Received: April 7, 2024. Revised: May 11, 2024.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Protection of the Image Data by Using Chaotic Maps and DNA Sequence

Salah Taha Allawi[1]* **Yasmin Makki Mohialden[1]** **Nadia Mahmood Hussien[1]**

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

Abstract: Transferring data through unsecured communication channels exposes it to the risk of sabotage and theft by unauthorized persons. Therefore, secure and modern methods must be provided to protect this data upon transmission. This study suggests a new way to use deoxyribonucleic acid (DNA) coding and chaotic maps to create two security levels for data protection. The first level includes generating a key using a one-dimensional logistic map and then converting the values to DNA codes. In contrast, the image color data is converted to DNA codes. After that, the XOR operation is applied between key and color codes by using four rules (2, 4, 6, and 8) from the encoding DNA rules. The second level includes generating three keys via a three-dimensional logistic map. After that, an XOR operation is performed between the keys and the result of the first level. Finally, the result is an encrypted image with two levels of security. The proposed method shows a high safety rate, which achieved an Entropy value rate of 7.997 and a Number of Pixels Changing Rate (NPCR) of 100% on the test image group.

Keywords: Colour image, Image encryption, DNA coding, Chaotic maps, NPCR test.

1. Introduction

In the current period of large data volumes, digital images serve as a vital tool for disseminating information, with their applications continually expanding. Images have the advantage of being both informative and easily transmittable. As a result, safeguarding the security of digital images has emerged as a pivotal aspect of image processing technology [1]. Conventional encryption techniques, such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Rivest-Shamir-Adleman (RSA), work well for text but are not effective for images. Digital images are characterized by redundancy and close associations between neighboring pixels. Minor modifications to individual pixel attributes have negligible effects on image quality and data volume. Therefore, traditional data encryption techniques are inadequate for effectively securing digital images [2, 3]. The data to be encrypted influences the complexity and effectiveness of the algorithm used to encrypt it; therefore, the image encryption techniques must be sophisticated because of their features and characteristics [4].

Chaotic systems offer numerous advantages, such as aperiodicity, notable sensitivity to initial values, and pseudo-randomness, rendering them suitable for image encoding purposes [5]. Scientist Lorenzo is credited with being the first to propose a chaotic system, and in recent years, researchers have used chaotic systems in many research studies [6]. The subject of DNA coding has entered image encryption because of scientific advancements and the need to use contemporary techniques in image encryption [7]. Modern encryption techniques that use DNA coding provide a high level of security because DNA's biological structure is a natural vector for strands as binary pairs [8-10]. Recently, many researchers have combined chaotic maps with DNA to provide more efficient and effective coding systems [11, 12].

This study aims to introduce a novel approach for safeguarding images transmitted via unsecured communication channels by implementing multiple layers of protection. The proposed method combines DNA encryption with chaotic maps. According to the PNCR measure, the method achieved an excellent result of 100%, as well as the histogram, which shows the data distribution after encryption uniformly.

The rest of this paper includes Section 2, which displays some of the previous methods, and Section 3, which displays background information regarding chaotic maps and DNA coding. Section 4 delineates the proposed method. Subsequently, Section 5 outlines the tests conducted and presents the results. Finally, Section 6 offers a conclusion and future work.

2. Related work

This section will review some methods used to encrypt images during the past period. In 2020, Ibtisam and Sarab [13] introduced a novel approach to picture encryption that uses a chaotic beta map with DNA coding. Their method involves using DNA addition to disperse plain image pixels and then rearranging the DNA color image using the new Beta map in the first phase. Subsequently, keys are produced using the proposed new Beta and Sine chaotic maps in the second phase. In the final stage, the encrypted image is generated by applying DNA XOR between the key and the results of the first step.

In 2021, Aditya et al. [14] proposed a novel technique for encrypting color images based on using two keys. The first key is used to scramble the image pixels, while the second is with the DNA to encrypt the image. In the same year, Yuwen et al. [15] proposed a novel approach to encrypting a grayscale image that combines DNA coding and chaotic mapping. In the first step, the positions of the image pixels are rearranged by a key generated by the Arnold function. While, in the second step, the image data is encoded using DNA encoding, where an XOR operation applies to the image data. Finally, the encrypted picture is obtained by reopening the DNA coding.

In 2022, Shaista et al. [16] proposed a scheme that uses statistical characteristics to change map parameters adaptively, ensuring robustness against plaintext attacks. Secret keys change with changes in the plain image, adding a layer of security. DNA encoding is also used. The experimental analysis reveals an average entropy of eight, a several-pixel change rate of 99.61%, and a unified average changing intensity of 33%. The correlation coefficients approach zero, ensuring the scheme's reliability and resilience against attacks. Using low-dimensional maps substantially decreases the scheme's computational expenses.

In 2023, Vinod and Gurpreet [17] introduced novel image encryption technique employing conservative, chaotic standard map-driven dynamic DNA coding. This approach involves the random selection of encoding rules, addition/subtraction operations, and decoding methods based on pseudo-random sequences derived from the conservative chaotic standard map. The algorithm creates and changes dynamic one-time pixels using feed-forward and feedback mechanisms. This characteristic renders the algorithm sufficiently sensitive to both plaintext and ciphertext. Assessments of the algorithm's performance have yielded promising results in defending against common cryptanalytic attacks. During the same year, Asmaa et al. [18] introduced a novel approach to image encryption termed 2DNALM, which combines double-dynamic DNA sequence encryption with a chaotic 2D logistic map. The algorithm comprises three primary steps. Initially, a positional key is employed to shuffle the pixels. Subsequently, the scrambled images undergo dual encoding via DNA cryptography. Finally, an XOR operation and chaotic keys encrypt the encoded image. Both entropy analysis and results show the algorithm's efficiency and robustness against statistical attacks.

Using chaotic encryption techniques with DNA encryption leads to excellent results and can successfully combat various threats. However, using multiple chaotic keys in the encryption process requires many tests to ensure the randomness of the generated numbers. Therefore, these processes increase the number of operations and the time needed to encrypt and decrypt the image. Most encryption algorithms rely on permuting and diffusing image data and using the XOR DNA in the diffusing phase.

In the permutation phase, the authors in [13] used the DNA addition operation, a new Beta chaotic map, and two chaotic maps in the diffusion phase. The authors [14] used a key in the permutation phase and another chaotic map with DNA coding in the diffusion phase. The authors in [15] used a 3D discrete chaotic map in the permutation phase and used the DNA XOR in the diffusion phase. In contrast, the authors in [16] use a method to encrypt the image based on three stages: the first using three chaotic maps, the second using DNA, and the third using XOR between adjacent points. Meanwhile The authors in [17] used the conservative chaotic standard map in a novel way to generate pseudo-random number sequences, which drives the entire process of DNA encryption. In addition, they used all eight possible DNA encoding rules and corresponding addition, subtraction, and decoding rules. In contrast, the authors in [18] used a chaotic key in the permutation phase. While in the diffusion phase, data was encrypted through two stages: the first, applying 2 DNA for each color, and the second, generating two keys; the first was used with even rows for each color, and the second with odd rows.

3. Methodology

In this section, background information about chaotic maps and DNA coding will be reviewed.

3.1 Chaotic systems

Chaos theory, a mathematical discipline defined by its nonlinear and deterministic nature, is notable for its heightened responsiveness to initial conditions and control parameters. Even slight adjustments to parameters lead to significant changes in the chaotic outputs. Leveraging chaotic systems in cryptographic frameworks serves to bolster security, owing to their inherently unpredictable and random output signals. [19].

The 1D logistic map stands out as one of the most widely recognized discrete chaotic systems, and it exhibits complicated, chaotic behaviour and a straightforward mathematical structure. [19, 20]. Eq. (1) defines it:

$$P_{i+1} = \mu_1 P_i (1 - P_i) \qquad (1)$$

Where μ, i, P_0 three variables: control parameter, the number of iterations, and the system initial state respectively. The parameter (μ) ranges from 0 to 4, with a closer value to 4 yielding better results. For all (i) the value of P_{i+1} is a number between (0-1).

A 3D logistic map is used in the encryption system to achieve high unpredictability. An authentic example of the 3D chaotic logistic maps is Eq. (2), Eq. (3), and Eq. (4):

$$X_{i+1} = \mu_2 X_i (1 - X_i) + \beta Y_i^2 X_i + \gamma Z_i^3 \qquad (2)$$

$$Y_{i+1} = \mu_2 Y_i (1 - Y_i) + \beta Z_i^2 Y_i + \gamma X_i^3 \qquad (3)$$

$$Z_{i+1} = \mu_2 Z_i (1 - Z_i) + \beta X_i^2 Z_i + \gamma Y_i^3 \qquad (4)$$

Where: (γ, μ_2, and β) are three parameters when $3.68<\mu_2<3.99$, $0<\beta<0.022$, $0<\gamma<0.015$ and it takes the values between (0, 1) [21-23].

3.2 DNA encoding

Adenine (A), cytosine (C), guanine (G), and thymine (T) represent the four chemical bases comprising the genetic code found in DNA. Base pairs are the complementary units formed when two bases bond, for instance, A with T and C with G. 00 and 11 are complements, much as 0 and 1 are in binary mathematics. In the same way, 01 and 10 go well together. Only eight of the 24 different coding group types are usable. [24-26]. Table 1 displays these eight groupings. Because of the development of DNA data encoding, several researchers have used algebraic operations, including XOR, addition, and subtraction [20]. Tables 2, show the XOR operation according to the rule 2.

Table 1. The 8 rules of DNA encoding

Rule No.	00	10	01	11
R1	A	C	G	T
R2	A	G	C	T
R3	T	C	G	A
R4	T	G	C	A
R5	C	A	T	G
R6	G	A	T	C
R7	C	T	A	G
R8	G	T	A	C

Table 2. XOR operation in DNA rule 2

	A 00	G 10	C 01	T 11
A 00	A	G	C	T
G 10	G	A	T	C
C 01	C	T	A	G
T 11	T	C	G	A

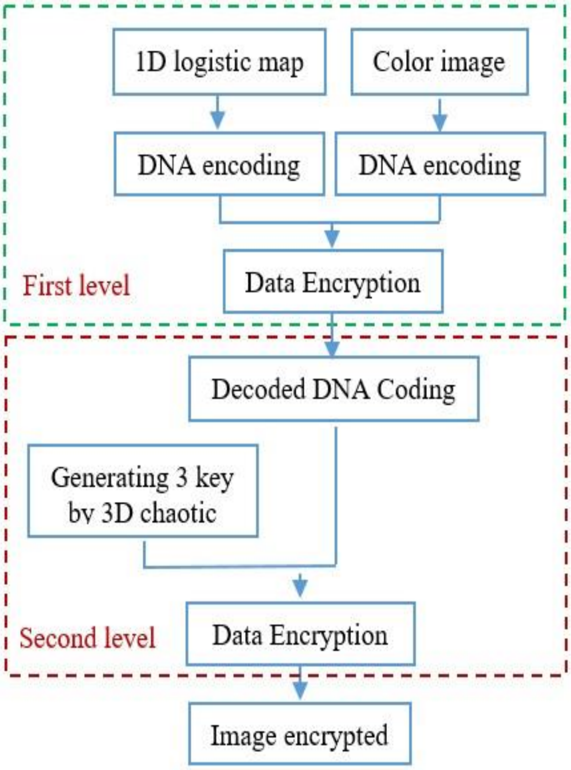


Figure. 1 The general outline for the proposed method

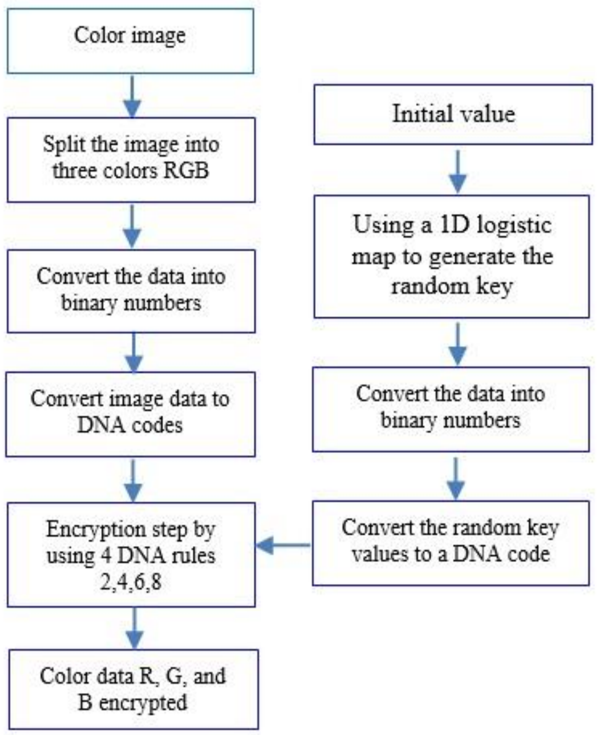

Color image
Split the image into three colors RGB
Convert the data into binary numbers
Convert image data to DNA codes
Encryption step by using 4 DNA rules 2,4,6,8
Color data R, G, and B encrypted
Initial value
Using a 1D logistic map to generate the random key
Convert the data into binary numbers
Convert the random key values to a DNA code

Figure. 2 The general outline for image encryption, first level.

4. Proposed method

The proposed method is divided into two stages: splitting the image into its three RGB essential and then encrypting it using a one-dimensional logistic map and DNA codes. The result of the first stage is then encrypted using three-dimensional chaotic maps to provide the second level of security. Fig. 1 shows the general outline for the proposed method. Each stage will be explained below.

4.1 Encryption by DNA and a 1D logistic map.

This phase includes several steps. Fig. 2 illustrates the general structure of image encryption using the four rules of DNA and the 1D logistic map. The input picture is first divided into its primary colors (RGB), and then every color's data is converted into a 1D array. In the second step, a key (k) will be generated using the 1D logistic map. The data for each color, as well as the key, is transformed into a binary number and then converted to the DNA code using the DNA codes (A = 00, C = 10, G = 01, and T = 11). The third step includes encrypting the image by applying the XOR operation between the key (K) codes and the pixel using four DNA rules (2, 4, 6, and 8).

Algorithm 1 displays the steps for encrypting images using DNA and the 1D logistic map.

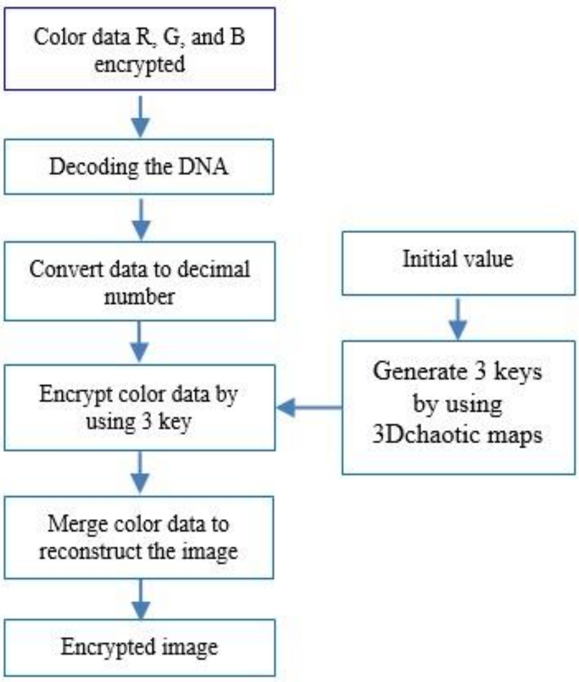

Color data R, G, and B encrypted
Decoding the DNA
Convert data to decimal number
Encrypt color data by using 3 key
Merge color data to reconstruct the image
Encrypted image
Initial value
Generate 3 keys by using 3Dchaotic maps

Figure. 3 The general outline to encrypt images by using 3D chaotic map

```
Algorithm I: General steps for the first level
Input: Color image
Output: Color values encrypted
1.  Entering a plain image.
2.  Splitting the image into the RGB.
3.  Converting the color data into a 1D array.
4.  Converting the color data into binary numbers.
5.  Encoding the binary numbers for each color using
    DNA coding.
6.  Generating a key (K) using a 1D logistic map.
7.  Convert the key (K) into a binary number
8.  Encoded the binary number for the key using
    DNA coding.
9.  Applying an XOR operation between the codes
    for the key and colors.
10. The result is data encryption for each color.
```

4.2 Encryption by 3D chaotic maps

The main framework for encrypting images with 3D chaotic maps is shown in Fig. 3. At this stage, three keys are generated using 3D chaotic maps, where a key is used for each color. After that, the encrypted data for each color that results from the (DNA coding and 1D logistic map) stages is converted into a decimal number. The XOR operation is then applied between the value of the key and the corresponding color data. The final step is to

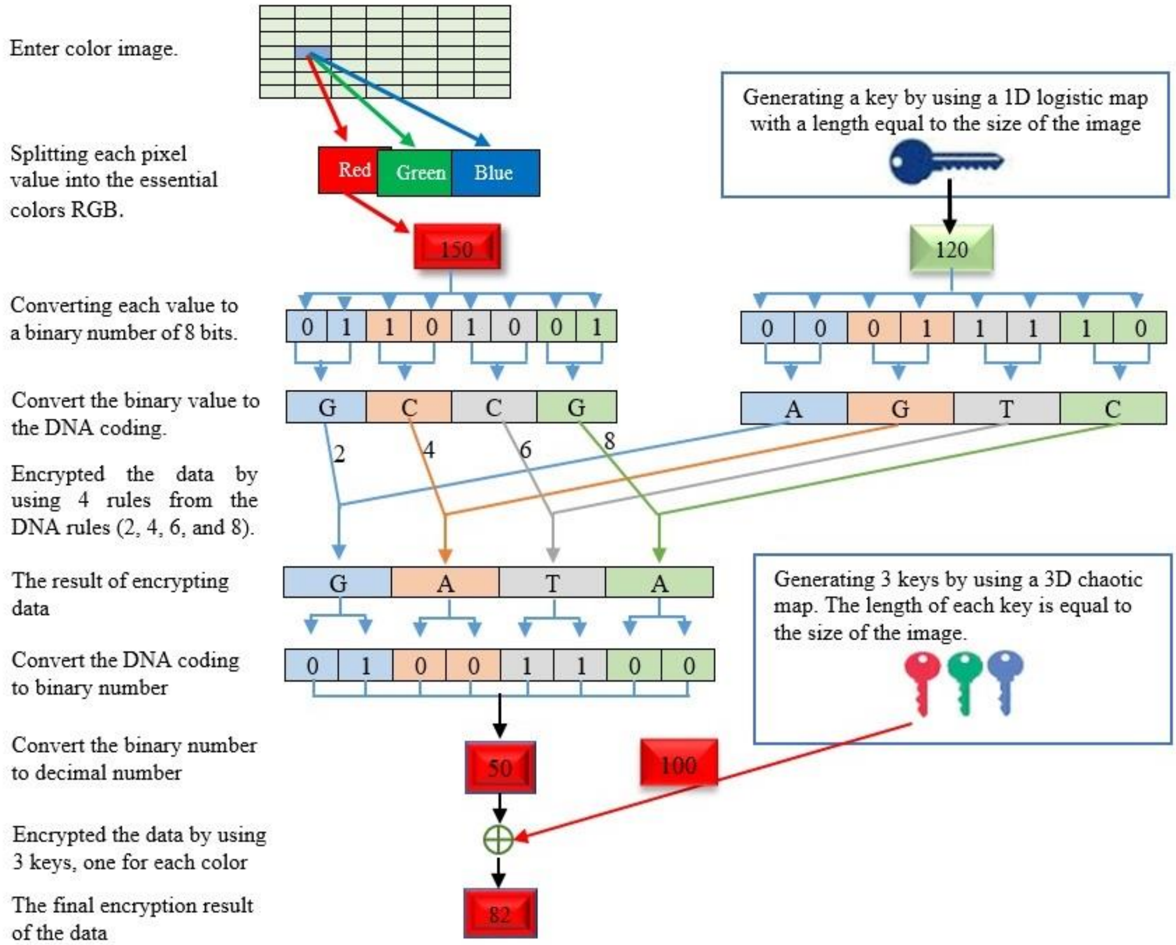

Enter color image.
Splitting each pixel value into the essential colors RGB.
Red
Green
Blue
150
Generating a key by using a 1D logistic map with a length equal to the size of the image
120
Converting each value to a binary number of 8 bits.
0 1 1 0 1 0 0 1
0 0 0 1 1 1 1 0
Convert the binary value to the DNA coding.
G C C G
A G T C
2
4
6
8
Encrypted the data by using 4 rules from the DNA rules (2, 4, 6, and 8).
The result of encrypting data
G A T A
Generating 3 keys by using a 3D chaotic map. The length of each key is equal to the size of the image.
Convert the DNA coding to binary number
0 1 0 0 1 1 0 0
Convert the binary number to decimal number
50
100
Encrypted the data by using 3 keys, one for each color
The final encryption result of the data
82

Figure. 4 An example of how to encode a single red value using the proposed method.

reassemble the color data to create the encrypted image. The procedures for encoding an image using 3D chaotic maps are shown in Algorithm 2. Fig. 4 shows an example of encrypting a single red value using the proposed method.

Algorithm II: General steps for the second level

Input: Color values encrypted
Output: Image encrypted

1. Decode the DNA code from the previous step and convert it to a decimal number.
2. Using the 3D chaotic maps to generate three keys.
3. Applying the XOR between the Keys and the colors values
4. Converting the data for each color to a 2D array.
5. Reassemble the colors of the image.
6. An encrypted image is the result.

5. Results and discussion

A set of images (Lena, Baboon, Barbara, Pepper, and Tiger) with a size of (256×256) were tested to see the strength and efficiency of the proposed method. The initial values and control parameters used to generate the key using a 1D logistic map are $\mu_1 = 3.99995$, $p_0 = 0.78916$. The initial values and control parameters used to generate three keys using a 3D chaotic map are: $\beta = 0.021$, $\gamma = 0.015$, $\mu_2 = 3.84$, $z_0 = 0.97$, and $x_0 = 0.97$, $y_0 = 0.67$. Fig. 5 shows examples of the images used in the testing stage.

In order to evaluate the efficacy and robustness of the proposed method, a battery of statistical tests was performed on the outcomes obtained from applying the method to the set of test images, including:

5.1 Key space analysis

A fundamental attribute of chaotic sequences is their sensitivity to initial circumstances and control settings. Therefore, the keys of the encryption system are derived from these initial conditions and control settings. Implementing high-level encryption methods will significantly increase the difficulty for attackers in searching through the key space,

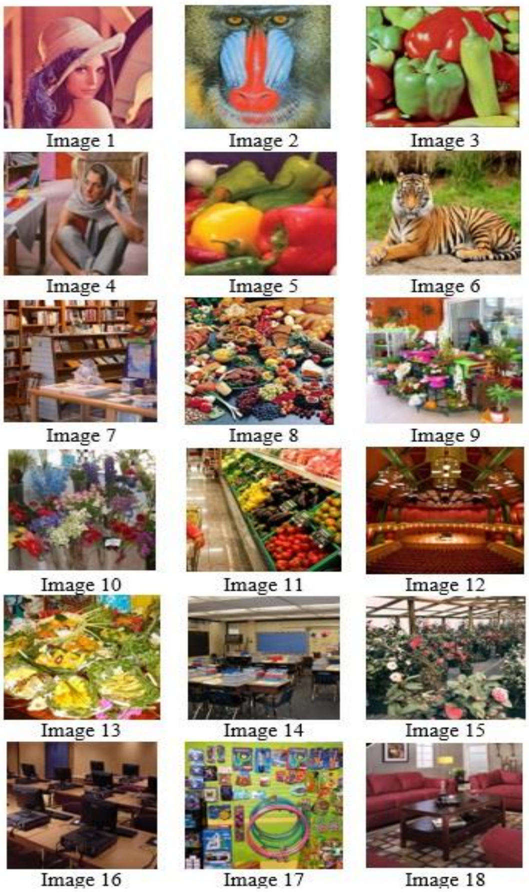


Figure. 5 Example of images used in the testing stage

requiring more time to break the key. A key space exceeding 128 bits in encryption methods ensures top security. The suggested algorithm comprises two keys: a 1D logistic map and a 3D chaotic map, in which the first key contains two parameters (μ_1, p_0) and the second key comprises six parameters (β, γ, μ_2, z_0, x_0, y_0). The index portion is a positive value for comparison, following the international standard IEEE 754. Because the significant digit of a double-precision floating-point type is 52 bits, the size of the control parameter's key pace will be $(2^{52})^8 = 2^{416}$, larger than 2^{128}. Besides, the DNA encoding and decoding rules and complementary DNA operations add more length to the key space.

5.2 Time analysis

All algorithms must consider security considerations, yet top-notch encryption must also show resilience and efficiency. The operational velocity of encryption and decryption algorithms is a critical factor. The algorithm's running speed depends on other conditions, such as the hardware device (speed of the processor and the memory), the type of image being used (color or grayscale), size of the image, the software environment, the number of operations implemented, and others. The suggested algorithm has been implemented on an Intel(R) Core (TM) i5-10210U CPU @ 1.60 GHz, 16 GB of memory, Windows 10 Pro, and MATLAB R2021a.

Our review examines all operations, including XOR and DNA XOR operations, making chaotic sequences, encoding and decoding DNA, converting numbers from decimal to binary and vice versa, and other operations. Table 3 illustrates the number of times all the operations are repeated in the suggested method. Table 4 illustrates a comparison with other methods.

5.3 Histogram test

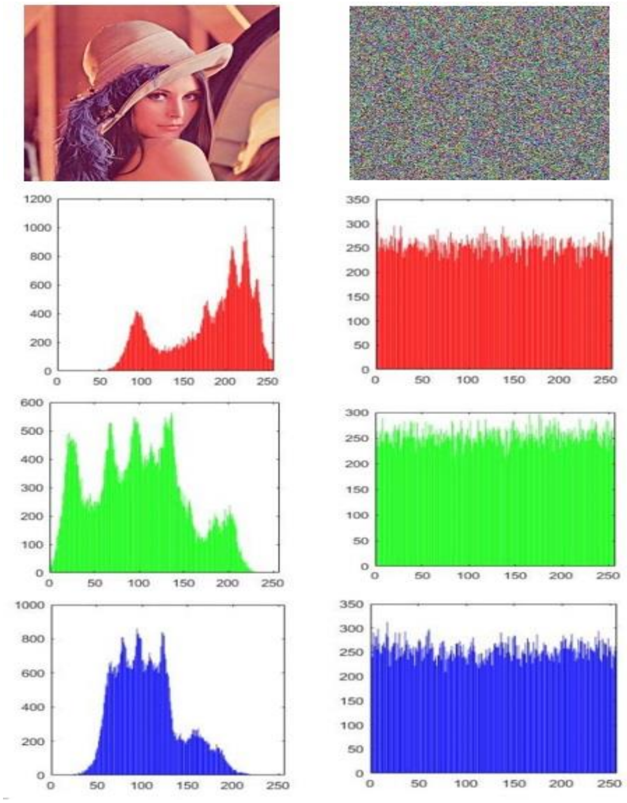
A histogram is a graphical representation that displays the frequency distribution of pixels in digital images. The attacker’s primary goal in using the graph is to get information that helps them reach the original image. Once an encryption technique has been applied to a picture to confuse potential attackers, the result should be highly uniform. The

Table 3. The computational complexity of the suggested method.

Operation	No. of times repeated
converting the color values from a 2D array to a 1D array and vice versa	2×3×(M×N)
Convert data from decimal to binary and vice versa	2×3×(M×N)
DNA data encoding	3×4×(M×N)
Generating one key by using 1D logistic map	1×(M×N)
DNA key encoding	1×4×(M×N)
DNA XOR	3×4×(M×N)
DNA data decoding	3×4×(M×N)
Generating three key by using 3D logistic map	3×(M×N)
XOR operation	3×(M×N)
Total	59×(M×N)

Table 4. The computational complexity of the suggested method.

Ref	Image size	Computational Complexity
[16]	256×256	O(59 × M × N)
[27]	256×256	O(12 × M × N)
[28]	256×256	O(168 × M × N)
Our method	256×256	O(59 × M × N)



(a) (b)

Figure. 6 The Histogram for the Lena's image: (a) original and (b) encrypted

Table 5. Results testing NPCR, UACI, Entropy.

Image name	NPCR	UACI	Entropy
Lena	100%	32.70	7.9969
Baboon	100%	32.83	7.9970
Barbara	100%	32.73	7.9971
Pepper	100%	32.77	7.9971
Tiger	100%	32.81	7.9972

homogeneity of encrypted pictures is a crucial factor in obscuring the actual content of digital images. Therefore, encryption methods prevent attackers from obtaining this information[16, 29]. Fig. 6 shows the histogram for the original and encrypted Lena's image.

5.4 NPCR & UACI test

An image encryption technique should possess the property that every slight alteration in the original image will cause a corresponding change in the encrypted image. The algorithm must show sensitivity to variations in the original image, rendering it resistant to differential assaults. Hence, two parameters are used to assess resistance against such attacks: The NPCR and the Unified Average Changing Intensity (UACI). NPCR determines the change rate between the original and encoded image points. When the value of NPCR is closer to 100, the image is more secure. In contrast, UACI detects the average difference between the encrypted and original images. A higher value for the UACI shows a higher change between the images [16, 20, 30]. The NPCR and UACI value is mathematically calculated by Eq. (5), Eq. (6), and Eq. (7):

$$NPCR = \sum_{i,j} \frac{P(i,j)}{N*M} \times 100 \tag{5}$$

$$P(i,j) = \begin{cases} 0 & if \;\; D_1(i,j) = D_2(i,j) \\ 1 & if \;\; D_1(i,j) \neq D_2(i,j) \end{cases} \tag{6}$$

$$UACI = \sum_{i,j} \frac{|D_1(i,j) - D_2(i,j)|}{255} \times 100 \tag{7}$$

Where D1(i, j) is the original image, D2 (i, j) is the encrypted image, N is the height of the image, M is the width of the image, and p(i, j) is the change rate between the pixels for the original and encoded image.

5.5 Entropy test

Information entropy is a defining characteristic of randomness. In this context, it is used to assess the level of unpredictability or randomness present in the image [25]. The value of the entropy is calculated by applying the following Eq. (8):

$$H(P) = -\sum_{i=0}^{255} q(p_i) log_2 \, q(p_i) \tag{8}$$

Where *q* (*pi*) is the probability of (*pi*) , the perfect value of information entropy for a grayscale image is 8 [23]. Table 5 shows the results of the *NPCR*, *UACI*, and Entropy tests on the group of test images.

5.6 Correlation test

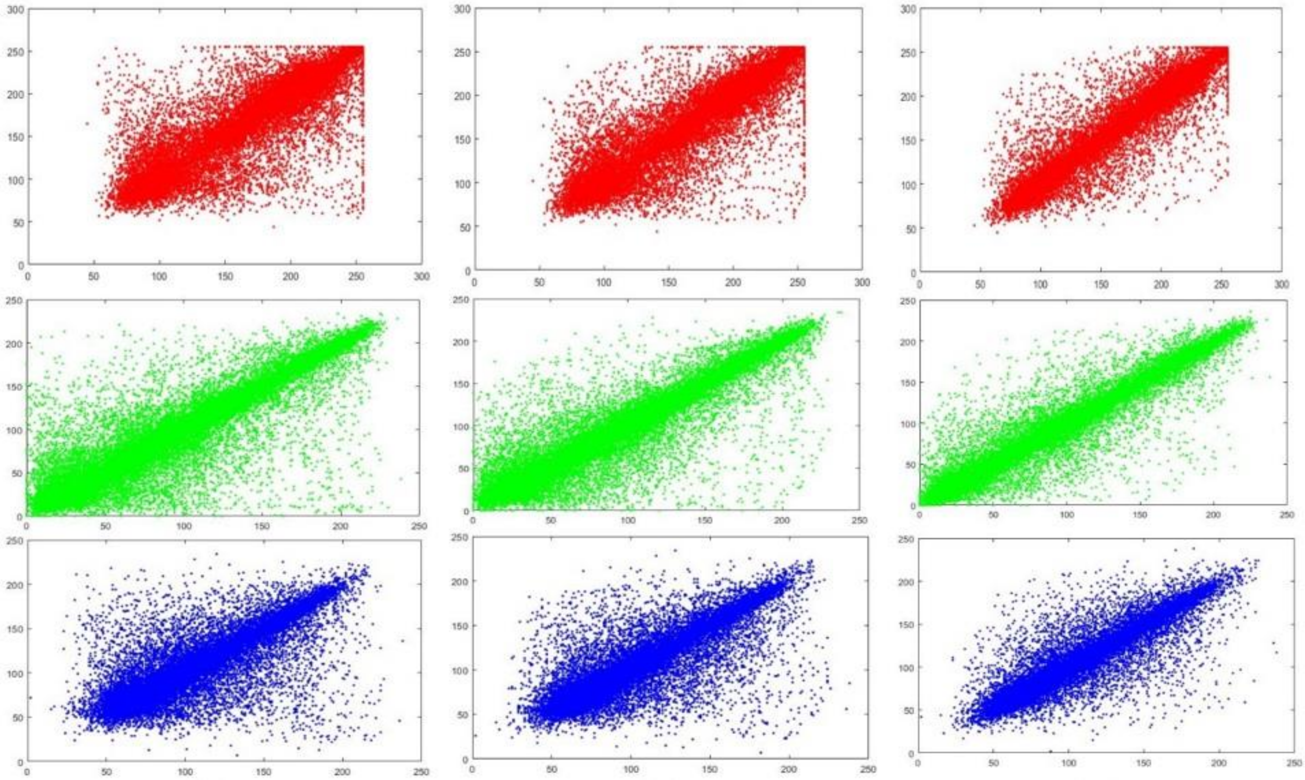
The correlation coefficient (CC) measures redundancy amongst the pixels in an image. The original image has substantial unnecessary repetition, but the encryption algorithm is highly efficient and effective when the result is an encrypted image with a very low correlation coefficient value [27]. For this test (2500), a neighbouring pair of pixels was chosen to assess the correlation strength between the encrypted and original images in horizontal, vertical, and diagonal directions. Table 6 presents the correlation coefficient values for the original images used in the test. In contrast, Table 7 presents the correlation coefficient values for the encrypted images used in the test.

Table 6. The correlation coefficient values for the original image.

Image name	Vertical	Horizontal	Diagonal
Lena	0.9418	0.8974	0.8847
Baboon	0.8099	0.8626	0.7857
Barbara	0.9184	0.8957	0.8723
Pepper	0.9437	0.9409	0.9025
Tiger	0.8953	0.8462	0.7879

Table 7. The correlation coefficient values for the encrypted image.

Image name	Vertical	Horizontal	Diagonal
Lena	-0.0005	0.0001	0.0006
Baboon	0.0013	0.0005	-0.0019
Barbara	0.0006	0.0028	0.0006
Pepper	-0.0014	0.0001	0.0009
Tiger	-0.0036	0.0003	0.0034



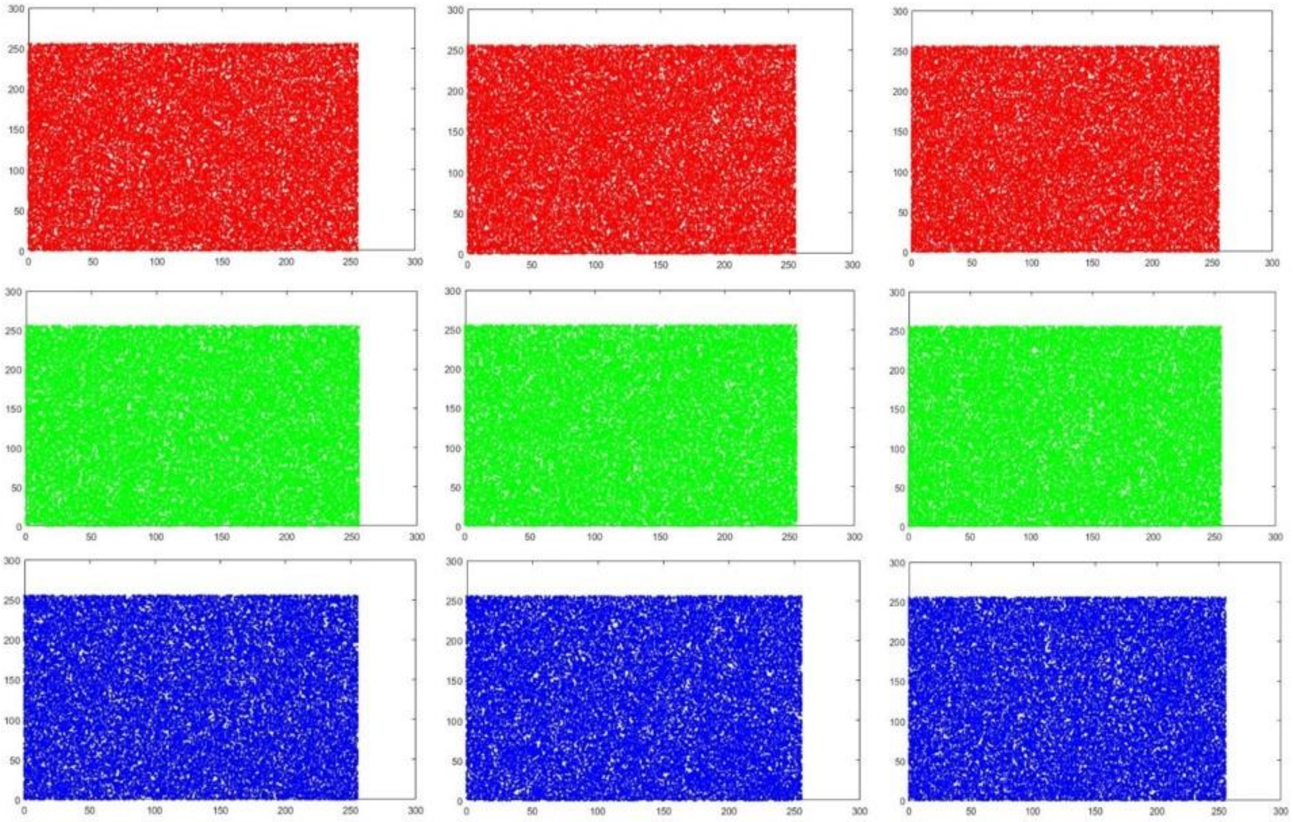
(a) (b) (c)

Figure. 7 Correlation coefficient distribution for an original Lena image: (a) Diagonal direction, (b)Horizontal direction, and (c) Vertical direction

Table 8. Comparison between the proposed method and other methods using Lena's image

Ref.	Image type	Image size	Key space	UACI	NPCR	Entropy	Correlation		
							Horizontal	Vertical	Diagonal
[2]	Grayscale	256×256		31.21	99.64	7.997	-0.0002	0.0052	0.0018
[4]	Color	256×256	2^{390}	33.28	99.59	7.997	0.0016	-0.0020	0.0047
[8]	Color	256×256	2^{365}	33.46	99.60	7.997	0.0003	0.0051	0.0028
[13]	Color	256×256	2^{292}	33.60	99.62	7.997	-0.0001	0.0002	-0.0001
[20]	Color	256×256	-	32.66	99.64	7.997	0.0096	-0.0071	-0.0079
[27]	Color	256×256	2^{312}	33.43	99.60	7.999	-0.0070	0.0011	0.0007
[31]	Grayscale	256× 256	2^{597}	33.43	99.61	7.99	-0.0032	-0.0046	-0.0015
[32]	Grayscale	256× 256	-	33.40	99.58	7.996	-0.0173	-0.0205	-0.0247
our method	Color	256× 256	2^{392}	32.70	100	7.997	0.0001	-0.0005	0.0006

Received: April 7, 2024. Revised: May 11, 2024.



(a) (b) (c)

Figure. 8 Correlation coefficient distribution for an encrypted Lena image: (a) Diagonal direction, (b)Horizontal direction, and (c) Vertical direction

Table 9. Comparison between the proposed method and other methods using Baboon's image

Ref.	Image type	Image size	UACI	NPCR	Entropy	Correlation		
						Horizontal	Vertical	Diagonal
[4]	Color	256× 256	33.25	99.62	7.997	0.0002	0.0017	0.0017
[13]	Color	256× 256	33.54	99.64	7.997	-0.0004	0.0002	0.0003
[20]	Color	256× 256	29.66	99.61	7.997	0.0016	-0.0023	-0.0087
[27]	Color	256× 256	28.75	99.54	7.999	0.0048	-0.0003	0.0013
our method	Color	256× 256	32.83	100	7.997	0.0005	0.0013	-0.0019

Table 10. Comparison between the proposed method and other methods using Pepper's image

Ref.	Image type	Image size	UACI	NPCR	Entropy	Correlation		
						Horizontal	Vertical	Diagonal
[13]	Color	256× 256	33.58	99.62	7.997	0.0001	-0.0001	0.0001
[20]	Color	256× 256	32.33	99.60	7.997	-0.0008	0.0015	-0.0134
[27]	Color	256× 256	28.73	99.5	7.999	0.0015	-0.0027	-0.0016
[32]	Grayscale	256× 256	33.51	99.60	7.996	-0.0443	0.0030	0.0274
our method	Color	256× 256	32.77	100	7.997	0.0001	-0.0014	0.0009

Fig. 7 illustrates the correlation coefficient distributions of the original Lena image across horizontal, vertical, and diagonal directions. In contrast, Fig. 8 displays the correlation coefficient distributions for the encrypted Lena image across the exact directions.

Tables 8, 9, and 10 illustrate the comparison between the results of applying the proposed method to Lena, Baboon, and Pepper images respectively, with the other methods.

6. Conclusion

Protecting information transmitted through insecure communication channels is the most essential thing researchers seek by providing new methods to encrypt the information. Our proposed work includes providing two levels of protection, as it relies on DNA coding and one-dimensional and three-dimensional chaotic maps. The first stage included the use of 1D logistic maps and DNA encoding. In contrast, the second stage included using chaotic three-dimensional maps. Experiments on a set of test images have proven that multiple levels of encryption provide high security. In addition, contemporary techniques prevent unauthorized individuals from accessing this information by combining chaotic maps and DNA. Several statistical tests (PNCR, UACI, Entropy, and Correlation) were performed on the results obtained by applying the suggested method to the test images, proving the method's efficiency. In addition, when using the histogram test, a uniform distribution of the encrypted images appeared, preventing unauthorized persons from obtaining information about the original image. Future work includes encrypting specific parts of the image (ROI) by introducing new methods to specify the parts to be encrypted.

Conflicts of Interest

The authors declare no conflicts of interest.

Author Contributions

Conceptualization, STA and YMM, and NMH; methodology, STA, YMM, and NMH; software, STA; validation, STA, YMM, and NMH; formal analysis, STA, YMM; investigation, STA, NMH; resources, STA, and NMH; data curation, STA, YMM; writing—original draft preparation, STA; writing—review and editing, YMM, NMH; visualization, STA, YMM, and NMH.

Acknowledgments

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

References

[1] X. Li, J. Zeng, Q. Ding, and C. Fan, “A Novel Color Image Encryption Algorithm Based on 5-D Hyperchaotic System and DNA Sequence”, *Entropy*, Vol. 24, No. 9, pp. 1-20, 2022

[2] 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.

[3] T. S. Ali and R. Ali, “A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box”, *Multimedia Tools and Applications*, Vol. 81, No. 15, pp. 20585–20609, 2022.

[4] 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.

[5] 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 Conf. MIPPR 2019: Remote Sensing Image Processing, Geographic Information Systems, and Other Applications*, Wuhan, China, Vol. 11432, pp. 363-369, 2020..

[6] Z. Li, C. Peng, W. Tan, and L. Li, “A novel chaos-based image encryption scheme by using randomly dna encode and plaintext related permutation”, *Applied Sciences*, Vol. 10, No. 21, pp. 1–19, 2020.

[7] 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 Conf. Series: Materials Science Engineering*, Erbil, Iraq, pp. 1-13, 2021.

[8] 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.

[9] P. Vinotha, and D. Jose, “VLSI Implementation of Image Encryption Using DNA Cryptography”, In: *Proc. of the Conf. Intelligent Communication Technologies and Virtual Mobile networks 2019*, Tirunelveli, India, pp. 1–9, 2020.

[10] K. S. Kumari, and C. Nagaraju, “DNA encrypting rules with chaotic maps for medical image encryption”, In: *Proc. of the 5th International Conf. on Intelligent Computing and Control Systems 2021*, Madurai, India, pp. 832–837, 2021.

[11] J. Chauhan, and A. Jain, “Survey On Encryption Algorithm Based On Chaos Theory And DNA Cryptography”, *International Journal of Advanced Research in Computer Communication Eng*ineering, Vol. 3, No. 8, pp. 7801–7803, 2014.

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

[13] S. M. Hameed and I. A. Taqi, “A new beta chaotic map with DNA encoding for color image encryption”, *Iraqi Journal of Science,* Vol. 61, No. 9, pp. 2371–2384, 2020.

[14] A. Pai, P. K. Pareek, G. Prasad, P. Singh, and B. K. Deshpande, “Image Encryption Method by Using Chaotic Map and DNA Encoding”, *Natural Volatiles and Essential Oils,* Vol. 8, No. 5, pp. 10391–10400, 2021.

[15] Y. Sha, Y. Cao, and H. Yan, “A gray image encryption algorithm based on 3D chaotic map and DNA operations”, In: *Proc. of the 8th EAI International Conf. on Green Energy and Networking,* Dalian, People's Republic of China, pp. 1-14, 2021.

[16] 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. 1-20, 2022.

[17] V. Patidar and G. Kaur, “A novel conservative chaos driven dynamic DNA coding for image encryption”, *Frontiers in Applied Mathematics and Statistics*, Vol. 8, pp. 1-21, 2023.

[18] 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

[19] 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*, Diyala, Iraq, pp. 1-13, 2021.

[20] 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.

[21] F. A. Salman and K. A. Salman, “Enhanced image encryption using two chaotic maps”, *Journal of ICT Research and Applications*, Vol. 14, No. 2, pp. 134–148, 2020.

[22] C. Li, G. Luo, and C. Li, “An Image Encryption Scheme Based on The Three-dimensional Chaotic Logistic Map”, *International Journal of Network Security*, Vol. 21, No. 1, pp. 22–29, 2019.

[23] S. T. Allawi and M. M. Abbas, “A New method for image encryption based on 2D-3D Chaotic Maps”, *International Journal of Computer Science and Information Security*, Vol. 18, No. 11, pp. 39–43, 2020.

[24] K. Singh and K. Kaur, “Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it”, *International Journal of Computer Applications*, Vol. 23, No. 6, pp. 17–24, 2011.

[25] R. I. Abdelfattah, H. Mohamed, and M. E. Nasr, “Secure Image Encryption Scheme Based on DNA and New Multi Chaotic Map”, In: *Proc. of Fourth International Conf. on Advanced Technology and Applied Sciences*, Cairo, Egypt ,Vol .1447, pp. 1-12, 2020.

[26] 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. 1-15, 2020.

[27] M. A. Wafik, M. Abdelfatah, and D. S. Abd Elminaam, “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, 2022

[28] M. Samiullah, W. Aslam, H. Nazir, M. I. Ali, B. Shahzad, M. R. Mufti, and H. Afzal, “An Image Encryption Scheme Based on DNA Computing and Multiple Chaotic Systems”, *IEEE Access*, Vol. 8, pp. 25650–25663, 2020.

[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. Babu, G. S. Devi, M.Y. Krishna, M.V. Prasanna, and N. Iswarya, “Image Encryption Using Chaotic Maps and DNA Encoding”, *Journal of Xidian Uni*versity, Vol. 14, No. 4, pp. 1817-1827, 2020.

[31] D. R. Alshibani and S. A. Qassir, “Image

enciphering based on DNA Exclusive-OR operation union with chaotic maps”, In: *Proc. of Al-Sadiq International. Conf. Multidisciplinary in IT and Communication. Science Applications*, Iraq, Baghdad, pp. 245–250, 2016,

[32] M. Sreenivasan, A. Sidhardhan, V. M. Priya, and V. Thanikaiselvan, “5D Combined Chaotic System for Image Encryption with DNA Encoding and Scrambling”, In: *Proc. of the 2019 International Conf. on Vision Towards Emerging Trends Communication and Networking*, Vellore, Tamilnadu, India, pp. 1-6, 2019.