

## Encryption and hiding text using DNA coding and hyperchaotic system

**Zeena N. Al-kateeb, Melad Jader**

Department of Computer Sciences, College of Computer Sciences and Mathematics,  
University of Mosul, Iraq

---

### Article Info

#### Article history:

Received Dec 10, 2019

Revised Feb 13, 2020

Accepted Feb 18, 2020

---

#### Keywords:

Color image

DNA sequence operation

Hyperchaotic system

---

### ABSTRACT

In this paper, a secure data encryption using DNA sequence operation in a new and innovative direction different from the traditional direction, DNA coding uses the eight rules of DNA code based on a sequence of letter in text that provides the possibility of encrypting the same letter or word in more than one form in one text-based on sequence of this letter or word in the text. Then hiding technique implemented based on a hyperchaotic system. To increase the security of encryption text, we use the hyperchaotic system for obtaining the color image position that used to hide on it. The proposed steganography method hides a letter of the encrypted text in each pixel of the cover image, thus giving the possibility of hiding large text data. Some metrics have been applied to the proposed algorithm such as NPCR analyses, MSE, Correlation, and BER, The results of the simulation and security analysis showed that the new DNA coding is suitable for text encryption/decryption and that the super-chaotic map is suitable for hiding/extract the encrypted data, which indicates that the proposed encryption algorithm has a good encryption and hiding effect. Can resist brute statistical attack, force attack, differential.

*Copyright © 2020 Institute of Advanced Engineering and Science.  
All rights reserved.*

---

### Corresponding Author:

Zeena N. Al-kateeb,

Department of Computer Sciences,

University of Mosul, Mosul, Iraq.

Email: zeenaalkateeb@yahoo.com , zeenaalkateeb@uomosul.edu.iq

---

## 1. INTRODUCTION

People who keep the attention of secret data information be interested in growth local information that transforms between peoples [1]. Many algorithms have been used to improve security. DNA coding is a branch of DNA cryptography, it mixed between old kind cryptography techniques with new pitches of genetic methods. Know data encryption based on fixed DNA coding is week security [1-2]. Chaotic technology that's used only in the cryptography system is not more safety [3-4]. Therefore, most researchers have integrated more than one technique of concealment and diffusion technology to obtain high-secret hybrid encryption and concealment system.

Propose an innovative way that associations, the DNA indexing algorithm with RC4 algorithm in 2017 [5], this work support strong data hiding in the framework of steganography. Consider a steganography procedure in the spatial domain for digital images based upon chaotic maps. By putting on chaos efficiently in secure communication, the gift of the overall anticipated, the algorithm has been improved to significant levels [6]. Where the Ref. [7] show multi kind of encryption method combines with chaotic in DCT domain for RGB, this approach has two steps for chaotic function, one that used encryption secret text, second, for hiding in the DCT color image. The Ref [8] proposed mechanism provides high imperceptibility toward steganalysis and uses various techniques, where this mechanism based on chaotic cat mapping, besides,

the Canny Edge Detection. A color image encryption algorithm based on fractional-order PWL hyperchaotic map combining with DNA sequence [9].

In this paper, new text encryption/decryption and hiding algorithm is present, where a different DNA coding is used, its Dynamic DNA based on many binary bits that the letters of text 0 converted to it. The aim of this approach is DNA computing and DNA is encoding that includes combine between biological and algebra operation on a sequence of DNA, which makes it more difficult to break and analyze the code, which in turn gives the proposed algorithm with more support and goodness. For more security, we used the hyperchaotic system to obtain a random float number that treated in several steps to consist of a pair number represented the position in color image used to hide on it without exchange the external appearance. DNA coding and encryption, secure text, and chaotic stenography technology are combined innovatively, uncomplicated calculations were used, the encrypted output dynamic DNA coding is hidden in a color image, the proposed algorithm can improve the security of transferring important and confidential data.

**2. BASIC CONCEPTS**

In this section, we will touch the most important basic concepts used in this work.

**2.1. DNA coding and decoding**

The research presentation (using pseudocode algorithm or other), how to test and getting out the data [1, 3]. The characteristic of the course must be stand up the reference, so the caption will be accepted [2, 4].

The figure and table are view center, as shown below and cited in the manuscript.

DNA cryptography contains enciphering the secure plain text using DNA computational techniques.

The use of this technique offers many advantages:

- a) Take very little time compared to traditional algorithms.
- b) The task of any cryptographic algorithm is to protect the data for a great period.
- c) DNA molecule expression parallel computation, that is meant DNA based processes can powerful processing.
- d) DNA based computers have a very reduced amount of power feeding, which is equal to one billionth of a traditional computer.

DNA sequence has 4 nucleic acid bases A(adenine), T(thymine), A(adenine) and C(cytosine), where C and G are complementary, T and A are complementary. By using the C, A, G and T to coded 01, 00,10 and 11, 4!=24 Is the number of combination kinds.

Table 1, show eight kinds of coding combinations, DNA is decoded by the inverse of DNA coding (c).

Table 1. DNA coding rules

Rule	1	2	3	4	5	6	7	8
11	T	T	A	A	C	C	G	G
10	G	C	G	C	A	T	A	T
01	C	G	C	G	T	A	T	A
00	A	A	T	T	G	G	C	C

**2.1.1. Algorithm of coding text using DNA rules**

Input: Secure text

- 1. Begin
- 2. Read the secure text
- 3. Convert it to binary code
- 4. Compute the length of binary code
- 5. Mode length by 8
- 6. The result of the previous step is between 0-7 that represented the number of rules that used from table 1 to coded
- 7. Divided the binary code to parts of 2 digits.
- 8. Substitute each part by a corresponding letter on the table.

Output: coded text

**2.2. Hyperchaotic liu system select the data distribution map**

Chaos is the study of the unforeseen, of the nonlinear and the eccentric. It demonstrates us to expect the unforeseen. While most good old science manages as far as anyone knows unsurprising wonders like chemical responses, electricity, or gravity, the theory of chaos is a care with nonlinear things that are effectively impossible to predict or control, like weather, turbulence, our brain states, the stock market, and so on [10-15]. Chaos theory is a branch of physics and mathematics [16-23], focus on the behavior of

dynamical systems that are highly influenced to initial conditions. This sensitivity is commonly known as the butterfly effect [24-25]. The chaos was used to encrypt and hide data because of its properties which are summarized as:

- a) Higher complexity and nonlinear behaviors.
- b) Sensitivity based on initial values.

When an initial value is given to a particular system, it is known that the future state of the system can be expected but in the systems of chaos. Predicting the long term is impossible to predict.

In the past few years, chaos and nonlinear dynamics have been used in the build-up of hundreds of cryptographic primitives. These algorithms contain image hash functions, encryption algorithms, and watermarking.

Introduce a hyperchaotic system which is called a hyperchaotic Liu system and described by [26]:

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) \\ \dot{x}_2 = rx_1 - kx_1x_3 + x_4 \\ \dot{x}_3 = hx_1^2 - px_3 \\ \dot{x}_4 = -qx_1 \end{cases} \quad (1)$$

where  $a, p, r, q, k, h$  are constant parameters. This system has chaotic attractors when the parameters  $a = 10, p = 2.5, r = 40, q = 10.6, k = 1$  and  $h = 4$  [18-20], [26]. There must be a prior agreement between the transmitter and the receiver on parameter values. Figure 1 shows the attractors of this system.

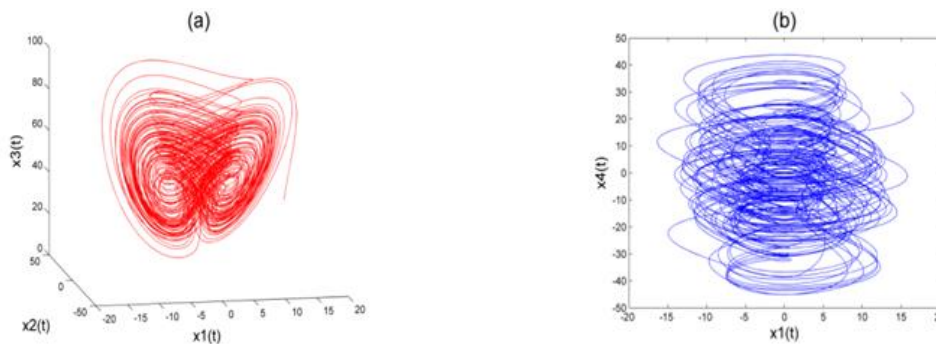


Figure 1. The attractors hyperchaotic Liu system in: (a)  $x_1, x_2, x_3$  space, (b)  $x_1, x_4$  plane

In this paper we use this system to scramble the pixel position for steganography, hyperchaotic Liu system can produce a four pseudo-random sequences whose lengths  $MX \times 4$ ; namely  $A = \{a_1, a_2, \dots, a_M\}, B = \{b_1, b_2, \dots, b_M\}, C = \{c_1, c_2, \dots, c_M\}, D = \{d_1, d_2, \dots, d_M\}$ , which shown as the Figure 2

9009x4 double				
	A	B	C	D
1	1	1	1	1
2	1.0002	1.0317	0.9981	0.9941
3	1.0007	1.0633	0.9962	0.9883
4	1.0017	1.0950	0.9943	0.9824
5	1.0029	1.1266	0.9925	0.9765
6	1.0145	1.2850	0.9842	0.9469
7	1.0345	1.4448	0.9770	0.9169
8	1.0626	1.6074	0.9712	0.8861
9	1.0984	1.7739	0.9667	0.8544
10	1.1532	1.9872	0.9634	0.8136
11	1.2195	2.2105	0.9628	0.7705
12	1.2972	2.4459	0.9654	0.7249
13	1.3864	2.6956	0.9717	0.6762
14	1.5057	3.0081	0.9846	0.6149

Figure 2. The four pseudo-random sequences which produce from hyperchaotic Liu system

We have practically just two sequence generators to determine the pixel which will contain the hidden data, it is possible to use any two sequences after the agreement between the sender and the receiver, it is worth mentioning that the strings generated by the hyperchaotic Liu system may contain negative values. Therefore, we have processed the negative values by taking the absolute values of the resulting values. In this paper *A* used to specify the row and *B* used to select the column of the pixels According to the following equation:

$$\begin{aligned}
 X[i] &= \text{fix}(A[i] \times v) && \text{if } X[i] < M \\
 Y[i] &= \text{fix}(B[i] \times v) && \text{if } Y[i] < N
 \end{aligned}
 \tag{2}$$

Where *M*, *N* is the length and width of the image, *v* is a constant parameter that can be 10 if the image size is small and can be 100 if the image size is large, After that, we will build a matrix *XY* of a random position resulting from *X* & *Y* matrix's after deletion the duplicate positions wherever found it. The duplicate positions may lead to twice hide in the same location which causing loss of some data. The long sequence produced by this system enables us to hide a large amount of data in the image. The deletion of repeated positions and deletion of positions who have coordinates higher than the resolutions of the image added an increase in randomness and ambiguity for our algorithm. Figure 3 summarizes the process of building the hiding position matrix.

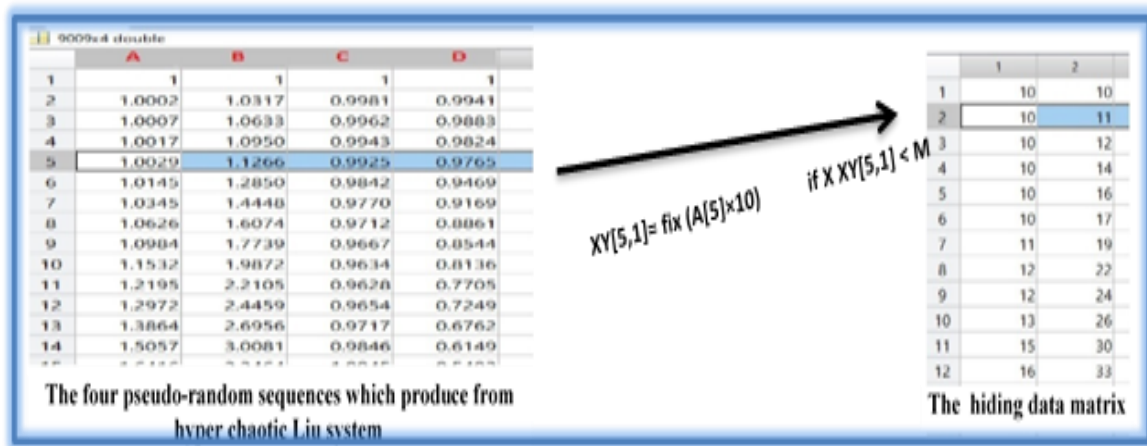


Figure 3. The building process of the matrix of hiding positions

**2.2.1. Algorithm of building the matrix of hiding positions**

Input: the constant parameters, *a*=10, *p*=2.5, *r*=40, *q*=10.6, *k*=1 and *h*=4, and the sequence of the array whose values will represent the rows *R*, and the sequence of the array whose values will represent the Columns *C*, the constant *con* which may be 10,100,100

1. Begin
  2. Solve the system and store the resulting matrix *MX* × 4
  3. Create a two-column *mn* matrix *X* derived from *MX*, the first column *R*, and the second column *C*
  4. For each cell *X*[*i*], perform the following operations Divided the binary code to parts of 2 digits.
  5. If *X*[*i*,1]<0                            then *X*[*i*,1]= *X*[*i*,1]\*-*con*                            else *X*[*i*,1]= *X*[*i*,1]\* *con*
  6. If *X*[*i*,2]<0                            then *X*[*i*,2]= *X*[*i*,2]\*-*con*                            else *X*[*i*,2]= *X*[*i*,2]\* *con*
  7. If *X*[*i*] = any cell in *XY* then Neglected                            else *XY*[*j*]= *X*[*i*]
- Output: the matrix of hiding positions *XY*

Each cell of the matrix *XY* contains two elements that representing the pixel coordinates in the image where confidential data will be hidden.

### 3. DATA HIDING METHOD

The most widely recognized strategy for information implanted is the LSB technique [15-16]. In the base method, eight bits of mystery information is considered for implanting at once in the LSB of RGB pixel estimation of the bearer image in 3, 3, 2 request individually. Along these lines, the initial three bits of the mystery message is disguised inside three (03) bits of the LSB of Red pixel, the following three bits in the three (03) bits of the LSB of Green pixel. The staying two bits of the mystery message is disguised in two (02) bits of the LSB of Blue pixel. The nitty-gritty procedure has been portrayed in Figure 4. The specific scattering design is produced thinking that the chromatic results of blue to the human eye are more than that of red and green pixels [15].

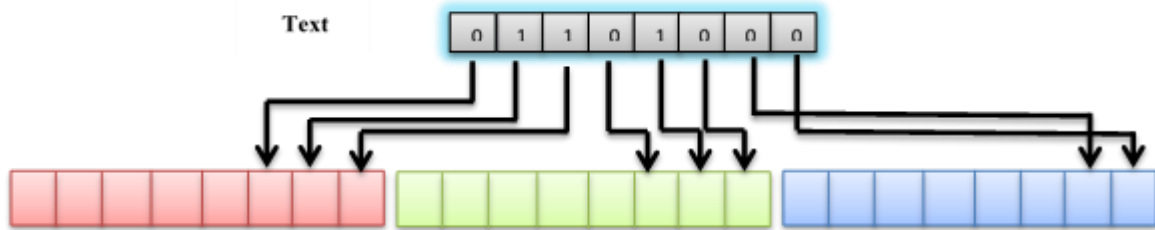


Figure 4. Distribute bits of confidential data on a pixel of the color image

We used the same algorithm with a simple modification to the sequence of hiding the bits of the secret text and retrieving it in the following form or any other form according to the prior agreement between the sender and the recipient.

#### 3.1. Message coding & embedding technology (MCET).

In our proposed algorithm the technology is divided into four central parts, coded the secure message, hide data is not sequential and diffusion pixels. These two steps must be taken before the data transfer by the sender when receiving the data by the recipient must perform the process of extracting the hidden data and then decoded the obtain an original form of secure. The following flowchart is shown that Figure 5.

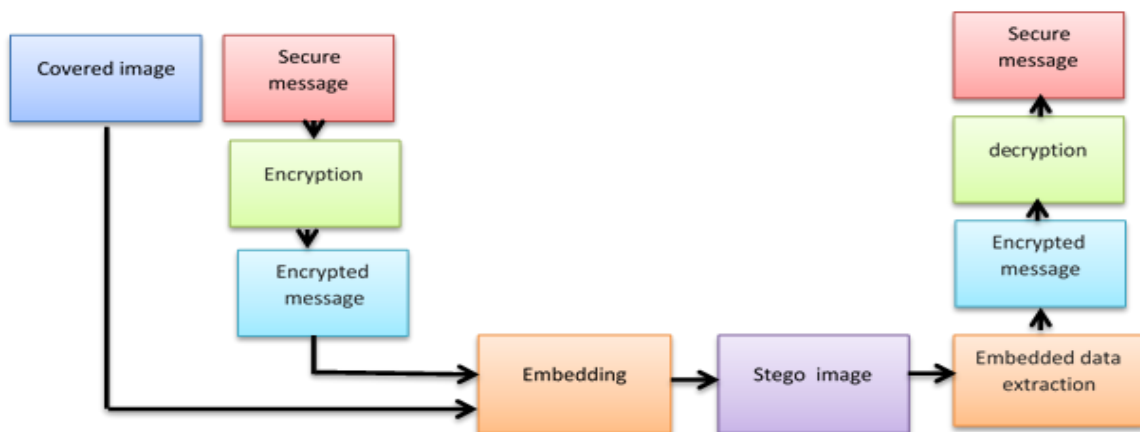


Figure 5. Message coding & embedding technology (MCET)

##### 3.1.1. Algorithm of message coding & embedding technology

To complete the coding and embedding process correctly, we must follow these steps

1. Enter the secret message  $S1$  and calculate its size, based on the size of the message we will choose which DNA role will be used for encryption.
2. Enter the cover image  $I1$  and calculate its dimensions.

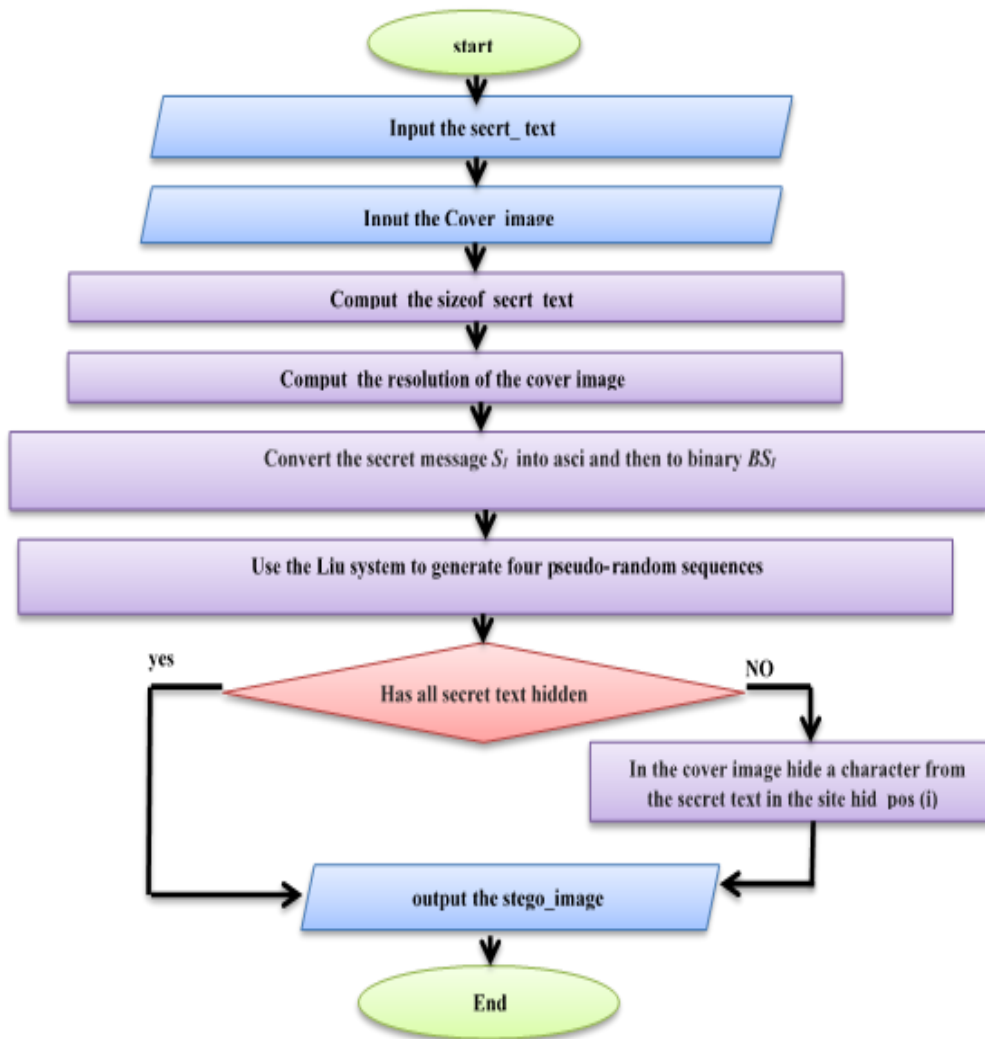
3. Convert the secret message  $S_1$  into ascii and then to binary  $BS_1$ .
4. Coded the binary secret text  $BS_1$  based on dynamic DNA coding EBS1.
5. Use the Liu system to generate four pseudo-random sequences.
6. Use only two pseudo-random sequences to generate a matrix of random pixels  $XY$  that specifies the pixels at which the data will be hidden.
7. Hide byte of encrypted data EBS1 in each pixel.  
The flowchart [1] explains these steps better.

**3.1.2. Algorithm of extract data embedding & message decoding technology**

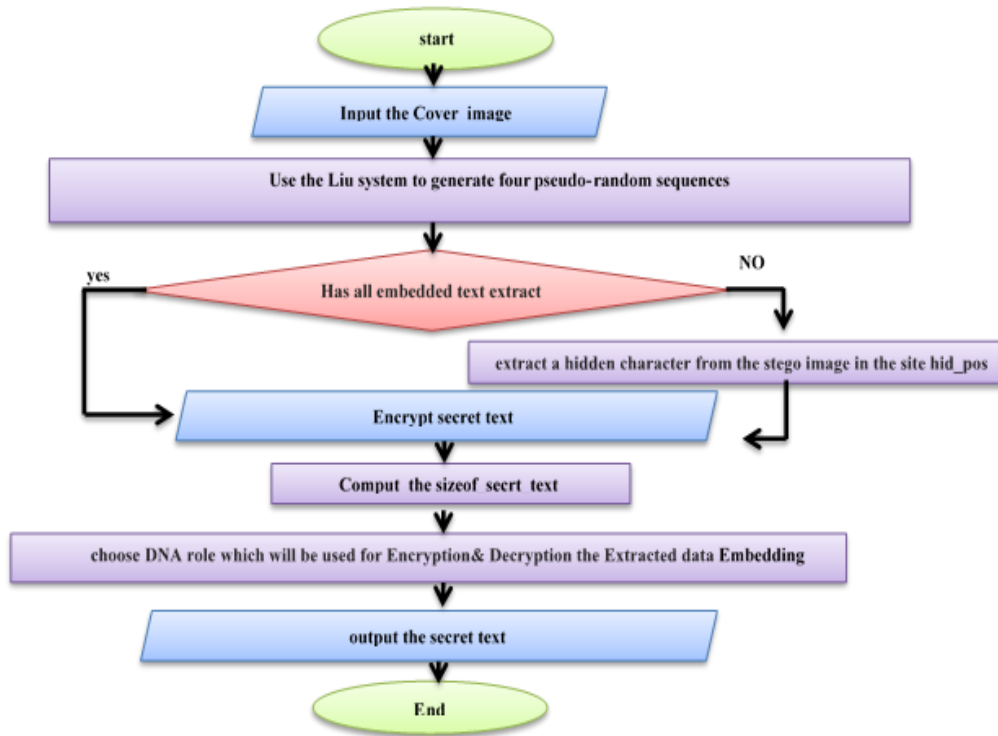
To complete the Extract data Embedding and decode process correctly, we must follow these steps

1. Use the Liu system to generate four pseudo-random sequences.
2. Choose the two sequences that have already been agreed previously to generate the data distribution map.
3. Extract data embedding.
4. Calculate the size of Extracted data Embedding, to choose DNA role which will be used for decoding.
5. Decode the Extracted data embedding.
6. Convert binary-coded Extracted data into ascii coding.
7. Convert ascii to char.

The flowchart [2] explains these steps better.



Flowchart 1. Embedding data & message coding flowchart



Flowchart 2. Extract embedded data & message decoding flowchart

#### 4. SIMULATION RESULTS ANALYSIS

The proposed technology (MCET) was applied to a set of color images and get a good result, here we applied the result of some different image size. We calculated the MES, PNCR, and Correlation to check the quality of the performance technology. We also draw a histogram for these images before and after the steganography, the Figure 6 illustrations the results obtained from applying the proposed algorithm on the image of mountains 259\*194.png, where we show that the human eye does not distinguish a clear difference between the two images a cover and stego image.



*Image before hiding*



*Image after hiding*



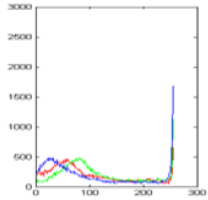
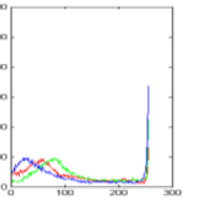


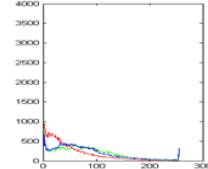
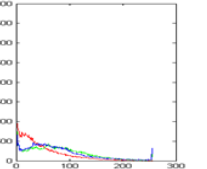


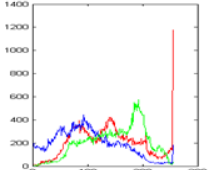
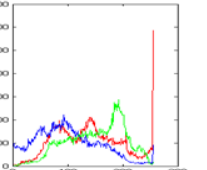


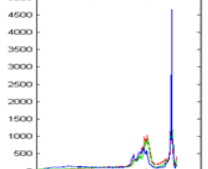
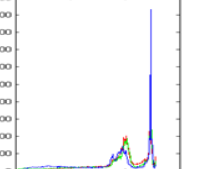


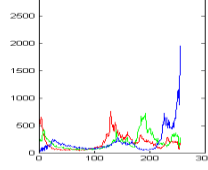
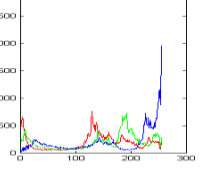
Figure 6. Mountains Image before and after data hiding

To verify the quality of the performance of the proposed algorithm was applied to more than one image, we chose images with different content and dimensions and different extensions and, the MES, PNCR, and Correlation values were calculated. Table 2 shows these results. It will be workable on a note that those histogram for an image which indicates by a chart the number about pixels at each transformed force esteem discovered in that image. That histogram assault is acknowledged a Factual attack, it gives human eye on differentiating that distinction the middle of the blanket Furthermore stego pictures though there may be An message embedded under channels, a 24-bit color image, 256 distinctive intensities to each of the 3 channels (red, green, blue) are could reasonably be expected. Therefore, a histogram to every channel camwood makes drawn separately. In Table 3 we embed those pictures previously, then after steganography and we bring settled on an drawing histogram for each about the individual's images.

Table 2. Shows the result of PSNR, MSE, CORRELATION, and BER for many pictures

Image name	MSE	PSNR	CORRELATION	BER	Size
Mountains	0.010674149849408	65.7499	0.999998203035093	0	259*194
Waterfall	0.009473390916690	65.7599	0.999996777534862	0	259*194
Flowers1	0.011826656888202	65.4359	0.999996886340445	0	251*201
Flowers2	0.013313247837836	64.9975	0.999996679792604	0	251*201
Penguin	0.010335814459526	65.5769	0.999998452568401	0	259*194
Ref[7] Girl	0.0584	60.5072	-----	-----	-----
Ref[7] Boy	0.0315	63.1627			
Ref[7] Sun	0.0516	61.0275			

Table 3. Show result for many pictures as PSNR, MSE, and CORRELATION

Image name	Image before hiding	Image after hiding	Histogram before hiding	Histogram after hiding	Size
Mountains image					259*194
Waterfall image					259*194
Flowers1 image					251*201
Flowers2 image					251*201
Penguin image					259*194

5. CONCLUSION

This research provided an effective way to protect confidential data through encryption and hiding processes where it first began to encrypt important text data using DNA sequence and rules in a modern and different way than previously used, our way enables us to encrypt the same character with more than one code depending on the sequence of its receipt in the secret text that provides strength and difficulty in breaking and analyzing the code, The proposed method includes hiding the data in the color images in scattered locations of the cover image, the locations map that show where the encrypted data will be built based on four-dimensional Hyperchaotic Liu system, The results showed the quality and efficiency of the encryption and decryption process where data was fully recovered without any loss of data BER=0, as well as



the quality of the hiding process through the use of metrics NPCR analyses, MSE and Correlation. Table 2, (3) show these results. Due to the quality of the obtained results, we can recommend using this method to encrypt another type of data and used the hiding method for another type of multimedia such as audio and video.

#### ACKNOWLEDGMENT

The authors are very grateful to the University of Mosul/ College of Computer Sciences and Mathematics for their provided facilities, which helped to improve the quality of this work.

#### REFERENCES

- [1] J. Zhang, *et al.*, "Image Encryption Algorithm Based on Dynamic Coding and Chen's Hyperchaotic System", *Mathematical Problems in Engineering*, vol. 2016, pp. 11, 2016.
- [2] H. D. Tiwari and J.H. Kim, "Novel Method for DNA-Based Elliptic Curve Cryptography for IoT Devices", *ETRI Journal*, vol. 40, pp. 396-409, 2018.
- [3] S. koppu and V.M. Viswanatham, "A Fast Enhanced Secure Image Chaotic Cryptosystem Based on Hybrid Chaotic Magic Transform," *Modelling and Simulation in Engineering*, vol. 2017, pp. 12, 2017.
- [4] W. Chen, *et al.*, "Optical Color Encryption Based on Arnold Transform and Interference Method", *Optics Communications*, vol. 282, pp. 3680-3685, 2009.
- [5] R. k. Ahmed and I. J. Mohammed, "Developing a New Hybrid Cipher Algorithm using DNA and RC4," *International Journal of Advanced Computer Science and Applications*, vol. 8, pp.171-176, 2017.
- [6] A. Anees, *et al.*, "A Technique For Digital Steganography Using Chaotic Maps", *Nonlinear Dynamics*, vol. 75, pp. 807-816, 2014.
- [7] M. J. Saeed, "A New Technique Based on Steganography and Encryption Text in DCT Domain For Color Image," *Journal of Engineering Science and Technology*, vol. 8, pp. 508–520, 2013.
- [8] V. L. Reddy, "Novel Chaos Based Steganography for Images Using Matrix Encoding and Cat Mapping Techniques," *Information Security and Computer Fraud*, vol. 3, pp. 8-14. 2015.
- [9] L. M. Zhang, *et al.*, "A Novel Color Image Encryption Scheme Using Fractional-Order Hyperchaotic System and DNA Sequence Operations," *Chinese Physics B*, vol. 26, 2017.
- [10] Z. N. Al-kateeb and M. R. Al-Bazaz, "Steganography in Colored Images Based on Biometrics," *Tikrit Journal of Pure Science*, vol. 24, pp.111-117, 2019.
- [11] V.K. Yadav *et al.*, "Synchronization Between Non-autonomous Hyperchaotic Systems with Uncertainties Using Active Control Method," 7th International Conference on Communication, Computing and Virtualization, *Procedia Computer Science*, vol. 79, pp. 963 – 970, 2016.
- [12] A. S. Al-Obeidi and S. F. AL-Azzawi, "Projective Synchronization for a Class of 6-D hyperchaotic Lorenz System," *Indonesian Journal of Electrical Engineering and Computer Science*, vol.16, pp. 692-700, 2019.
- [13] A. S. Al-Obeidi, S. F. AL-Azzawi, "Complete Synchronization of a Novel 6-D Hyperchaotic Lorenz System with Known Parameters," *International Journal of Engineering & Technology*. vol. 7, pp. 5345-5349, 2018.
- [14] A. S. Al-Obeidi and S. F. AL-Azzawi, "Chaos Synchronization of a Class 6-D Hyperchaotic Lorenz System," *Modelling, Measurement and Control B.*, vol. 88, pp. 17-22, 2019.
- [15] S.F. AL-Azzawi and M.M. Aziz, "Strategies of Linear Feedback Control and Its Classification," *Telkommika*, vol.17, pp.1931-1940, 2019.
- [16] M. M.Aziz and S. F. AL-Azzawi, "Control and Synchronization With Known and Unknown Parameters," *Applied Mathematics*, vol. 7, pp.292-304, 2016.
- [17] S.F. AL-Azzawi, "Stability and Bifurcation of Pan Chaotic System by Using Routh-Hurwitz and Gardan Method," *Applied Mathematics and Computation*, vol. 219, pp. 1144-1152, 2012.
- [18] M. M.Aziz and S. F. AL-Azzawi, "Anti-Synchronization of Nonlinear Dynamical Systems Based on Cardano's Method," *Optik*. vol.134, pp.109–120, 2017.
- [19] M. M. Aziz and S. F. AL-Azzawi, "Hybrid Chaos Synchronization Between Two Different Hyperchaotic Systems via Two Approaches," *Optik*. vol.138, pp. 328–340, 2017.
- [20] S. F. AL-Azzawi and M. M. Aziz "Chaos Synchronization of Nonlinear Dynamical Systems via A Novel Analytical Approach," *Alexandria Engineering Journal*, vol. 57, pp. 3493–3500. 2018.
- [21] S. Al-hayali and S. F. AL-Azzawi, "An Optimal Nonlinear Control for Anti-Synchronization of Rabinovich Hyperchaotic System," *Indonesian Journal of Electrical Engineering and Computer Science*, vol.19, 1, 2020.
- [22] S. Al-hayali and S. F. AL-Azzawi, "An Optimal Control For Complete Synchronization of 4D Rabinovich Hyperchaotic Systems," *Telkommika*, vol.18, no. 2, 2020.
- [23] Z. Sh. Al-Talib and S. F. AL-Azzawi, "Projective and Hybrid Projective Synchronization of 4-D Hyperchaotic System Via Nonlinear Controller Strategy," *Telkommika*, vol.18, no. 2, 2020.
- [24] A. S. Al-Obeidi and S. F. AL-Azzawi, "A Novel Six-Dimensional Hyperchaotic System with a Self-Excited Attractors and Its Chaos Synchronization," *International Journal of Computing Science and Mathematics*. vol.11, 2020.
- [25] M. M. Aziz., S. F. AL-Azzawi., "Some Problems of Feedback Control Strategies and its Treatment," *Journal of Mathematics Research*, vol. 9, pp. 39-49, 2017.
- [26] F.Q. Wang and C.X. Liu, "Hyperchaos Evolved From the Liu Chaotic System," *Chin. Phys.* vol. 15, pp. 963–968, 2006.