Image Encryption and decryption using CAST-128 with proposed adaptive key

L. Enas Tariq **Dr.Ekhlas Falih**

110038@uotechnology.edu.iq ١١٠٠٢٢@uotechnology.edu.iq

Computer Sciences Department / University of Technology/Baghdad/ Iraq

Abstract

Encryption of an Image is an interesting region in the security of an information field. Encrypting of an image is various from text because of its features. It is difficult for dealing with encryption of an image by employing conventional methods of encryption. The suggested methodology had been employed CAST-128 algorithm with proposed adaptive key for encrypting images. CAST-128 is a procedure that is designing for symmetric algorithm for encryption which has Feistel classical network containing 16 rounds and can operate on 64-bits blocks of plain text to introduce 64-bit blocks of cipher-text. A key's size varies from 40 bits to 128 bits in 8-bit increments. The proposed adaptive 128-bits key can be extracted from the main diagonal of the original image before encryption and apply MD5 hash function to increase the key security. The experimental results explained that the time consuming for both encryption and decryption when using proposed adaptive key is less than static key.

Keywords -Cryptography**,** CAST-128 Algorithm, Image encryption, Feistel classical network, image decryption.

التشفير وفك التشفير للصوره بالأعتماد على Cast-128 مع المفتاح المتكيف المقترح

م. أيناس طارق **م.د.أخلاص فالح**

قسم علوم الحاسوب / الجامعه التكنولوجيه / بغداد / العراق

الخلاصه

تشفير الصوره يعتبر منطقه مهمه في مجال أمنية المعلومات . يكون تشفير الصوره مختلف عن النص بسبب صفاتها. فمن الصعوبه التعامل مع تشفير الصورة عن طريق استخدام طرق تقليدية للتشفير. لقد استخدمت الطريقه المقترحة خوارزمية CAST-128 مع المفتاح المتكيف المقترح

لتشفير الصور. CAST-128 هو إجراء يتم تصميمه لخوارزمية التشفير المتناظره والتي تحتوي على شبكة Feistel الكلاسيكية حيث تحتوي على ١٦ دوره ويمكن أن تعمل على مقاطع ذات ٦٤ بت من نص عادي لإدخال مقاطع ذات ٦٤ بت من النص المشفر. يختلف حجم المفتاح من ٤٠ بت إلى ١٢٨ بت بزيادات ٨ بت. يمكن استخراج المفتاح المقترح المتكيف ذات ١٢٨ بت من القطر الرئيسي للصورة الأصلية قبل التشفير وتطبيق دالة التجزئة MD5 لزيادة أمان المفتاح. أوضحت النتائج التجريبية أن التشفير وفك التشفير باستخدام المفتاح المتكيف المقترح ياخذ وقتًا أقل مقارنةً بالمفتاح الثابت

1. Introduction

Security of information became an essential case in information transmission and storage. It often needs that data has been kept secure from unauthorized process. The best defense line is physical security. Physical security cannot always an option because of efficiency considerations and/or cost. Instead, most computers are interconnected with each other openly via establishing them and the communication channels which they employ. Cryptography can be realized as the study and science of secret writing concerns the methods that data and communications will encode for preventing their contents to be discovered via message or eavesdropping interception, ciphers, using codes, and other methods, so that the real message can see only by a certain people .Respecting to confidentiality, cryptography can be employed for data encryption that reside on storage devices or travel via communication passages for ensuring that every unlawful access was not successful. Cryptography also can be employed to secure the method of authenticating various parties trying every function on the system. Passwords are the most classical and clear credential. They are encrypted to protect versus unlawful usage [1].The multimedia information included data of an image unlike text messages has several special features such as high pixels' correlation and redundancy. Security is the major goal that must achieve through the transition of information via the network. This mechanism will be made the information to transmit into an unclear form via encryption and only the persons who are authorized can retrieve the information correctly. Encryption can be defined as chunk of information converting method which can be recognized as plain-text by employing an algorithm which can be recognized as cipher-text for making it unable to read by anyone unless these possessing knowledge especially such as a key, the output can be defined as cipher-text. The invert method

of converting cipher-text into plain-text can be known as decryption. Images are widely employed in many processes like the Internet; image data protection from unauthorized access is very substantial. Cryptography of an Image is a special type of encryption mechanisms to be hided data in an image for original message's encryption and decryption depend on some key amount. They are various algorithms that provide calculations hardness and it can make complex to break a key to extract the original image. Image storage and transmission through industrial and research methods require protection of an image [1].

2. Related work

Bimal K and Gunasekaran G.[2] have been proceeded the mechanism that employed for securing data which could know as encryption. The encrypted data can be transferred via the network, and the encrypted data can decrypt by employing presented algorithm which could know as decryption. The secret information can be hided within an image and it can be transferred with the secret key. Secure the information in past times using by invisible ink and wax tablets but now it is a recent society so the security is fully changed. A day's pictures, images, voices and videos are able to carry the message in transmitting from one site to another site with the assist of network communication. Himanshu Y., Ambika O., Anurag J., et. al.[3] have been recommended the encryption of an image is a mechanism that converts the original image to other shape which is complex for understanding. Therefore, without knowledge the key of decryption no one can arrival to the information. The encryption of an image has implementations in corporate world such as military operations, health care and multimedia systems. The Genetic Algorithm concept and RSA in modified method has been introduced by Abdel-karim S. and Hassan *et al.* [4]. This approach mixes both asymmetrical RSA with symmetrical Genetic optimization and for ensuring that make the key very difficult to reinforce impedance to the cryptanalysis. The first procedure is symmetrical by employing GIC to obtain the key from plain-text then the second procedure of the new mechanism of ciphering which can be performed by algorithm of RSA.Shankar K. et al. [5] have been produced recent algorithm of VSS to protect an image from illegitimates using by applying Elliptic Curve Cryptography with the Technique of Optimization. This approach shares are established from the secret image and every share

can be given as input to the process of encryption and decryption via the algorithm of ECC. A public key can be randomly generated in the operation of encryption and decryption operation and a private key can be generated optimally using techniques of optimization. Then, an image performance can be taken as a value of fitness to be considered as values of PSNR.

3. Symmetric Key Cryptography

Symmetric key cryptography is called also shared key or secret-key cryptography. The receiver and sender can share a common key in this mechanism for both decryption and encryption. The key require sharing via secret communication. If it is compromised then the encrypted message can be simply decrypted by the attacker. This kind of cryptographic technique is needed because it provides faster service without employing numerous resources [6].

4. Suggested Methodology

A suggested methodology for encryption of an image has two steps. The values of the main diagonal of an image can be extracted as a key in the first step. Secondly the steps of CAST-128 can be calculated.

4.1CAST-128 Key Generation

The key of CAST-128 can be extracted from the main diagonal of an image. The size of an image is 128x128.The key is calculated from the following formula:

1) for i=1 to image_width
2) for j=1 to image_height
3) if (i=j) then key[i]=pixel[i,j]

4.2 CAST-128

CAST-128 employs a pair of sub keys per round as quantity of 5-bits [kr_i] which can be employed as a key of rotation for rounding [i] and a quantity of 32-bits [km_i] is employed as a key of masking for round [i]. Three various functions for round can be employed in the algorithm of CAST-128 [7]. These rounds can be illustrated bellow:-

1) Data input [D] to the operation [I_a] and [I_d] are the extreme worthy byte via least significant byte for [I] .
2) [S_i] is the number of s-box such as s_1,s_2,s_3,s_4.
3) [O] is the operation's output.

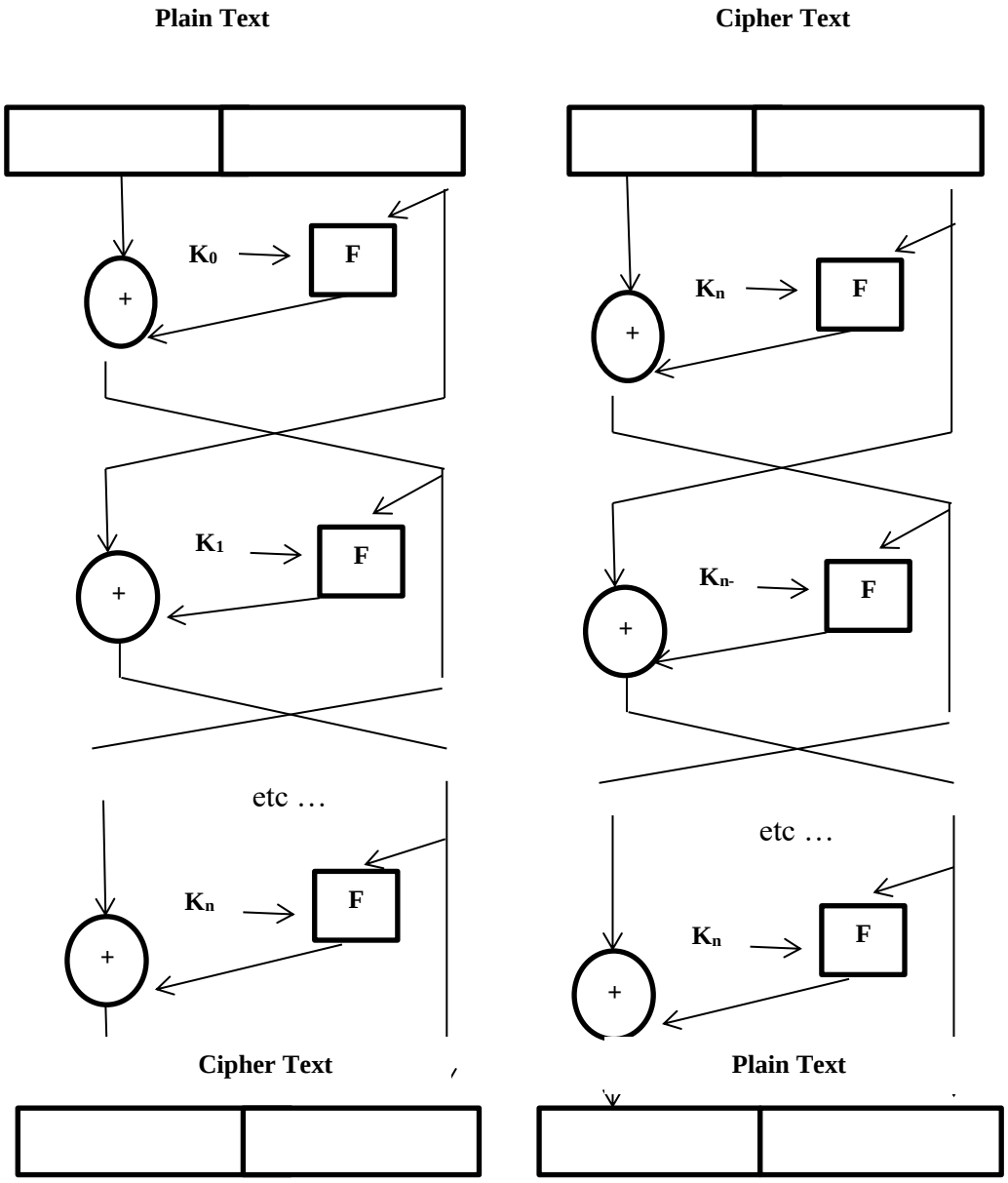


Fig.(1) : Encryption and Decryption of CAST-128 [8].

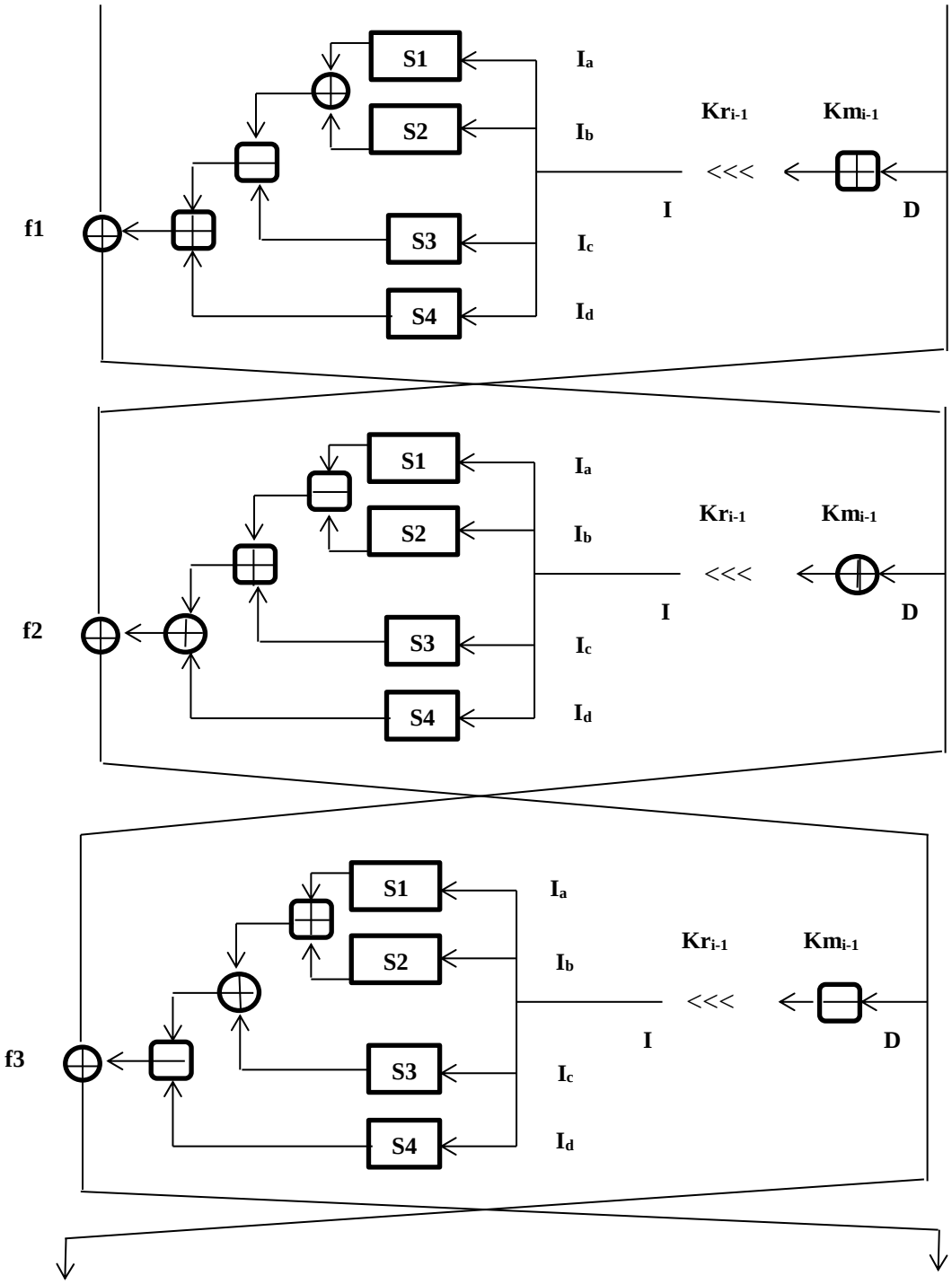


Fig. (2) : Encryption Procedure for CAST-128 [9]

The function F in Fig. 2 was prepared to obtain good diffusion, confusion and the features avalanche. It employs the substitutions of S-box, exclusive OR operations, mod 2 subtraction and addition and key dependent rotation. The F function's strength is depended primarily on the S-boxes' strength. Further uses of operations such as Boolean, arithmetic, and rotate is adding with its strength. A function F encompass employing four S-boxes, each of size 8 x 32, the left circular rotation operation and four operation functions which is different relying on the number of round. It can refer to these operation functions in Fig. 2as [$f1_i$], [$f2_i$],[$f3_i$] and [$f4_i$] .It can be used I to define the intermediate value of 32-bits beyond the function of left circular rotation and labels [I_a], [I_b], [I_c] and [I_d] to define to [I] of 4 bytes ,where [I_a] is the most-significant and [I_d] is the least-significant [8].

Function (F) can be defined for these conventions as bellow:

1-Rounds 1,4,7,10,13,16 $I = ((Km_i + R_{i-1}) <<< Kr_i)$, $F = ((S_1[I_a] \wedge S_2[I_b]) - (S_3[I_c])) + S_4[I_d]$

2- Rounds 2,5,8,11,14 $I = ((Km_i \wedge R_{i-1}) <<< Kr_i)$, $F= ((S_1[I_a] - S_2[I_b]) + (S_3[I_c])) \wedge S_4[I_d]$

3- Rounds 3,6,9,12,15 $I = ((Km_i - R_{i-1}) <<< Kr_i)$,$F= ((S_1[I_a] + S_2[I_b]) \wedge (S_3[I_c])) - S_4[I_d]$

where D is the data input to the round function. Kri is 5-bit “rotation key” of round i, and Kmi is 32-bit “masking key” of round i. $I = (I_a, I_b, I_c, I_d)$ is the state after rotation key operation. S1, S2, S3 and S4 are four 8 × 8 bits S-boxes.$\ll$,$\oplus$,+and − denote circular left-shift operation, bitwise XOR, addition modulo 2^{32} and subtraction modulo 2^{32} respectively. Note that the round number starts from 1, so for CAST-128,rounds 1, 4, 7, 10, 13 and 16 use f1 as round function, round 2, 5, 8, 11 and 14 use f2 as round function, and rounds 3, 6, 9, 12, and 15 use f3 as round function. The consecutive 3-round encryption procedure is described in Fig. 2.

4.3 Suggested algorithm

The algorithm of suggested methodology can be illustrated as:

Input : Image with 128x128 from database

Output : Encrypted image

begin

Step1: i=1 ,j=1

While (i<= 128) **Do**

While (j<= 128) **Do**

//Get Proposed adaptive key from an image

IF (i= =j) **Then** Get one value from pixel [i,j] , and put in key [i]

End IF

j=j+1

While End j

i=i+1

While End i

Step2: // CAST-128 steps

2.1 Calculate 16 sub-keys pairs {Kmi, Kri} from K -key schedule.

2.2 (m1...m64) → (L0,R0) // Split the original images to left and right 32-bits, halves L0 = img1...img32 and R0 = img33...img64.

2.3 Apply MD5 has function to key to increase the key's secuirity

2.4 **While** (i<= 16) **Do**

L[i]= R[i-1];

R[i] = L[i-1] ^ f(R[i-1],Kmi,Kri)

i=i+1

While End i

2.5 (R16,L16) →(c1...c64).

2.6 Replace final L16, R16 blocks and then merge to produce the cipher text.

End.

5. Experimental Outcomes

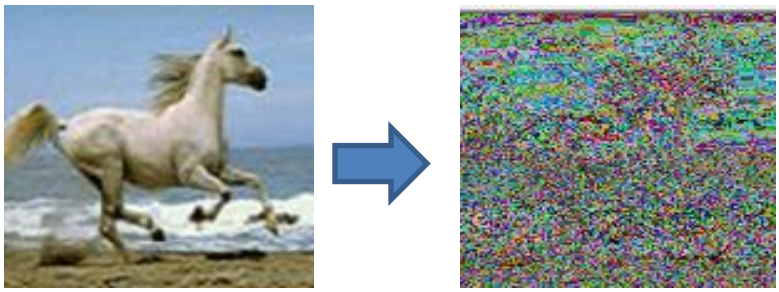
This section displays the results of the proposed methodology. The proposed methodology is implemented using C#. Twenty images are employed of type BMP and JPEG, true color, and with size 128 × 128 pixels. The proposed methodology steps can be illustrated as:

1) The first step of the suggested method extracts the pixels of the main diagonal from the original image and encrypts these pixels using MD5 hash function as illustrated in Fig.3.

```
Encrypt. Key:   b48a3293-7345-453e-978d-201e3c864922
```

Fig. (3) :Key encryption with MD5 hash function

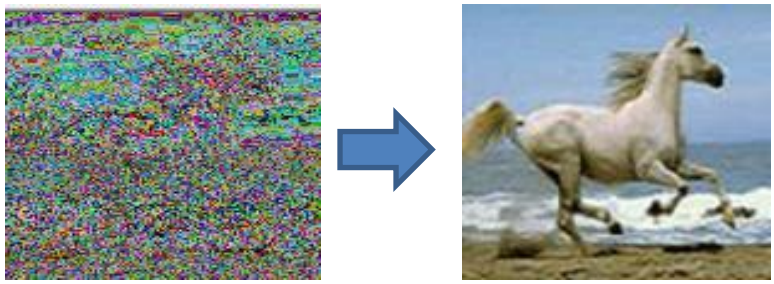
2) The second step involve loads an image and encrypt it using CAST-128 as illustrated in Fig.4**.**



a) **b)**

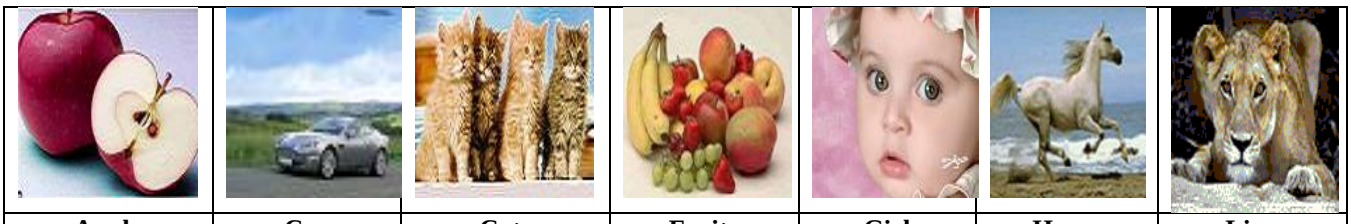
Fig.(4): Horse Images Status a) Load original image
b) Encrypted image using CAST-128

3) The third step involve loads an encrypted image and decrypt it to extract the original image as illustrated in Fig.5**.**



a) **b)**

Fig.(5): Horse Images Outcomes a) Encrypted image using CAST-128
b) Image after Decryption



Apple	Car	Cats	Fruits	Girl	Horse	Lion

Fig.(6): Database of Images Outcomes

Table1: Computational time in Milliseconds' when using static key and adaptive key on samples of different images

	Time Consuming for Static Key		Time Consuming for Adaptive Key	
Image Name	Encryption	Decryption	Encryption	Decryption
Apple.BMP	23	46	15	34
Car.BMP	57	34	15	11
Cats.JPG	78	93	11	15
Fruits	10	93	4	12
Girl.JPG	31	46	15	31
Horse.BMP	8	12	4	7
Lion	15	62	6	29

Fig. 7 and Fig. 8 illustrate time consuming for both encryption and decryption process when using different keys

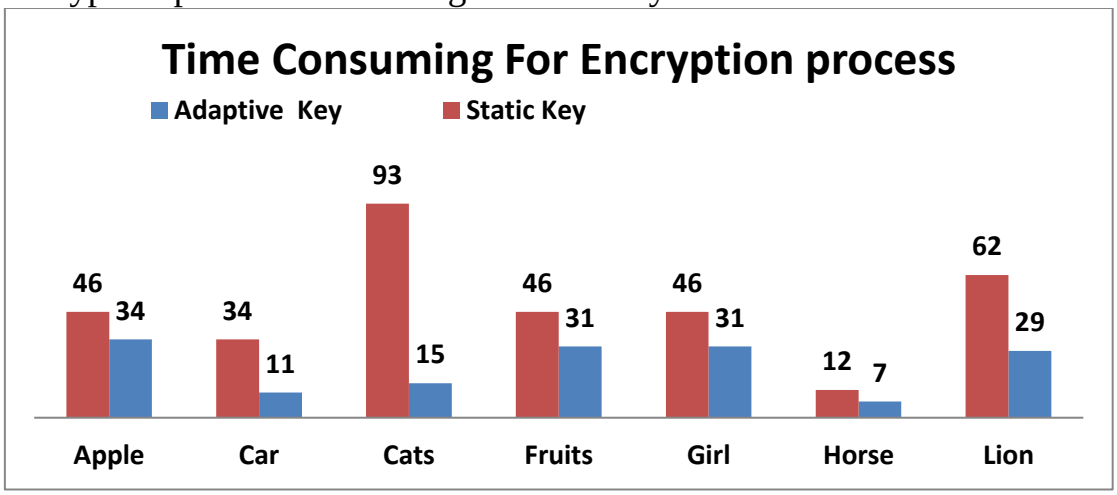


Fig.(7) encryption time consuming for static and proposed adaptive keys

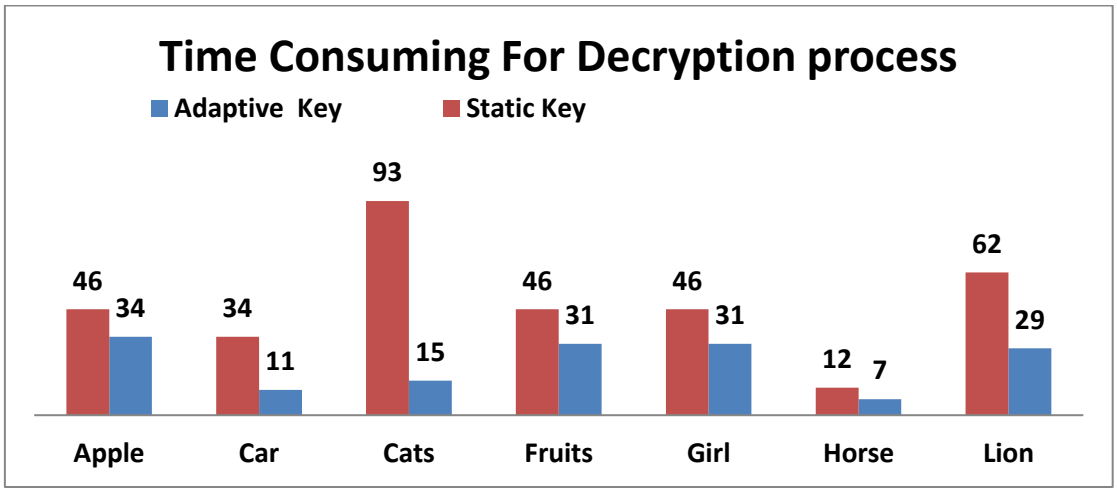


Fig.(8) encryption time consuming for static and proposed adaptive keys

Conclusion

The communication network can be mainly employ for data transmitting from one to other places. Much of data can be corrupted and hacked by everyone. To overcome this problem, it can be applied the techniques encryption to secure send the data from one user to another user. This research employed CAST-128 algorithm with proposed adaptive key to encrypt an image and compare the results with static key.CAST-128 employs fixed s-boxes and shows to own good impedance to linear, differential and related-key cryptanalysis. The experimental results explained that the time consuming for both encryption and decryption when using proposed adaptive key is less than static key.

REFERENCES

[1] Samson Ch, "An RGB Image Encryption using RSA Algorithm", International Journal of Current Trends in Engineering & Research (IJCTER) e-ISSN 2455–1392 Volume 3 Issue 3, pp. 1 – 7, March., 2017.

[2] Gunasekaran G. and Bimal K. , "Encrypting And Decrypting Image Using Computer Visualization Techniques", Journal of Engineering and Applied Sciences VOL. 9, NO. 5, ISSN 1819-6608, May, 2014.

[3] Ambika O., Himanshu Y. and Anurag J., "A Review: Image Encryption Techniques and its Terminologies", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-3, Issue-4, April, 2014.

[4] Abdel-karim S., Hassan, A. and Naglaa F., "Modifications on RSA Cryptosystem Using Genetic Optimization",International Journal of Research and Reviews in Applied Sciences, vol.19, issue.2, page(s): 150, 2014.

[5] Shankar K. and Dr Eswaran P., "A Secure Visual Secret Share (VSS) Creation Scheme in Visual Cryptography using Elliptic Curve Cryptography with Optimization Technique", Australian Journal of Basic and Applied Sciences, Vol.9, Issue.36, pp:150-163 , 2015.

[6] Sourabh Ch. and Smita P.," A comparative survey of symmetric and asymmetric key cryptography", International Conference on Electronics, Communication and Computational Engineering (ICECCE) , 2014.

[7] Thippanna G., " A Re-Examine on Assorted Digital Image Encryption Algorithm's Techniques", Biostatistics and Biometrics Open Access Journal 4(2): BBOAJ.MS.ID.555633, 2018.

[8] Krishnamurthy G., " Encryption Quality Analysis and Security Evaluation of CAST-128 Algorithm and its Modified Version using Digital Images", International Journal of Network Security & Its Applications (IJNSA), Vol.1, No 1, April, 2009.

[9] Shaomei W., Tingting C., and Meiqin W., "Improved Differential Cryptanalysis of CAST-128 and CAST-256", Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan 250100, China, Springer International Publishing AG, 2017.