004 InternationalConference on Knowledge Discovery and Data Mining (KDD '04).Seattle, WA.
- [10] Lior C., Gil A., Abraham K., Ben-Gurion University of the Negev Department of Information Systems Engineering , Dept. of Computer Science and Engineering, University of South- Florida, Tampa, Florida, "**Incremental Classification of Non stationary Data Streams**", 2009.
- [11] Thien Le, Frederic Stahl, JoãoBártolo Gomes, Mohamed MedhatGaber and Giuseppe Di Fatta, "**Computationally Efficient Rule-Based Classification for Continuous Streaming Data**", School of Computing Science and Digital Media, Robert Gordon University, Riverside East, Garthdee Road, Aberdeen AB10 7GJ, UK, Springer International Publishing Switzerland 2014 M. Bramer and M. Petridis (eds.), Research and Development in Intelligent System.
- [12] Long H., Kwong W. Y., and Keong N., "**A survey on data stream clustering and classification**", Data Analytics Department, Institute for Infocomm Research (I2R) Agency for Science Technology and Research (A*STAR), Singapore, Singapore, springer 2014.
- [13] Albert Bifet, Geoff Holmes, Richard Kirkby and Bernhard Pfahringer (may 2011) Data Stream Mining A Practical Approach.
- [14] Ketan Sanjay DesaleME scholar, Roshani Ade Assistant Professor , "**A Case Study: Stream Data Mining Classification**", International Journal of Computer Applications (0975–8887) National Conference on Advances in Computing (NCAC 2015) .
- [15] Bifet, Albert, "**mining big data in real time**", informatica 37, pp. 15-20. (1013).

Skin Cancer Detection Using Artificial Neural Network

Iman Hussein AL-Qinani Mushtaq Talib Ajjah Mustafa H. Ali
Computer Science Dept., Mustansiriyah University, Baghdad, Iraq
iman.alqinani@uomustansiriyah.edu.iq altaib.mushtaq@gmail.com
mustafa.h@uomustansiriyah.edu.iq

Abstract:

In the last years skin cancer is the most common type of cancers and considered as a lethal type. Many of skin cancers are accepting for recuperation at the early stage, so saving the patient's life connected to the early detection of the skin cancer and with the development of technology used to detect this disease the early detection become possible.

This paper proposed one of the new technologies that used to detect the skin cancer is using 2-D Fourier transform in compound with the Neural Network which constructs an image shows cancerous or non- cancerous case by applying MATLAB software.

Keyword: Skin cancer detection, Fourier transform algorithm, Neural Network, training, testing

الكشف عن سرطان الجلد عن طريق الشبكة العصبية الاصطناعية

ايمان حسين رحيم مشتاق طالب عجه مصطفى حسين علي

المستخلص

في السنوات الأخيرة مرض سرطان الجلد هو النوع الأكثر شيوعاً من أنواع السرطان ويعتبر نوع قاتل. العديد من سرطانات الجلد قابلة للاستشفاء في المرحلة المبكرة من المرض، لذلك إنقاذ حياة المريض المتصلة بالكشف المبكر عن سرطان الجلد ومع تطور التكنولوجيا المستخدمة للكشف عن هذا المرض يصبح الاكتشاف المبكر ممكناً.

اقترح في هذه الورقة واحدة من التقنيات الجديدة التي تستخدم للكشف عن سرطان الجلد وهي استخدام تحويل فورييه ثنائية الأبعاد مع الشبكة العصبية الاصطناعية التي تبني صورة تظهر حالة سرطانية أو غير سرطانية من خلال تطبيق برنامج ماتلاب.

الكلمات المفتاحية: الكشف عن سرطان الجلد، خوارزمية تحويل فورييه، الشبكة العصبية، التدريب، الاختبار.

I. Introduction

Body made of many types of cells that divided normally to give new cells will replace the old cells, If there is cancer disease some cells have different shape and function from each other because they split and grow in uncontrolled steps so causing cancer [1].

The skin cancer can be defined as a cancer affecting the skin and may be in two forms malicious or harmless. The Harmless form can be considered as a moles appear on the skin but the malicious form is sores where cause bleeding they appear in the outer layer of the skin. The most deadly form of the skin cancer is the malicious one. It's originated from cancerous growth in pigmented skin suffering and it is name come from the melanocyte which is the cell which arises from. If this form diagnosis in early time it will be treat in the right way [2].

The skin cancer diagnosis or detection it is very difficult and needs laboratory tests and sampling, can be distribute to the all parts of the body by the blood or the lymphatic system. The cancer detection speed can be made in better way by computer based prosopopoeia depend on the disease symptoms, here a problem appeared the similarities between the skin harm make the detection of the malicious cell difficult job. But there are some symptoms especially for the melanoma like: Asymmetry, Border irregularity, Color variation and Diameter, all of these symptoms can be named the ABCD parameters [2]. This paper give a new technique to detect the skin cancer disease depend signal processing technique which called the 2-D Fourier transform.

This paper is divided into several parts as bellow: part I introduce an introduction about the subject (Skin cancer detection using 2-D Fourier transform), part II present the literature survey, part III present the material and methods, part IV shows the result and discussion, conclusion and the future work.

II. Literature Survey

The work shows in this paper is concentrate on develop a new technique used to detect the skin cancer disease; Energetic research has been done on skin cancer detection with different technologies. In this section we check many papers interested in skin cancer detection. The technique used by many different researcher differ from each other in the type of training method, the feature extracted and he classification model used.

Author in [3] suggested a new way to the method of diagnosis, classification and recognition in image which is digital. Start with the classification way which is depending on applied a group of features that contain parameters are fractal like the Lacunarity and Fractal Dimension. This technique based on mix the parameters on an object in terms of its texture.

The main cases with the recognition of the object is contained two harry division method for which C++ code is supplied. To build a new decision making by using the fuzzy logic and membership function showed and a new method for the extraction and make an information from the function of the membership which considered. In their work concentrate on improvement and application of a skin cancer testing and detection system that can be used to divide harmless from the abnormal situations [3].

Author in [4] concentrated on a technique has been used the segmentation technique for the skin cancer images. This method depends on the texture and the color available in the images of the skin cancer. The distribution for the features of the color and the features of the texture has been used for the discrimination of the color texture. The suggested segmentation technique has been tested depending on the experiments which have been used the images of the skin cancer. 15 different images representative the lesion of the skin have been used for the testing. The images include several skin lesions like the malignant melanoma, carcinoma of the basal cell and carcinoma of the squamous cell. The images of the skin cancer used were of different size. It was observable which the lesions had a huge differences in the size such as contrast and color to the neighboring skin. In some images of skin cancer, there are hairs have been surrounded a skin lesion shall be noticed that had have a disturbing power on the divergence of the right boundaries.

Author in [5] presented a new technique "Fuzzy Co- Clustering Method for the images (FCCI)" and they apply this algorithm prosperity to the color division of the medical images. The aim of the proposed work is to provide their method by embedded the features of the texture like the parameter of clustering for detecting the fault in the skin depend on the information from the color. The function objective is using the foraging bacteria method that gives specific values for the image to the parameters embedded in the method.

Author in [6] mixed the concepts of computer engineering with the areas such as oncology and dermatology. Discuss the skin cancer images, as a special skin cancer, this represent the shared points or other style for the disease of skin, by using the recognition of image. In their work based on ABCDE rules, which is usually used by dermatologists for skin cancer detection and diagnosis, to knowledge the parameters can be analyzed by software. After that different methods and ways applied containing the ellipse- fitting method to measure and extract these parameters and determine whether the point is a skin cancer or not.

Author in [7] concentrated on the automatic skin cancer division system. The inputs used in his suggestion system is come from collecting data image, then many various image processing methods used to promote the properties of the image. Here, he work on two division methods one for detection the harmless skin cancer from the malignant one and then debrief an information from these images that traff to the classifier for the testing and training. The properties used for the divisions are the factors used for by the Wavelet decomposition and simple wrapper curve.

Author in [8] work on the image division which is considered as an important method used to solve many difficult problems, like detection skin cancer. Start his as built a technique used to divide the method of MRI (Magnetic Resonance Images), which using the Unsupervised neural network technique (UNNT). This method has two difficulties: 1) The trained network has a long time to find the desired results (desired output), 2) the results from the training technique in the NN are not pure they have a noise. UNN such as Kohonen Network took the image resulted and the process of trained and then discovering to the original images. Here, a decreasing of the training time and then

access to the results in the process so give a good ability of detection and diagnosis the skin cancer disease.

III. Material and Method

This part shows the method have been compound to make the classification of the images in two groups which are the cancerous and the non-cancerous one.

a) 2D Fourier Transform

It is an application considered as a huge and contains wide range of topics like optics, geology, astronomy, communications, signal processing and image processing. Here, Fourier transform can be prolonging to n dimensions easily. The force of the Fourier transform it is attended by a group of tools of the properties of operational which make the calculation of the most complex transforms by using these standard rules in a simple way.

The group of tools of the Fourier transform includes the scaling results, multiplication, convolution and translation, for the transforms done basically for the Dirac- delta function and complicated exponential are so important to the interface of the shift, convolution results and the multiplication. The above basic toolset can be used for the 1-D and 2-D Fourier transforms [9].

2-D Fourier transform considered as a simple and fast method to filter an image in the local domain if the size is small (8 x 8 pixels). Involution of large one can be made faster by transfer image in the spatial domain to the frequency one, then implement a filter by doing point by point multiplication. The images which filtered in the frequency domain then will be transfer to the spatial domain by apply an inverse Fourier transform. The high pass filter use to reduce the weight of the low frequency ingredient to implement the detection of the edge. Then the pixels which are black equal to zero and white equal 1 but the gray scale is between zero and one values. The four nooks in the frequency domain of the image considered as the locations of the low frequency ingredients. Near the center of the image the high frequency ingredients are located.

b) Neural Network

Neural Network considered as a mathematical model include an interconnected set of artificial neurons, and the information processes using the approach of the connectionist of the computation.

c) The proposed method:

The methodology of diagnosing through using image processing method and the artificial intelligence, the processing technique used is the 2-D Fourier transforms and the artificial intelligence is the Neural Network. The skin cancer dermoscopic image was taken and it was subjected to different preprocessing for remove the noise and improves the image. After that the image was segmented via thresholding. This gave specific unique features for the regions of the skin cancer like features that were extracted by using the technique of the feature extraction which is the 2-D Fourier transform. These features have been considered as an input of the neural network. The Back Propagation Neural network has been used for the classification method, which classifying the data group in non cancerous or cancerous. The proposed flowchart is shown in the following figure (1).

1) Data or Image acquisition

Here the data based images have been used which contains the dermoscopic images and the digital photo; these images were collected by the researcher in collaboration with a group of hospitals and these images are classified into two groups the first group contains cancerous images and the second group contains non cancerous images. The first step for this is to resize the image to obtain a fixed height and width.

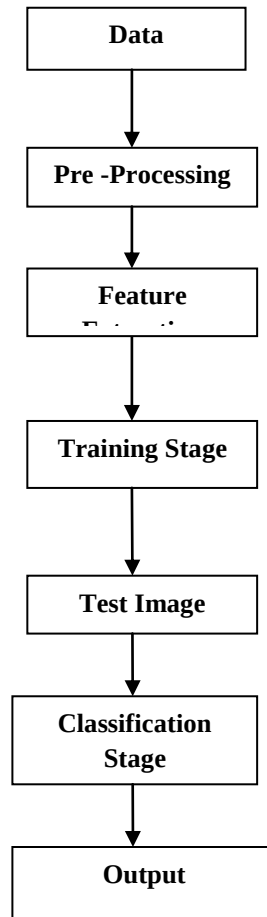


Fig. (1): Proposed system method

2) Pre-processing

This step contained several processes that aimed at the radiometric and geometric correction, standardization or improvement of the imagery to enhance the ability the component of the image quantitatively and qualitatively. So raise the reliability of the image by making a filtration for it via removing the noise and making edge filtration.

3) Two-Dimensional Fourier Transform

Before using Fourier transform image segmentation must be done. If the data base include 200 images and each size of the image is 512 x 512 pixels, to create the number but with small size that related to the same class each of the previous image segmented into 128 x 128 sub images, thus built 16 sub images of every image. Here, the first 12 sub images have been used for the training and the other 4 sub images have been used for the testing data set.

After the images have been segmented, every sub image was transformed via using the Fourier transformation. After that the phase values supply little information, just the matrices of coefficient magnitude was used for the texture characterization. All the 128 x 128 pixel sub images gains from the image segmentation have been transformed through the 2-D FT based on the following equation [9].

$$Ff(u, v) = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \exp \left(-j2\pi \left(\frac{ux}{M} + \frac{vy}{N} \right) \right) \quad (1)$$

and the magnitude of the coefficient matrix calculated by the following equations [9]:

$$F'(u, v) = \frac{|F(u, v)|}{\sqrt{u, v (u \neq 0)(v \neq 0) |F(u, v)|^2}} \dots (2)$$

To decrease the size of the input that supplied to the neural network the standard deviation and the mean value has been calculated for every row in the sub image has the size equal to 128 x 128 pixels via using the pixels value for every Fourier image domain.

4) Decision Making System

The BPNN (Back Propagation Neural Network) used to identify the image is cancerous or not. To make the classification by the BPNN two classes are appear S1 which include the cancerous images and the S2 which include the non cancerous images. The extracted feature or coefficient achieved before used here as input to the classifier of the neural network.

The BPNN has been trained by regulating the weight now it has the ability to know the class if zero or one. The classification technique divided into two phases; the training phase and the testing phase. In the first one the training phase a known data has been given like the proposed method here trained 100 images and tested 100 images. Now the classifier ability to classify the object in the right class was dependent on the features have been extracted before and the classification accuracy based on the training efficiency.

Iv. Results and Discussion

The suggested system was applied on MATLAB then tested with different images of Skin Cancer and other disease but not cancer to make the classification for them. In our database 200 images were included, 100 images are cancerous and 100 non-cancerous type. The proposed system consider all image as one input and include it in the system as one matrix and the features of the images have been extracted are calculated and then classify the image if cancerous or non-cancerous.

The designed neural network contains one input layer, two hidden layers and one output layer, by the using of back propagation algorithm. The used activation functions for the hidden layers aretansig, the tansig (tansigmoid) activation function map the net neuron input into values between +1 and -1. And for the output layer is the purelin activation function which calculates a layer's output from its net input. The used Back propagation network training function is the trainlm that updates weight and bias values according to Levenberg-Marquardt optimization, trainlm is often the fastest back propagation algorithm.

100 images are used for the training stage that contains 50 cancerous images and 50 non-cancerous images, for the testing stage another 100 images are used that are 50 cancerous images and 50 non-cancerous images. 32 features are used for the training and testing stages, which are the pixel features that use the histogram of the images that is resulted after applying the Fourier transform for the images. The network performance is calculated using the Mean Square Error (MSE) that measures the network's performance according to the mean of squared errors.

In this paper three test cases were adopted on the proposed system based on the number of features and iterations as explain in the following:

In first case the network target is 0.0001 and it is reached after 502 epochs as shown in figure 2.

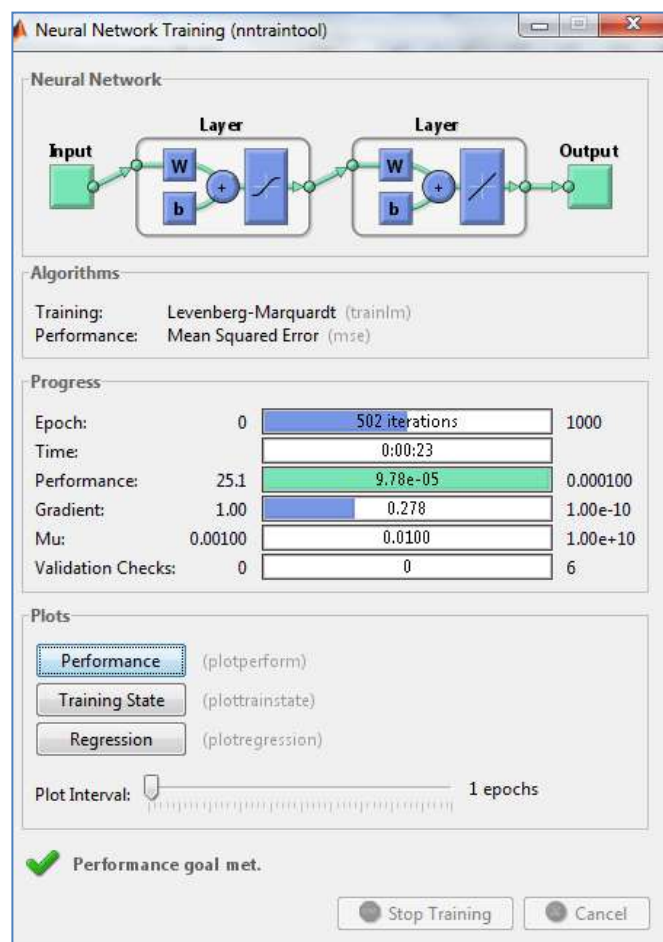


Fig. (2): Neural Network Training using 10 features.

The network performance for this case shown at figure 3 illustrates that the network needs 502 epochs to reach the used network goal.

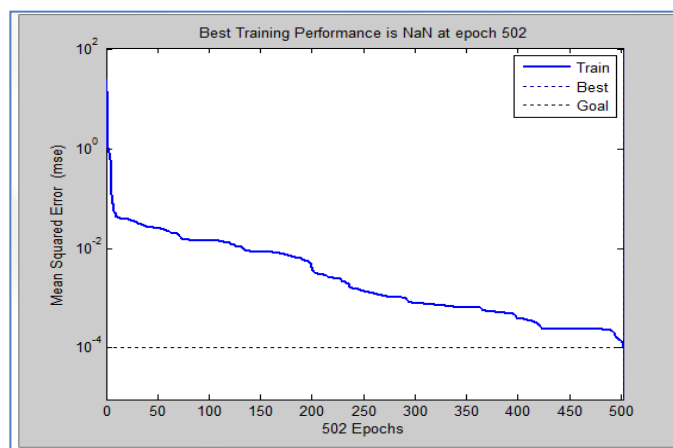


Fig.(1): The network performance at 502 iterations

In second case the network target is 0.0001 and it is reached after 28 epochs using 20 features as shown in figure4.

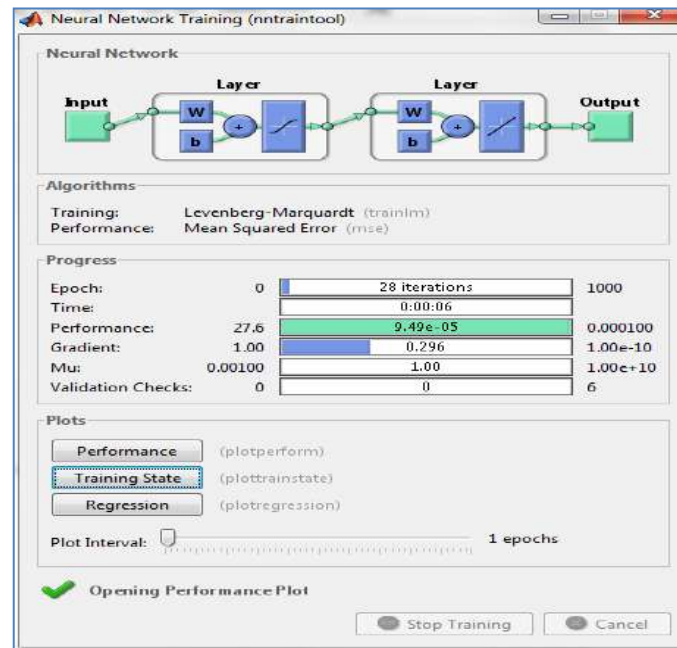


Fig. (4): Neural Network Training using 20 features

The network performance for this case shown at figure 5 illustrates that the network needs 28 epochs to reach the used network goal.

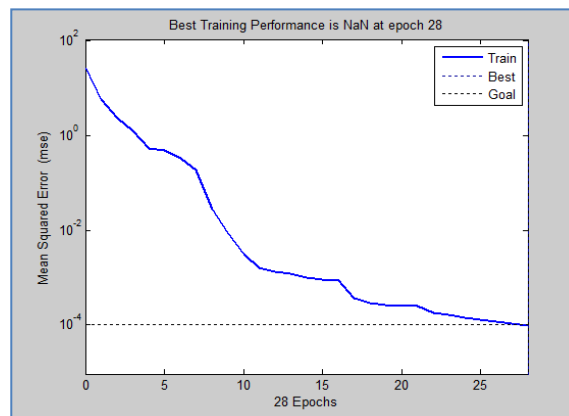


Fig.(5): The network performance at 28 iterations

In third case the network target is 0.0001 and it is reached after 181 epochs using 32 features as shown in figure 6.

The network performance for the third case shown at Figure 7 illustrates that the network needs 181 epochs to reach the used network goal.

The table (1) shows different accuracy values resulted from the using of different number of features, where the number of iterations will be different too.

The relationship between accuracy and the number of iterations is illustrated in figure 8.

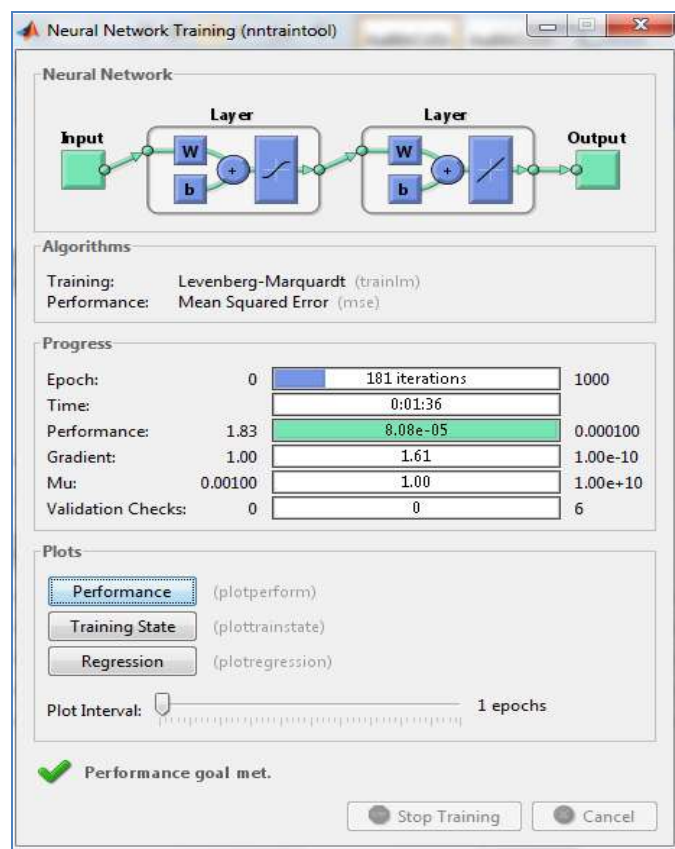


Fig.(6): The network performance at 181 iterations.

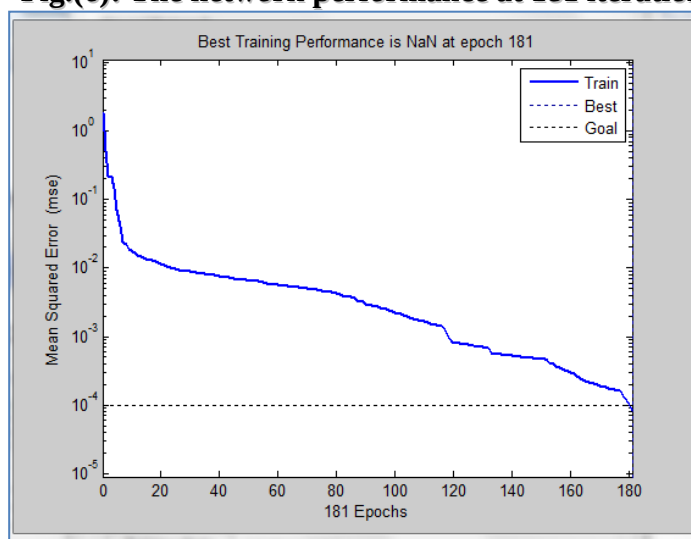


Fig.(7): The network performance at 181 iterations.

Table (1) the accuracy using different number of Features

Number of Features	Number of Iterations	Accuracy%
10	502	65.1515
20	28	68.1818
32	181	71.2121

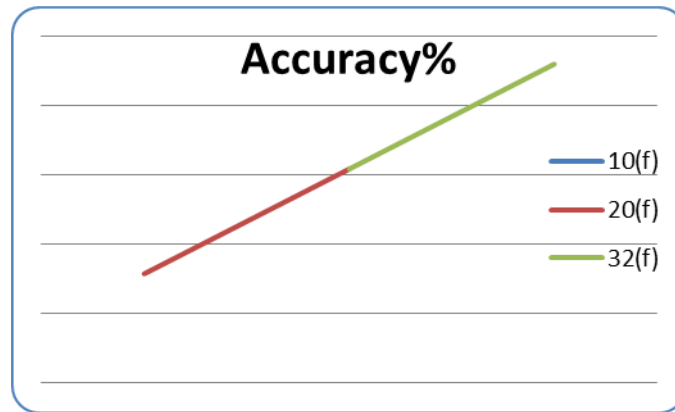


Fig.(8): Accuracy and the number of features relationship

Figure (9) represents an image of the sample adopted in this paper.

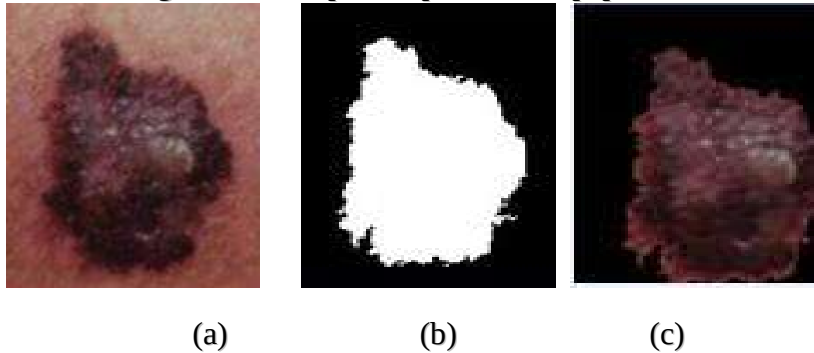


Fig.(8): (a) original image, (b), (c) Image after segmented via thresholding

Figure (10) illustrates the magnitude after applying the 2D Fourier transform method on the image.

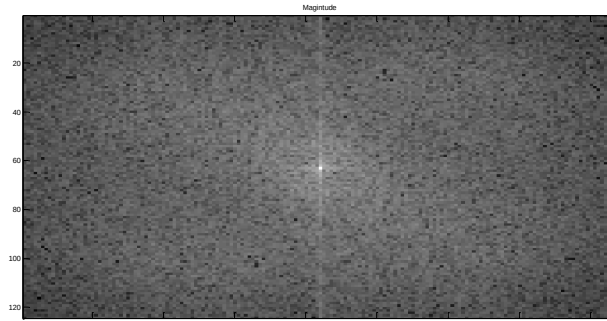


Fig. (10): The magnitude of the image

The phase spectrum of the image after the Fourier Transform shown in Figure (11).

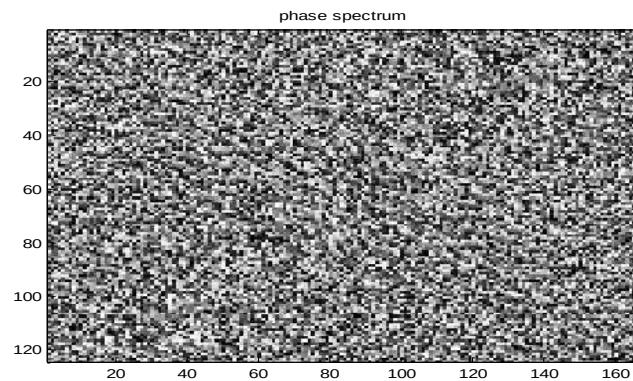


Fig. (11): The phase spectrum

V. Conclusion

Methodology of diagnosing here was using the Digital Image processing Techniques and the ANNs (Artificial Neural Networks) for making the classification of the Cancerous images (Malignant Melanoma) from the other disease of skin. The images have been collected and processed by the Image processing techniques. The region considered as cancerous one was splitted from the other considered as healthy region through the segmentation method.

The features of the images have been segmented have been extracted via the 2-D Fourier transform. Depending on these features the images have been classified by the Neural Network as non-cancerous and the cancerous one. Through making a variation for the Image processing technique and the classifiers this will help in enhance the accuracy of the system. One of the disadvantages for the image processing technique was the noise as a hair or bubbles ...est.; these will make the system inaccuracy in the classification stage, so the pre-processing and the post processing have been done. The system in the future will be a hybrid system consists of the Neural Network (NN) and the Support Vector Machine (SVM). This system makes a classification for the data. It is considered as a common form in the machine learning. Assume some data points given every one have been related to the one of two classes and the aim is to make a decision which the class of the new data will be in.

Vi. Acknowledgment

The authors would like to thank Mustansiriyah University ([www. uomustansiriyah.edu.iq](http://www.uomustansiriyah.edu.iq)) Baghdad-Iraq for its support in the present work.

References

- [1] J. Yogendra and J. Megha. "**Comparison between different classification methods with application to skin cancer**". International Journal of Computer Application, 53(11) 0975-8887, Septemper 2012
- [2] J. AbdulJaleel, S. Salim and A. R.B." **Artificial Neural Network Based Detection of Skin Cancer**". International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 1(3)2278- 8875, September 2012.
- [3] J. Blackledge, Fellow, IET and D. Adoubovitskiy. "**Object Detection and Classification with Applications to Skin Cancer Screening**",Isast Transactions On Intelligent Systems, 1(2)1-12, 2008.
- [4] P, Nammalwar, G, Ovidiu and W, Paul. "**Segmentation of Skin Cancer Images**", 2008.
- [5] K. Madasu and B. Lovell "**Blotch Detection in Pigmented Skin Lesions Using Fuzzy Co-Clustering and Texture Segmentation**", dicta, Digital Image Computing: Techniques and Applications, pp.25-31, 2009.
- [6] H. Ganzeli, J. Bottesini, L. Paz and M. Ribeiro. "**Skan: Skin Scanner – System for Skin Cancer Detecting Using Adaptive Technique**", IEEE Latin America Transactions, 9(2) 206- 212, April 2011.
- [7] M. Abu Mahmoud. "**The Automatic Identification of Melanoma by Wavelet and Curve let analysis**", pp. 680-685, December 2011.
- [8] A. Abdalbaki. "**Skin Cancer Image Segmentation & Detection by Using Unsupervised Neural Network (UNN)**". The 13th international Arab Conference on Information Technology ACIT'2012, pp: 506-515, Dec.10-12, 2012.
- [9] Y. Tao, V. Muthukkumarasamy, B. Vermaand M. Blumenstein. "**A Texture Feature Extraction Technique Using 2D-DFT and Hamming Distance**". Proceedings of the Fifth International Conference on Computational Intelligence and Multimedia Applications. 2003.

Iris Recognition Using Neural Network

Assistant Professor Safana Hyder Abbas Eman Abdulmunem
Mustansiriyah University/ College of Education/ Computer Science Department
eman_abdalmnam@yahoo.com

Abstract:

Iris recognition is the process of recognizing a person by analyzing the random pattern of the iris. Before recognition of the iris takes place, the iris is located using landmark features.

These landmark features and the distinct shape of the iris allow for imaging, feature isolation, and extraction. Localization of the iris is an important step in iris recognition because, if done improperly, resultant noise (e.g., eyelashes, reflections, pupils, and eyelids) in the image may lead to poor performance.

In this paper a proposed iris identification methodology consists of four major fundamental stages: image preprocessing, iris localization, iris feature extraction, and iris recognition. The features of two person's iris images are extracted and then recognized by using back propagation neural network.

1- Introduction:

The High protection mechanism and security is very essential things in grow of computer world. Biometric authentication is in rider seat of the computer society. Biometrics based on the Iris is among the most accurate existing techniques for human identification and verification because of uniqueness and long-term stability [1]. The probability of two individuals having the same Iris pattern is 1 in 1078 and even twins has different Iris pattern. Moreover iris patterns remain stable from 6 month of age to death [2]. Iris region is the part between the pupil and white sclera. This field is called Iris texture which provides many minute characteristics such freckles, coronas, stripes, furrows, crypts, etc. Information from Iris patterns is unique [3] for each subject and dispersed randomly and non-uniformly over the region of the Iris, but on notice that there is a concentration of characteristics at the region near the pupil. Due to this great quantity of information, good recognition efficiency can be achieved with only 50% of iris region available for analysis [3]. Today with the development of Artificial Intelligence algorithm, Iris recognition system may gain speed, hardware simplicity, accuracy and learning ability.

2- Iris images:

The first stage in the IRS recognition is eye image acquisition by using special digital camera. From important conditions these images should have high quality and good resolution with good format like JPEG or BMP. The image quality is affected by camera type, the illumination intensity, the space between the camera and the eye, and all events in image capturing environment [4]. Early researches were obstructed by the lack of iris images. Now, multi free datasets exist on the internet for testing usages. A well-known dataset is CASIA (Institute of Automation of the Chinese Academy of Sciences) iris image dataset developed by Chines Academy of Sciences has been released to the international biometrics community Intervals consist of images set captured with self-developed closely iris-camera as shown in Figure (1). CASIA-Iris Interval dataset consists of 249 subjects and each subject has two (left and right) samples, each one has 6 or 7 iris-images acquired from the same eye. The iris images are gray scale 8-bits jpeg format with a resolution of 320*280 pixels captured in two sessions for most iris-images in an indoor environment [5].

3- The proposed method

In this paper the features for a special person is extracted according to the method proposed by [6]. The block diagram of the proposed system is shown in figure (2).

3-1-Images acquisition

One image is selected from CASIA dataset as shown in figure (3).

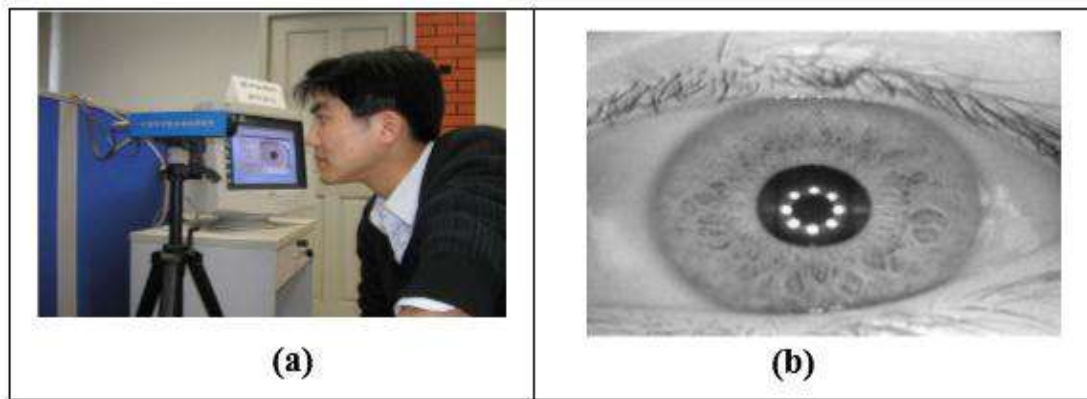


Fig.(1): Iris Image Capture: (a) Self-Developed Iris Camera Used for Set of CASIA-Iris-Interval V. 4.0, (b) Example of image in "CASIA Iris-Interval V. 4.0" [5]

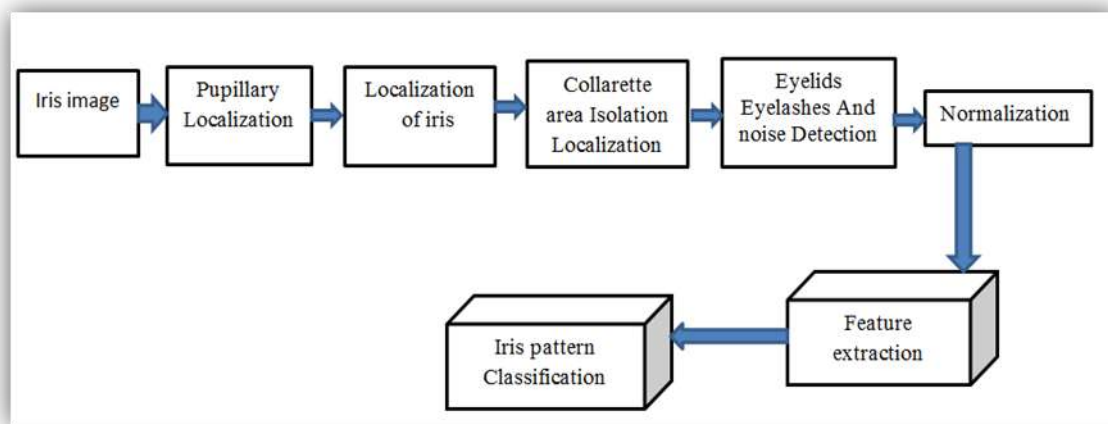


Fig. (2): Flow diagram of the proposed iris recognition scheme

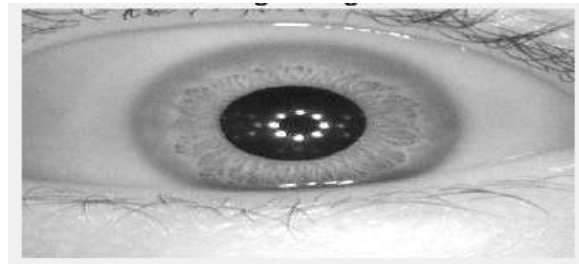


Fig.(3): original iris image

3-2 Preprocessing

In general, the work on the IRS requires images of the iris should be pure, clear, free of noise (eyelashes and eyelid), and separated from the area of the pupil of the eye, therefore several processing operation are needed for the whole image to get pure iris image. Preprocessing contains set of operations contain (Localization, Segmentation, Normalization, Enhancement), these operations have been utilized to locate the iris region and isolating it from the surrounded area in the image (noise & pupil). The basic steps of preprocessing are illustrated below:

3-3 Iris Localization

The localization phase consists of determining the external edge of the iris and detecting the pupil region to locate the internal edge of the iris, it aims to extract the iris region. The previous selected image is subjected to iris localization in [] and the result shown in figure (4).

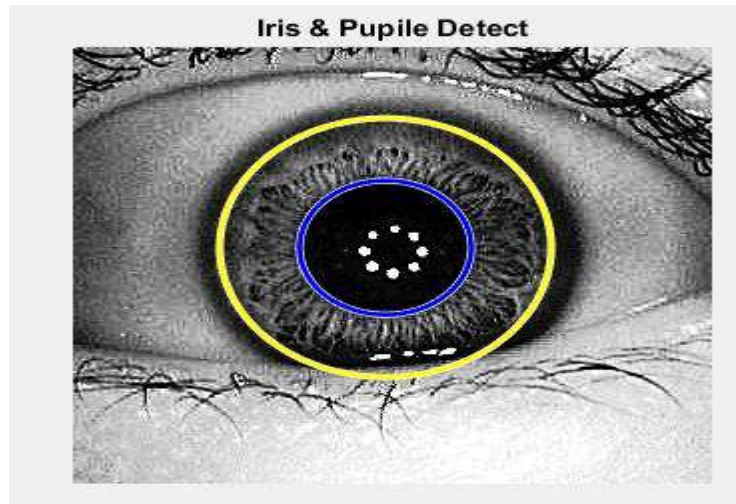


Fig. (4): Localization iris and pupil

3-4 Eyelids, Eyelashes, and noise detection

In this step, the region of interest (ROI) will be determined from the image of iris mask after removing the noise region (eyelash & eyelid) from it, as shown in Figure (5)

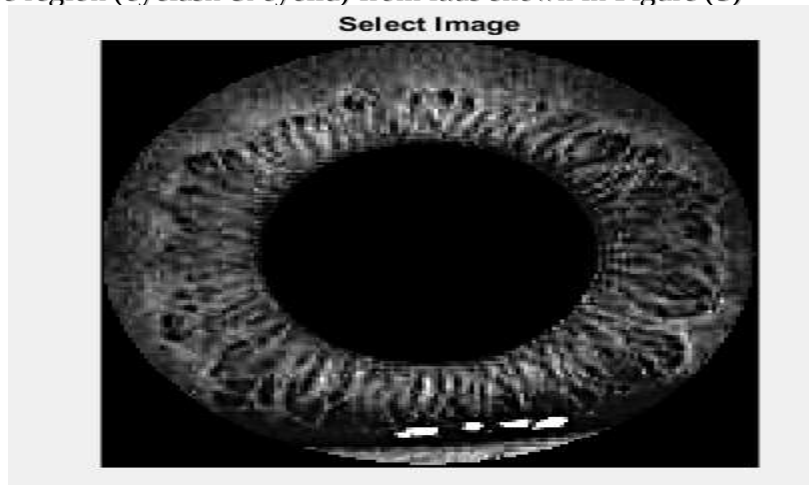


Fig.(5): Removing Eyelids, Eyelashes, and noise detection

3-5 Iris Normalization

The normalization process includes transforming the iris region that is determined in the rings shape to a rectangular shape with a fixed size. The size, normalization and shape conversion is accomplished by unwrapping the iris region and map all the points lay between the iris boundaries from the original Cartesian coordinates $I(x, y)$ into their equivalent normalized polar coordinates $I(r, \phi)$.



Fig. (6): Iris Normalization

3-6 Feature extraction

Every iris image has distinctive feature that makes it distinguishable from others. So, good extracted features should have high discrimination power in terms of identifying the iris images. The iris feature extraction operation aims to extract iris code from iris normalization image that could be represented as feature vector, these vectors are used in the process of pattern matching. The features of the previous normalized image are extracted using GLCM method.

3-6-1 Gray Level Co-occurrence Matrix (GLCM):

In this paper the Grey Level Co-occurrence Matrix (GLCM) is used [6]. The technique uses the GLCM of an image and it provides a simple approach to capture the spatial relationship between two points in a texture pattern. It is calculated from the normalized iris image using pixels as primary information.

Algorithm: Feature Extraction for Second Method (GLCM for 3offset)

```

Goal: Extract feature from three blocks from IRIS region
Input: blockq () // block of iris image
blokN=3 // number of block
Offset=1 // the value of distance
theta [0, 45, 90] // array of one dimension save the value of angles
Output: Vect() // array of one dimension contain feature for iris image
Step1: Basic loop and vector for this algorithm
Vect ← zero (1*90) // create initial array
For k=1 → 3 // the basic, loop of number of blocks input the algorithm
Step1.1: Find GLCM for each theta
no ← 0 // initial value
[blokhig, blokwid] ← size (blockq(k)) // the two dimension of block
s ← value(theta) // size of array
For theta= 0 → s // loop around the value of theta
no ← no+1 // compute the number of GLCM created
For x= 1 → blokhig // loop around the row of block
For y= 1 → blokwid // loop around the column of block
Set i ← blockq (x,y)
Check if theta =0 // if (1)
Set j ← blockq(x,y+offset) // offset [0 1]
glcm(i,j) ← glcm(i,j)+1
Endif //(1)
Check if theta =45 // if (2)
Set j ← blockq(x- offset, y+offset) // offset [-1 1]
glcm(i,j) ← glcm(i,j)+1
Endif //(2)
Check if theta =90 // if(3)
Set j ← blockq(x- offset, y) // offset [-1 0]
glcm(i,j) ← glcm(i,j)+1
Endif //(3)
Endfor // y
End for // x
Endfor // theta
Step1.2: Calculating Statistical Measurements
Vectfeat (k) ← zero (1*30) // create initial array
[hig, wid] ← size (glcm) // the two dimension of block
For m=1 → no // loop around the number of glcm created
Feature (m) ← [set of value] //compute set of statistical measurements using eq.(2.14) to eq.(2.24)
Vectfeat(k)= Vectfeat (k) + Feature(m)
Endfor //m
Step1.3: Gathering Vectors of Features
Vect= Vect +Vectfeat (k)
Endfor // (k)the basic, loop of number of blocks input the algorithm
Step5: Return Vect() array

```

The result will be 120 values which will be saved in array with one dimension (vector) as shown in table (1).

Table (1) Example of the extracted feature for person 1

1	2	3	4	5	6	7	8	9	10
0.778468	0.596273	0.110128	2.512415	0.720024	0.220704	6.184393	4.565631	0.935712	5.864596
11	12	13	14	15	16	17	18	19	20
0.908355	0.663388	0.101531	2.569492	0.691346	0.197783	6.22283	4.578431	0.928661	5.837596
21	22	23	24	25	26	27	28	29	30
0.555042	0.455882	0.130127	2.374587	0.781856	0.252941	6.186497	4.564286	0.950414	5.979412
31	32	33	34	35	36	37	38	39	40
1.091219	0.724638	0.097796	2.624492	0.673601	0.197357	6.21942	4.578858	0.923342	5.746803
41	42	43	44	45	46	47	48	49	50
0.564803	0.4853	0.137285	2.26818	0.7653	0.239752	7.621285	5.27619	0.946959	7.416563
51	52	53	54	55	56	57	58	59	60
0.751918	0.589088	0.122447	2.368256	0.721679	0.209719	7.687185	5.303495	0.936315	7.396846
61	62	63	64	65	66	67	68	69	70
0.437395	0.39958	0.152975	2.176274	0.803992	0.257143	7.652489	5.290336	0.956022	7.52479
71	72	73	74	75	76	77	78	79	80
0.719949	0.564791	0.126611	2.353638	0.73312	0.22208	7.674504	5.302217	0.938941	7.410486
81	82	83	84	85	86	87	88	89	90
1.552209	0.927041	0.060179	3.07119	0.597622	0.103748	10.83699	6.119813	0.903555	10.14993
91	92	93	94	95	96	97	98	99	100
1.722183	0.989369	0.056689	3.114875	0.577296	0.100638	11.06529	6.201276	0.897767	10.33239
101	102	103	104	105	106	107	108	109	110
0.602941	0.516106	0.088015	2.712779	0.75063	0.166667	11.04867	6.20098	0.94362	10.87885
111	112	113	114	115	116	117	118	119	120
1.819986	1.012048	0.05649	3.129206	0.572615	0.102055	11.054	6.201276	0.895956	10.28278

4- The detection stage using back-propagation (BP) algorithm:

The previous 120 extracted features in table (1) and another 120 value for person 2 are entered to the BP neural network to recognize two selected person. The number of nodes in input layer is equal to two with 120 value in each row which represent the extracted features and the number of nodes in the output layer is two with 120 value in each row which represent the two persons codes and the number of nodes in the hidden layer is 10 which determined by trial and error. The neural network reached the solution after 16 epoch. The BPNN details are shown in figure (7).

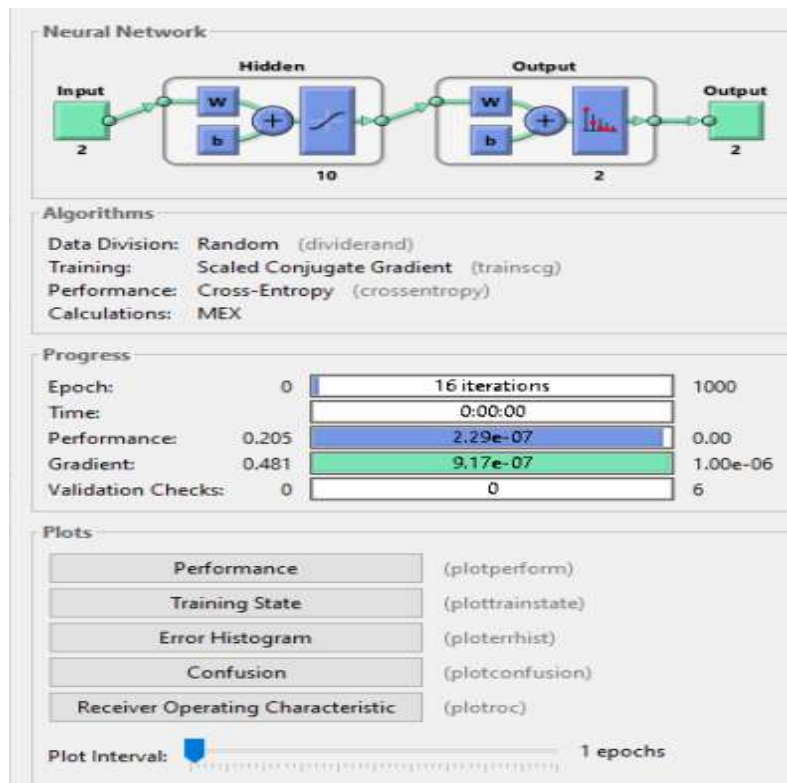


Fig. (7): the BPNN performance

The error curve with respect to number of epochs is shown in figure (8).

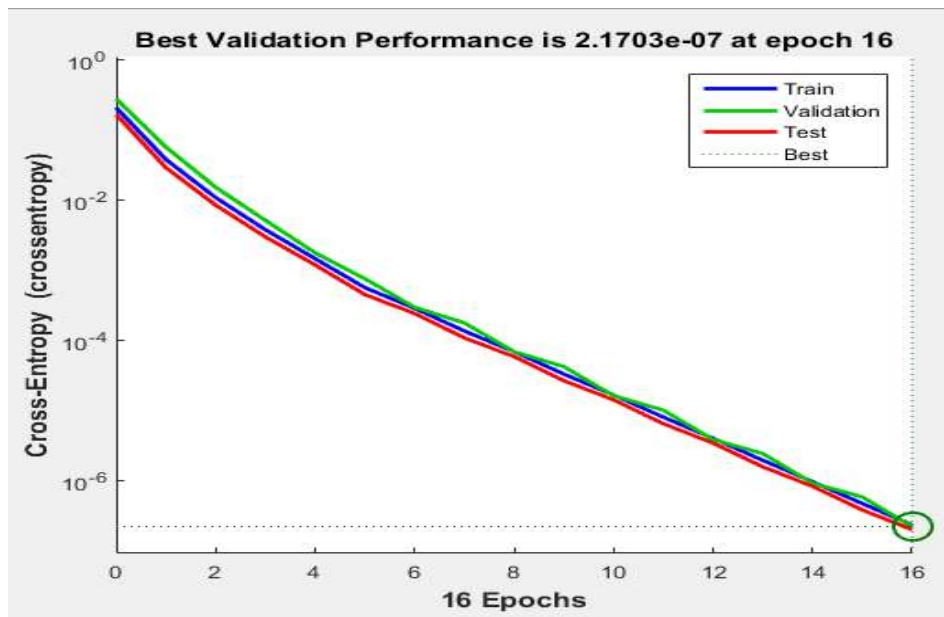


Fig. (8): Error curve

5- Conclusions:

In this paper the iris features for a two persons are extracted and prepared as an input to back propagation neural network. The neural network is trained with these inputs and the corresponding output codes correlated for each person. It reaches the final solution after 16 iteration (epochs) with error = 2.1703 e-07. The error curve was smooth and there is no local minimum. The two person were recognized correctly using their iris images.

References

- [1] Daugman J, "Complete Discrete 2-D Gabor Transforms by Neural Networks for Image Analysis and Compression", IEEE Transactions on Acoustics, Speech, and Signal Processing, Vol. 36, no. 7, July 1988, pp. 1169-1179.
- [2] Daugman, J., "How Iris Recognition Works", available at http://www.ncits.org/tc_home/m1htm/docs/m1020_044.pdf.
- [3] G. Savithiri and A. Murugan, "Performance Analysis of Iris Recognition Algorithms", Proceedings of the International Conference on Millennium Development Goals (MDGICT) pp. 294-299, Dec. 2009.
- [4] Daugman. J, "Biometric Personal Identification System Based on Iris Analysis", U.S. Patent No. 5,291,560, March 1, 1994
- [5]. Y. S. González, J. L. Rodríguez and E. G. Llano, " Iris Segmentation Methods and Current Challenges: State of the Art", Advanced Technology Application Center (CENATAV), RT_059, Serie Azul, ISSN: 2072 – 6287, Jan 2014
- [6] Shymaa A. H., "Iris recognition system using PNN and Co-occurrence matrix", M.Sc. thesis, Department of Computer Science, Mustansiriyah University, 2016.

Master Eye Region Based on Multiwavelet Transform Using Association Rules

Raniah Ali Mustafa Zahraa Salah Dhaief
Computer Science Dept., College of Education, Mustansiriyah University
rania83computer@yhoo.com zehraa_84@yahoo.com

Abstract:

As technology is advancing, the demand of face recognition which is one of the biometric technologies is increasing day by day. During the last years, many researchers had introduced different techniques and different algorithms for accurate and reliable face patterns recognition. Since eye movements are regarded as an important tool for studying visual information processing. The proposed system passes through two main phases the training phase and retrieval phase. The two phases share the two main modules of the system (preprocessing module and feature extraction module). The preprocessing includes three stages; face clip detection, eye block detection and edge detection. In this paper main idea that using master eye blocks and then feature extraction using algorithm depends on multiwavelet transforms. This algorithm depend on the idea of extracting features from master eye images person to extract association rules between these features eye images person retrieval. These rules obtain from using Frequent Pattern (FP-growth) Association Rules (AR) where give for each features code. These rules are id for master eye block for person. The system was tested over a database collected from 30 volunteers, where 15 images for each person were collected under different lighting conditions, varied in expression, orientations, illumination, background, ages. The achieved training rate was 100% and the average of precision (74%) was achieved.

Key words: Master eye, Wavelet Decomposition, Multiwavelet, Data mining, Association Rules, Apriori Algorithm, FP growth.

مقطع العين الأساسية على أساس تحويلات متعددة الموجات باستخدام قوانين الرابطة

م. م. رانية علي مصطفى م. م. زهراء صلاح ضايف

المستخلص:

مع التقدم التكنولوجي، فإن الطلب على التعرف على الوجه الذي هو واحد من القياسات الحيوية يتزايد يوماً بعد يوم. وخلال السنوات الأخيرة، أدخل العديد من الباحثين تقنيات مختلفة وخوارزميات مختلفة للتعرف على أنماط الوجه الدقيقة والموثوق بها. منذ ذلك حركات العين أداة هامة لدراسة معالجة المعلومات البصرية. يمر النظام المقترح عبر مرحلتين رئيسيتين مرحلة التدريب ومرحلة الاسترجاع. وتشترك المرحلتان في النموذجين الرئيسيين للنظام (المعالجة المسبقة واستخراج الخصائص). وتشمل المعالجة المسبقة ثلاث مراحل: face clip detection، eye block detection و edge detection. في هذه الورقة الفكرة الرئيسية أن استخدام مقطع العين الأساسية ومن ثم ميزة استخراج باستخدام خوارزمية تعتمد على Multiwavelet transforms. هذه الخوارزمية تعتمد على فكرة استخراج الخصائص من صور العين الشخص لاستخراج قواعد الترابطية بين هذه الخصائص وذلك لاسترجاع صور عين الشخص. هذه القواعد يتم الحصول عليها من استخدام نمط مكرر (FP-النمو) قواعد ترابطية (AR) إذ تعطي رمز لكل الخصائص. هذه القواعد هي معرف مقطع العين الرئيسية للشخص. وقد تم اختبار النظام على قاعدة بيانات جمعت من 30 متطوعاً، إذ تم جمع 15 صورة لكل شخص تحت ظروف الإضاءة المختلفة، وتتنوع في التعبير والتوجهات والإضاءة والخلفية والأعمار. نسبة التدريب حققت 100٪، وتم تحقيق متوسط الدقة (74٪).

الكلمات المفتاحية: العين الأساسية، تحليل الموجات، تحويلات الموجات المتعدد، قواعد ترابطية، خوارزمية Apriori، FP growth.

1. Introduction

Face is the index of mind, it is our first center of attention in social life and it is playing a main role in carrying identity [1]. Face recognition has received a great deal of attention over the last few years because of its many applications in security, surveillance, and general identity verification and image database investigations in various domains. Face recognition is a biometric based technique which has risen as the most promising option for perceiving people, instead of authenticating people and granting them access to physical and virtual domains based on passwords, PINs, smart cards, and plastic cards. Biometric based techniques are essentially pattern recognition applications that acquire certain biometric attributes from an individual, extract a salient feature set from that attributes, compare this feature set against the feature set(s) enrolled in the database, and finally produce a final decision that based on the result of the comparison. A generic biometric system can be viewed as having four main modules: sensor, quality assessment and feature extraction, matching and a database [2]. The system illustrate in the figure (1) below:

- Retrieval Part: This part is concerned with retrieving the most 10 similar images listed in the database to the user's query image according to their Association Rules. Retrieval part depends on two steps Similarity Association Rules and Image Fetching.
- Similarity Association Rules: This step is used to compute the distances between the user's query image Association Rules and Association Rules for all images in the database to find nearest images.
- Image Fetching: Image Fetching is responsible for fetching the image due to its corresponding path and then displaying nearest 10 images.

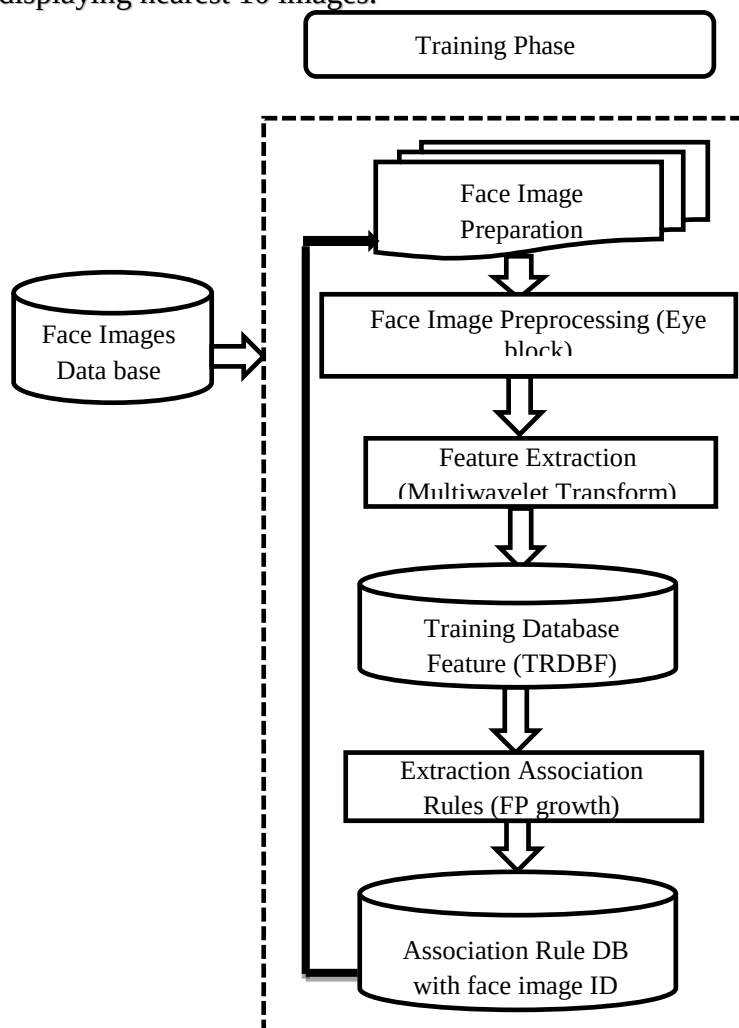


Fig. (1): the framework of the proposed face recognition system

2. Background Theorem

The proposed system depends on the fact that any master eye image person has multi unique features. These features are different from one master eye image to another. In this paper an attempt is done to propose algorithms to extract features from the person master eye image. These algorithms depend on the idea of extracting features from master eye images of persons to find association rules (FP growth) between these features to retrieve master eye images of persons. Feature extraction based on multiwavelet transforms.

2.1 Wavelet Transforms

A "wave" is usually defined as an oscillating function of time or space, such as a sinusoid. A "Wavelet" is a "small wave", which has its energy concentrated in time to give a tool for the analysis of transient or time-varying phenomena [3].

Wavelets are mathematical functions that cut up data into different frequency components, and then study each component with a resolution matched to its scale. Wavelets were developed independently in the fields of mathematics, electrical engineering, and seismic geology.

Interchanges between these fields during the last ten years have led to many new wavelet applications such as image compression, astronomy, acoustics, nuclear engineering, signal and image processing, neurophysiology, music, speech discrimination, optics, fractals, pure mathematics applications such as solving partial differential equations and earthquake prediction [4]. Figure (2) shows the wave (sinusoid) and the wavelet.

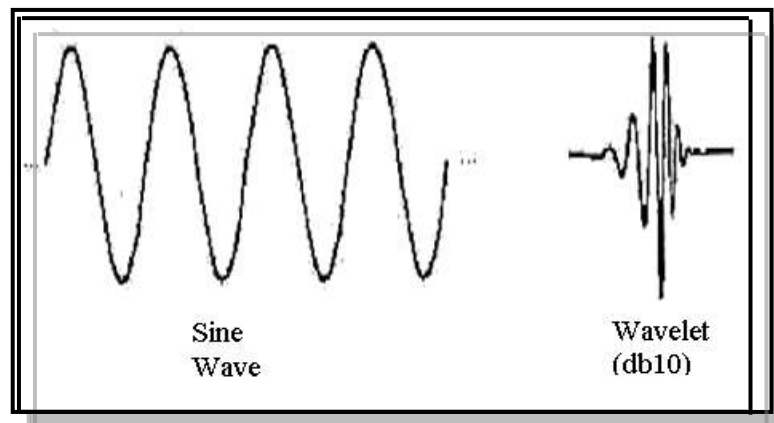


Fig. (2): A wave and wavelet

The main characteristic of wavelets (if compared to other transformations) is the possibility to provide a multi resolution analysis of the image in the form of coefficient matrices.

2.2 Wavelet Decomposition

Multi-resolution methods provide powerful signal analysis tools, which are widely used in feature extraction, image compression and denoising applications. Wavelet decomposition is the most widely used multi-resolution technique in image processing.

The two-dimensional wavelet transform is performed by consecutively applying one-dimensional wavelet transform to the rows and columns of the two-dimensional data. In figure (3), the tree representation of one level two-dimensional wavelet decomposition is shown. In this figure, L denotes low-pass filtering (LPF) and H denotes high-pass filtering (HPF), while $\downarrow 2$ represents down sampling by a factor of 2. In the final stage of the decomposition we have four $N/2 \times N/2$ resolution sub and images: LL, the scaling component containing global low-pass information, and three wavelet components, HL, LH, and HH corresponding respectively to the horizontal, vertical and diagonal details [5].

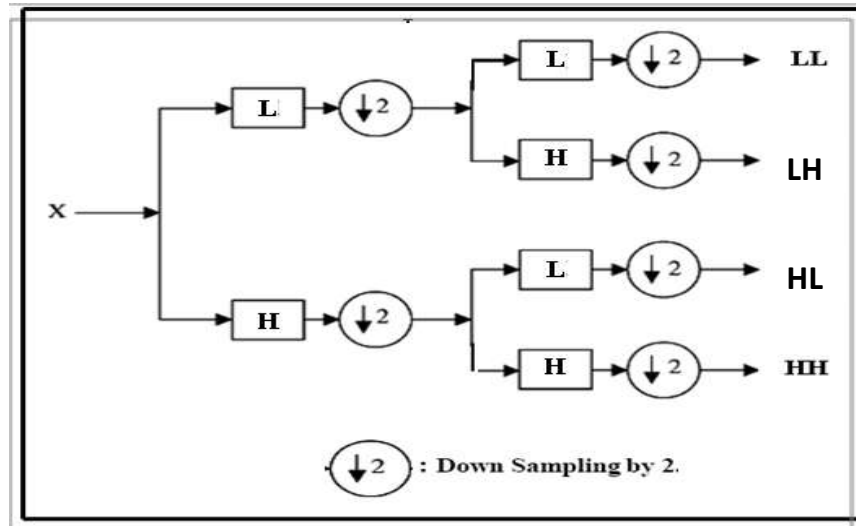


Fig. (3): Tree representation of one-level 2D wavelet decomposition

The data in sub band "LH" was obtained from high pass filtering of the rows and then by low pass filtering of the columns.

Also, the low information image can be decomposed into another four images as shown in figure (4).

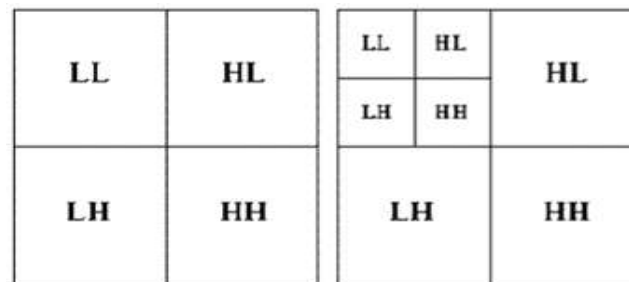


Fig. (4): Wavelet decomposition: (a) Single level decomposition;
(b) Two levels decomposition

1.2 Multiwavelet Transforms

Wavelet theory is based on the idea of multi-resolution analysis (MRA), in which the standard multi-resolution has one scaling function $\phi(t)$. However, one can imagine a more general MRA setting when several scaling functions are allowed, this idea is the notion of multiwavelet, which has several advantages in comparison to scalar wavelets. Such features as short support, orthogonality, symmetry, and vanishing moments are known to be important in signal processing. A scalar wavelet cannot possess all these properties at the same time. On the other hand, a multiwavelet system can simultaneously provide perfect reconstruction while preserving length (orthogonality), good performance at the boundaries (via linear-phase symmetry), and a high order of approximation (vanishing moments). Thus multiwavelets offer the possibility of superior performance for image processing applications, compared with scalar wavelets [6, 7].

The 2×2 matrix filters in a multiwavelet filter bank require vector inputs. Thus, a 1D input signal must be transformed into two 1D signals. This transformation is called "preprocessing".

Preprocessing is a mapping process which is done by a pre-filter. The aim of preprocessing is to associate the given scalar input signal of length N to a sequence of length-2 vector in order to start multiwavelet transformation process.

However, the result after one cascade step can be realized as the following matrix:

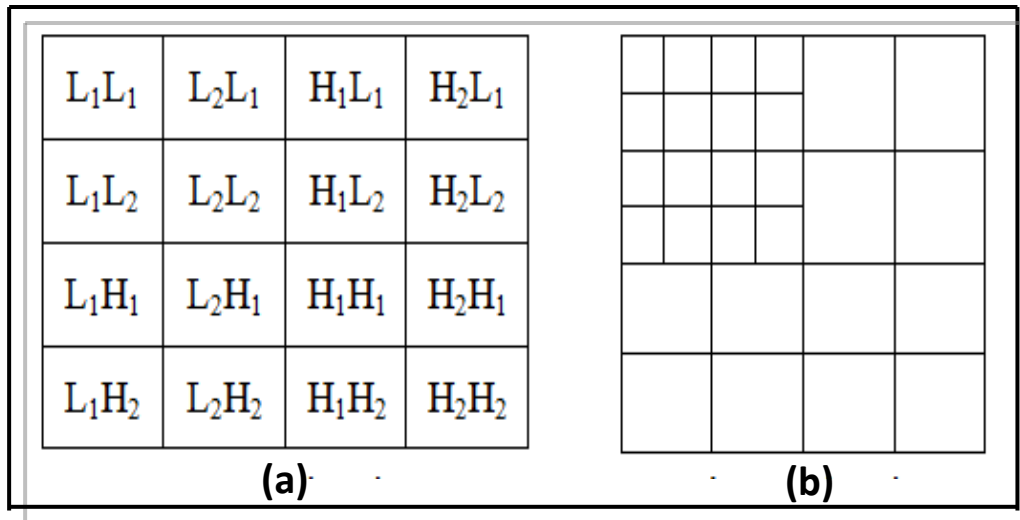


Fig. (5): Multiwavelet image decomposition: (a) one level, (b) two levels

At the end of the first level of two dimension multiwavelet decomposition, we have a 16-subband intermediate image as shown in figure (5-a). The decomposition is started from an initial square matrix, and L-Level multiwavelet produces $4(3L+1)$ sub-images.

Here a typical block H_2L_1 contains low-pass coefficients corresponding to the first scaling function in the horizontal direction and high-pass coefficients corresponding to the second scaling function in the vertical direction.

The next step of the cascade will decompose the "low-low-pass" sub matrix

L_1L_1	L_2L_1
L_1L_2	L_2L_2

 in a similar manner. The result is 28 sub-images as shown in figure (5-b).

3. Statistical Measures as Discriminating Features

The statistical measures, such as Mean, Standard Deviation, Variance, Energy, Entropy is typically useful to representation characteristics or features of data, it is simple and needs minimal calculation load [8, 9].

• **Mean:** Is a set of intensity values for the elements of image are divided by the number, and is represented by the following equation:-

$$\mu = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N x(i, j), \dots \dots \dots (1)$$

• **Standard Deviation:** The Standard Deviation is the most utilized indicator of variability and is a measurement concerning to the average distance of the scores from their mean value. It is computed on the basis of the positive square root of the variance, and is represented by the following equation:-

$$\sigma = \sqrt{\frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (x(i, j) - \mu)^2}, \dots \dots \dots (2)$$

The standard deviation is significant in detecting the details contented in an image.

• **Variance:** Is the average of the total square deviations values for the arithmetic mean. In fact it is almost identical to the standard deviation, and is represented the following equation:-

$$\sigma^2 = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (|x(i, j)| - \mu)^2, \dots \dots \dots (3)$$

• **Energy:** Is intended power to distribute information in the image, which is usually the factor that image is approaching compressibility, and is represented by the following equation:-

$$ENE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N x^2(i, j), \dots \dots \dots (4)$$

- **Entropy:** Numerical value representing the entropy of the gray image. Entropy is a statistical measure of the random that could be utilized to describe the texture information of the input image, and is represented by the following equation:-

$$ENT = - \sum_{i=1}^M \sum_{j=1}^N (x(i, j) \log_2(x(i, j))), \dots \dots \dots (5)$$

Where N and M are size of row and column of the $x(i, j)$, a wavelet coefficient.

4. Related work

Some of the published works related to the objectives of this work are given in the following paragraphs:

Ammar Fakhri Mahdi (2012) in this work, a technique for the recognition of the still face image is proposed. This technique is based on extract features using two levels of the two Dimensional Discrete Multiwavelet Transform (2D-DMWT). These features will be used for classifying the face images with Probabilistic Neural Network (PNN) and Minimum Euclidean Distance (MED) respectively [10].

Hashem Bedr Jehlol (2013) proposed an algorithm which combines the image algorithms and data mining algorithms to get an approach that retrieves images depending on color and texture features; and to hybrid them using an association rules activity. The proposed algorithm uses many features, some of them are extracted from texture such as (Mean, Contrast, Entropy, Energy, Homogeneity and Inverse Difference Moment) and the others are extracted from color space such as (RGB, HSV, YUV and YIQ). The proposed system Image retrieval that is based on Association Rules (IRBAR) has higher accuracy (73%) [11].

Samar Amil Yousif (2014) the system work flow passes through two main phases the enrollment phase and the recognition phase. The two phases share the two main modules of the system (preprocessing module and feature extraction module). The preprocessing include three stages; face clip detection, eye block detection and edge detection. After read face image as bmp file, the face detection stage pass through these steps; convert to HSV color space for skin color modeling, segmentation process is done for detect the skin area, noise removal, face localization. The eyes blocks detection stage include these steps; image smoothing, convert to gray scale, contrast enhancement and extract master eye cutouts block. The third stage consists of applying canny edge detection and thinning. All these steps to obtain the main edges of eye block. In this research the features vector that represent the face attributes consists of fifteenth feature obtained by applying moment invariant, color moment and geometric features. Probabil-istic neural networks (PNN) have been used to make a decision in matching stage. The system was tested over a dataset col-lected from 30 volunteers, where 10 images for each person were collected in different pose, expression and orientation. The achieved training rate was 100% and an excellent recognition rate 88.5% was achieved [12].

Sarra`a Mowaffaq Abood (2014) in this thesis introduces a proposal to advance e-learning over online social network, facebook, through using data mining for analyzing the structure of this network and the behavior of its users, the proposal include constructing a proposed student's facebook dataset for Iraq student's society, on this data set applying two algorithms once customized Frequent Pattern (FP-growth) Association Rule (AR) technique as a ranker (since it calculates the frequency of attributes) and mining technique (since it extracts knowledge to predict decision making to support e-learning over facebook through analyzing student's behavior). Second algorithm is proposed Modified k-mean techniques to introduce the structure of network's users;

Experiments were conducted to show the effectiveness of the proposed system done on IPHES dataset; customized FP-growth took much less time and space than traditional apriori, the last is deadlocked with proposed system. Modified k-mean give results with higher accuracy than traditional ones; due to weighting of important attributes according AR ranking, selecting centroid, and converting Euclidian distance to output complete vectors [13].

5. Association Rules Technique

Association rules are one of the most researched areas of data mining and have recently received much attention from the database community. They have proven to be quite useful in the marketing and retail communities as well as other more diverse fields [14]. Association rules, first introduced in 1993 are used to identify relationships among a set of items in a database. These relationships are not based on inherent properties of the data themselves, but rather based on co-occurrence of the data items [15].

6. Apriori Algorithm

This algorithm is one of the algorithms that have the influence on frequencies item sets for association rules (AR). It was proposed through Srikant and Agrawal [16]. The algorithm of names relies on the truth that the algorithm utilizes prior knowledge of frequencies item set characteristics. Algorithm which utilizes a repeated way also it is identified as a level-wise (L-w) seeking, where k-item sets are utilized for exploration of (k+1)-item sets. Initially, the group of frequencies of 1-itemsets is found out. This set is indicated through L1. L1 is utilized to find out L2, the set of frequencies of 2-itemsets that is utilized to find out L3, and other, even when no more frequent k-item sets could be discovered. To find out of every L_k needs one entire scan of the DB [17].

7. FP-Growth Algorithm

Recently, an FP-tree based frequent pattern mining method, called FP-growth, developed by Han et al achieves high efficiency, compared with an Apriori-like approach. The FP-growth method adopts the divide-and-conquer strategy, uses only two full I/O scans of the database, and avoids iterative candidate generation [18]. FP-growth is used for mining the complete set of frequent patterns by pattern fragment growth. Efficiency of mining is achieved with three techniques [19]:

1. A large database is compressed into a highly condensed, much smaller data structure, which avoids costly, repeated database scans.
 2. FP-tree-based mining adopts a pattern fragment growth method to avoid the costly generation of a large number of candidate sets.
 3. A partitioning-based divide-and-conquer method is used to dramatically reduce the search space.
- The frequent Pattern mining problem can be formally defined as follows. Let $I = \{i_1, i_2, \dots, i_m\}$ be a set of items, and DB be a transaction database, where each transaction T is a set of items and $T \subseteq I$. A unique identifier, called TID, is assigned with each transaction. A transaction T contains a pattern P, a set of items in I, if $P \subseteq T$. The support of a pattern P is the number of transactions containing P in DB. We say that P is a frequent pattern if P is less than a predefined minimum support threshold ξ , frequent pattern mining which consists of two steps [20]:

1. Construct a compact data structure, frequent pattern tree (FP-tree), which can store more information in less space.
2. Develop an FP-tree based pattern growth (FP-growth) method to uncover all frequent patterns recursively.

Apriori algorithm may still suffer from the following two nontrivial costs [21, 22]:

1. It may still need to generate a huge number of candidate sets. For example, if there are 10^4 frequent 1-itemsets, the Apriori algorithm will need to generate more than 10^7 candidate 2-itemsets.
2. It may need to repeatedly scan the whole database and check a large set of candidates by pattern matching. It is costly to go over each transaction in the database to determine the support of the candidate item sets.

8. The Proposed system

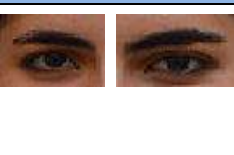
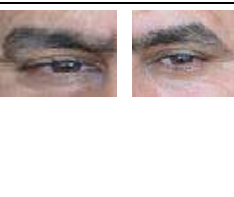
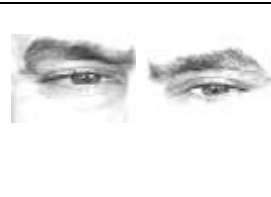
The main idea for proposed system that using master eye blocks and then feature extraction using algorithm depends on multiwavelet transforms.

The proposed system passes through two main phases the training phase and retrieval phase. The two phases share the two main modules of the system (preprocessing module and feature extraction module). The retrieved images are ranked according to some calculated similarity by applying best match association rules technique. Also proposed Content Based Image Retrieval (CBIR) system that supports querying by example to retrieve similar face images from a database depends on the visual content of face images. All the features extracted from the training face images are stored into database features and then used to choose the closest one to the requested face image.

Step1: Preprocessing: After reading the color face image as bmp file format, the first module is preprocessing which consists of three stages:

1. Face Detection: the goal of this stage is to determine the location of face in the image and extract it. It consists of the following steps; skin color modeling, skin segmentation, noise removal, face localization and clipping.
2. Eye detection: this stage includes the following steps; image smoothing, convert to gray scale, contrast enhancement, the main goal of this stage is determining and extracting master and second eye blocks.
3. Edge Detection: the aim of this stage is to obtain main edge of eye block. It consists of two steps, canny edge detection and thinning process. The table (1) illustrate preprocessing:

Table (1) The preprocessing

Class	F-C	Eyes	Gaussian $\delta=0.8$	Threshold=140	TMin20	TMax 100
C1						
C2						

Step2: Apply Multiwavelet Transform:

In this paper is used multiwavelet on eye block where obtained sub image but four is low frequency.

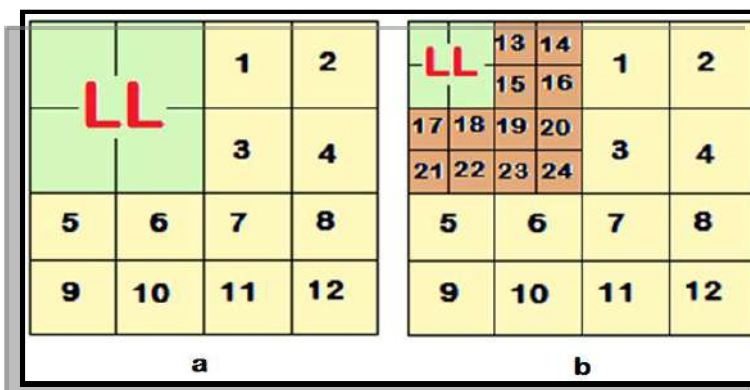


Fig.(6):Decomposition of Discrete Multiwavelet Transform:
(a) One level; (b) Tow levels

Step3: Apply Statistical measures for extract Features:

In this paper, we will computed statistical measures for for each sub image (L1L1,L2L1,H1L1,H2L1,L1L2,L2L2,H1L2,H2L2,L1H1,L2H1,H1H1,H2H1,L1H2,L2H2,H1H2,H2H2,LH1, HL1, HH1, LL2, HL2, LH2 and HH2 bands) are usually useful to represent characteristics or features of data; it is simple and requires less computation load.

Statistical measures adopted by:

a. Energy b. Entropy c. Standard Deviation d. Variance e. Mean

The result is a vector with (28) for energy values $E = (E1, E2, \dots, E28)$, (28) for entropy values $En = (En1, En2, \dots, En28)$, (28) for standard deviation values $ST = (ST1, ST2, \dots, ST28)$, (28) for variance values $V = (V1, V2, \dots, V28)$, and (28) for Mean values $M = (M1, M2, \dots, M28)$. Therefore will obtain (140) features for eye block.

Step4: Training Database Features (TRDBF)

The extracted features from multiwavelet coefficients by applied a set of simple measures are stored in database which is called (TRDBF). This database includes (5) attributes for features such as (Energy, Entropy, Standard deviation, Variance, Mean,)

Table (2) Result of Extracted Features for Some Sample of Eye Block Database (Before Normalization)

Class	Features					
	Sub-Image	Energy	Entropy	Standard deviation	Variance	Mean
C1	L1L1	16411.568	3.087813957	5796.45435	2.51992E+11	496264
	L2L1	18736.1788	3.061537848	6566.867519	3.23428E+11	562223
	H1L1	14367.966	2.639113038	5032.18496	1.89922E+11	430831
	H2L1	15850.55707	6.932309863	10712.03577	8.60608E+11	917112
	L1L2	16755.6576	3.091456802	5904.659562	2.61488E+11	505528
	L2L2	21320.31813	3.354804996	7472.116714	4.18744E+11	639726
	H1L2	13038.46867	2.352252421	4553.601157	1.55515E+11	389857
	H2L2	18266.20037	3.14686265	12746.84417	4.87446E+12	2195087
	L1H1	21193.99467	3.248849991	14738.60045	6.51679E+12	2538080
	L2H1	16178.59873	2.653851651	11217.40545	3.77491E+12	1931708
	H1H1	18872.8084	6.744231835	11774.03302	1.03971E+12	1008035
	H2H1	17394.31613	3.185350277	6129.958605	2.81823E+11	524817
	L1H2	21580.32213	3.399725618	7565.698338	4.29298E+11	647738
	L2H2	13493.06333	2.355156011	4705.490253	1.66062E+11	402861
	H1H2	8042.975333	1.825859549	2833.413936	60211759008	242583
	H2H2	9241.383333	1.800343612	3229.956139	78244624932	276533
	LH1	5354.5896	1.086654612	1861.424179	25986749820	159366
	HL1	15063.71027	6.545281314	10311.30038	7.97422E+11	882803
	HH1	14041.74747	2.59529715	4940.1568	1.83039E+11	422952
	LL2	14571.33427	2.744680606	5125.019051	1.96994E+11	438779
	LH2	10333.24213	1.86919829	3596.748915	97024520687	307936
	HL2	13816.28023	2.481215083	9625.379001	2.77944E+12	1657551
	HH2	14329.75567	2.637181773	9980.238239	2.98815E+12	1718660
	LH1	9987.999333	1.818135789	6909.340322	1.43217E+12	1189832
	HL1	19151.1496	6.498624726	11910.51596	1.06395E+12	1019720
	HH1	15654.89227	2.782001884	5513.326723	2.27976E+11	472024
	LL2	15706.93053	2.979210414	5538.006949	2.30021E+11	474137
	LH2	10498.5992	1.925073984	3657.298982	1.00319E+11	313120
	HL2	21127.0548	4.84227906	7834.727974	4.60372E+11	670771
	HH2	18903.22067	4.175987868	6906.947709	3.57794E+11	591339

Step5: Extracted Features after Normalization: Then apply normalization frequency on the data base where to obtain the following results.

Table (3) Result extracted features from sample Eye Block Database (After Normalization)

Class	Features					
	Sub-Image	Energy	Entropy	Standard deviation	Variance	Mean
C1	L1L1	0.3949	0.1606	0.122	0.0152	0.0495
	L2L1	0.667	0.1549	0.1977	0.0264	0.0802
	H1L1	0.1556	0.0626	0.047	0.0054	0.0191
	H2L1	0.3292	1	0.6047	0.1108	0.2454
	L1L2	0.4352	0.1614	0.1327	0.0167	0.0538
	L2L2	0.9696	0.2189	0.2866	0.0414	0.1163
	H1L2	0	0	0	0	0
	H2L2	0.9548	0.1958	1	1	1
	L1H1	0.3676	0.0659	0.6543	0.569	0.7177
	L2H1	0.683	0.9589	0.7089	0.139	0.2878
	H1H1	0.5099	0.1819	0.1548	0.0199	0.0628
	H2H1	1	0.2287	0.2957	0.043	0.12
	L1H2	0.0532	0.0006	0.0149	0.0017	0.0061
	L2H2	0.612	0.1735	0.8044	0.7418	0.8403
	H1H2	0.1949	0.1354	0.0967	0.0116	0.0534
	H2H2	0.2817	0.1307	0.1362	0.0176	0.0751
	LH1	0	0	0	0	0
	HL1	0.7037	1	0.8409	0.2604	0.464
	HH1	0.6297	0.2764	0.3064	0.053	0.169
	LL2	0.668	0.3037	0.3248	0.0577	0.1792
	LH2	0.3609	0.1434	0.1727	0.024	0.0953
	HL2	0.6133	0.2555	0.7726	0.9295	0.9608
	HH2	0.6505	0.2841	0.8079	1	1
	LH1	0.3358	0.134	0.5023	0.4747	0.6609
	HL1	1	0.9915	1	0.3504	0.5518
	HH1	0.1949	0.1354	0.0967	0.0116	0.0534
	LL2	0.2817	0.1307	0.1362	0.0176	0.0751
	LH2	0	0	0	0	0
	HL2	1	0.5227	0.3316	0.0483	0.1387
	HH2	0.7593	0.39	0.2479	0.0333	0.1037

Step6: Apply FP-growth: After get features will apply FP-growth algorithm where features encoding to find repetition and draw tree then find the rule.

Algorithm (1): Customized FP-Growth Algorithm

Input: A transactional database DB, minimum support threshold

Output: Its frequent pattern tree, tree structure

Process

Begin

The FP-tree is constructed in the following steps:

Scan the transaction database DB once. Collect the set of frequent items F and their supports. Sort F in support descending order as L, the list of frequent items;

Create the root of an FP-tree, T, and label it as "root";

While Trans in DB do begin:

Select and sort the frequent items in Trans according to the order of L;

Sorted frequent item list = [p | P], where p is the first element and P is the remaining list;

Call *insert tree function* ([p | P], T);

Call *FP-growth* (FP-tree, null). // The FP_tree is mined

End Process;

Insert tree function ([p | P], T):

Begin

If T has a child N such that (N.item-name = p.item-name) then

Increment N's count by 1;

Else

Create a new node N, and let its count be 1, its parent link be linked to T, and its node-link be linked to the nodes with the same item-name via the node-link structure;

```

End If;
If P is nonempty, call insert_tree (P, N) recursively;
End;
FP-growth function (FP-tree, null):
// Procedure FP-growth(Tree, A)
Begin
If Tree contains a single path P then
for each combination (denoted as B) of the nodes in the path P generate pattern B ∪ A with
support=minimum support of nodes in B
Else
for each ai in the header of the Tree do
{
Generate pattern B = ai ∪ A with support = ai.support;
Construct B's conditional pattern base by traverse the FP-tree by following the
link of each frequent item and accumulate all of transformed prefix paths of that item;
Construct B's conditional FP_tree (Tree B) by accumulate the count for each item
in the conditional pattern base >= minimum support;
If Tree B ≠ ∅ then
call FP-growth(Tree B, B);
End If;
}
End If;
End;

```

In this paper using FP-growth, where will encode the features to find the frequency and that the advantages of the algorithm is to reduce of scan and then will build the tree and then extract the rules for retrieval eye images person. The table (4) illustrates the data base after encoding and table (5) illustrate the frequency.

Table (4) Encoding database

Id Set (class)	Item_Set
C1	a,b,c,d,e
C2	e,b,e,d,e
C3	a,b,a,d,d
C4	a,e,d,e
C5	c,b,c,d,c
C6	d,b,d,d,e
C7	a,a,c,d,a
C8	a,b,c,d,e
C9	a,b,c,b
C10	a,b,d,e

Table (5) Frequency Item set (First step of FP-growth algorithm)

Item ID	Support Count
A	10
B	8
C	7
D	12
E	9

Then will build the tree and then extract the rules for retrieval eye images person. The table (6) illustrates rules (id) will used for retrieval eye images person.

Table (6) Result Association Rules Extracted database (FIAEDB) and their Confidence from sample eye images person

Class	Association Rules			
C1	Symbol	Equation	Relation	Confidence
	C26	A,C,/A,	0.1094/0.1094	A-->C
	C26	B,G,/B,	0.1094/0.1094	B-->G
	C26	C,D,/D,	0.1094/0.1094	D-->C
	C26	E,G,/E,	0.1094/0.1094	E-->G

Step7: Retrieval Phase: Retrieval operation where used the following critical retrieval image eye personal. The evaluating performance of face retrieval system is measured through how many face images for specific query are truly relevant to are a query. The retrieval efficiency is generally evaluated through two well- known metrics, precision and recall. The formula for calculating these measures are given as in equations (6) and (7) respectively.

1. Precision: is defined as the ratio between the numbers of retrieved images that are relevant to the number of retrieved images.

$$\text{Precision} = \frac{\text{No.Relevant Images Retrieved}}{\text{Total No.Images Retrieved}}, \dots \dots \dots (6)$$

2. Recall: is defined as the ratio between the numbers of retrieved images that are relevant to the total number of relevant images.

$$\text{Recall} = \frac{\text{No.Relevant Images Retrieved}}{\text{Total No.Images in the Collection}}, \dots \dots \dots (7)$$

9. The Results of Average Precision and Recall for Eye block

For the multiwavelet transform, Table (7) shows the averages of precision and recall values for (30x15).

Table (7) The Averages of Precision and Recall for Multiwavelet Transform

Wavelet	Average	
	Precision	Recall
	74%	49%

10. Dataset

The dataset that collected from 30 volunteers of different samples; 10 samples for each person, the images were taken under different lighting conditions, varied in expression, orientations, illumination, skin color, background, ages, and faces shapes (the mouth and eyes are open or closed, with or without glasses, male and female... etc), the face is in frontal position. The face images are 24 bit RGB, 300x400 pixels resolution of (BMP) format. For training purpose, training face image set which refers to a set of entire face image is extracted from the dataset to be used for extract association rules, the training set are used to generate training pattern set, five samples for each person is used. Test face image set, refers to a set of entire samples extracted from the dataset to be used for generate testing pattern set, ten samples for each person are used. Retrieval face image set, refers to a set of entire samples extracted from the dataset to be used for generate query pattern set; fifteen samples for each person are used for training, ten samples for each person are used for query. So, the total number of face samples in the dataset is 300 (30*15).





11. Conclusion

In this paper eye region detection operation achieved good result and the algorithm used give good results. Where using multiwavlete to extract the features give the best result in retrieval because there change in expression, noise and lighting. Applying Association FP growth in retrieval achieved good result because use multiwavlete from where extraction. The system proposed achieved good percentage (74%).

References

- [1] G. G., Beveridge J. R., Draper B. A., and Bolme D., "A Statistical Assessment of Subject Factors in the PCA Recognition of Human Faces", Colorado State University, 2003.
- [2] A. K. Jain, P. F. and A. A. Ross, "Handbook of Biometrics" springer, in 2007.
- [3] M. M., Misity Y., Oppenheim G., and Pogg J. M., "Wavelet Toolbox: Computation, Visualaization, and Programming", Useres guide, ver. 2, The MathWorks, 2002.
- [4] A. Graps, "An Introduction to Wavelets", IEEE Computational Science and Engineering, Vol. 2, No. 2, May 2004.
- [5] H. K. Ekenel and B.Sankur, "Multiresolution Face Recognition", Electrical and Electronic Engineering Department, Bog̃azic̃i University, Bebek, İstanbul, Turkey, Image and Vision Computing 23 (2005) 469–477.
- [6] S., V., Heller, P.N., S., G., Topiwala, P., and Heil, C., "The Application of Multiwavlet Filterbank to Image Processing", IEEE Transactions on Image Processing, Vol. 8, No. 4, pp. 548-563, April 1999.
- [7] P. G., and S. V., "From Wavelets to Multiwavelets ", Mathematical Methods for Curves and Surfaces, 1998, pp. 375-399.
- [8] A. W. S. Ibrahim, "Face Recognition Using Skin Color and Texture Features", Ph.D. Thesis, Department of Computer Sciences of the University of Technology, 2005.
- [9] Z. M. Hussain, "Development of a Face Recognition System Based on Canonical Correlation Analysis", Ph.D. Thesis, Informatics Institute for Postgraduate Studies at the Iraqi Commission for Computers and informatics, October 2006.
- [10] A. F. Mahdi, "Face Recognition System Based on Artificial Neural Networks", M.Sc Thesis, Informatics Institute for Postgraduate Studies at the Iraqi Commission for Computers and informatics, January 2012.
- [11] H. B. Jehlol, "Image Retrieval Using Association Rules", M.Sc Thesis, Informatics Institute for Postgraduate Studies at the Iraqi Commission for Computers and informatics, January 2013.
- [12] D. A. Alzubaydi, S. A.Yousif, "Hybrid Features Extraction based on Master Eye Block for Face Recognition", International Journal of Scientific & Engineering Research, Volume 5, Issue 12, December-2014.
- [13] S. M. Abood, "Proposed Mining Model for Online Social Network Analysis (Facebook,)", M.Sc. thesis, Department of Computer Sciences of the University of Technology, 2014.
- [14] T. M. Mitchell, "Machine Learning and Data Mining", Communications of the ACM, book, 1999.
- [15] M. H. Dunham, Xiao Y., Gruenwald L., and Hossain Z., "A Survey of the Association Rules", PDF, 2000.
- [16] I. H. Witten, E. Frank and M. A. Hall, "Data Mining Practical Machine Learning Tools and Techniques", Elsevier Inc, 2011.

- [17] R. Agrawal, T. Imielinski and A. Swami, "**Mining Association Rules Between Sets of Items in Large Database**", Washington, USA, May 1993.
- [18] F. Verhein, "**Frequent Pattern Growth (FP-Growth) Algorithm An Introduction**", School of Information Technologies, the University of Sydney, Australia, PDF, 2008.
- [19] Han J., Pei J., and Yin Y., "**Mining Frequent Patterns without Candidate Generation**", University of Illinois at Urbana-Champaign, PDF, 2000.
- [20] J. Han J. and Yin Y., "**Mining frequent patterns without candidate generation**", In Proc. of the ACM SIGMOD Conference on Management of data, PDF, 2000.
- [21] Mazman S., and Usluel Y., "**The Usage of Social Networks in Educational Context**", World Academy of Science, Engineering and Technology, PDF, 2009.
- [22] Agrawal R. and Srikant R., "**Fast Algorithms for Mining Association Rules in Large Databases**", Proceedings of the Twentieth International Conference on Very Large Databases, PDF, 1994.

الخوارزميات الجينية ومعايير الضبط المثلى للأداء المنفصل

جنان رضا مطر

الجامعة المستنصرية- كلية التربية - قسم علوم الحاسبات

jinan-redha@yahoo.com

المستخلص

الخوارزميات الجينية هي طرائق بحث وتحسين (تطوير) تعتمد على تقنية الانتقاء الطبيعي وعوامل التزاوج الجيني. اكتسبت الخوارزميات الجينية شعبية كبيرة بسبب سهولة وقوة تطبيقها على مدى واسع من المسائل المعقدة بدون الحاجة إلى معرفة مسبقة لهذه المسائل، وعلى الرغم من فوائد الخوارزمية الجينية فإنها تعاني من مساوئ منها: صعوبة تحديد معايير ضبط المثلى (Control Parameters) للخوارزمية ولهذه المشكلة تأثير على الكفاءة التقليدية.

من أجل تسريع البحث وتحسين كفاءة الخوارزمية الجينية يتم من خلال تحديد معايير الضبط المثلى للخوارزمية الجينية والتي يجب ان تضبط لصالح الكفاءة.

تم في هذا البحث تصميم خوارزمية جينية تبحث في المجال المعير بسبعة معايير لتحديد الخوارزميات الجينية الكفوة على مجموعة من مسائل التحسين العددية، وسميت هذه الخوارزمية بالخوارزمية الجينية مستوى فوق، إذ استطاعت هذه الخوارزمية المقترحة إيجاد خوارزميات جينية مثلى تتفوق على الخوارزميات الجينية المثلى السابقة بالنسبة للأداء المنفصل (Off-Line Performance). تم تدقيق النتائج (نتائج الطريقة المقترحة الجديدة والطرائق السابقة) على مجموعة أخرى من المسائل. أوضحت النتائج اقتدار وكفاءة الخوارزمية المقترحة مقارنة بالأعمال السابقة.

Genetic Algorithm and Optimal Control Parameters for Off-Line Performance

Abstract:

Genetic algorithms (GA's) are methods of research and optimization (development) based on natural selection technique and genetic crossover factors. GA's have gained popularity because of their ease and power over a wide range of complex problems without prior knowledge of these problems. In spite of the benefits of the GA's, it suffers from disadvantages: the difficulty of determining the optimal control parameters of the algorithm and this problem has an impact on traditional efficiency. In order to speed up and improve the GA performance is optimization of control parameters for GA's, which should be tuned for efficiency. This work describes experiments that search a parameterized space of GAs defined by seven control parameters in order to identify efficient GAs for the task of optimizing a set of numerical functions. Metalevel GA performs this search. The proposed genetic algorithm has enabled to found optimized genetic algorithm and exceeds over the previous genetic algorithm for the off-line performance only. These optimized algorithms represent a big statistically significant improvement over the expected off-line performance of the previous optimizing GA's. The results are validated (both the new proposed method & the previous methods) on another set of problems. The results showed the ability and the effectiveness of the proposed genetic algorithm as compared to the optimization rates of the previous GA's.

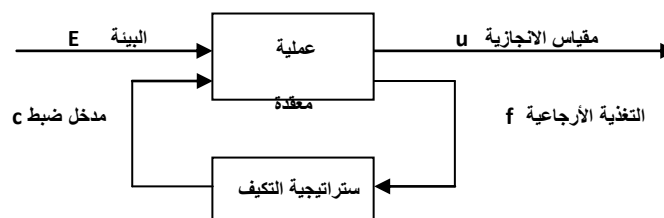
Keyword: Genetic Algorithm

1 - المقدمة

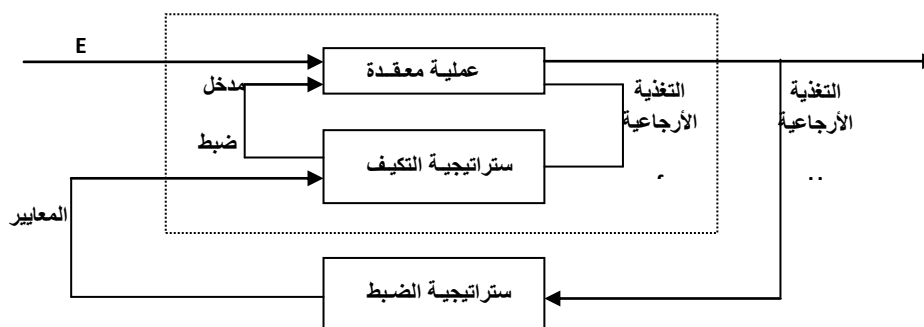
مسألة الضبط الديناميكي لعملية معقدة، غالباً ما تختزل إلى مسألة تحسين دالة عددية. إن بيئة كل مهمة تحدد سطح استجابة الأداء (performance response surface) والذي يجب أن يستطلع بصورة شاملة بواسطة تقنيات بحث مباشرة لغرض تحسين معايير الضبط ذات الأداء العالي (انظر الشكل رقم 1). عندما يكون سطح الاستجابة بسيطاً جداً تستعمل تقنيات الضبط أو التحسين اللاخطي التقليدية. لكن المهام الصعبة (مثل أنظمة التشغيل الحاسوبية) تتصف بصعوبة البحث عن سطح استجابة لها (مثلاً مدخل ضبط ذو أداء ضوضائي أو متقطع أو عالي الأبعاد)، في هذه الحالات قد تكون اختيارات تقنيات التحسين غير واضحة حتى عند توفر أصناف مناسبة من خوارزميات التحسين. هناك العديد من المعايير التي يجب ضبطها (مثل حجم الخطوة) في مختلف التقنيات القياسية وغالباً ما يكون لاختيار المعايير تأثيراً كبيراً على فعالية خوارزمية التحسين. أن معضلة ضبط معايير

الخوارزمية ابتدائيا تمثل معضلة ثانوية أو مستوى فوقي للتحسين (انظر الشكل رقم 2). والخوارزمية الجينية تستعمل عددا من المعايير لضبط بحثها التطوري لحل معضلاتها المعطاة بعض هذه المعايير تشمل معدل التزاوج، معدل الطفرة، العدد الأقصى للأجيال، عدد الأفراد في المجتمع ... وغيرها [5].

شكل (1) نظام نوع تكيفي ذو مستوى واحد



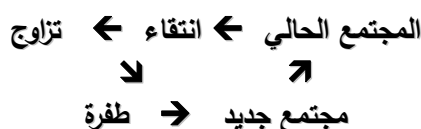
شكل (2) نظام نوع تكيفي ذو مستويين



يهدف هذا البحث إلى إيجاد معايير الضبط المثالية لصنف من طرائق التحسين العالمية تدعى بالخوارزميات الجينية التي تعمل لكل الحالات العامة باستعمال خوارزمية جينية مستوى فوقي. ويصف البحث التجارب التي تبحث المجال المعير بسبعة معايير للخوارزميات الجينية لكي تحدد خوارزميات جينية كفوة لمهام تحسين مجموعة من الدوال العددية عددها خمس دوال. الهدف هو البحث خلال فضاء من مدخلات الدالة (كل منها تمثل بخيط من الثنائيات) لإيجاد المدخل الأعلى (أو الأقل) حسب دالة الهدف المعطاة. الخوارزمية الجينية تبدأ بانتقاء مجتمع من الكروموسومات الممثلة بخيوط (Strings). الخوارزمية الجينية تستعمل خيوط المجتمع الحالي لخلق مجتمع جديد، الخيوط في المجتمع الجديد تكون ذو معدل افضل من تلك الموجودة في المجتمع الحالي (الانتقاء يعتمد على قيم الصلاحية).

ثلاث من العمليات توازي الموجود في الطبيعة تستعمل لغرض الانتقال من مجتمع واحد إلى آخر وهذه العمليات هي (الانتقاء selection والتزاوج mating or crossover والطفرة mutation) كما في الشكل (3):

شكل (3) الدورة الأساسية للخوارزمية الجينية



1) عملية الانتقاء (Selection): تحدد أي من الخيوط في المجتمع الحالي ستختار لخلق المجتمع الجيل التالي وهذا يتأتى من استعمال الانتقاء العشوائي بطريقة تضمن بان الخيوط الأفضل في المجتمع الحالي لها احتمال كبير في انتقاءها.

(2) **عملية التزاوج (Crossover):** تحدد الشكل الحقيقي للخيوط في الجيل التالي. اثنين من الأباء المختارين تتزاوج إذا كان طول كل خيط هو r ، يتم اختيار رقم عشوائي بين 2 و r يسمى s ثم نحدد الثنائيات التي تبدأ من 1 إلى $(s-1)$ من الأب الأول مع الثنائيات التي تبدأ من s إلى r من الأب الثاني ينتج خيط جديد واحد (طفل جديد) والعكس بالعكس بالنسبة للخيط الجديد الثاني.

(3) **احتمالية الطفرة (Mutation):** يتم وضعها في بداية الخوارزمية الجينية، احتمال تعرض الثنائيات في كل الخيوط الجديدة إلى التغير اعتمادا على هذه الاحتمالية.

واحدة من أكثر الدراسات المبكرة لمعايير ضبط الخوارزمية الجينية كانت لـ (De Jong) [3]، الذي أوجد صنف الخوارزميات الجينية لتحسين الدوال. تجارب De Jong أظهرت أن أفضل خوارزمية جينية لها معايير الضبط الموضحة في الجدول (1).

جدول (1) الخوارزمية الجينية المثلى لـ De Jong

حجم المجتمع (Pop. Size)	طريقة الانتقاء (Selection Strategy)	طريقة التزاوج (Crossover)	احتمالية التزاوج (Cross. Prob.)	احتمالية الطفرة (Mutation Prob.)	فجوة الجيل (Generation Gap)	نافذة التقييس (Scaling window)	استراتيجية النخبة (Elitism strategy)
50	عجلة الروليت (RW)	one point crossover	0.6	0.001	1.0	7	نعم

Grefenstette [5] رأى بأن مسألة ضبط معايير الضبط للخوارزمية الجينية ابتدائيا تعد مسألة تحسين ثانوية أو مسألة تحسين مستوى فوقي وكان أول من طبق طريقة الخوارزمية الجينية مستوى فوقي. نتائجه التجريبية أظهرت الخوارزمية الجينية (الفرد) الأعلى صلاحية نسبة لمقياس الأنجازية المنفصلة (off-line) هي الموضحة في الجدول (2).

جدول (2) الخوارزمية الجينية المثلى لـ Grefenstette نسبة لمقياس الانجازية المنفصلة (off-line)

حجم المجتمع (Pop. Size)	طريقة الانتقاء (Selection Strategy)	طريقة التزاوج (Crossover)	احتمالية التزاوج (Cross. Prob.)	احتمالية الطفرة (Mutation Prob.)	فجوة الجيل (Generation Gap)	نافذة التقييس (Scaling window)	استراتيجية النخبة (Elitism strategy)
80	عجلة الروليت (RW)	two point crossover	0.45	0.01	0.9	1	لا

نتائج (Grefenstette) أظهرت تحسن قليل (3%) ولكنه غير مهم إحصائيا لانجازية (off-line) نسبة إلى إعدادات (De Jong). بصورة عامة معايير السيطرة لـ (Grefenstette) كانت مقتصرة على طريقة انتقاء واحدة وهي انتقاء عجلة الروليت (Roulette wheel selection) وطريقتي تزاوج وهي عامل تزاوج المقطع الواحد (one point Crossover) وعامل تزاوج المقطعين (two point Crossover) فلذلك تعد هذه المعايير محددة في عدم استعماله باقي طرائق الانتقاء والعوامل الجينية الأخرى. سكافير، كاروانا، ايشلمان، داس [20] وسعوا من مجموعة الاختبار لـ (De Jong) و أنجزوا دراسة نظامية في تأثيرات معايير الضبط. حيث قضوا أكثر من سنة وقت معالجة (CPU time) مختبرين مدى واسع من تراكيب من المعايير. كانت انجازية (on-line) للخوارزمية الجينية لمجموعة من المعايير على عدد من مسائل الامثلية العددية تشمل دوال اختبار De Jong مع مسائل أخرى. بعد انقضاء فترة اختبارهم أوجدوا أفضل إعدادات (settings) لحجم المجتمع ومعدل التزاوج ومعدل الطفرة والتي تكون مستقلة عن المسائل في مجموعة اختبارهم. هذه الإعدادات مشابهة لإعدادات (Grefenstette): حجم المجتمع [20..30] ومعدل التزاوج [0.75..0.95] ومعدل الطفرة [0.005..0.01].

2 - التصميم التجريبي للخوارزمية الجينية المقترحة

نصف التجارب التي أجريناها لغرض تحسين أداء الخوارزميات الجينية على مجموعة من مسائل تحسين الدوال. قمنا بتصميم هذه التجارب للبحث في مجال الخوارزميات الجينية المعرفة بسبع معايير ضبط للخوارزميات الجينية ولتعريف أفضل إعدادات معايير بالنسبة لنوع من مقاييس الانجازية.

أن البحث عن الخوارزميات الجينية المثلى تم تنفيذه بواسطة الخوارزميات الجينية وهذا يوضح كفاءة وقدرة الخوارزميات الجينية كتنقيات تحسين ذات مستوى فوق.

2-1- مجال الخوارزمية الجينية المقترحة (the space of the proposed genetic algorithm)

هذا البحث مخصص لنوع فرعي محدد من الخوارزميات الجينية يتميز بسبع معايير وبالترتيب التالي:

1- **حجم المجتمع (population size) (N):** إن حجم المجتمع يؤثر على الأداء النهائي وكفاءة الخوارزمية الجينية. في تجارب البحث، حجم المجتمع يتغير في المدى [10..160] بزيادة [10] في كل مرة.

2- عدد الأجيال الأقصى (Maximum number of generation) (M-gen):

عدد الأجيال الأقصى لكل خوارزمية وبالإمكان استخدامها كمقياس توقف الخوارزمية الجينية. في تجارب البحث، يتغير هذا المعيار في المدى [50..360] وبزيادة [10] في كل مرة.

3- استراتيجية الانتقاء (Selection strategy) (S): يقارن البحث بين أربعة من طرائق الانتقاء:

S=3	S=2	S=1	S=0
انتقاء المجموعات الصدفية (طريقة كولديبرج)	انتقاء المجموعات الصدفية (طريقة وايتلي)	انتقاء الترتبة	انتقاء عجلة الروليت

وقد استعملت مع كل طرائق الانتقاء تلك استراتيجية النخبة (elitist strategy) الذي يشترط على الهيكلين ذو الأداء الأفضل البقاء على حالها إلى الجيل القادم، في غياب هكذا استراتيجية فإنه من الممكن لأفضل الهياكل أن تختفي بسبب أخطاء أخذ العينات أو التزاوج أو الطفرة [19]. في تجارب البحث، يتغير هذا المعيار في المدى [0..3] بزيادة [1] في كل مرة.

4- عامل التزاوج (Crossover Operator) (O): يقارن البحث بين أربعة أنواع من عوامل التزاوج:

O=3	O=2	O=1	O=0
خط بين تزاوج المقطعين والتزاوج المنتظم.	التزاوج المنتظم (uniform-crossover)	تزاوج المقطعين (two point- crossover)	تزاوج المقطع الواحد (one point -crossover)

في تجارب البحث، يتغير هذا المعيار في المدى [0..3] بزيادة [1] في كل مرة.

5- **معدل التزاوج (crossover rate) (C):** معدل التزاوج يسيطر على التكرار الذي بموجبه يطبق عامل التزاوج (crossover operator). كلما كان معدل التزاوج أعلى كلما ساعد في استكشاف فضاءات جديدة من الحلول وإيجادها في المجتمع بصورة أسرع [19]. أما إذا كان معدل التزاوج واطئاً جداً فإن البحث قد يختنق بسبب انخفاض معدل الاستكشاف. في تجارب البحث، يتغير هذا المعيار في المدى [0.4..1.0] بزيادة [0.04] في كل مرة.

6- **معدل الطفرة (Mutation rate) (M):** الطفرة هي عامل بحث ثانوي في عمله ولكنه مهم جداً، تزيد من التنوع في المجتمع. بعد الانتقاء فإن موقع كل ثنائية (بت) لكل فرد في المجتمع الجديد ينفذ تغير عشوائي باحتمالية تساوي معدل الطفرة (M) بالنتيجة تقريباً $(M*N*L)$ طفرة تحدث لكل جيل (L: طول الكروموسوم). إن الطفرة ذات المعدل الواطئ تؤدي إلى منع أي موقع معين (بت) من البقاء إلى الأبد مربوطاً إلى قيمة واحدة في عموم المجتمع [21]. الطفرة ذات المعدل العالي تنتج بحث عشوائي ويبدأ الناتج بفقدان ارتباطه مع الأصل ويكون عادة معدل الطفرة في المدى $0.001 \leq M \leq 0.005$. أما في تجارب البحث، يتغير هذا المعيار في المدى (0.005) إلى (0.2) بزيادة (0.013) في كل مرة.

7- احتمالية عامل التزاوج المنتظم (Uniform Probability) (UX-P)

يكون التزاوج بطريقة العامل المنتظم على مستوى الجينة الواحدة حيث يستنسخ الأبوين إلى طفلين ثم يتم المرور على جينات الطفلين وباحتمالية معينة (UX-P) يتم مبادلة قيمتي الجينتين. ويتراوح مدى هذا المعيار من (0.4) إلى (0.7) بزيادة (0.02) في كل مرة. ونشير إلى الخوارزمية الجينية بالإشارة إلى قيمها الخصوصية للمعايير (N, M-gen, S, O, C, M, UX-P). الناتج الديكارتي للمديات المشار إليها للمعايير السبعة (N, M-gen, S, O, C, M, UX-P). تحدد مجال 2^{25} خوارزمية جينية. من الممكن التخمين بكيفية تأثير تغير معيار واحد فقط على أداء الخوارزميات الجينية مع افتراض أن باقي المعايير ثابتة. ومع ذلك، فإن من الصعب التخمين بكيفية تفاعل المعايير المختلفة. مثلاً، ما هو تأثير زيادة حجم المجتمع بينما يتم تقليل معدل التزاوج؟ أن التحسين التحليلي لهذا المجال يقع خارج مدى فهمنا الحالي للخوارزميات الجينية. فأسلوبنا هو، تطبيق الخوارزميات الجينية مستوى فوق لمساائل تحديد الخوارزميات الجينية ذات الأداء العالي.

الخوارزمية الجينية مستوى فوق هي الخوارزمية الجينية نفسها لكن أفرادها عبارة عن معايير الضبط للمسألة المطلوب حلها، مثلاً المطلوب من بحثنا هذا هو إيجاد معايير الضبط المثلى للخوارزميات الجينية باستعمال خوارزمية جينية مستوى فوق، بمعنى أن كل فرد من أفراد مجتمع الخوارزمية الجينية مستوى فوق عبارة عن خوارزمية جينية خاصة. كل فرد في المجتمع للخوارزمية المقترحة مكون من متجه (vector) ذو 25 ثنائية التي عرفت خوارزمية جينية، أداء كل خوارزمية جينية قد قيس خلال أداء سلسلة من دوال التحسين (بيئة المهام Task Environment). الخوارزمية الجينية مستوى فوق تستعمل هذه المعلومات لارشاد البحث باتجاه الخوارزميات ذات الأداء العالي. إن الخوارزمية الجينية ذات المستوى الفوقي يمكنها أن تبحث بالمثل أي فضاء آخر ذو إجراءات تحسينية مُعَيَّرة.

2-2 بيئة المهام (Task Environment)

بالنسبة للخوارزمية الجينية مستوى فوق فإن كل فرد من أفراد مجتمعها هو عبارة عن خوارزمية جينية ولتقييم كل فرد (خوارزمية جينية) يتم من خلال استعماله لاداء مجموعة مهام امثلية (مجموعة دوال اختبار) مختارة بعناية. أن الدوال المكونة لبيئة المهام قد درست في الدراسات السابقة للخوارزميات الجينية والدوال المتضمنة ذات الخواص المختلفة من ضمنها الدوال الضجيجية ذات الأبعاد المتعددة والغير المستمرة (جدول 3 يعطي وصف مختصر لدوال الاختبار). وتبعاً لهذه المهام ينسب إلى الفرد (الخوارزمية الجينية) قيمة صلاحية تبعاً لإحدى مقاييس الانجازية الموضحة في أدناه [5].

جدول (3) يوضح مجموعة من دوال الاختبار

Fun.	Dim	Description
F1	3	Sphere function
F2	2	Rosenbrock's valley
F3	5	Step function
F4	30	Stochastic Function
F5	2	Shekel's foxholes

2-3 مقاييس الانجازية (Performance Measures)

في هذا البحث تم استعمال احد مقاييس الانجازية لاستراتيجية البحث المكيف أخذت بنظر الاعتبار، الانجازية المنفصلة (off-line Performance) [3] [4] [5].

• الانجازية المنفصلة (Off-Line Performance)

الأنجازية المنفصلة لاستراتيجية البحث (s) على سطح الاستجابة (e) تعرف كما يلي:

$$U_e^*(s, T) = ave_t(u_e^*(t)) \quad , \quad t = 0, 1, \dots, T \quad \dots (1)$$

إذ أن $U_e^*(t)$ هي افضل انجازية في الفترة $[0, t]$. الأداء المنفصل هو متوسط أداء افضل هياكل الاختبار خلال دورة البحث.

أي أن $\max_i$ = الصلاحية الأفضل في الجيل i،

$$U_e^*(s, T) = \sum_{i=0}^t \max_i / (t + 1) \quad U_e^*(s, T)$$

أثناء تطور الخوارزمية الجينية تتقارب $U_e^*(s, T)$ اتجاه قيمة ثابتة وعند ثبوتها لعدد كاف من تقديرات الصلاحيات فإننا نوقف محاكاة الخوارزمية الجينية، وتعد (E) التي توقفت عندها الخوارزمية الجينية هي مقياس أداء الخوارزمية للمسالة. ولقياس الرزانة العالمية تعرف المقاييس لكل سطوح الاستجابة: للأجارية المنفصلة

$$U_E^*(s, T) = ave_e(U_e^*(s, T)) \quad , \quad e \text{ in } E \quad \dots (2)$$

اذ ان $U_E^*(s, T)$ مقياس أداء الخوارزمية الجينية لمجموعة من المسائل والمستعمل لتقييم الخوارزمية الجينية بالنسبة للأجارية المنفصلة. 4-2- الإجراءات التجريبية (Experimental Procedures):

تم إجراء تجربتين لتحسين الأداء المنفصل و لكل تجربة كان لها إجراءاتها الخاصة للحصول على خوارزمية جينية مثالية وكما يلي:

- تجارب الأداء المنفصل (off-line Experiments):

1- تطبيق الخوارزمية الجينية المثلى لـ دي جونج ولتكن (DGA) الموضحة في الجدول (1) على الطريقة المقترحة كالآتي:

أ. قيمت (1000) خوارزمية جينية باستعمال الخوارزمية الجينية المقترحة لتتجز بحث خلال فضاء من الخوارزميات الجينية المعرفة بسبعة معايير ضبط للخوارزمية الجينية ويشتمل تقييم كل خوارزمية جينية بتنفيذها على كل دالة من دوال الاختبار الخمسة (بيئة المهام) أي (5000) تقييم دالة.

2- تطبيق الخوارزمية الجينية المثلى لـ Grefenstette لتكن (GGA1) للأداء المنفصل الموضحة في الجدول (2) على الطريقة المقترحة كالآتي:

أ. قيمت (1600) خوارزمية جينية باستعمال الخوارزمية الجينية المقترحة لتتجز بحث خلال فضاء من الخوارزميات الجينية المعرفة بسبعة معايير ضبط للخوارزمية الجينية ويشتمل تقييم كل خوارزمية جينية بتنفيذها على كل دالة من دوال الاختبار الخمسة (بيئة المهام) أي (8000) تقييم دالة.

بالنسبة لـ (1) و (2)، أن أداء كل خوارزمية جينية خلال محاولة مفردة على كل مسألة من مسائل الاختبار الخمسة يمثل نموذج من توزيع الاداءات. لذلك تؤخذ مجموعة من الخوارزميات الجينية التي أظهرت افضل أداء خلال الخطوة (أ) وتخضع إلى اختبارات أوسع وكل خوارزمية جينية من الـ (20) خوارزمية جينية الأفضل في الخطوة (أ) تنفذ مرة أخرى مقابل بيئة المهام لكن هذه المرة (10) محاولات لكل دالة اختبار والخوارزمية الجينية التي تُظهر افضل أداء في هذه الخطوة تعد الفائزة لتلك التجربة.

3- نتائج التجربة

تم تصميم التجربة للبحث عن الخوارزمية الجينية المثلى للأداء المنفصل على بيئة المهام (E).

أولاً: في حال استعمال خوارزمية De Jong (DGA) كمعايير ضبط للخوارزمية الجينية مستوى فوق المقترحة فكانت النتيجة الحصول على خوارزمية جينية مثلى نسبة إلى الأداء المنفصل لتكن (GA3) تتفوق على أداء (DGA). والجدول (4) يوضح الخوارزمية الجينية المثلى (GA3).

جدول (4) الخوارزمية الجينية المثلى (GA3) لتجربة الأداء المنفصل وباستعمال خوارزمية (DGA)

معايير ضبط للخوارزمية المقترحة

حجم المجتمع	العدد الأقصى للأجيال	طريقة الانتقاء	طريقة التزاوج	إحتمالية التزاوج	إحتمالية الطفرة
120	350	عجلة الروليت	Two point crossover	0.96	0.005

وفي مقارنة مطولة أظهرت الخوارزمية (GA3) تحسناً بنسبة (0.1547) أعلى من خوارزمية (DGA) (1000) تنفيذ لكل خوارزمية على بيئة المهام (E). كذلك في مقارنة مطولة أظهرت الخوارزمية (GA3) تحسناً بنسبة (0.1203) أعلى من الخوارزمية (GGA1) (1000) تنفيذ لكل خوارزمية على بيئة المهام (E).

أن تحسن الأداء فيما بين (GA3) و (DGA) وبين (GA3) و (GGA1) يمكن أن يعزى إلى تفاعل عدد من العوامل:

1. حجم المجتمع الكبير يعني أن المجتمع يحوي على الأغلب عدد كبير من نماذج التماثل، وبالنتيجة فإن المجتمع الكبير يحبط التقارب المبكر للحلول غير المثالية مع معدل طفرة واطئ والذي يؤدي دور مهم في إنعاش القيم المفقودة ومنع أي موقع معين (ثنائية) من البقاء إلى الأبد مربوطاً إلى قيمة واحدة في عموم المجتمع ويميل معدل التزاوج العالي إلى إخلال في الهياكل (الأفراد) المختارة للتكاثر بمعدل عالي مما يؤدي إلى ازدياد في معدل الاستكشاف.
 2. استعمالها لطريقة انتقاء عجلة الروليت.
 3. واستعمالها لطريقة تزاوج المقطعين.
- ثانياً: في حال استعمال خوارزمية Grefenstette (GGA1) كمعايير ضبط للخوارزمية الجينية مستوى فوقي المقترحة فكانت النتيجة الحصول على خوارزمية جينية مثلى نسبة إلى الأداء المنفصل لتكن (GA4) تتفوق على أداء (GGA1). والجدول (5) يوضح الخوارزمية الجينية (GA4).

جدول (5) الخوارزمية الجينية المثلى (GA4) لتجربة الأداء المنفصل وباستعمال خوارزمية (GGA1)

معايير ضبط للخوارزمية المقترحة

حجم المجتمع	العدد الأقصى للأجيال	طريقة الانتقاء	طريقة التزاوج	إحتمالية التزاوج	إحتمالية الطفرة
140	360	وايتلي	2X	1.00	0.005

وفي مقارنة مطولة أظهرت الخوارزمية (GA4) تحسناً بنسبة (0.1195) أعلى من الخوارزمية (GGA1) (1000) تنفيذه لكل خوارزمية على بيئة المهام ((E)). كذلك في مقارنة مطولة أظهرت الخوارزمية (GA4) تحسناً بنسبة (0.1539) أعلى من الخوارزمية (DGA) (1000) تنفيذه لكل خوارزمية على بيئة المهام ((E)).

أن تحسن الأداء فيما بين (GA4) و (DGA) وبين (GA4) و (GGA1) يمكن أن يعزى إلى تفاعل عدد من العوامل وهي نفس العوامل المذكورة في أولاً فيما عدا استعمالها لطريقة انتقاء المجموعات الثنائية (طريقة وايتلي). الخوارزميات الجينية المثلى التي تم الحصول عليها من تجارب الأداء المنفصل، (GA3) و (GA4) تمثلان تحسن كبير ومهم إحصائياً نسبة إلى الأداء المنفصل للخوارزميات الجينية المثلى السابقة، (DGA) و (GGA1).

4- مسائل لتثبيت صحة النتائج

أخذنا مجموعة من الدوال بغية تثبيت صحة نتائجنا وتتميز هذه الدوال بأنها (Scalable) أي أن متغيرات هذه الدوال متحركة وقابلة للتسلسل أي بالإمكان زيادة عدد متغيرات الدالة، أداء كل دالة من هذه الدوال هو أداء تصغير (Minimized performance) [15]. هذه المجموعة من الدوال متضمنة دوال ذات خواص مختلفة، من ضمنها دوال ذات أبعاد متعددة والمستمرة وغير المستمرة والمحدبة وغير المحدبة والجدول (6) يعطي وصف مختصر لمجموعة من دوال التثبيت.

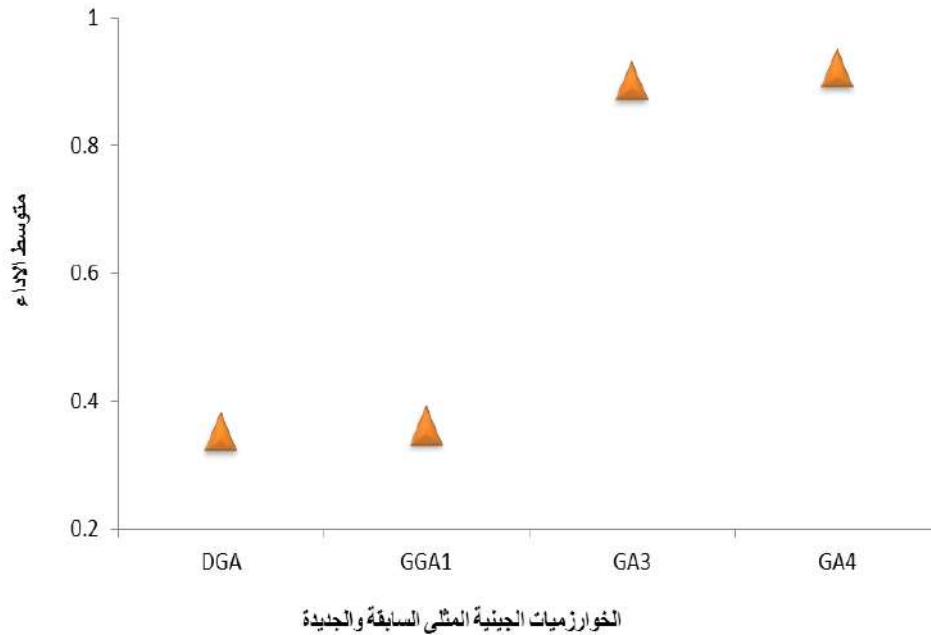
جدول (6) يوضح مجموعة من دوال التثبيت

Fun.	Dim	Description
F6	7	Rastrigin's function 6
F7	5	Rotated hyper-ellipsoid
F8	5	Schwefel's function 7

أرشدتنا التجارب إلى المقارنة بين الخوارزميات الجينية المثلى السابقة والجديدة نسبة إلى أداءها المنفصل وكل تجربة تتألف من تنفيذ كل خوارزمية جينية مثلى نسبة إلى أداءها المنفصل (10000) تنفيذه على كل مسألة (دالة) من المسائل أعلاه وعند التطبيق كانت النتائج الآتية:

1. Rastrigin's function 6 (F6):

- الأداء المنفصل (off-line performance): تنفيذ الخوارزميات الجينية المثلى السابقة والجديدة (نتيجة الطريقة المقترحة) ذات الأداء المنفصل على هذه الدالة. والشكل (4) يقارن بين متوسطات الأداء المنفصل للخوارزميات DGA و GGA1 و GA3 و GA4 على هذه الدالة.



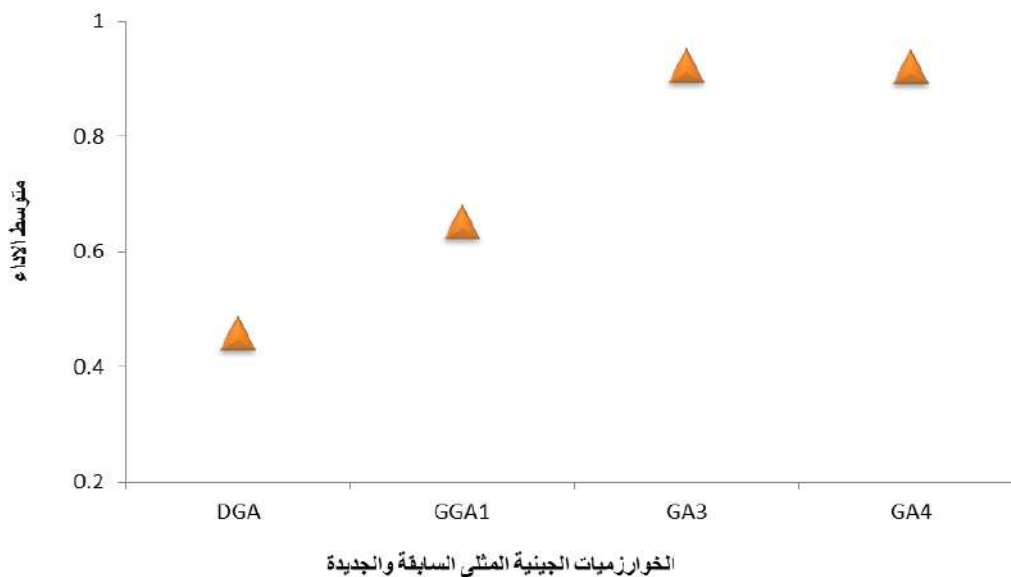
شكل (4) الأداء المنفصل للخوارزميات الجينية المثلى السابقة والجديدة على دالة (7) Rastrigin's Function

2. (F7) Rotated hyper-ellipsoid:

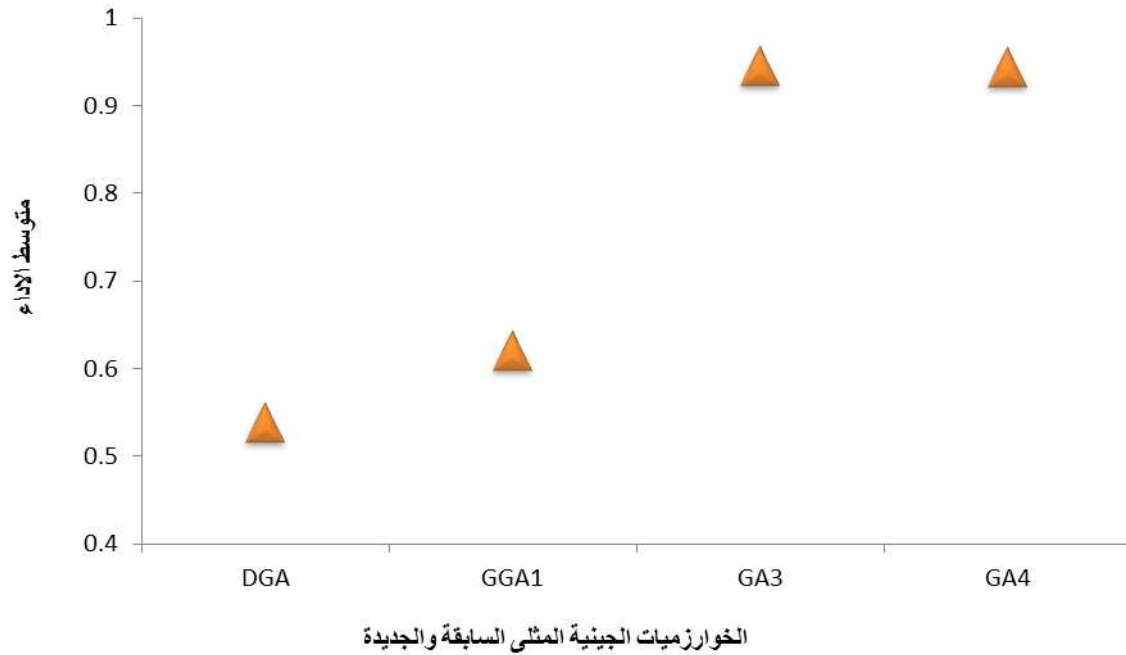
• الأداء المنفصل (off-line performance): تنفيذ الخوارزميات الجينية المثلى السابقة والجديدة (نتيجة الطريقة المقترحة) ذات الأداء المنفصل على هذه الدالة. والشكل (5) يقارن بين متوسطات الأداء المنفصل للخوارزميات DGA و GGA1 و GA3 و GA4 على هذه الدالة.

3. (F8) Schwefel's function 7:

• الأداء المنفصل (off-line performance): تنفيذ الخوارزميات الجينية المثلى السابقة والجديدة (نتيجة الطريقة المقترحة) ذات الأداء المنفصل على هذه الدالة. والشكل (6) يقارن بين متوسطات الأداء المنفصل للخوارزميات DGA و GGA1 و GA3 و GA4 على هذه الدالة.



شكل (5) الأداء المنفصل للخوارزميات الجينية المثلى السابقة والجديدة على دالة (Rotated hyper-ellipsoid function)



شكل (6) الأداء المنفصل للخوارزميات الجينية المثلى السابقة والجديدة على دالة

5- مناقشة Discussion

1. كما تم توضيحه في بداية الفقرة (4) بان من مزايا هذه المسائل هي دوال قابلة للتسلق (Scalable) أي بالإمكان تغيير (زيادة أو نقصان) في عدد متغيرات الدالة، وعندما يكون عدد متغيرات الدالة قليل (أقل من n متغير المحدد لكل دالة في أعلاه) فإنه لا يوجد فرق ملحوظ بين نتائج الخوارزميات الجينية المثلى السابقة والجديدة بمعنى آخر جميعها بنفس الجودة في الوصول إلى الحلول المثلى، لكن في حالة ازدياد عدد متغيرات الدالة (n متغير فأكثر) ليس بإمكان الخوارزميات الجينية المثلى السابقة الوصول إلى الحل الأمثل، أما بالنسبة للخوارزميات الجينية المثلى الجديدة لها القدرة في الوصول إلى الحل الأمثل كلما ازداد عدد متغيرات الدالة مما يؤكد رصانة الخوارزميات الجينية المثلى الجديدة وهي افضل جودة من الخوارزميات الجينية المثلى السابقة بالنسبة للأداء المنفصل.
2. الأشكال (4) و (5) و (6) تقارن بين متوسطات الأداء المنفصل للخوارزميات الجينية المثلى السابقة والجديدة (نتائج الخوارزمية المقترحة) للمسائل الثلاث، والأشكال توضح مدى التحسن الكبير بين الخوارزميات الجينية المثلى السابقة والحالية. وهذه النتائج تتفق مع النتائج الواردة في التجربة (1) الموضحة في الفقرة (3) من هذا البحث، وتشير هذه النتائج بأنها قد تكون قابلة للتطبيق على مسائل تحسين أخرى.

6- الاستنتاجات ومقترحات لأعمال مستقبلية

1. اثبت هذا البحث اقتدار الخوارزمية الجينية المقترحة في ضبط معايير الضبط للخوارزميات الجينية نسبة إلى مقياس الانجازية المنفصل.
2. لقد لاحظنا من خلال نتائج تطبيق الخوارزميات الجينية المثلى السابقة والجديدة (نتيجة الطريقة المقترحة) بالنسبة للأداء المنفصل على دوال (مسائل) أخرى غير مشمولة في بيئة المهام (مسائل قابلة للتسلق) بأنه لا يوجد فرق ملحوظ بينهما من حيث العثور على الحلول المثلى عندما يكون عدد متغيرات الدالة قليل (أقل من حد معين)، لكن وصول الخوارزميات الجينية المثلى السابقة إلى الحل الأمثل يكون معدوم مقارنة مع الخوارزميات الجينية المثلى الجديدة التي لها قدرة الوصول إلى الحل الأمثل عند زيادة عدد متغيرات الدالة عن حد معين مما يؤكد رصانة الخوارزميات الجينية المثلى الجديدة في وصولها إلى الحلول المثلى افضل من الخوارزميات الجينية المثلى السابقة.
3. من خلال النتائج نلاحظ بان جميع الخوارزميات الجينية المثلى الجديدة لها معدل طفرة قليل (0.005)، وهو ما يؤدي بان معدل الطفرة الواطئ يؤدي دور مهم في إنعاش القيم المفقودة ومنع أي موقع معين (ثنائية) من البقاء إلى الأبد مربوطا إلى قيمة واحدة في عموم المجتمع.
4. استطاعت الخوارزمية الجينية المقترحة إيجاد خوارزميات جينية مثلى تتفوق على الخوارزمية الجينية المثلى لـ دي جونج بالنسبة للأداء المنفصل (off-line) وهذه الخوارزميات المثلى أظهرت تحسن كبير ومهم إحصائيا نسبة إلى خوارزمية دي جونج، في حين الخوارزمية الجينية المقترحة لـ جرفنستيب لم تتوصل إلى ذلك.

5. لقد لاحظنا من النتائج عند تطبيق الخوارزميات الجينية المثلى لـ جرفنستيت (GGA) للأداء المنفصل كمعايير ضبط للخوارزمية المقترحة كانت ذي تقييم أعلى بقليل من نتائج تطبيق الخوارزمية الجينية المثلى لـ De Jong (DGA) للأداء المنفصل كمعايير ضبط للخوارزمية المقترحة ومن خلال هذا الفارق القليل الذي يعطي إثبات بان طريقة العمل صحيحة وكما هو مذكور في الفقرة (1) بأنه يوجد تحسن طفيف للخوارزميات الجينية المثلى لـ جرفنستيت للأداء المنفصل عن الخوارزمية الجينية المثلى لـ De Jong للأداء المنفصل.
6. حجم المجتمع الكبير يعني أن المجتمع يحوي على الأغلب عدد كبير من نماذج التماثل، وبالنتيجة فإن المجتمع الكبير يحبط التقارب المبكر للحلول غير المثالية.
7. طريقة الانتقاء وإبتي هي طريقة الانتقاء الأفضل والتي أعطت نتائج أفضل من تلك التي أعطتها طريقة انتقاء عجلة الروليت والطريقتان أفضل من طريقة انتقاء كولديبرج وطريقة انتقاء الرتبة.
8. عامل تزواج المقطعين هو عامل التزاوج الأفضل والذي أعطى نتائج أفضل من عامل تزواج المقطع الواحد والعاملين أفضل من عامل التزاوج المنتظم.

نتيجة للنتائج والإمكانيات التي تمتعت بها الخوارزمية الجينية نقترح:-

1. دراسة تأثير إضافة عوامل أخرى للطريقة المقترحة على أداء الخوارزمية الجينية: مثل عامل الزحام (crowding factor) واستراتيجيات انتقاء وعوامل تزواج أخرى مثل (Boltzmann select) و (multipoint crossover).
2. تطبيق الطريقة المقترحة نفسها في تحديد معايير الضبط للخوارزمية الجينية ولكن بدلا من استعمال مجموعة من المسائل العددية في تقييم الخوارزمية الجينية تُضمّن الشبكات العصبية للقيام بعملية التقييم وذلك لتقليل الوقت الحسابي.
3. للتمكين من الوصول أو التقارب إلى الامثلية تستعمل خطة الطفرة التكيفية في الخوارزميات الجينية، أي تعميم استعمال الطفرة التكيفية في الخوارزميات الجينية.

المصادر

- [1] Biesbroek R. (2000). "Genetic Algorithm Tutorial Home Page ", E-mail: Robin.Biesbroek@jaqar.demon.nl.
- [2] Dawn, T.,(1995). "Nature Shows the Way to Discover Better Answers". Scientific Computing World 6 (1995), 23-27.
- [3] De Jong, K.A.,(1975). "Analysis of the Behavior of a Class of Genetic Adaptive Systems". Ph.D. thesis, Dept. Computer and Communication Sciences, Univ. of Michigan, 1975.
- [4] Goldberg D.E. (1989), "Genetic Algorithms in Search, Optimization & Machine Learning". Reading: Addison-Wesley, 1989.
- [5] Grefenstette, J. (1986). "Optimization of control parameters for genetic algorithms". IEEE Transactions on Systems, Man, & Cybernetics 16(1): 122-128.
- [6] Heitkoetter, J. and D. Beasley, **The Hitch-Hiker's Guide to Evolutionary Computation: A List of Frequently Asked Questions (FAQ)**. USENET: comp.ai.genetic. Available via anonymous FTP from "ftp://rtfm.mit.edu/pub/usenet/news.answers/ai-faq/genetic/", 1994.
- [7] Hue, X. (1997). "Genetic Algorithm Algorithms for Optimization Background & Applications", Edinburgh Parallel Computing Center, The University of Edinburgh. Available from <http://www.epce.ed.uk/Epce-tec/documents>.
- [8] Kadim A.M. (2000). "Effects of Selection schemes & Scaling strategies on the Performance of genetic algorithms". M.Sc. thesis, Univ. of Al-nahreen, December 2000.
- [9] Li C., Licheng j (1998). "Hybrid Genetic Algorithm and its modification". International Conference on Neural Networks and Brain proceeding (ICNN & B'98), pp 278-281
- [10] Luger G.F., Stubblefield W.A. (1998). "Artificial Intelligence Structures and Strategies for Complex Problems". Third Edition, Addisonn Wesley Longman.
- [11] Maričić B. (1991). "Current Trends in Neural Network Design Tools Research ". EC-Newsletter, Vol.3, No. 1, pp 37-45.
- [12] Michalewicz, Z. (1996). "Genetic Algorithm Algorithms + Data Structures = Evolution Programs", third revised & extended edition, Springer - Verlag, Berlin.

- [13] Mitchell M. (1996). "**An introduction to Genetic Algorithms**".Abradford book.
- [14]Patterson D. W. (1996)."**Artificial Neural Networks Theory And Application**", Prentice Hall.
- [15] Quagliarella D., Vicini A. (1997).Genetic Algorithms and Evolution Strategy in Engineering and Computer Science,"Coupling Genetic Algorithms and Gradient Based Optimization Techniques",Johen Wiley & Sons.
- [16] Rzempoluck E.J. (1998). "**Neural Network Data Analysis Using Simulant**",Springer-Verlag.
- [17] Schmidt M., Stidsen T. (1997)."**Hybrid Systems: Genetic Algorithms, Neural Networks and Fuzzy Logic**", DAIMIIR.
- [18] Tang,S.K.& Man, F. k. and Kwony, S(1996) "**Genetic Algorithms Concepts & Applications**",IEEE Transactions on Industrial Electronics. VOL.43.NO.5.
- [19] Thomas Weise,Second Edition (2009), "**Global Optimization Algorithms – Theory and Application –**"
- [20] Vincent A. Cicirello & Stephen F. Smith (2000), "**Modeling Genetic Algorithm Performance for Control Parameter Optimization**", Robotics Institute, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, vincent+@cs.cmu.edu.

[21] أ. بحبوح - ح. ريشة (2007)، "تأثير متغيرات الخوارزميات الجينية في مسائل إيجاد الحل الأمثل" مجلة جامعة دمشق للعلوم

الهندسية-المجلد 23-العدد 2

Braille character recognition using Modify Bidirectional Associative Memory (MBAM)

Assist. Prof. Safana H. Abbas

Computer Science Dept., Education collage, Mustansiriyah University

safanahyder@yahoo.com

Abstract:

Braille is a very important communication code for blind people. In this paper, the Modified Bidirectional Associative Memory (MBAM) algorithm is used to recognize a single side Braille English document. The work is consisting of two stages: The preprocessing stage and the recognition stage. The implemented algorithm achieved average accuracy for correct letters was 91.87%, average accuracy for correct words was 51.26% and the processing time about 3.4 sec for each page.

Key words: Braille, Optical character recognition, Associative Memory.

1- Introduction:

Braille system is invented by Louis braille in 1821; this system is used by blind persons to help them in reading and writing through touch. A word is consisting of raised spots coordinated in a cell which represents a natural text in braille code. Six dots represent the single cell and arranged in 3 x 2 for each alphabet or numeral [9], as shown in Figure(1). The locations of the six dots are representing 64 various braille characters. The braille code is written using a specialized machine [2]. Braille Character Recognition (BCR) is a mechanism to recognize Braille document and saved as an image, such as jpg, tiff, etc and convert it into normal ASCII text. [4].

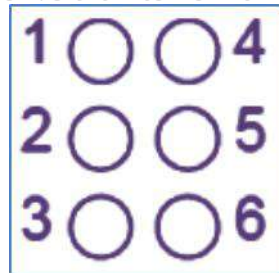


Fig. (1): Braille cell

A cell is a group of dots that consisting of at least one raised dot and a maximum of six, on Braille sheet, as shown in Figure (2). The dots are created by using a special printer or a manual machine that embosses the dots. Today, braille printers are available and used by connecting them to computers, these are generally known as Braille Embossers.

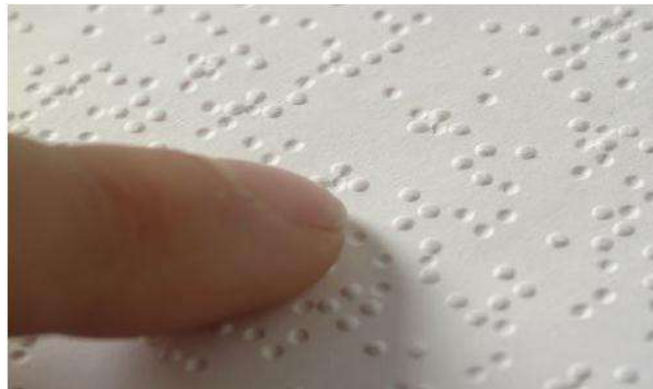


Fig. (2): Braille sheet [5].

Grade1 Braille and grade2 Braille are the two main types of alphabet Braille. Letters, numbers and punctuation, are represented basically by Grade1 Braille [4,3]. It is a direct replacement of the Braille English alphabet to normal print letters. Now because Braille books are so much larger than print ones, large contractions have been introduced to make them smaller and faster to read. Grade 2 is used for this purpose. It makes use of more than 300 contractions (in addition to the normal alphabet.). For example, the word **for** represented by only one letter in grade2 while in grade1 it takes three letters which is the number of the word letters as shown in table (1). This is much faster and easier for everyone to enjoy a Braille book.

Table (1): Example of Grade 1 and Grade 2 Simplification [4, 6, 3 and5].

The word	Grade 1	Grade 2
For		
Question		

2- Literature Review:

This section contains a review of the literature correlated to Braille character recognition, with a development that improves Braille character recognition.

Shreekanth.T, V. Udayashankara in 2014 [10] This paper presents a new algorithmic approach to recognize a Braille document with double side. The suggested method depends on the variation in the gray level values of the Braille image. It consists of two main duties, first is to realize the p Braille dots that are printed and the second is to differentiate these dots as recto and verso dots. This is implemented by few processes such as, center detection, thresholding, placement of designed mask on the center detected dots and differentiating recto dots from verso dots. Dots from Braille document can be separated into recto and verso dots with a single scan and with the average processing time of 5.6 seconds. The experiments are implemented on the developed database and obtained an excellent recognition rate of 99%.

Abdul Malik Al-Salman, and etc. in 2014 [1] they proposed a new techniques to realize braille documents by using a standard scanner. The suggested system has been tested with a different Braille documents, single and double side, that are written in Arabic language. The ratio of the correctly realized dots was 99%, with double and single-side documents.

zainb. Authman, Zamen F. Jebr in 2013 [12], they proposed an automatic system to recognize printed Braille cells. Adaptive and local thresholds have been used. Shrinking technique is combined to the system This proposed system was efficient and it takes seventeen seconds to realize green braille sheets and twenty one seconds to realize yellow braille sheet.

S. Padmavathi, and etc. in 2013 [11], they proposed a technique to transform a scanned braille sheet into a text. The braille cells in each image are partitioned and the dots for each cell is extracted and transformed in to a suitable language alphabets. The text is converted to a voice signal. Each braille cell has representations that are standard but the translation is different for each language. In this paper, accuracy of text conversion 97.8% -100%. For English, Hindi and Tamil are considered.

Mohammed Y. Hassan, Ahmed G. Mohammed in 2011 [6]. They proposed using the feed forward artificial neural network (ANN) to transform English characters into grade1 braille code. The ANN is designed with reduced structure like the layers number, and nodes number for each layer. Input patterns with noise were implemented to the NN by adding of STD 0.2 noise to the characters, so one or two characters were wrongly detected when each time running the program. A sequence of characters with and without noise were tested using the designed NN and the results were very accurate.

3- Modified Bidirectional Associative Memory (MBAM) [7, 8]:

The Bidirectional associative memory (BAM) network size (network neurons number) is depending on the length of the pattern used by the network that's mean a pattern with length eight needs size

of eight for BAM network. Since MBAM is an improved BAM NN, then it follows the same property of size. "According to the first principle, the pattern will be divided into a number of vectors with length two; this means that the size of the network will be fixed "as shown in figure (3). Therefore, parts of the pattern the network will be deled with instead of the whole pattern as one vector. This results to an advantage of dealing with the reduced network size no matter how long the pattern is.

The modified structure allows the prospect of not to learn the same vectors "(which represents a certain part of the pattern)" many times. This configuration fulfills the second concept illustrated before. A bipolar pattern representation for the inputs were selected, where the elements will be (1 or -1).

Anywise, just like the ordinary BAM NN, every neuron is linked to each other neuron" but not to itself "as shown in figure (3). Weight of each vector in the pattern is represented by connections in the network. Although the predictable number of vectors is equal to the number of links and it is only four that helps to deal with the smallest network size no matter how long the pattern is. Technically, this modified network has two stages, learning and convergence phases as with the original BAM.

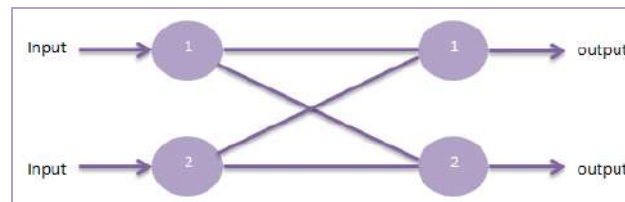


Fig. (3). The Modified bidirectional associative memory (MBAM).

The MBAM algorithm is shown below in algorithm (1) where (a) is the learning phase and (b) the convergence phase.

Algorithm (1) MBAM

(a) The learning stage

Algorithm MBAM for learning phase
Input: training patterns p with code c , n .
Output: lookup table for all n corresponding stored patterns.
Process:
Step1: Repeat steps 1.1 and 1.2 to the end of training pattern p with code c :
Step 1.1: Divide the training pattern p to n vectors v with length two.
Step 1.2: For each vector v , repeat steps 1.2.1, 1.2.2 and 1.2.3:
Step 1.2.1: Assign the weight for each n vectors v , weights matrix w as follows:
$w_i = v_i * c$
Where: c is code
Step 1.2.2: Assign the stored vector weight svw as follows:
$svw = f(\text{Decode}(v)) \begin{cases} 0 & \{\text{means } w0\} \\ 1 & \{\text{means } w1\} \\ 2 & \{\text{means } w2\} \\ 3 & \{\text{means } w3\} \end{cases}$
Where: Decode is a function to convert the binary number to decimal number.
Step 1.2.3: Save svw for this vector in the lookup table .
Step 2: End.

(b) The convergence stage

The convergence code algorithm for the traditional convergence
Input: n of unknown patterns p and lookup table.
Output: Convergence code c .
Process:
Step 1: Repeat steps 1.1 and 1.2 until the end of unknown pattern p :
Step 1.1: Divide the unknown pattern p to n vectors v with length two.
Step 1.2: Sum up the energy function for all n vectors v in the unknown pattern each with its corresponding vector in the stored patterns:
$ep = -0.5 * \sum_{i=1}^n (y_i)^2$
Where n is the number of vectors.
Where y_i is :
$y_i = v_i * s * w_i$
Step 2: Determine the stored code number $minc$ with the minimum energy function to converge the unknown pattern towards it:
$minc = \min(ep)$
Where the min function is to determine the minimum energy function in ep array.
Step 3: End.

4- Proposed BCR Module:

The proposed BCR module is illustrated in Figure (4). First, the Braille document is scanned by a scanner and then entered to the proposed system and the estimated results are saved in a text file. Each phase is discussed in details in the next subsections.

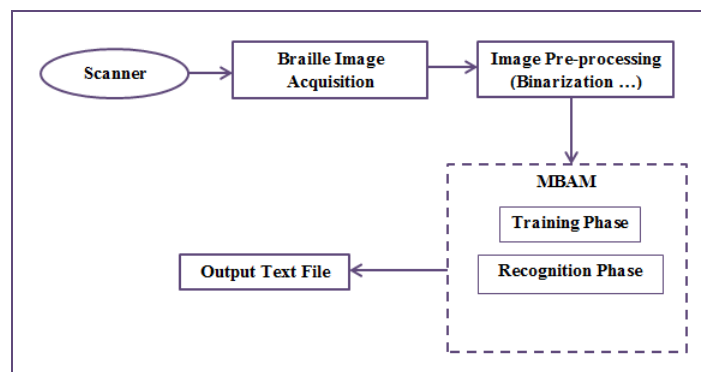
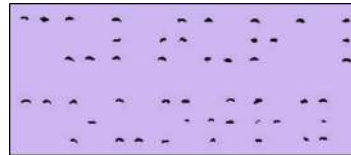


Fig. (4): The proposed BCR module.

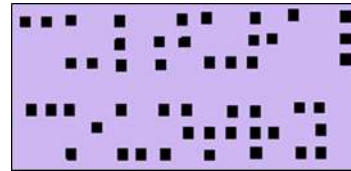
4-1 Image Acquisition: The job of the scanner is to scan the braille document by using Brather MFC-J470DW scanner with vertical and horizontal resolution” 200 dpi “.The image data are taken from the scanner and entered to the computer and saved as” JPG image format”.

4-2 preprocessing: The pre-processing phase contains a set of processes that make the scanned image more convenient for the next steps:

- 1- The conversion to gray scale is the first operation in the preprocessing phase.
- 2-By using the thresholding the image is transformed into white and black format.
- 3-Next using dilation to expand the dots in braille image and to be clearer, as illustrated in Figure (5).



(a)



(b)

Fig.(5): (a)The complemented image, (b) Te image after dilation

4- Character Area Allocation: Braille document in this step is localized vertically and horizontally to locate space for each character. Each character comprises four locations (X_{up} , X_{low} , Y_{up} , Y_{low}) which are upper and lower borders of the character as illustrated in Figure(6).

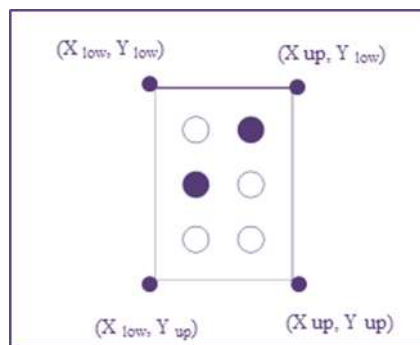


Fig. (6): Character space specified by (X_{up} , X_{low} , Y_{up} , Y_{low}).

4-3 Character Recognition using MBAM:

The proposed BCR module will use the Braille characters as a training image during learning phase and is implemented for each English character to be saved in a "lookup table" in MBAM to be recalled during recognition stage. The recognition phase is implemented for the braille image and detecting each character in it, by using the lookup table that is built during the training Phase.

5-Results

Different single side English scanned Braille documents are tested with the proposed method. The dataset used is composed from 46 Braille documents. The system is working on Grade 1 Braille English. Figure (7) shows the translation of one paper as an example for the proposed system translation.

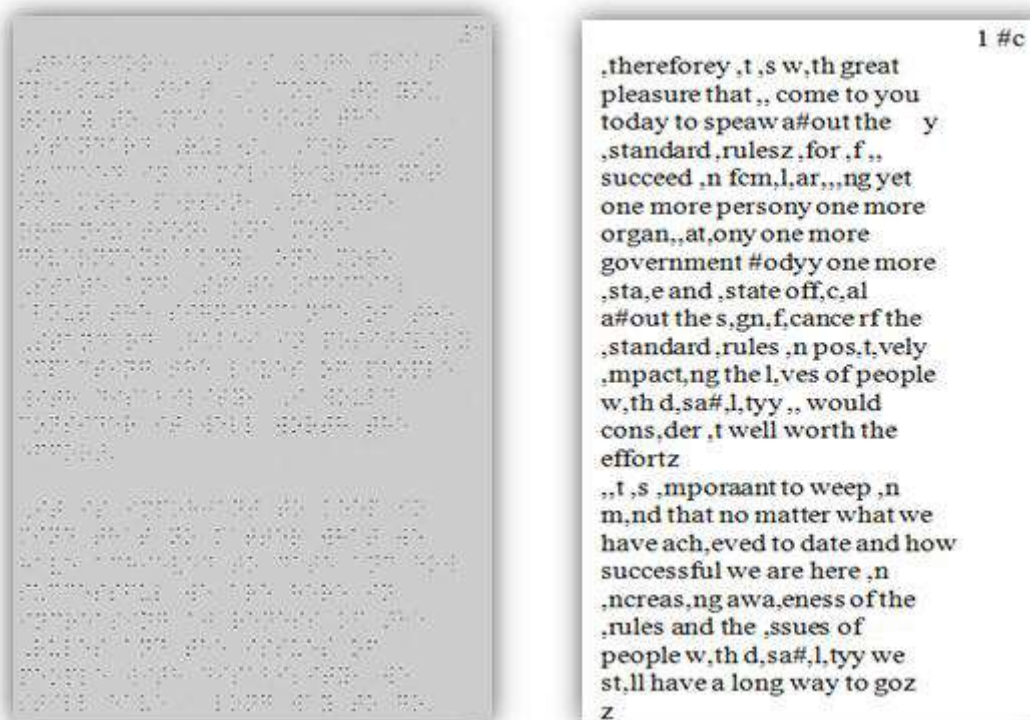


Fig.(7): Translation of Braille to English text by using (MBAM).

The average accuracy for correct letters was 91.87% as shown in figure(8), the average accuracy for correct words was 51.26% as shown in figure(9) The average processing time around 3.4 sec per page as shown in figure (10).

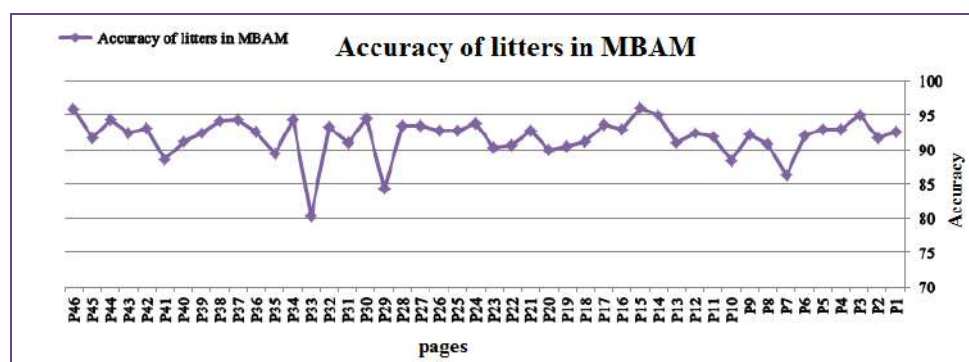


Fig. (8): Accuracy of letters for each page.

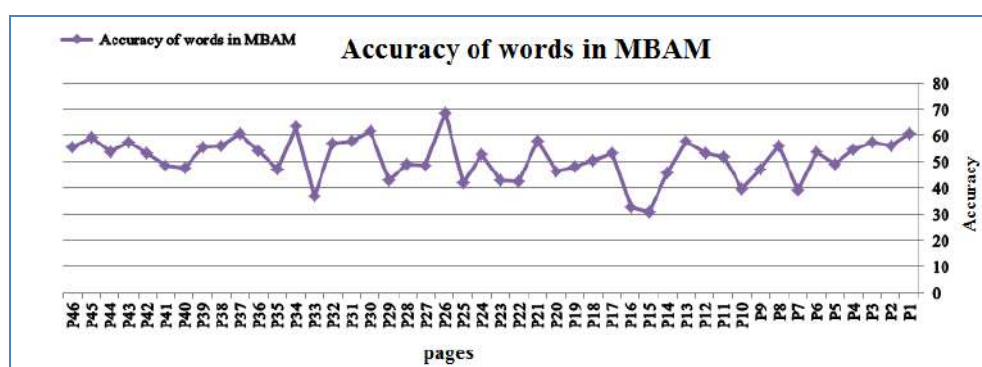


Fig. (9): Accuracy of words for each page.

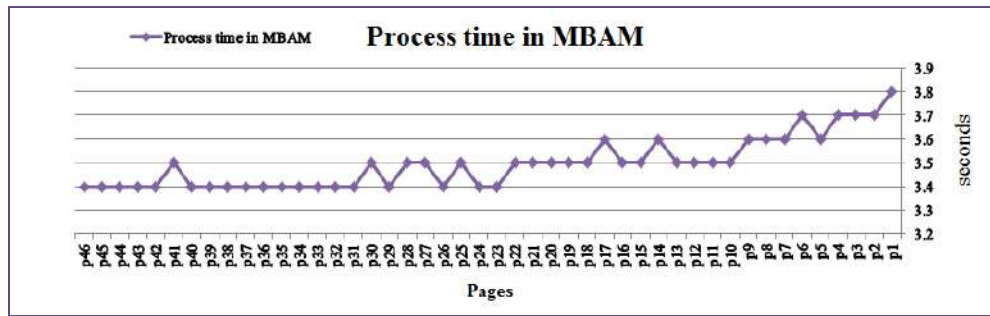


Fig. (10): Process time for each page.

Different threshold values were tested on five Braille images as shown in table (1). The best value of accuracy was when threshold= 0.7

Table (1): The accuracy With Different Thresholds using (MBAM).

By using (MBAM) Algorithm with different threshold								
Pages	0.5		0.6		0.7		0.8	
	L	W	L	W	L	W	L	W
P1	54.46%	019. %	92.07%	51.37%	92.63%	60.55%	0%	0%
P2	50.55%	1.75%	86.83%	46.49%	91.62%	56.14%	0%	0%
P3	74.77%	1.47%	92.85%	36.76%	94.97%	57.35%	0%	0%
P4	62.72%	1.21%	88.28%	30.48%	92.85%	54.76%	0%	0%
P5	58.81%	3.65%	89.73%	36.58%	92.96%	48.78%	0%	0%
Average	60.26	1.65	89.95	40.33	93	55.51	0	0

Where:

P1, p2, p3, p4, p5: page1, page 2,

L: accuracy for correct letters.

W: accuracy for correct words

6- Conclusions:

This work focused on the development of a BCR to recognize single side English document by using a new technique (i.e. MBAM) that will enable the researchers in the future to develop more efficient BCR in increasing accuracy and speed using associative memories. The proposed method is consisting of two stages: the preprocessing stage and the recognition stage. The output of the recognition stage is converted into voice signal. Braille sheets are used as an input forms in the tested experiments. These sheets are scanned and used as an input to the proposed BCR. The best accuracy value was when the threshold= 0.7 where for letters= 93% and for words =55.51%.

References:

- [1] AbdulMalik Al-Salman, Abdullah AlRajih and YosefAlOhali, Mohammed AlKanhhal "An Arabic Optical Braille Recognition System", ICTA'07, April 12-14, Hammamet, Tunisia.
- [2] Aisha Mousa, Raja Alomari, HazemHiary and LoaiAlnemer, "Smart Braille System Recognizer", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 6, No 1, November 2013, ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784.
- [3] Gordon E. Legge, Cindee Madison and J.Stephen Mansfield, "Measuring Braille Reading Speed With The Mnread Test", University of Minnesota, 75 East River Road, Visual Impairment Research, 2000 (in press).
- [4] Hind MwafaqTaha, "Robust Braille Recognition System Using Image Processing And Feature Extraction Algorithms", University TunHussienOnn Malaysia, January, 2014.
- [5] Manzeet Singh and Parteek Bhatia, "Enabling The Disabled With Translation of Source Text To Braille", Thapar University, Patlala-147004, July – 2010.
- [6] Mohammed Y. Hassan and Ahmed G. Mohammed, "Conversion of english characters into Braille using Neural network", IJCCCE, Vol. 11 No.2, 2011.
- [7] Nisreen A. Jabr, Emad I. Abdul Kareem, "Modify bidirectional associative memory (MBAM)", International Journal of modern trends in Engineering and Research, ISSN (Online) 2349-9754, ISSN: 2393-8161, 2015.
- [8] Nisreen A. Jabr, Emad I. Abdul Kareem, "Novel hetero-associative memory: A modified bidirectional associative memory", International Journal of Engineering Research and Advanced Technology (IJERAT), ISSN: 2454-6135 (Online), Volume. 02 Issue.02, 2016.
- [9] SantanuHalder, AbulHasnat, AminaKhatun, Debotosh Bhattacharjee, MitaNasipuri, "Development of a bangla character recognition (BCR) system for generation of bengali text from Braille notation", International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-3, Issue-1, June 2013.
- [10] Shreekanth, T., V. Udayashankara, "An algorithmic approach for double sided Braille dot recognition using image processing techniques", International Journal Image Processing and Visual communication, ISSN (Online) 2319-1724:Volume2, Issue 4, June 2014.
- [11] S.Padmavathi, Sphoorthy Reddy. S, Meenakshy. D. and Manojna K.S.S, "Conversion of braille to text in english, hindi and tamil languages", International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.3, No.3, June 2013.
- [12] Zainab. Authman, Zamen F. Jebr, "Algorithm prototype for regular feature extraction of Arabic Braille scripts", International Journal of Scientific Knowledge Computing and Information Technology, Vol. 2, No.1, ISSN 2305-1493, 2013.

Archaeology Areas Selecting independent of GIS with Fuzzy logic

Samira A. Hussain¹ Sundos A. Hameed Al-Azawi² Muna Jaffer³
Mustansiriyah University/ Collage of Sciences/ Computer Science Dept.
¹samira.hussain1212@gmail.com ²ss.aa.cs@gmail.com ³munnmnmun@yahoo.com

Abstract:

The proposed of this research is to implemented a system that can used in GIS environment to edit properties table and adding a new fields gives an important for the archaeology areas, depending on that fields it can allocate a big important area automatically Affected on a set of criteria by applying a Fuzzy logic for each criteria.

Keyword: GIS, archaeology areas, fuzzy logic.

اختيار المناطق الاثرية بالاعتماد على نظام المعلومات الجغرافية والمنطق المضبب

سميرة عبد القادر حسين سندس عبد الامير حميد منى جعفر

المستخلص

الهدف من هذا البحث هو عمل نظام يدخل الى بيئة (GIS) يقوم بتحديث جدول الخصائص (properties table) باضافة حقول جديدة تعطي اهمية خاصة للموقع الاثري (archaeology areas)، وبالاعتماد على هذه الحقول يمكن تحديد المواقع الاكثر اهمية من بصورة اوتوماتيكية. وهذه العملية تتم بالاعتماد على مجموعة من المعايير الخاصة بهذه المواقع وباستخدام المنطق المضبب (Fuzzy logic).

الكلمات المفتاحية: نظام المعلومات الجغرافية، المناطق الاثرية، المنطق المضبب.

1. Introduction

The knowledge and understanding of the origin and development of human society is of fundamental importance to humanity in determining its cultural and social origins. Archaeological civilization is the basic information of ancient human activities. Their protection and proper management are therefore essential to facilitate their study and interpretation by archaeologists and other researchers for the benefit of present and future generations [1, 2].

The protection of this heritage may not depend solely on the application of archeology techniques. This requires a broader base of knowledge and professional and scientific techniques. Some parts of the monuments are the components of architectural structures and in such cases they must be protected based on criteria found to protect these areas [3]. Therefore, finding a procedure to identify the most important archaeological areas is a very important and effective work

In this research we attempted to analyze the important properties in determining the appropriate effects areas. These characteristics may include the height and area of the archaeological area, distance from the main street and the architecture of the archaeological areas. Here the most important characteristics were selected and then the use of a fuzzy logic-based GIS approach, the use of a mysterious procedure due to the fact of the identification of the most important archaeological areas[5]. With the use of ambiguous it is possible to achieve the optimal solution based on the various uncertainties exist in the selection of effects areas

In this system, the moving characteristics and statistical data of the selected archaeological areas were collected in the city of Babylon. To determine the archaeological area. Among a number of influential properties, four were selected and formulated in a mysterious inference system. It is an "area of archeology", "high archeological areas", "distance from the archaeological area to the main street" and "architecture in the field of archeology". Raster data and transporters are used in this study.

2. Fuzzy logic

Fuzzy logic widely used areas of problem analysis and resolution. A mysterious group is a group of elements that have organic degrees. A fuzzy group element can be a full-member member or a custom partial membership value for an item that is no longer limited to only two values, but can be

0, 1, or any value between them. A mathematical equation that determines the degree of element membership in a vague set may be called an organic function. The advantage of this function is the ability to describe the problem linguistically and not in terms of the relationships between numerical values. On the one hand, the foggy system has the ability to represent classification decisions in the form of ambiguous rules. Fuzzy sets allow partial and multi-valued membership.

Fuzzy logic systems take advantage of fuzzy, inaccurate or uncertain information to generate simpler models that are easier to handle and more familiar in human thinking. The human expert is the main source of the mysterious rules, so it is possible to improve the performance of the system by adding new rules, removing faulty rules or updating existing rules in the knowledge base. However, the construction of the knowledge base, especially fine-tuning the parameters a mysterious set of fuzzy rules in the mysterious system of experts, is a daunting and objective process [6, 7].

2.1. Fuzzy Set

A fuzzy set is a set of containing elements that have varying degrees of membership in the set. Elements of a fuzzy set are mapped to a universe of membership values using a function theoretic [6].

A fuzzy set A in a universe of discourse X is defined as set:

$$A = \{(\mu_A(x): x \in X) \mid \dots\} \quad (1)$$

Where, $\mu_A(x): X \rightarrow [0,1]$ is a mapping called the membership function of fuzzy set A and $\mu_A(x)$ is called the degree of belongingness or membership value or degree of membership of $x \in X$ in the fuzzy set A . we write (1) in the following form:

$$A = \{\mu_A(x) / x: x \in X\} \quad \dots (2)$$

We often equate fuzzy sets with their membership functions. That by instead of a fuzzy set A characterized by $\mu_A(x)$ we say fuzzy sets μ_A [7, 8].

2.2. Membership Function

The trapezoid membership function is used for converting the crisp set into fuzzy set. A trapezoid membership function is determined by four elements (a, b, c, d) that shown in (Figure1) [9]:

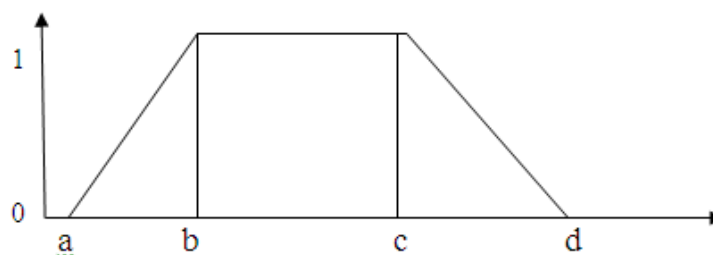


Fig. (1): Trapezoid membership function.

3. Geographic Information Systems (GIS)

One of the main characteristics of the GIS is to link features of geographic representation on a map with characteristic data for geographic feature description [10]. In GIS environment, the user input, analysis and process a data that is communicate with some elements in the world. By using cartography software in GIS that can to display information at any area and as a different layers which can be turned on or not. Each layer views some different site of same place on the Earth. That layer can view the things like a place network, topographic, green land cover, water bodies, etc. [2, 3].

4. Proposed System

The proposed methods of this system are clear in (Figure 2)

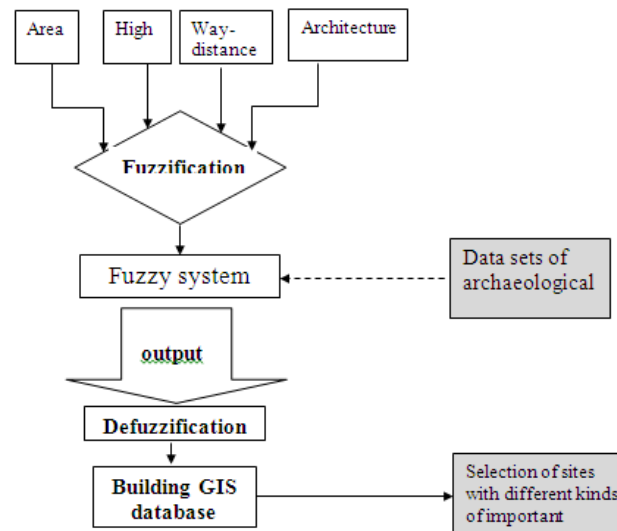


Fig. (2): workflow of the proposed GIS- based fuzzy system for selection of archaeology area

4. 1. Fuzzy system for locating the most important archaeology area

A programming language VB.NET has been developed to inter a data in to GIS environment and convert the elements value to fuzzy values by using the trapezoid membership function.

4. 2. Determine (input / output) parameters

The selected of 4 parameters considering on the experimental investigations. The linguistic parameter and fuzzy range have been defined in (Table 1):

Table (1) Determine input parameters

Parameter's Name	Input parameters
area	Area of archaeology areas
high	High of archaeology areas
Way-dist	Distance from archaeology area to main street
architecture	Architectural of archaeology areas

In the next stage, for each of the parameters a specific membership function has been defined. A trapezoidal function has been used for all variables. One feature of this function is a specific range in its middle the maximum weight is equal to 1.

Table (2) indicates the chosen amounts for area variable. The other variables have been indicated in Tables (3) and (4). In Tables (2) to (4), parameters A, B, C and D are trapezoidal parameters functions for each linguistic variable. The data used is illustrated in figure (3).

Table (2) linguistic variables /area of archaeology area

Area					
Values (m ²)	Linguistic variable	A	B	C	D
0 - 2000	Small	0	0	500	2000
500 - 10000	Medium	500	2500	7000	10000
6000 - 50000	Big	6000	10500	20000	50000

Table (3) linguistic variables/ high of archaeology area

High					
Values(Meter ³)	Linguistic variable	A	B	C	D
0 - 4	Low	0	0	2	4
2 - 10	Medium	2	5	7	10
7 - 30	High	7	11	20	30

Table (4) linguistic variables / distances from main streets

Way_distant					
Values(Meter)	Linguistic variable	A	B	C	D
0 - 3000	Good	0	0	500	3000
750 - 10000	Not good	750	2000	8000	10000

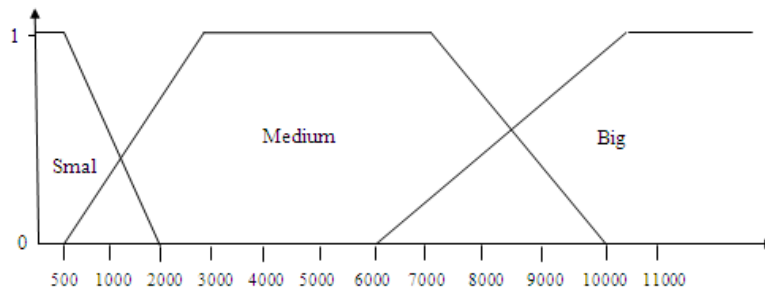


Fig. (3): illustrated the data used

The output is divided into 4 classes for goodness of the selected areas. There exists four input parameters which two of them attain three membership functions and the others have two membership functions, so we could define ($3 \times 3 \times 2 \times 2 = 36$) laws as the number of combinations. The procedure for defining the laws is such that for each input parameters, one of the functions has been selected, when "AND" operator applied with another membership function of another parameter and ultimately one of the possible output parameters to this new assumption has been assigned. Table (6) introduces the laws used by fuzzy system. The defined laws and their corresponding membership functions have been employed in a VB.NET program. The four sets of the classes are illustrated in Table (5):

Table (5) the four sets of the classes

Class number	Description
1	Most Suitable
2	Suitable
3	Weakly Suitable
4	Unsuitable

Table (6) Rules applied for the archaeology areas selection

No	area			High			Way_dis		arch		class
	small	medium	big	low	medium	high	Not good	good	visible	Not visible	
1	*			*			*		*		3
2		*		*			*		*		3
3			*	*			*		*		3
4	*				*		*		*		2
5		*			*		*		*		3
6			*		*		*		*		3
7	*					*	*		*		2
8		*				*	*		*		3
9			*			*	*		*		3
10	*			*				*	*		2
11		*		*				*	*		2
12			*	*				*	*		3
13	*				*			*	*		1
14		*			*			*	*		2
15			*		*			*	*		3
16	*					*		*	*		1

17		*				*		*	*		1
18			*			*		*	*		2
19	*			*			*			*	3
20		*		*			*			*	4
21			*	*			*			*	4
22	*				*		*			*	3
23		*			*		*			*	4
24			*		*		*			*	4
25	*					*	*			*	3
26		*				*	*			*	3
27			*			*	*			*	3
28	*			*				*		*	3
29		*		*				*		*	3
30			*	*				*		*	3
31	*				*			*		*	3
32		*			*			*		*	3
33			*		*			*		*	3
34	*					*		*		*	2
35		*				*		*		*	3
36			*			*		*		*	3

5. System Implementation

The study area is Babylon archaeology area at Babylon province. First the map has been exported to Arc Map and add a polygon shapefile which its properties table contain the values of 4 parameters. These values should be entered in programming language VB. NET environments.

The result of fuzzy process has been used to find the best archaeology area. One field have been added for reduce the output value. The output field has values between 1 into 4.

When the output value is 1, it is concluded that our polygon is most important, the figure below shows the GIS environments, raster, vector layers have been used, and the selection of the most important area by changing color of selected polygons.

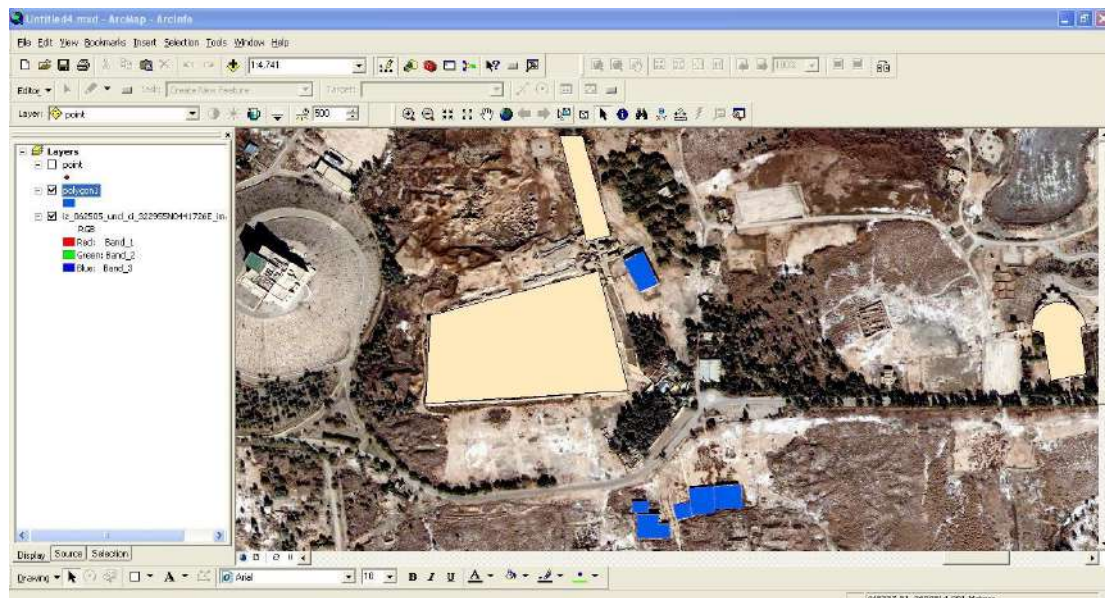


Fig. (4): GIS environments with two layers

6. Conclusions

In this system to achieve more precise results, all the influencing parameters should be used, not only the four parameters were considered for archaeology area. The fuzzy system will be used when we have uncertainty in our parameters and its value, however, using other parameters and their

associated ranges may give different answers. In this project we select the trapezoidal functions because they provided better results with respect to other functions.

References

- [1] G. Bojadziev and M. Bojadziev, "**Fuzzy Logic for Business, Finance, and Management**", "Advances in Fuzzy Systems: Applications and Theory- World scientific Publishing Co. Ltd, Vol.23, 2007.
- [2] Gemitzi et al, "**Evaluating Landslide susceptibility using environmental factors, Fuzzy Membership Functions and GIS**", Global NEST Journal, Vol. 13, No 1, pp. 28-40, 2011.
- [3] Decker D.; "**GIS Data Sources**"; John Wiley and Sons, New York, 2000.
- [4] Hualong Zhao, "**Urban Planning Management Information System based on GIS**", International Symposium on Web Information Systems and Applications, 2009.
- [5] Irfan Rafique, Jingnong Weng, Yunhong Wang, "**Software Learnability Evaluation, An Overview of Definitions and Evaluation Methodologies for GIS Applications** ", The Seventh International Multi-Conference on Computing in the Global Information Technology, 2012.
- [6] Franck Deroncourt, "**Introduction to fuzzy logic** ", MIT Massachusetts Institute of Technology, 2013.
- [7] R.S. Yadav et al., "**Modeling Academic Performance Evaluation Using Soft Computing Techniques: A Fuzzy Logic Approach**", International Journal on Computer Science and Engineering (IJCSSE), 2011.
- [8] T. J. Ross, "**Fuzzy Logic with Engineering Applications**", John Wiley & Sons Ltd, 2010.
- [9] D. Hyam; "**The GIS files**", Corporate Publishing, 2003.
- [10] M. Roumi, "**Implementing Texture Feature Extraction Algorithms on FPGA**", MSc Thesis; Delft University of Technology, 2009.

Modulation and Energy Components for Speaker Recognition System

Tariq A. Hassan

Ammar M. Kamel

College of Education/ Computer Science Department/ Mustansiriyah University

Abstract:

This paper presents a model the use the modulation and energy components for speaker recognition application, that is mainly follows the short-term scenario in speech signal processing, and also introduce a parameter combination that includes the instantaneous components and the energy parameters. This will describe the importance of short-term speech analysis in estimating the modulation parameters and the role of the instantaneous energy in estimating the speaker-dependent parameters. Simply, the short-term scenario is used to, first; avoid the silent and background noise speech portions that present in speech signals, and also to benefit from the stationary concept of the short-term processing in the speech signal. The energy components, on the other hand, are adopted purely in many speech parameterisation models, such as, linear predictive coding (LPC) and Mel-frequency cepstral coefficients (MFCCs). The main ideal of our mixture parameter (or MFCC/AM-FM model) is to determine the extent of these components to contribute together in extracting the parameters that are more related to the speaker more than anything else presented in the speech signal. We evaluated both models using the text-dependent and text-independent speech corpora. The accuracy results show that the frame-based AM-FM model achieves better performance comparing with the traditional structure of the AM-FM modulation model (the model presented in [1]). The MFCC/AM-FM parameters, on the other hand, perform much better, in terms of text-dependent, comparing with the AM-FM parameters and the MFCC parameters. In the case of the text-independent, however, the MFCC/AM-FM model provide better results than the MFCC features but less performance comparing to the AM-FM modulation parameters.

معاملات الطاقة والنمذجة لغرض بناء نظام تحديد المتكلمين

المستخلص:

يقدم هذا البحث نموذجاً للتعديل واستخدام مكونات الطاقة لتطبيق التعرف على المتكلمين، وهو في المقام الأول يتبع السيناريو على المدى القصير في معالجة الإشارات الكلام، ويدخل أيضاً وهذا يشمل مكونات مزيج المعلمة والمعاملات الطاقة لحظية. هذا البحث يقوم في وصف أهمية تحليل الكلام على المدى القصير في تقدير تعديل المعاملات ودور الطاقة لحظية في تحديد المعاملات التي تعتمد على اللغة. ببساطة، يتم استخدام السيناريو على المدى القصير، أولاً؛ تجنب الصمت والضوضاء الخلفية موجودة في أجزاء الكلام هذا إشارات الكلام، وأيضاً للاستفادة من مفهوم الثابت في المدى القصير في معالجة الإشارات الكلام. مكونات الطاقة، من ناحية أخرى، قد استخدمت في كثير من الإيات معرفة الكلام المعتمدة نماذج البارامترات، مثل، التنبؤي الترميز (LPC) وميل التردد معاملات cepstral الخطية (MFCCs). الغرض الرئيسي للخليط في المعاملات (أو نموذج MFCC/ AM-FM) هو لمعرفة مدى قدرة كلاهما على المساهمة هذه المكونات معا في استخراج المعلمات التي هي أكثر ارتباطاً للمتكمّل أن أي شيء آخر أكثر قدم في إشارة الكلام. قمنا بتقييم كلا النموذجين باستخدام التي تعتمد على النص والنص المستقل المجاميع الكلام. أظهرت النتائج دقة هذا النموذج AM-FM الإطار القائم على تحقيق أداء أفضل مقارنة مع الهيكل التقليدي للنموذج تعديل AM-FM (نموذج الواردة في [1]). المعلمات MFCC/ AM-FM، من ناحية أخرى، وأداء أفضل بكثير، من حيث يعتمد النص، مقارنة مع المعلمات AM-FM والمعاملات MFCC. في حالة النص مستقلة، إلا أن نموذج MFCC/ AM-FM تقدم نتائج أفضل من الميزات MFCC ولكن أقل أداء مقارنة لمعاملات تعديل AM-FM.

1. Introduction

In most cases, speaker identification and verification usually constitute the main activities of all speaker recognition models. Basically, speaker identification is the task of assigning an unknown voice to one of the speakers known by the system, while speaker verification refers to the case of accepting or denying a claim to be one particular speaker [2]. Whether the application was identification or verification, the most important part in constructing a speaker model is to find

measurable quantities that minimise intra-speaker variability and, at the same time, maximise inter-speaker variability [3]. These materials are then used as speech parameters in a process of code generating in speaker identification or verification tasks.

One recent example of those parameters is the signal modulation components, i.e., the instantaneous amplitude (envelope) and instantaneous frequency (phase). In fact, these parameters came to be an alternative to source-filter model parameters, namely, linear predictive coding (LPC), Mel-frequency cepstral coefficients (MFCCs) and perceptual linear prediction (PLP) coefficients. As it is well-known, the source-filter model majorly relies on the energy components of the speech signal, and ignores any other speech components especially those related to the phase parameter [4], [5].

Practically, the AM-FM modulation parameters are actually the only ones that describe the speech signal in terms of its energy information, represented by the instantaneous amplitude, and the its phase information represented by the instantaneous frequency. The representing of the speech signals by its envelope and phase comes from the desire to understand the speech signal processing function performed by the auditory periphery, particularly the cochlea. AM and FM signals provide important parameters in understanding the information transmission in the nervous system [6].

The first applying of these parameters in speaker identification is presented by [1]. The modulation model adopted in is actually based on the multiband demodulation analysis (MDA) described in [7] as a method for tracing the speech formants frequency and bandwidths. This model, however, adopted what we call it as, segment-based AM-FM modulation processing. This is, simply, dealing with the speech signal as one segment, no matter how long this signal is or the amount of low-energy periods that come along with the speech. In this paper, we suggest a new style in dealing with the speech signal in terms of the modulation components estimating. The model that we suggest is the frame-based AM-FM modulation model. This model, however, is simply presented in order to avoid the contribution of the low-energy periods in modulation parameter estimation, and, at the same time, exploit the stationary properties of the speech signal within short time periods. This is archived by cutting the signal into fixed length frames and then applying the filtering and the modulation parameter estimation on each frame of the speech.

In addition to that, we also suggest to use, what we called, and the instantaneous energy parameters along with the modulation components. This will give us a chance to appreciate to what extent that the signal energy around each filter channel can contribute along with the instantaneous parameters in identifying the speaker identity.

In the next sections, we will first give a brief of the AM-FM modulation model as presented in [1], then we move to explain our model in estimation the modulation components. After that, we will describe the mixture model (the MFCC/AM-FM model) and give the formula to achieve such combination. Finally, we will present our proposed model and its performance compared with the segment-based AM-FM modulation model presented in [1].

2. The Segment-based AM-FM Model

AM-FM speech signal modulation is a procedure that is used to decompose a speech signal into its modulated components of envelope (instantaneous amplitude) and phase (instantaneous frequency). Subject to nonlinear and time-varying phenomena during speech production (the frequency content changes with time) the AM-FM modulation model comes to seek and exploit the rich set of time-varying frequencies inherent in the speech signal and employed them in many speech signal applications. For example, in [7] AM-FM approach is adopted in the context on formant tracking while in [8] the model is employed in the speech recognition application. In [1] and [9] the AM-FM model is adopted for the purpose of speaker identification, both works used speech signal in the parameters encoding for speaker identification.

In order to characterise a modulation component for a speech signal, a single-valued frequency signal must be generated by breaking the signal down into its frequency components. To do so, a filter bank consist of set of band pass filters are adopted. The idea is to perform the method of multi

band demodulation analysis (MDA) as it's described in [7]. We used the Gabor band pass filters because they are optimally compact and smooth in both the time and frequency domains [10]. This characteristic guarantees accurate amplitude and frequency estimates in the demodulation stage [7]. The analytic signal is then constructed for each band pass output waveform; it is a transformation of the real signal into the complex domain and it is adopted because it permits the characterisation of the real input in terms of instantaneous amplitude and frequency [11]. Mathematically, given a real input signal $s[n]$, its analytic signal can be computed as

$$s_a[n] = s[n] + jH[s[n]] = s[n] + js^{\wedge}[n]; \quad \dots\dots\dots(1)$$

Where the quadrature signal $s^{\wedge}[n]$ is the Hilbert transform of speech signal $s(t)$. From the analytic and speech signal the phase (t) can be calculated as:

$$\phi[n] = \arctan \left(\frac{\hat{s}[n]}{s[n]} \right). \quad \dots\dots\dots(2)$$

The instantaneous frequency (IF) of the signal can be computed directly from the phase as:

$$f[n] = \frac{1}{2\pi} \cdot \frac{d\phi[n]}{dt}. \quad \dots\dots\dots(3)$$

The instantaneous amplitude is computed as:

$$\hat{a}[n] = \sqrt{s^2[n] + \hat{s}^2[n]}. \quad \dots\dots\dots(4)$$

To get the proper values of instantaneous frequency, instantaneous amplitude and instantaneous frequency are combined together to obtain a mean-amplitude weighted short-time estimate F_i of the instantaneous frequency for each band pass filter output (waveform) [7].

$$F_i = \frac{\int_{n_0}^{n_0+\tau} [f[n] \cdot \hat{a}^2[n]] dt}{\int_{n_0}^{n_0+\tau} [\hat{a}^2[n]] dt}, \quad \dots\dots\dots(5)$$

Where τ is selected length of the time-frame. The adoption of a mean amplitude weighted instantaneous frequency in is motivated by the fact that it provides more accurate frequency estimates and is more robust for low energy and noisy frequency bands when compared with an unweighted frequency mean [7]. The computation of the short-time instantaneous frequency for each signal leads to the extraction of the speaker descriptors set that used as a system parameter.

This model, however, does not follow any principles in speech signal processing, it is simply constructed in a way that allows to use the MDA method to generate the pyknoqram parameters (originally presented by [7] as a time-frequency representation of the speech signal) and used them for speaker identification. Also, Although is quite obvious that the contribution of the low-energy period have detrimental effect in many speech signal analysis models, however, the authors in did not show that the contributing of the low-energy periods can affect the recognition performance.

Therefore, our aim is to modify the processing structure of the AM-FM model and makes it more appropriate with the general structure of speech signal processing usually adopted in previous models, such as the source-filter model. The next section will explain the main steps of our suggested frame-based AM-FM modulation model.

3. The Frame-based AM-FM Model

This model basically follows the processing style adopted in most speech signal analysis systems. In this model, instead of dealing with the whole signal as one segment (the demodulation method adopted in [1]), the speech signal is initially divided into fixed-length frames. These frames are

actually characterised by their own energy which is, in this case, the parameter that we need to decide which frames will be contributed in the demodulation processing.

To be more clear, each frame is regarded as one limited-length speech signal (one unit) and the modulation components extracted from one frame are unrelated to the other frame of the signal. This means, each frame will represent a unique case in the feature vector in terms of the modulation parameters.

In fact, this approach is very similar to the standard procedure used in MFCC encoding, the main difference is the output of each channel is a single-band signal (single-valued frequency signal), and also no discrete cosine transform (DCT) will be applied on the filter channels outputs. From this signal, however, the modulation components (the instantaneous amplitude and frequency) will be estimated and, from these components, the mean amplitude weighted instantaneous frequency (equ. 5) is calculated.

Figure 1 explains the block diagram of our main step of the frame-based AM-FM modulation model. The signal is first divided into fix-length frames (25ms in our experiment with 10ms overlap) then energy value of each frame is calculated. If the energy value is equal to, or more than, the threshold (0.1 in our experiment) then the segment is taken, otherwise it is regarded as a silence segment and no more process is done on it. A high emphasis filter (1 0:98Z 1) is applied to the accepted segments (in order to balance the signal spectrum) and a 25 ms Hamming window is applied to the emphasised speech every 10 ms.

The speech segments are then passed through a set of Gabor band pass filters (30 channels in our experiment) with center frequencies that are mel-spaced on the frequency axis with critical bandwidth computed through the equation:

$$Bw(n) = 25 + 75 \cdot 1 + 1:4(f_c(n)=1000)^{2 \cdot 0:69} \dots \quad (6)$$

The idea of non-uniform frequency analysis comes from the actual processing of the speech signal by the basilar membrane inside the human ear. In this case, the frequency responses overlap significantly since points on the basilar membrane cannot vibrate independently of each other. The critical bandwidth, on the other hand, has been defined and measured using a variety of methods, showing that the effective bandwidths are constant at about 100 Hz for center frequencies below 500 Hz, and with a relative bandwidth of about 20% of the center frequency above 500 Hz [12].

For each band pass filter channel output, an analytic signal is constructed by Hilbert transform of real-valued signal, the instantaneous amplitude and frequency are then computed directly through the equations (3). Instantaneous amplitude and frequency are combined together to obtain a mean amplitude weighted instantaneous frequency and encoded them as parameters for speaker identification.

After the demodulation analysis, the feature vectors of each speaker can be represented by an $N \times F$ matrix, where N corresponds to the number of Gabor filters used in the filter bank and F corresponds to the number of frames that have energy equal to or more than the energy threshold of 0.01. For the decision making step, GMM classification is adopted with the number of component densities in the mixture model chosen depending on the identification task (text-dependent or -independent).

4. The Frame-based AM-FM model and MFCC Features Combination

In an attempt to generate a new set of speaker identification features, [13] adopted the AM-FM model along with LPC analysis to produce a feature set derived from both models. The LPC/AM-FM model, as they called it, is used to extract features that are described to be robust over a degraded channel. In this work, the LPC analysis is applied to estimate the location of the speech formants. This estimates the spectral envelope of the speech signal, and ignores the source features present in the speech. The AM-FM parameters are used to generate three waveforms for each single-band signal. These waveforms represent; the energy, the envelope (the instantaneous amplitude), and the phase (the instantaneous frequency) for each formant estimated in the previous step.

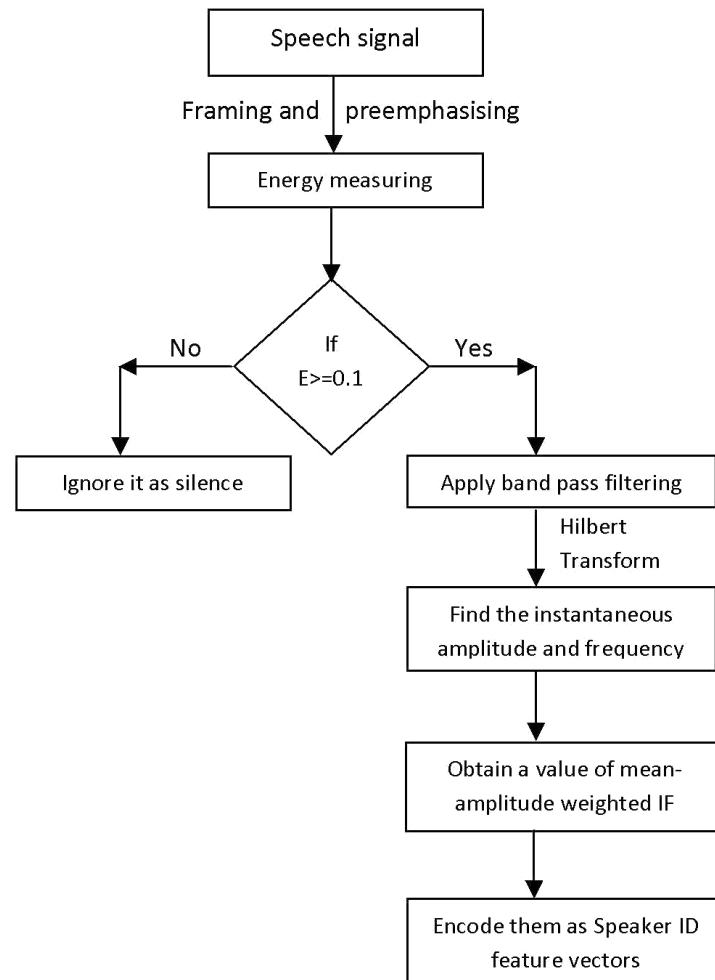


Fig. (1): Block diagram of our suggested method

In our work however, we also try to benefit from the idea of mixing features from more than one model of the speech signal in an attempt to improve the performance of the speaker identification system. Our proposed idea is to make some type of mixture between the spectrum parameters that are usually adopted in MFCC and LPC analysis and the modulation parameters of the AM-FM model.

In this approach, which we call the MFCC/AM-FM model; instead of only estimating the modulation components of each single-band signal (frame) the energy components are also computed. The both parameters (the modulation and the energy parameters) are then computed together to generate one parameter values represent the effect of the modulation parameters and the energy around each filter channel in the system.

The discrete cosine transform (DCT) is applied in order to obtain the instantaneous parameters affected cepstral coefficients, which is simply represent three combined components (the instantaneous amplitude, the instantaneous frequency and the signal energy at one specific time). That is, the speech signal will be represented by an N C matrix of features, where N is the number of channels of the Gabor filter bank and C is the number of DCT coefficients. Mathematically, the MFCC/AM-FM process can be described as:

$$En_i = \sum_{t=1}^{\tau} s_n(t)^2$$

$$EnF_i = En_i \times \left[\frac{\int_1^{\tau} [f(t) \cdot \hat{a}^2(t)] dt}{\int_1^{\tau} [\hat{a}^2(t)] dt} \right]$$

Where E_{ni} represents the energy of the band passed waveform s_n for the i th frame, L is the frame length, and E_{nFi} is the modulated energy that is later used to obtain the MFCC/AM-FM parameters.

5. Speech Database

Two speech corpora were used to evaluate our proposed model. The first is the text-dependent British Telecom Millar database, specifically designed and recorded for text-dependent speaker recognition research. This data set consists of 60 (46 males and 14 females) native English speakers saying the digits one to nine, zero, nought and oh obtained in five different sessions over a time span of about three months. Each speaker in the corpus participated in five recording sessions. The first and second recording sessions (10 repetitions) were used for training while the rest of the data (15 repetitions) were used for testing.

The second data set is the NTIMIT corpus [14]. A subset of the NTIMIT database is used in our work. This subset (38 speakers from the New England dialect region) contains 10 sentences of read speech for each speaker. The male subset contains 24 speakers, while the female subset contains 14 speakers.

6. Results

To evaluate how the framing of the speech signals affects the speaker identification performance, we compare the performance of our proposed method (frame-based AM-FM model) with the traditional AM-FM modulation model presented in [1]. The two approaches are evaluated using both the text-dependent (BT-Millar) and text-independent (NTIMIT) speech corpora.

In the case of text-dependent evaluation, the assessment includes the original, clean tokens of the BT-Millar database and also noisy versions of these corpus (to which Gaussian white noise has been added at 40% SNR). This is done because noisy speech is more realistic for an application, but also explicitly to see the effect of noise on both performances. In the case of text-independent evaluation, however, we use the telephone-quality NTIMIT corpus as it stands, because realistic noise is already presented in the speech.

In both cases, GMM is used with a diagonal covariance matrix. This choice is based on the empirical evidence that diagonal matrices outperform full matrices and the fact that the probability density modeling of an M th-order full covariance matrix can equally well be achieved using a diagonal covariance larger-order mixture [15]. The number of component densities in the mixture model is chosen to be between (7-15) Gaussians. Our experiment shows that increasing the number of Gaussians beyond these values does not improve the performance of the classifier with AM-FM features.

In terms of the instantaneous frequency parameters, the text-dependent speaker identification results are shown in Figures 2, 3. These Figures describe the recognition results of both frame-based and segment-based demodulation approaches for text-dependent speaker identification using both the clean and the noisy speech data of the Millar corpus.

From these figures, we can notice that the frame-based AM-FM model can achieve very much better performance compared with the segment-based model. Applying a one-tail t-test of significance (two-sample, equal variance) to the results for all 60 speakers yields, in case of clean database, a probability of $p = 3.28 \times 10^{-13}$, while in the case of noisy database a probability of $p = 3.21 \times 10^{-12}$ that the differences in mean accuracy between our method and the segment-based method.

Figure 4 shows the recognition results of the text-independent speaker identification of the frame-based model and segment-based model. As in the case of text-dependent identification, our proposed method outperforms Grimaldi and Cummins' method. A one-tail t-test of significance (two-sample, equal variance) applied to the results for all 38 speakers gives a probability of $p = 1.12 \times 10^{-6}$ that the differences in mean accuracy between our method and the segment-based method.

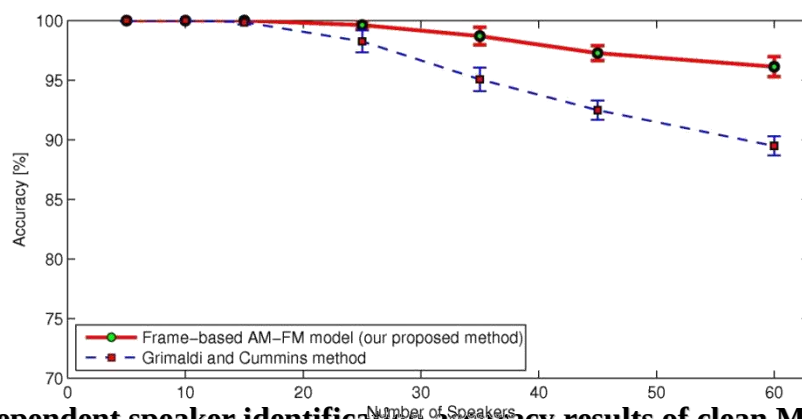


Fig.(2):Text-dependent speaker identification accuracy results of clean Millar database with mel-scaled centre frequency and bandwidth and frequency range of 0–8 kHz. Error bars are standard deviations across the 10 folds of training/test data.

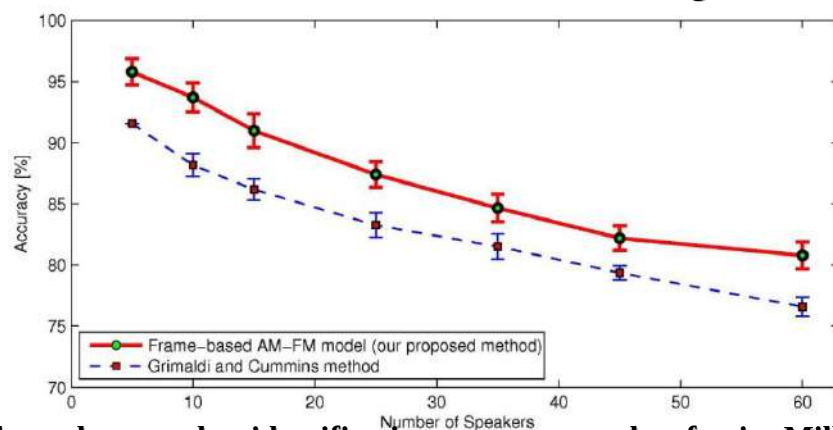


Fig. (3): Text-dependent speaker identification accuracy results of noisy Millar database with mel-scaled centre frequency and bandwidth and frequency range of 0–8 kHz. Error bars are standard deviations across the 10 folds of training/test data.

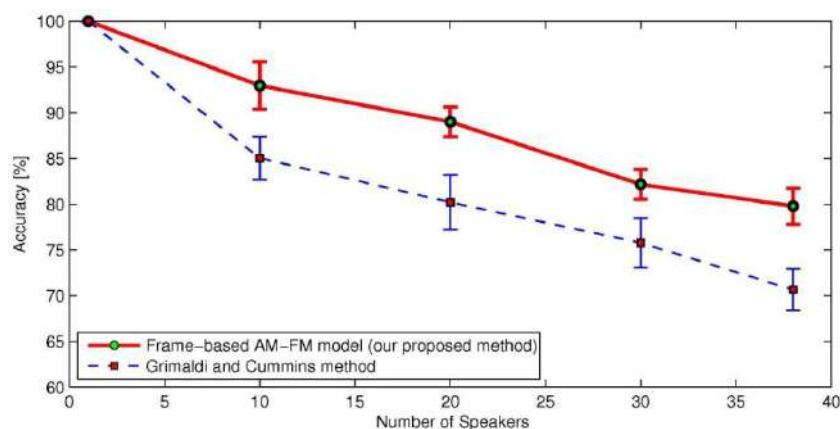


Fig. (4): Text-independent speaker identification accuracy results of telephone quality NTIMIT database with mel-scaled centre frequency and bandwidth and frequency range of 0–8 kHz. Error bars are standard deviations across the 10 training/test folds.

Figures 5, 6, 7 are presenting the MFCC/AM-FM model performance in terms of text-dependent (clean and noisy) and text-independent speaker identification. The figures show the recognition results for three models parameters (instantaneous frequency, instantaneous amplitude, and the MFCC coefficients). From these figures we can see that the performances of the MFCC/AM-FM parameters are varying depends on the speech data type (dependent and independent). In the context of text-dependent (clean and noisy), it is clear that our MFCC/AM-FM method achieves better performance than traditional MFCC method. Applying a one-tail t-test of significance (two sample, equal variance) to the results for all 60 speakers yields a probability of $p = 0.006$ (clean), $p = 9.9 \times 10^{-10}$ (noisy).

9 (noisy) that the differences in mean accuracy between our MFCC/AM-FM and the MFCC method. In the context of text-independent, however, the AM-FM model gives better results comparing with the other models. This might, as we think, there is a much bigger performance penalty to introducing MFCC parameters for the text-independent NTIMIT database than for the text-dependent Millar database. Hence, we might expect the use of MFCCs along with AM-FM parameters to perform less well than the frame-based AM-FM model, which uses modulation parameters only.

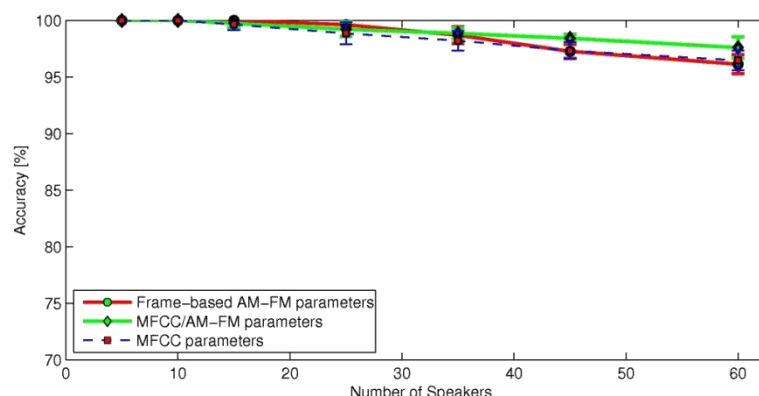


Fig. (5): Performance of the MFCC/AM-FM method relative to the frame-based AM-FM and MFCC approaches for text-dependent identification using clean Millar speech with mel-scaled centre frequency and bandwidth and frequency range of 0–8 kHz.

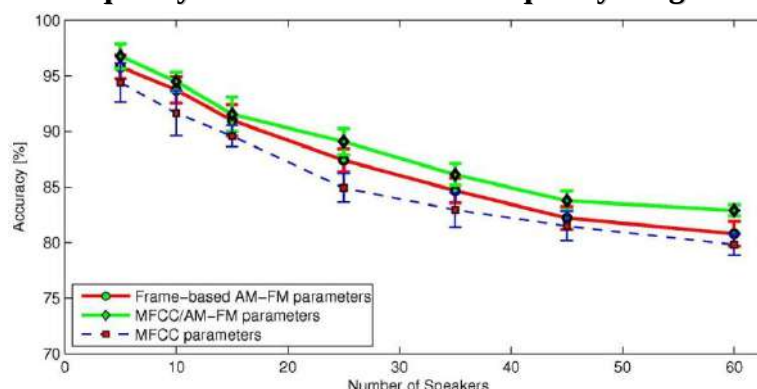


Fig. (6): Performance of the MFCC/AM-FM method relative to the frame-based AM-FM and MFCC approaches for text-dependent identification using noisy Millar speech with mel-scaled centre frequency and bandwidth and frequency range of 0–8 kHz.

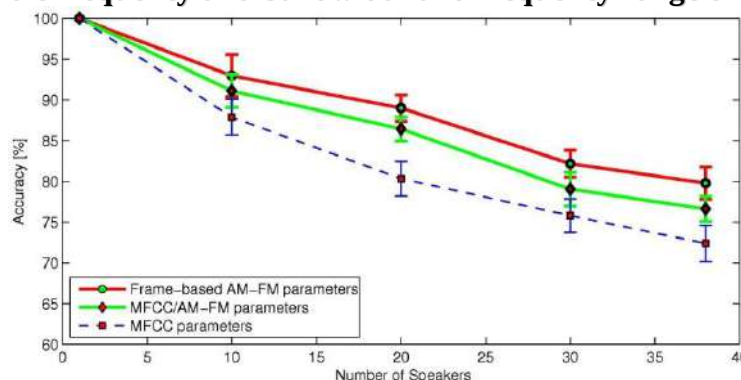


Fig. (7): Text-independent speaker identification results for frame-based AM-FM parameters, MFCC parameters, and the MFCC/AM-FM parameters using the NTIMIT database with mel-scaled centre frequency and bandwidth and frequency range of 0–8 kHz.

7. Conclusion

From this work, we can conclude that the adopting of frame-based AM-FM modulation model can achieve two important points. First, this model allows only these parts of speech signal with reasonably high energy (0.01 in our experiment) to contribute in the modulation components estimating. This means, the will only deal with those parts that hold a useful information about the speaker. The second benefit is the importance of the short-time stationary assumption of the speech signal. Simply, the fixed-length frames are tending to be quasi-stationary in terms of its harmonics (excitation frequencies) and resonance (formant frequencies) [16, Sec. 5.3].

The accuracy results confirms the important role of the short-time stationary aspect of the speech signal in estimating the modulation parameters with high accuracy compared with long-term processing of speech. Also, the contribution of the energy parameter can improve the recognition performance, especially in the case of text-dependent identification. In the text-independent, however, it seems the effect of the energy parameter does not help that much, but it still give us good results comparing with the traditional MFCC method.

References

- [1] M. Grimaldi and F. Cummins, "Speaker identification using instantaneous frequencies", IEEE Transactions on Audio, Speech, and Language Processing, vol. 16, no. 6, pp. 1097–1111, Aug. 2008.
- [2] P. Joseph Campbell, "Speaker recognition: a tutorial", Proceedings of the IEEE, vol. 85, no. 9, pp. 1437–1462, 1997.
- [3] Tony Brian Alderman, Forensic speaker identification: a likely hood ratio-based approach using vowel formants, Lincom Studies in Phonetics, LINCOM, Munich, Germany, 2005.
- [4] M. Foundez-Zanuy, S. McLaughlin, A. Esposito, A. Hussain, J. Schoentgen, G. Kubin, W. B. Kleijn, and P. Maragos, "Nonlinear speech processing: Overview and applications", Int. J. Control Intelligent System, vol. 30, no. 1, pp. 1–10, 2002.
- [5] Mohammadi Zaki, J Nirmesh Shah, and Hemant A Patil, "Effectiveness of multiscale fractal dimension-based phonetic segmentation in speech synthesis for low resource language", in International Conference on Asian Language Processing (IALP), 2014. IEEE, 2014, pp. 103–106.
- [6] S.M. Khanna and M.C. Teich, "Spectral characteristics of the responses of primary auditory-nerve fibers to frequency-modulated signals", Hearing Research, vol. 39, no. 1-2, pp. 159 – 175, 1989.
- [7] Alexandros Potamianos, Ros Potamianos, and Petros Maragos, "Speech formant frequency and bandwidth tracking using multiband energy demodulation", J. Acoust. Soc. Amer, vol. 99, pp. 3795–3806, 1996.
- [8] Niko Moritz, Jorn Anemuller, and Birger Kollmeier, "An auditory inspired amplitude modulation filter bank for robust feature extraction in automatic speech recognition", IEEE/ACM Transactions on Audio, Speech, and Language Processing, vol. 23, no. 11, pp. 1926–1937, 2015.
- [9] Karthika Vijayan, Pappagari Raghavendra Reddy, and K Sri Rama Murty, "Significance of analytic phase of speech signals in speaker verification", Speech Communication, vol. 81, pp. 54–71, 2016.
- [10] Ibrahim Missaoui and Zied Lachiri, Gabor Filterbank Features for Robust Speech Recognition, pp. 665–671, Springer International Publishing, Cham, 2014.
- [11] A. Rao and R. Kumaresan, "On decomposing speech into modulated components", IEEE Transactions on Speech and Audio Processing, vol. 8, no. 3, pp. 240–254, May 2000.
- [12] E. Zwicker and H. Fastl, Psychoacoustics: facts and models, Berlin; New York: Springer-Verlag, 1990.
- [13] R. Jankowski, T. Quatieri, and D. Reynolds, "Measuring fine structure in speech: application to speaker identification", in International Conference on Acoustics, Speech, and Signal Processing (ICASSP'95), May 1995, vol. 1, p. 325.
- [14] C. Jankowski, A. Kalyanswamy, S. Basson, and J. Spitz, "NTIMIT: a phonetically balanced, continuous speech, telephone bandwidth speech database", White Plains, NY, April. 1990, vol. 1, pp. 109–112.
- [15] D.A. Reynolds and R.C. Rose, "Robust text-independent speaker identification using gaussian mixture speaker models", Speech and Audio Processing, IEEE Transactions on, vol. 3, no. 1, pp. 72–83, Jan 1995.
- [16] J. D. Jr., J. Hansen, and J. Proakis, Discrete-Time Processing of Speech Signals, second ed., IEEE Press, New York, 2000.

Design Concept of Vehicle Alarming System using Smartphone Sensors and Bluetooth Technology

Dr. Eng. Asst. Prof. Saad A. Makki

Dept. of Computer Science/ College of Education, Mustansryiah University – Baghdad – Iraq,
drsaadamaki@yahoo.com

Abstract:

The Bluetooth technology is low energy wireless network that connect more than one device together in short limit. The usage of Bluetooth technology is wide spread mostly in the smartphones devices. The Bluetooth network used to transfer data and fields between 2 closing nodes. The modern technology is used for alarming from danger that is facing the humans; most of the Vehicle is vulnerability to the Danger whether in road or parking. Smartphones are used in wide spread applications such as social networks and web navigation. This research will make use of the smartphones communication capabilities in order to connect more than one smartphone device using Bluetooth network and connecting them together in order to transform information's between them. These information's also forwarded to a home PC using a wireless router that connects the smartphone device with the PC.in order to alarm the user for a specific type of danger.

1- Introduction

Smartphone Bluetooth is a short range wireless radio network that connects 2 devices together with the Bluetooth hardware devices available [1]. An example for a Bluetooth network is the connection between the wireless mouse and the PC were the mouse is connecting to the pc throw the Bluetooth network.



Fig. (1): shows the connected Bluetooth devices

The main aim of the Bluetooth technology in the proposed system is to connect the smartphones together in order to transfer the data between these devices in short range. The Bluetooth technology is required the Line of Site in order to work. It means that the receiver must be at the range of the Bluetooth devices of the sender in order to connect between the 2 devices. BWT devices randomly hop between frequencies up to 1600 times per second—much faster than other types of devices that use the ISM band. This means that if another device, such as a 2.4-GHz cordless phone, interferes with a BWT network at a particular frequency, the Interference only lasts for about 1/1600 of a second until the BWT devices hop to another frequency. This gives BWT Networks a high immunity to interference from other 2.4-GHz devices [2].

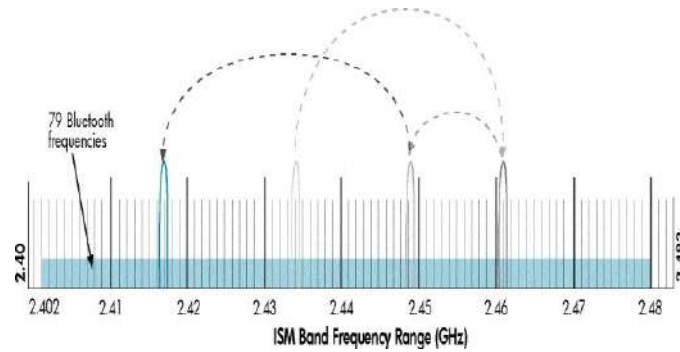


Fig. (2): shows the ISM frequency Range

2- Smartphones Sensors

Sensors are new advanced technology that makes use of the mechanical and thermal sensors Micro Electro Mechanical Systems (MEMS) is a technology of turning the sensors from its original size into micro sized sensors built in chips inside small devices. [3][4] These MEMS sensors are built in the smartphone in order to achieve more usability of the mobile devices these sensors are used to measures different environmental characteristics like pressure, thermal, and mechanical characteristics in the environment [5][6].The smartphone sensors are extracted there features from the around environment were each sensor has its own range of measurements, There are several types of sensors, acceleration sensor, magnetic sensor, gyroscope sensor, temperature sensor. And much more sensors under development each sensor is different from other in its reading data and features. The proposed system is make use of more than one MEMS sensor in order to works together to get more reliable results. [7][8].

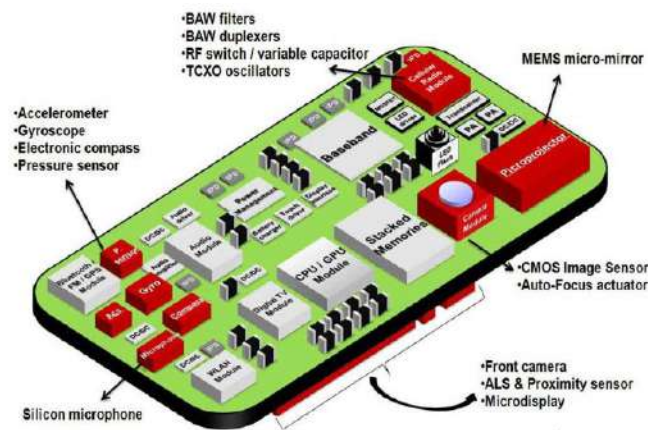


Fig. (3): shows the MEMS sensor in the smartphones

3- MEMS sensor Types:

There is a multiple types of MEMS sensor, the MEMS sensors can be summarized as follows

Table (1) shows the main MEMS types

No	Sensor type	Description
1	The Accelerometer	This sensor hardware measures the acceleration force In m/s^2 . This sensor used the three axis X, Y and Z Including the force of gravity.
2	The Gyroscope	This sensor measures the device rotation rate. Like when rotating the device it will determine the rotation state. Also its uses the X, Y, and Z physical axis
3	The temperature sensor	Measures the room temperature

4	The gravity sensor	Measures the Gravity that is applied on the smartphone in all three physical axis X, Y, and Z
5	The light sensor	Measures the light level (luminance)
6	The Magnetic field sensor	Measures the geomagnetic field in all three physical axis X, Y, and Z
7	The pressure sensor	Measure the air pressure sensor that is around the device
8	The proximity sensor	Measure the proximity of an object wither the device is held in ear or not
9	The orientation sensor	Measures the orientation of the current state of the device

4- Detecting Vehicle problems using smartphones.

Car accident is the main purpose for many deaths around the world. So its became so necessary to implement a new technology for preventing or pre-detecting the problems that causes the accident. When detecting a problem in the car it will be issuing an alarm signal in the smartphone and the Home PC. The communication process is as follows.

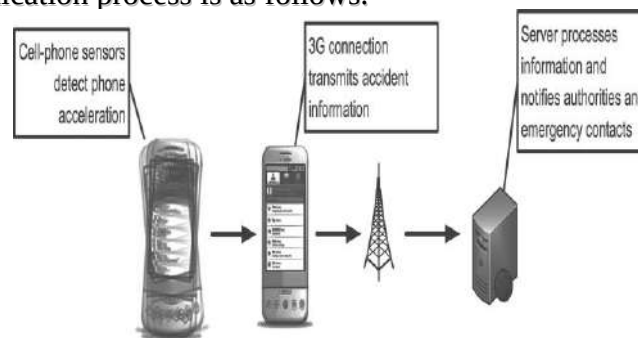


Fig. (4): shows the data transmutation scenario

The smartphone sensor will detect the change in the environmental characteristics as in acceleration and pressure sensors the smartphone will detect that there is a change and with the smartphones are connected together it will simply be more accuracy. The transmutation of the signal is going to be through the 3G technology that will be enabled when it's met the Danger Condition. The smartphones will be distrusted over the car. Connecting together using Bluetooth network, and will be transfer the data between them. The Sensors used in the system is the Temperature sensor, acceleration sensor, GPS system, Gyroscope, Camera Sensor and the magnetic sensor. All these sensors are worked together to monitor the Vehicle state from the accident and alarming the danger if it's happened [9].



Fig. (5): shows the smartphone positions

The acceleration sensors will measures the change in the smartphone acceleration, if the acceleration is to high then it will be considered as adanger acceleration. The accelerometer is a 3-axis based sensor which measures the X, Y, and Z coordinates.

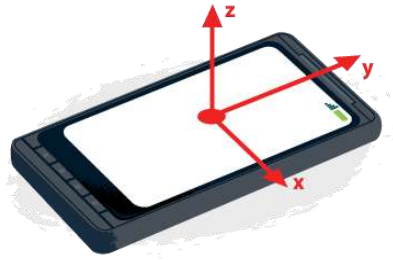


Fig. (6): 3-axis accelerometer

The temperature sensor is using to measures heat around the smartphone devices. The temperature sensor will monitor the temperature for any change in the heat around the device in case any suddenly rising of the heat degree then it will be noticed by the temperature sensor [10].



Fig. (7): shows the temperature sensor app

With any unusual rising in the temperature the heat sensor will be notify the user with this changing. The heat changing could be caused by a fire or a burning part in the car, this sensor can detect these changes in order to prevent a nearly future damage.

GPS is so necessary for position allocation. GPS use satellite data to calculate an accurate position on the earth. These calculations can relate the user's position to almost any map projection within mille-seconds. All GPS work in a similar manner but they often look very different and have different software. The most significant difference between GPS receivers is the number of satellites they can simultaneously communicate with. Most receivers are described as 12 channels meaning they can communicate with 12 satellites. Older models may be 8 or even 5 channel with More modern receivers capable of communicating with 14 20. Given the current makeup of the GPS satellite's constellation 12 channels is more than adequate [11].

A Gyroscope will determine the orientation of the smartphone. In case the smartphone is flipped or changing position for any reasons the orientation of the device will be changed. This effect can be noticed by the orientation sensor that can monitor if the car were Gyroscopes function differently depending on their type. Traditional spinning gyroscopes work on the basis that a spinning object that is tilted perpendicularly to the direction of the spin will have a precession. The significant size reduction of multi-axis MEMS gyroscope structures and their integration with digital interface into a single package of a few square millimeters of area at an affordable cost have accelerated the penetration of MEMS gyroscopes into hand-held devices. [12].

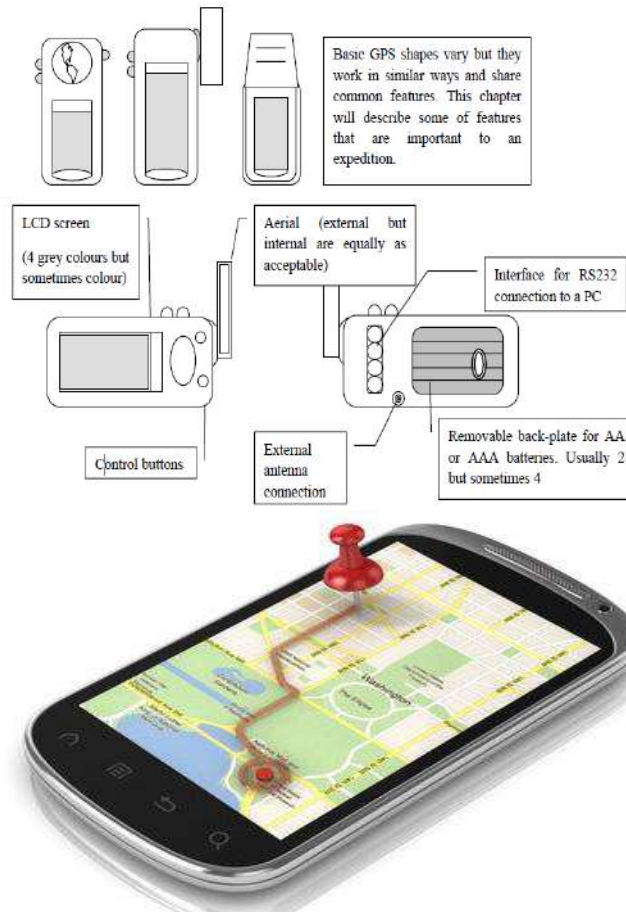


Fig. (8): shows the basic of GPS and GPS app



Fig. (9): Gyroscope application in smartphones

Magnetic sensor is massive usage sensors at all types were the magnetic sensor is measuring the magnetic field around the smartphone. The magnetic sensor is 3-axis magnetometer. Here are a lot of magnetic sensor applications such as medical and industrial applications. Magnetic sensor is measuring the magnet and the materials that effected with the magnet. Such as metal [13]. Any massive change in the magnetic field will lead to a notification by the magnetic field sensor app that is in turn will transfer a notification signal into the other connected devices in order to notify that there is something not right.



Fig. (10): shows the MEMS sensor Technology

Camera sensor is responsible of determining the camera state and monitor the operation of imaging in the smartphones. The camera sensor objective in the system is to open the smartphone camera if the alarming condition is occur and taking images in the current situation of the vehicle. These images can be useful later in Identification of a possible theft



Fig. (11): shows the camera sensor

5- App structure

The application that is designed to measures the sensor information's must be multithreaded program in order to deal with such a situation. The app is designed using the eclipse IDE that is Java based programming language and with the android SDK installed in the development PC the app must display all sensor information's. The programmer of the system will put the Conditions to from the practical experiments that when there is a threat or something not right in the physical characteristics in the normal situations the alarm will be initiates. The app will gathered information's from the sensors framework that will enables the app from getting the sensors readings and display these readings on the screen

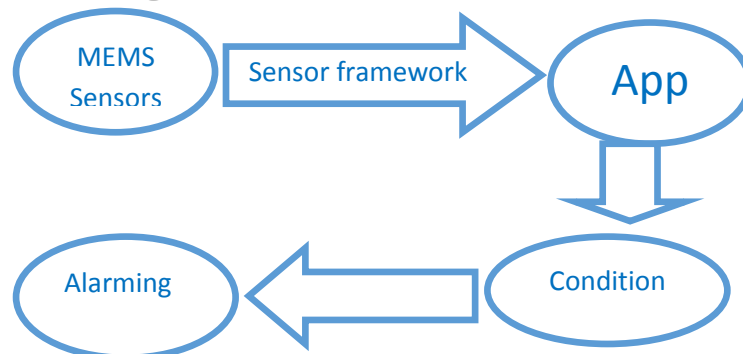


Fig. (12): shows the app architecture

6- The communication between the smartphones

The app will be designed in a Master – Slave architecture where 3 smartphones that pre-installed the app will monitor the environmental characteristics and send the data into the Master smartphone that is receiving the data from the slaves continuously. The connection between the smartphone devices is going to be through the Bluetooth wireless network where this network is suitable for this kind of applications.

7- The communication with the Home PC

After the smartphones are connected the Master Smartphone must be connected to the Home PC using the Client-Server architecture. The PC and the Master Smartphone will be on the same router in order to accomplish the communication locally. A program has to be built in Java programming language in order to receive the incoming alarming signal from the Master Smartphone network architecture can be used. In general network architecture is fall into 2 basic types, the peer-to-peer architecture, and the client – server architecture. In this research the proposed technique is using the client- server architecture. The master smartphone when gained data from environment and other smartphones it should forward the data to a server (PC) that runs in the same network environment. The connection will be made through the socket, the socket in the Network acting as the Door of the house, all the connection that were in and out from the devices in the network are made through there socket.

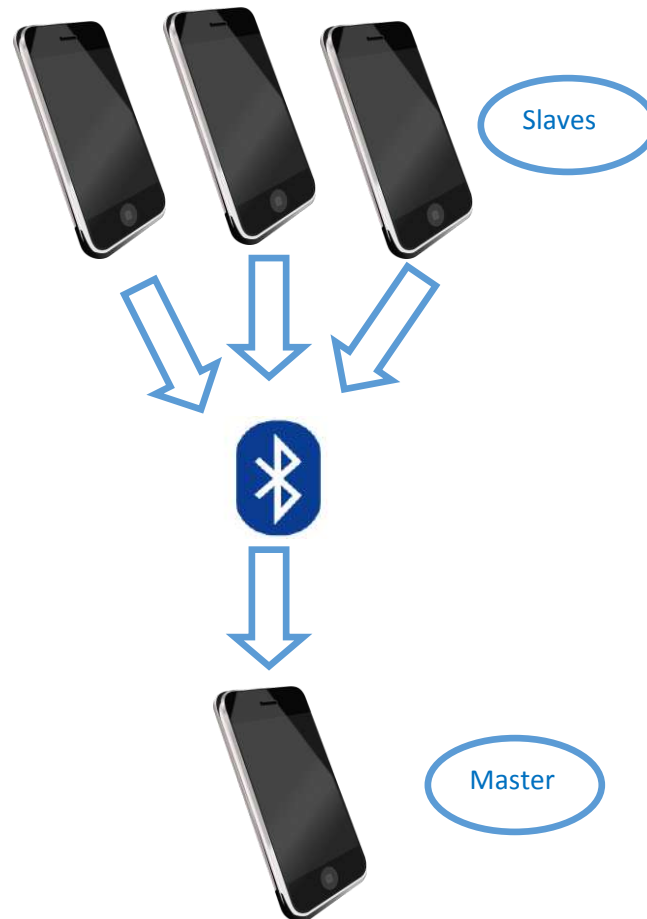


Fig. (13): shows the connection between the smartphones

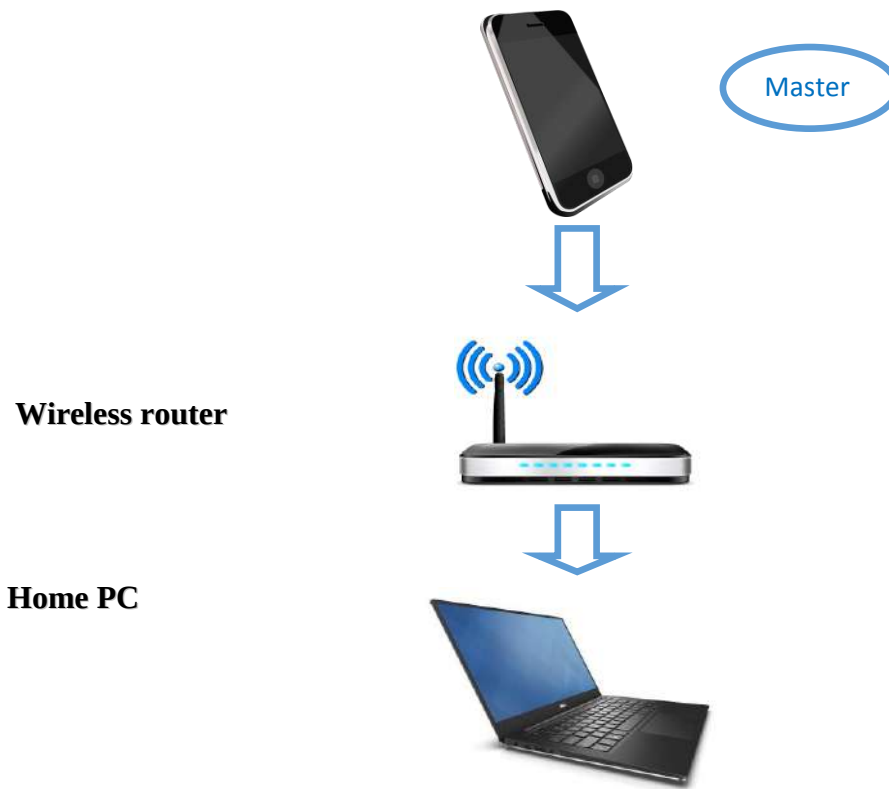


Fig. (14): shows the client-server arch. In the system

8- Programming Strategy

For example of smartphones an Android based OS smartphones are chosen (since they are the most widely spreader around the world) [9]. And the server that going to be created is made using Java programming language (in order to achieve compatibility between the smartphone app and the java program because they are all java based). There are several android app development Environments that can be used to developed android app (eclipse, android studio, Visual Studio with Xamrin) installing any one of the mentioned IDE's and with the Software Development Kit (SDK) that installed from the official website of the android developer. Another basic requirement is the Java Development Kit (JDK) and can be downloaded easily from the official Oracle Website. After all the requirements is satisfied, the programming is going underway. The programming needs a specific requirement for starting the programming such as a 4GB of ram and 1GB of Graphic card in order to deal with the graphical layouts and a flexible and good hard drive space in order to fit with the expansion changing in the programming.

9- Applications

There are many applications that can make use of the remote data transfer between the smartphone sensor and the PC. These applications can be summarized as follows:

- 1- alarming: such a system are used to alarming from incoming threats
- 2- warning from problems: if there is any problems with the car the system can simply diagnosis were the problem is
- 3- In case of accident the smartphones can use the 3G Technology to transfer the Alarm into a central server that could act and locate the accident location.
- 4- Monitoring: this system can be used for monitoring the environmental characteristics and make use of the m in scientific research.

References

- [1] Joe Decuir, Bluetooth 4.0: Low Energy, IEEE Region, CSR plc. 2010.
- [2] HP, Bluetooth wireless technology basics, found at <http://www.hp.com/ctg/Manual/c00186949.pdf>
- [3] Ming Liu, "A Study of Mobile Sensing Using Smartphones", University of Electronic Science and Technology of China, Chengdu, 2013.
- [4] Prime faraday partnership "An Introduction to MEMS (Micro-electromechanical Systems)", Loughborough University, 2002.
- [5] M.Sc. Maximilian Schirmer, "Smartphone Hardware Sensors", mobile media group.
- [6] Dr. Lynn Fuller," Smart Phone MEMS Labs", ROCHESTER Institute of Technology Microelectronic Engineering, 2013
- [7] Ryan Z. Amick¹ Jeremy A. Patterson² Michael J. Jorgensen¹, "Sensitivity of Tri-Axial Accelerometers within Mobile Consumer Electronic Devices", Department of Industrial and Manufacturing Engineering, Wichita State University, Wichita, KS, 2013.
- [8] Dr. Thomas F. Marinis, "The Future of MEMS", Draper Laboratory chnology Square, Cambridge, 2011.
- [9] Chris Thompson, Jules White, Brian Dougherty, Adam Albright, and Douglas C., **Using Smartphones to Detect Car Accidents and Provide Situational Awareness to Emergency Responders.** Vanderbilt University. Nashville, TN USA, found at www1.cse.wustl.edu/~schmidt/PDF/wreckwatch.pdf
- [10] Chi-Yuan Lee, Chien-Hen Lin and Yi-Man Lo, "Fabrication of a Flexible Micro Temperature Sensor for Micro Reformer Applications", Department of Mechanical Engineering, Yuan Ze Fuel Cell Center, Yuan Ze University, Taiyuan,, 2011.
- [11] Richard Teeuw, Martin Whiteside, Nicholas McWilliam, and Paul Zukowskyj, " Field Techniques: GIS, GPS and Remote Sensing ". Geography Outdoors, 2005.
- [12] Jay Esfandyari, Roberto De Nuccio, Gang Xu, "Introduction to MEMS Gyroscope" STMicroelectronics, 2010.
- [13] Agustín L. Herrera-May, Luz A. Aguilera-Cortés ², Pedro J. García-Ramírez ¹ and Elías Manjarrez, "Resonant Magnetic Field Sensors Based On MEMS Technology", sensors ISSN 1424-8220, 2009.

A Review of Personalization Techniques for Recommender Systems

Asst. Prof. Dr. Ahmed Hashim Mohammed¹

Ahmed Rashid Abdullah²

Mustansiriyah University, College of Education

¹ dr.ahmedh@outlook.com

² Ahmad.rasheed1@yahoo.com

Abstract:

Today numbers of ecommerce users who make day to day transactions are increasing. The largest E-commerce sites offer millions of products for sale. Choosing among so many options is challenging for consumers. This rapid expansion has resulted in new challenges to both companies as well as customers. Customers are overloaded with multiple choices for a specific product, which results in a confused and lost state.

Personalized recommendation is the key technology to solve some of the challenges that face and affect the performance of Ecommerce system. This paper mainly introduces personalized recommendation system and its role as well as it discusses several widely used recommendation technologies through comparing and analyzing the strengths and weaknesses of recommendation technology, and also through discussing some of the issues and challenges that are found when applying these recommender systems.

Keywords: Personalization, recommender systems, Ecommerce.

1. Introduction

The World Wide Web (www) is a popular and interactive medium to disseminate information today. The ability to track user's web surfing behavior down to individual mouse clicks has brought the e-commerce and customer closer than ever before. It is now possible for e-commerce vendor to personalize the product message for individual customers at a big scale which is referred as Personalization. **Personalization** is an attempt at addressing a service provider's desire to push additional information to users visiting their domains while at the same time restricting the flow of irrelevant recommendations. This is achieved by predicting a user's requirements and needs so that accurate results can be generated during the course of a user's web navigation. Different personalization systems give somewhat different recommendations based on the type of web data they collect and the methods they choose to employ for analyzing and generating recommendations [1]. In general, the process of obtaining personalized information involves a few steps as shown in figure (1) [2].

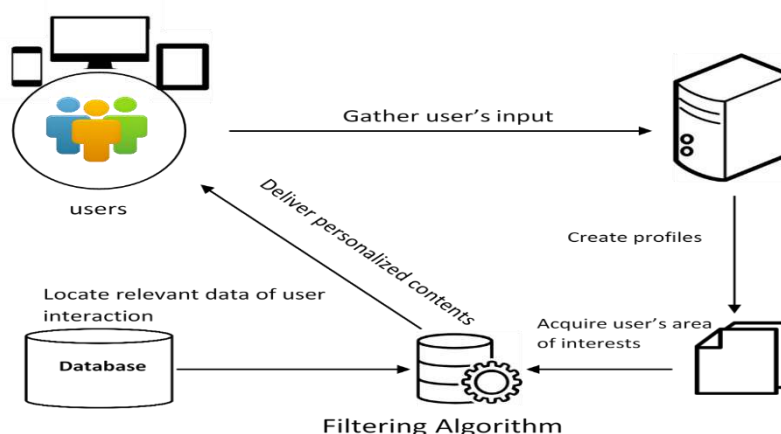


Fig. (1): General architecture of web personalization [2]

Current personalization efforts depend mostly on feedbacks provided by users. Information obtained with such approach is known as **explicit input**. Explicit input plays a much passive role in

the process. One typical example is to request users to give rating based on the degree of interests they have towards a particular product. One major problem with this approach is that web sites which personalize with such method usually find themselves having information that is already obsolete about the users. This is understandable since most users are reluctant to provide feedbacks as hoped for by Web sites owners, which led to an infrequent updates of user information[2].

Realizing the limitations of using explicit input, researchers have sought to look at alternative ways, e.g. using implicit input. **Implicit input** refers to information gathered in an unobtrusive manner. For instance, the time a reader takes to go through an article, or the browsing sequence or browsing habits of a given user. Such an approach can benefit any personalization system as every interaction of the users can be utilized to better understand the users' needs (). Furthermore, the use of implicit input removes the burden of explicitly providing feedbacks. By this approach, personalized content can be delivered to the users at virtually no cost. Consequently, effort of personalization will be considered as a value added service, which is an important element in attracting returning visits from users. These repeating visits can be particularly valuable for businesses, as it fertilizes the growth in sales.

The remainder of this paper is as follows: in **Section 2** we will present some related works of the personalized recommending systems. In **section 3**, we will give a brief introduction about recommending systems and its role in personalization, types of recommending systems and also we will show some advantages and disadvantages of these techniques. Challenges and issues facing us in recommending systems will be covered in **section 4**. Finally, in **Section 6**, we give our conclusion.

2. Personalized Recommending Systems

The largest E-commerce sites offer millions of products for sale. Choosing among so many options is challenging for consumers. Recommender systems have emerged in response to this problem. A Personalized recommender system for an E-commerce site receives information from a consumer about which products he/she is interested in, and recommends personalized products that are likely to fit his/her needs or interests.

The job the of recommender systems is to support the user in the search process by providing personalized recommendations or meta information such as ratings and user reviews to make Internet based shopping easier [3].

One of the interesting applications of personalization on web is the recommender systems. A recommender system basically delivers personalized content to users in the form of suggestions. A typical example is in which recommender systems can retrieve a list of interesting links that are relevant to a given user, and posting it on the user's first page or the list of links can appear in a separate window in order to attract the attention of that user.

Hence, a given recommender system basically performs several tasks which include [2]:

1. learning of user interests.
2. storing the information learned from users.
3. filtering relevant contents based on stored information.
4. suggesting users of the filtered contents.

Recommender systems are generally used by E-commerce sites for suggesting various products to their consumers and also to provide them with information to help them decide which products to purchase. The products suggested can be chosen based on best sellers on a site, on the locality of the consumer, or on basis of the previous buying pattern of the consumer as a prediction for future buying behavior. Various forms of recommendation consist of suggesting products to the consumer, presenting tailor made product information and providing community reviews.

Recommender systems increase E-commerce sales in three ways:

1. **Convincing Browsers into Buyers:** Recommender systems can persuade consumers to find products they wish to purchase.
2. **Increasing Cross-sell:** Recommender systems improve sales by suggesting extra products for the customer to purchase. If the recommendations are good, it will increase the average order size.

3. Building Loyalty: In a world where a site's rivals are only few clicks away, acquiring consumer loyalties is an essential business strategy. Recommender systems develop loyalty by building a value-added relationship between the site and the consumer. Sites often make investment in learning about their consumers, use recommender systems to learn consumer behavior, and to develop powerful custom interfaces that match consumer needs[4].

3. Types of Personalized Recommender Systems

Basically personalization recommender systems can be divided into two main traditional categories: collaborative-filtering systems and content-filtering filtering systems.

3.1 Collaborative-Filtering Systems

(CF-based) techniques can be grouped into two general classes: memory-based and model-based[5]. Memory-based techniques basically are heuristics that make rating predictions based on the entire collection of previously rated items by the users, which include user-based and item-based CF approaches[6]. The model-based CF algorithms use the existing ratings to build a model which is then used to make predictions for un-rated items. Building a model is a fundamental step for the model-based recommendation techniques.

3.2 Content-Based Recommender Systems

The task of a recommender system is to help customers to quickly identify items of interest from a large number of choices. An intuitive way to achieve this goal is to find items that have similar attributes to those previously preferred by a user; this information is usually stored as a content-based user "profile" [7].

3.3 Context-Aware Systems

Context is the information about the environment of a user and the details of situation he/she is in. Such details may play much more significant role in recommendations than ratings of items, as the ratings alone don't have detailed information about under which circumstances they were given by users. Some recommendations are more suitable to the user in evening and doesn't match his preferences in the morning at all and he/she would like to do one thing when it's cold and completely another when it's hot outside. The recommender systems that pay attention and utilize such information in giving recommendations are called context-aware recommender systems. One of the biggest problems of context-aware recommender systems is obtaining context information. The information can be obtained explicitly by directly interacting with user asking him/her to fill out a form and making a survey [8]. Although it is mostly desirable to obtain context information without making the whole rating and reviewing process complicated. Another way is gathering information implicitly using the sources like **GPS**, to get location, or a timestamp on transaction[9]. The last way of information extraction is analyzing users and observing their behavior or using data mining techniques.

3.4 Hybrid Recommender Systems

To achieve higher performance and overcome the drawbacks of the recommendation techniques, a hybrid recommendation technique that combines the best features of two or more recommendation techniques into one hybrid technique has been proposed. According to [10], there are many basic hybridization mechanisms of combinations used in recommender systems to build hybrids:

1. **Weighted:** scores of each of the recommendation approaches are combined numerically to produce a single prediction [11].
2. **Mixed:** results from different recommendation approaches are presented together, either in a single presentation or combined in separate lists [12];
3. **Switching:** one of the recommendation approaches is selected to make the prediction when certain criteria are met using decision criteria[13];

The table (1) compares the advantages and disadvantages of Collaborative filtering and Content-based recommendation approaches. [14]

4. Issues and Challenges in Personalized Recommending Systems

This section investigates issues and challenges in recommender systems and presents different solutions provided by researchers to handle these issues.

Table (1) show a brief comparison between CF and CB recommendation systems

Recommendation technologies	Advantage	Disadvantage
Collaborative filtering (CF) recommendation	It can make recommendation across types; there is no need of domain knowledge and others' experiences are shared; and it has good self-adaptability. Along with time, the recommendation quality shall be improved. Sufficient implicit feedback can reduce users' quantity of feedback and accelerate the personalized study. It works for any type of items without the need to extract textual descriptions related to the items.	Cold start problem, sparsity problem, new-user problem, the problem that quality is decided by history dataset; and bad recommendation quality when a system starts.
Content-based (CB) recommendation technology	a CB recommender system would be able to recommend new items and unpopular items. Furthermore, it does not need to have information about preferences of other users in making recommendations, so it does not suffer from the rating sparseness problem.	The sparsity problem, new user problem; complex properties that are not easy to be handled; the need of adequate data structure categorizer.

4.1 Cold Start Problem

4.2 Synonymy

Synonymy arises when an item is represented with two or more different names or entries having similar meanings[15]. In such cases, the recommender cannot identify whether the terms represent different items or the same item. For example, a memory-based CF approach will treat "comedy movie" and "comedy film" differently. To alleviate the problems of synonymy, different techniques including ontologies[16], the Single Value Decomposition (SVD) techniques, and Latent Semantic Indexing (LSI) could be used.

4.3 Shilling Attacks

What happens if a malicious user or competitor enters into a system and starts giving false ratings on some items either to increase the item popularity or to decrease its popularity[17]. Such attacks can break the trust on the recommender system as well as decrease the performance and quality of recommenders. This threat is of more concern in CF techniques but lesser threat to the item-based CF technique.

4.4 Grey Sheep

Grey sheep occurs in pure CF systems where opinions of a user do not match with any group and therefore, is unable to get benefit of recommendations[15]. Pure CB filtering can resolve this issue where items are suggested by exploiting user personal profile and contents of items being recommended. Grey sheep users can be identified and separated from other users by applying offline clustering techniques including k-mean clustering[18].

4.5 Sparsity

In online shops that have a huge amount of users and items there are almost always users that have rated just a few items. Using collaborative and other approaches recommender systems generally create neighborhoods of users using their profiles. If a user has evaluated just few items, then it's pretty difficult to determine his taste and he/she could be related to the wrong neighborhood. Sparsity is the problem of lack of information[6].

To cope with this situation, several approaches can be used including multidimensional recommendation model [19], SVD techniques[20], demographic filtering[21], and using content-boosted CF algorithm [22].

4.6 Scalability

With the growth of numbers of users and items, the system needs more resources for processing information and forming recommendations. Majority of resources is consumed with the purpose of determining users with similar tastes, and goods with similar descriptions[8].

The problem can be addressed by reducing dimensionality through SVD by pre-processing that combines clustering and content-analysis with CF algorithms [23].

4.7 Latency Problem

CF recommenders face latency problem when new items are added more frequently to the database, where the recommender suggests only the already rated items as the newly added items are not yet rated. Using CB filtering can reduce waiting times but it may introduce overspecialization. To cope with this situation, the category based approach in combination with the user stereotype can be used[24]. To further increase performance, several clustering techniques[25]. can be applied and calculations can be made offline. Model-based CF approaches can also enhance the scalability and performance.

4.8 Evaluation and the Availability of Online Datasets

The available evaluation metrics are for general-purpose recommenders and are not applicable in different domains especially in evaluating context-aware recommenders.

Another issue related to RS, is the non-availability of benchmark dataset that can be used in evaluating a recommender system in a particular domain. Such datasets are important as their availability encourages research and development of recommenders. Most of the available datasets are proprietary and therefore, cannot be used as benchmark datasets especially in evaluating context-aware recommenders. Fortunately, some datasets have been released for evaluating context-aware recommenders that include Food, Movie and LDOS-CoMoDa1[10].

In table (2) below, we present the latest research papers for different researchers who have worked in the recommending systems field. This table gives much information about the researcher name and the year of the published work. In addition to that, we have shown the method that has been implemented with the technology. Application column shows the field the research work has designed for.

Table (2) lists a collection of researches have been done in the domain of personalized recommender systems.

	researcher	Year	Method	Technology	Application
1	Zhongqi Lu et al.[26]	2015	hybrid	Clustering	News Recommendation
2	Koren et al. [27]	2009	collaborative filtering	matrix factorization	Movies recommender
3	Jose San Pedro[28]	2014	collaborative filtering	Bayesian approach	Question Recommendation
4	Aaron van den Oord et al.[29]	2013	Content-based	latent factor model	music recommendation
5	Kawai et al. [40]	2016	hybrid	Non-negative matrix factorization	movie recommendation
6	S.Pandya et al. [30]	2016	hybrid	Combining clustering with Eclat Algorithm	E-commerce
7	Astha Sharma et al.[31]	2016	Context-aware	machine learning	General.
8	Praveena Mathew et al.[32]	2016	hybrid	association rule mining	Books Recommendation
9	CHHAVI RANA[33]	2012	Content-base	Data mining	online book shopping
10	Jian Wei et al.[34]	2016	collaborative filtering	Neural network SADE	Netflix movie recommendation
11	Titipat Achakulvisut et al. [35]	2016	Content-Based	e Latent Semantic Analysis (LSA)	Scientific Publications recommendation
12	Mojtaba Salehi et al.[36]	2012	collaborative filtering	sequential pattern mining	e-learning systems
13	Li Sa [37]	2011	Collaborative filtering	Clustering	E-commerce
14	Mingsong Mao[39]	2015	hybrid	bipartite graph random walk model	E-commerce
15	Yoon Ho Cho[38]	2004	Collaborative filtering	Web usage mining	E-commerce
16	ZhengXian Li[39]	2016	hybrid	machine learning	recipe recommendation
17	Cyrus Shahabi[23]	2001	Collaborative filtering	Classification	Web based application
18	Heng Tang[40]	2013	Context-aware	mining multidimensional sequential rules	Mobile Personalized Marketing

5. Conclusion

Web recommendation systems are used to recommend pages to users. These systems can be used for personalized recommendation to give personalized recommendation based on users browsing history. Throughout this paper we have discussed many aspects of web personalized recommendation systems. We have shown a comparison between the main types of recommendations, also we presented a related works and problems associated with existing recommendation systems.

References

- [1] P. S. Lokhande and B. B. Meshram, "Analysis and Design of Web Personalization Systems for E-Commerce", no. 1, pp. 187–193, 2015.
- [2] P. Y. JYH, "Web Personalization Using Implicit Input", no. June, 2006.
- [3] M. Wium, "Design and Evaluation of an Personalized Mobile Tourist Application", Dep. Comput. Inf. Sci., vol. Master, no. June, p. 86, 2010.
- [4] D. Agarwal, S. P. Tripathi, and R. P. Agarwal, "Web Personalization and Recommendation Model for Trust in E-Commerce Websites From an Indian Perspective", 2013.
- [5] Y. Shi, M. Larson, and A. Hanjalic, "Collaborative Filtering beyond the User-Item Matrix : A Survey of the State of the Art and Future Challenges", ACM Comput. Surv., vol. 47, no. 1, pp. 1–45, 2014.
- [6] B. Sarwar, G. Karypis, J. Konstan, and J. Riedl, "Item-based collaborative filtering recommendation algorithms", Proc. 10th ..., vol. 1, pp. 285–295, 2001.
- [7] V. V. Kumari, "a C Ategorical R Eview of R Ecommender S Ystems", vol. 3, pp. 73–83, 2012.
- [8] U. H. Wanaskar, S. R. Vij, and D. Mukhopadhyay, "A Hybrid Web Recommendation System Based on the Improved Association Rule Mining Algorithm", J. Softw. Eng. Appl., vol. 2013, no. August, pp. 396–404, 2013.
- [9] L. Baltrunas and X. Amatriain, "Towards time-dependant recommendation based on implicit feedback", Work. Context. Recomm. Syst., pp. 25–30, 2009.
- [10] Y. Zheng, R. Burke, and B. Mobasher, "Splitting approaches for context-aware recommendation", Proc. 29th Annu. ACM Symp. Appl. Comput. - SAC '14, pp. 274–279, 2014.
- [11] B. Mobasher, R. Cooley, and J. Srivastava, "Web usage mining can help improve the scalability, accuracy, and flexibility of recommender systems.", Commun. ACM, vol. 43, no. 8, pp. 142–151, 2000.
- [12] B. Smyth and P. Cotter, "A personalized television listings service", Commun. ACM, vol. 43, no. 8, pp. 107–111, 2000.
- [13] Billsus Daniel and Pazzani Michael J., "User modeling for adaptative news access. ", User Model. User-adapt. Interact., vol. 10, pp. 147–180, 2002.
- [14] L. Ya, "The Comparison of Personalization Recommendation for E-Commerce", Phys. Procedia, vol. 25, pp. 475–478, 2012.
- [15] X. Su and T. M. Khoshgoftaar, "A survey of collaborative filtering techniques", Adv. Artif. Intell., vol. 2009, no. Section 3, pp. 1–19, 2009.
- [16] A. Lau, E. Tsui, and W. B. Lee, "An ontology-based similarity measurement for problem-based case reasoning", Expert Syst. Appl., vol. 36, no. 3 PART 2, pp. 6574–6579, 2009.
- [17] I. Gunes, C. Kaleli, A. Bilge, and H. Polat, "Shilling attacks against recommender systems: a comprehensive survey", Artif. Intell. Rev., vol. 42, no. 4, pp. 767–799, 2012.
- [18] M. A. Ghazanfar and A. Pr??gel-Bennett, "Leveraging clustering approaches to solve the gray-sheep users problem in recommender systems", Expert Syst. Appl., vol. 41, no. 7, pp. 3261–3272, 2014.
- [19] G. Adomavicius, R. Sankaranarayanan, S. Sen, and A. Tuzhilin, "Incorporating contextual information in recommender systems using a multidimensional approach", ACM Trans. Inf. Syst., vol. 23, no. 1, pp. 103–145, 2005.
- [20] D. Billsus and M. J. Pazzani, "Learning collaborative information filters", Proc. Fifteenth Int. Conf. Mach. Learn., vol. 54, p. 48, 1998.
- [21] G. Adomavicius and A. Tuzhilin, "Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions", IEEE Trans. Knowl. Data Eng., vol. 17, no. 6, pp. 734–749, 2005.
- [22] P. Melville, R. J. Mooney, and R. Nagarajan, "Content-Boosted Collaborative Filtering", Proc. 2001 SIGIR Work. Recomm. Syst., p. 9, 2001.

- [23]C. Shahabi, F. Banaei-Kashani, Y. Chen, and D. McLeod, "**Yoda: An accurate and scalable web-based recommendation system**", Coop. Inf. Syst., no. September, pp. 418–432, 2001.
- [24]M. Sollenborn and P. Funk, "**Category-based filtering and user stereotype cases to reduce the latency problem in recommender systems**", Adv. Case-Based Reason., no. September, pp. 395–405, 2002.
- [25]B. Mobasher, H. Dai, T. Luo, and M. Nakagawa, "**Improving the Effectiveness of Collaborative Filtering on Anonymous Web Usage Data**", Proc. IJCAI 2001 Work. Intell. Tech. Web Pers., pp. 2010–9, 2001.
- [26]Z. Lu, Z. Dou, J. Lian, X. Xie, and Q. Yang, "**Content-based collaborative filtering for news topic recommendation**", AAAI 2015 Proc. Twenty-ninth AAAI Conf. Artif. Intell., pp. 217–223, 2015.
- [27]Y. Koren, R. Bell, and C. Volinsky, "**coverfeature matrix techniques for**", pp. 30–37, 2009.
- [28]J. S. Pedro and A. Karatzoglou, "**Question Recommendation for Collaborative Question Answering Systems with RankSLDA**", RecSys, pp. 193–200, 2014.
- [29]A. van den Oord, S. Dieleman, and B. Schrauwen, "**Deep content-based music recommendation**", Electron. Inf. Syst. Dep., p. 9, 2013.
- [30]J. M. Shah and L. Sahu, "**A Hybrid Based Recommendation System based on Clustering and Association**", vol. 5, pp. 36–40, 2015.
- [31]A. Sharma, S. Krishnan, S. Raj, and M. K. Sharma, "**Context Aware Smart Recommendation using Social Network Influences**", vol. 6, no. 4, pp. 4669–4671, 2016.
- [32]M. P. Mathew, M. B. Kuriakose, and V. Hegde, "**Book Recommendation System through Content Based and Collaborative Filtering Method**".
- [33] C. Rana and S. K. Jain, "**Building a book recommender system using time based content filtering**", WSEAS Trans. Comput., vol. 11, no. 2, pp. 27–33, 2012.
- [34] J. Wei, J. He, K. Chen, Y. Zhou, and Z. Tang, "**Collaborative filtering and deep learning based recommendation system for cold start items**", Expert Syst. Appl., vol. 69, pp. 1339–1351, 2017.
- [35] T. Achakulvisut, D. E. Acuna, T. Ruangrong, and K. Kording, "**Science Concierge: A fast content-based recommendation system for scientific publications**", PLoS One, vol. 11, no. 7, pp. 1–11, 2016.
- [36] M. Salehi, I. Nakhai Kamalabadi, and M. B. Ghaznavi Ghouschi, "**Personalized recommendation of learning material using sequential pattern mining and attribute based collaborative filtering**", Educ. Inf. Technol., pp. 1–23, 2012.
- [37] L. Sa, "**Collaborative filtering recommendation algorithm based on cloud model clustering of multi-indicators item evaluation**", Proc. 2011 Int. Conf. Bus. Comput. Glob. Informatiz. BCGIn 2011, pp. 645–648, 2011.
- [38] Y. H. Cho and J. K. Kim, "**Application of Web usage mining and product taxonomy to collaborative recommendations in e-commerce**", Expert Syst. Appl., vol. 26, no. 2, pp. 233–246, 2004.
- [39] Z. Li, J. Hu, J. Shen, and Y. Xu, "**A Scalable Recipe Recommendation System for Mobile Application**", 2016 3rd Int. Conf. Inf. Sci. Control Eng., pp. 91–94, 2016.
- [40] H. Tang, S. S. Liao, and S. X. Sun, "**A prediction framework based on contextual data to support Mobile Personalized Marketing**", Decis. Support Syst., vol. 56, no. 1, pp. 234–246, 2013.

Cloud Based Iraqi E-Government

Lecturer. Rawaa M. Abdulhussein Asst. Prof. Dr. Ahmed H. Mohammed
Mustansiriyah University
mescrawaahm@gmail.com dr.ahmedh@outlook.com

Abstract:

Internet applications and its wide spread use by people initiate the idea of cloud computing that give completely different type of services to the users like hardware or software as a service. This trend leads the government to exploit technology in providing better services to their citizens. Using cloud computing in building e-government is considered as a promising technology which takes the importance of many researchers and developed countries around the world in the recent years due to its easy implementation and less expenditures, green effect to the environment, better resource utilization. cloud environment enable superior partnership capabilities easy scalable and better disaster upturn capabilities because it relay on virtual machine environment, so if any error happen in one of the resources, the whole system will not be affected.

This paper proposes to use cloud computing technology in designing E-Government in IRAQ by using three suggested scenario that is different either in the number of data centers used or in the location of these data centers, these scenarios consider three regions in IRAQ the north, middle and the south denoted by R1 R2 R3 respectively. These scenarios are simulated by using cloud simulator analyst, by comparing the response time of each one separately; a final recommendation is introduced that consider the lower latency scenario as the most effective one.

I. Introduction

As it is obvious how the applications of government is different and various and sometime relay on each other, so if these application can be introduced to the people with transparency and in a simplest way, this will enhance the function of the whole nation. E-Governance means making use of technology to produce better services to the citizens. E-government can be classified as Government-to-Government, Government-to-Business, Government to Consumer, and Government to Employees [1].

The idea of using cloud computing in e-government is adapted by developed country recently as it provides consistent e-Governance, cheap IT setups and many other advantages [2].

Cloud computing means using common networking standards and internet protocols to access virtualized resources distributed on network that make the physical systems hidden from the user who benefit from the services and applications of unlimited resources [3]. The NIST define Cloud paradigms as shown in Figure (1) [4].

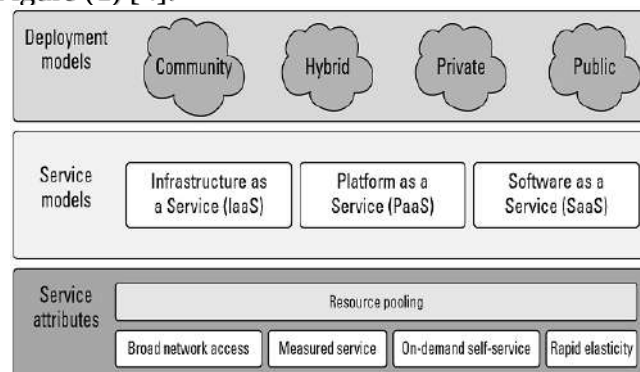


Fig. (1): Cloud paradigm

II. Cloud Characteristics

Cloud systems have the following characteristic which is defined by NIST

A. On-Demand Self-Service

User issues a request via an API virtual resource then cloud computing establish new machine online, the services will be provided as needed each time by the service provider [5].

B. Broad Network Access

There are many devices available such as laptops, PDA, and mobile phones that provide access over the internet, user can use any one of these devices that have different operating systems in order to access cloud which provides independent platform [6].

C. Resource Pooling

It means collecting all the resources in one group then assigning these resources as needed to the users, this action will result in increasing resource utilization with minimum cost [7].

D. Rapid Elasticity

Elasticity is a major notion in cloud computing which refers to the ability of cloud to response dynamically to how much resources are needed and specify the resource that currently consumed, so one of the most common cloud service that amazon provides is named amazon elastic which can provision resources rapidly and elastically [7].

E. Measured Service

The amount of services for both the consumer and the provider should be measured in order to control, report and monitor the resource utilization of the cloud system [4].

II. Cloud Services Model

The client needs nothing to setup on his computer when he aims to access and use the cloud service [8]. The main services that cloud computing delivered to the client as a service are [9].

A. Software

This services is accessed through a web browser by means of the internet such (web-based e-mail) [In this service the user disregard where the software is hosted, what type of operating system it uses, or whether it is written in Java, PHP, or.NET. And, above all else, user don't have to setup a single piece of software anywhere 10-41]. For example, Gmail is nothing more than email software used in a browser. It provides the same services as Apple Mail or Outlook, but without the fat client [8].

B. Platform

It can be defined as progression of web hosting, whereas many companies have provided web hosting service in latest years through complete software stacks for developing web sites, this service takes a step further by providing lifecycle management capabilities to control all software development stages from planning to maintenance [11].

C. Infrastructure

Making the hardware available as a service is one of the important characteristic of cloud system. Hardware is virtualized in the cloud to make virtual storage, virtual machines, virtual infrastructure, and other hardware component [3].

III. E-Government Challenges

A. Practical Challenge

It involves many aspects related to either hardware or software like physical safety of hardware equipment, protection of software, transparency of actions, isolation and interoperability of existing hardware, limiting and controlling the access to authorized party and scalability, these challenges should be taken in the consideration as the number of user increase over time [12].

B. Economical Challenge

As the idea of E- government is new, so all the equipment should be purchased and prepared, saving Revenues can be achieved by accurate and deep planning of project also the applications used by the departments can be reused because this project is applied to the whole country. The economical and technical experts should collaborate to give their advice in order to reduce the cost of this project as least as possible [13].

C. Social Challenge

Every person in the nation will need to make use of the application of e-government; some of these people have very simple knowledge so the government must not forget those people to avoid the difficulties of using the applications of E-government [14].

IV. Cloud Computing Benefits In E-Governance

The challenges of e-governance can be resolved by cloud computing technology as will described in the following sections:

A. Supporting Green Environment

The implementation of e-government by using cloud system is considered as green IT environment, as there are an obvious reduction in the IT infrastructure because the cloud will provide all the required resources (hard ware and software) as a service and exactly as needed by the users[15].

B. Cost Effective

The unification of all the information system in all the centers will reduce the redundant of the equipment and decrease the maintenance effort and upgrades, so a salient reduction in the cost will be produced.

C. Availability Service

Ensuring continuous service at all the time especially in the situations like natural disasters is a key demand for E-Government system, cloud computing ensure the availability of the services by implementing backups in the data centers which are located in different regions, so even if a natural disaster take place in any region, the service will be provided from another data center in another location [14].

D. Policy Management

The security and integrity of different application in E-Government is the main factor to ensure soft administration of the government policy, the different policies is integrated between different data centers then all the people will be constrained by the government policy.

E. Quality of Service

this feature helps to increase the process of completing the user request then avoiding needless expenditures of resources. The management, monitoring and maintenance in cloud environment is uncomplicated, because it is administrated by particular experts, this will limits the number of user errors and ensure accurate service response.

F. Scalability

As E-Government interact directly with people so the number of users will increase over a time, without previous consideration the system cannot adapt to the over load and this result in decreasing resource utilization of the system. Whereas in cloud computing the system dynamically assign as much resources as needed resulting in better resource utilization [16].

V. Proposed Model

IRAQ begin to plan for E-Government by using information and communications technology to improve the foundations of good governance through the provision of services to citizens and the business sector and civil society institutions.

The main role of e-government is to meet the public's needs for high quality and accessible services and to increase transparency and efficiency in state administration. Iraq harnesses ICT tools to improve basic services and to promote all-round good governance including increased public participation, better social equity and justice as well as general enhancement of the effectiveness of public institutions. Many e-government have been implemented since the launch of the first version of the strategic action plan for electronic governance in April 2010. This plan includes the first program for training the presidents trainers in Amman in July 2010, which was followed by the launch of the national program to train e-governance in many training centers in all parts of Iraq. Until the end of 2010 nearly 3,000 government employees were trained around the country, the second train was for the training of master trainers, led by the Iraqi government and the support of the United Nations Development Program to train 200 major coach in a series of five training programs conducted during the period from September until the end of 2011 then the national program train 10,000 government employees with the end of 2012.

Depending on a real statistic that takes the actual population of Iraqi people in each province, a suggestion is made to group them into three regional areas.

The ministry Iraqi planning in 2014 showed that after Baghdad (7) million the population of Nineveh province was the next with (3.5) million and Basra (2.750) million, while the number of

residents of the province of Kurdistan for three provinces (Arbil, Sulaymaniyah and Dohuk) was (5) million. The other provinces Kirkuk (1.5) million, Diyala (1,548) million, Anbar (1.675) million, Babylon (1.953) million, Karbala (1.151) million, Wasit (1.303) million, Salahaldean (1.509) million, Najaf (1.389) million, Diwaniyah (1.220) million, DhiQar (1.979) million, and Maysan (1) million in 2014.

Depending on this Census, three regional areas can be considered: North, Middle, and South with 11.509, 12.793, and 11.562 respectively

The implementation of E-Government using cloud simulator supposes three regional areas (R1, R2, and R3), three parameters (datacenter, user base, regional area) will be specified and interoperated to produce three different scenarios. The first one use one data center to the whole country located in region2 which is the middle region as shown in figure (2) and the second scenario model put three data centers located in one region as shown in figure (3) and the final scenario supposes using separate data center to each area located inside each region as shown in figure (4).

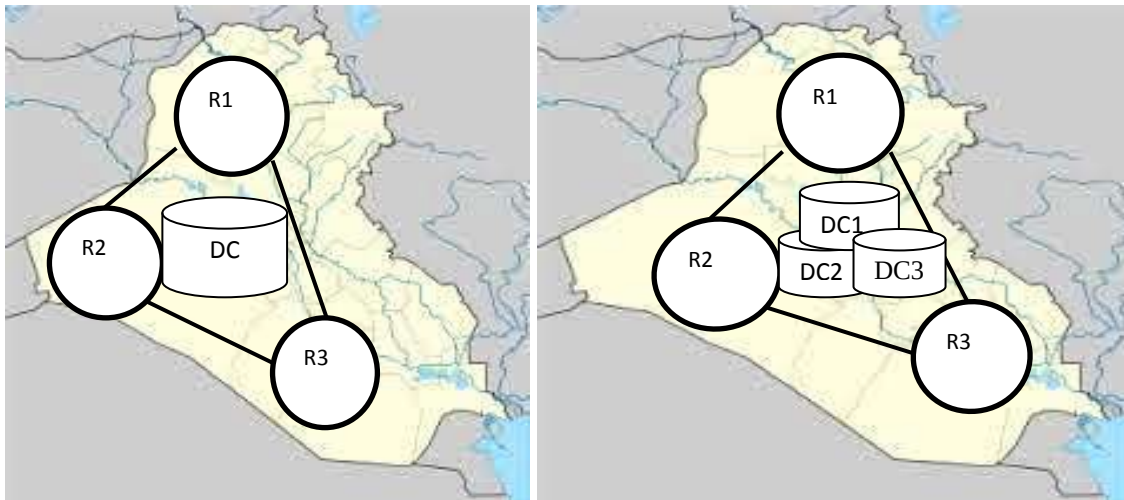


Fig. (2): Scenario One Fig. (3): Scenario Two

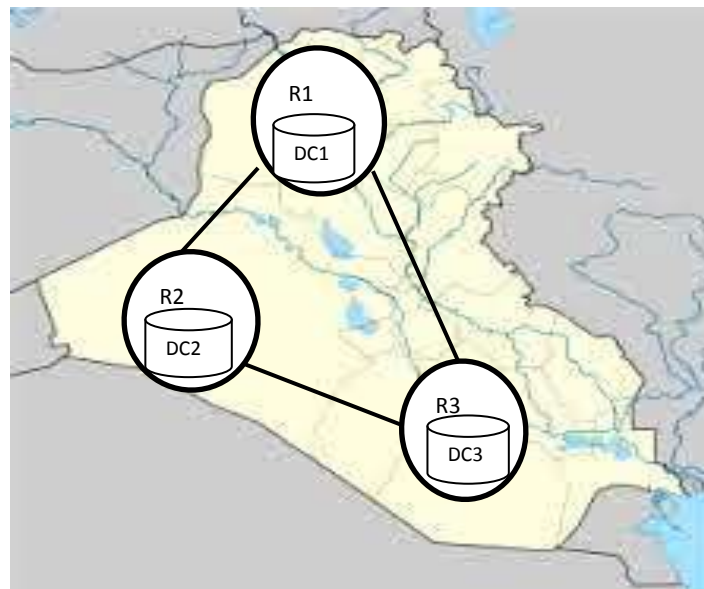


Fig. (4): Scenario Three

Cloudsim is embedded with three service broker policies (Nearest Datacenter Policy, Optimize Response Time Policy and Dynamically reconfigurable routing with load balancing) of data center brokers to determines which data center should be selected to provide services to requests from the user base.

The scheduling algorithm used in the simulation was nearest data center algorithm, the obtained result measure the overall response time that will be considered to evaluate the effectiveness of each scenario.

VI. Evaluation of Scenario

In this paper, three scenarios has been simulated using Cloud simulator to check and evaluate the proposed scenarios.

The implementation of this experiment is done by using cloudsim analyst and the configuration parameters which are used in the simulation of the three scenarios can be shown in table (1).

Table (1) Configuration Parameters

Parameter		Values
Virtual Machine	Image Size	10000MB
	Memory	1GB
	Bandwidth	1000bps
Data Center	OS	Linux
	Architecture	X86
	VMM	Xen
	Number of Machines	25
	Memory per Machine	2GB
	Storage per Machine	1GB
	Bandwidth per Machine	1000bps
	Number of processors per machine	5
	Processor Speed	1000MIPS
	VM Policy	Time Shared
Grouping Factor	User Grouping Factor	100000 User
	Request Grouping Factor	10000 Request
	Executable Instruction Length	10000 bytes

After running the simulation of the three scenario, three parameter will be produced which are overall response time, processing speed and finally the total cost.

The overall comparison parameters obtained from the three scenarios independently can be shown in table (2).

Table (2) Scenario Evaluation

	Scenario one	Scenario two	Scenario three
Overall response time (ms)	246.97	132.49	50.26
data center processing speed (ms)	0.37	0.61	0.78
Total Cost of (\$)	\$0.68	\$0.68	\$0.68

The following figures represent each parameter in a separate figure independently in scenario1, scenario2, scenario3.

It is obvious from figure(5) which presents the overall response time that scenario three has the lowest response time with 50.26 ms whereas in scenario two and one it was 132.49 ms, 246.97 ms respectively.

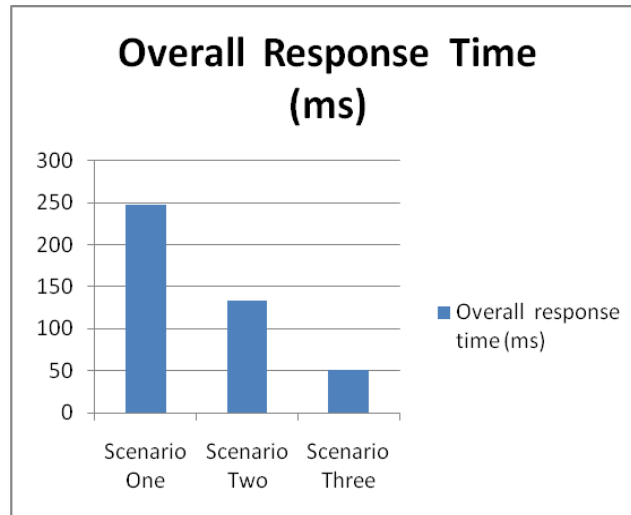


Fig.(5): Overall Response Time

As can be shown from figure (6) that the speed of processing time in scenario three is the highest with (0.78 ms) compared to 0.61ms in scenario two and 0.37 ms in scenario one.

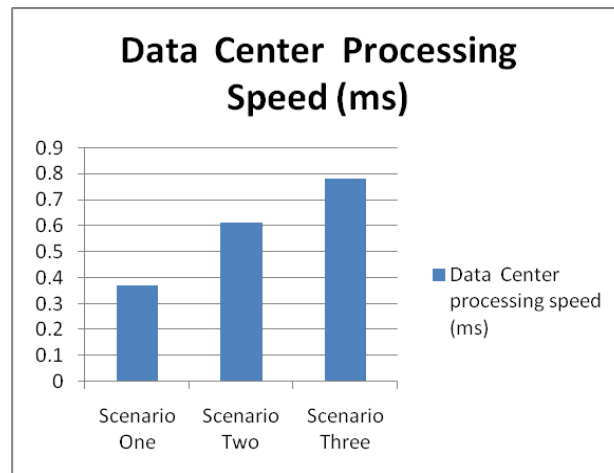


Fig. (6): DC Processing Time

The overall cost of each scenario is present in figure (7). it can be seen here that the cost was the same for the three scenarios, this is because exactly the same number of virtual machine was used in each scenario, which is twenty five virtual machines.

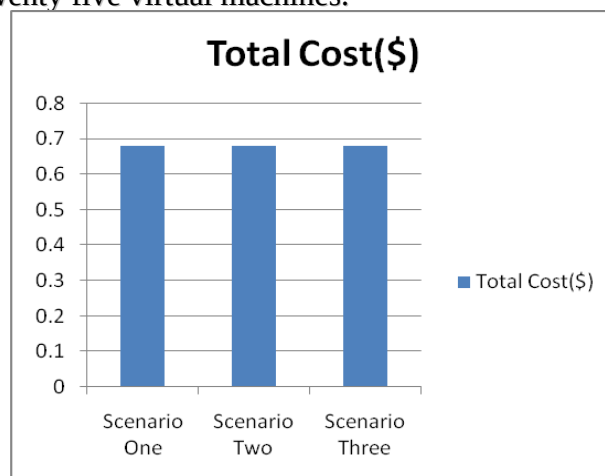


Fig. (7) Overall Cost Each Scenario

After this comparison it is undoubtedly clear that scenario three is the best since it take the lowest time, highest speed with the same cost. Based on this conclusion a final recommendation is given for Iraqi government to consider scenario three to help in implementing well-organized E-Government in IRAQ.

VII. Conclusion

It can be concluded that there are many factors which help to increase the efficiency of cloud computing system one of it is how many data centers to be used and where is the best place for this data center to be located.

From the previous evaluation, it is clear that distributing the data center is far more effective than centralized data center which is implemented in scenario three, this situation is compatible with E-Government function that have distributed and cooperated nature. Therefore for any country it is important to make previous research study of its populations and regional areas to produce best results of e-government cloud based system as well as the benefits of cloud computing technology over the traditional e-government technology.

References

- [1] W. Cellary and S. Strykowski, "E-Government Based on Cloud Computing and Service-Oriented Architecture", Proc. 3rd Int. Conf. Theory Pract. Electron. Gov. ICEGOV '09, vol. 6, no. 3, p. 5, 2009.
- [2] C. Science and S. Engineering, "Cloud Computing Architecture Supporting e-Governance", vol. 2, no. 8, pp. 370–375, 2012.
- [3] B. Sosinsky, Cloud Computing Bible.2011.
- [4] I. Jansch and V. Chin, PHP Development in the Cloud. 2011.
- [5] B. Furht and a. Escalante, Handbook of Cloud Computing [Hardcover]. 2010.
- [6] I. Jansch, and V. Chin, Cloud, Grid and High Performance Computing: Emerging Applications, vol. 27, no. 8. 2011.
- [7] J. Rosenberg and A. Mateos, The Cloud at Your Service. 2011.
- [8] A. Fallis, Cloud Application Architectures, vol. 53, no. 9. 2013.
- [9] T. Mather, S. Kumaraswamy and S. Latif, "Cloud Privacy and Security", Gov. An Int. J. Policy Adm., p. 336, 2009.
- [10] Ronald L. Krutz and R. D. Vines, cloud security a comprehensive guide to secure cloud computing. 2010.
- [11] J. Hurwitz, R. Bloor and M. Kaufman. Cloud Computing FORDUMmIES. Wiley Publishing, Inc., Indianapolis, Indiana, 2010.
- [12] D. Claiborne, J. Rotenstein, and N. Gabrani, Development with the Force. com Platform, Second Edition.
- [13] K. Chaudhari and P. T. Karule, "Electronic Governance for Rural India Based on the Cloud Computing Model for Sustainable Development", vol. 3, no. 3, pp. 43–52, 2014.
- [14] S. Mathew, "Implementation of Cloud Computing in Education - A Revolution", Int. J. Comput. Theory Eng., vol. 4, no. 3, pp. 473–475, 2012.
- [15] H. O. Lee and M. Kim, "Implementing cloud computing in the current it environments of korean government agencies", Int. J. Softw. Eng. its Appl., vol. 7, no. 1, pp. 149–160, 2013.
- [16] IIT, Hyderabad, " Cloud Computing for E-Governance", A white paper, January 2010.

A Review on Fog Computing and Quality of Services (QoS)

Ammar Abdulateef Hadi
Ministry of Science and Technology
alshida1973@yahoo.com

Abstract:

Regardless of the growing needs of cloud computing, many snags still uncrossed consequent to the inherent matters of cloud computing such as limited connectivity, the speed of data transmission between cloud and end user devices and the connections delay. Fog computing, is a cloud computing extension to the edge network, it can address the quality of services (QoS) problems by providing near resources and services to end users, In other words, the position of the fog devices between cloud and end user devices makes a shortcut between the users and resources, which will provide high-speed connections and short distances between the nodes To prevent falling into the hole of bandwidth lake, non-connected nodes that out of coverage area. This review discusses the fog computing as a solution to improve QoS for real-time application, location awareness reliable services, storage capacity.

Keyword: Fog Computing, Cloud Computing, QoS, IoT, Edge Network, Heterogeneous Network, SDN, NFV.

I. Introduction

Recent years CISCO Sparked the Revolution of fog computing to bring the functionality of cloud computing to the network edge [1]. Networking, storage, and computing all of those services located in fog computing as a new paradigm between end users and cloud computing data centers. Fog computing allows edge devices such as routers, access point to host the services. And this technique Reflected positively with applications to run speedily to handle massive data that produced from fog nodes. Comparing with cloud computing, the services and applications hosted in cloud servers which are required a high level of QoS to satisfy the end users. Cloud computing allows the end user to enjoy many benefits, such as the availability of storage resources, unlimited computation, and network communications. However, this appropriate incubator has reflected a problem for applications that requires a high level of QoS [2]. Thus, the idea of fog computing was appeared to place all data at a near place for the end user and distributed it between fog devices, to reduce the service latency, improve QoS and minimize the obstacles of data transfer. And because of the geographical distribution of fog resources, it will be a well poisoned for an application required a high QoS such as data streaming and supports the computing mobility [3].

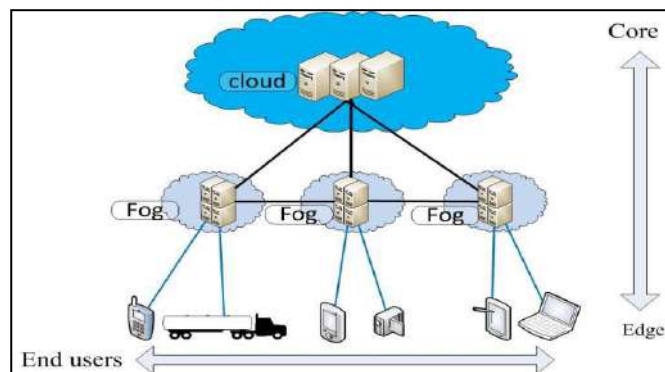


Fig. (1): Fog computing between core and edge

Referring to fig. (1), which illustrates the position of fog nodes as a neighbor to the end users and the physical distance comparing with the cloud servers.

The neighboring and the geographic positions near each others of fog nodes in order to directly communicate with gateway nodes, since the cloud provide the services via the internet. Fog minimizes the feedback latency in order to produce a high processing performance that supports real time applications and big data mining [4]. Video streaming application is one of the

applications that depending on high bandwidth and low latency [5], and it is not efficient to deliver video streaming from just one or two data centers for many end users, fog computing allow to deliver amount of video streaming directly to the end users from neighbor fog nodes [2].

Internet of things (IoT) are an embedded devices connected to the internet to perform a scalable platform, which requires a network services, mobility support and storage capability to serve M2M data processing and storage, for both the fixed IoT and mobile IoT that distributed over the wide geographic area [6]. IoT platform is demand a high level of QoS such as low latency and high bandwidth, additionally to mobility support and availability of storage recourses in order to satisfy the IoT applications as real-time applications, streaming applications, a connected vehicle. Cloud computing infrastructure it is able to meet the requirement of IoT platform. There are many facilities in cloud computing which support an IoT platform but also there are challenges waiting for IoT applications that require a low latency, high bandwidth, mobility support, real-time processing and a wide range of coverage area.



Fig. (2): IoT running via cloud computing

Fog computing is the extension of cloud computing to the edge network. Both of them provide similar services in the context of computation, storage resources, and networking. Furthermore, fog computing has the precedence because of the extra benefits resulted from nearly data position, services recourses and mobility support [1]. Therefore, fog computing allows IoT applications and services running in the edge network so as from end devices such as M2M gateway, routers, access points, smart phones. Consequently, that paradigm will improve QoS [6]. In parallel with, non-consuming of the bandwidth in case of the transmission of data between IoT devices and fog data hosting nodes, because of the localization of fog computing [3], whereas data and services hosted at the edge devices.

In this paper, we will review QoS as an important factor for fog computing, the fog network parameters with management software, the applications of computing and arrest of paper for QoS metrics in fog network.

1. Fog as a network

The number of connected devices will be 50 billion by 2020 as Cisco estimation [7]. The growing of connected devices will be in parallel with the increasing number of IoT devices [8]. Fog network is a heterogeneous network due to positioned at edge network in order to a manage multi kinds of devices, IoT such as Google Glass, Microsoft HoloLens, and smart watches, additionally to the personal mobile devices such as mobile phones, iPad, and tablets. And fog nodes which belong to the infrastructure of edge network (routers, access points, switches, set-top-boxes) [9]. Therefore, fog network responsible for connecting and managing all component of fog in the context of networking, connectivity maintain and services providing in case of IoT at the large scale [10]. The management of such heterogeneous network is complicated in the case without assistance from high-level techniques. Especially, there are a billion heterogeneous end devices which running applications and demanded services from fog nodes or from another edge device due to the concept

of services in everywhere at fog computing. Therefore, the term of network softwareisation has appeared in manner of network management.

A. Network Softwareisation

Because of the huge number of heterogeneous component and services of fog network must completely manage by automated techniques. Software Defined Networking (SDN) and Network Function Virtualization [11] are emerging methods to improve fog network [12]. The combination of emerging software and fog network are to achieve a flexible and dynamic management of network environment. SDN as software handled with hardware to rendering the fog network controllable by software. Every fog node must able to represent a router to the neighbor nodes and do the function of a router to the near nodes, which is mean the end nodes at fog network it can be a controller [2]. The merging of SDN with fog network is to support the mobility of fog nodes and the unreliable of wireless connections. The environment of mobile vehicular ad hoc MANET/VANET is similar to the environment of fog network in the context of the mobile nodes and data transmission between VANET/MANET nodes. Therefore, the challenges of dynamic nodes and the unreliable of wireless connections are common for both fog network and MANET/VANET.

In [13] proposed tow architectures for DSN-based mobile cloud which designed for MANET/VANET, and transform the network media from wired network to the wireless network to support the virtualization of wireless network by making the allocation of wireless traffic a programmable control, SDN control the removing or assigning the flows to channels according to the traffic condition, the emergency traffic gets a high priority comparing with others. The proposed SDN makes a specific sequence according to time slot schedule in order to wireless nodes coordinating and hop crossing channels, consequently, guarded flow against eavesdropping or jamming by dropping it on a frequency hopped mode. The proposed methods improve the matric packet delivery ratio with reasonable overhead. The mobility of wireless nodes affected negatively about the performance of packet delivery, the packet delivery depending on the availability of next node within transmission area.

There are many challenges make the DSN an active research area such as the mobility of wireless nodes, latency, scalability, if there are many controllers in fog network how can corporate between them, Additionally to node churn and updating. NFV gather the virtualization techniques to manage network services in inflexible and dynamical ways [12]. In order to prevent the lake of agility of fog network and to achieve reliable infrastructure, NFV establishes a virtual machines (VM's). The management and functions of the fog network virtually through those VM's. Fog network takes benefit by NFV in many functions by virtualized switches, gateways, firewalls. Furthermore, the Creation and destruction of those VM's can be dynamical.

Many researches demonstrate the positive aspect of using hardware accelerators such as Digital Signal Processor (DSP) or Graphical Processing Unit (GPU) in order to support the fog network by high-performance capabilities in parallel with the benefits in the context of network management provided by NFV [14]. The idea of using hardware accelerators is refused from the primary concepts of NFV and major snag facing network programmability [11]. The proposed in [15] contradicted this concept, and refute it by proving the compatibility between hardware accelerator and virtualization techniques, and the combination between them is greatly improving the infrastructure of the network. The proposed use GPU as hardware accelerators and T-NOVA [16] as VNF, T-NAVA is a platform to control and supervise the using of hardware accelerator and named the problems of using some hardware accelerator in NFV's. This investment is able to improve the establishment of VNF on the heterogeneous fog network with the ability of hardware accelerator to the deployment of VNF. Furthermore, work as repository of network topology services and representation of featuring network infrastructure, optimizing network resources, the ability of configurability QoS provision according to the customer needs, communicate with cloud controller to available computing and storage for VNF incarnation, monitor and optimize the networking, computing and storage resources to achieve the decision making for VM migration or reconfiguration of virtual network.

3. Fog computing applications

According to [17], The applications that used by IoT and fog devices that are depending on the parameters of QoS such as capacity, delay, connectivity and reliability, In context of services satisfaction for applications that affected negatively from the lake of QoS, such as the Real-Time applications and Augmented Reality applications (AR). Which are very popular on smartphones, tablets, I-pads and smart glasses such as Google Glasses, smart Eyeglass from Sony and HoloLens from Microsoft. To satisfy services AR must be supported by high power, low delay and high bandwidth to achieve the processing of video streaming. However, fog computing supports AR in order of maximizing the throughput and latency reducing by both the transmission and processing. Fog computing can support the surveillance system that placed cameras along the ways and on a connected vehicle. However, Fog can achieve the processing of video streaming on a low bandwidth. one of the methods to the latency reducing and bandwidth saving, fog computing can support caching technique that implementing in fog nodes. Because of the near resources to end devices at fog computing, big data can be handled speedily without snag of cloud, latency. In the cloud, the data must be transmitted to the data center at the core of the network and after processing the result data will be sent to end devices.

4. Fog computing and Quality of Services (QoS)

Fog computing paradigm crossed the Obstacles of cloud computing, but fog computing still faces challenges in the context of QoS. In this section, we will review recent researches concerned to the enhancement QoS in order to obtain a high level of satisfaction about the application running and services via fog computing. Generally, capacity, delay, connectivity, and reliability, are the parameters of QoS.

A. Delay and Capacity

The locality is one of the benefits of fog computing in order to reduce the delay to process the data and saving the bandwidth to transmit the data from the source node to destination node. Furthermore, the computing of divided data over many nodes will destroy the efficiency of the locality. Therefore, firstly must investigate the way to place the data on fog network according to the main goal of locality. Data placement is an optimized way in order to reduce the data scheduling time between fog nodes and consequently reducing computation time.

In [18] the researcher proposed a data placement technique to placed dataset having a relationship with each other at the same node in order to reduce computation time and a capacity load of the node. This technique is solving the problem when a one of the fog nodes compute a data hosted at multi-nodes since the computation cannot start before aggregating all data from multiple nodes. The real-time application it is the cornerstone of applications executed via fog computing as an important application for IoT, and it is a noun as latency sensitive application.

The researcher in [4] introduce a computing system consist of wirelessly connected nodes with enhanced wireless technique to achieve the capability of collecting, processing, and execute mathematical model to for delay sensitive application and power consumption. The core of this research stand on the allocation of time slots to the servers in efficiency way and sleep time to transmit real-time application in excepted delay time and reduce the power consumption. For the huge data that contained by fog computing node, it is necessary to redesign a search engine able to cover all that data [19]. Caching is one of the good solutions to saving the bandwidth and minimizes the delay, therefore, implementing a cache on the fog nodes to utilize temporal locality and to cover all end nodes at fog network by.

In [20] implement cache at end device to achieve next hope computing. And in [21] the edge node such as routers it is a short path to computing and Strategic occupation because of routing connection with end devices. Using caching in edge nodes in parallel with replacing the node IP addresses with names making the accessing to the data closer [22], representing the main role of fog computing nodes to make the computing, processing and storage at the edge devices gathering with heterogeneity to create the concept of IoT.

B. Connectivity

Connectivity is an important goal for heterogeneous fog network in order to achieve the QoS. Trimming data and the high cost for transmitting data from source to destination it is a nightmare for all mobile network. Therefore, ad-hoc wireless network betakes to a geographic solution such as clustering a partitioning to prevent distorted data and the cost for retransmitting the same data, bandwidth, and delay. Wireless networks are susceptible to some node down and disconnect from other nodes which are a large-scale damage, which usually cause divided the network into disjoint partitions. In order to prevent the Wireless network from being inefficient, restoring the connectivity of the wireless network is fateful.

In [23] the researcher proposed an effective design to achieve a connectivity goal by building a double connection between network partitions in order to an alternative connection. This proposed will minimize the long path between nodes pairs for partitions and employ the lowest number of relay nodes. In [24] proposed a method controlled by the end user in order to affect positively in the context of the connectivity and performance of fog network by choosing the relay fog which achieves the availability of services for a partition or cluster or a single end user.

C. Reliability

The delivery of a complete and non-distortion data is an important issue to fog nodes in order to achieve the satisfaction of end users that require an online service and running real-time and streaming applications. In section II, We discussed the nature of fog networks and the similarity with MANET/ VANET. Therefore, fog network facing a complicated challenge which is Reliability. Fog responsible about the data transmission in the end devices with each other's at edge network and the edge devices with the core at the cloud. Typically, the data transmissions via wireless environment needs a reliable method in order to acknowledgement retransmit lose data by checkpoints [25]. Normally, the reliability procedures such as retransmission undelivered data and rescheduling will reduce a high latency. The recent researches demonstrate the negative aspect of latency in context of reliable connections to transmit applications required a high QoS such as real-time and streaming applications.

In [26] the researcher used a multi connections TCP transport layer protocol to deliver video streaming via wireless network to the end user. The multi connections implement extra multi connections for retransmission packet directly without waiting time for free connection, in parallel with a buffer on the sink node to aggregate and arrange the sequence of arrived packets before showing the video to the end user. The method above, works effectively at fog environment, since the high bandwidth connections which characterized the fog network connections. In the context of the evaluation of fog network in aspect of reliability, the evaluation technique for ad hoc network is Appropriate for fog network because of the similar concept. In [27] proposed a mathematical method to evaluate the reliability of ad hoc network stand on Markov model.

5. Conclusion

In this review, we discussed the fog computing as a cloud computing extension to the edge network, the snag of cloud computing in the context of QoS crossed by fog. The similar service for both, besides the benefit of fog in mobility provides IoT applications and services the ability to running at the heterogeneous end devices. The researches in MANET/VANET are able to apply in fog network because of the similarity among them. The sensitive applications for QoS such as real-time applications, streaming, and big data is achieved in fog computing because of the low latency, locality in parallel with the enhancement for the connectivity and the challenges of fog nodes mobility. We think fog computing will be the superior environment to hold the application of real time and video streaming in regions with low QoS internet, just in case implementing a strong security procedure.

References

- [1] Bonomi, F., et al., "**Fog computing and its role in the internet of things**". in Proceedings of the first edition of the MCC workshop on Mobile cloud computing, 2012. ACM.
- [2] Stojmenovic, I., "**Fog computing: A cloud to the ground support for smart things and machine-to-machine networks**". in Telecommunication Networks and Applications Conference (ATNAC), 2014 Australasian. 2014. IEEE.
- [3] Hajibaba, M. and S. Gorgin, "**A review on modern distributed computing paradigms: Cloud computing, jungle computing and fog computing**". CIT. Journal of Computing and Information Technology, 2014. 22(2): p. 69-84.
- [4] Suto, K., et al., "**An Energy-Efficient and Delay-Aware Wireless Computing System for Industrial Wireless Sensor Networks**". Access, IEEE, 2015. 3: p. 1026-1035.
- [5] Yuan, Z. and G.-M. Muntean, "**iVoIP: an intelligent bandwidth management scheme for VoIP in WLANs**". Wireless networks, 2014. 20(3): p. 457-473.
- [6] Yannuzzi, M., et al., "**Key ingredients in an IoT recipe: Fog Computing, Cloud computing, and more Fog Computing**". in Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2014 IEEE 19th International Workshop on. 2014. IEEE.
- [7] Evans, D., "**The internet of things: How the next evolution of the internet is changing everything**". CISCO white paper, 2011. 1: p. 14.
- [8] Nam, T. and T.A. Pardo. "**Smart city as urban innovation: Focusing on management, policy, and context**". in Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance. 2011. ACM.
- [9] Willis, D.F., A. Dasgupta, and S. Banerjee. "**ParaDrop: a multi-tenant platform for dynamically installed third party services on home gateways**". in Proceedings of the 2014 ACM SIGCOMM workshop on Distributed cloud computing. 2014. ACM.
- [10] Wang, Y., T. Uehara, and R. Sasaki. "**Fog Computing: Issues and Challenges in Security and Forensics**". in Computer Software and Applications Conference (COMPSAC), 2015 IEEE 39th Annual. 2015. IEEE.
- [11] ETSI, G., "**Network Functions Virtualisation (NFV): Architectural Framework**". ETSI GS NFV, 2013. 2: p. V1.
- [12] Manzalini, A. and R. Saracco. "**Software Networks at the Edge: a shift of paradigm**". in Future Networks and Services(SDN4FNS), 2013 IEEE SDN for. 2013. IEEE.
- [13] Ku, I., Y. Lu, and M. Gerla. "**Software-defined mobile cloud: Architecture, services and use cases**". in Wireless Communications and Mobile Computing Conference (IWCMC), 2014 International. 2014. IEEE.
- [14] Monteleone, G. and P. Paglierani. "**Session Border Controller Virtualization Towards Service-Defined Networks Based on NFV and SDN**". in Future Networks and Services (SDN4FNS), 2013 IEEE SDN for. 2013. IEEE.
- [15] Paglierani, P. "**High Performance Computing and Network Function Virtualization: A major challenge towards network programmability**". in Communications and Networking (BlackSeaCom), 2015 IEEE International Black Sea Conference on. 2015. IEEE.
- [16] Xilouris, G., et al. "**T-NOVA: a marketplace for virtualized network functions**". in Networks and Communications(EuCNC), 2014 European Conference on. 2014. IEEE.
- [17] Yi, S., C. Li, and Q. Li, "**A Survey of Fog Computing: Concepts, Applications and Issues**". 2015.
- [18] Wang, T., et al., "**DCCP: an effective data placement strategy for data-intensive computations in distributed cloud computing systems**". The Journal of Supercomputing, 2015: p.1-28.
- [19] Wang, H., C.C. Tan, and Q. Li, "**Snoogle: A search engine for pervasive environments**". Parallel and Distributed Systems, IEEE Transactions on, 2010. 21(8): p. 1188-1202.
- [20] Zhang, Y., C. Tan, and L. Qun. "**CacheKeeper: a system-wide web caching service for smartphones**". in Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing. 2013. ACM.

- [21] Wang, X., et al., "**Cache in the air: exploiting content caching and delivery techniques for 5G systems**". Communications Magazine, IEEE, 2014. 52(2): p. 131-139.
- [22] Abdullahi, I., S. Arif, and S. Hassan, "**Ubiquitous Shift with Information Centric Network Caching Using Fog Computing**", in Computational Intelligence in Information Systems. 2015 Springer. p. 327-335.
- [23] Lee, S., M. Younis, and M. Lee, "**Connectivity restoration in a partitioned wireless sensor network with assured fault tolerance**". Ad Hoc Networks, 2015. 24: p. 1-19.
- [24] Xu, F., et al. "**Designing a practical access point association protocol**". in INFOCOM, 2010 Proceedings IEEE. 2010. IEEE.
- [25] Madsen, H., et al. "**Reliability in the utility computing era: Towards reliable Fog computing**". in Systems, Signals and Image Processing (IWSSIP), 2013 20th International Conference on. 2013. IEEE.
- [26] Kim, D. and K. Chung, "**Adaptive Multiple TCP-connection Scheme to Improve Video Quality over Wireless Networks**". KSII Transactions on Internet & Information Systems, 2014. 8(11).
- [27] Choudhary, A., O. Roy, and T. Tuithung, "**Reliability Modeling of a Cluster Based Distributed Mobile Ad-hoc Network**". Int. J. Com. Dig. Sys, 2015. 4(3).