Al-Salam Journal for Engineering and Technology
Journal Homepage: http://journal.alsalam.edu.iq/index.php/ajest
ISSN: 2790-4822

A Review in Use of 4D Hyper chaotic Systems and DNA for Image Encryption

Sahera Abued Sead Almola[1,*]
Department of information system, College of Computer Science and Information Technology, University of Basrah, Iraq

Corresponding Author: Sahera Abued Sead Almola

DOI: https://doi.org/10.55145/ajest.2023.01.01.0011
Received October 2022; Accepted December 2022; Available online Junuary 2023

ABSTRACT: Recently, the color image encryption technique using the chaotic system and DNA bases has attracted great interest from the research community.The current research presents a study in an efficient method for color image encryption by using Hyper-chaotic Lorenz system with Hyper-chaotic Rösler system and DNA coding. Where the Secure Hashing Algorithm-256/384 was presented first, due to the need for chaotic systems to have initial values (primary key), which are obtained using this hashing function.Then the study presented the use of Hyper-chaotic Lorenz system and its chaotic sequences generated, as it turns the normal color image into a distorted image. By mixing the three components (red, green and blue) of the color image. Finally, the use of a combination of methods to encode mixed components is shown to achieve significant randomness, Hyper-chaotic Rösler system is shown as well as XOR operations are applied between image DNA components and DNA sequences that are generated on the basis of Hyper-chaotic Rösler system. then decode the DNA components of the image; Thus, the final encoded image is generated. The use of these methods of encryption is more efficient when compared to the previous many color image encryption algorithms, as these methods are safer for attacks, and this was proven by studying the histogram (graph) in addition to the use of DNA and its characteristics, the most important of which is DNA encryption additional technique. It has characteristics, such as wide parallelism and large storage capacity, which make it a very promising field and thus use DNA and messy functions will provide image protection in an efficient way. Messy maps and DNA technology are two of the most popular topics currently used in image coding, in combination or separately. These two technologies have good security features and can be used to secure digital images. Chaotic systems' sensitive initial conditions, unpredictable and non-periodic ideal statistics, and other attributes enable them to build secure cryptographic systems. Numerous beneficial properties of computational parallel DNA computing have been discovered on a large scale, less power loss, and a large amount of storage space. This is what this study sought to find an encryption technology that maintains a high level of strength against encryption attacks.

Keywords: Encryption, DNA, Chaotic System, Image, hybrid chaotic, decryption

1. INTRODUCTION

Information is one of the most important things that a person wants to keep and share in order to be safe from attacks of various kinds [1]. This means that only authorized persons can access their personal information. To keep information secure, it must be hidden from unauthorized persons. In our time, Internet networks have become an essential part of storing information, as well as transferring it from one place to another, which can be, for example, text, images, audio, or video. In order for the information transfer process to take place, its confidentiality and integrity must be preserved [2]. Therefore, information can be penetrated at any point between the source and destination, so that Internet networks face different types of information threat [3] The use of images in a variety of applications is increasing nowadays. In addition, many of these applications such as confidential video conferencing, military image communications medical imaging systems, and others require reliable security in storing and transmitting digital images. In the field of information security, image encryption plays a major role. Many encryption algorithms have been proposed in order to provide security, and to change the image to a less recognizable image. This is what the image encryption technology means [4], and then again from an encrypted image the decryption is made and the original image is restored.Encryption is a method that allows only the parties who have permission to access [5] to know and view the information, whether the encryption is a message, a picture, or any other information, it generally maintains the confidentiality of the information. But the image file size is larger than other digital data such as text or sound [6]. This leads to the fact that encoding digital images requires large amounts of computational information,

*Corresponding author: author@organization.edu.co

hence the need to devise special algorithms to deal with this type of data. Conventional encryption techniques such as Advanced Encryption Standard (AES) [7] and Data Encryption Standard (DES) [8] are good but most of the traditional encryption of text data is developed without considering the individual properties of image files[9]. However, due to the difference between the size of the image files and other data, the encryption algorithms require a very large amount of computation. This means that the above-mentioned methods are not only ineffective but also less secure [10]. Messy mapping and DNA technology are currently the most popular methods for encrypting images. These two technologies have good security features and can be used to secure digital images [11].

The rest of this paper is organized as follows: Section 2 introduces the definition of encryption. Section 3 introduces chaos theory. Section 4 describes DIFFUSION phase , Section 5 describes the DNA and coding. Section 6 presents conclusions. Finally, he presents future work in Section 7.

2. ENCRYPTI

While IT security seeks to protect our physical assets - networked computers, databases, servers, and so on - encryption protects the data that lives on and between those assets. It is one of the strongest ways to keep data secure, and although it cannot be hacked, it is a great deterrent to hackers. Even if the data were stolen, it would be unreadable and almost useless if encrypted.Cryptography based on the ancient art of cryptography uses computers and algorithms to convert plain text into unreadable code. To decrypt this ciphertext into plaintext, we need an encryption key, which is a string of binaries (0,1) that decrypt the text[12]. The key is the only thing that you or the intended recipient has. Computers can crack the code by guessing the encryption key, but for highly sophisticated algorithms, this may take a very long time as shown in Fig. 1.

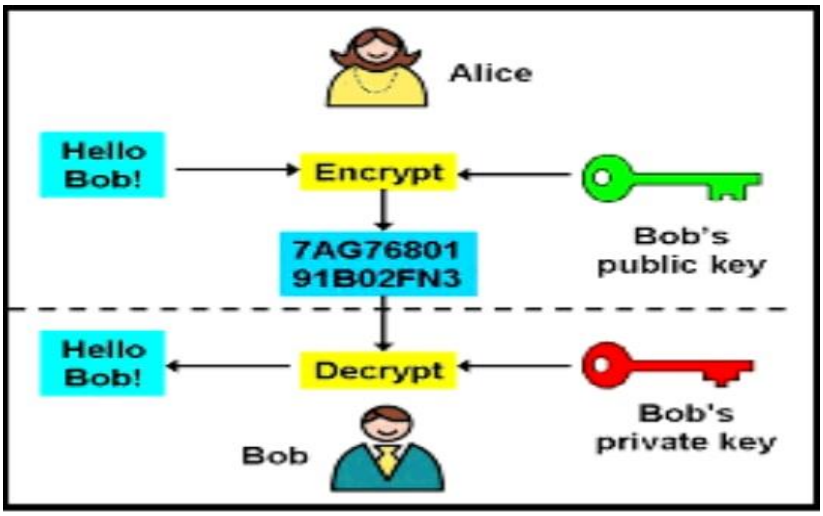


FIGURE 1. - Protecting Information From Hacking

Encryption is able to provide a number of security objectives to keep data confidential from hacking using encryption software. Given the security advantages of encryption, encryption has many applications today [13].The goals of encryption can be summarized as follows [14]:-

1.Confidentiality: The data transmitted in the computer must be accessible only to the authorized party and not accessible to unauthorized parties.

2.Authentication: Obtaining proof that the received information came from a person who has the authority to transmit, for example the identity of the sender.

3.Integrity: giving full authority to the parties authorized to amend the information that was sent and prohibiting the modification of the parties who are not authorized to access the information between the sender and the receiver.

4.Non-denial: The transmission request cannot be rejected between the receiver and the transmitter.

.5.Access Control: Private parties have full access to certain information

3. CHAOS THEORY

The term chaos does not have a uniform definition but it can be defined by observing the phenomenon in nature. Chaos or randomness and order are opposites and interdependent with the system. Present chaos theory is used to predict future behavior. Its use in everyday life is increasing. Chaos theory is the study of complex, nonlinear, and dynamical systems [15]. It is a branch of mathematics that deals with systems that appear to be ordered (deterministic) but, in fact, perform chaotic behaviors. It also deals with systems that appear chaotic, but actually have a fundamental order. Chaos theory studies the behavior of dynamical systems that are highly sensitive to initial conditions, an effect commonly referred to as the butterfly effect. Chaos is the science of surprises, the science of nonlinearity and the unexpected. It teaches us to expect the unexpected. Chaos theory deals with nonlinear things that are impossible to predict or control effectively, such as turbulence, weather, the stock market, states of our brains, etc., while most traditional science deals with supposedly predictable phenomena such as gravity, electricity, and chemical reactions. Many natural objects exhibit fractal properties, including landscapes, clouds, trees, organs, and rivers. Many systems exhibit complex and chaotic behavior. Realizing the chaotic and fractal nature of our world can give us new insight, strength, and wisdom. In other words, chaos theory studies the behavior of dynamical systems that are highly sensitive to initial conditions and response commonly referred to as the butterfly effect. Small differences in the initial conditions lead to widely different outcomes for such dynamic systems, making long-term prediction generally impossible. This occurs even though these systems are deterministic, meaning that their future behavior is determined entirely by their initial conditions, with no random elements involved. The deterministic nature of any system does not make it predictable. This behavior is known as deterministic chaos Simply a mess. This theory was summed up by Edward Lorenz [16]. Among the most important steps of encryption using chaotic methods are:-

A. Generate the secret key

Since the generation of the primary key plays a major role in the encryption process, we assume that both the sender and the user share one key in this algorithm. Since a single key is used for both encryption and decryption, these are known. *SKC* method in the name of secret key encryption. The most desirable feature of any image encryption algorithm is to make the secret key as strong as possible. So that it cannot be hacked and protected from being discovered by unauthorized parties. Therefore, the key is generated in a rather complicated way, so that it is difficult for an attacker to know and predict the key. The hash of the original image is used to generate the secret key. The image initialization operations are first done before applying the encryption steps. These operations include:

1. Inserting the color image: In this step, the image to be encoded is entered.
2. Image scaling: The reason for the standardization process is the possibility that the image comes in a very large or small size, so in this process the image is made to a suitable size for the work, the standardization is 100 * 100.
3. Converting image data into symbols: It is known that the hash function that is used to generate the secret key works on symbols, so the image data is converted into symbols.

The secret key generation scheme is as shown in Fig. 2 which is a hashing algorithm that typically converts a plain text/image or password into a fixed-length string of characters. Hash codes, hash values, hash sums, or simply hashes are the values returned by the hash function matrix.. The steps to create the secret key are as follows:

Step 1: The original key is generated by the *SHA-256* hash function

Where the image is entered into the function, as in equation (1):-

$$K_0 = f_{SHA-256}(I_0) \qquad (1)$$

Where as

I_0 represents the original image. Through hashing using SHA-256

We can get, K_0

It is a one-time key because K_0 differs in different images, i.e. the output of this function is a string of 256-bit bits.

This value is usually represented as a 64-digit hexadecimal number. It results in a large difference between two images if a single bit change occurs in the hash value input. This increases the security of the image, as changing one bit will produce a radically different image from the input image, and here proves the strength of encryption.

Step 2: To add more complexity and strength to the secret key, the previous step is inserted into the hash function 284, as in the following equation (2):-

$$K_i = f_{SHA-384}(K_0) \qquad (2)$$

Step 3: The initial key can be used to obtain the initial parameters of the chaotic system once it has been generated, K_i =*384*bit, Divided into 8-bit blocks and we get 48 blocks *b1, b2, . . . , b48,* Then, all 4 blocks are stacked together, making 12 group*(G1, G2, ..., G12)*, As in the following equation (3).

$$G_i = \{b_{4i-3}; b_{4i-2}; b_{4i-1}; b_{4i}\}, (1 \le i \le 12) \qquad (3)$$

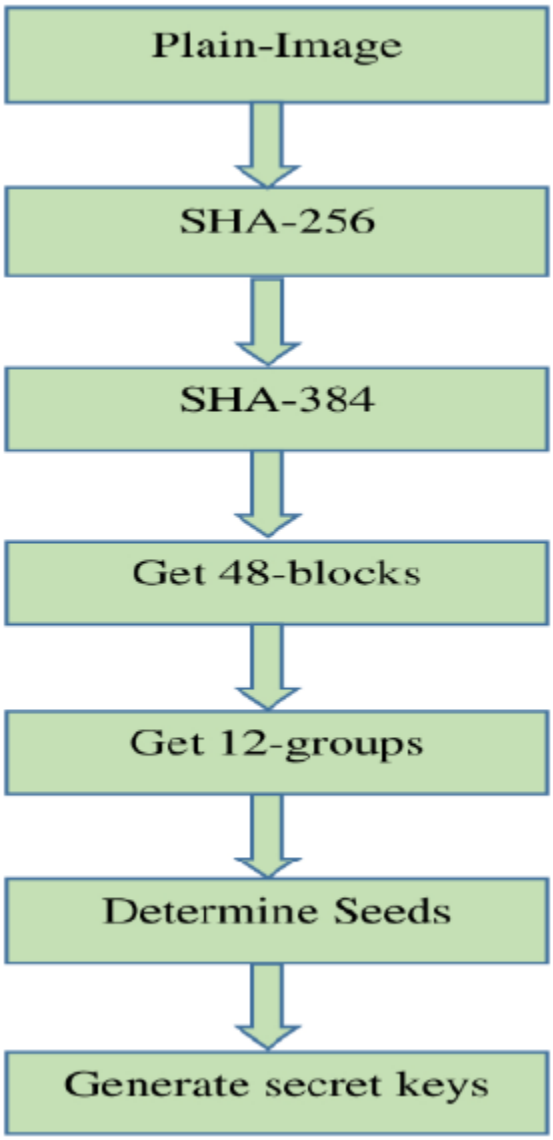


FIGURE 2. Schematic diagram of secret key generation

Step 4: Seed according to our chaotic systems *S1, S2, . . ., S12* as follows:

$$S_i = \sum_{M=0}^{3} \frac{b_{4i-m}}{2^6}, (1 \le i \le 12) \qquad (4)$$

Step 5: The final keys are obtained by applying equation (5) to the seeds calculated in the previous stage:-

$$\begin{aligned} X_1 = A_1 &= S_1 + S_2 + S_3 \\ Y_1 = B_1 &= S_4 + S_5 + S_6 \\ Z_1 = C_1 &= S_7 + S_8 + S_9 \\ W_1 = D_1 &= S_{10} + S_{11} + S_{12} \end{aligned} \qquad (5)$$

B. Hyper-chaotic Lorenz system

Since the chaotic sequence formed by the Hyper-chaotic Lorenz system [17] has greater unpredictability and randomness, it is used to encode the image . The chaotic Lorenz system can be determined mathematically as in the following equation(6)

$$\begin{cases} \hat{X} = a(Y - X) + W \\ \hat{Y} = cX - Y - XZ \\ \hat{Z} = XY - bZ \\ \hat{W} = -YZ + rW \end{cases} \quad (6)$$

When *X,Y,Z,W* are system state variables. The control parameters of the system are *a,b,c and r*.
After generating the chains, we arrange the chains, two of which are ascending and two descending, and this process (arrangement) increases the randomness because the chains that are generated in Lorenz.

$$\begin{cases} [\sim, Index_x] = sort(X,' ascend') \\ [\sim, Index_y] = sort(Y,' descend') \\ [\sim, Index_z] = sort(Z,' ascend') \\ [\sim, Index_w] = sort(W,' descend') \end{cases} \quad (7)$$

C. Mixing process using chaotic sequences

Step 1: The color image is formatted and segmented. The image must be separated into the layers that make it up, which are red, green and blue. Then I work with each layer and try to produce a shape for the image after its segmentation, as shown in Fig. 3.

FIGURE 3.: (a) Image Lina (100 x 100), (b) Red layer (c)Green layer (d) Blue layer

Step 2: Mix the pixel positions using the Lorenz sequences, so that they swap their positions according to the four series and sequentially for all the chains, and get Y, then swap according to the second series *X* of the Lorenz sequences, mixed matrices, so a shape is produced after the switching process (an encrypted image). The switch is applied to all layers (red, green, and blue).

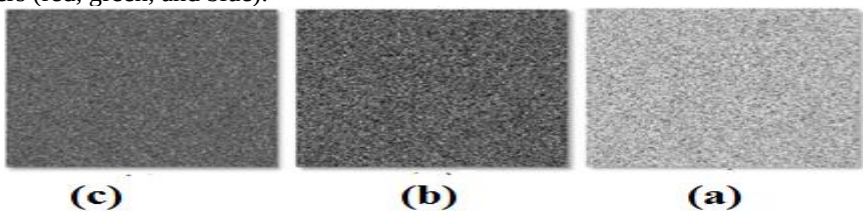


FIGURE 4. Mixed images (a) Red (b) green. (c) blue.

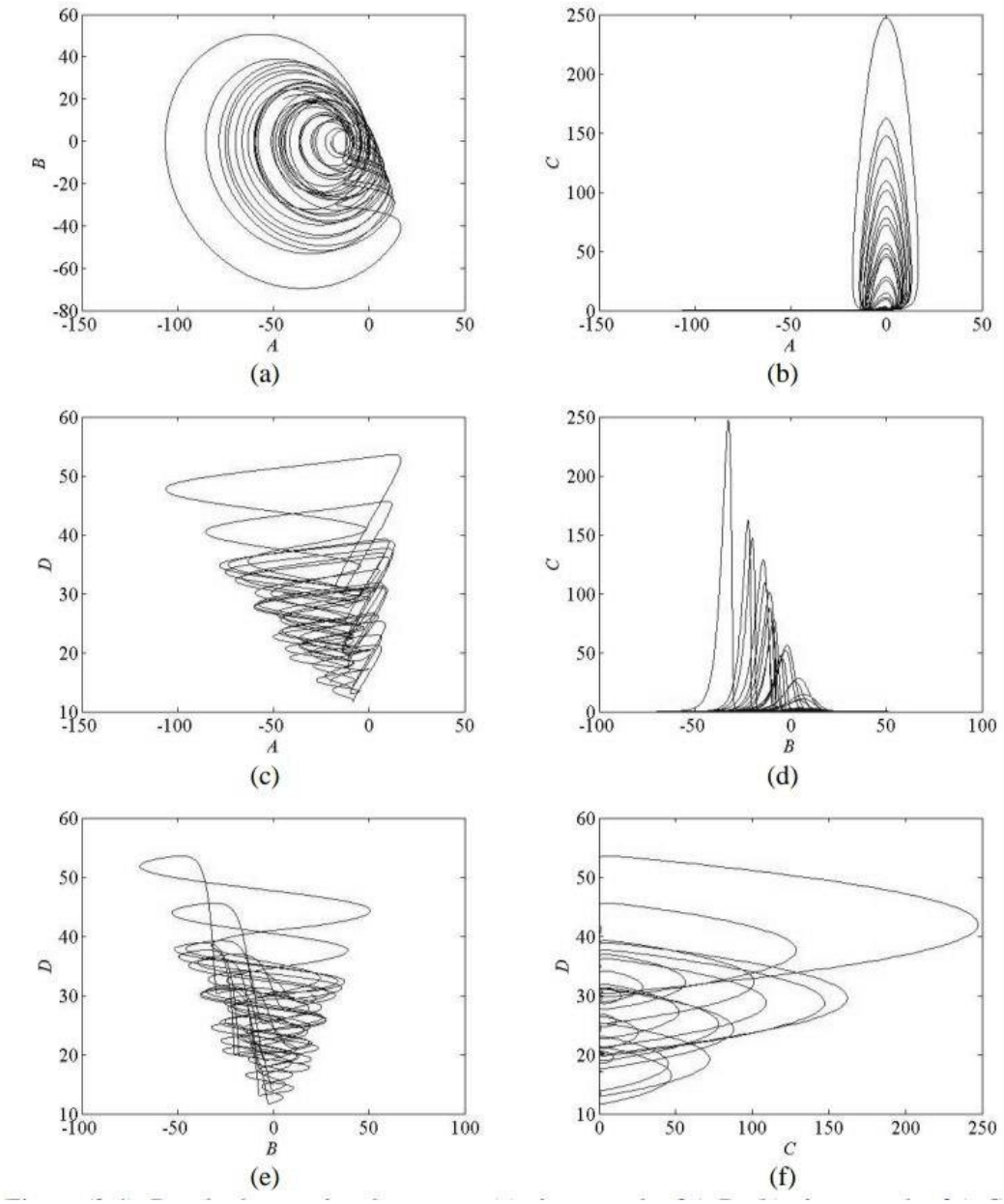
D. Hyper-chaotic Rossler system

The Hyper-chaotic Rossler system [18] is a nonlinear dynamical system. It is characterized by the features of unpredictability, sensitivity to control parameters and initial conditions. Since these properties are compatible with cryptographic research, it is used in image ciphers [19] Equation (8) describing Hyper-chaotic Rossler system is given below:

$$\begin{cases} \acute{A} = -B - C \\ \acute{B} = A + \alpha B + D \\ \acute{C} = \beta + CA \\ \acute{D} = \gamma D - \delta C \end{cases} \quad (8)$$

That is, (A, B, C, D) are the basic variables, and (β,α, γ, δ,) are the control parameters. When

(α = 0.25, β = 3, γ = 0.05, and δ = 0.5) the above system is in an extremely chaotic state. Charts the branching of the six states *(A - B, A - C, A - D, B - C, B - D, and C - D)* are shown in Fig. 5



.

FIGURE 5. The Rossler Hyper-Chaotic System: (a) Plane graph of AB (b) Plane graph of AC (c) Plane graph of AD, (d) Plane graph of BC, (e) Plane graph of BD, (f) Graph of CD.

4. DIFFUSION PHASE

In the previous operations, the locations of the image were changed, while the values remained the same, and this may expose the image to attack because the image was encrypted with the results obtained in the previous form, but it may have a weakness in terms of histogram. In this step, the image values are changed according to the following steps:

Step 1: The step of generating the chaotic Roesler strings Here, 4 Roesler strings are generated as in equation (9) and depend on the secret key that was previously generated

$$A=[A_1,A_2,A_3,\ldots\ldots\ldots\ldots\ldots A_{MN}]$$
$$B=[B_1,B_2,B_3,\ldots\ldots\ldots\ldots\ldots B_{MN}] \quad (9)$$
$$C=[C_1,C_2,C_3,\ldots\ldots\ldots\ldots\ldots C_{MN}]$$
$$D=[D_1,D_2,D_3,\ldots\ldots\ldots\ldots\ldots D_{MN}]$$

, where image-sized strings are generated

They are random strings and we try to delete the repeated and initial values until we get the values of four strings the size of an image and according to equation (9)

Step 2: The step of finding the number of laws that we use in the addition process by converting the first series from into values between (0-7) according to equation (10)

DNA The benefit of these values is to be used to determine the 8 laws. Which of these laws is used in the addition process in the next steps? This step is dynamic in the addition process because each element will generate a different number than the element after it, and these numbers are confined between 0-7, for example, element 3. It generates a value of 4, i.e. the collection of elements is according to base 4, for example, with element 7, the value of 6 is generated, so the collection of elements is according to base 6, and so on... If the numbers that are generated for this series after conversion are the ones that will be the numbers of the rules that will be used in the operations.

$$A = mod(round(A * 10\text{^}4),8) \quad (10)$$

Step 3: We take the rest of the strings that belong to Rossler *B, C, and D* each of these chains we convert

Its values to a range between (0-255) according to equation (11) so that when performing the *XOR* operation with the image data, the data is supposed to be equivalent with values confined between (0-255), while these strings

B,C,D When generating these strings from Rossler, they are random fractional values. Therefore, when using the *XOR* between the two parts, these 3 strings must also be confined between (0-255).

$$B=mod(round(B*10\text{^}4),256)$$
$$C=mod(round(C*10\text{^}4),256) \quad (11)$$
$$D=mod(round(D*10\text{^}4),256)$$

5. DNA AND CODING

DNA is named after the genes that store the information of our cells Contains instructions for building and working cells. It is the key to genetic inheritance. *DNA* is the source code for life. One cubic cm of *DNA* can store 10 terabytes of data [19] Fig. 6 shows how digital data is encoded in DNA sequences and the latter is decoded and returned to digital data[20].

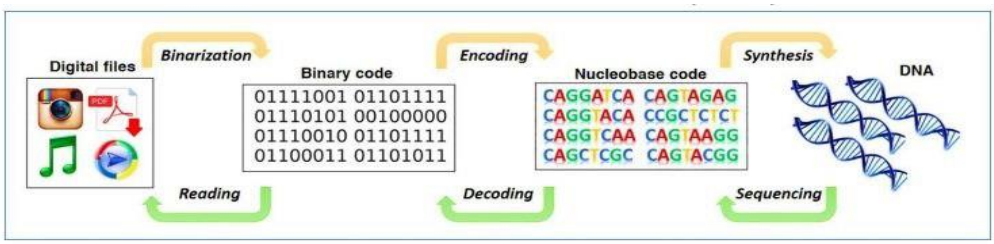


FIGURE 6. *DNA* and coding

DNA cryptography is a new field that has developed as a result of advances in *DNA* computation. Recently, it was discovered that *DNA* is capable of storing large amounts of data [31] *DNA* cryptography is an emerging technology. It is a new technology that is used to securely store data while at rest and also in motion. *DNA* cryptography has shown new ways of securing data. *DNA* provides data security with the help of its nucleotides. These nucleotides contain four nitrogen bases, a phosphate group and a carbon sugar and they are adenine, cytosine, guanine and thymine. They are abbreviated as *A, C, G, and T,* respectively. These have a unique sequence structure, making them the basis for coding *DNA*. Such a *DNA* structure makes living organisms unique. Likewise, the use of their encryption techniques makes

encryption algorithms unbreakable. It has the following important properties [21]:
1.Data storage capacity: DNA has a data density of about one bit per cubic nanometer, while traditional storage technologies require 1012 cubic nanometers to hold a single bit.

2.Data Security: Data security is required by the community. DNA provides this ability because its unique structure makes data encryption algorithms unbreakable.

3.Energy Requirements: Less energy is required to compute DNA because the chemical bonds of DNA work without any external force. As digital data is under constant threat, new approaches to securing data are needed. Organizations need to be ahead of attackers to protect their data and customer information for future needs.

5.1 DNA CINDING AND COMPUTEING PROCESSES

Here as four deoxy *DNA* nucleotides which are *A, G, C and T* bases. Among them *G* and C are complementary, as well as *A and T*. Normally in binary system, 0 and 1 are complementary to each other. Thus, 00, 11, 01, 10 can be encoded in The four rules. According to the structures, there are 24 possible types of *DNA* coding methods. Given the complementary relationship between only the four 8 coding groups, it is effective, as shown in Table (1). In image coding, the gray value of an image pixel can be expressed as its corresponding binary sequence, and then this binary sequence can easily be encoded into a *DNA* sequence. On the other hand, a *DNA* sequence can easily be translated into a pixel value. For example: the pixel value is 196 and its binary sequence is 11000100 . can be encoded into a *GCAC DNA* sequence using *DNA* encoding rule 4. and applying *DNA* decoding rule 6 to this sequence, the pixel value retrieved is 55 [22]. Furthermore, different operations have been applied to the *DNA* sequence to encode the image. As with binary digits, the DNA sequence can be added and XORed in the same way, and the results are affected by the rule used to perform these operations. Details of the *DNA* addition process according to rule 0 and *DNA XOR* process according to rule 4 are shown in Table (2) and Table (3) respectively.

Table 1. DNA encoding rules.

Rule	Rule 0	Rule 1	Rule 2	Rule 3	Rule 4	Rule 5	Rule 6	Rule 7
00	A	A	T	T	C	C	G	G
01	C	G	C	G	A	T	A	T
10	G	C	G	C	T	A	T	A
11	T	T	A	A	G	G	C	C

Table 2. ADD operation DNA.

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

Table 3. XOR operation DNA.

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

6. CONCLUSION

Based on what was previously suggested, the use of a combination of the *SHA-2* hash function, highly chaotic systems, and *DNA* in encryption. It will lead to the design of a secure and strong algorithm for encrypting color images. Chaos theory applications have made great progress in recent years, and are now widely used in the field of network and communications security. The following can be concluded:-

1.Encryption in this way enjoys a high level of security, as the use of highly chaotic systems will produce eight chaotic chains, four of which are used to mix pixel locations and dismantle the interrelationships between them (confusion process, i.e. the link between adjacent pixels is reduced to resist statistical attacks in the vertical, horizontal and

diagonal directions) . The other four are used to change the pixel value (diffusion process). Additional technologies, *SHA-256 and SHA-384* are used to act as a power source for normal image sensitivity by mixing.

2.The initial key for chaotic systems is based on the original color image, which makes prediction more difficult.

3..Any change in the parameter of the chaotic system has a direct effect on the chaotic sequences. As a result, the initial values will have a significant impact on the outcome of the encoding or decoding process.

4.To increase security, do not use the initial part of the generated chaotic sequences, and instead choose the last part of the chaotic sequences.

5.Dynamic *DNA* addition process, in which the addition rules are based on the chaotic matrix, can add more security. *DNA* encryption is an additional technology with characteristics such as wide parallelism and large storage capacity.

6.. The histogram of the encoded image has been uniformly distributed as in Fig. 7. It can be concluded that when the method is used in encryption, it will be effective in thwarting the histogram attack.

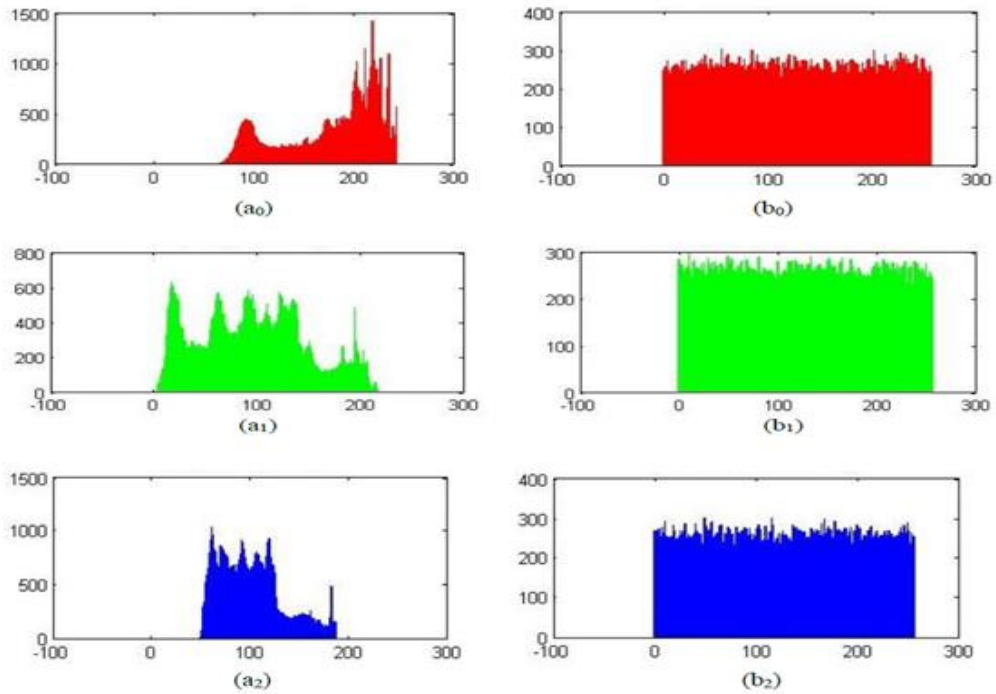


FIGURE 7: Histogram Analysis; *(a0, a1, a2)* shows the histograms for channels (red_com., green_com., and blue_com.) of plain Lena image; (b0, b1, b2) shows the histograms of the encrypted image for channels (red_com., green_com., and blue_com.) of image Lena.

7. FUTURE WORKS

Here is a summary of future work:-

1. The use of this study to design an algorithm to encode images, videos and speech

2. Combine image encryption with image data compression technology to achieve image security with appropriate compression.

3.Using a highly chaotic new system with high precision control values is an important aspect of stochastic cryptography in order to expand the key space and increase security.

4.It is suggested that parallel methods be used, which saves time while encoding images.

ACKNOWLEDGEMENT

Authors would like to thank the anonymous reviewers for their valuable comments

CONFLICTS OF INTEREST

The authors declare no conflict of interest

Funding

No funding received for this work

References

[1] C Li, G. Luo, and C. Li, "An Image Encryption Scheme Based on The Three dimensional Chaotic Logistic Map.," Int. J. Netw. Secur., vol. 21, no. 1, pp 22–29, 2019, doi: 10.6633/IJNS.201901 21(1).04

[2] D.A.Trujillo-Toledo, O.R.López-Bonilla, E.E.García-Guerrero, E.Tlelo-Cuautle, D.López-Mancilla, O.Guillén-Fernández, and E.Inzunza-González, "Real-time RGB Image Encryption for IoT Applications Using Enhanced Sequences From Chaotic Maps," Chaos, Solitons & Fractals, vol. 153, p. 111506, 2021, doi: 10.1016/j.chaos.2021.111506.

[3] V. Kakkad, M. Patel, and M. Shah, "Biometric Authentication and Image Encryption for Image Security in Cloud Framework," Multiscale Multidiscip. Model. Exp. Des., vol. 2, no. 4, pp. 233–248, 2019, doi: 10.1007/s41939-019-00049-y.

[4] X. Wang and L. Liu, "Image Encryption Based on Hash Table Scrambling and DNA Substitution," IEEE Access, vol. 8, pp. 68533–68547, 2020, doi: 10.1109/ACCESS.2020.2986831

[5] S. Mozaffari, "Parallel Image Encryption With Bitplane Decomposition and Genetic Algorithm," Multimed. Tools Appl., vol. 77, no. 19, pp. 25799–25819, 2018.

[6] T. Sivakumar and R. Venkatesan, "A Novel Image Encryption Approach Using Matrix Reordering," WSEAS Trans. Comput., vol. 12, no. 11, pp. 407–418, 2013.

[7] James Nechvatal, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, and Edward Roback, "Report on the Development of the Advanced Encryption Standard (AES)," J. Res. Natl. Inst. Stand. Technol., vol 106, no. 3, p. 511, 2001.

[8] F. Pub, "Data Encryption Standard (DES)," FIPS PUB, pp. 43–46, 1999.

[9] L. Chen, H. Yin, L. Yuan, J. A. T. Machado, R. Wu, and Z. Alam, "Double Color Image Encryption Based on Fractional Order Discrete Improved Henon Map and Rubik's Cube Transform," Signal Process. Image Commun., vol. 97, p. 116363, 2021

[10] Leo Yu Zhang, Yuansheng Liu, Fabio Pareschi, Yushu Zhang, Kwok-Wo Wong, Riccardo Rovatti, and Gianluca Setti, "On the Security of a Class of Diffusion Mechanisms for Image Encryption," IEEE Trans. Cybern., vol. 48, no. 4, pp. 1163– 1175, 2017.

[11] M. G. A. Malik, Z. Bashir, N. Iqbal, and M. A. Imtiaz, "Color Image Encryption Algorithm Based on Hyper-Chaos and DNA Computing," *IEEE Access*, vol. 8, pp. 88093–88107, 2020.

[12] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "A Novel Color Image Encryption Algorithm Based on DNA Sequence Operation and Hyper-Chaotic System," *J. Syst. Softw.*, vol. 85, no. 2, pp. 290–299, 2012.

[13] A. Kumar and N. S. Raghava, "An EfficientImage Encryption Scheme Using Elementary Cellular Automata with Novel Permutation Box," Multimed. Tools Appl., vol. 80, no. 14, pp. 21727–21750, 2021.

[14] L. A. Shihab, "Technological Tools for Data Security in the Treatment of Data Reliability in Big Data Environments," Int. Trans. J. Eng. Manag. Appl. Sci. Technol., vol. 11, no. 9, pp. 1–13, 2020.

[15] S. A. Mehdi and Z. L. Ali, "Image Encryption Algorithm Based on a Novel SixDimensional Hyper-Chaotic System," Al-Mustansiriyah J. Sci., vol. 31, no. 1, p. 54, 2020.

[16] E. N. Lorenz, "Deterministic Nonperiodic Flow," J. Atmos. Sci., vol. 20, no. 2, pp. 30–141, 1963.

[17] X. Wang and M. Wang, "A Hyperchaos Generated from Lorenz System," Phys. A Stat. Mech. its Appl., vol. 387, no. 14, pp. 3751–3758, 2008

[18] O. Rossler, "An Equation for Hyperchaos," Phys. Lett. A, vol. 71, no. 2–3, pp. 155– 157, 1979.

[19] X. Zhang, L. Wang, Z. Zhou, and Y. Niu, "A Chaos-Based Image Encryption Technique Utilizing Hilbert Curves and H-Fractals," IEEE Access, vol. 7, pp. 74734– 74746, 2019.

[20] S. A. El-Seoud, R. Mohamed, and S. Ghoneimy, "DNA Computing: Challenges and Application.," Int. J. Interact. Mob. Technol., vol. 11, no. 2, 2017.

[21] J. K. Panjiyar, "From Punch Card to DNA Data Storage," 2018. https://medium.com/zerone-magazine/from-punch-card-to-dna-data- storage5c15dcc4803e.

[22] X. Zhang and Y. Hu, "Multiple-Image Encryption Algorithm Based on the 3D Scrambling Model and Dynamic DNA Coding," Opt. Laser Technol., vol. 141, p. 107073, 2021.

[23] M. Jarjar, S. Hraoui, S. Najah, and K. Zenkouar, "New Technology of Color Image Encryption Based on Chaos and Two Improved Vigenère Steps," Multimed. Tools Appl., pp. 1–25, 2022.