Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 10, No. 04, December 2024.

IMAGE ENCRYPTION TECHNIQUE BASED ON BINARY COMBINATION OF MULTIPLE CHAOTIC MAPS AND DNA SEQUENCE OPERATIONS

Nisreen I. R. Yassin

(Received: 11-May-2024, Revised: 17-Jul.-2024, Accepted: 30-Jul.-2024)

ABSTRACT

The huge advance of digital communication and networks has led to enormous storage and transmission of information over public networks. Nevertheless, the assurance of information security remains incomplete across these unsecured networks. Currently, digital images are the primary mean for sharing information over open networks. Consequently, the confidentiality of digital images during storage and transmission has become a crucial concern, particularly when sharing sensitive information. Image encryption has emerged as a solution to this problem. This paper presents an image encryption technique based on multiple one-dimensional chaotic maps and DNA coding. The technique employs three one-dimensional chaotic maps, including the logistic map, tent map and piecewise map, multiple times to produce 18 random sequences with different initial values and parameters. SHA-512 hash function is used to indicate the initial values of chaotic maps. For encrypting images, the binary elements from various sequences of chaotic maps are amalgamating to alter the pixel intensities of the image in the diffusion process. Dynamic DNA coding is performed through random selection of DNA rules and operations (XOR, XNOR and Addition) to each pixel in the image. The technique is enforced using circular rotations which are applied randomly to each key. The proposed technique is evaluated using many standard images. Different performance metrics have been measured. The empirical findings illustrate the security and resilience of the suggested method and its ability to resist statistical and differential attacks.

KEYWORDS

Information security, Cryptography, Chaotic maps, Image encryption, DNA.

1. INTRODUCTION

The transmission and sharing of information and confidential data mostly occur *via* digital networks and the internet, using digital images, texts, voice messages and videos. This transmission includes online banking, e-commerce transactions and the military, which has increased the need for data protection and privacy preservation. Of all the data types, digital images have the ability to efficiently communicate visual information with compact storage sizes, thus they are the most commonly used on social applications [1]. Digital images are widely shared through various communication media, so it is essential to ensure the security of these images from malicious and unlicensed access attempts [2]-[3].

Cryptography is one of the information-security techniques used by many security companies to protect social data, government communications and personal transactions. Cryptography uses a secret key to convert data into an unreadable format that has no textual or visual meaning. In this case, the attacker cannot access the content directly, but tries to find the key or disrupt the access process. Therefore, the basic goal is to increase the computational cost of the unauthorized decryption process to make it infeasible [4]-[5]. Classical encryption algorithms such as Data Encryption Standard (DES) [6] or Advanced Encryption Standard (AES) [7] which are used for text encryption have demonstrated ineffectiveness in encrypting images due to strong image pixel correlation, high redundancy and the large size of images [8]-[9]. For instance, when an image undergoes encryption *via* a substitution cipher, it merely alters the colour of the image, allowing retrieval or comprehension by a malicious entity. Image encryption depends on two processes which are confusion and diffusion. The confusion process aims to change the locations of image pixels, thus breaking the correlation between adjacent pixels and each pixel in the cipher image will be related to a part of the used key. The diffusion process aims to alter the image-pixel values, therefore diffusing the frequencies of the plain-image pixels [10].

Chaos systems are nonlinear, deterministic, but unpredictable systems, first introduced by Matthews for image encryption [11]-[12]. Chaos systems are characterized by strong randomness and high sensitivity to parameters and initial conditions. Chaotic maps are one-dimensional or high-dimensional maps.

N. Yassin is with National Research Centre, Cairo, Egypt. Email: nisreen.yassin20@gmail.com

One-dimensional chaotic maps are easy to implement in software and hardware due to their simple structure. The cryptosystems based on one- or two-dimensional chaotic maps are characterized by simplicity and low execution time, but the defects are small key space and restricted complexity, which lead to soft security [13]-[15]. On the other hand, high-dimensional chaotic maps have a larger number of initial conditions and control parameters, which leads to a larger key space and thus more security [16]. The drawback of these maps is the increased execution time required to solve high-dimensional equations. As a solution, researchers used a combination of simple chaotic maps instead of high-dimensional maps [3].

Scientists have found that using only chaotic maps for image encryption is not enough to achieve high security. DNA coding has been combined with chaotic maps to improve the diffusion of the image-encryption process. Using this mixture has led to promising results according to randomness and nonlinearity. This study aims to leverage the characteristics of one-dimensional chaotic maps, specifically the simplicity of their construction and their pronounced sensitivity to initial conditions. Meanwhile, it seeks to address the limitations linked to these properties, including a limited key space and constrained complexity. The idea is to generate multiple maps with different initial values and different control parameters, therefore achieving the necessity of large key space. SHA- 512 hash function and DNA coding are combined with chaotic maps to increase security and enhance the diffusion process. In this paper, a novel image-encryption technique is proposed. The technique is a pixel-based technique that uses three one-dimensional chaotic maps (Logistic Map, Tent Map and Piecewise Map) multiple times to generate random sequences required for permutation and diffusion processes. The keys of the diffusion process are formed by mixing the corresponding binary digits of the random sequences followed by a circular rotation performed randomly according to a random-number generator. DNA coding for image pixels and generated keys is performed using a randomly selected rule number. Then, a randomly selected operation of the three DNA mathematical operations (XOR, XNOR and Addition) is performed. To enhance security, XOR is applied with another mixed key to obtain the final cipher image.

The main contributions of the proposed work are as follows:

- The manuscript introduces a resilient and efficient method for encrypting images by amalgamating the binary elements from various sequences of chaotic maps to alter the pixel intensities in the image.
- Erratic DNA coding is performed using randomly selected DNA rule numbers and DNA mathematical operations.
- The technique is reinforced by using the SHA-512 hash function and randomly circular rotations.
- The technique is designed to have multiple initial conditions and control parameters and a large key space.

The remainder of the paper is arranged as follows: related works are introduced in Section 2, preliminary works are given in Section 3, the proposed method is given in Section 4, the analysis results are shown in Section 5 and conclusions are stated in Section 6.

2. RELATED WORK

Image encryption techniques depend mainly on two phases, the confusion phase and the diffusion phase. In this section, some related state-of-the-art techniques are presented. Qobbi et al. [17] presented an image-encryption system based on two 1D chaotic maps, which are logistic and tent maps. These maps are used to generate permutation and substitution table. The proposed system is highly related to the plain image. Kumar and Girdhar [18] developed a scheme for image encryption based on DNA coding and chaotic maps. Lorenz and Rossler chaotic maps are used to diffuse the image at the pixel level, then a 2D logistic map is performed at the bit level to confuse the image. Rahul et al. [19] used the logistic map, the Henon map and the Lorenz system associated with DNA encoding to safeguard digital images. Their approach included enhancing the system through the utilization of the SHA-256 hash function and zigzag traversal. Akraam et al. [3] proposed an encryption algorithm based on a combination of the chaotic maps: logistic map, piecewise linear chaotic map, tent map and Henon map. These maps are used to generate two keys which are used to diffuse the decimal pixels of the image. Li et al. [20] used a classical chaotic map and a two-dimensional Lorenz chaotic map to encrypt and decrypt the image.

Niu et al. [21] proposed an image-encryption scheme based on chaotic maps and DNA. They used logistic and Henon maps to perform pixel permutation and diffusion. Bidirectional exclusive OR operations are used to strengthen the scheme. Ibrahim et al. [14] used a logistic chaotic function to generate random round keys, which are used to modify individual pixels using the DNA Playfair matrix. Wu et al. [22] proposed a new map called two-dimensional Hénon-Sine map. DNA encoding and XOR function are applied to encrypt the image. Gera and Agrawal [23] proposed an image-encryption approach based on a 4D discrete hyperchaotic map and DNA coding. Global scrambling is performed on the binary image, then DNA algebraic operations are applied for diffusion. Wan et al. [24] used a modular operation to form a new one-dimensional chaotic map based on several existing one-dimensional chaotic maps. The new chaotic map combined with DNA coding is used to encrypt the image. Enayatifar et al. [25] proposed an encryption system based on DNA coding and logistic map and using a genetic algorithm to indicate the best DNA mask for encryption. Liu et al. [26] introduced a novel image-encryption method designed to encrypt numerous medical images simultaneously. This proposed approach relies on a recent chaotic model and a novel DNA operation. Lai et al. [27] introduced a novel memristive Hopfield neural network (HNN) which was utilized for the creation of an image-encryption scheme. Lai et al. [28] introduced a theoretical structure aimed at the creation of the ultraboosting memristive hyperchaotic map. The framework gives rise to four distinct hyperchaotic maps, all of which are utilized in the design of an image-encryption technique. Liu et al. [29] proposed an encryption technique to encrypt remotely sensed airport images. The technique is based on indicating the positions of sensitive information then encrypting these positions using high-speed index-dynamic diffusion. Liu et al. [30] enhanced sine cross coupled mapping lattice (ISCCML) to produce a better key stream. Moreover, a fractal disordered matrix (FDM) is introduced, which exhibits iterative and out-of-order characteristics, designed for the concurrent scrambling diffusion of images. Wang et al. [31] proposed an image-encryption scheme based on two-parameter wide-range system with a mixed coupled map lattice model (TWMCML). Three-dimensional bit-level coupled XOR technique is used to scramble the significant regions of the image. Liu et al. [32] proposed a chaotic system called improved sinusoidal dynamic non-adjacent coupled mapping lattice (ISDNCML). Based on the proposed chaotic system, the private and non-private regions of an image have been encrypted. Lia and Liu [33] derived a 2D-hyperchaotic map used to encrypt colour images. Strong encryption is obtained by using circular-shift confusion and bidirectional-parallel diffusion.

3. PRELIMINARY WORKS

3.1 Chaotic Maps

Chaotic maps are mathematical functions that generate a highly erratic pattern based on the initial seed value. These dynamic systems can generate millions of bits in a period before the pattern repeats with ultimate sensitivity to initial conditions or changes in control parameters. This feature of chaotic maps leads to their extensive use in multimedia encryption, where a hacker cannot implement pattern-analysis attacks [34]. This section describes three chaotic maps used in the proposed technique.

3.1.1 Logistic Map

The logistic map is characterized by its simplistic nature, yet intricate dynamical behaviour. It is defined by Equation (1) [10], [17].

$$X_n = rX_{(n-1)}\left(1 - X_{(n-1)}\right) \tag{1}$$

where X_n is the population at time n and $0 < X_n < 1$. r is the control parameter that lies in the interval $[0\ \ 4]$. The logistic map exhibits chaotic behaviour for r values exceeding 3.569945. Figure 1(a) shows the bifurcation diagram of the logistic map using control parameters in the range of [3 4].

3.1.2 Tent Map

The tent map is a simple chaotic map calculated using Equation (2) [17], [35].

$$T_{n+1} = \begin{cases} uT_n, & if \quad T_n < 0.5 \\ u(1 - T_n), & otherwise \end{cases} \tag{2}$$

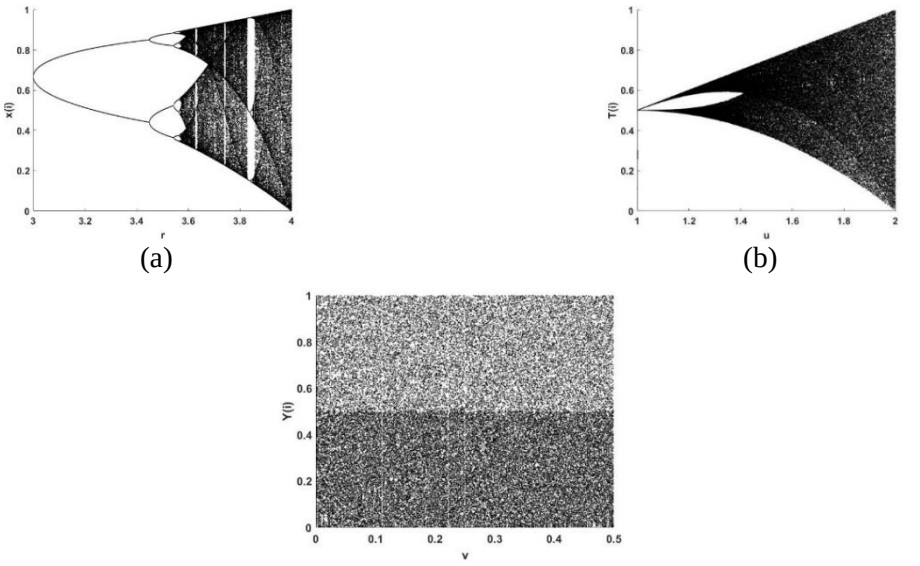
where $0 \leq u \leq 2$ is the control parameter and $T_n \in [0\ \ 1]$. T_0 is the initial value. Figure 1(b) shows the bifurcation diagram of the tent map using control parameters in the range of [1 2].

3.1.3 Piecewise Linear Chaotic Map

The mathematical representation of the piecewise linear chaotic map is shown in Equation (3) [36].

$$Y_{n+1} = \begin{cases} \frac{Y_n}{v}, & if \quad 0 \le Y_n < v \\ \frac{Y_n - v}{0.5 - v}, & if \quad v \le Y_n < 0.5 \\ 1 - Y_n, & if \quad 0.5 \le Y_n < 1 \end{cases} \tag{3}$$

The initial value Y_0 is in the interval $[0 \ \ 1]$ and $v \in [0 \ \ 0.5]$ is the control parameter. Figure 1(c) shows the bifurcation diagram of the piecewise linear chaotic map using control parameters in the range of [0 0.5].



(a) (b) (c)

Figure 1. Bifurcation diagrams of (a) logistic map, (b) tent map and (c) piecewise linear chaotic map.

3.2 DNA Encoding

Deoxyribonucleic acid (DNA) is a chemical compound that is responsible for generating all types of cell proteins in living organisms. It consists of four nucleic acid bases: adenine (A), thymine (T), guanine (G) and cytosine (C). The relationship between these bases is elucidated by the Watson-Crick rules [37], which posit that T (11) is the complement of A (00) and C (01) is the complement of G (10). There are eight rules that represent the binary encoding of DNA nucleotides, where the utilized binary bases are 00, 11, 01 and 10. The binary representation of DNA encoding rules is illustrated in Table 1. The proposed technique employs the use of DNA mathematical operations, especially XOR, XNOR and Addition, during the diffusion process. The DNA representation of these operations is presented in Table 2.

Table 1. DNA encoding rules.

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

Table 2. DNA mathematical functions.

	XOR				**XNOR**				**Addition**			
	A	**T**	**C**	**G**	**A**	**T**	**C**	**G**	**A**	**T**	**C**	**G**
A	A	T	C	G	T	A	G	C	A	T	C	G
T	T	A	G	C	A	T	C	G	T	C	G	A
C	C	G	A	T	G	C	T	A	C	G	A	T
G	G	C	T	A	C	G	A	T	G	A	T	C

4. THE PROPOSED TECHNIQUE

The proposed technique comprises three distinct stages: key generation, permutation and diffusion. The key-generation process depends on the SHA 512 hash function of the plain image to compute the initial conditions of the chaotic maps. Therefore, any change in the plain image directly affects the algorithm keys. The permutation process involves the random positioning of pixels of the original image according to the coordinates of chaotic-map sequences. The diffusion process entails the mixing of binary bits from a set of generated chaotic maps and DNA coding. The detailed steps of the proposed technique are as follows.

1- The initial step is to read the plain image I of size MxN, where M and N are the dimensions of the image in terms of rows and columns, respectively.

2- Generate the SHA 512 hash function of I to be used as a unique key. Convert it into a binary sequence B of length l_B. Divide B into a number of parts P according to the required number of initial values ni as illustrated in Equation (4).

$$P = \{P_1,\ P_2, \dots, P_{ni}\} = \lfloor (l_B/ni) \rfloor \tag{4}$$

where l_B is the length of SHA 512 hash function which is 512 bits and ni =18.

3- Divide each part p into groups of eight bits, as indicated by Equation (5). The initial conditions of the chaotic maps, designated as x_i, are calculated. In the proposed technique, the number of required initial conditions is 18, therefore 18 keys are generated by XOR bits from each group.

$$K(i) = \left\{(k_1 \oplus k_2 \oplus k_3)_{P_1}, \dots, (k_1 \oplus k_2 \oplus k_3)_{P_{ni}}\right\} = \lfloor \{P_1,\ P_2, \dots, P_{ni}\}/8) \rfloor \tag{5}$$

$$x_i = K(i)/256 \tag{6}$$

where each k is a fold of 8 bits and i is a number from 1 to n_i.

4- Reshape I into one-dimensional array I_1 of size $L = 1xMN$. For RGB images, concatenate the three colour channels R, G and B of the image I to be an image of size $Mx3N$, then reshape I into one-dimensional array I_1 of size $L = 1x3MN$.

5- Generate two chaotic sequences $X_1$and T_1 of size L using logistic map and tent map illustrated by Eq. (1) and Eq. (2) using two initial values calculated by Equation (6).

6- Sort sequences X_1 and T_1 ascendingly to get the positions of their members P_1 and P_2. The two arrays P_1 and P_2 contain L random numbers, which will be used for permutation the image I_1.

7- Arrange the pixels of the image I_1 according to the random numbers P_1 in order to obtain the permutated image I_2. The second permutation process involves arranging the pixels of the image I_2 according to the random numbers' array P_2 resulting in the image I_3.

8- For the diffusion process, generate eight chaotic sequences using multiple chaotic maps: the logistic map, the tent map and the piecewise map with eight initial conditions derived from Eq. (6). For example, three sequences using the logistic map $[X_2, X_3, X_4]$, two sequences using the tent map $[T_2, T_3]$ and three sequences using the piecewise map $[Y_1, Y_2, Y_3]$. All generated sequences are of size L.

9- Consider z as in Equation (7) as a representation for the generated maps

$$z = \{X_{2(i-L)}, T_{2(i-L)}, Y_{1(i-L)}, X_{3(i-L)}, T_{3(i-L)}, Y_{2(i-L)}, X_{4(i-L)}, Y_{3(i-L)}\} \tag{7}$$

10- Convert each element i in each sequence of z into binary representation z_{ib} using Equations (8, 9).

$$z_i = \lfloor (z_i * 10)/10 \rfloor \tag{8}$$

$$z_{ib} = \begin{cases} 0 & 0 \le z_i \le 0.5 \\ 1 & 0.5 < z_i < 1 \end{cases} \tag{9}$$

11- Concatenate z_{ib} from each corresponding sequence in z to form the binary sequence w as in Equation (10).

$$w = \{w_1, \dots, w_L\} = \{[X_{21}T_{21}Y_{11}X_{31}T_{31}Y_{21}X_{41}Y_{31}], \dots, [X_{2L}T_{2L}Y_{1L}X_{3L}T_{3L}Y_{2L}X_{4L}Y_{3L}]\} \tag{10}$$

12- For each pixel in I_3, two random numbers are generated, R_1 being in the range from one to

eight, indicates the DNA rule number, while R_2 in the range from 1 to three indicates the DNA operation. The mathematical expression used for generating pseudo random numbers is described by Equation (11).

$$R_{n+1} = (aR_n + c)\ mod\ m \tag{11}$$

The integers $a, c, and\ m$ indicate the characteristics of the random-number generator.

13- Convert each pixel in I_3 to the corresponding binary form. To diffuse the image I_3, DNA encoding process is employed based on a random rule number R_1 and one randomly selected operation from three DNA operations: XOR, XNOR and ADD using R_2.
14- Shift the value of $w(i)$ left or right according to the DNA rules. For the first four DNA rules, $w(i)$ is shifted left by a value from one to four bits, while for the second four DNA rules, $w(i)$ is shifted right.
15- Encode $I_3(i)$ and $w(i)$ using DNA rule numbers indicated by R_1. Perform one DNA operation between $I_3(i)$ and $w(i)$ according to the random value of R_2 . This value should be interpreted as follows: one indicates XOR operation, two indicates XNOR operation and three indicates Addition operation.
16- Decode the result from DNA representation to binary representation using the same rule numbers R_1 to obtain the diffused image I_4.
17- Repeat steps (8-10) to generate $\grave{w}$ another combination of a binary sequence of different eight maps using the initial conditions produced by Eq. (6).
18- Shift $\grave{w}(i)$ and $I_4(i)$ left or right according to two random numbers R_3 and R_4 generated from one to four.
19- Apply XOR function between the shifted $\grave{w}(i)$ and $I_4(i)$ to obtain the diffused image I_5. Reshape I_5 to be the cipher image.

The proposed technique is illustrated in Figure 2. By repeating the same steps in reverse order, the cipher image is decrypted to its original state.

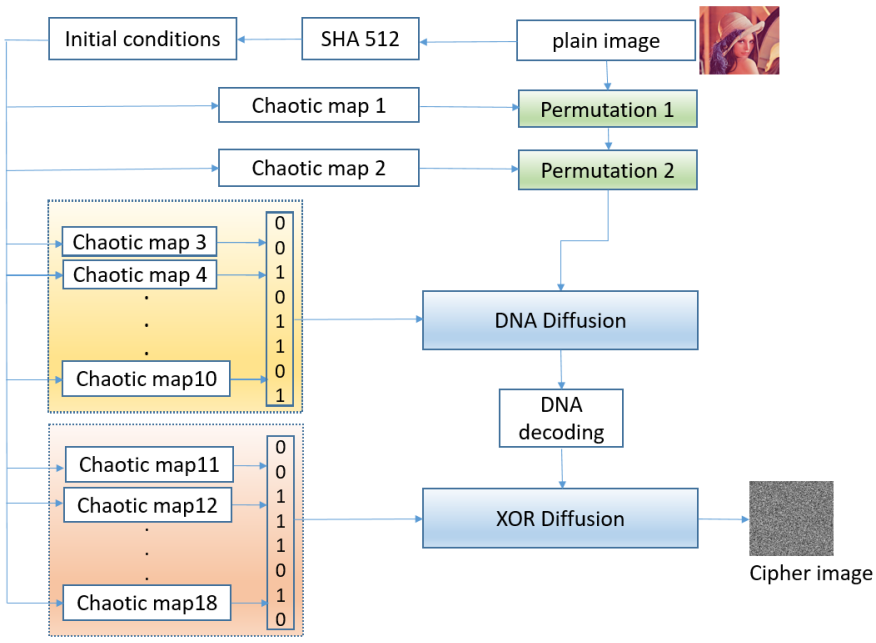


Figure 2. Summary of the proposed cryptosystem.

The proposed system is described by an example as follows.

1- Initialization:
   - Suppose an original image I_1 of size 4x4. Convert the image into 1D vector of size 1x16.

130	118	110	100
198	193	187	179
99	119	138	153
49	47	47	49

I_1	130	198	99	49	118	193	119	47	110	187	138	47	100	179	153	49

- A key is generated using the hash 256 function of the image. Let the generated key as K. All generated initial conditions are in the range [0 1], K such as

K	204	124	……	201	154

- Generate 6 chaotic sequences from each map illustrated by Eqs. (1-3) using K. The control parameter of the logistic map X is 3.8956 for the first sequence, then an increment of 0.001 is used to indicate the remaining control parameters. The same criterion is used for the tent and piecewise linear maps. For the tent map T, the control parameter of the first sequence is 1.5 with an increment of 0.05 for the following tent sequences. The control parameter of the first sequence of piecewise linear map Y is 0.25678900 with an increment of 0.0000111.
- Generate two integer random numbers, the first for DNA rule numbers in the range of [0 7] and the second for DNA operations in the range of [1 3], where one indicates XOR, two indicates XNOR and three indicates ADD.

DNA rule no. (R_1)	1	7	……	3	6
DNA operations (R_2)	2	2	……	1	3

2- Permutation:
- First permutation: sort X(1), then get the index P_1. Rearrange I_1 according to P_1 to obtain the first permutated image vector I_2.

P_1	3	10	13	16	6	4	1	8	11	14	7	5	15	12	9	2

- Second permutation: sort T(1) to obtain P_2 and I_3.

P_2	4	10	16	14	8	2	12	6	5	11	1	7	13	15	9	3

- The permutation result

Original	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
image I_1	130	198	99	49	118	193	119	47	110	187	138	47	100	179	153	49
1st perm	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
I_2	119	49	130	193	47	118	138	47	153	198	110	179	99	187	100	49
2nd perm	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
I_3	110	118	49	119	153	47	179	47	100	49	198	138	99	193	187	130

3- DNA diffusion:
- Select eight sequences from X, T and Y. Transform them into the binary form, then generate the combination W illustrated by Eq. (10). Transform pixels of I_3 into binary representation.

$I_3(1) = 110$	01101110
W = {X(2),T(2),Y(1),X(3),T(3),Y(2),Y(3),X(4)}(1)	10000100

- Perform circular shift for W, then encode the binary values into DNA representation using DNA rule number R_1.

$I_3(1)$	01101110	GCTC
Circular shift	00100001	ACAG

- Perform DNA operation R_2. Transform the obtained DNA code into binary form and obtain the diffused pixels.

XNOR	GCTC	
ACAG	CTAA	10110000
		$I_4(1) = 176$

I_3	110	118	49	119	153	47	179	47	100	49	198	138	99	193	187	130
I_4	176	181	217	43	221	91	73	69	207	206	27	97	252	112	248	135

4- XOR diffusion

- Select eight sequences from X, T and Y. Transform them into the binary form, then generate the combination W' illustrated by Eq. (10). Transform pixels of I_4 into binary representation.

$I_4(1) = 176$	10110000
W' = {X(5),T(4),Y(4),X(6),T(5),Y(5),Y(6),T(6)}(1)	01001001

- Apply circular shift, then XOR function to obtain the cipher image I_5.

XOR	10110000	
10100100	00010100	$I_5(1) = 20$

I_4	176	181	217	43	221	91	73	69	207	206	27	97	252	112	248	135
I_5	20	213	159	255	222	82	195	116	91	221	127	107	14	124	176	112

130	118	110	100
198	193	187	179
99	119	138	153
49	47	47	49

Original image

20	222	91	14
213	82	221	124
159	195	127	176
255	116	107	112

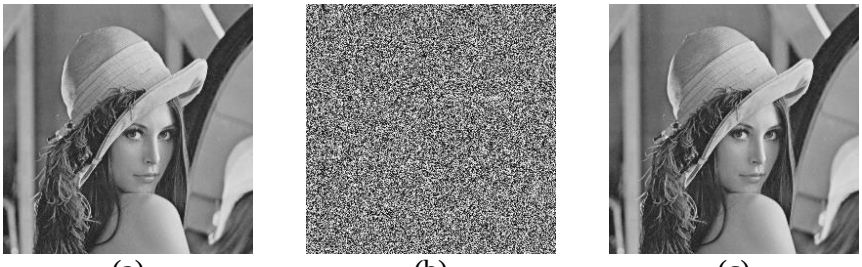
Encrypted image

5. EXPERIMENTAL RESULTS

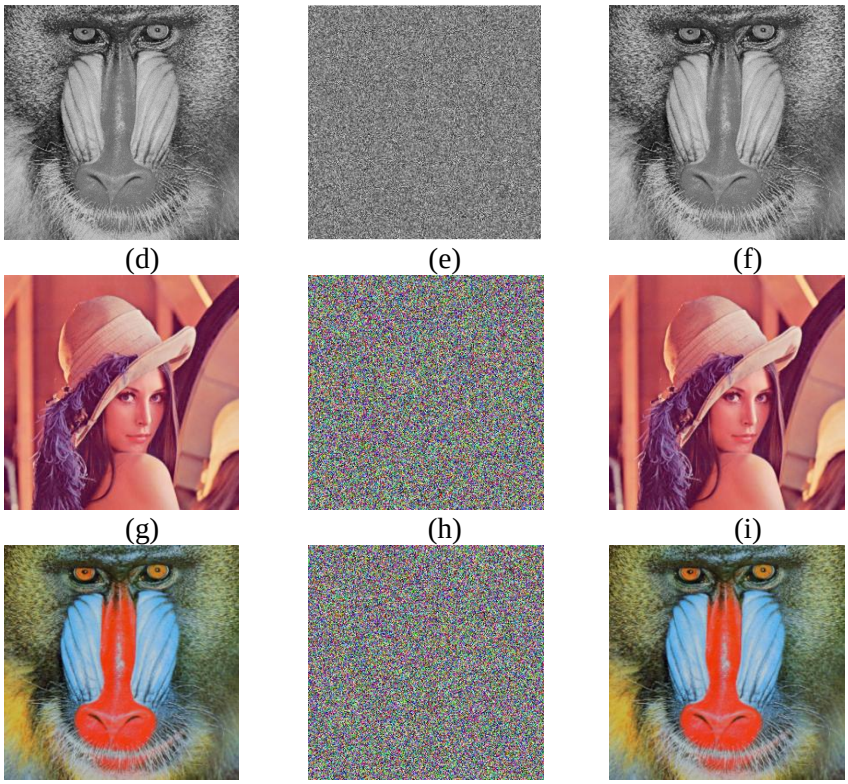
The performance of the proposed cryptosystem is evaluated using the images "Lena ", "Baboon ", "Peppers ", "Boat", "Barbara " and "Airplane ", of size 256x256 and 512x512 from the USC-SIPI image database [38]. RGB images of size 256x256x3 were also used to test the system. The simulation is performed using MATLAB R2017b on a computer with Windows 10 operating system, 4GB RAM and 3.40 GHz processor. Key generation is an important step in the encryption process. The initial values of the used chaotic maps are identified based on the generated key. There is a unique SHA 512 hash function for each original image; therefore, it is excellent to be used to generate a unique key for each image. In the proposed technique, the hash value is used to generate 18 initial values which are used to generate 18 chaotic sequences with multiple use of control parameters r=3.8956, u=1.5 and v=0.25678900. Two permutation steps are performed on the image using two chaotic maps. The keys for the diffusion process are generated by mixing the binary digits of eight chaotic maps. The first diffusion uses DNA coding along with three generated random numbers to indicate the DNA rule number, the DNA operation and the amount of circular left or right shift. The second diffusion employs an XOR operation between randomly shifted processed pixels and randomly shifted keys. Figure 3 shows original, encrypted and decrypted versions of Lena and Baboon images using the proposed technique.

5.1 Histogram Analysis

The histogram declares the distribution of pixels of an image. Figure 4 shows the histogram of gray images of Lena and Baboon before and after the encryption process. Similar results are obtained for RGB images. The difference between the histogram of the plain images and the histogram of the encrypted images is apparent. The histogram of encrypted images is flat and equally distributed, which is the opposite of a typical histogram. Therefore, the images encrypted by the proposed technique are robust against statistical attack.



(a) (b) (c)



(d) (e) (f)

(g) (h) (i)

(j) (k) (l)

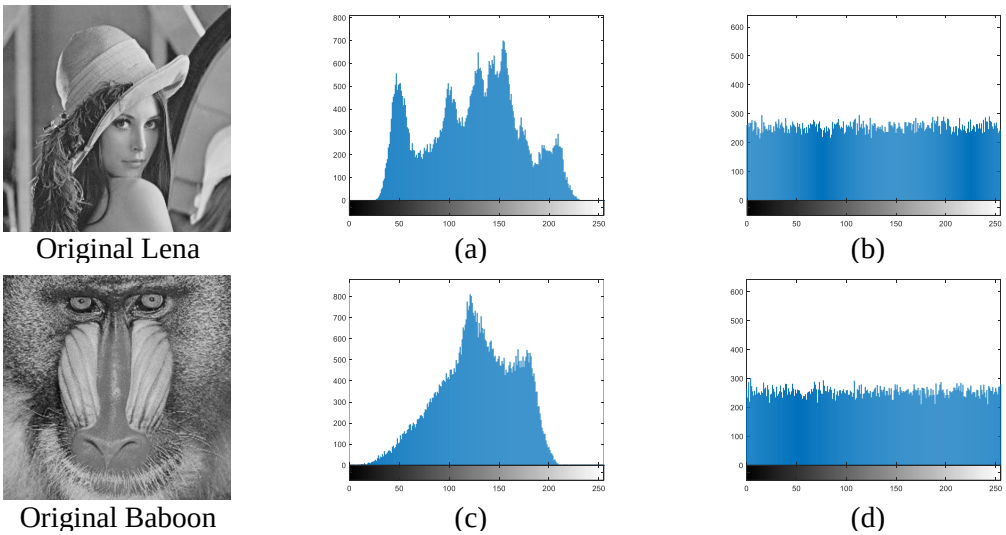
Figure 3. Plain images, cipher images and decrypted images: (a-c) gray Lena 256x256 (d-f) gray Baboon 512x512 (g-i) RGB Lena (j-l) RGB Baboon.

5.2 Chi-square Test (X^2)

X^2 test is a test that measures how well a model fits the observed data. In the case of encryption, the distribution of pixels in an image can be measured using X^2. The theoretical value of X^2 for the encrypted image is 293.24783 [39]. Any encrypted image should have an X^2 value lower than the theoretical value. The value of X^2 can be calculated using Equation (12).

$$X^2 = \sum_i^{256} (p_i - 256)^2/256 \quad (12)$$

where i is the gray scale levels and p_i is the corresponding frequency occurrences. Tables 3 and 4 display the X^2 values for the plain images Lena, Baboon, Boat, Peppers, Barbara and Airplane, as well as their respective X^2 values after encryption. It is evident that all X^2 values of encrypted images are lower than the theoretical values.



Original Lena (a) (b)

Original Baboon (c) (d)

Figure 4. Histogram analysis: (a, b) histogram of original and encrypted Lena 256x256, (c-d) histogram of original and encrypted Baboon 512x512.

Table 3. Chi-square values of plain images (256x256) and the corresponding cipher images.

Images	Lena	Baboon	Boat	Peppers	Airplane	Barbara
Plain	39868.726	58107.609	100674.875	33094.195	174458.335	27793.562
Encrypted	243.3984	280.1857	246.8359	216.6406	239.1250	290.2109
[29]	252.7891	261.3301	282.5039	-	-	-
[3]	286.4766	219.5625	-	214.7813	-	-
[21]	222.0156	247.9766	-	237.375	-	-

Table 4. Chi-square values of RGB plain images (256x256x3) and the corresponding cipher images.

Images	Lena	Baboon	Boat	Peppers	Airplane	Barbara
Plain	65305.64	29129.86	54151.70	57105.97	167182.92	28923.28
Encrypted	312.0391	268.7500	238.2422	199.8281	237.7109	236.9219

5.3 Entropy Analysis

Entropy measures the randomness of the data. According to images, it shows the distribution of pixels in an image. The maximum value of entropy is eight, where all the pixels are uniformly distributed with $1/256$ probability of occurrence for each. Therefore, an encrypted image achieve randomness if its entropy is close to eight. The entropy is computed using Equation (13).

$$E(m) = \sum_{i=0}^{2^n-1} p(m_i) \log_2 \frac{1}{p(m_i)} \tag{13}$$

where n is the number of bits used to represent a pixel and $p(m_i)$ is the probability of occurrence of a pixel (m_i). Tables 5 and 6 show entropy values of the proposed technique using standard images. It is clear that all measured entropy values are close to eight approximately above 7.997 for 256x256 images and 7.9992 for 512x512 images, which ensures the randomness of the proposed technique.

Table 5. Entropy of the proposed technique using standard images of size 256x256.

Images	Plain Image	Cipher Image	[3]	[23]	[20]
Lena	7.4429	7.9979	7.9969	7.9972	7.9894
Peppers	7.5620	7.9976	7.9976	-	-
Airplane	6.7261	7.9974	-	-	-
Baboon	7.2374	7.9972	7.9976	-	-
Boat	7.1587	7.9973	-	-	-

Table 6. Entropy of the proposed technique using standard images of size 512x512.

Images	Proposed technique	[29]	[31]	[20]
Lena	7.9994	7.99935	-	7.9916
Peppers	7.9992	7.99921	7.9993	-
Airplane	7.9993	-	-	7.9916
Baboon	7.9992	7.99928	7.9993	7.9914
Boat	7.9993	7.99921	-	7.9916

5.4 Correlation Analysis

Correlation analysis is used to measure the similarity between the original image and the encrypted image. In the original image, the correlation between adjacent pixels is approximately one because of high similarity between adjacent pixels. In the encrypted image, the similarity between adjacent pixels should be none; therefore, the correlation between them should be zero. The correlation between adjacent pixels can be calculated using Equations (14-17) [38].

$$\bar{x} = 1/N \sum_{i=1}^{N} x_i \tag{14}$$

$$D(x) = 1/N \sum_{i=1}^{N} (x_i - \bar{x})^2 \tag{15}$$

$$cov(x, y) = 1/N \sum_{i=1}^{N} (x_i - \bar{x})(y_i - \bar{y}) \tag{16}$$

$$C_r = cov(x, y)/\sqrt{D(x)D(y)} \quad (17)$$

where N is the total number of pixels $m * n$. To calculate the correlation between adjacent pixels for both original image and encrypted image, two arrays x, y are created of 3000 randomly selected pixels and their corresponding adjacent pixels for the three directions horizontal, vertical and diagonal. Table 7 shows the correlation values between adjacent pixels for both original and encrypted standard gray images Lena, Peppers, Airplane, Baboon, Boat and Barbara. It is clear that the correlation value of adjacent pixels of encrypted images obtained using the proposed technique is significantly reduced, where the maximum value is 0.007. Table 8 shows the correlation of adjacent pixels for both original and encrypted standard RGB images Lena, Peppers, Airplane, Baboon, Boat and Barbara. As we can see, the correlation between adjacent pixels for the three colour channels of the encrypted images is very low. The introduced results are emphasized by Figure 5, which depicts the correlation of plain and encrypted Lena images in the three directions horizontal, vertical and diagonal. These results indicate the security and resistance of the proposed algorithm.

Table 7. Correlation analysis of the gray images using the proposed technique.

Gray Image	***Plain Image***			***Cipher Image***		
	Horizontal	**Vertical**	**Diagonal**	**Horizontal**	**Vertical**	**Diagonal**
Lena	0.9258	0.9593	0.9037	-0.0029	0.0019	0.0076
Baboon	0.8700	0.8410	0.7888	0.00003	-0.00003	-0.0082
Airplane	0.9396	0.9331	0.8883	0.0010	0.0012	-0.0039
Peppers	0.9675	0.9729	0.9432	0.0040	0.0034	0.0085
Boat	0.9268	0.9452	0.8833	0.0081	-0.0024	0.0039
Barbara	0.9342	0.9567	0.9056	-0.0072	-0.0016	0.0031

Table 8. Correlation analysis of the RGB Images using the proposed technique.

Image	**Color channels**	**Original Image**			**Encrypted Image**		
		H	**V**	**D**	**H**	**V**	**D**
Lena	R	0.9558	0.9781	0.9336	-0.0034	0.0053	0.0030
	G	0.9401	0.9695	0.9180	-0.00009	-0.0010	0.00007
	B	0.9189	0.9495	0.8948	0.0037	0.00005	0.0029
Peppers	R	0.9646	0.9680	0.9369	0.0064	0.0012	0.0027
	G	0.9698	0.9750	0.9466	0.00002	0.0043	0.0051
	B	0.9570	0.9636	0.9263	-0.0004	-0.0038	0.0044
Airplane	R	0.9389	0.9239	0.8738	-0.0040	-0.0019	0.0053
	G	0.9309	0.9343	0.8814	-0.0007	-0.0054	-0.0036
	B	0.9503	0.9089	0.8800	0.0076	-0.0030	-0.0013
Baboon	R	0.9105	0.8595	0.8474	0.0035	-0.0017	0.0028
	G	0.8594	0.7755	0.7434	0.0011	-0.0012	-0.0004
	B	0.8953	0.8697	0.8296	-0.0003	0.0050	-0.0063
Boat	R	0.9563	0.9539	0.9274	0.0038	-0.0054	-0.0060
	G	0.9558	0.9527	0.9225	0.0019	0.0032	-0.0034
	B	0.9603	0.9645	0.9369	-0.0003	0.0033	-0.0001
Barbara	R	0.9526	0.9611	0.9182	0.0038	-0.00003	0.0005
	G	0.9445	0.9543	0.9029	0.0007	-0.0046	-0.0027
	B	0.9526	0.9624	0.9182	0.0014	0.0015	-0.0004

5.5 Plaintext Sensitivity Analysis

A cryptosystem must be robust against any slight change in the plaintext image. Therefore, if a randomly selected pixel of the plaintext image is slightly changed, the resulting encrypted image will be different. Two metrics are used to evaluate the plaintext sensitivity of a cryptosystem: NPCR (number of pixel changing rate) and UACI (unified averaged changed intensity) [40]. The mathematical representations of NPCR and UACI are given by Equations (18) and (19).

$$NPCR(E_1, E_2) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)=\begin{cases}1, & if\ E_1(i,j)\neq E_2(i,j)\\ 0, & if\ E_1(i,j)=E_2(i,j)\end{cases}}{M\times N} \times 100\% \quad (18)$$

$$UACI(E_1, E_2) = \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|E_1(i,j)-E_2(i,j)|}{255} \times 100\% \quad (19)$$

where E_1 and E_2 are two encrypted images corresponding to two plaintext images differing by a slight difference in only one randomly selected pixel. M and N are the dimensions of the image. The cryptosystem is robust and sensitive to plaintext image if the value of NPCR is greater than 99% and the value of UACI is around 33% [3]. Table 9 shows the achieved values of NPCR and UACI for the images Lena, Pepper, Airplane, Baboon, Boat and Barbara. The results demonstrate the robustness of the proposed cryptosystem against differential attacks.

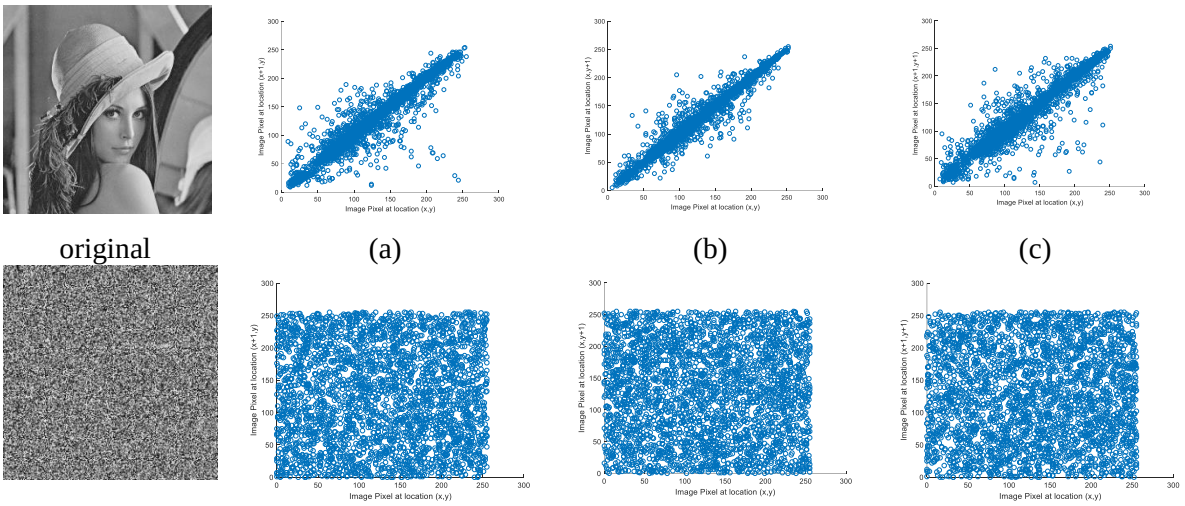


Figure 5. Correlation of adjacent pixels of plain and encrypted Lena images: (a, d) horizontal direction, (b, e) vertical direction, (c, f) diagonal direction.

Table 9. NPCR and UACI values for grayscale images of size 256x256.

Image	**Selected pixel**	**NPCR(%)**	**UACI(%)**	**[3]**
Lena	P(1,1)	99.63	33.46	99.64/33.42
Peppers	P(167,233)	99.61	33.50	99.64/33.40
Airplane	P(217,17)	99.64	33.57	-
Baboon	P(34,50)	99.68	33.61	99.64/33.43
Boat	P(128,128)	99.63	33.45	-
Barbara	P(256,256)	99.68	33.47	-

5.6 Speed Analysis

An important issue of the cryptosystem is the time efficiency. The speed of the proposed technique is evaluated based on Intel Core™i7 CPU at 2.60 GHz computer using Matlab 2017b. The proposed technique consumes about three seconds on average to encrypt an image of size 256x256.

5.7 Key Space Analysis

The key space is the total number of possible keys used in a cryptosystem. To be secure against brute-force attacks, the key space must be so large that it is infeasible for an intruder to compute the key and decrypt the image. The encryption algorithm is robust if the key space is larger than 2^{100} [3]. In the proposed technique, the key is formed from 18 chaotic maps with 18 initial conditions and 18 control parameters. If each variable has a computational accuracy of 10^{-15}, then the provided key space is 10^{540}. This large key space indicates that the proposed technique is highly resistant to brute-force attacks.

5.8 Key Sensitivity Test

The encryption system is key sensitive if the encrypted image is completely changed according to any slight change in the key. Therefore, the decryption process should fail if the original key is altered by small margin. To test the sensitivity of the proposed system, one initial condition is changed by adding 10^{-15} to its original value. The sensitivity-test results are shown in Figure 6. It is shown that the decryption of the cipher image failed due to the minor alteration that was introduced.

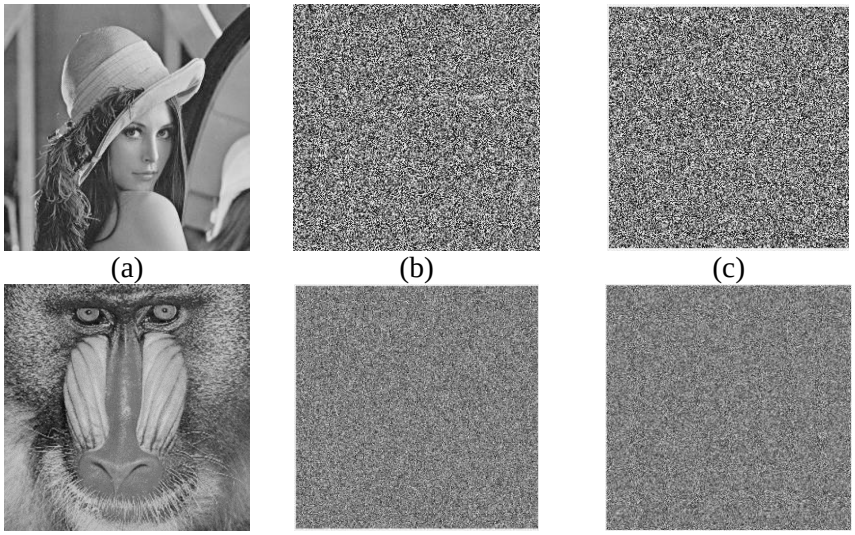


Figure 6. Key sensitivity test: (a, d) original images of Lena and Baboon, (b, e) encrypted images, (c, f) decrypted images.

5.9 Robustness Test

Images that are conveyed *via* communication channels may experience degradation due to the presence of noise introduced by either a malicious attacker or inherent characteristics of the channel, resulting in a decline in the overall quality of the encrypted images. The decrypted images' quality is influenced to some extent by noisy pixels; hence, the encryption method should possess a degree of resilience against noise interference. The robustness of the proposed technique is tested by adding 10% and 30% of salt and pepper noise to the original images, then encrypting the noisy images. Figures 7 and 8 show the encrypted and decrypted images subjected to salt and pepper noise. The figures illustrate the efficacy of the proposed system in effectively handling noisy images and extracting crucial data to the fullest extent.

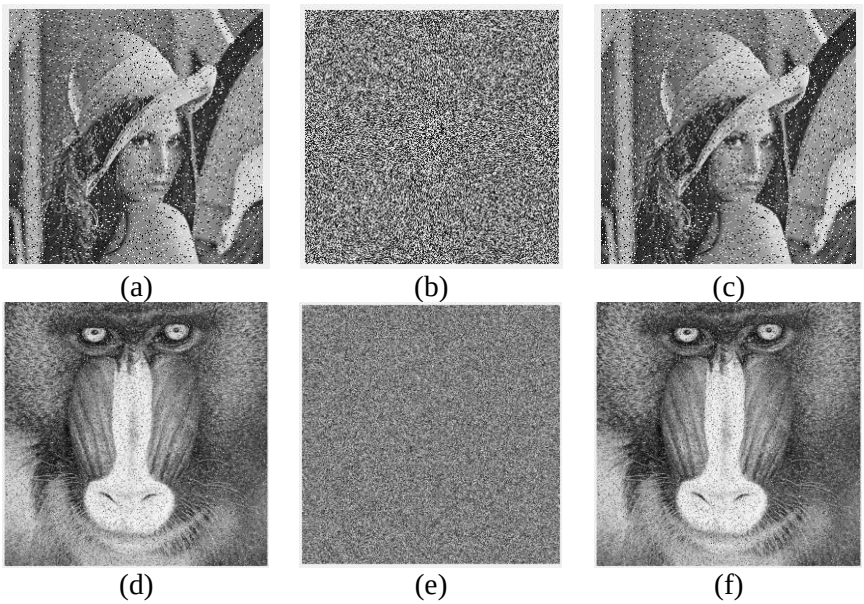


Figure 7. Robustness test (10% salt and pepper noise): (a, d) noisy original images of Lena and Baboon, (b, e) encrypted images, (c, f) decrypted images.

Table 10. Statistical test comparison for Lena images of size 256x256.

Metric	*Entropy*	*Chi-square*	*NPCR (%)*	*UACI (%)*	*Correlation Analysis*		
					Horizontal	**Vertical**	**Diagonal**
Proposed	7.9979	243.3984	99.63	33.46	-0.0029	0.0019	0.0076
[3]	7.9969	286.4766	99.64	33.42	0.0222	0.0354	0.0006
[20]	7.9894	-	99.66	33.42	0.0044	0.0015	0.0019
[41]	7.9992	-	99.614	33.364	0.0019	0.0014	0.0052
[21]	7.9976	222.0156	99.61	33.51	0.0305	−0.0043	0.0042
[23]	7.9972	-	99.63	-	-0.0028	-0.00006	-0.0011

Table 11. Statistical test comparison for Baboon images of size 512x512.

Metric	*Entropy*	*Chi-square*	*NPCR (%)*	*UACI (%)*	*Correlation Analysis*		
					Horizontal	**Vertical**	**Diagonal**
Proposed	7.9992	302.7969	99.61	33.45	4.644e-04	2.42e-04	8.622e-04
[41]	7.9998	-	99.645	33. 426	0.0024	0.0054	0.0041
[22]	7.9992	-	0.9959	0.3352	0.9671	0.9744	0.9381
[42]	7.9992	-	0.9960	0.3349	0.7508	0.8562	0.7153

The outcomes of the statistical and differential analyses of the proposed technique are compared with those of a few schemes in the literature for the images of Lena and Baboon as illustrated in Tables 10 and 11, respectively. The comparison evinces the efficacy and resilience of the proposed technique.

6. CONCLUSIONS

This paper proposes a new encryption technique based on the multiple use of different one-dimensional chaotic maps. Two chaotic sequences are used to scramble the pixel positions. The key stream for the diffusion process is composed of the concatenation of the corresponding binary digits of the generated random sequences. Each generated key is circularly rotated by a random value. DNA coding is applied based on three different DNA functions (XOR, XNOR and Addition). Random-number generators are used to select the DNA function, the DNA rule number and the value of the circular rotation. The proposed technique is applied to standard grayscale images and RGB images. The simulation results demonstrate the effectiveness and high security of the proposed technique.

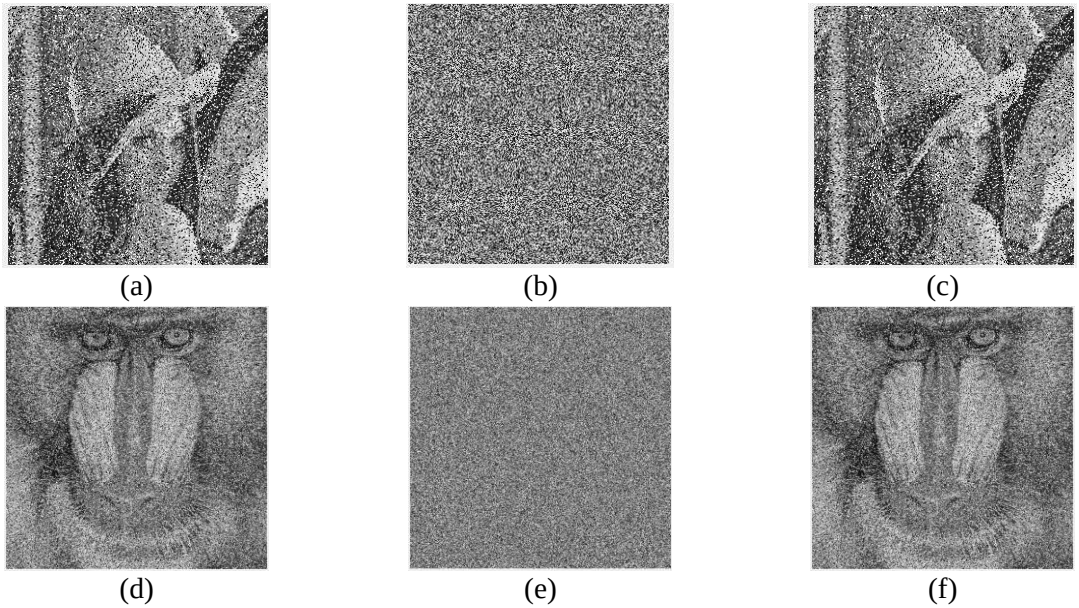


Figure 8. Robustness test (30% salt and pepper noise): (a, d) noisy original images of Lena and Baboon, (b, e) encrypted images, (c, f) decrypted images.

CONFLICT OF INTERESTS

The author declares no conflict of interests.

REFERENCES

[1] N.-R. Zhou, L.-J. Tong and W.-P. Zou, "Multi-image Encryption Scheme with Quaternion Discrete Fractional Tchebyshev Moment Transform and Cross-coupling Operation," Signal Processing, vol. 211, p. 109107, 2023.

[2] E. Yavuz, "A Novel Chaotic Image Encryption Algorithm Based on Content-sensitive Dynamic Function Switching Scheme," Optics & Laser Technology, vol. 114, pp. 224-239, 2019.

[3] M. Akraam, T. Rashid and S. Zafar, "A Chaos-based Image Encryption Scheme is Proposed Using Multiple Chaotic Maps," Mathematical Problems in Engineering, vol. 2023, DOI: 10.1155/2023/2003724, 2023.

[4] J. Fridrich, Steganography in Digital Media: Principles, Algorithms and Applications, DOI: 10.1017/CBO9781139192903, Cambridge University Press, 2009.

[5] J. Buchmann, Introduction to Cryptography, 2nd Edn, ISBN: 0387207562, Springer, 2004.

[6] S. Toughi, M. H. Fathi and Y. A. Sekhavat, "An Image Encryption Scheme Based on Elliptic Curve Pseudo Random and Advanced Encryption System," Signal Processing, vol. 141, pp. 217-227, 2017.

[7] E. Tromer, D. A. Osvik and A. Shamir, "Efficient Cache Attacks on AES and Countermeasures," Journal of Cryptology, vol. 23, pp. 37-71, 2010.

[8] R. Shivhare, R. Shrivastava and C. Gupta, "An Enhanced Image Encryption Technique Using DES Algorithm with Random Image Overlapping and Random Key Generation," Proc. of the 2018 IEEE Int. Conf. on Advanced Computation and Telecommunication (ICACAT), pp. 1-9, Bhopal, India, 2018.

[9] Q. Zhang and Q. Ding, "Digital Image Encryption Based on Advanced Encryption Standard (AES)," Proc. of the 2015 5th IEEE Int. Conf. on Instrumentation and Measurement, Computer, Communication and Control (IMCCC), pp. 1218-1221, Qinhuangdao, China, 2015.

[10] H. Kolivand, S. F. Hamood, S. Asadianfam and M. S. Rahim, "Image Encryption Techniques: A Comprehensive Review," Multimedia Tools and Applications, pp. 1-36, DOI: 10.1007/s11042-023-17896-0, 2024.

[11] U. Zia et al., "Survey on Image Encryption Techniques Using Chaotic Maps in Spatial, Transform and Spatiotemporal Domains," Int. Journal of Information Security, vol. 21, pp. 917-935, 2022.

[12] R. Matthews, "On the Derivation of a "Chaotic" Encryption Algorithm," Cryptologia, vol. 13, pp. 29-42, 1989.

[13] B. Yang and X. Liao, "A New Color Image Encryption Scheme Based on Logistic Map over the Finite Field ZN," Multimedia Tools and Applications, vol. 77, pp. 21803-21821, 2018.

[14] L. Meng, S. Yin, C. Zhao, H. Li and Y. Sun, "An Improved Image Encryption Algorithm Based on Chaotic Mapping and Discrete Wavelet Transform Domain," Int. Journal of Network Security, vol. 22, pp. 155-160, 2020.

[15] B. Mondal, S. Singh and P. Kumar, "A Secure Image Encryption Scheme Based on Cellular Automata and Chaotic Skew Tent Map," Journal of Information Security and Applications, vol. 45, pp. 117-130, 2019.

[16] D. S. Malik and T. Shah, "Color Multiple Image Encryption Scheme Based on 3D-Chaotic Maps," Mathematics and Computers in Simulation, vol. 178, pp. 646-666, 2020.

[17] Y. Qobbi, A. Jarjar, M. Essaid and A. Benazzi, "Image Encryption Algorithm Using Dynamic Permutation and Large Chaotic S-Box," Multimedia Tools and Appli., vol. 82, pp. 18545-18564, 2023.

[18] V. Kumar and A. Girdhar, "A 2D Logistic Map and Lorenz-Rossler Chaotic System Based RGB Image Encryption Approach," Multimedia Tools and Applications, vol. 80, pp. 3749-3773, 2021.

[19] B. Rahul, K. Kuppusamy and A. Senthilrajan, "Dynamic DNA Cryptography-based Image Encryption Scheme Using Multiple Chaotic Maps and SHA-256 Hash Function," Optik, vol. 289, p. 171253, 2023.

[20] T. Li, B. Du and X. Liang, "Image Encryption Algorithm Based on Logistic and Two-dimensional Lorenz," IEEE Access, vol. 8, pp. 13792-13805, 2020.

[21] Y. Niu, Z. Zhou and X. Zhang, "An Image Encryption Approach Based on Chaotic Maps and Genetic Operations," Multimedia Tools and Applications, vol. 79, pp. 25613-25633, 2020.

[22] J. Wu, X. Liao and B. Yang, "Image Encryption Using 2D Hénon-Sine Map and DNA Approach," Signal Processing, vol. 153, pp. 11-23, 2018.

[23] U. K. Gera and S. Agrawal, "Image Encryption Using a Combination of 4D Discrete Hyperchaotic Map and DNA Encoding," Multimedia Tools and Applications, vol. 83, pp. 38037-38054, 2023.

[24] Y. Wan, S. Gu and B. Du, "A New Image Encryption Algorithm Based on Composite Chaos and Hyperchaos Combined with DNA Coding," Entropy, vol. 22, p. 171, 2020.

[25] R. Enayatifar, A. H. Abdullah and I. F. Isnin, "Chaos-based Image Encryption Using a Hybrid Genetic Algorithm and a DNA Sequence," Optics and Lasers in Engineering, vol. 56, pp. 83-93, 2014.

[26] H. Liu, L. Teng, Y. Zhang, R. Si and P. Liu, "Mutil-medical Image Encryption by a New Spatiotemporal Chaos Model and DNA New Computing for Information Security," Expert Systems with Applications, vol. 235, p. 121090, 2024.
[27] Q. Lai, L. Yang, G. Hu, Z.-H. Guan and H. H.-C. Iu, "Constructing Multiscroll Memristive Neural Network with Local Activity Memristor and Application in Image Encryption," IEEE Transactions on Cybernetics, vol. 54, no. 7, pp. 4039-4048, 2024.
[28] Q. Lai, L. Yang and G. Chen, "Design and Performance Analysis of Discrete Memristive Hyperchaotic Systems with Stuffed Cube Attractors and Ultraboosting Behaviors," IEEE Transactions on Industrial Electronics, vol. 71, no. 7, pp. 7819-7828, 2023.
[29] P. Liu, X. Wang, X. Zhao and S. Unar, "Target-based Image Encryption *via* Infinite Interval Chaotic System with Ill-conditioned Parameter and 3DBDM," Expert Systems with Applications, vol. 232, p. 120811, 2023.
[30] P. Liu, X. Wang and Y. Su, "Image Encryption *via* Complementary Embedding Algorithm and New Spatiotemporal Chaotic System," IEEE Transactions on Circuits and Systems for Video Technology, vol. 33, pp. 2506-2519, 2022.
[31] X. Wang and P. Liu, "A New Full Chaos Coupled Mapping Lattice and Its Application in Privacy Image Encryption," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 69, pp. 1291-1301, 2021.
[32] P. Liu, X. Wang, Y. Su, H. Liu and S. Unar, "Globally Coupled Private Image Encryption Algorithm Based on Infinite Interval Spatiotemporal Chaotic System," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 70, pp. 2511-2522, 2023.
[33] Q. Lai and Y. Liu, "A Cross-channel Color Image Encryption Algorithm Using Two-dimensional Hyperchaotic Map," Expert Systems with Applications, vol. 223, p. 119923, 2023.
[34] R. B. Naik and U. Singh, "A Review on Applications of Chaotic Maps in Pseudo-random Number Generators and Encryption," Annals of Data Science, vol. 11, pp. 25-50, 2024.
[35] C. Li, G. Luo, K. Qin and C. Li, "An Image Encryption Scheme Based on Chaotic Tent Map," Nonlinear Dynamics, vol. 87, pp. 127-133, 2017.
[36] X. Wang and C. Jin, "Image Encryption Using Game of Life Permutation and PWLCM Chaotic System," Optics Communications, vol. 285, pp. 412-417, 2012.
[37] I. I. Cisse, H. Kim and T. Ha, "A Rule of Seven in Watson-Crick Base-pairing of Mismatched Sequences," Nature Structural & Molecular Biology, vol. 19, pp. 623-627, 2012.
[38] R. Enayatifar, F. G. Guimarães and P. Siarry, "Index-based Permutation-diffusion in Multiple-image Encryption Using DNA Sequence," Optics and Lasers in Engineering, vol. 115, pp. 131-140, 2019.
[39] L. Liu, Y. Lei and D. Wang, "A Fast Chaotic Image Encryption Scheme with Simultaneous Permutation-Diffusion Operation," IEEE Access, vol. 8, pp. 27361-27374, 2020.
[40] Y. Wu, J. P. Noonan and S. Agaian, "NPCR and UACI Randomness Tests for Image Encryption," Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), vol. 1, pp. 31-38, 2011.
[41] Y. Qobbi, A. Jarjar, M. Essaid and A. Benazzi, "Image Encryption Algorithm Based on Genetic Operations and Chaotic DNA Encoding," Soft Computing, vol. 26, pp. 5823-5832, 2022.
[42] X. Chai, Z. Gan, K. Yang, Y. Chen and X. Liu, "An Image Encryption Algorithm Based on the Memristive Hyperchaotic System, Cellular Automata and DNA Sequence Operations," Signal Processing: Image Communication, vol. 52, pp. 6-19, 2017.

ملخص البحث:

تقدّم هذه الورقة تقنيةً لتشفير الصُّور بناءً على خرائط فوضى متعدّدة أحادية البُعد مع ترميز DNA. وتستخدم الطريقة المقترحة ثلاث خرائط فوضى أحادية البُعد، هي الخريطة اللوجستية، وخريطة الخيمة، وخريطة "قطعة - قطعة" عدّة مرّات لتوليد ثمانية عشر تتابعاً عشوائياً بقيم ابتدائية مُختلفة ومتغيرات مُختلفة. ولتشفير الصُّور، تُستخدم العناصر الثّنائية من التّتابُعات المتنوّعة لخرائط الفوضى لتغيير شدّة إضاءة النُّقَط في الصّورة المزمع تشْفيرها في عملية الانتشار. ويستخدم ترميز DNA من خلال الاختيار العشوائي للقواعد والعمليات الخاصّة بكلّ نقطة من نُقَط الصّورة.

وقد جرى تقييم التّقنية المقترحة باستخدام العديد من الصُّور المعيارية، وذلك بناءً على قياس عددٍ من معايير الأداء. وقد برهنت نتائج التّقييم على توفُّر أمْن المعلومات في الطّريقة المقترحة وقدرتها على مقاومة الهجمات.