Received: November 5, 2024. Revised: December 2, 2024.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

A New Image Encryption Method Combining the DNA Coding and 4D Chaotic Maps

Salah Taha Allawi[1]* **Yasamin Hamza Alagrash[1]**

[1]*Computer Science Department, College of Science, Mustansiriyah University, Baghdad, Iraq*
* Corresponding author's Email: salah.taha@uomustansiriyah.edu.iq

Abstract: With the tremendous technological progress in many fields, especially in communications, and to protect the information transmitted through communication channels, especially digital images, researchers in this field try to find new methods that provide a high level of security. Combining chaotic maps and DNA encryption provides a high level of security because of their high randomness, complexity, and sensitivity to initial conditions. This study presents a novel technique for protecting images by encrypting their data at three levels. The first level involves redistributing the image points. In contrast, the second level combines a 1D chaotic map (PWLCM) and DNA sequences. In the third level, three keys are produced using three 1D chaotic maps (Logistic maps, Tent maps, and Sine maps). Each key encrypts data of a specific color. The results of the statistical tests showed that the suggested technique provides a good security level compared to the methods, achieving an average Number of Pixels Change Rate (NPCR) of 99.62, a Unified Average Changing Intensity (UACI) of 32.83, and an entropy of 7.9972.

Keywords: Image encryption, DNA coding, Chaotic maps, Statistical tests.

1. Introduction

With the increase in Internet use and the increasing fame of social networking platforms, images have become a popular medium for sharing content online. However, these images are endangered by unauthorized interception, modification, or devastation. Researchers focus on developing security mechanisms to protect digital images [1]. Encryption offers security for multimedia data, principally images. Various encryption types exist for image data, such as whole, selective, and partial. Therefore, any encryption type can be used, depending on the application will be used [2]. Digital images hold a large volume of personal visual data, and it is complex to fully ensure their secure transmission in community channels and confident storage in cloud environments [3]. Traditional text encryption systems such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), and International Data Encryption Algorithm (IDEA) cannot meet the needs of image encryption because digital images differ from text information in terms of large data size, redundancy, and pixel correlation [4–7].

Because of the chaos theory's characteristics, such as the ability to produce random sequences and sensitivity to changes in time, chaos-based cryptography is widely used in image encryption. It offers advantages such as high randomness, complexity, and sensitivity to initial conditions and system parameters [5, 6, 8].

DNA sequences and DNA computing have emerged as a recent area of research. As a result, the technology for encoding, reading, and writing information using DNA molecules as a storage medium, along with encryption and information-hiding techniques based on various DNA structures and reactions, is becoming increasingly accessible [9]. Current encryption methods that utilize DNA coding offer robust security, as DNA's natural building naturally makes it an ideal medium for encoding binary pairs [7, 10, 11]. Due to the combined benefits of DNA coding and chaotic systems, scientists incorporate both in image cryptosystems to create

more secure and robust systems that are harder to penetrate or break [12, 13].

Confusion and diffusion are crucial features of any cryptosystem, as they introduce randomness to the output. Diffusion obscures the connection between plain and ciphertext, making it impossible to determine the original message. Conversely, confusion complicates the relationship between the ciphertext and the encryption key [14].

Many general image encryption systems have been proposed over the past few decades and have reached a certain level of security. With technological development in all fields, especially information security, modern and advanced systems must be developed to protect image information. This paper aims to present a new image encryption technique that uses four 1D chaotic maps and DNA encryption to provide more than one level of protection. The significant contributions of this paper are:

1. Using four 1D chaotic maps to encrypt image data at multiple levels.
2. Using DNA encryption to increase security.
3. Applying the features of confusion and diffusion to provide more randomness to the encrypted image.
4. The effectiveness of the proposed method is evaluated through experiments and comparison results.

The residue of this paper comprises Section 2, which exhibits several related works, and Section 3, which displays information about DNA coding and chaotic maps. Meanwhile, the proposed method is described in Section 4. Afterwards, Section 5 shows details of the tests performed and the outcomes. Lastly, Section 6 displays the conclusions and suggests some outlook work.

2. Related work

Many image encryption methods have been proposed over the past period. This section will introduce some of these algorithms.

In 2020, Babu et al. [15] proposed a new image encryption method divided into two stages. The first stage involves separating the image into four parts and using a secure-strength algorithm, DNA sequence encryption, Arnold-Cat RSA map algorithm, and chaotic substitution encryption techniques to encrypt these parts in order. The second stage involves producing the final encrypted image by generating a random key and applying the XOR operation between the combined cipher image resulting from the first stage and the key. In the same year, Heba et al. [16] proposed a two-stage coding system. In the first stage, there are a series of steps performed on each color. First, the color data is divided into several parts, and then the sequence of these parts is rearranged. After that, the data of each part is shuffled in isolation from the rest of the parts. These operations are performed using a hybrid chaotic map. At the end of the first stage, the image is reconstructed. In the second stage, the logic of the human mitochondrial genome (mtDNA) is used to spread the previously confused pixel values.

In 2021, Yuwen et al. [17] presented a novel grayscale image encryption scheme using 3D chaotic maps and DNA sequencing operations. The scheme is designed based on the permutation and diffusion frameworks. The initial values for generating the random keys used in the encryption process are obtained by the SHA function, which takes its initial values from the image data. First, the pixel positions in the image are rearranged using the key generated by the Arnold function. Then, the image data is encrypted by applying the DNA XOR operation using the chaotic keys. In the same year, Aditya et al. [18] suggested a novel encryption scheme for color images using two keys. The first key rearranges the pixel's position in the image; the second key uses DNA coding to encrypt the image data.

In 2022, Lun et al. [19] presented a new image encryption algorithm based on DNA and 3D chaos maps. This algorithm is divided into two stages; the first involves generating three keys using a 3D Arnold map where an XOR operation is applied between one key and the image data after encoding the data with DNA codes. In contrast, the other keys are used to rearrange the positions of the pixels in the image. After that, three keys are generated using a 3D logistic map to encrypt the image data generated in the first stage. In addition, Shaista et al. [20] presented an adaptive encryption technique for color images that utilize DNA computing combined with Multiple Distinct Chaotic Maps (MDCM). They chose three chaotic maps to encrypt the blue, green, and red colors: a 2D-Henon map, a Tent map, and a Logistic map, respectively. In the proposed method, they used the statistical characteristics of the plain image, such as mean, variance, and median, to adjust the initial conditions and control parameters of all three maps dynamically.

In 2023, Alrubaie et al. [21] proposed a new image encryption algorithm based on a 2D chaotic logistic map and dynamic double-stranded DNA sequence encryption. The algorithm is divided into three steps: the first step involves rearranging the pixel location. The second step involves encrypting the image generated from the previous stage using double-stranded DNA encryption and different rules.

Table 1. Examples of challenges facing the presented methods

Method	Challenges of the Method
Ref [15]	Employing multiple encryption algorithms for different image segments adds computational complexity, which could pose challenges for real-time applications or resource-constrained systems. Managing and securely transmitting multiple keys for different encryption algorithms can increase deployment complexity and potential security risks.
Ref [16]	Employing multiple encryption phases, such as hyper-chaotic sequences and mitochondrial DNA (mtDNA) diffusion, significantly increases processing time and resource requirements. Dividing images into multiple parts and using various keys to rearrange the locations of the points in these parts and encrypting them. This may lead to the inability to retrieve the original data in case of any change, even if it is simple, in the initial values for generating any key.
Ref [17]	Combining 3D chaotic maps, DNA operations, and optimized Arnold transformations significantly increases computational complexity. The system's dependence on a large and intricate key space complicates secure key generation, distribution, and storage.
Ref [18]	The proposed algorithm has been tested on small grayscale images. The approach has not been evaluated on various test types or applications.
Ref [19]	Using multiple encryption layers, including 3D chaotic maps, 3D Arnold maps, and DNA operations, significantly increases computational complexity and implementation challenges. The management and secure transmission of multiple keys for various encryption algorithms adds complexity to deployment and creates additional security risks.
Ref [20]	Reliance on image data for key generation may prevent the recovery of the keys if the image is exposed to distortion during transmission. The method has been evaluated mainly on specific standard datasets.
Ref [21]	The method has been evaluated mainly on specific standard datasets.

Finally, the third step involves using the 2D logistic map to create keys and implemented an XOR operation between the image generated from the second step and the keys.

Researchers are integrating DNA encryption with chaotic systems to enhance the security of image encryption, as relying solely on DNA encryption is not enough. Table 1 shows some challenges facing the presented methods.

3. Methodology

3.1 Chaotic systems

Chaos theory is a mathematical field focusing on nonlinear and deterministic behavior, with high sensitivity to initial conditions and control parameters. Its unpredictable and random output signals are connected to cryptography properties like confusion and diffusion, helping researchers enhance the security level of cryptographic systems [14].

- A 1D Logistic Map features a straightforward mathematical structure and is one of the most commonly used discrete chaotic systems, exhibiting intricate chaotic behavior. The Eq. (1) represents the 1D logistic map [11, 14].

$$q_{i+1} = \mu_1 q_i (1 - q_i) \tag{1}$$

Where
- (μ_1) the control parameter in the ranges (0-4).
- (q_0) initial state (value between 0-1),
- (i) the number of iterations.
- q_{i+1} the next state value.

- The Tent Map is a basic dynamical system that shows chaotic behavior at specific values of its control parameter. The Eq. (2) represents the tent map [22]:

$$t_{n+1} = \begin{cases} \mu_2 t_n & if\ t_n < 0.5 \\ \mu_2 (1 - t_n) & if\ t_n \geq 0.5 \end{cases} \tag{2}$$

Where
- μ_2 is a control parameter in the range (0-2).
- t_n is the initial state (value between 0-1).
- t_{n+1} the next state value.
- n the number of iterations.

- The Sine Chaotic Map is a repeating map with a 1D that produces a series with chaotic behavior. [23]. The form for the sine chaotic map is displayed in Eq. (3).

$$s_{n+1} = \mu_3 . sin\ (\pi s_n) \tag{3}$$

Where
- μ_3 is a control parameter (the range 0-1).
- s_n is the initial state (value between 0-1).

- s_{n+1} the next state value.
- *n* the number of iterations.

- The *Piecewise Linear Chaotic Map* (PWLCM) is a type of chaotic map. Because of its simplicity and chaotic behavior, it is widely used in chaos-based cryptography and random number generation [24, 25]. The formula for the PWLCM is shown in Eq. (4).

$$p_{n+1} = \begin{cases} \frac{p_n}{k} & if\ p_n < k \\ \frac{1-p_n}{1-k} & if\ p_n \geq k \end{cases} \quad (4)$$

Where
- k is a control parameter in the range (0-1).
- p_n is the initial state (value between 0-1).
- s_{n+1} the next state value.
- *n* the number of iterations.

3.2 DNA sequences

Cryptography secures information over a lengthy period. In the DNA method, the bases are ordered arbitrarily, and the message data are encrypted through these bases. These novel methods form the foundation of modern cryptographic systems, which are awaited to substitute classic encryption methods.

In the mathematical field, DNA cryptography is being substituted for DNA chemistry, and the production of this safety method is almost impossible to smash using quantum or classic computational methods [26, 27].

DNA comprises four bases: cytosine (C), adenine (A), thymine (T), and guanine (G), where T pairs with A and C pair with G. Similarly, in binary code, 1 and 0 are complementary, with 11 corresponding to 00, and 01 complementing 10 [28]. There are 24 kinds of coding sets, though we only utilize 8 of them. Table 2 displays rules (2, 4, 6, and 8) [10, 27].

The plaintext is encoded by converting into ASCII in the first step, then to binary form, and finally mapped to the DNA bases A, G, C, and T, (C=01, G=10, T=11, A=00) [26]. For instance, when a pixel value is 108, its binary representation would be (**00110110**). Since DNA coding converts every two bits into one code, the resulting code would be (**ATCG**).

Table 2. The set of rules (2, 4, 6, and 8)

Rule No.	**00**	**10**	**01**	**11**
Rule 2	A	G	C	T
Rule 4	T	G	C	A
Rule 6	G	A	T	C
Rule 8	G	T	A	C

4. Proposed method

The proposed method includes three stages. In the first stage, the image pixels are redistributed. In the second stage, a 1D chaotic (PWLCM) key is generated, converting the key value and the image data to DNA codes. The XOR operation is then implemented among these codes. Finally, three 1D chaotic keys (Logistic Map, Tent Map, and Sine Chaotic Map) are generated, and the XOR operation is implemented among each key and its corresponding color. Fig. 1 illustrates the proposed method's overall structure, while algorithm 1 shows its general steps.

Algorithm 1. Overall steps for the proposed encryption method.

Input: Plain image
Output: Encrypted image

1. Input the plain image (M×N).
2. Isolate the image data into essential components (RGB).
3. Dividing the image into four equal parts
4. Rearranging the data of the four parts to create a 1D vector
5. Using the 1D chaotic map (PWLCM) to produce a key of the size (M×N).
6. Converting the color data from decimal to binary and converting it to DNA codes.
7. Converting the key data from decimal to binary and converting it to DNA codes.
8. Implemented the XOR operation among the color codes and the key.
9. Steps (3-8) are executed for each color.
10. Decoding the DNA encryption of the data of each color.
11. Using a 1D Logistic Map to produce a key of the size (M×N) to encrypt the red color data by applying the operation (XOR).
12. Using a 1D Tent Chaotic Map to produce a key of the size (M×N) to encrypt the green color data by applying the operation (XOR).
13. Using a 1D Sine Chaotic Map to produce a key of the size (M×N) to encrypt the blue color data by applying the operation (XOR).
14. Transforming the data of each color to a 2D vector.
15. Reconstructing the image.
16. The output is an encrypted image

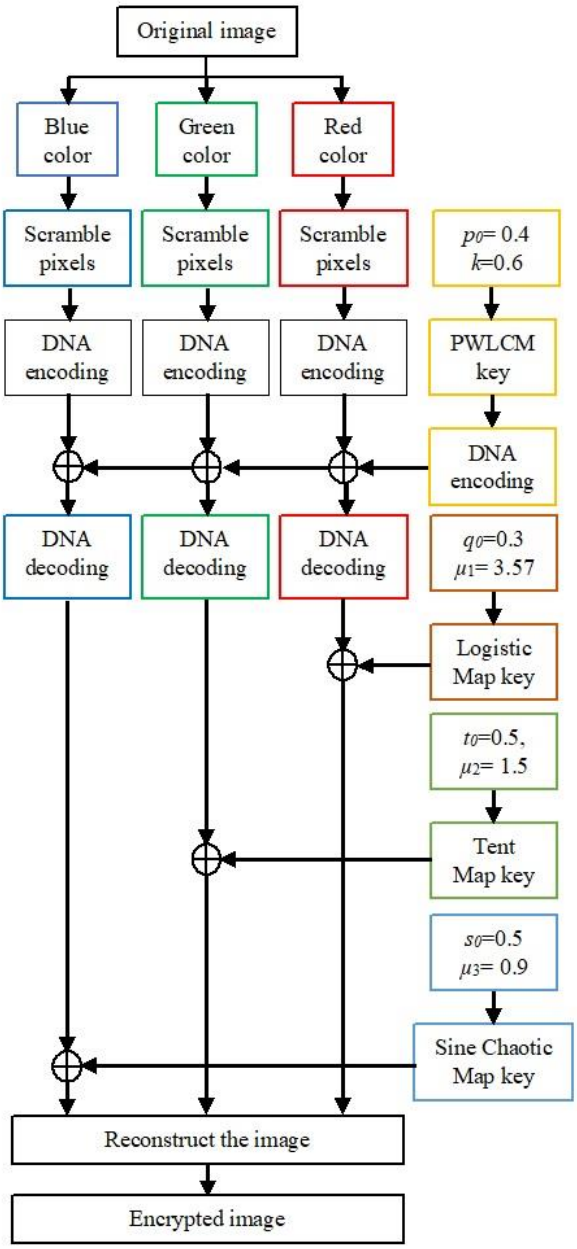

Figure. 1 The general outline for the suggested approach

4.1 Confusion stage

This stage includes several steps. First, the original image is isolated into its original RGB components. Then, in the second step, the image is

separated into four equal parts. Finally, in the third step, the locations of the points of the four parts are rearranged, and the data is converted into a one-dimensional matrix. The second and third steps are applied to each color. Fig. 2 shows the mechanism of rearranging the pixel locations.

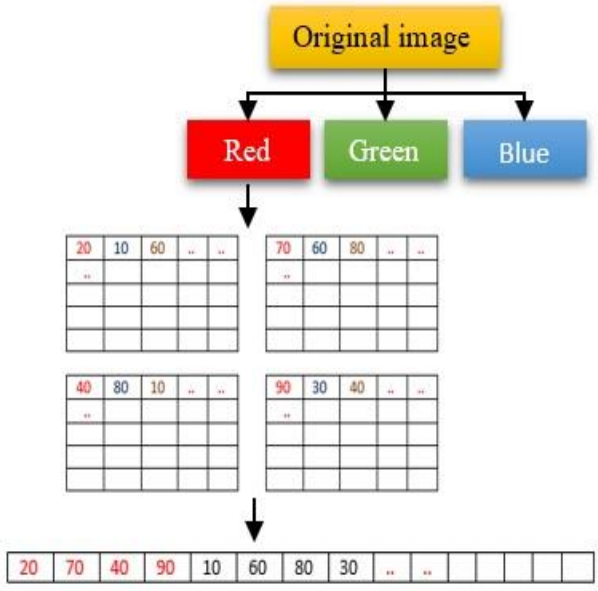

Figure. 2 Rearranging the pixel locations in the image

4.2 DNA encryption

This stage includes several steps. The first step involves produce a key using a 1D chaotic map (PWLCM). In the second stage, key and color values are converted to binary form and then encoded using DNA codes, as shown in section 3.2. In the third step, the XOR is performed between the color and key codes using four DNA encoding rules (2, 4, 6, 8). Finally, the DNA code is decoded, and the color value is converted to decimals. The control parameters and primary values used to generate the key are k = 0.6 and p_0 = 0.4. The same steps are applied to each color.

4.3 Encryption by chaotic maps

This stage performs several steps to encrypt the image in its final form. Firstly, using the chaotic maps (Logistic map, Tent map, Sine map), 3 keys are generated, each with a size equal to the image. Each key encrypts a specific color (Logistic map for red color, Tent map for green color, and Sine map for blue color). The control parameters and primary values used to create the keys are q_0 = 0.3, $\mu 1$ = 3.57, t_0 = 0.5, $\mu 2$ = 1.5, s_0 = 0.5, $\mu 3$ = 0.9. Secondly, the XOR is implemented between the values of the color and the equivalent key. Finally, the image is reconstructed by collecting the encrypted data of the three colors. Algorithm 2 shows the general steps of the data encryption process in this stage. Fig. 3 shows examples of the first 100 elements in the random sequence generated by chaotic maps (logistic, tent, sine, and PWLCM).

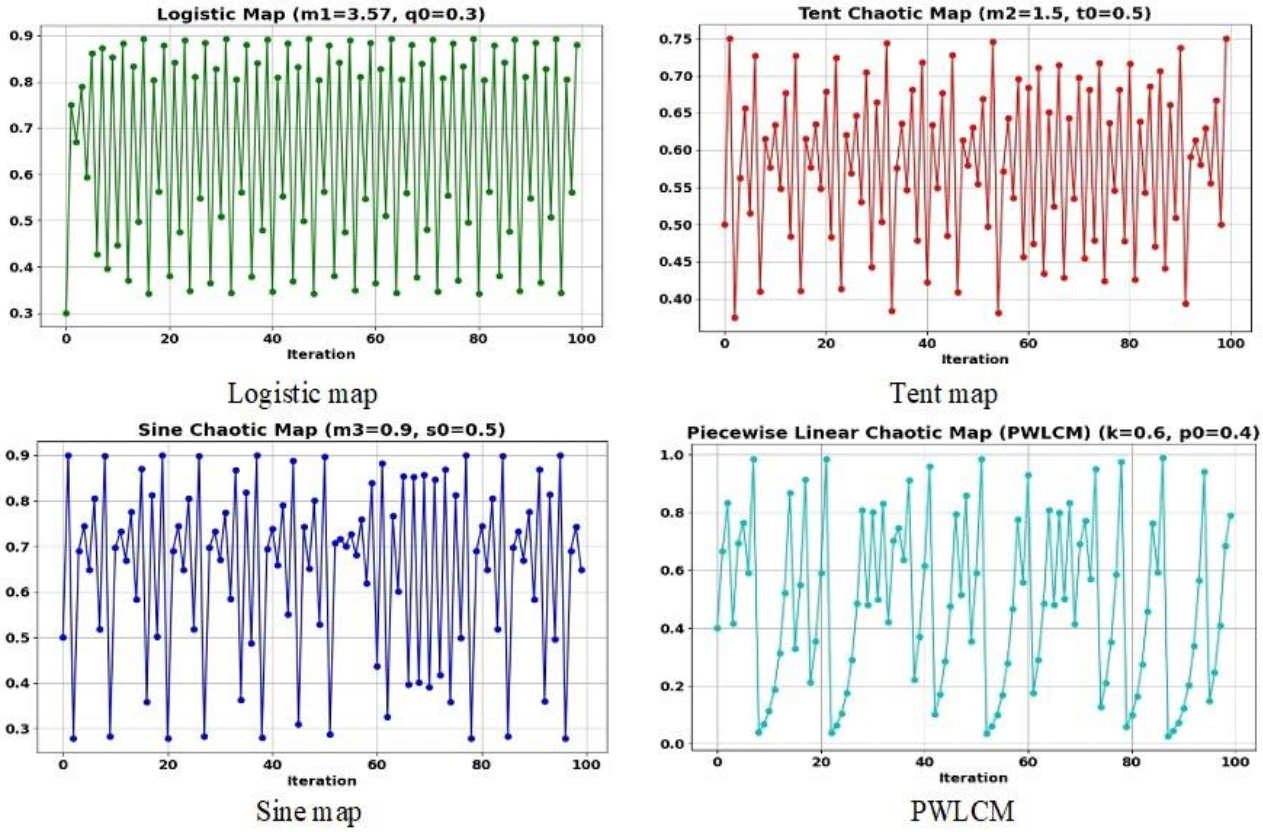

Figure. 3 The variation for the first 100 iterations of the chaotic maps (logistic, tent, sine, and PWLCM)

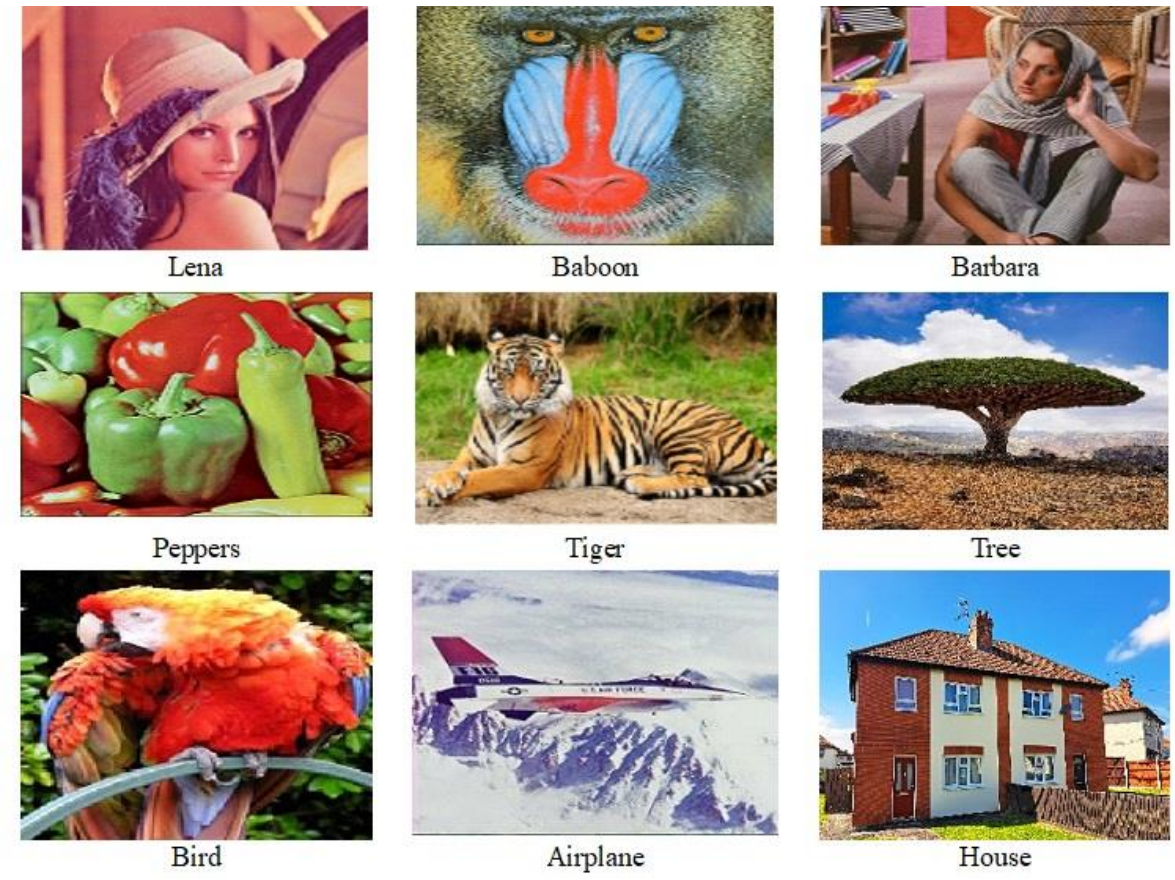

Figure. 4 Original images

5. Results and discussion

A group of images (Baboon, Lena, Peppers, Tiger, Barbara, Tree, Bird, Airplane, and House) of sizes 256×256 were chosen to test the suggested approach's robustness and efficiency. Fig. 4 displays the original images utilized to evaluate the proposed approach.

The results were subjected to a sequence of statistical tests to evaluate the strength of the suggested approach, such as histogram analysis, the Unified Average Changing Intensity (UACI), the Number of Pixels Change Rate (NPCR), entropy, and correlation test.

5.1 Histogram analysis

The histogram shows the distribution of pixel values in images. Attackers may analyse histograms to gather information that could help them reconstruct the original image. However, after encryption applies to an image, the pixel distribution should appear highly uniform, making it difficult for attackers to extract meaningful data. The uniformity of encrypted images is critical for concealing their actual content, as effective encryption methods obscure the original pixel information [20, 29]. Fig. 5 presents the histograms of Lina, Baboon's, and House's encrypted and original images. The histogram of these images shows that the proposed method provides good security. It works to hide the original information and thus prevents attackers from finding any data about the plain images.

5.2 UACI & NPCR test

Encryption methods must ensure that limited modifications to the state of the plain image will significantly modify the encrypted image. Therefore, encryption methods must be sensitive to such changes. Two main parameters, UACI and NPCR, measure the resistance to such attacks.

UACI measures the average difference between the image before and after the encryption process. A higher UACI value indicates a significant difference between the images. In an ideal encryption scheme, the typical range for UACI is between 30% and 35%, but it varies depending on the image and algorithm used. Meanwhile, NPCR measures the rate of change between the image pixels before and after encryption. The image is more secure when the NPCR value is closer to 100 [15, 27]. The value of the UACI and NPCR is measured by Eq. (5)-(7):

$$NPCR = \sum_{m,n} \frac{R(m,n)}{X * Z} \times 100 \quad (5)$$

$$R(m,n) = \begin{cases} 0 & if \ P_1(m,n) = P_2(m,n) \\ 1 & if \ P_1(m,n) \neq P_2(m,n) \end{cases} \quad (6)$$

$$UACI = \sum_{i,j} \frac{|P_1(i,j) - P_2(i,j)|}{255} \times 100 \quad (7)$$

Where:

P1 (m, n) original image and *P2 (m, n)* encrypted images. *X* and *Z* represent the height and width of the image. *R (m, n)* represents the rate of change among the pixels before and after the encryption.

Table 3 shows the results of applying the UACI and NPCR measures.

5.3 PSNR and MSE analysis

One essential test for assessing the effectiveness of image coding systems is the Peak signal-to-noise ratio (PSNR). When the PSNR value falls below 10, it shows that the encryption system is highly effective. Meanwhile, the Mean Squared Error (MSE) measures the change between the encrypted and original images, with an ideal MSE value being very high to show strong encryption [10, 27]. The value of the *PSNR* and *MSE* is measured by Eq. (8), and Eq. (9):

$$MSE = \frac{1}{NM} \sum_{ij} (p(i,j) - q(i,j))^2 \quad (8)$$

$$PSNR = 10 \times log_{10}(\frac{255^2}{MSE}) \quad (9)$$

Where:

p (i, j) and q (i, j) are the original and encrypted images, respectively. *N* and *M* are the height and width of the image.

Table 3 illustrates the outcomes of applying the PSNR and MSE measures. The significant differences between the encrypted and original images, indicated by low PSNR and high MSE values, demonstrate the effectiveness of the proposed method.

5.4 Entropy test

Entropy is a crucial measure of randomness used to evaluate unpredictability or randomness within an image. The entropy value is measured by Eq. (10):

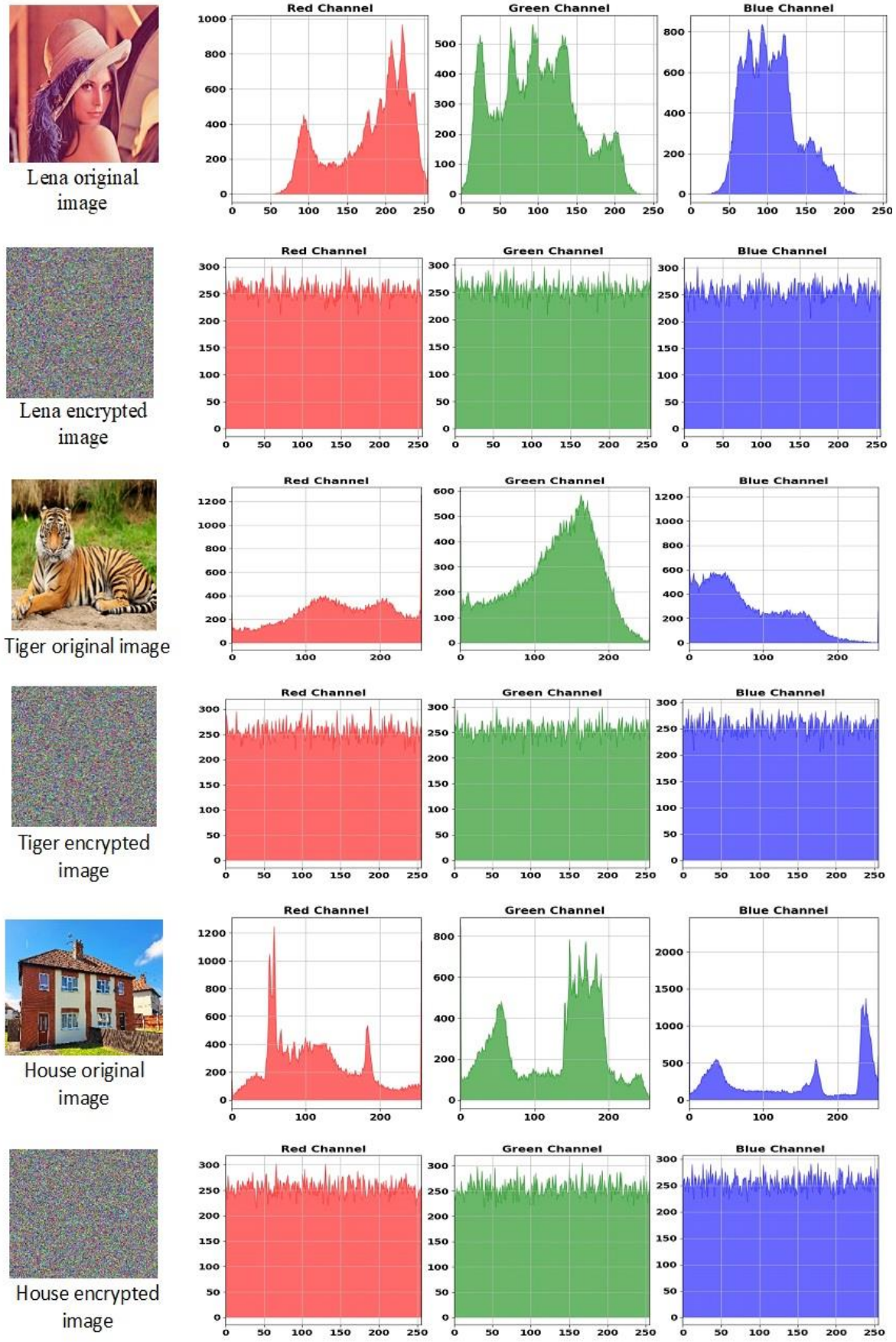

Figure. 5 Examples of the histogram of the original and encrypted image

Table 3. The Measure results for (UACI, NPCR, MSE, PSNR, and Entropy).

Measure type	color	Lena	baboon	Barbara	Peppers	Tiger	Tree	Bird	Airplane	House
UACI	Red	33.14	31.49	30.67	28.66	32.04	34.19	36.92	32.02	31.05
	Green	30.68	30.00	31.11	33.41	30.15	32.82	35.61	33.00	31.34
	Blue	27.78	34.25	32.40	34.22	34.14	36.21	38.37	33.09	37.66
NPCR	Red	99.62	99.60	99.60	99.61	99.62	99.65	99.61	99.63	99.58
	Green	99.62	99.64	99.61	99.63	99.62	99.62	99.60	99.61	99.62
	Blue	99.65	99.56	99.66	99.64	99.59	99.61	99.58	99.63	99.63
MSE	Red	105.40	105.25	105.58	105.68	105.56	105.66	105.65	105.69	105.60
	Green	105.41	105.70	105.75	105.82	105.32	105.36	105.60	105.97	106.10
	Blue	104.47	105.19	106.16	105.68	105.29	105.22	104.59	105.02	105.90
PSNR	Red	27.90	27.91	27.89	27.89	27.90	27.89	27.89	27.89	27.89
	Green	27.90	27.89	27.89	27.88	27.91	27.90	27.89	27.88	27.87
	Blue	27.92	27.91	27.87	27.89	27.91	27.91	27.94	27.92	27.88
Entropy original image	Red	7.30	6.50	6.39	7.58	7.88	7.85	7.69	6.82	7.65
	Green	7.60	6.44	6.43	7.42	7.72	7.78	7.64	6.81	7.62
	Blue	7.07	6.27	6.32	7.51	7.52	7.33	7.15	6.42	7.40
Entropy encrypted image	Red	7.9974	7.9973	7.9970	7.9964	7.9971	7.9967	7.9972	7.9972	7.9976
	Green	7.9974	7.9970	7.9976	7.9973	7.9975	7.9976	7.9974	7.9971	7.9971
	Blue	7.9971	7.9969	7.9971	7.9973	7.9972	7.9975	7.9974	7.9971	7.9974

Table 4. The correlation values for the plain images.

Image	Horizontal			Vertical			Diagonal		
	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue
Lena	0.9190	0.9205	0.8527	0.9551	0.9568	0.9134	0.9088	0.9091	0.8361
Baboon	0.8879	0.7798	0.8564	0.8366	0.6883	0.8327	0.8239	0.6588	0.8007
Barbara	0.9417	0.9280	0.9289	0.9491	0.9428	0.9490	0.9070	0.8875	0.8941
Peppers	0.9021	0.8831	0.9019	0.9228	0.9082	0.9242	0.8790	0.8577	0.8803
Tiger	0.8458	0.8308	0.8620	0.9025	0.8852	0.8983	0.7900	0.7674	0.8064
Tree	0.7735	0.7372	0.8511	0.7476	0.7107	0.8351	0.7404	0.7045	0.8320
Bird	0.9790	0.9656	0.9593	0.9779	0.9591	0.9563	0.9614	0.9328	0.9251
Airplane	0.9124	0.9298	0.8738	0.8937	0.9136	0.8371	0.8404	0.8706	0.7668
House	0.7743	0.7952	0.9024	0.7822	0.8120	0.9140	0.6851	0.7206	0.8679

$$E(q) = -\sum_{i=0}^{255} p(q_i) log_2 p(q_i) \quad (10)$$

Where

- $p\ (qi)$ is the probability of (qi).

A grayscale image's perfect entropy value is 8, which indicates a completely random distribution of grayscale values, indicating that each intensity level appears to have an equal probability in the image[10]. Table 3 shows the results of applying the entropy measure.

5.5 Key space analysis

A crucial feature of chaotic sequences is their sensibility to primary conditions and control parameters. Therefore, encryption schemes based on chaotic keys increase the time and difficulty of attackers trying to crack them. The proposed algorithm includes four chaotic keys, each with two parameters, for a total of eight parameters. Key spaces larger than 128 bits in encryption methods ensure the highest level of security [19]. According to the IEEE 754 international standard, the double-precision floating-point type is 64 bits. Therefore. the size of the control parameter key frequency will be $(2^{64})^8 = 2^{512}$, which is larger than 2^{128}. Additionally, the DNA encoding and decoding rules and additional operations further expand the length of the key space.

5.6 Correlation test

This test assesses the redundancy among pixels in an image. While the original image typically contains significant, redundant information, a robust encryption algorithm produces an image with a low correlation coefficient [30].

In this test, 3000 neighboring pixel pairs were selected to evaluate the correlation robustness among

Table 5. The correlation values for the encrypted images.

Image	Horizontal			Vertical			Diagonal		
	Red	**Green**	**Blue**	**Red**	**Green**	**Blue**	**Red**	**Green**	**Blue**
Lena	0.0001	0.0030	-0.0006	-0.0009	-0.0073	-0.0047	-0.0008	0.0020	0.0050
Baboon	-0.0076	-0.0028	0.0023	0.0005	0.0053	-0.0008	0.0030	-0.0005	-0.0022
Barbara	-0.0022	-0.0063	-0.0054	0.0018	0.0035	-0.0006	-0.0024	-0.0013	0.0012
Peppers	-0.0010	-0.0027	-0.0007	-0.0021	0.0043	0.0067	0.0004	0.0035	-0.0003
Tiger	-0.0016	-0.0043	0.0025	-0.0069	0.0019	0.0005	0.0007	-0.0012	-0.0029
Tree	0.0025	-0.0049	-0.0004	0.0016	0.0090	0.0050	0.0020	-0.0011	0.0008
Bird	-0.0012	-0.0035	0.0018	0.0015	0.0059	0.0015	0.0046	-0.0020	-0.0022
Airplane	-0.0008	-0.0012	0.0026	-0.0016	-0.0016	-0.0016	0.0016	0.0031	0.0001
House	0.0038	-0.0047	-0.0076	-0.0007	-0.0002	0.0022	-0.0012	-0.0014	-0.0001

Table 6. Comparison of the Lena images with other methods.

Measure	**Color**	**Proposed method**	**Ref [10]**	**Ref [16]**	**Ref [19]**	**Ref [20]**	**Ref [21]**	**Ref [23]**	**Ref [27]**
UACI	Red	33.14	33.50	33.47	33.21	32.95	32.81	33.09	33
	Green	30.68	33.46	33.34	33.31			30.72	32
	Blue	27.78	33.40	33.46	33.31			27.70	33
NPCR	Red	99.62	99.61	99.61	99.59	99.61	99.55	99.63	99.63
	Green	99.62	99.61	99.62	99.60			99.51	99.65
	Blue	99.65	99.59	99.61	99.60			99.63	99.63
MSE	Red	105.40	84.21	-	8980.4	-	3238.15	8966.97	106.80
	Green	105.41	78.05						90.63
	Blue	104.47	70.45						72.15
Entropy encrypted image	Red	7.9974	7.9967	7.9973	7.9976	7.9973	7.9898	7.9971	7.9973
	Green	7.9974	7.9974	7.9975	7.9976	7.9972		7.9971	
	Blue	7.9971	7.9974	7.9975	7.9975	7.9974		7.9973	
Correlation	Horizontal	0.0009	0.0003	0.0058	0.0016	0.0002	-0.0432	0.0079	0.0096
	Vertical	-0.0043	0.0051	0.0033	-0.0020	0.0462		-0.0001	-0.0071
	Diagonal	0.0021	0.0028	0.0010	0.0047	0.0010		0.0011	-0.0079

the original and encrypted images in the horizontal, diagonal, and vertical directions. Tables 5 and 6 show the results of applying the correlation measures on the groups of original and encrypted images used in the testing phase.

Fig. 6 and Fig. 7 show the correlation coefficient distributions of the original and encrypted Lena images in the diagonal, horizontal, and vertical directions.

Tables 4 and 5 show the correlation coefficient distributions of the original and encrypted images in the horizontal, vertical, and diagonal directions.

Tables 6, 7, 8, and 9 compare the results of applying NPCR, MSE, UACI, entropy, and correlation coefficient measures to the images of Lina, Baboon, and Airplane and Peppers with the results of other methods, respectively.

6. Conclusion

Researchers are constantly striving to develop effective methods for data protection, given the rapid advancement of communication technology and the increasing need to protect data transmitted over communication channels. This work proposes an image encryption approach involving several steps integrating chaotic systems with DNA sequences. In the first step, the image is divided into four equal parts, and the image pixel positions are rearranged to enhance confusion. While in the second step, a 1D chaotic key (PWLCM) is produced to encrypt the image data by implementing an XOR operation after converting both the key and the image values into DNA sequences. In addition, in the third step, three additional chaotic keys (logistic map, tent map, and pocket map) are generated, each of which is used to encrypt a specific color channel (red, green, or blue) by implementing an XOR operation among the key and the corresponding color values. This multi-layer encryption strategy ensures strong data security against potential threats. The results of statistical experiments such as Correlation, Entropy, UACI, and PNCR that were implemented on a set of images showed that the suggested technique provides a good level of security compared to other proposed methods, achieving an average NPCR of 99.62, a UACI of 32.83, and an entropy of 7.9972. Furthermore, the

histogram analysis demonstrated a uniform distribution, effectively preventing unauthorized individuals from deducing information about the original image. Future research will focus on encrypting specific regions of the image to reduce the time required for encryption and decryption.

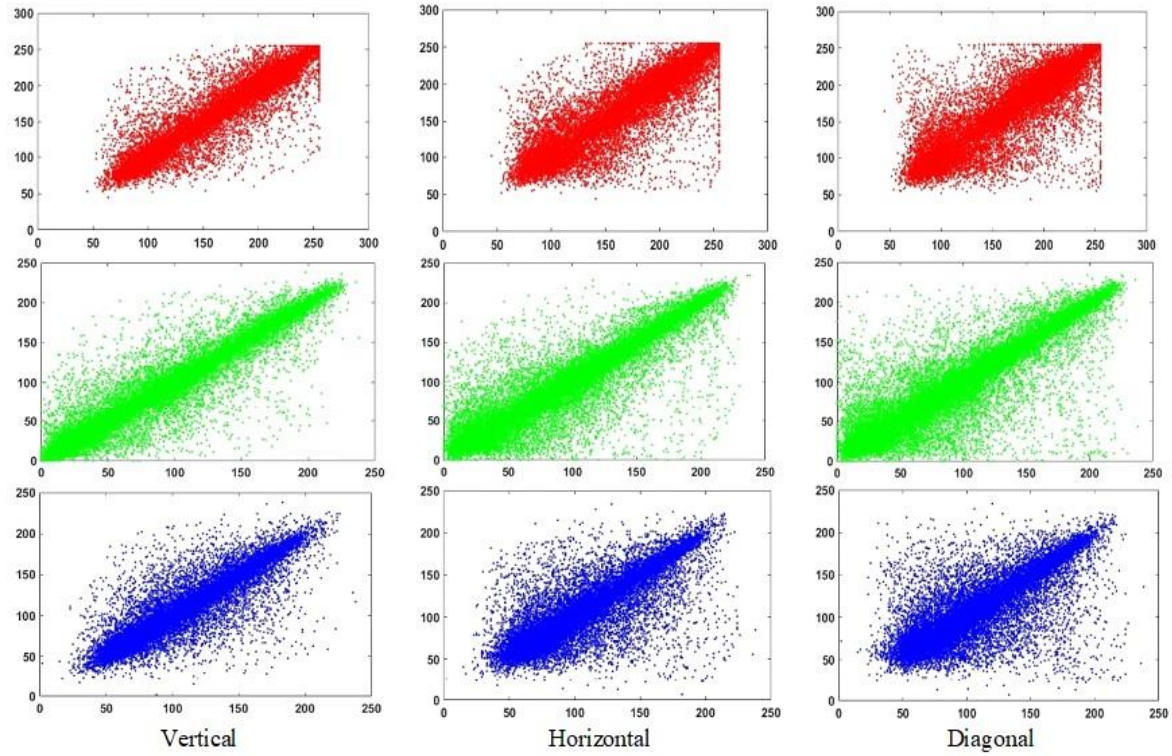

Figure. 6 Correlation coefficient distribution for an original Lena image

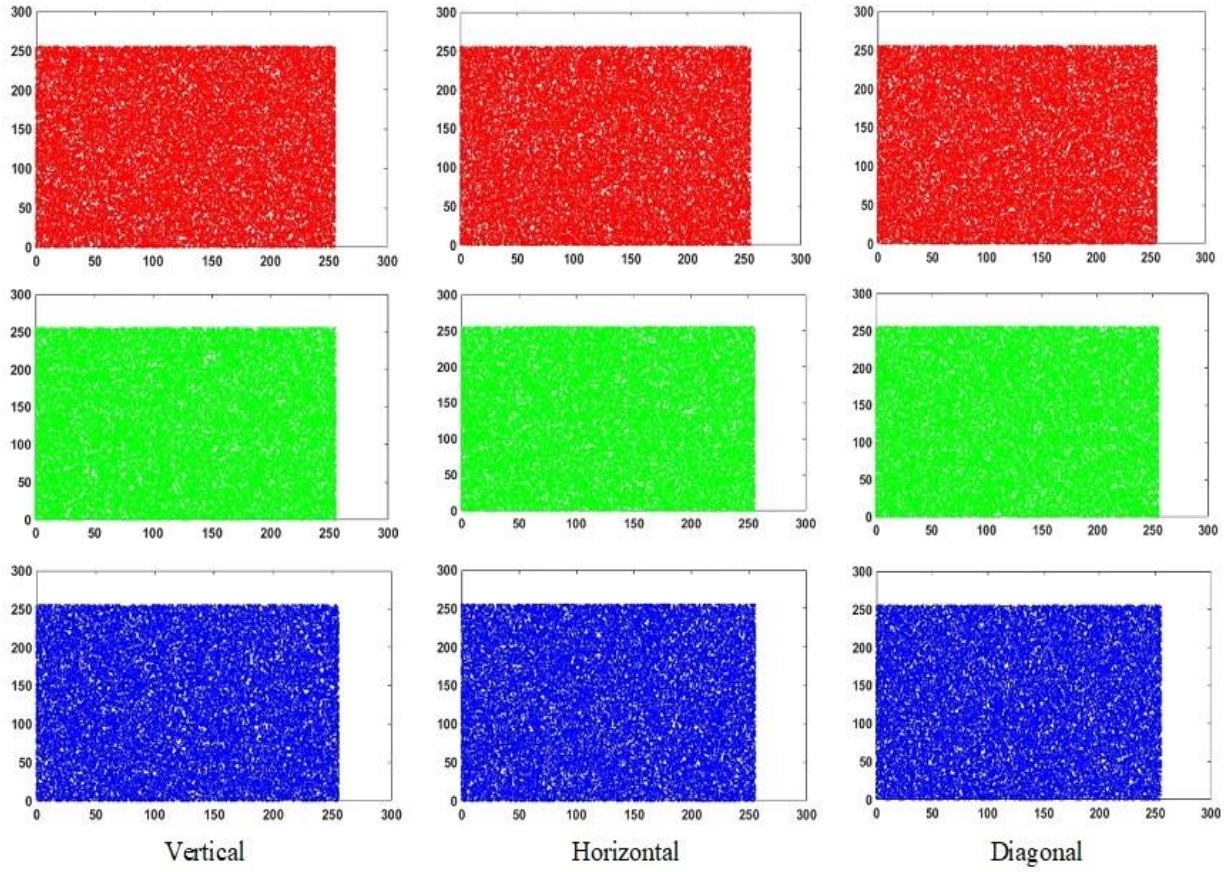

Figure. 7 Correlation coefficient distribution for an encrypted Lena image

Table 7. Comparison of the Baboon images with other methods

Measure	Color	Proposed method	Ref [10]	Ref [16]	Ref [19]	Ref [20]	Ref [21]	Ref [27]
UACI	Red	31.49	33.53	33.34	33.22	33.05	33.80	30
	Green	30.00	33.53	33.46	33.22			28
	Blue	34.25	33.33	33.49	33.29			31
NPCR	Red	99.60	99.57	99.61	99.63	99.62	99.54	99.61
	Green	99.64	99.58	99.60	99.61			99.60
	Blue	99.56	99.59	99.62	99.62			99.62
MSE	Red	105.25	76.45	-	8129.1	-	3236.65	84.35
	Green	105.70	72.49					74.11
	Blue	105.19	79.41					91.46
Entropy encrypted image	Red	7.9973	7.9971	7.9970	7.9975	7.9972	7.9975	7.9971
	Green	7.9970	7.9969	7.9978	7.9976	7.9970		
	Blue	7.9969	7.9973	7.9987	7.9974	7.9973		
Correlation	Horizontal	-0.0027	-	0.0013	0.0002	0.0021	-0.0324	0.0016
	Vertical	0.0017		0.0025	0.0017	-0.0540		-0.0023
	Diagonal	0.0001		0.0010	0.0017	0.0010		-0.0087

Table 8. Comparison of the Airplane images with other methods

Measure	Color	Proposed method	Ref [10]	Ref [23]
UACI	Red	32.02	33.37	-
	Green	33.00	33.46	-
	Blue	33.09	33.44	-
NPCR	Red	99.63	99.59	-
	Green	99.61	99.61	-
	Blue	99.63	99.60	-
MSE	Red	105.69	81.49	10352.3
	Green	105.97	84.66	
	Blue	105.02	83.39	
Entropy encrypted image	Red	7.9972	7.9971	7.9974
	Green	7.9971	7.9970	7.9967
	Blue	7.9971	7.9974	7.9968
Correlation	Horizontal	0.0002	-	-0.0022
	Vertical	-0.0003	-	0.0017
	Diagonal	0.0016	-	0.0013

Table 9. Comparison of the Peppers images with other methods

Measure	Color	Proposed method	Ref [20]	Ref [21]	Ref [23]	Ref [27]
UACI	Red	28.66	33.50	32.96	-	29
	Green	33.41				34
	Blue	34.22				34
NPCR	Red	99.61	99.60	99.75	-	99.62
	Green	99.63				99.60
	Blue	99.64				99.59
MSE	Red	105.68	-	3245.63	10049.4	77.85
	Green	105.82				110.63
	Blue	105.68				114.97
Entropy encrypted image	Red	7.9964	7.9974	7.9893	7.9969	7.9972
	Green	7.9973	7.9971		7.9974	
	Blue	7.9973	7.9972		7.9971	
Correlation	Horizontal	-0.0014	-0.0011	-0.0210	-0.0020	-0.0008
	Vertical	-0.0021	-0.0267		-0.0015	0.0015
	Diagonal	-0.0012	-0.0008		0.0006	-0.0134

Conflicts of Interest

The authors declare no conflicts of interest.

Author Contributions

Conceptualization, STA and YHA; methodology, STA and YHA; software, STA; validation, YHA; formal analysis, STA, YHA; investigation, STA, YHA; resources, STA and YHA; data curation, STA, YHA; writing original draft preparation, STA; writing review and editing, YHA; visualization, STA and YHA; supervision, not found; project administration, not found; funding acquisition, not found.

Acknowledgment

The authors would like to thank Mustansiriyah University (www.uomustansiriyah.edu.iq) in Baghdad, Iraq, for supporting this work.

References

[1] J. Wang, L. Liu, M. Xu, and X. Li, "A novel content-selected image encryption algorithm based on the LS chaotic model", *Journal of King Saud University – Computer and Information Sciences*, Vol. 34, No. 10, pp. 8245–8259, 2022.

[2] K. Kiran, "Selective Image Encryption of Medical Images Based on Threshold Entropy and Arnold Cat Map", *Bioscience Biotechnology Research Communications*, Vol. 13, No. 13, pp. 194–202, 2020.

[3] X. Meng, J. Li, X. Di, Y. Sheng, and D. Jiang, "An Encryption Algorithm for Region of Interest in Medical DICOM Based on One-Dimensional eλ-cos-cot Map", *Entropy*, Vol. 24, No. 7, pp. 1–28, 2022.

[4] J. Lin, K. Zhao, X. Cai, D. Li, and Z. Wang, "An image encryption method based on logistic chaotic mapping and DNA coding", In: *Proc. of Remote Sensing Image Processing, Geographic Information Systems, and Other Applications*, Wuhan, China, Vol. 11432, pp. 363-369,14 February 2020.

[5] M. Asgari-Chenaghlu *et al.*, "Cy: Chaotic yolo for user intended image encryption and sharing in social media", *Information Sciences*, Vol. 542, pp. 212–227, 2021.

[6] S. W. Kang and U. S. Choi, "ROI Image Encryption using YOLO and Chaotic Systems", *International Journal of Advanced Computer Science and Applications*, Vol. 12, No. 7, pp. 466–474, 2021.

[7] P. Vinotha and D. Jose, *VLSI Implementation of Image Encryption Using DNA Cryptography*, Springer Nature Switzerland AG, pp. 1-9, 2020.

[8] N. E. El-Meligy, T. O. Diab, A. S. Mohra, A. Y. Hassan, and W. I. El-Sobky, "A Novel Dynamic Mathematical Model Applied in Hash Function Based on DNA Algorithm and Chaotic Maps", *Mathematics*, Vol. 10, No. 8, pp. 1-21, 2022.

[9] Z. Tang, Z. Yin, R. Wang, X. Wang, J. Yang, and J. Cui, "A Double-Layer Image Encryption Scheme Based on Chaotic Maps and DNA Strand Displacement", *Journal of Chemistry*, Vol. 2022, pp 1-10, 2022.

[10] N. Iqbal, S. Abbas, M. A. Khan, T. Alyas, A. Fatima, and A. Ahmad, "An RGB Image Cipher Using Chaotic Systems, 15-Puzzle Problem and DNA Computing," *IEEE Access*, vol. 7, pp. 174051–174071, 2019.

[11] K. S. Kumari and C. Nagaraju, "DNA encrypting rules with chaotic maps for medical image encryption", In: *Proc. of the Fifth International Conf. on Intelligent Computing and Control Systems*, Madurai, India, pp. 832–837, 2021.

[12] M. K. Nalini and R. K. Radhika, "Secured Key Generation for Biometric Encryption using Hyper-chaotic Map and DNA Sequences", In: *Proc. of International Conf. on IoT based Control Networks and Intelligent Systems*, Kottayam, Kerala, India, pp. 585–595, 2021.

[13] R. Ismail Abdelfattah, H. Mohamed, and M. E. Nasr, "Secure Image Encryption Scheme Based on DNA and New Multi Chaotic Map", *Journal of Physics: Conference Series*, Vol. 1447, No. 1, 2020.

[14] M. S. Fadhil, A. K. Farhan, and M. N. Fadhil, "Designing Substitution Box Based on the 1D Logistic Map Chaotic System", In: *Proc. of the 2nd International Scientific Conf. of Engineering Sciences*, Vol. 1076, No. 1, pp. 012041, 2021.

[15] B. M, G.Shamala Devi, M.Yamini Krishna, M.Viswa Prasanna, and N.Iswarya, "Image Encryption Using Chaotic Maps and DNA Encoding", *Journal of Xidian University*, Vol. 14, No. 4, pp.1817-1827, Apr. 2020.

[16] H. G. Mohamed, D. H. ElKamchouchi, and K. H. Moussa, "A Novel Color Image Encryption Algorithm Based on Hyperchaotic Maps and Mitochondrial DNA Sequences", *Entropy*, Vol. 22, No. 2, pp. 158, Jan. 2020.

[17] Y. Sha, Y. Cao, and H. Yan, "A gray image encryption algorithm based on 3D chaotic map and DNA operations", In: *Proc. of the e 8th EAI International Conf. on Green Energy and*

Networking, Dalian, People's Republic of China, pp. 407,2021.

[18] A. P. H, P. K. Pareek, G. P. M. S, and P. Singh, "Image Encryption Method by Using Chaotic Map and DNA Encoding", *Natural Volatiles & Essential Oils Journal*, Vol. 8, No. 5, pp. 10391–10400, 2021.

[19] P. N. Lone, D. singh, and U. H. Mir, "Image encryption using DNA coding and three-dimensional chaotic systems", *Multimedia Tools and Applications*, Vol. 81, No. 4, pp. 5669–5693, 2022.

[20] S. Mansoor, P. Sarosh, S. A. Parah, H. Ullah, M. Hijji, and K. Muhammad, "Adaptive Color Image Encryption Scheme Based on Multiple Distinct Chaotic Maps and DNA Computing", *Mathematics*, Vol. 10, No. 12, pp.2004, 2022.

[21] A. H. Alrubaie, M. A. A. Khodher, and A. T. Abdulameer, "Image encryption based on 2DNA encoding and chaotic 2D logistic map", *Journal of Engineering and Applied Science*, Vol. 70, No. 1, pp. 1–21, 2023.

[22] E. Kopets, V. Rybin, O. Vasilchenko, D. Butusov, P. Fedoseev, and A. Karimov, "Fractal Tent Map with Application to Surrogate Testing", *Fractal and Fractional*, Vol. 8, No. 6, pp. 344, 2024.

[23] W. Alexan, M. Gabr, E. Mamdouh, R. Elias, and A. Aboshousha, "Color Image Cryptosystem Based on Sine Chaotic Map, 4D Chen Hyperchaotic Map of Fractional-Order and Hybrid DNA Coding", *IEEE Access*, Vol. 11, No. June, pp. 54928–54956, 2023.

[24] S. Li, G. Chen, and X. Mou, "On the dynamical degradation of digital piecewise linear chaotic maps", *International journal of Bifurcation and Chaos*, vol. 15, no. 10, pp. 3119–3151, 2005.

[25] Y. Hu, C. Zhu, and Z. Wang, "An improved piecewise linear chaotic map based image encryption algorithm", *The Scientific World Journal*, Vol. 2014, No. 1, 2014.

[26] Q. S. Alsaffar, H. N. Mohaisen, and F. N. Almashhdini, "An encryption based on DNA and AES algorithms for hiding a compressed text in colored Image", In: *Proc. of the IOP Conf. Series: Materials Science and Engineering*, Vol. 1058, No. 1, p. 012048, 2021.

[27] S. T. Allawi and D. R. Alshibani, "Color Image Encryption Using LFSR, DNA, and 3D Chaotic Maps", *International Journal of Electrical and Computer Engineering Systems*, Vol. 13, No. 10, pp. 885–893, 2022.

[28] J. Zheng and T. Bao, "An image encryption algorithm based on cascade chaotic map and DNA coding", *IET Image Processing*, Vol. 17, No. 12, pp. 3510–3523, 2023.

[29] S. T. Allawi and N. A. A. Mustafa, "Image encryption based on combined between linear feedback shift registers and 3D chaotic maps", *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 30, No. 3, pp. 1669–1677, 2023.

[30] M. A. Wafik, M. Awad, and D. AbdElminaam, "Secure Image encryption algorithm based on DNA Encoding and Chaos map for cloud computing", *Journal of Computing and Communication*, Vol. 1, No. 2, pp. 9–23, Aug. 2022.