Color Image Encryption Using LFSR, DNA, and 3D Chaotic Maps

Original Scientific Paper

Salah Taha Allawi
Mustansiriyah University,
Department of Computer Science, College of Science
Baghdad, Iraq
salah.taha@uomustansiriyah.edu.iq

Dina Riadh Alshibani
Mustansiriyah University,
Department of Computer Science, College of Science
Baghdad, Iraq
dinashibani@uomustansiriyah.edu.iq

Abstract *– One of the most important challenges facing researchers is to find new methods to protect data sent over the Internet and prevent unauthorized access to it. In this paper, we present a new method for encrypting image data divided into two stages. The first stage requires redistributing the positions of the pixels by using a key of random numbers generated by linear feedback shift registers and then encrypting the data using deoxyribonucleic acid rules. The data generated in the previous stage is encrypted again using chaotic maps to increase the level of security in the second stage. Several statistical tests were implemented to verify the efficiency of the proposed method and compare the results with the work of other researchers. The results of the tests proved a reasonable safety rate compared to other techniques.*

Keywords*: DNA encoding, LFSR, 3D chaotic maps, Encrypted image*

1. INTRODUCTION

Currently, there are many ways to transfer and store information. While modern technology affords easy transmission of information, many risks affect the security and safety of this information [1]. Traditional encryption systems, such as DES and AES, are effective and secure encryption systems when dealing with text data. However, they are not effective when dealing with images because of the characteristics of images, such as redundancy and strong correlation between adjacent pixels [2], [3].

The efficiency, strength, and complexity of the algorithm used to encrypt data are based on the data type. Since images are unique type of data, the algorithm used to encrypt them must be complex [4]. These reasons prompted researchers to discover new methods to protect image data that is transmitted through unsecured networks. One of the essential methods in this field is using chaotic maps to encrypt image data [5]. The scientist Lorenzo is the founder of chaos theory, which has various advantages when applied to image encryption. Chaotic maps are suitable for designing image-encryption systems. During the last decade, various studies and research in this field have been published [6]. As a result of scientific advancement in the field of image encryption, DNA computing was introduced [7]. Recent studies have proved that deoxyribonucleic acid (DNA) coding technology can effectively resist chosen plain-text attacks, improving the security of cryptosystems [8], [9]. Many image-encryption schemes use DNA technology because of its advantages: ultra-low energy consumption, large storage density, and high parallelism [10]. New methods of encrypting information using DNA provide increased security through the use of the biological structure of DNA, which is a natural carrier of information in binary form, by encoding information according to the four bases of DNA (T-11, C-01, G-10, and A-00) [11], [12]. Researchers have recently merged chaotic mapping and DNA technology to create more effective image-encryption methods [13].

In this paper, we provide a literature review on a selection of previous research on image encryption using DNA (Section 2). Then, chaotic maps and DNA encoding are explained in Sections 3 and 4, respectively. Sections 5 and 6 outline the proposed method and experiments to test the image-encryption system. Section 7 explains the test results and makes comparisons with the results of other methods. Finally, we discuss the conclusions in Section 8.

2. LITERATURE REVIEW

This section reviews some methods that use DNA to encode image data.

In [4], the authors proposed a new method comprising of two stages for encrypting color images based on 3D chaotic maps and DNA coding. In the first stage, the initial step is to generate a key using a 3D Arnold map and encode the image data and the key according to the DNA coding rule. The second step involves using the same key to reopen the image data codes and redistribute the image pixel positions after applying the XOR between the key and image codes. In the second stage, a 3D logistic map encrypts image data by generating three data-encryption keys.

In [14], the authors proposed a new method to encrypt images that combined chaotic maps and DNA to produce an algorithm that provides security and protection for confidential data when sent.

In [15], the authors proposed a new method to encrypt and confuse color images based on the DNA sequence with a new Beta chaotic map. First, the DNA addition operation is used to diffuse each component of the original image, and then a new Beta chaotic map shuffles the resulting image. Finally, to produce the encrypted image, a DNA XOR operation is applied between the shuffled DNA image and the key generated by the two new proposed chaotic maps, Beta and Sine chaotic maps.

In [16], the authors proposed a new method for encoding color images that combined a hybrid chaotic map and DNA. This method first requires dividing each image color into n parts and then rearranging the parts of the image. A Chaotic hybrid map redistributes the pixel positions of these parts, and then the parts are grouped to form the encrypted image. Finally, the image data is encoded using DNA technology.

In [17], the authors proposed a new method of encrypting images based on DNA sequence encryption and an enhanced 2D logistic Sine chaotic map (2D-LSMM). The logistic map is used to control the input of the Sine map, and the 2D-LSMM chaotic sequences are used to determine the operation and encoding rules of DNA sequences.

In [18], the authors proposed a new method that presented a hybrid model that uses the Lorenz–Rossler chaotic map to encode color images. The random sequences that are generated using Lorenz–Rossler chaotic systems are used to encode the essential components (red, green, and blue [RGB] channels) of the color image. To encode the original image, they used the rules of a DNA encoding system.

3. CHAOTIC SYSTEMS

Chaos theory is a branch of mathematics that is based on nonlinear and deterministic behavior. Any change in control parameters or initial values leads to a change in the chaotic output, which means chaotic systems have a higher sensitivity to their initial conditions. Chaotic systems are used in various areas, such as data encryption, data hiding, watermarking, and other areas that require unexpected results and outputs [19], [20]. Simplicity is a characteristic of a logistic map. Equation 1 explains the chaotic behavior of a 1D logistic map [21].

$$P_{i+1}=\mu * P_i * (1-P_i) \quad (1)$$

Where (μ) is the system control parameter, (P_0) is the initial state, (i) is the number of iterations, and the value of (P_{i+1}) is between (0 and 1) for all (i). The value of the control parameter (μ) is between (0 and 4), and the best result occurs when it is closer to 4. A 3D logistic map is better than a 1D logistic map [22]. Equations 2, 3, and 4 explain the chaotic behavior of a 3D logistic map.

$$x_{i+1}=\alpha x_i (1-x_i)+\beta y_i^2 x_i+\gamma z_i^3 \quad (2)$$

$$y_{i+1}=\alpha y_i (1-y_i)+\beta z_i^2 y_i+\gamma x_i^3 \quad (3)$$

$$z_{i+1}=\alpha z_i (1-z_i)+\beta x_i^2 z_i+\gamma y_i^3 \quad (4)$$

Where (β, α, γ) are three parameters ($0 < \beta < 0.022$), ($0 < \gamma < 0.015$), ($3.53 < \alpha < 3.81$), and z_0, y_0, x_0 take a value between (0 and 1).

4. DNA ENCODING

Information in DNA is stored as a code comprising four chemical bases: guanine (G), adenine (A), thymine (T), and cytosine (C). The rules are that "A" corresponds to "00", "C" corresponds to "01", "G" corresponds to "10", and "T" corresponds to "11". As in binary math, 1 and 0 are complements, so 11 and 00 are also complements. Similarly, 10 and 01 are complements. There are 24 types of coding groups, however, we use only 8 of them. Table 1 summarizes these rules [23]–[26].

Table 1. The rules of DNA encoding

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

Many researchers used algebraic operations like subtraction, addition, and XOR due to the rapidly developing nature of DNA computations. Tables 2–5 explain the results of applying XOR with the rules (1, 3, 5, 7).

Table 2. Result applying XOR operation on DNA rule 1

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

Table 3. Result applying XOR operation on DNA rule 3

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

Table 4. Result applying XOR operation on DNA rule 5

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

Table 5. Result applying XOR operation on DNA rule 7

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

5. PROPOSED METHOD

The method proposed in this paper has two stages: encryption and decryption. Fig. 1 explains the general layout of the proposed method.

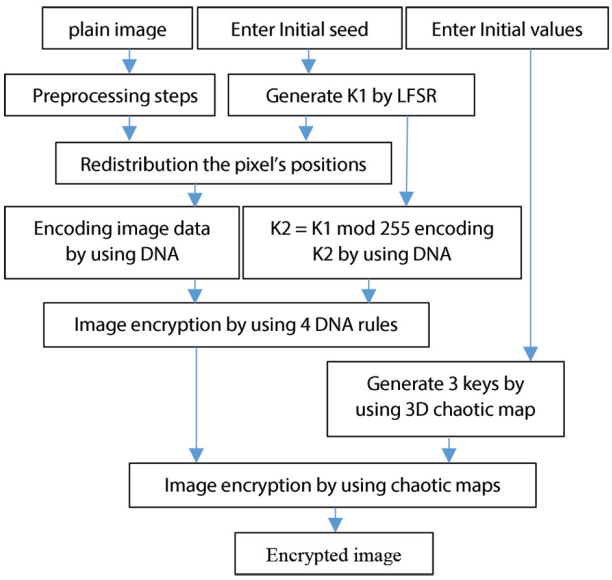


Fig. 1. The general layout for the proposed method

5.1. ENCRYPTION STAGE

The encryption stage aims to remove the correlation between adjacent pixels first by redistributing their positions and then changing the data values of the pixels by encrypting them using the rules of DNA coding and 3D chaotic maps.

5.1.1. PIXEL POSITION REDISTRIBUTED

In this stage, the original image's colors are separated into their essential RGB components, and then each color is divided into two equal parts (P1, P2). Using LFSR, generating a random key (K1) with non-repeated numbers of size (SK = H * W/2, where H and W represent the height and width of the image) and use the key to redistribute the positions of the pixels for each part (P1, P2). The random key is generated by using three registers with lengths of 29, 31, and 37 and join functions (2, 7, 13), (1, 2, 3), (1, 2, 3, 4, 5), respectively, and different initial values for each register. Fig. 2 explains the lengths and join functions for the registers.

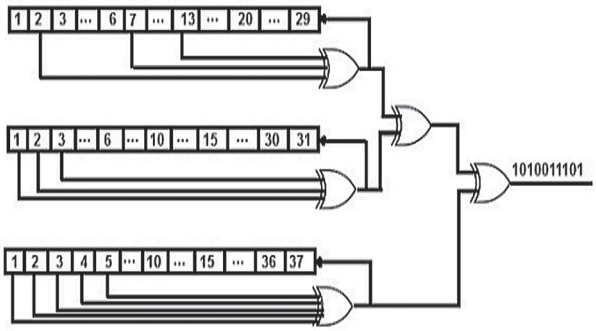


Fig. 2. Simplified drawing of a LFSR.

5.1.2. IMAGE ENCRYPTION USING DNA AND LFSR

The data for each color (P1, P2) is first converted to a binary value and then encoded using the first rule of DNA (A = 00, T = 11, C = 10, G = 01).

For example, if a pixel's value is (228), the binary number will be (11100100), rule 1 will be applied, and the outcome will be (TGCA).

A new key is calculated in the second step (K2 = K1 mod 256), then encoded using the first rule of DNA. The third step involves applying an XOR operation between the key (K2) values and the image data (P1, P2) that are coded to produce the encrypted image.

For example, when applying the XOR between the first code from the key (T) and the pixel (A) using Table 2, the result is (T). When applying the XOR between the second code from the key (C) and the pixel (G) using Table 3, the result is (A). This work continues until all image data is encrypted.

Algorithm 1 explains image data encryption using the rules of DNA and the LFSR.

Algorithm 1: The process of image encryption using the rules of DNA encoding and LFSR

Input: Plain color image
Output: Image encrypted by DNA encoding and LFSR

1. Enter an original color image (H * W).
2. Isolate image colors to essential RGB components.
3. Divide each color into two equal parts (P1, P2).
4. Convert data for each part (P1, P2) into a 1D array.
5. Generating a key (K1) with random non-duplicate numbers using LFSR with size (SK = H * W/2).
6. Redistribute pixel positions for each part (P1, P2) using the random key (K1).
7. Encode the data for each part (P1, P2) using the rule of DNA coding (rule 1) after converting it to a binary number.
8. Calculate a new key (K2 = K1 mod 256) with values ranging from (0 to 255).
9. Encode the key (K2) using the rule for coding DNA (rule 1) after converting it to a binary number.
10. Apply an operation XOR between the key and the data for each part (P1, P2) by using four DNA encoding rules (1, 3, 5, 7).

5.1.3. IMAGE ENCRYPTION USING 3D CHAOTIC MAPS

To encode the image data, generate three keys (Kr, Kg, Kb) by using 3D chaotic maps (refer to Equations 2, 3, 4), where one key is used to encrypt data relating to a specific color.

For example, encrypt the data for the color red (P1, P2) using the key (Kr).

Finally, the colors are combined to get the encoded image after the locations of the two parts (P1, P2) change for each color.

Algorithm 2 explains the process of image encryption using 3D chaotic maps.

Algorithm 2: The process of image encryption using 3D chaotic maps

Input: Image encrypted by DNA and LFSR
Output: Image encrypted
(result of the proposed method)

1. Generate 3 keys (Kr, Kg, and Kb) using the 3D chaotic map equations.
2. Apply the XOR operation between the keys and the color values.
3. Convert each part (P1, P2) into a 2D array.
4. Change the location of the two parts (P1, P2).
5. Reconstruct the image colors.
6. The result is an encrypted image.

5.2. DECRYPTION STAGE

Recovering the original image includes two stages. The first stage comprises entering the encrypted image, isolating the primary colors for the image (RGB), and dividing each color into two equal parts (P1, P2). Then, the data for each color is decrypted by generating the same three keys using 3D chaotic maps.

The second stage comprises the decryption of the data using the DNA rules (1,3,5,7) and the key generated by LFSR first. Second, recover the original position for each pixel using the key generated by LFSR. Algorithm 3 describes the decryption stage for images.

Algorithm 3: Process of image decryption

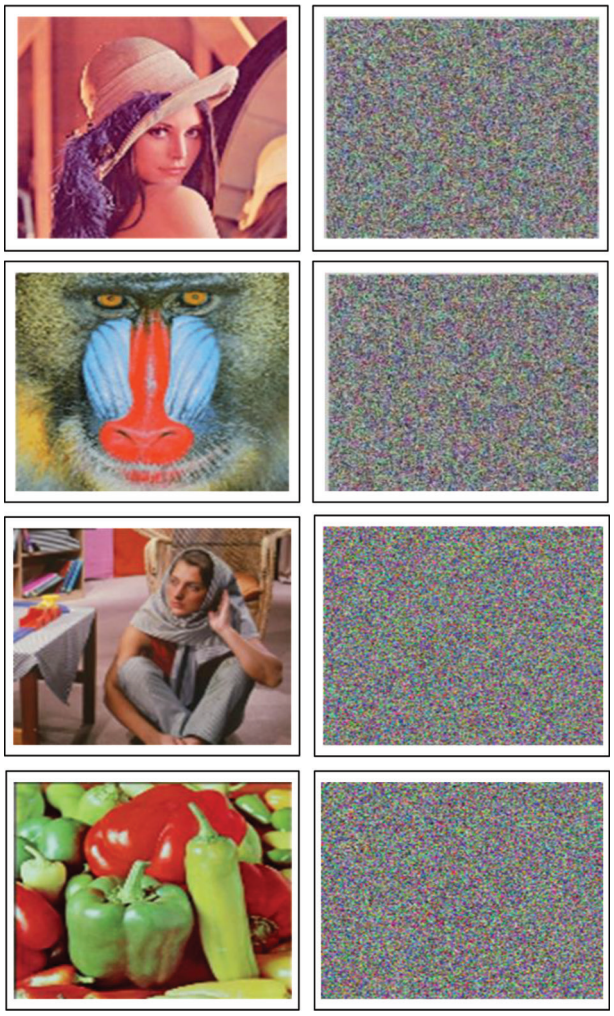
Input: Encrypted image
Output: Original color image

1. Enter the encrypted image (H * W).
2. Isolate the image colors into their essential RGB components.
3. Divide each color into two equal parts (P1, P2).
4. Convert the data for each part into a 1D array.
5. Generate 3 keys (Kr, Kg, and Kb) using 3D chaotic maps.
6. Apply the XOR operation between the keys and the color values.
7. Convert the data for each part (P1, P2) into a binary number and then encode it using the rule of DNA coding (rule 1).
8. Generate a key (K1) with random non-duplicate numbers using LFSR with size (SK = H * W/2).
9. Calculate a new key (K2 = K1 mod 256) with values ranging from (0 to 255).
10. Convert the key (K2) values to a binary number and then encode it using the rule for coding DNA (rule 1).
11. Apply an XOR operation between the key (K2) and each part (P1, P2) by using four DNA coding rules (1, 3, 5, 7).
12. Restore the original pixel positions using the key (K1).
13. Convert each part (P1, P2) into a 2D array.
14. Change the location of the parts (P1, P2).
15. Reconstruct the image colors.
16. The resulting image is the original image.

6. EXPERIMENTS

The proposed method for testing used a group of images (Lena, Peppers, Baboon, and Barbara) that were (256 * 256) in size. Fig. 3a shows the images used in the tests. The random number is generated using a group of bits generated through LFSR. The length of a series of bits depends on the number count required for the key.

The initial parameters $\beta = 0.02$, $\gamma = 0.015$, $\alpha = 3.84$, $y0 = 0.67$, $z0 = 0.97$, and $x0 = 0.97$ were used to produce the best results in the suggested method at the stage of data encoding using 3D chaotic maps. The proposed method's results are shown in Fig. 3 (b).



(a) (b)

Fig. 3. (a) Original images (b) Encrypted images

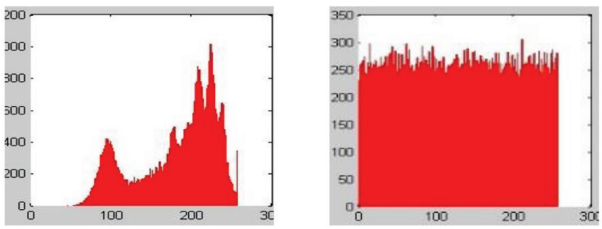
7. RESULTS AND DISCUSSION

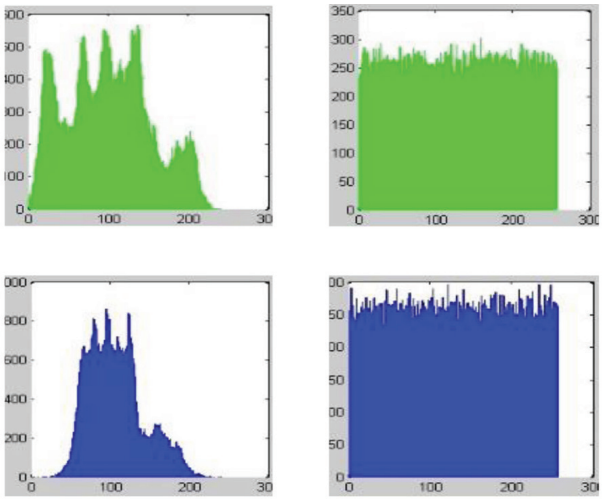
This section will present the results of applying various tests to the proposed method.

7.1. HISTOGRAM ANALYSIS

A histogram is employed to determine how pixels are arranged in an image and to learn more about the image's features. One method for attackers to discover an original image is to get the histogram of the encrypted image [27].

Fig. 4 (a) shows the original RGB histogram for the Lena image, and Fig. 4 (b) shows the RGB histogram for the encrypted Lena image.





(a) (b)

Fig. 4. RGB histogram analysis for the Lena image (a) Original image (b) Encrypted image

7.2. ENTROPY TEST

Entropy measures the strength and level of randomness provided by the encrypting system in terms of the amount of disorganization achieved in the image. Equation 5 is used to measure entropy [28].

$$H(q) = -\sum_{i=0}^{255} P(q_i)\ log_2\ P\ (q_i) \tag{5}$$

Where P(qi) is the probability of (qi) of pixels; the best value for the entropy of the encrypted image is the one closest to 8. Table 6 shows the entropy values of the images used in the experiments. The results show that the proposed method has excellent results and is near 8.

Table 6. Entropy values for the experiment's images.

image	Original image	Encrypted image
Lena	7.326	7.9973
Baboon	7.574	7.9974
Barbara	7.509	7.9971
Peppers	7.329	7.9972

7.3. UACI & NPCR TESTS

UACI tests determine the difference between the original and encrypted images. The variation rate between image pixels before and after the encryption is determined using a NPCR test. Equations 6, 7, and 8 are used to measure the NPCR and UACI tests [29].

$$UACI = \frac{1}{RC}\left[\sum_{i,j}\frac{|P_1(i,j)-P_2(i,j)|}{255}\right] * 100 \tag{6}$$

$$NPCR = \frac{\sum_{i,j} N(i,j)}{R*C} * 100 \tag{7}$$

$$N(i,j) = \begin{cases} 0, & if\ P_1(i,j) = P_2\ (i,j) \\ 1, & if\ \ P_1(i,j)\ \neq P_2\ (i,j) \end{cases} \tag{8}$$

Where P2 (i, j) is the original image, P1 (i, j) is an encrypted image, C is the image's width, and R is the

height of the image. Table 7 shows the results of applying the tests (NPCR and UACI) to the images used in the experiments after applying the proposed method.

Table 7. NPCR and UACI values for the experiment image

Image	NPCR			UACI		
	Red	Green	Blue	Red	Green	Blue
Lena	99.63	99.65	99.63	33	32	33
Baboon	99.61	99.60	99.62	30	28	31
Barbara	99.61	99.64	99.63	29	29	31
Peppers	99.62	99.60	99.59	29	34	34

7.4. CORRELATION TEST

The correlation test is one of the most important statistical tests used to assess the strength and effectiveness of the encryption system. An encryption algorithm removes and destroys the strong correlation between each pixel and its neighbors in the original image [30]. Use Equations 9, 10, and 11 to calculate the correlation coefficient.

$$r_{p,q} = \frac{\sum_{i=1}^{M}(p_i-\bar{p})(q_i-\bar{q})}{\sqrt{[\sum_{i=1}^{M}(p_i-\bar{p})^2][\sum_{i=1}^{M}(q_i-\bar{q})^2]}} \quad (9)$$

$$\bar{p} = \frac{1}{M}\sum_{i=1}^{M} p_i \quad (10)$$

$$\bar{q} = \frac{1}{M}\sum_{i=1}^{M} q_i \quad (11)$$

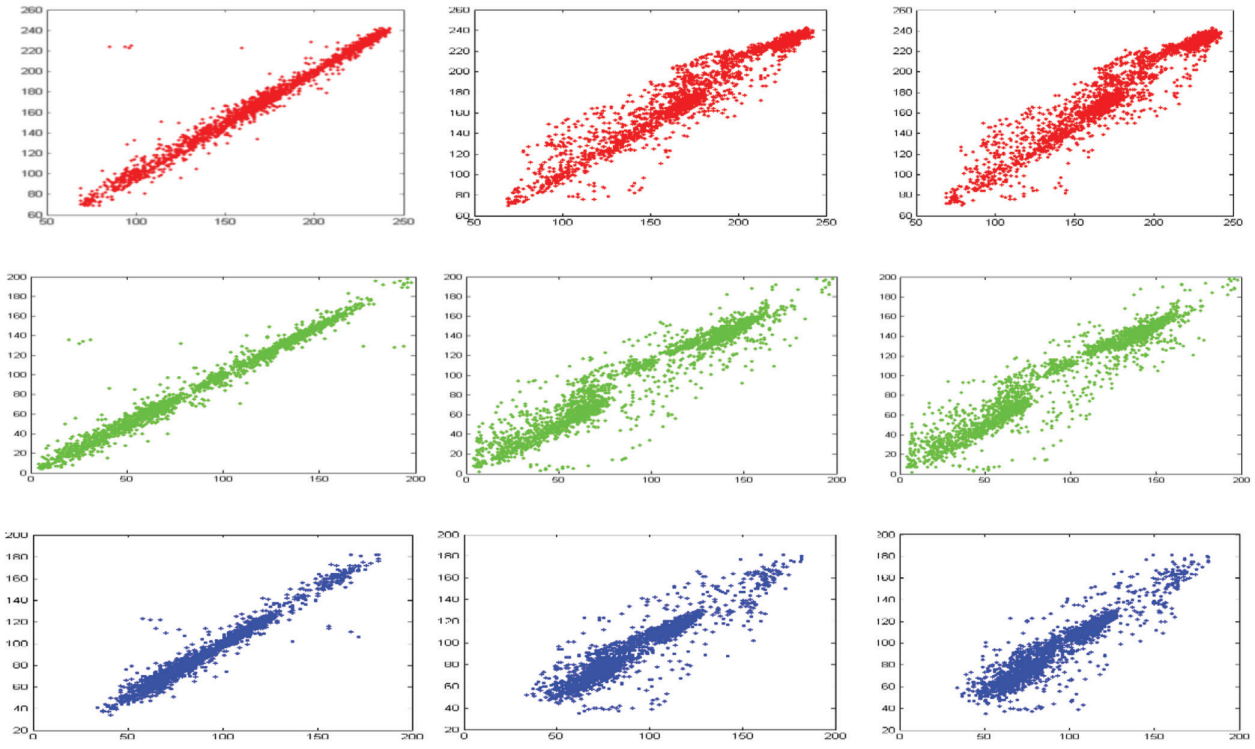
Where (pi) represents the value of the pixel (i-th) selected, (qi) represents the value of the adjacent pixel, and (M) represents the number of pixels selected from the image. Fig. 5 shows the results of applying the correlation test to the Lena image in the horizontal, vertical, and diagonal directions before and after applying the suggested method for 3000 pixels. Tables 8 and 9 show the correlation coefficient values for the test images before and after the suggested method was applied. Original image correlation coefficients are near 1, while cipher image correlation coefficients are close to 0. The results show that the proposed method's correlation coefficients achieve outstanding results close to 0.

Table 8. Correlation coefficients values for the original images

Image	Horizontal	Vertical	Diagonal
Lena	0.9534	0.9866	0.9540
Baboon	0.7289	0.6122	0.6324
Barbara	0.8974	0.9123	0.8427
Peppers	0.8780	0.9460	0.8542

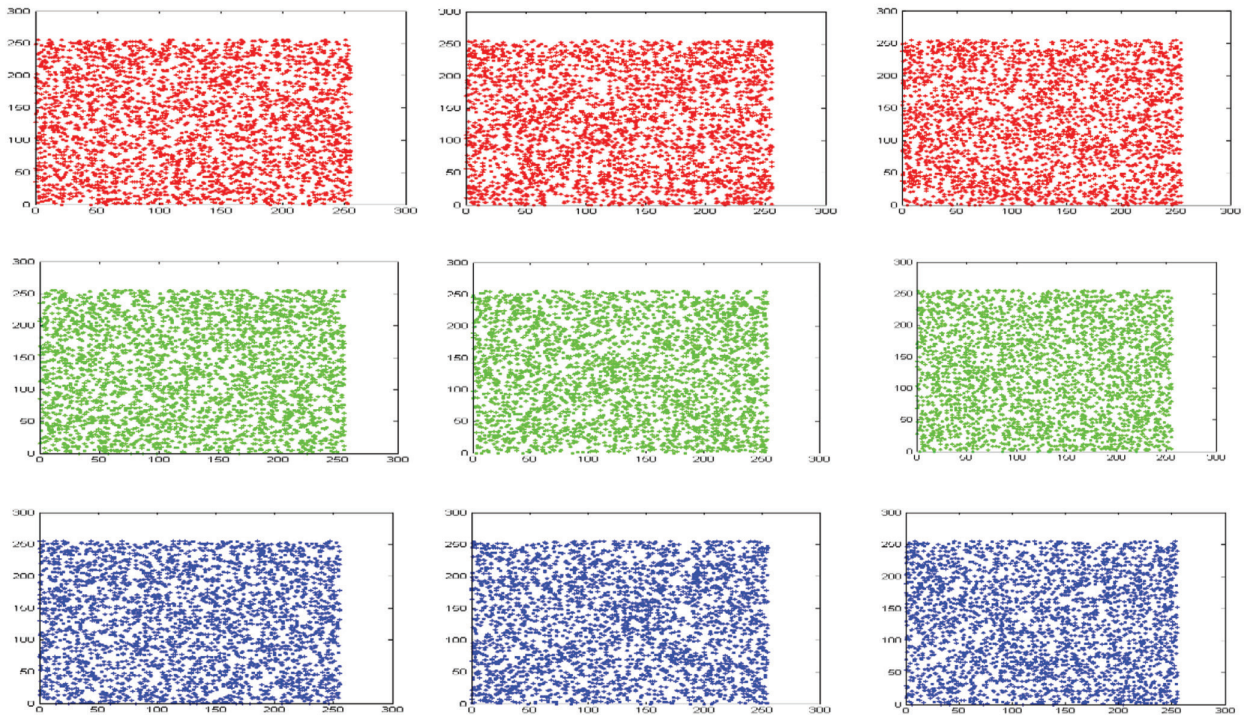
Table 9. Correlation coefficient values for the encrypted images

Image	Horizontal	Vertical	Diagonal
Lena	0.0096	-0.0071	-0.0079
Baboon	0.0016	-0.0023	-0.0087
Barbara	0.0030	-0.0068	-0.0147
Peppers	-0.0008	0.0015	-0.0134



Vertical Horizontal Diagonal

(a)



Vertical Horizontal Diagonal

(b)

Fig. 5. The RGB correlation test for the Lena's image (a) Original image (b) Encrypted image

7.5. PSNR ANALYSIS

One of the most crucial tests to evaluate the effectiveness of image coding systems is PSNR. When the PSNR value is less than 10, the encryption system's strength is excellent and ideal [31]. MSE represents the difference between the encrypted image and the original, and the optimal value of MSE is when it is very high [30], [31]. Use Equations 12 and 13 to calculate the PSNR and MSE values.

$$MSE = \frac{1}{mn}\sum_{ij}(M(i,j) - N(i,j))^2 \quad (12)$$

$$PSNR = 10log_{10}\left(\frac{P^2}{MSE}\right) \quad (13)$$

Where M (i, j) is an encrypted image, N (i, j) is the original image, (i, j) is the coordinate, and P is the range of pixels in the image [32]. Table 10 shows the results of MSE and PSNR values on the images after applying the proposed method. The results show differences between the original and encrypted image, as explained by the high MSE and low PSNR values.

Table 10. PSNR and MSE for the encrypted images

image	PSNR			MSE		
	Red	Green	Blue	Red	Green	Blue
Lena	7.845	8.558	9.548	106.80	90.63	72.15
Baboon	8.869	9.431	8.518	84.35	74.11	91.46
Barbara	9.016	8.956	8.444	81.55	82.67	93.03
Peppers	9.218	7.692	7.524	77.85	110.63	114.97

We compare the results of applying the proposed method with the results of other methods applied to the Lena image to determine the strength and effectiveness of the proposed method. Table 11 presents a comparison of the test results for entropy, MSE, PSNR, and correlation using the suggested method and other researchers' results on the Lena image.

Table 11. A comparison between the proposed method and some other methods.

Method	Entropy	NPCR	UACI	Correlation		
				H	V	D
Proposed method	7.997	99.64	32.66	0.0096	-0.0071	-0.0079
REF. [4]	7.997	99.59	33.28	0.0016	-0.0020	0.0047
REF. [15]	7.999	99.61	33.47	-0.0001	0.0002	-0.0001
REF. [16]	7.997	99.62	33.42	0.0058	0.0033	0.0010
REF. [18]	7.997	99.63	33.37	-0.0010	-0.0030	-0.0051

8. CONCLUSION

Encryption is one of the most important ways to maintain the secrecy of data and prevent unauthorized access. This paper suggests a new encryption method for data at two levels to increase data security. The first level of protection combines LFSR and DNA coding, while the second uses chaotic maps. The randomness of LFSR in rearranging the locations of pixels at the first level and the 3D chaotic map in data encryption at the second give strength and robustness to this method. Several statistical tests were carried out to prove the ef-

fectiveness of the proposed method. The results of the tests revealed a high level of security compared to the results of other methods. Future work should aim to use other types of chaotic maps and DNA coding.

ACKNOWLEDGMENTS

The authors would like to thank Mustansiriyah University (www.uomustansiriyah.edu.iq) in Baghdad, Iraq, for supporting this work. The authors also appreciate the comments of reviewers.

9. REFERENCES

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

[2] J. Lin, K. Zhao, X. Cai, D. Li, Z. Wang, "An Image Encryption Method Based on Logistic Chaotic Mapping and DNA Coding", Proceedings of Remote Sensing Image Processing, Geographic Information Systems, and Other Applications, Vol. 11432, 2019.

[3] J. Chauhan and A. Jain, "Survey On Encryption Algorithm Based On Chaos Theory And DNA Cryptography", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, No. 8, 2014, pp. 7801-7803.

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

[5] S. T. Allawi, "Image Encryption Based on Chaotic Mapping and Random Numbers", Journal of Engineering and Applied Sciences, Vol. 14, No. 19, 2019, pp. 6954-6958.

[6] Z. Li, C. Peng, W. Tan, L. Li, "A Novel Chaos-Based Image Encryption Scheme by Using Randomly DNA Encode and Plaintext Related Permutation", Applied Sciences., Vol. 10, No. 21, 2020, pp. 1-19.

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

[8] Y. Wang, X. Li, Q. Wang, " Integral Imaging Based Optical ImageEncryption Using CA-DNA Algorithm", IEEE Photonics Journal, Vol. 13, No. 2, 2021.

[9] T. V. Medha Sreenivasan, A. Sidhardhan, V. M. Priya, "5D Combined Chaotic System for Image Encryption with DNA Encoding and Scrambling", Proceedings of the International Conference on Vision Towards Emerging Trends in Communication and Networking, Vellore, India, 30-31 March 2019.

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

[11] P. Vinotha, D. Jose, "VLSI Implementation of Image Encryption Using DNA Cryptography", Intelligent Communication Technologies and Virtual Mobile Networks, Springer Nature, Switzerland, 2020, pp. 190-198.

[12] K. S. Kumari and C. Nagaraju, "DNA encrypting rules with Chaotic Maps for Medical Image Encryption", Proceedings of the 5th International Conference on Intelligent Computing and Control Systems, Madurai, India, 6-8 May 2021 pp. 832-837.

[13] Nalini M. K and Radhika K. R, "Secured Key Generation for Biometric Encryption using Hyper-Chaotic Map and DNA Sequences", SSRN Electronic Journal, 2021, pp. 585-595.

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

[15] S. M. Hameed, I. A. Taqi, "A New Beta Chaotic Map with DNA Encoding for Color Image Encryption", Iraqi Journal of Science, Vol. 61, No. 9, 2020, pp. 2371-2384.

[16] K. H. Moussa, H. G. Mohamed, D. H. ElKamchouchi, "A Novel Color Image Encryption Algorithm Based on Hyperchaotic Maps and Mitochondrial DNA Sequences", Entropy, Vol. 22, No. 158, 2020, pp. 1-15.

[17] J. Zheng and L. F. Liu, "Novel Image Encryption by Combining Dynamic DNA Sequence Encryption and the Improved 2D Logistic Sine Map," IET Image Process., vol. 14, no. 11, pp. 2310–2320, 2020, doi: 10.1049/iet-ipr.2019.1340.

[18] A. Girdhar, V. Kumar, "A RGB image encryption technique using Lorenz and Rossler chaotic system on

DNA sequences", Multimedia Tools and Applications, Vol. 77, No. 20, 2018, pp. 27017-27039.

[19] M. S. Fadhil, A. K. Farhan, M. N. Fadhil, "Designing Substitution Box Based on the 1D Logistic Map Chaotic System", IOP Conference Series: Materials Science and Engineering, Vol. 1076, No. 1, 2021, p. 012041.

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

[21] C. L. Chunhu Li, G. Luo, "An Image Encryption Scheme Based on The Three-Dimensional Chaotic Logistic Map", International Journal of Network Security, Vol. 21, No. 1, 2019, pp. 22-29.

[22] M. B. Hossain, M. T. Rahman, A. B. M. S. Rahman, S. Islam, "A New Approach of Image Encryption Using 3D Chaotic Map to Enhance Security of Multimedia Component", Proceedings of the International Conference on Informatics, Electronics & Vision, Dhaka, Bangladesh, 23-24 May 2014.

[23] K. Singh, 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, 2011, pp. 17-24.

[24] K. A. Kumari, B. Akshaya, B. Umamaheswari, K. Thenmozhi, R. Amirtharajan, P. Praveenkumar, "3D Lorenz Map Governs DNA Rule in Encrypting DICOM Images", Biomedical and Pharmacology Journal, Vol. 11, No. 2, 2018, pp. 897-906.

[25] B. Wang, S. Zhou, X. Zheng, C. Zhou, J. Dong, L. Zhao, "Image watermarking using chaotic map and DNA coding", Optik, Vol. 126, No. 24, 2015, pp. 4846-4851.

[26] S. J. Sheela, K. V. Suresh, D. Tandur, "A Novel Audio Cryptosystem Using Chaotic Maps and DNA Encoding", Journal of Computer Networks and Communications, Vol. 2017, 2017.

[27] F. A. Salman, K. A. Salman, "Enhanced Image Encryption Using Two Chaotic Maps", Journal of ICT Research and Applications, Vol. 14, No. 2, 2020, pp. 134-148.

[28] M. Tanveer et al. "Multi-Images Encryption Scheme Based on 3D Chaotic Map and Substitution Box", IEEE Access, Vol. 9, 2021, pp. 73924-73937.

[29] S. Agarwal, "Secure Image Transmission Using Fractal and 2D-Chaotic Map", Journal of Imaging, Vol. 4, No. 1, 2018.

[30] A. M. Alabaichi, "Color Image Encryption using 3D Chaotic Map with AES Key Dependent S-Box", International Journal of Computer Science and Network Security, Vol. 16, No. 10, 2016, pp. 105-115.

[31] C. Liu, Q. Ding, "A Color Image Encryption Scheme Based on a Novel 3D Chaotic Mapping", Complexity, Vol. 2020, 2020.

[32] S. T. Allawi, M. M. Abbas, R, H. Mahdi, "New Method For Using Chaotic Maps To Image Enceyption", International Journal of Civil Engineering and Technology, Vol. 9, No. 13, 2018, pp. 244-231.