Text Encryption Based on Biological Operations in Chaotic Image Hiding

Musaab Riyadh[1], Shymaa Akram Alrubaie[2*], Dina Riadh Alshibani[1]

[1]Computer Science Department, Collage of Science, Mustansiriyah University
[2]*Continuous Education Center, Middle Technical University

m.shaibani@uomustansiriyah.edu.iq
ShymmaAkram35@mtu.edu.iq
dinashibani@uomustansiriyah.edu.iq

Abstract

This paper presents a Central Dogma of Molecular Biology (CDMB) based text encryption and a chaotic based image steganography algorithm. CDMB based security systems have drawn the attention of many researchers for more than a decade and lots of work have been done in this direction, but still many gaps have been found in the evolutionary phase. The proposed work contributes to such a motive to improve the overall security of these steganography techniques. The proposed system mainly consists of three steps: Firstly a text to be hidden is encrypted as a series of proteins. Secondly, the host image will be scrambled using Fibonacci-Q Transform. Finally, the Gauss map is used to generate random numbers to determine the hiding location in host image. The PSNR and SSIM measures that are used for comparison and result analysis shows that the proposed scheme provide efficient level of security.

Keywords: Central Dogma of Molecular Biology (CDMB), DNA Cryptography, Host Image (HI).

تشفير النص بالاعتماد على العمليات البيولوجية في إخفاء الصور الفوضوي

م.د. مصعب رياض عبد الرزاق[1] م.م. شيماء اكرم الربيعي[2] م. دينا رياض الشيباني[1]

[1]الجامعة المستنصرية/ كلية العلوم/ قسم علوم الحاسوب

[2]الجامعة التقنية الوسطى/ مركز التعليم المستمر

الملخص:

في هذا البحث تم تقديم طريقة تشفير النص القائم على العقيدة المركزية للبيولوجيا الجزيئية (CDMB) وخوارزمية إخفاء الصور القائمة على الفوضى. جذبت أنظمة الأمان القائمة على CDMB انتباه العديد من الباحثين لأكثر من عقد من الزمان وقد تم إنجاز الكثير من العمل في هذا الاتجاه، ولكن لا يزال هناك العديد من الثغرات الموجودة في المرحلة التطورية. يساهم العمل المقترح في هذا الدافع لتحسين الأمان العام لتقنيات إخفاء المعلومات هذه. يتكون النظام المقترح بشكل أساسي من ثلاث خطوات: أولاً يتم تشفير النص المراد إخفاؤه كسلسلة من البروتينات. ثانيًا، سيتم خلط صورة المضيف باستخدام Fibonacci-Q Transform. أخيرًا، تُستخدم خريطة Gauss لتوليد أرقام عشوائية لتحديد موقع الاخفاء في صورة المضيف. تُظهر مقاييس PSNR و SSIM المستخدمة للمقارنة وتحليل النتائج أن المخطط المقترح يوفر مستوى فعالًا من الأمان.

الكلمات المفتاحية: العقيدة المركزية للبيولوجيا الجزيئية (CDMB)، تشفير الحامض النووي، صورة المضيف.

1. Introduction

Recently, the rapid development of the communication and e-commerce leads to increase the interest in maintaining the security of information to be able of keep abreast of continuous technical changes. Various techniques of cryptography and steganography have been suggested, but these techniques are still not sufficient to provide the required security information. Due to this, Bio-molecular concepts such as DNA computing gives us a promising approach of unbreakable algorithms in the field of data security [1]. The DNA cryptography is a technology employs DNA sequences which are works on the principles of DNA computing for ciphering and hiding the data. DNA is the genetic repository of the cell carrying parental traits (information) from the parents to their offspring. There are multi DNA cryptography techniques such as: Bio-molecular structure, One Time Pad, Central dogma of molecular biology (CDMB) for encrypting the data [2]. The main idea of CDMB technique which is supported by this study is based on matching of DNA sequences and the protein sequence. It is founded by the Watson Crick who called the name (Transcription and Translation) to this process [3]. The transcription is the process in which the DNA strands is converted in RNA strands whereas the Translation converts the RNA strands into protein sequence. Based upon the building of DNA codon, the amino acid is made [4]. The DNA structure depends on the human deoxyribonucleic acid (DNA), Adenine (A), Thymine (T), Guanine (G), and Cytosine (C) so each letter of the alphabet of the plain text can be converted into a different combination of the four nitrogen. On the other hand, the only difference between RNA (Ribonucleic Acid) and DNA structure is that the Thymine (T) is replace with Uracil (U) [3]. In this study, the plain text is encrypted based on CDMB concept and chaotic map, and then the encrypted text is inserted into scrambled host image. The Chaotic maps behaviour is managed by mathematical equations and sensitive to any change in initial conditions. This behaviour seems random and disorderly, but really depends on specific patterns. In cryptosystem confusion and diffusion processes use chaotic output signals, which present random statistical characteristics [5], [6]. The rest of the paper has been organized as Section 2 illustrates Related Work, Methodology, in Section 3, 4 explain the main steps of the algorithm, section 5 displays the evaluation of the algorithm, section 6 conclude the study.

2. Related Work

Many works have been suggested based on chaotic map and CDMD, Meettu et al. [7], proposed a new method, the method deal with different data by converting to binary format then based on three steps: first, the information encrypt by DNA & amino acids cipher text. Second, the formed DNA (cipher text) hidden using reference DNA by insertion technique. Third, the key generated in step1 encrypted with conventional RSA algorithm. This method is characterized more security because ensures double level of security (RSA with DNA), and able to save a large data in small DNA, but its defect by high biological modification rate. Eihab et al. [8], suggested two steganography algorithms for hiding a cipher message in artificial DNA sequences by using chaotic maps, the first one has low computational requirements but vulnerable to statistical attacks while the second one is an improvement of the first one which can be used to hide both short and long encrypted messages. A steganography algorithm is proposed by Suman & Samir [9]. it consists of two phases: in the first phase, the secret information is converted into a grayscale image by DNA sequence (combination of four nucleotides A, C, G&T). While in the second phase, the generated image will be hidden based on standard steganography procedure. The proposed method hides two secret images with unique steganography algorithm without distortion of cover image. As well, Ghada et al. [10], made a blind crypto-stego techniques depend on the double layered secured system in cryptography and steganography. The proposed method consists of two phases: Firstly, the proposed generic N-bits binary coding rule used to apply data to DNA.

Then, use an ambiguity encryption of DNA and amino acids Playfair. Secondly, the ambiguity cipher text is placed by 3:1 placement strategy, then random positions created by using a true real random number seed will be used to hide DNA. This technique provides lower cracking probability, while the ambiguity that performs some kind of data overhead. Well, while DNA steganography with improved DNA insertion algorithm is offer by Malathi et al. [11]. The modification of the DNA insertion algorithm is used because of its low cracking probability. The information is hidden inside the DNA sequence. XOR-ing repeatedly adds additional security to the confidential message and it is very difficult for an intruder guess how the XOR-ing is done. The proposed method obtains lower cracking probability than the other existing methods for hiding inside DNA sequence.

3. Methodology

The proposed algorithm is based on building a model of steganography by using Central Dogma of Molecular Biology CDMB) with DNA Vigenere cipher to encrypt the text file, while the image is chaotic by using Fibonacci-Q Transform and Gauss Maps. This technique utilizes characteristics of DNA & RNA to secure encrypt, and then uses the features of chaotic maps to increase the security of steganography algorithm. Thus, the basic steps to implement the model are illustrated as follows:

3.1 Central Dogma of Molecular Biology (CDMB)

The biological concepts of CDMB can be explained as a converting procedure of DNA sequence to corresponding proteins. It consists of two major operations called as transcription and translation. The process of converting the DNA strands to RNA strands is called transcription, while the process of converting the RNA strands into protein sequence is called translation as illustrated in Figure 1 [3], [12].Various digital systematic procedures are proposed based on the biological CDMB concepts which are used to convert the plaintext message to protein format such as converting plain text to ASCII code, and convert ASCII to binary, then a binary form of the plain text is converted into a DNA strands[13].

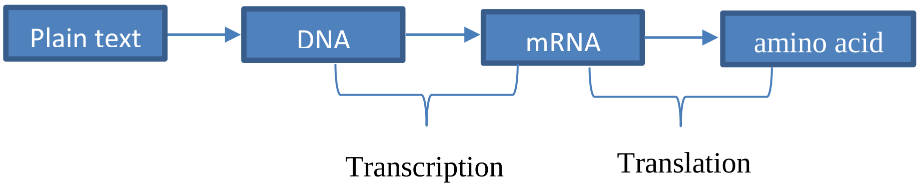
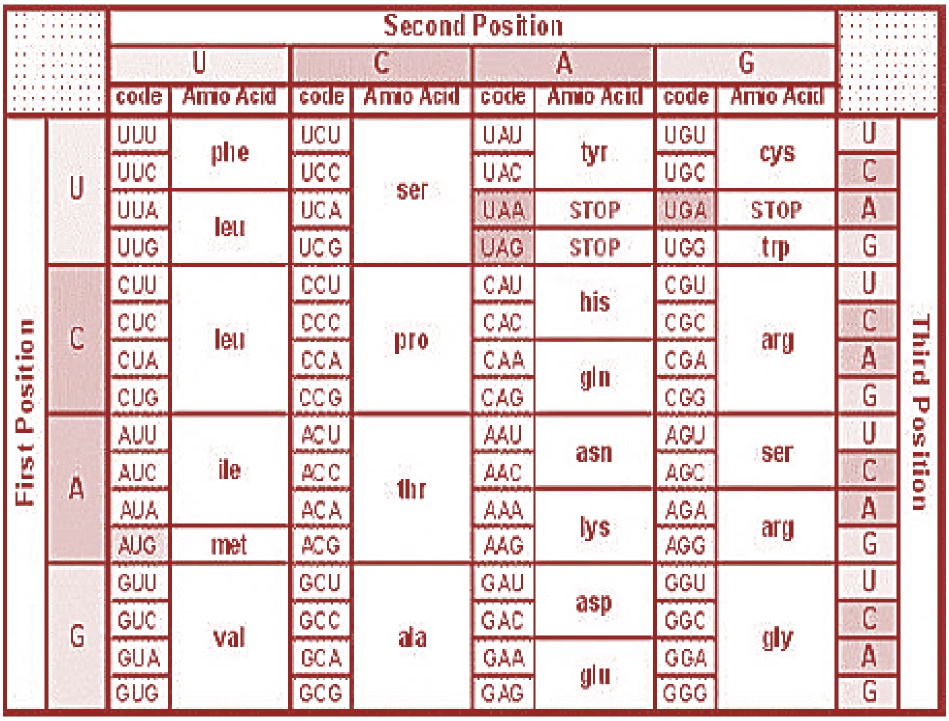


Figure 1. Plain text conversion into a series of proteins [3].

On the other hand, the DNA strands are converted into RNA which is translated into chains of amino acids are represented by abbreviated form of specific proteins as defined in **Figure** 2. The protein format of cipher text can be efficiently transferred through public channels due to its small size as compared with the original message.



		Second Position								
		U		C		A		G		
		code	Amio Acid	code	Amio Acid	code	Amio Acid	code	Amio Acid	
First Position	U	UUU	phe	UCU	ser	UAU	tyr	UGU	cys	U
		UUC		UCC		UAC		UGC		C
		UUA	leu	UCA		UAA	STOP	UGA	STOP	A
		UUG		UCG		UAG	STOP	UGG	trp	G
	C	CUU	leu	CCU	pro	CAU	his	CGU	arg	U
		CUC		CCC		CAC		CGC		C
		CUA		CCA		CAA	gln	CGA		A
		CUG		CCG		CAG		CGG		G
	A	AUU	ile	ACU	thr	AAU	asn	AGU	ser	U
		AUC		ACC		AAC		AGC		C
		AUA		ACA		AAA	lys	AGA	arg	A
		AUG	met	ACG		AAG		AGG		G
	G	GUU	val	GCU	ala	GAU	asp	GGU	gly	U
		GUC		GCC		GAC		GGC		C
		GUA		GCA		GAA	glu	GGA		A
		GUG		GCG		GAG		GGG		G

Third Position

Figure 2. RNA to amino acids conversion [4].

3.2 Image Scramblers & Fibonacci-Q Transform

Various techniques are used in this work such as Fibonacci-Q Transform.The Fibonacci-Q Transform can be defined as mapping the original pixel location with the new location to produce a scrambled image in order to maximize the security of steganography as defined in equation (1).

$$\begin{pmatrix} i' \\ j' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} i \\ j \end{pmatrix} \bmod N \qquad (1)$$

Where i, j are the original image coordinates, i',j' are the scrambled image coordinates and N represents the image size more details can be found in [14]. The inverse of Fibonacci-Q Transform is defined as in equation (2).

$$\begin{pmatrix} i \\ j \end{pmatrix} = \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{-1} \end{pmatrix} \begin{pmatrix} i' \\ j' \end{pmatrix} \ \mathbf{mod\ N} \qquad (2)$$

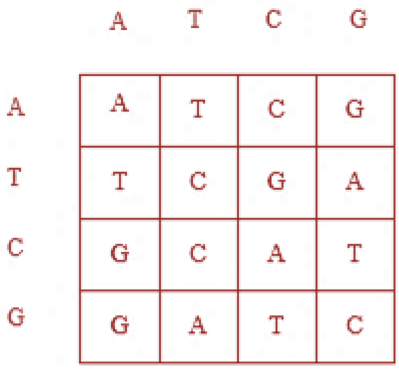
Gauss map is supported in this work as a nonlinear iterated map of real values to randomly generate a pseudo numbers. As defined in equation (3):

$$\mathbf{Xn + 1 = exp(-\alpha\, Xn2) - \beta} \qquad (3)$$

Where Xn+1 is the presented chaotic value and Xn is the current chaotic value, β is -0.58, α is 4.90 will be taken in the proposed method [15] [16].

3.3 DNA Vigenere cipher

The DNA Vigenere method is proposed based on the Vigenere cipher concept [17]. The proposed method consists of two steps: firstly, construct the DNA-Vigenere table of size 4x4 which represent DNA strands as illustrated in Figure 3. Secondly, the DNA strands is ciphered based on the DNA-Vigenere table and the secrete key. For example, "A" is the first character of the transformed plaintext, and "G" is the first character of the secret key which means column 1, row 4. Thus, the value of (4,1) is replaced with the plaintext "A".



	A	T	C	G
A	A	T	C	G
T	T	C	G	A
C	G	C	A	T
G	G	A	T	C

Figure 3. DNA-Vigenere Table [11].

3.4 Least Significant Bit Hiding LSB

A brief summary of LSB replacement is explained in this section. The replacement algorithm of LSB make use of the advantage of human eye perceptual system. Many pixels forms an image a number between 0 to 255 are used to express each pixel, in fact it can be represented by 8 bits. It is been noticed that the human eye can never realizes any alteration in the LSB of a pixel.The new information bit is overwrites the LSB. If the secret bit is not equal to the LSB of the given pixel then ±1 is added randomly to the pixel while keeping the altered pixel value in the range of [0, 255] [18].

4. Suggested Algorithms

The proposed Biological Encrypted Text in image steganography using Chaotic maps algorithm (BET_ISC) consists mainly of two stages: The Biological Choatic Encryption (BCE) stage and the Choatic Hiding (CH) stage. In this first stage, the DNA-Vigenere cipher and central dogma molecular biological principle are used to encrypt the plain text. While the choatic hiding (CH) stage will hide the results of the BCE in a host color image.as shown in the block diagram in Figure 4.

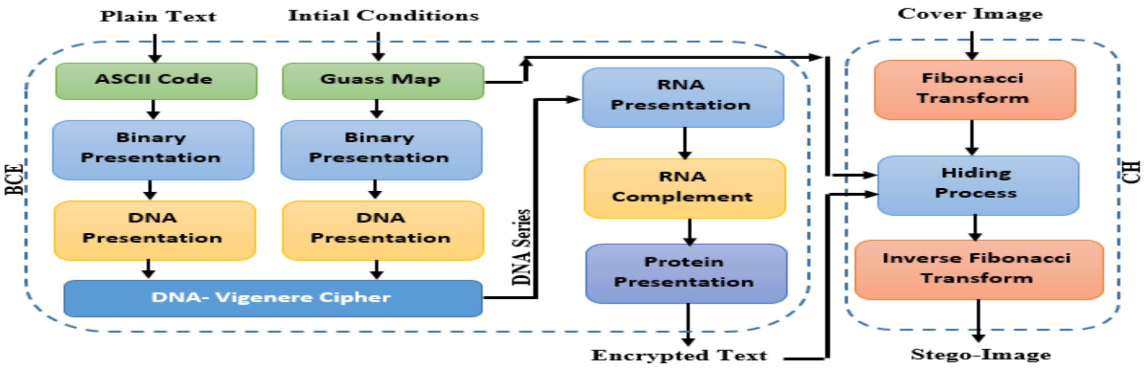


Figure 4. Block Diagram for BET_ISC algorithm

4.1 Biological Chaotic Encryption (BCE):

In the first stage, the BSE algorithm is used to encrypt the plain text as shown in algorithm 1.**Algorithm 1: BEC**

Input: plain text file, intial conditions, facts for Gauss map

Output: encrypted text file.

Step1: Read text file of length L.
Step2: BinMat (Lx8) is gained by transforming text into its corresponding ASCII code then into a binary presentation.
Step3: **Extract** the DnaMat (Lx8)/2 by subsuming each pair of binary bits form Binmat with Dna representation such that "A=11", "C=01", "G =10" and "T=00".
Step4: The DnaSecKey of length $(\mathrm{L} \times 8)/2$ is generated after iterating Guass map as explained in Algorithm 2.
Step5: Encrypts Dnamat based on the DNA-Vigenere cipher and Dnaseckey by considering dnaMat (row index) and dnaSecKey (column index) as parameters to produce dnaMat'.as explained in section 3.4.
Step6: Calculate the rnaMat (lx8)/2 by converting DNA into RNA by replacing each T with U.
Step7: amnoAcidMat is constructed based on rnaMat and table 1 as following: let’s assume that the first four elements in rnaMat are "ACUG" then the first four element of amnoAcidMat are A4leu. **Note:** the first character is still the same and followed by a number which is referring to the order of the> RNA series in Figure 2 to avoid ambiguity. As there are three STOP codons, UAA would be referred to as 1stop, UAG would be referred to as 2sto and UGA would be referred to as 3stop.
Step8: Save the resulted text which represents the encrypted text into separate file.

Algorithm 2: dnaSecKey generation
Input: initial condition (xg0,yg0,vg0,wg0, zg0), facts (σ,β)
Output: mask key

Step1: Iterate Guass map Eq. (3) with its initial values (xg0,yg0,vg0,wg0, zg0) and facts for L × 8 times to produce initial series xg ={xg1,xg2,…,xgL× 8}, yg={yg1,yg2,…,ygL× 8}, vg={vg1,vg2,…,vgL× 8}, wg={wg1,wg2,…,wgL× 8}, zg={zg1,zg2,…,zgL× 8}.
Step2: Convert initial real values series (yg,vg,wg and zg) into a binary series (ygbin, vgbin, wgbin and zgbin) by using the following formula:

$$\mathrm{ygbin}_{\mathrm{L\times 8}} = \begin{cases} 0 & \text{if ygi} > 0 \\ 1 & \text{otherwise} \end{cases} \quad ….4$$

$$\mathrm{vgbin}_{\mathrm{L\times 8}} = \begin{cases} 0 & \text{if vgi} > 0 \\ 1 & \text{otherwise} \end{cases} \quad ….5$$

$$\mathrm{wgbin}_{\mathrm{L\times 8}} = \begin{cases} 0 & \text{if wgi} > 0 \\ 1 & \text{otherwise} \end{cases} \quad ….6$$

$$\mathrm{zgbin}_{\mathrm{L\times 8}} = \begin{cases} 0 & \text{if zgi} > 0 \\ 1 & \text{otherwise} \end{cases} ….7$$

Where the range of I from 1 to Lx8

Step3: Construct kBinS matrix of length L× 8 from ygbin, vgbin, wgbin and zgbin series by using the elements of xg series as a selection control to determine their order in **kBinS**. See Figure 5. First, transforming xg elements into an integer numbers with a range from 1 to 24 by using the following equation:

$$\mathrm{temp_i} = \ \mathrm{mod}\ (\mathrm{Abs}(\mathrm{floor}(\mathrm{xg_i}) \times 10^{15}), 24 \qquad (8)$$

Note that $\mathrm{temp_i}$ belongs to [1, 24]. According to elemets of kBinS matrix is determined. For example, if $\mathrm{temp_i}$= 1 that means ygbin, vgbin, wgbin and zgbin will be arragmed according to the 1'st row in Table 1, $\mathrm{temp_i}$= 2 corresponds to the 2'nd row in Table 1 and so on.
Step 4: KDnaS is constructed of length of L× 4 by conversion of kBinS to a DNA form as A=11, C=01, G =10 and T=00.

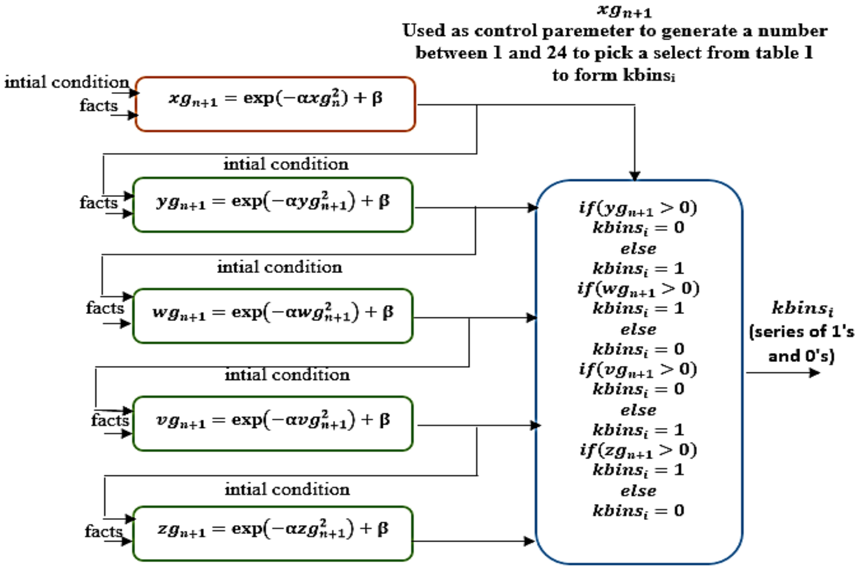

xg_{n+1}
Used as control paremeter to generate a number between 1 and 24 to pick a select from table 1 to form kbins$_i$
intial condition
facts
$xg_{n+1} = \exp(-\alpha xg_n^2) + \beta$
intial condition
facts
$yg_{n+1} = \exp(-\alpha yg_{n+1}^2) + \beta$
intial condition
facts
$wg_{n+1} = \exp(-\alpha wg_{n+1}^2) + \beta$
intial condition
facts
$vg_{n+1} = \exp(-\alpha vg_{n+1}^2) + \beta$
intial condition
facts
$zg_{n+1} = \exp(-\alpha zg_{n+1}^2) + \beta$
$if(yg_{n+1} > 0)$ $kbins_i = 0$ $else$ $kbins_i = 1$
$if(wg_{n+1} > 0)$ $kbins_i = 1$ $else$ $kbins_i = 0$
$if(vg_{n+1} > 0)$ $kbins_i = 0$ $else$ $kbins_i = 1$
$if(zg_{n+1} > 0)$ $kbins_i = 1$ $else$ $kbins_i = 0$
$kbins_i$ (series of 1's and 0's)

Figure 5. Kbins Matrix Construction

Table 1. Kbins Matrix Construction.

NO.	Kbins(i)	Kbins(i+1)	Kbins(i+2)	Kbins(i+3)
1.	yg_{n+1}	wg_{n+1}	vg_{n+1}	zg_{n+1}
2.	yg_{n+1}	wg_{n+1}	zg_{n+1}	vg_{n+1}
3.	yg_{n+1}	vg_{n+1}	wg_{n+1}	vg_{n+1}
4.	yg_{n+1}	zg_{n+1}	vg_{n+1}	wg_{n+1}
5.	yg_{n+1}	zg_{n+1}	wg_{n+1}	zg_{n+1}
6.	yg_{n+1}	vg_{n+1}	zg_{n+1}	wg_{n+1}
7.	wg_{n+1}	yg_{n+1}	vg_{n+1}	zg_{n+1}
8.	wg_{n+1}	yg_{n+1}	zg_{n+1}	vg_{n+1}
9.	wg_{n+1}	vg_{n+1}	yg_{n+1}	zg_{n+1}
10.	wg_{n+1}	vg_{n+1}	zg_{n+1}	yg_{n+1}
11.	wg_{n+1}	zg_{n+1}	yg_{n+1}	vg_{n+1}
12.	wg_{n+1}	zg_{n+1}	vg_{n+1}	yg_{n+1}
13.	vg_{n+1}	yg_{n+1}	wg_{n+1}	zg_{n+1}
14.	vg_{n+1}	yg_{n+1}	zg_{n+1}	wg_{n+1}
15.	vg_{n+1}	wg_{n+1}	zg_{n+1}	yg_{n+1}
16.	vg_{n+1}	wg_{n+1}	yg_{n+1}	zg_{n+1}
17.	vg_{n+1}	zg_{n+1}	yg_{n+1}	wg_{n+1}
18.	vg_{n+1}	zg_{n+1}	wg_{n+1}	yg_{n+1}
19.	zg_{n+1}	yg_{n+1}	wg_{n+1}	vg_{n+1}
20.	zg_{n+1}	yg_{n+1}	yg_{n+1}	wg_{n+1}
21.	zg_{n+1}	wg_{n+1}	yg_{n+1}	vg_{n+1}
22.	zg_{n+1}	wg_{n+1}	vg_{n+1}	yg_{n+1}
23.	zg_{n+1}	vg_{n+1}	wg_{n+1}	yg_{n+1}
24.	zg_{n+1}	vg_{n+1}	yg_{n+1}	wg_{n+1}

4.2 Hiding Layer

The basic idea behind the hiding stage in BET_ISC algorithm is to use key based LSB substitution to hide the encrypted text in the host image. Here once again chaotic Guass map is used to determine what location in the cover image is used to hold the current bit of the encrypted text. The hiding process is explained in Algorithm 3 & 4.

Algorithm 3: CH
Input: cover image, encrypted text
Output: stego image.

Step1: cImg is gained by reading a color image of size R × R × 3.

Step2: Separate cImg into red, green and blue bands. Then extract the red band of cImg in rMat of size R × R.

Step3: frMat is gained by dividing rMat into a number of non-overlapping blocks of size 8 × 8 then apply Fibonacci-Q Transform to each block.

Step4: frMat' is gained by applying Fibonacci-Q Transform to frMat.

Step5: chtMat is gained by iterating equation (2) for (L*8)/2 to gain pixel location to hide the encrypted text. As explained in Algorithm 4 and Figure 6.

Step6: Update frMat' by modifying the LSB of the pixels controls by chtMat values as an index.

Step7: ifrMat is gained by applying inverse Fibonacci-Q Transform.

Step8: ibifrMat' is gained by dividing ifrMat into a number of non-overlapping blocks of size 8 × 8 then apply Fibonacci-Q Transform to each block.

Step9: Reform stego-image by combing ibifrMat' with other green and blue band of the cover image.

Algorithm 4: chtMat generation
Input: initial condition (xg,yg), facts (σ,β) in the acceptable interval
Output: chtMat

Step1: xgi={xg1,xg2,…,xg((((L×8)/2) ×8) ×2)/2}, ygi={yg1,yg2,…,yg((((L×8)/2) ×8) ×2)/2} are generated by iterating Guass map Eq. (2) with its initial values (xg0,yg0) and facts.

Step2: ranMat of size $(((L \times 8)/2) \times 8) \times 2)$ is constracted by cross coupled xg and yg series as explained in Figure 6.

Step3: Convert initial real values series ranMat into an integer series (chtMat) by using the following equation (9):

$$\text{chtMat}_{\text{i}} = (\text{ranMat}_{\text{i}} \times 10^{14}) \bmod (\text{L}) \qquad (9)$$

chtMat and chtMat +1 are used to determine the current coordinates x,y of the pixels in the cover image in order to hide the current character of the encrypted text.

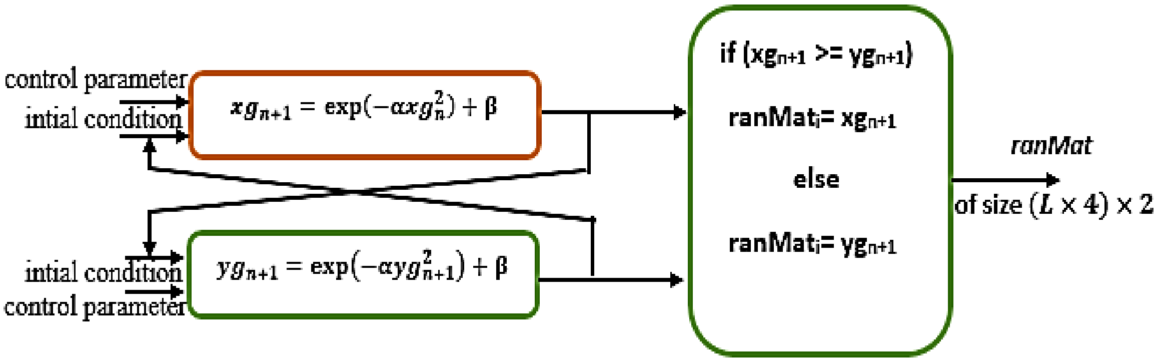

control parameter
intial condition
$xg_{n+1} = \exp(-\alpha xg_n^2) + \beta$
intial condition
control parameter
$yg_{n+1} = \exp(-\alpha yg_{n+1}^2) + \beta$
if (xg_{n+1} >= yg_{n+1})
ranMat_i= xg_{n+1}
else
ranMat_i= yg_{n+1}
ranMat
of size $(L \times 4) \times 2$

Figure 6. Chtmat constriction

The inverse of BET_ISC process is like described above, but in backwards procedure.

5. Simulation Result

BET_ISC algorithm performance is evaluated by measuring stego-image quality. Histogram, Peak Signal to Noise Ratio (PSNR) and SSIM are used to assets the stego-image quality.

Note that the BET_ISC algorithm has been performed using C# programming language, Windows-10 pro operating system has been used to perform the experiments using the laptop computer processor: Intel® Core™ i5-4300U CPU @ 190 GHz 2.50 GHz, and (4GB) RAM. Also, the time complicity of the proposed approach is calculated using Ɵ (n^2). In all the experiments, 256×256 color image is used as the host image.

To start with, Figure 7 (C) make an evident that there is no difference between host image A and Stego image B.where C is resulted from subtract stego image B from host image A. Figure 8 shows the histogram of the stego-image is much like the host image histogram for the three bands red, green and blue, that's mean hiding the secret encrypted text into the cover image have made intangible distortion to the cover image.

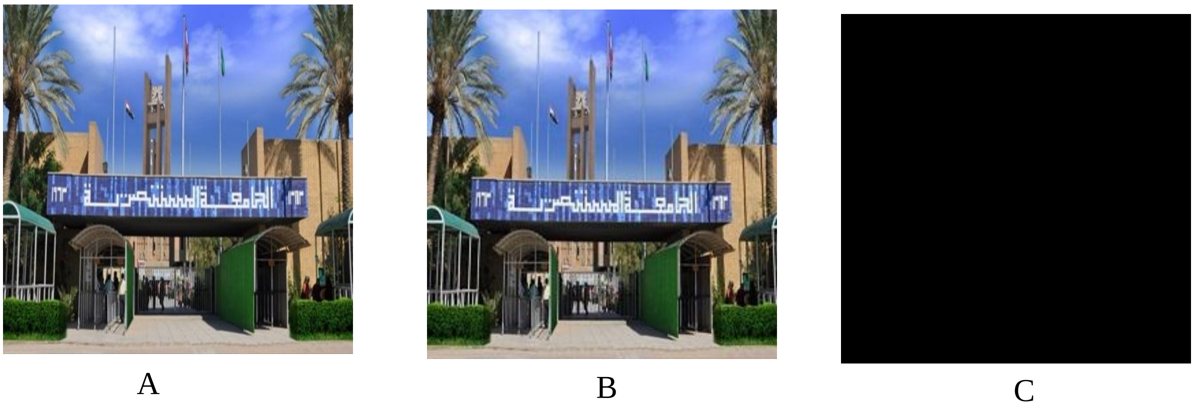
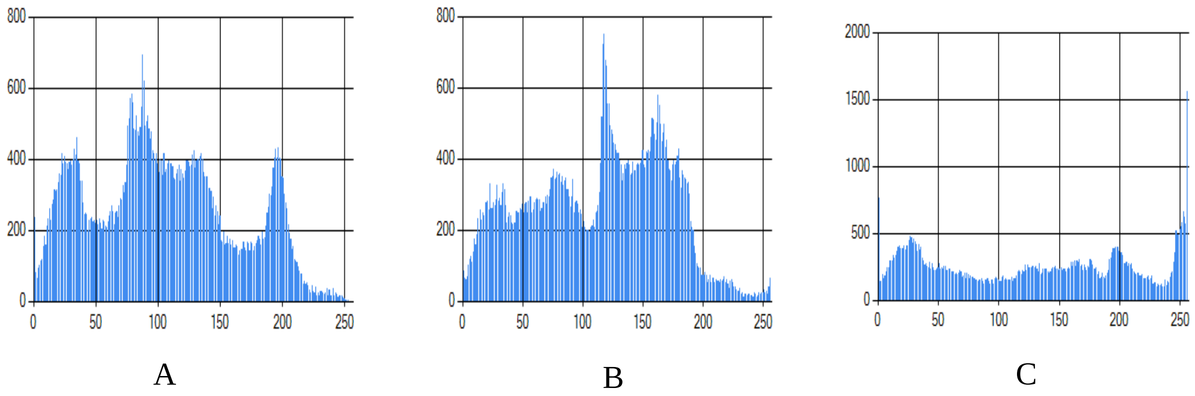


Figure 7. Outcome of the BET_ISC algorithm: (A) original image, (B) stego image, (C) Difference between original image and stego image.



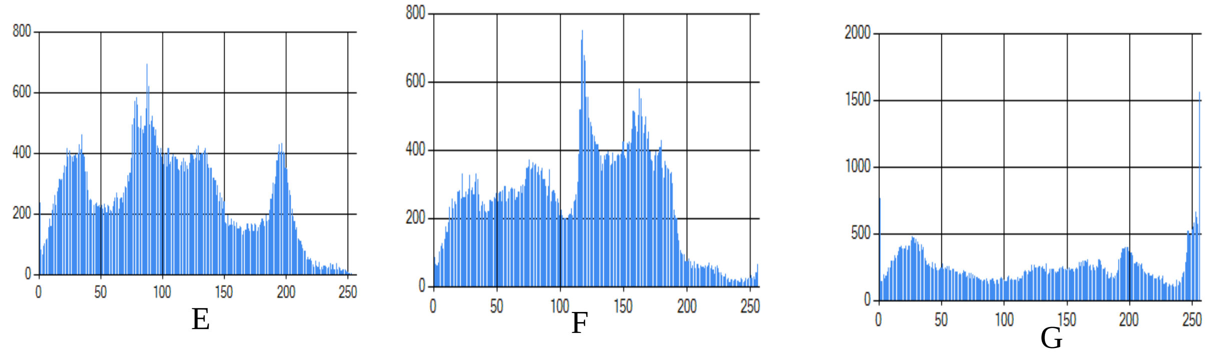


Figure 8. Histogram Evaluation: (A) red of original image, (B) green of original image, (C) blue of original image, (E) red image after stego, (F) green image after stego, (G) blue image after stego.

Furthermore, the PSNR and SSIM are calculated and the results show that there is almost no distortion to the cover image and the visual quality of the stego-image is good. Finally, hiding capacity as shown in Table 2.

Table 2. PSNR and SSIM ratios

NO.	Text File Size	PSNR	SSIM
	1KB	58.4399	0.9992
	3KB	56.1426	0.9957
	2KB	57.1589	0.9989
	2KB	57.1568	0.9991

6. Conclusion

The BET_ISC algorithm provides higher security and can protect the message from stego image. The hiding process of the encrypted text is controlled by a secret key. This operation provides sufficient secrecy. Comparison of BET_ISC algorithm is done through the imperceptibility measure PSNR. Furthermore, respectable privacy is maintained with the help of key which is generated through chaotic map. Since no message can be extracted without the key. Experimental result shows that PSNR value and SSIM of BET_ISC algorithm is fair enough to pass imperceptibility. A PSNR value up to 58 dB has been achieved which is a major advantage of the proposed approach**.**

7. References

[1] UbaidurRahman NH, Balamurugan C and Mariappan R. 2015. A novel DNA computing based encryption and decryption algorithm. Procedia Computer Science. 46 pp 463-75.

[2] Padmapriya M.K. 2016. A Study on DNA based Information Security Methodologies. IJCSMC, 5(4) pp 100-104

[3] Kalsi, S., Kaur, H. and Chang, V., 2018. DNA cryptography and deep learning using genetic algorithm with NW algorithm for key generation. Journal of medical systems, 42(1), p.17.

[4] Alshibani DR, Shati NM and Ahmed NT. DNA 2019. Genetic Recombination based Image Encryption using Chaotic Maps. Indian Journal of Public Health Research & Development. 10(6).

[5] Gupta A and Gupta A. 2015. Image Encryption Using Chaotic Maps. International Journal of Advanced Technology In Engineering And Science. 03(01).

[6] Ragab, A.H.M., Allah, O.S.F., Magld, K.W. and Noaman, A.Y., 2014. Security Evaluation of Robust Chaotic Block Cipher. International Journal of Soft Computing and Engineering (IJSCE), 3(6), pp.9-16.

[7] Skariya M and Varghese M. 2013. Enhanced double layer security using RSA over DNA based data encryption system. International Journal of Computer Science& Engineering Technology (IJCSET). 4(06) pp746-50.

[8] Bashier E, Ahmed G, Othman HA and Shappo R. 2013. Hiding secret messages using artificial DNA sequences generated by integer chaotic maps. International Journal of Computer Applications. 70(15).

[9] Chakraborty S and Bandyopadhyay SK. 2015. Data Hiding by Image Steganography Appling DNA Sequence Arithmetic. International Journal of Advanced Information Science and Technology (IJAIST). 44(44)

[10] Hamed G, Marey M, Amin SE and Tolba MF. 2016. Hybrid randomized and biological preserved dna-based crypt-steganography using generic n-bits binary coding rule. InInternational Conference on Advanced Intelligent Systems and Informatics (Cham) pp 618-627.

[11] Malathi P, Manoaj M, Manoj R, Raghavan V and Vinodhini RE. 2017 Highly Improved DNA Based Steganography. Procedia Computer Science.115 pp 651-9.

[12] Yang, J., Pu, H., Lian, J., Gu, J. and Fan, M., 2018. Modeling and analysis of protein synthesis and DNA mutation using colored Petri nets. IEEE Access, 6, pp.22386-22400.

[13] Alshibani DR and Qassir SA. 2016. Image enciphering based on DNA Exclusive-OR operation union with chaotic maps. Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA) IEEE. pp. 1-6.

[14] Alias Sathya, S.P. and Ramakrishnan, S., 2018. Fibonacci based key frame selection and scrambling for video watermarking in DWT–SVD domain. Wireless Personal Communications, 102(2), pp.2011-2031.

[15] Sahay A and Pradhan C. 2017. Gauss iterated map based RGB image encryption approach. International Conference on Communication and Signal Processing (ICCSP) (IEEE) pp 0015-0018.

[16] Sharma MC and Sharma P. 2017. Image Encryption based on Random Scrambling and Chaotic Gauss Iterative Map. International Journal of Computer Applications. 157(3) pp. 18-23.

[17] Aung, T.M. and Hla, N.N., 2019, January. A Complex Polyalphabetic Cipher Technique Myanmar Polyalphabetic Cipher. In 2019 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-9). IEEE.

[18] Chatterjee, A., Ghosal, S.K. and Sarkar, R., 2020. LSB based steganography with OCR: an intelligent amalgamation. Multimedia Tools and Applications, pp.1-19.