entropy

MDPI

Article

A Bijective Image Encryption System Based on Hybrid Chaotic Map Diffusion and DNA Confusion

Dalia H. ElKamchouchi [1,2], Heba G. Mohamed [2,3,*] and Karim H. Moussa [4]

[1] Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh 11671, Saudi Arabia; dhelkamchouchi@pnu.edu.sa
[2] Electrical Department, College of Engineering, Alexandria Higher Institute of Engineering and Technology, Alexandria 21421, Egypt
[3] Electrical Department, College of Engineering, Princess Nourah Bint Abdulrahman University, Riyadh 11671, Saudi Arabia
[4] Electrical Department, College of Engineering, Horus University-Egypt, New Damietta 34518, Egypt; Khassan@horus.edu.eg
* Correspondence: hegmohamed@pnu.edu.sa

Received: 31 December 2019; Accepted: 2 February 2020; Published: 5 February 2020

Abstract: Modern multimedia communications technology requirements have raised security standards, which allows for enormous development in security standards. This article presents an innovative symmetric cryptosystem that depends on the hybrid chaotic Lorenz diffusion stage and DNA confusion stage. It involves two identical encryption and decryption algorithms, which simplifies the implementation of transmitting and receiving schemes of images securely as a bijective system. Both schemes utilize two distinctive non-consecutive chaotic diffusion stages and one DNA scrambling stage in between. The generation of the coded secret bit stream employs a hybrid chaotic system, which is employed to encrypt or decrypt the transmitted image and is utilized in the diffusion process to dissipate the redundancy in the original transmitted image statistics. The transmitted image is divided into eight scrambled matrices according to the position of the pixel in every splitting matrix. Each binary matrix is converted using a different conversion rule in the Watson–Crick rules. The DNA confusion stage is applied to increase the complexity of the correlation between the transmitted image and the utilized key. These stages allow the proposed image encryption scheme to be more robust against chosen/known plaintext attacks, differential attacks, cipher image attacks, and information entropy. The system was revealed to be more sensitive against minimal change in the generated secret key. The analysis proves that the system has superior statistical properties, bulkier key space, better plain text sensitivity, and improved key sensitivity compared with former schemes.

Keywords: hybrid chaotic; image; encryption; decryption; secured; communications; DNA

1. Introduction

Securing multimedia communications is a very important process in modern communication networks [1–5]. Recently, various researches have been dedicated their efforts to developing several schemes to fortify personal digital images. Digital images have many discriminative properties, for instance a wide spectrum and high correlation within the neighboring pixels. These properties make some conventional data encryption schemes not convenient for securing the processing of such information. Therefore, new schemes and approaches, such as deoxyribonucleic acid (DNA) [6–8] and chaotic maps [9,10] have been utilized in modern digital image safeguarding schemes. These approaches help to improve robustness against chosen/known plaintext attacks, enriched statistical properties, enhanced key space, amended plain text sensitivity, and upgraded key sensitivity than earlier schemes.

In [11], Qiang et al. introduced a scheme that depended on a DNA series matrix and chaos using dual logistic maps to execute a pair process to the DNA sequences. Following [12], Zhang et al. suggested a new proposal that encoded the plaintext into American Standard Code for Information Interchange (ASCII) code and then converted it into DNA sequential data which will be combined using Exclusive OR (XOR) operation and chaotic map. Subsequently, in [13], Wei et al. developed a new image encryption process reliant on DNA, chaotic images combination, and utilized hamming distance to generate a robust crypto-keys. Then in [14], Rasul et al. recommended an encryption system with the aid of chaos function accompanied by a modified genetic algorithm, and DNA structure is employed for more security. Liu et al. [15] proposed an algorithm depending on a DNA rule merged with chaotic map. In addition, they constructed a cipher procedure based on a one-time encryption key and the chaotic maps to improve the safety and the dynamic deprivation of the proposed procedure, where the primary conditions are created by the MD5 of mouse positions. Later in 2014, Yushu et al. [16] examined the role of image fusion, which depends on crypto-analysis for the encryption method and hiding the information using DNA classification combined with the chaotic map for covering the information [17]. In 2015, Zhang et al. proposed that an image cryptosystem depends on the lookup table concept. They built a different cipher for a digital image cryptosystem that depends on the Latin square and chaos theories [18]. Following in 2017, an efficient digital image encryption process utilizing adaptive rearrangement diffusion and an arbitrary DNA coding is presented [19]. Haider et al. in 2017 [20] proposed a different hybrid encryption algorithm that employs triangular scrambling where DNA mapping and the chaotic map was utilized to increase the security of the scheme. These articles have no robustness against noise, and their conclusions appeared to have a relatively small local and global entropy of the encoded image. On the other hand, the number of pixel change-rates (NPCRs) and the unified average changing intensity (UACI) of the resulted cipher image is far off from the proofed theoretical values, which means that these procedures are not receptive enough to small variations of the input image.

A perfect cryptosystem must satisfy some performance analysis such as large key space, sensitivity to slight change in the secret key, and nearly no correlation between two consecutive adjacent pixels [21]. In 2019, Chengqing Li et al. [22] solving scenario-oriented image security problems by introducing an algorithm with new technologies. In the same year, Zhongyun et al. proposed a cryptosystem that depends on the principles of the Josephus problem and the filtering tools. The algorithm utilizes a standard diffusion and confusion configuration [23]. In [24], a new color image scheme with energetic DNA and a 4D hyperchaotic system is proposed that satisfies the above requirements.

In this article, a new secured encryption algorithm is presented to encrypt an image utilizing an identical encryption and decryption schemes to improve the performance and the security analysis by employing a genome scrambling stage that depends on the DNA mutation process to be robust against several attacks. The plain image is divided into eight scrambled matrices according to the position of the pixel in every splitting matrix. Then, each binary matrix of the eight scrambled matrices is converted using a different conversion rule in the Watson–Crick rules. For example, we scrambled the first matrix with rule 1, the second matrix with rule 2, and so on. This mutation process increases the complexity of the relationship between the transmitted image and the utilized key and allows the proposed encryption algorithm to be more robust against chosen/known plaintext attacks.

The presented algorithm is given in an accurate mathematical language with no exceptional elements and tested against the list given in [25]. It is a bijective algorithm, and its key space is evaluated and tested. The two diffusion processes are presented in mathematical prepositions and the DNA diffusion stage is well defined with numerical examples. The procedure follows Kerckhoffs' principles, as it does not comprehend any stealthy factors except for the key. It also follows Shannon's two primitive proposes as it contains two non-consecutive diffusion stages employing the hybrid chaotic map and one confusion stage between them via DNA. From the numerical analysis, it passes many statistical and randomness tests such as histogram analysis, NPCR, UACI, and various correlation tests, and its scores are better than previously presented schemes in most of the tests. The proposed

encryption and decryption are more robust against brute force, differential cipher images, and entropy attacks than previous schemes. It has a bigger key space and it is more sensitive to minimal change in the chosen secret key than former techniques.

The remainder of the article is structured as follows. Section 2 details the related background for the employed chaotic map and the DNA cryptography approach. Following is the explanation and discussion of the proposed encryption/decryption procedure in Section 3. Section 4 gives the numerical simulation results, while the security performance of the presented scheme is analyzed in Section 5. Finally, Section 6 presents the whole presented work and conclusions.

2. Related Background

2.1. Employed Chaotic System

Chaotic cryptography is an essential tool to develop fortified encryption schemes that improve the security analysis performance of cryptographic algorithms where the distinct chaotic assets such as the nature of determinism, random performance, nonlinear conversion, sensitivity to preliminary conditions, and structure parameters have approved "chaos" as an encouraging substitute for conventional and public key cryptographic algorithms. Since Matthews employed chaos into cryptology for the first time in 1989 [26], many chaotic systems have been employed in image encryption [27–29]. In 1963, Lorenz [30] discovered the three-dimensional (3D) independent chaotic system. Other chaotic systems introduced in succession include the Chen-Lu chaos system [31] and Liu chaos system [32]. Both employed the 3D chaos system, which provides only a single positive Lyapunov exponent (PLE). However, the chaotic system with multiple PLE improves the vibrant behaviors of such a structure, making it more complicated and difficult to predict. Recently, the adaptive control methods for the four-dimensional (4D) chaotic systems were introduced in [33,34], which are stiffer to expect than previous systems. In different chaotic image encryption schemes, the chaotic map initial values or parameters are employed as private keys, and the iterations of chaotic systems are operated as a producer of pseudo-random sequences that convert original images into noise-like encrypted cipher images. These systems behave as non-periodic in state space due to their sensitivity to the chaotic parameters and chaos initial conditions. Wang et al. presented the perceptual conception of artificial neural network into the chaotic system and proposed that an image chaotic encryption algorithm relied on perceptron [35]. In addition, they [36,37] have reported the hyper-chaos Lorenz system as

$$\begin{aligned} \frac{dx}{dt} &= a(y-x)+w, \\ \frac{dy}{dt} &= cx-y-xz, \\ \frac{dz}{dt} &= xy-bz, \\ \frac{dw}{dt} &= -rw-yz, \end{aligned} \tag{1}$$

where $b > 0$, $a > 0$, $r > 0$, and $c > 0$ are the constraints of the Lorenz hyper-chaos structure which determine the chaotic behaviors and bifurcation of the hyper-chaos Lorenz map. When $b = 8/3$, $a = 10$, $c = 28$, and $r = 1$, the system behaves in a hyper-chaotic manner. The actual ranges of primary variables are as follows: $w_0 \in (-250,\ 250)$, $y_0 \in (-40,\ 40)$, $z_0 \in (1,\ 81)$ and $x_0 \in (-40,\ 40)$, which are always considered as part of the chosen secret key. The step size is equal to 2×10^{-3} when digitizing (1) by the Runge Kutta method in the fourth order [38].

2.2. DNA Cryptography

DNA cryptography is a promptly emerging technology that depends on theories of DNA structures and is known as a promising technology for unbreakable robust algorithms. It is defined as hiding

data in terms of DNA sequences and is used in transmitting or storing data. The DNA is the genetic material in living organisms, which includes all the essential information to construct and sustain it. The strands of DNA are long polymers of several units named nucleotides. The nitrogen base consists of quad nucleic acids: Adenine (A), Cytosine (C), Guanine (G), and Thymine (T). The DNA has a dual helix arrangement formed by coupling dual chains of nucleic acids all together. Every chain is a complement to the other one; T and A are paired duos, while C and G are alternative paired duos. The 0 and 1 are a complement pair in a binary operation; thus, 0 0 and 1 1 are a complement pair, and 0 1 and 1 0 are another complement pair. For example, the A, T, G, and C nucleic acid bases can be encoded as 0 0, 1 1, 1 0, and 0 1, correspondingly. Table 1 indicates the utilized DNA eight possible encoding guidelines that satisfy complementary rubrics [39].

Table 1. Watson–Crick rubrics.

	A	T	C	G
R 01	0 0	1 1	1 0	0 1
R 02	0 0	1 1	0 1	1 0
R 03	1 1	0 0	1 0	0 1
R 04	1 1	0 0	0 1	1 0
R 05	1 0	0 1	0 0	1 1
R 06	0 1	1 0	0 0	1 1
R 07	1 0	0 1	1 1	0 0
R 08	0 1	1 0	1 1	0 0

2.3. Traditional Chaotic Encryption System

The traditional chaotic image encryption algorithm depends on x repeated confusion stages and y repeated diffusion stages, and both of these stages are reiterated n periods to generate the ciphered image from the original plain one, as shown in Figure 1a. To recuperate the plain image from the ciphered one, the chaotic decryption algorithm is applied and it is the contrary of the encryption algorithm presented in Figure 1b.

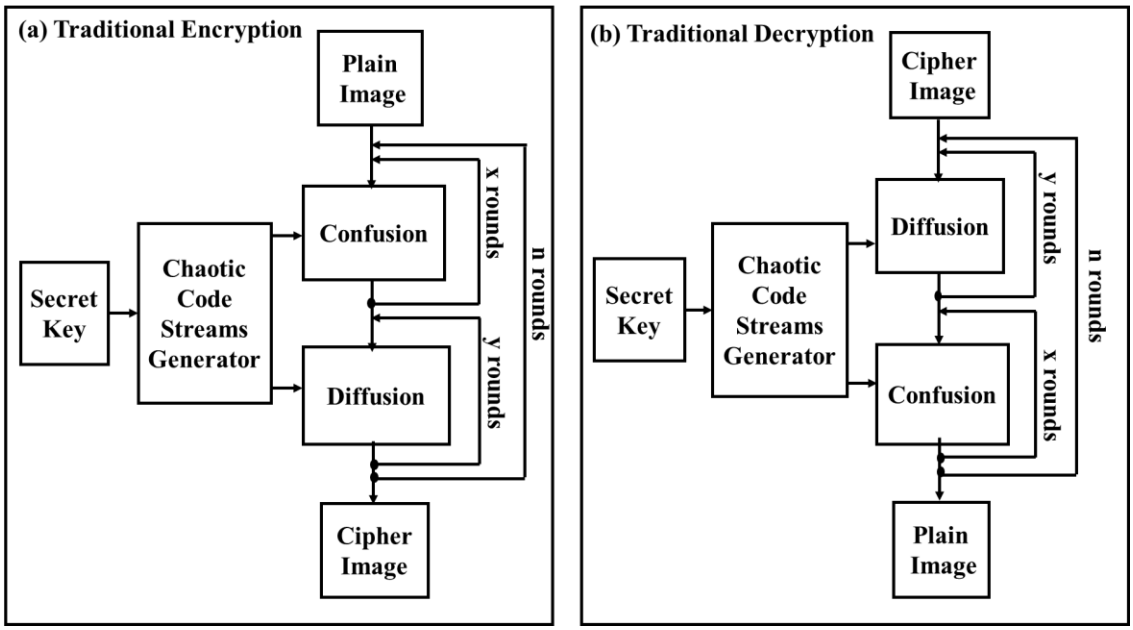


Figure 1. An example of image securing scheme that depends on a chaotic map: (**a**) traditional encryption, (**b**) traditional decryption.

3. Proposed Image Cryptosystem

Let **P** represent the originally transmitted image, which is exemplified by a matrix with size $W \times H$ where W and H are the size of the columns and rows of the matrix **P**, respectively. Each element of the grayscale original image is signified by 8-bit i.e., 256 intensity levels. The presented encryption scheme is illustrated in Figure 2. Its private key is defined as $S = \{x_0,\ y_0,\ z_0,\ w_0,\ a_1,\ a_2\}$, where $y_0, x_0,\ z_0$, and w_0 are the initial parameters of the 4D hyperchaotic system, whose value ranges are $y_0 \in (-40,\ 40)$, $x_0 \in (-40,\ 40)$, $w_0 \in (-250,\ 250)$, and $z_0 \in (1,\ 81)$ where a_1 and a_2 are 8-bit random numbers selected by the user. The step size of $x_0,\ y_0,\ z_0$ is 10^{-13}, while the step size of w_0 is 10^{-12}. In the encryption process, there are dual pseudo-random matrices **X** and **Y** that are produced by repeating the hyperchaotic system to encrypt the original image. In the decryption algorithm, the pseudorandom matrices are produced by the indistinguishable methods utilized in the encryption algorithm; then, these matrices are rotated a half cycle to generate new different matrices designated by $\mathbf{Y_{New}}$ and $\mathbf{X_{New}}$.

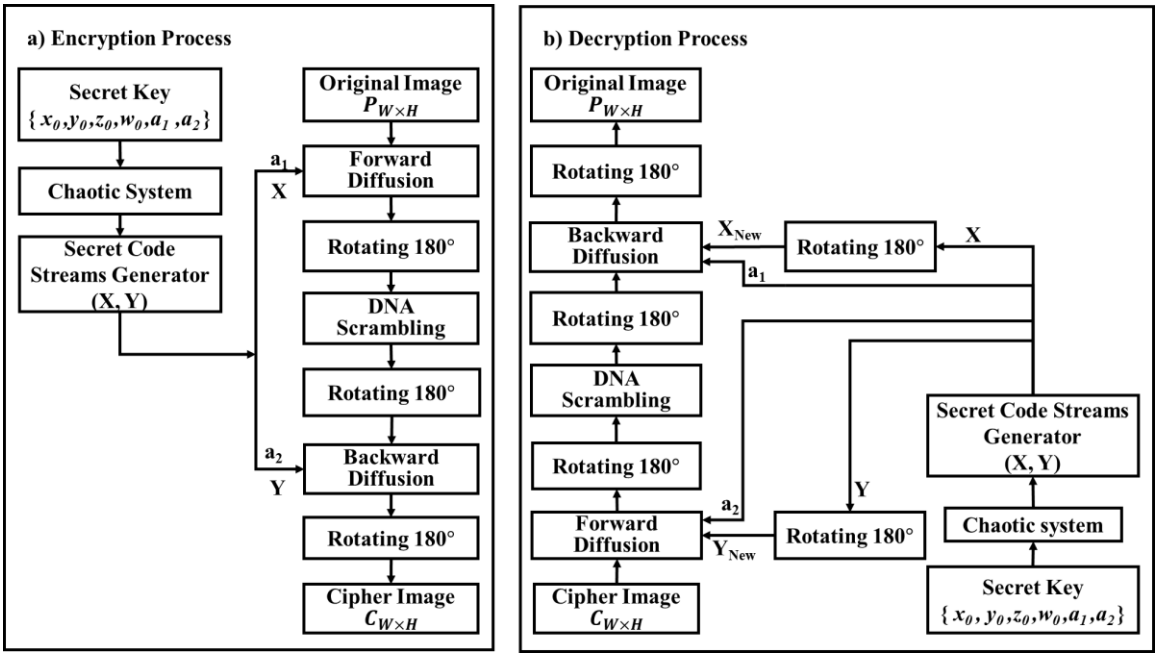


Figure 2. The proposed securing system for images: (**a**) encryption process, (**b**) decryption process.

In the presented scheme, the encryption and decryption algorithm are the same, both counting the exact identical stages of the forward image diffusion stage, circling the resulting image by 180 degrees, scrambling the outcome with the DNA confusion stage, rotating the consequence by 180 degrees, utilizing the backward image diffusion, and rotating it by 180 degrees again. The algorithm comprises four main stages, as portrayed in the subsequent sections.

3.1. Secret Code Stream Generator

There are two pseudo-random matrices are generated using the hyperchaotic Lorenz system given by Equation (1), represented by **X** and **Y,** and both of the size $W \times H$. Iterate this equation beginning with the four initial values defined in the private key S for $a_1 + a_2$ times in order to avoid the ephemeral values of the hyperchaotic Lorenz system, and then resume iterating for $W \times H$ to get four pseudo-noise streams, which are designated by $\{x_i\}$, $\{y_i\}$, $\{z_i\}$, and $\{w_i\}$, $i = 1, 2, \cdots, W \times H$, separately. Generate the two matrices **X**, **Y** from the sequences $\{x_i\}$, $\{y_i\}$ by

$$\mathbf{X}(k,l) = Floor((x_{(k-1)\times H+l} + 500 \bmod 1) \times 10^{13}) \bmod 256, \quad (2)$$

$$\mathbf{Y}(k,l) = Floor((y_{(k-1)\times H+l} + 500\text{mod}1) \times 10^{13})\text{mod}256, \quad (3)$$

where *Floor(f)* yields the largest principle integer number not as much of *f*, and "+500" is used to translate any negative numbers to positive numbers. These two matrices are used for forward and backward diffusion in the encryption process. However, for the decryption procedure demonstrated in Figure 2b, new matrices $\mathbf{X_{New}}$ and $\mathbf{Y_{New}}$ are generated by spinning the novel matrices **X** and **Y** by 180 degrees, correspondingly. They are generated utilizing

$$\mathbf{X}_{New}(i,\ j) = \mathbf{X}(i,\ W+1-j),\ for\ i = 1 \ldots H,\ j = 1 \ldots W, \quad (4)$$

$$\mathbf{Y}_{New}(i,\ j) = \mathbf{Y}(i,\ W+1-j),\ for\ i = 1 \ldots H,\ j = 1 \ldots W. \quad (5)$$

3.2. Forward Diffusion Stage

In this stage, the algorithm obtains a new matrix denoted by **Q** by applying XOR (⊕) operation between the two matrices of the original image **P** elements and the pseudo-random matrix X elements according to the subsequent formulas

$$\mathbf{Q}(1,1) = \mathbf{P}(1,1) \oplus \mathbf{X}(1,1) \oplus a_1 \quad (6)$$

$$\mathbf{Q}(1,j) = \mathbf{P}(1,j) \oplus \mathbf{X}(1,j) \oplus \mathbf{Q}(1,j-1),\ for\ j = 2,3,\ldots,W \quad (7)$$

$$\mathbf{Q}(i,\ 1) = \mathbf{P}(i,\ 1) \oplus \mathbf{X}(i,\ 1) \oplus \mathbf{Q}(i-1,\ 1),\ for\ i = 2,3,\ldots,H \quad (8)$$

$$\begin{gathered}\mathbf{Q}(i,\ j) = \mathbf{P}(i,\ j) \oplus \mathbf{X}(i,\ j) \oplus \mathbf{Q}(i-1,\ j)\ \oplus\ \mathbf{Q}(i,\ j-1) \oplus \mathbf{Q}(i-1,\ j-1), \\ for\ i = 2,3,\ldots,H,\ and\ j = 2,3,\ldots,W\end{gathered} \quad (9)$$

Then, we rotate matrix **Q** by 180 degrees to attain a matrix designated by **A** using

$$\mathbf{A}(i,\ j) = \mathbf{Q}(i,\ W+1-j),\ for\ i = 1,2...H,\ and\ j = 1,2...W \quad (10)$$

which is the input to the next DNA scrambling stage described in the following subsection.

3.3. DNA Mutation Scrambling Stage

To improve the fight of the encryption process against chosen/known plaintext attacks, we introduce a new scrambling stage that depends on the DNA mutation process. Utilizing this stage improves the complex relative between the plain image, the encrypted one, and the utilized key. A small difference in the original image or key will affect a major divergence in the encrypted image with assent. The steps to get the scrambled matrix are as follows.

1. Divide matrix **A** into two equally matrices by selecting the even columns together and create the first matrix $\mathbf{A}_{\mathrm{E}}$; then, select the odd columns and create the second matrix $\mathbf{A}_{\mathrm{O}}$. Both matrices have the size of $H \times W/2$.
2. Generate two new matrices $\mathbf{A}_{\mathrm{OE}}$ and $\mathbf{A}_{\mathrm{OO}}$ from $\mathbf{A}_{\mathrm{O}}$ by selecting the even rows together and the odd rows together. Repeat for $\mathbf{A}_{\mathrm{E}}$ to generate $\mathbf{A}_{\mathrm{EE}}$, $\mathbf{A}_{\mathrm{EO}}$ matrices. The four matrices have the size $W/2 \times H/2$.
3. Repeat Step 2 to generate eight new matrices $\mathbf{A}_{\mathrm{EEE}}$, $\mathbf{A}_{\mathrm{EEO}}$, $\mathbf{A}_{\mathrm{EOE}}$, $\mathbf{A}_{\mathrm{EOO}}$, $\mathbf{A}_{\mathrm{OEE}}$, $\mathbf{A}_{\mathrm{OEO}}$, $\mathbf{A}_{\mathrm{OOE}}$ each of size $W/2 \times H/4$. Figure 3 illustrates the output of every step applied to matrix **A** with a size of 10×10.
4. Convert each pixel into the eight matrices to 8-bit binary values, each of size $4W \times H/4$. For example, the first three elements in matrix $\mathrm{A}_{\mathrm{OOO}}$ are '31', '33', and '35', which will be converted to '00011111', '00100001', and '00100011'.
5. Encode every binary element in the eight matrices with the DNA encoding rules. Each binary matrix is encoded using a different conversion rule, as shown in Table 1. For instance, rule 1 is used

to encode the first matrix, rule 2 is used for the second matrix, etc. The outputs of this stage are eight DNA encoded matrices with the size of $2W \times H/4$. For illustration, '00011111', '00100001', and '00100011' will be encoded with Rule 8 to 'GACC', 'GTGA', and 'GTGC', respectively.

6. Mutate the existing DNA pairs to their mutated values according to Table 2. For illustration, the 'GACC', 'GTGA', and 'GTGC' will be mutated to 'CAGC', 'CTCA', and 'CTCC', respectively.
7. Convert the mutated DNA values to their corresponding binary values according to Table 1. For example, 'CAGC', 'CTCA', and 'CTCC' will be mutated to '11010011', '11101101', and '11101111', correspondingly.
8. Concert the binary values to their decimal values in the range from '0' to '255'. For instance, the '11010011', '11101101', and '11101111' will be converted to 211, 237, and 239, respectively.
9. Concatenate the eight matrices into one decimal matrix denoted by I of size $W \times H$ with the new confused values and rotated by 180 degrees to generate a matrix denoted by **B** fed to the next stage of backward diffusion.

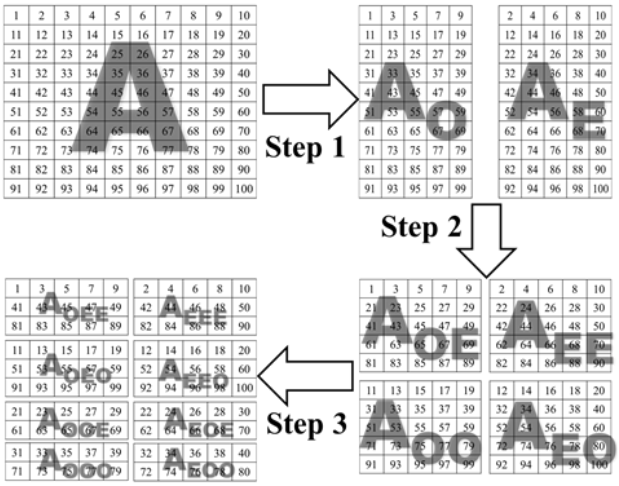


Figure 3. The effect of applying the first three steps of the DNA mutation scrambling stage on a 10×10 matrix.

Table 2. DNA mutation rules.

DNA	Mutate	DNA	Mutate	DNA	Mutate	DNA	Mutate
A A	T A	C A	G A	G A	C A	T A	A A
A C	T C	C C	G C	G C	C C	T C	A C
A G	T G	C G	G G	G G	C G	T G	A G
A T	T T	C T	G T	G T	C T	T T	A T

3.4. Backward Diffusion Stage

In the backward image diffusion stage, the matrix **B** is converted into a matrix signified by **E**, with the XOR process and the pseudo-noise matrix **Y** by

$$\mathbf{E}(H, W) = \mathbf{B}(H, W) \oplus \mathbf{Y}(H, W) \oplus a_1 \tag{11}$$

$$\mathbf{E}(H, j) = \mathbf{B}(H, j) \oplus \mathbf{Y}(H, j) \oplus \mathbf{B}(H, j+1), \ for\ j = W-1, \ldots, 1 \tag{12}$$

$$\mathbf{E}(i, W) = \mathbf{B}(i, W) \oplus \mathbf{Y}(i, W) \oplus \mathbf{B}(i+1, 1), \ for\ i = H-1, \ldots, 1 \tag{13}$$

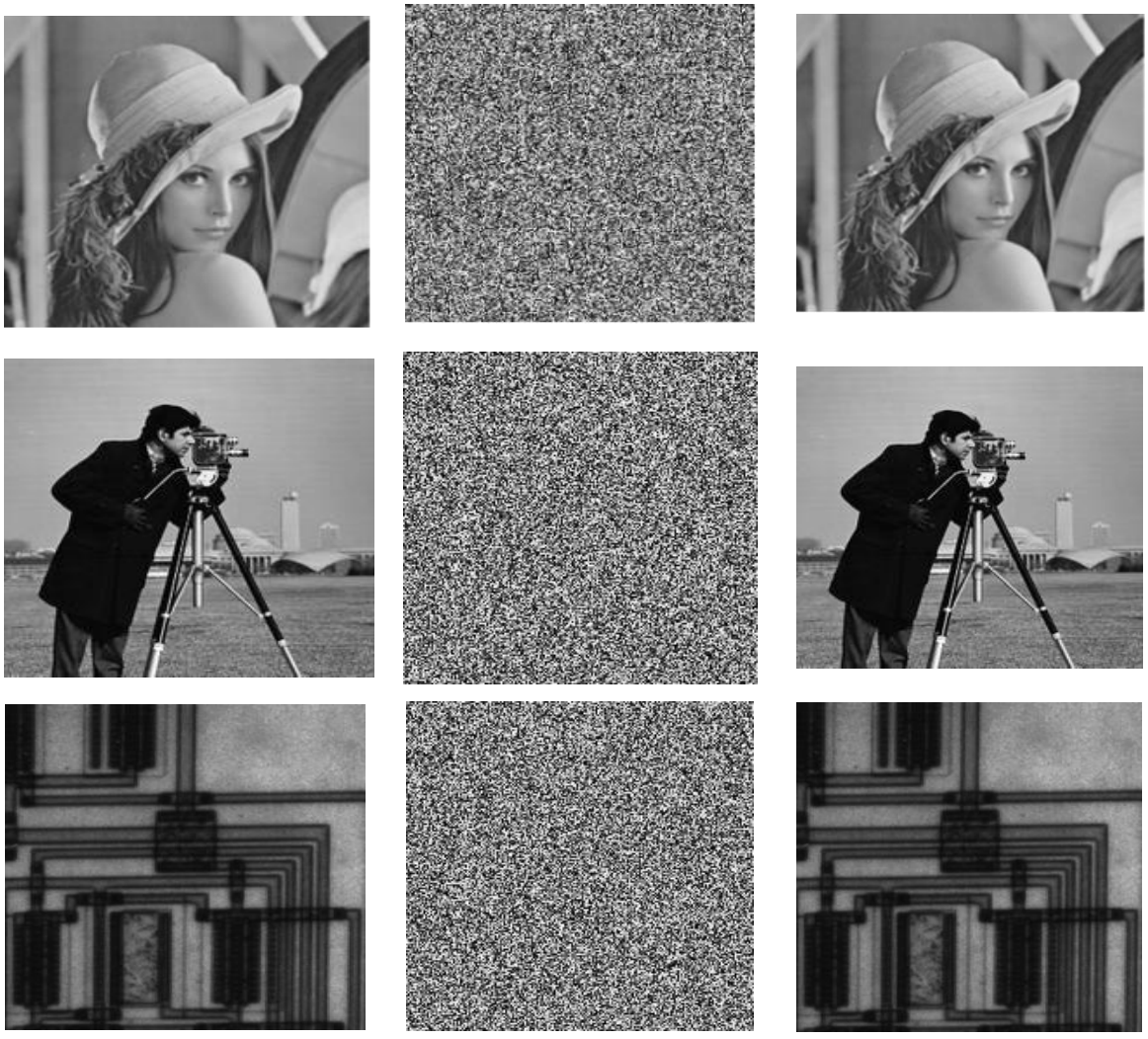
$$\begin{gathered}\mathbf{E}(i, j) = \mathbf{B}(i, j) \oplus \mathbf{Y}(i, j) \oplus \mathbf{B}(i+1, j) \oplus \mathbf{B}(i, j+1) \oplus \mathbf{B}(i+1, j+1), \\ for\ i = H-1, \ \ldots, 1, \ for\ j = W-1\ , \ \ldots, 1\end{gathered} \tag{14}$$

Turn around the matrix **E** by 180 degrees to get a ciphered image matrix symbolized by **C** using

$$\mathbf{C}(i,j) = \mathbf{E}(i, W+1-j), \ for\ i = 1, 2...H, \text{and } j = 1, 2...W \tag{15}$$

4. Simulation Effects

The algorithm is carried out on the Lena, Cameraman, and Circuit images. 'Mathematica 11' software is used to apply the proposed symmetric encryption and decryption scheme. The utilized secret symmetric key is set to $S = \{3.3133, 12.0546, 40.8879, -34.5677, 35, 201\}$, which is employed in each encryption and decryption algorithm, and the used plain images with size 200×200 pixels are illustrated in Figure 4a. The corresponding cipher image is generated using the encryption algorithm, and it is shown in Figure 4b. Then, we decrypted the cipher image Figure 4b with the correct secret key S to get the perfectly reconstructed image, as shown in Figure 4c. The histograms of the plain images and the corresponding generated cipher images are shown in Figure 5a,b, respectively. It's clear from Figures 4 and 5 that the pattern of the cipher image is noise-like and is not related to the original plain image. The recovered image is a perfectly reconstructed version of the original plain image, while the histogram of the cipher image is almost flat, which ensures that no statistical information from the original image can be discovered consequently.



(**a**) (**b**) (**c**)

Figure 4. Simulation results. (**a**) plain images, (**b**) Generated cipher images of (a), (**c**) Recovered image from (b).

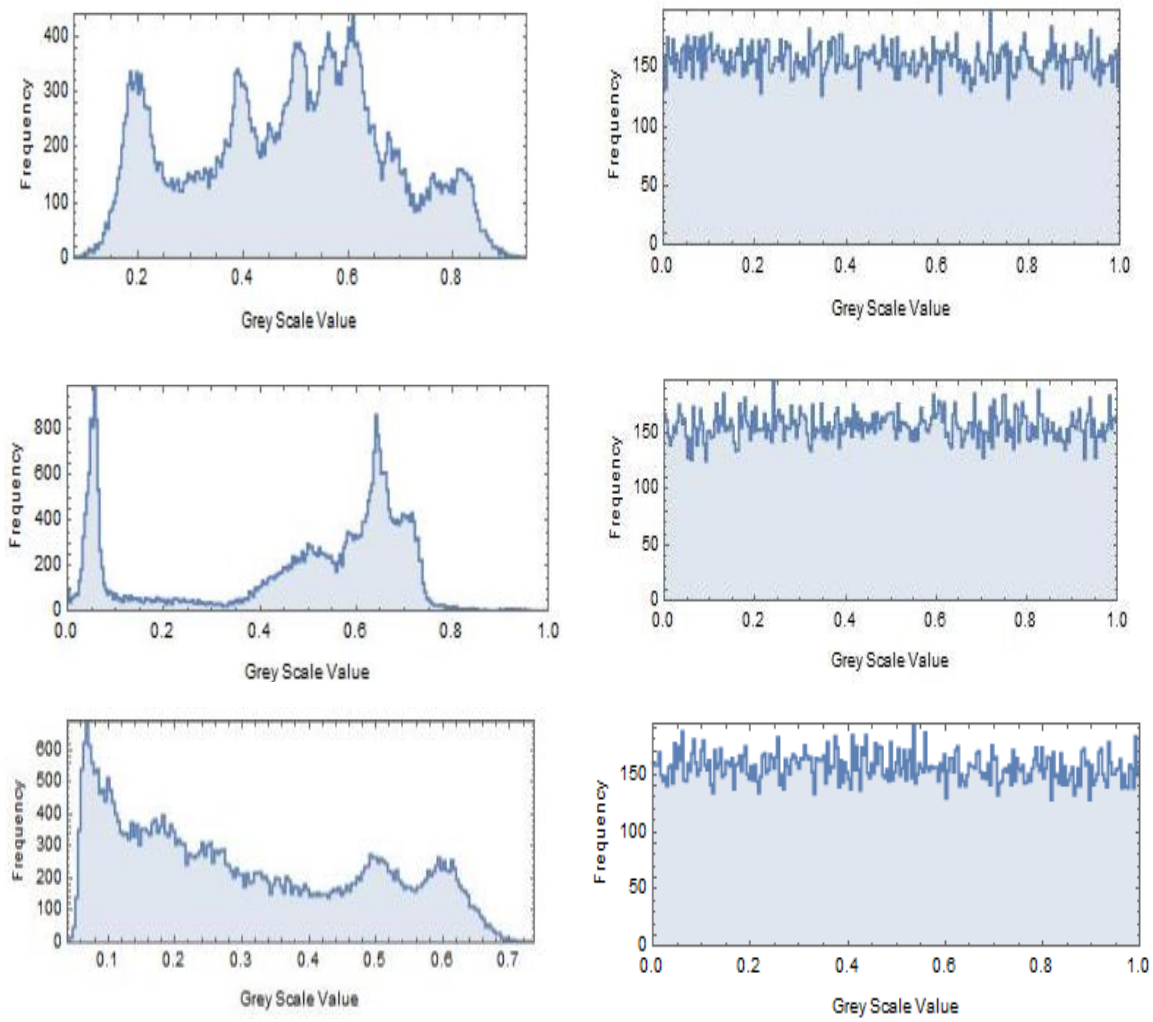


Figure 5. Histograms analysis. (**a**) Histograms of plain images, (**b**) Histograms of cipher images.

5. Performance and Security Analysis

5.1. Key Space

The key space is usually designed to be large enough to prevent an opponent from using a brute-force attack to find the key used to encrypt the plain images. In this article, the key space of the presented cryptosystem consisted of the initial conditions of the hyperchaotic Lorenz system x_0, y_0, z_0, w_0, a_1 and a_2. The value ranges were $x_0 \in (-40, 40)$, $y_0 \in (-40, 40)$, and $z_0 \in (1, 80)$ each with a step size of 10^{-13}, while the value range of $w_0 \in (-250, 250)$ had a step size of 10^{-12}. a_1 and a_2 are two 8-bit random numbers whose value ranges are [0,255] with a single step size. Therefore, the key space of the proposed algorithm is 1.6777×10^{64}, and that space is large enough to resist brute-force attacks. It would take 2.03451×10^{21} days to crack the systems if 17 billion attempts are tried hourly using a very high-performance machine.

5.2. Statistical Attacks Analysis

The encryption process should have the ability to struggle against statistical confrontation, and this can be assessed by histogram analysis and a chi-square test.

5.2.1. Image Histogram Analysis

The histograms of the original images of Lena, Cameraman, and Circuit shown in Figure 5a are non-uniform. The characteristic peak is clear and most of the images' information can be obtained effortlessly. On the other hand, Figure 5b displays the histograms of the cipher images with a nearly uniform statistical distribution. These two aspects prove the statement of resisting the statistical attacks and the cipher images attack in our proposed encryption process. The correlation among nearby pixels signifies the randomness of the encrypted resulted gray levels. Now, we discuss the correlation in the horizontal, the vertical and the diagonal directions. Choose a random N duos of nearby pixels, and (x_i, y_i) are the concerned pixel values of the i-th pair ($i = 1, 2, \ldots, N$). After that, the correlation coefficient r can be computed by

$$r = \frac{\sum_{i=1}^{N}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{N}(x_i - \overline{x})^2}\sqrt{\sum_{i=1}^{N}(y_i - \overline{y})^2}} \tag{16}$$

where r is the sample size, (x_i, y_i) are the distinct sample points with index I, $\overline{x} = 1/N\sum_{i=1}^{N} x_i$ is the sample mean, and similarly for $\overline{y}$. Now, let $N = 2000$, and the resulted different correlation coefficients of the cipher image and original image are recorded in Table 3. The correlation in the horizontal course for each image is shown in Figure 6. The correlation of plain images is high and close to 1. In contrast, the correlation of the cipher images is low and near to 0, which indicates that encrypted pixels are valued and distributed randomly in the encrypted images.

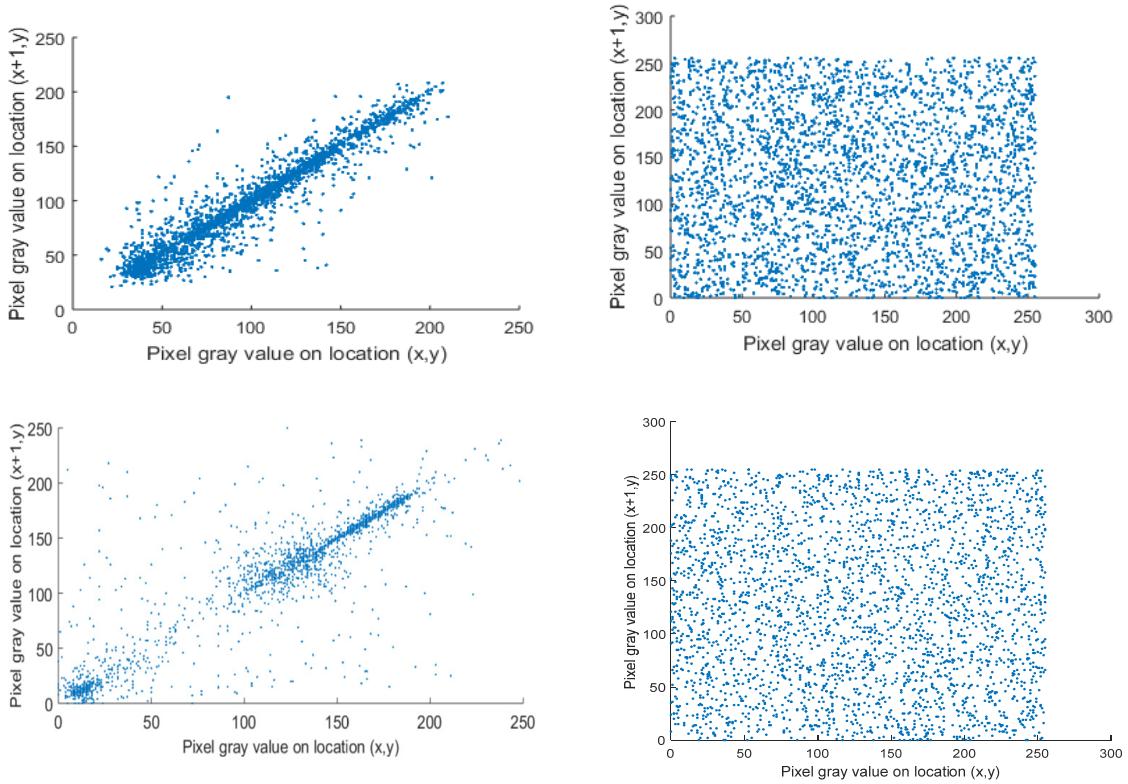
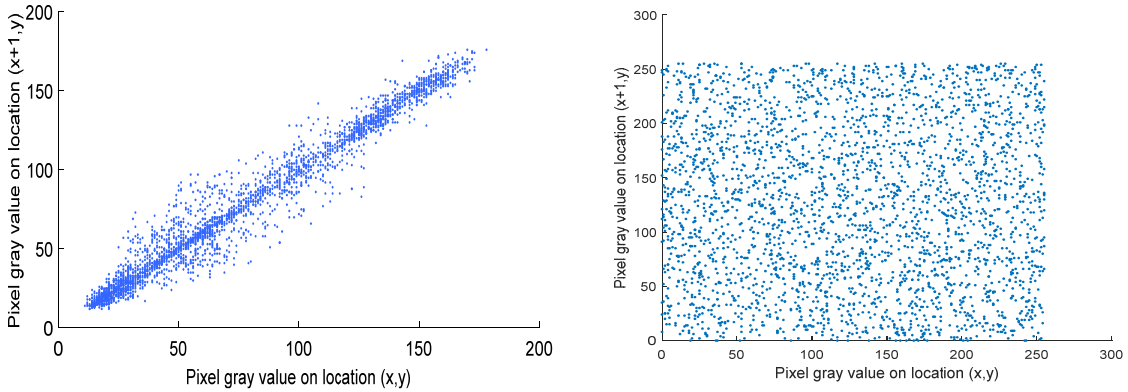


Figure 6. *Cont.*



(**a**) (**b**)

Figure 6. Correlation analysis plot. (**a**) Horizontal direction correlation for plain images Lena, Cameraman, and Circuit, (**b**) Horizontal correlation for their cipher images respectively.

Table 3. Calculated correlation coefficients.

Correlation	Plain Image			Cipher Image		
	Horizontal	**Vertical**	**Diagonal**	**Horizontal**	**Vertical**	**Diagonal**
Lena	0.9650	0.9144	0.9056	0.0082	−0.0032	−0.0025
Cameraman	0.9560	0.9140	0.9077	0.0074	−0.0029	−0.0019
Circuit	0.9580	0.9230	0.9118	0.0078	−0.0034	−0.0021

5.2.2. Chi-Square Test

To proof the uniform distribution of the resulted ciphered images in a more precise manner, we perform the chi-square test to show that the cipher image is a uniform distribution. The chi-square test is described

$$\chi^2 = \sum_{i=0}^{L-1} \frac{(o_i - e_i)^2}{e_i} \tag{17}$$

where L is the number of pixel grayscale levels, o_i is the occurrence frequency of each gray level (0–255) in the histogram of the resulted encrypted images, and e_i is the probable frequency of the uniform distribution. The uniform distribution of the histogram is assessed with the aid of the chi-square χ^2 test. The null hypothesis is only accepted when the p-value is greater than the significance amount $s(s \in [0,1])$. Table 4 presents the chi-square score and their p-value for the histogram of the encrypted Lena, Cameraman, and Circuit images and the significance level amount of 0.05. The obtained score is smaller than χ^2_{th} (255, 0.05) = 293.247, while their p-value is larger than 0.05. Therefore, the null hypothesis is achieved, and the histogram of the encrypted images is uniformly distributed. Based on that, the presented encryption algorithm is strong against statistical attacks.

Table 4. Histogram chi-square test.

Image	χ^2 Test		
	Score	***p*-Value**	H_0
Lena	246.804687	0.6834	Accepted
Cameraman	246.817237	0.6670	Accepted
Circuit	246.794528	0.6754	Accepted

5.3. Key Sensitivity Analysis

To test the key sensitivity of a secret key, we can create a different secret key S_2 after the secret key $S = \{x_0, y_0, z_0, w_0, a_1, a_2\}$ by changing $\{a_1, a_2\}$ by 1 or any component of $\{x_0, y_0, z_0\}$ by 10^{-13} or w_0 by

10^{-12}. First, encrypt the plaint image **P** for the presented encryption system with the secret keys of S_1 and S_2 to get dual cipher images, symbolized by $\mathbf{C}_1$ and $\mathbf{C}_2$, correspondingly. Contrast $\mathbf{C}_1$ and $\mathbf{C}_2$ to get two gauges named $Diff_1$ and $Diff_2$ using [40]

$$Diff_1 = \left(\frac{1}{W \times H}\right)\sum_{i=1}^{W}\sum_{j=1}^{H}\left|Sign\left(\mathbf{C}_1(i,j) - \mathbf{C}_2(i,j)\right)\right| \times 100\% \tag{18}$$

$$Diff_2 = \left(\frac{1}{W \times H}\right)\sum_{i=1}^{W}\sum_{j=1}^{H}\frac{\left|\mathbf{C}_1(i,j) - \mathbf{C}_2(i,j)\right|}{256} \times 100\% \tag{19}$$

where $Sign(\cdot)$ is the sign role, and (W, H) are the width and height of the original image, correspondingly. Correspondingly, the hypothetical values for $Diff_1$ and $Diff_2$ in the case of dual arbitrary images are 99.6094% and 33.3328%.

Another way to assess the secret key sensitivity and secure the plain image $\mathbf{P}_1$ utilizing the secret key S_1 of the presented system to get the ciphered image **C**, and then decrypt the ciphered image **C** by the new secret key S_2 to retrieve the plain image signified by $\mathbf{P}_2$. Compare $\mathbf{P}_1$ and $\mathbf{P}_2$ to get $Diff_3$ and $Diff_4$ respectively, using [40]

$$Diff_3 = \left(\frac{1}{W \times H}\right)\sum_{i=1}^{W}\sum_{j=1}^{H}\left|Sign\left(\mathbf{P}_1(i,j) - \mathbf{P}_2(i,j)\right)\right| \times 100\% \tag{20}$$

$$Diff_4 = \left(\frac{1}{W \times H}\right)\sum_{i=1}^{W}\sum_{j=1}^{H}\frac{\left|\mathbf{P}_1(i,j) - \mathbf{P}_2(i,j)\right|}{256} \times 100\%. \tag{21}$$

Assume that the plain image denoted by $\mathbf{P}_1$ and another random image is denoted by $\mathbf{P}_2$; then, the hypothetical values of $Diff_3$ and $Diff_4$ are 99.6094% and 28.5059%, respectively [40]. To test the plaintext sensitivity, 100 trials are done for the Lena, Cameraman, and Circuit images and calculate the average values of $Diff_1$, $Diff_2$, $Diff_3$, and $Diff_4$. Table 5 shows that the calculated results of $Diff_1$, $Diff_2$, $Diff_3$, and $Diff_4$ are nearly equal to their hypothetical values; these values indicators are designating that the presented scheme is very sensitive to minimal alteration in the generated secret key.

Table 5. Key sensitivity tests results (%).

Theoretical Values	$Diff_1$ (99.6094)	$Diff_2$ (33.3328)	$Diff_3$ (99.6094)	$Diff_4$ (28.5059)
Lena	99.6225	33.3962	99.6250	28.3191
Cameraman	99.6122	33.3876	99.6299	28.3245
Circuit	66.6179	33.3471	99.6134	28.3770

5.4. Differential Attack

An opponent can get valuable information by altering several pixels of the plain image. The NPCR and UACI are usually employed to measure the resistance of the encrypted image against differential raids. We utilize the presented encryption scheme to encrypt $\mathbf{P}_1$ and $\mathbf{P}_2$ to get their corresponding cipher images denoted by $\mathbf{C}_1$ and $\mathbf{C}_2$ with the same secret key, where $\mathbf{P}_2$ (i, j) = [$\mathbf{P}_1$ (i, j) + 1] mod 256. Then, the NPCR and UACI are given by

$$\text{NPCR} = \frac{1}{W \times H}\sum_{i=1}^{W}\sum_{j=1}^{H}\left|Sign(\mathbf{C}_1(i,j) - \mathbf{C}_2(i,j))\right| \times 100\% \tag{22}$$

$$\text{UACI} = \frac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} \frac{\left| Sign(\mathbf{C}_1(i,j) - \mathbf{C}_2(i,j)) \right|}{256} \times 100\% \tag{23}$$

The theoretical values of NPCR and UACI for any two random images with 256 gray levels are 99.609% and 33.464%, respectively. The NPCR and UACI test outcomes are presented in Tables 6 and 7, respectively. If one bit of the input image is altered, the NPCR and UACI of traditional methods, in CCAES [41], CDCP [42], and CHC [43] are close to hypothetical values. DNA-based methods, C-DNA [44] and HC-DNA [45], have a better noise attack performance than the previous works. Furthermore, the values are compared against the critical values as in [46,47]. These demonstrate the capability of the proposed algorithm to stand for differential attacks. So, the presented cryptosystem attains high performance by getting NPCR values and UACI values near to their hypothetical values.

Table 6. Number of pixel change rat (NPCR) test analysis (%).

Algorithms	**NPCR (%)**	**NPCR Critical Values**		
		$N^*_{0.05}$ **99.5693%**	$N^*_{0.01}$ **99.5527%**	$N^*_{0.001}$ **99.5341%**
Proposed	99.6150	Successful	Successful	Successful
CCAES [41]	99.5697	Successful	Successful	Successful
CDCP [42]	100	Successful	Successful	Successful
CHC [43]	99.6605	Successful	Successful	Successful
C-DNA [44]	15.25×10^{-4}	NA	NA	NA
HC-DNA [45]	59.7406	NA	NA	NA

Table 7. Unified average changing intensity (UACI) test analysis (%).

Algorithms	**UACI (%)**	**UACI Critical Values**		
		$U^*_{\pm 0.05}$ **+33.2824% −33.6447%**	$U^*_{\pm 0.01}$ **+33.2255% −33.7016%**	$U^*_{\pm 0.001}$ **+33.1594% −33.7677%**
Proposed	33.4205	Successful	Successful	Successful
CCAES [41]	33.4767	Successful	Successful	Successful
CDCP [42]	33.5752	Successful	Successful	Successful
CHC [43]	33.4263	Successful	Successful	Successful
C-DNA [44]	8.97×10^{-6}	NA	NA	NA
HC-DNA [45]	25.0487	NA	NA	NA

5.5. Cipher Image Sensitivity Analysis

To measure the differential attacks based on ciphered image analysis, we obtain the cipher image $\mathbf{C}_1$ by encrypting the plain image $\mathbf{P}_1$ using the corresponding secret key S_1 Then, generate a new cipher image $\mathbf{C}_2$ from $\mathbf{C}_1$ by shifting the randomly selected pixel of the $\mathbf{C}_1(i,j)$ value by 1 where $\mathbf{C}_2(i,j) = [\mathbf{C}_1(i,j) + 1] \text{mod} 256$ for a selected pixel position (i,j) in a random manner. To analyze cipher image sensitivity firstly, decrypt the ciphered image $\mathbf{C}_2$ utilizing the presented algorithm with the secret key S_1 to get $\mathbf{P}_2$, which is the recovered image. Analyze the difference between the two recovered images $\mathbf{P}_1$ and $\mathbf{P}_2$ by using Equations (15) and (16) to calculate the values of $Diff_3$ and $Diff_4$. Secondly, change any element of the secret key S_1 to get new secret key S_2, and decrypt $\mathbf{C}_1$ and $\mathbf{C}_2$ by the proposed scheme with the new secret key S_2 to obtain their corresponding recovered images $\mathbf{P}_3$ and $\mathbf{P}_4$, correspondingly. Later, compute the indicators named $Diff_3$ and $Diff_4$ among $\mathbf{P}_3$ and $\mathbf{P}_4$. Finally, reiterate the overhead steps 100 times and compute the middling values. The calculated value of $Diff_3$ equal to 99.6150 and $Diff_4$ equals to 28.4170, which are near its hypothetical values. Therefore, the presented scheme is shown to be very vulnerable to the slight alteration of cipher images and can withstand the differential cipher images attacks.

5.6. Resisting Chosen/Known Plaintext Attacks

The chosen/known plaintext attack [48,49] can occur when an attacker chooses an arbitrary plaintext and its corresponding cipher text to distinguish the algorithm or the secret key, which allows it to decrypt any cipher text using this algorithm. Assume that dual plain images $\mathbf{P}_1$ and $\mathbf{P}_2$ are identical except for $\mathbf{P}_1$ (i, j) ≠ $\mathbf{P}_2$ (i, j) where $\mathbf{P}_2$ (i, j) = [$\mathbf{P}_1$ (i, j) + 1] mod 256. In the forward image diffusion stage, the plain images $\mathbf{P}_1$ and $\mathbf{P}_2$ are transformed to matrices denoted by $\mathbf{Q}_1$ and $\mathbf{Q}_2$ with the XOR logic process and the pseudo-noise matrix X. Consequently, rotate $\mathbf{Q}_1$ and $\mathbf{Q}_2$ by 180 degrees to get $\mathbf{A}_1$ and $\mathbf{A}_2$. Thus, the pixel located at (1, 1) swaps its position with the pixel located at (w_1, h_1) in $\mathbf{A}_1$, while the pixel located at location (1, 1) swaps its position with the pixel located at (w_2, h_2) in $\mathbf{A}_2$. After one time of DNA scrambling operation, on the pixel (1, 1), the value of $\mathbf{I}_1$ (1, 1) ≠ $\mathbf{I}_2$ (1, 1). In a similar way, the value of $\mathbf{I}_1$ (1, 2) ≠ $\mathbf{I}_2$ (1, 2). This means that as for images $\mathbf{I}_1$ and $\mathbf{I}_2$, we have $\mathbf{I}_1$ (i, j) ≠ $\mathbf{I}_2$ (i, j). Rotate $\mathbf{I}_1$ and $\mathbf{I}_2$ by 180 degrees to obtain $\mathbf{B}_1$ and $\mathbf{B}_2$, respectively; then, we get $\mathbf{B}_1$ (i, j) ≠ $\mathbf{B}_2$ (i, j) for i = 1, 2, · · ·, W, j = 1, 2, · · ·, H and $\mathbf{B}_1$ (W, 1) ≠ $\mathbf{B}_2$ (W, 1). According to Figure 2, by backward diffusion operation, $\mathbf{E}_1$ and $\mathbf{E}_2$ are generated from $\mathbf{B}_1$ and $\mathbf{B}_2$ respectively, so according to the proposed algorithm described, we can get $\mathbf{E}_1$ (i, j) ≠ $\mathbf{E}_2$ (i, j). Thus, $\mathbf{C}_1$ (i, j) ≠ $\mathbf{C}_2$ (i, j), i = 1, 2, · · ·, W, j = 1, 2, · · ·, H. These revealed that for identical plain images $\mathbf{P}_1$ and $\mathbf{P}_2$ with just one pair of pixels being dissimilar, their ciphered images $\mathbf{C}_1$ and $\mathbf{C}_2$ will be unique for each corresponding pixel location, even when they are cyphered with an identical secret key. Therefore, the presented encryption algorithm can withstand the chosen/known plaintext attacks.

5.7. Global Information Entropy

The global information entropy indicates the uncertainty of global image information, which is denoted by $H(m)$ of matrix m, and evaluated as

$$H(m) = -\sum_{i=0}^{255} p(m_i) \log_2((p(m_i)) \tag{24}$$

where $p(m_i)$ represents the probability of m_i. The theoretical value of the global information entropy intended for an 8-bit grayscale random image is nearer to 8. The global information entropy calculated results are presented in Table 8. We take the plain image Lena and the corresponding ciphered image as an example with a grayscale level L of 256. In the proposed system, the information entropy of the plain image is equal to 7.4430 and the entropy of the cipher image is equal to 7.9882, which demonstrates that the proposed cryptosystem can resist entropy attacks efficiently.

Table 8. Information entropy.

Average Performance	Proposed System			CCAES [41]	CDCP [42]	CHC [43]	C-DNA [44]	HC-DNA [45]
	Lena	Cameraman	Circuit					
Plain	**7.443**	**7.432**	**7.438**	**7.422**	7.438	7.441	7.428	7.431
Cipher	7.988	7.997	7.995	7.997	7.966	7.997	7.996	7.996

5.8. Local Shannon Entropy

Wu et al. [50] have expressed a new entropy gauge to regulate the real randomness by picking the non-overlapping blocks inside the encrypted image. The local Shannon entropy (LSE) is computed by calculating the mean of several global Shannon entropies on every one of the building blocks. Taking into account the randomness of the ciphered image, but the global entropy analysis in the previous section, the LSE can be defined by

$$H_{k,l}(m) = -\sum_{i=0}^{k} \frac{H(m_i)}{k} \tag{25}$$

where m_1, m_2, ... , m_k are k selected image blocks, while l is the amount of pixels for each block. The local entropy values for the encrypted image are presented in Table 9. It can be shown that the local entropy value is nearer to the optimum hypothetical value (≈8). Therefore, the proposed algorithm has good randomness.

Table 9. Local Shannon entropy.

Image	Proposed System	[51]	[52]	[53]	[54]
Lena	7.903462	7.902838	7.900975	7.904512	7.904671

5.9. Complexity Analysis

To compute the complications of performing the presented algorithm, the image size as $W \times H$ is taken into consideration. Let n indicate the quantity of pixels inside the image. The complexity of the presented algorithm can be determined by the following discussed operations. These operations consist of binary data conversion, DNA scrambling operation, secret key generation, forward and backward image diffusion, and decimal data conversion. The complexity of binary data conversion is O(n^2) and that of the DNA scrambling operation is equal to O($4n^2$). The secret key creation process consists of tri-sub-operations such as pseudo-random sequence production, binary transformation, and DNA scrambling with a complexity of O($6n^2$). In contrast, the complexity of forward and backward diffusion operations is O($62n^2$). The conversions from DNA to binary data and binary data to decimal data take O($5n^2$). Therefore, the overall complexity of the presented image encryption scheme is O($78n^2$).

5.10. Encryption and Decryption Speed

The computer used was constructed with Intel Duo Core I7 M460@2.53 GHz, 8 GB DDR3 RAM, Windows 10. For the encryption time T_E and decryption time T_D, the effect of $a_1 + a_2$ can be neglected due to its very small value contrasted to the effect of the original image size. So, we put the values of a_1 and a_2 to 128. We made the experiments on the pictures with the size of 200 × 200 pixels and recorded the encryption/decryption algorithm duration in Table 10.

Table 10. Encryption/Decryption time.

Algorithms	Proposed System	CCAES [41]	CDCP [42]	CHC [43]	C-DNA [44]	HC-DNA [45]
Time	0.19253	2.9	2.70264	3.17265	2.15572	0.27783

From Table 10, we can see that for 1000 pieces of images encrypting or decrypting, the execution times of different encryption schemes was listed. As can be seen, the encryption speed of our proposed algorithm is sufficiently fast to meet real-time performance necessities.

6. Conclusions

This article introduced a new bijective algorithm which is dedicated to secure image transmission over the data communication systems. Both encryption and decryption algorithms are identical and each have two diffusion processes and one DNA confusion process, which reduces hardware implementation complexity according to Shannon's' proposal. The diffusion process employs the hyperchaotic system and the confusion process uses the DNA, which both enhance the proposed algorithm security. When compared with former algorithms, the statistical tests proved that the proposed cryptosystem has a larger key space to resist brute-force attack, and the randomness tests showed that the encrypted pixels are distributed more randomly through the ciphered image. In addition, the proposed system was revealed to be more sensitive than former techniques against minimal change in secret key and better resistance against the known plaintext, the chosen plaintext, the differential cipher image attacks, and entropy attacks.

Finally, as future research, we advise an additional investigation of the simulation analysis of the chaotic performance by using an exponential chaotic model and other confusion techniques to generate a robust chaotic image encryption technique with the addition of fault-tolerance technology for the purpose of enhanced transmission of high-quality and secure data.

Author Contributions: Methodology, D.H.E., H.G.M. and K.H.M.; Software D.H.E., H.G.M. and K.H.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: This research was funded by the Deanship of Scientific Research at Princess Nourah Bint Abdulrahman University through the Fast-track Research Funding Program.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Psannis, K.E.; Plageras, A.P.; Ishibashi, Y.; Kim, B.-G. Algorithms for efficient digital media transmission over IoT and cloud networking. *J. Multimed. Inf. Syst.* **2018**, *5*, 1–10.
2. Stergiou, C.; Psannis, K.E.; Kim, B.-G.; Gupta, B. Secure integration of IoT and cloud computing. *Future Gener. Comput. Syst.* **2018**, *78*, 964–975. [CrossRef]
3. Memos, V.A.; Psannis, K.E.; Ishibashi, Y.; Kim, B.G.; Gupta, B.B. An Efficient Algorithm for Media-based Surveillance System (EAMSuS) in IoT Smart City Framework. *Future Gener. Comput. Syst.* **2017**. [CrossRef]
4. Psannis, K.E.; Stergiou, C.; Gupta, B.B. Advanced Media-based Smart Big Data on Intelligent Cloud Systems. *IEEE Trans. Sustain. Comput.* **2018**, *4*, 77–87. [CrossRef]
5. Stergiou, C.; Psannis, K.E. Recent advances delivered by Mobile Cloud Computing and Internet of Things for Big Data applications: A survey. *Int. J. Netw. Manag.* **2017**, *27*, 1–12. [CrossRef]
6. Liu, L.; Zhang, Q.; Wei, X. A RGB image encryption algorithm based on DNA encoding and chaos map. *Comput. Electr. Eng.* **2012**, *38*, 1240–1248. [CrossRef]
7. Gahlaut, A.; Bharti, A.; Dogra, Y.; Singh, P. DNA-based Cryptography. *Asp. Mol. Comput. Lect. Notes Comput. Sci.* **2003**, *2950*, 167–188.
8. Adleman, L.M. Molecular computation of solutions to combinatorial problems. *Science* **1994**, *266*, 1021–1024. [CrossRef]
9. Li, S.; Chen, G.; Zheng, X. Chaos-based encryption for digital images and videos. In *Multimedia Security Handbook*; CRC Press: Boca Raton, FL, USA, 2004; pp. 133–167.
10. Mazloom, S.; Eftekhari-Moghadam, A.M. Color image encryption based on Coupled Nonlinear Chaotic Map. *Chaos Solitons Fractals* **2009**, *42*, 1745–1754. [CrossRef]
11. Zhang, Q.; Guo, L.; Wei, X. Image encryption using DNA addition combining with chaotic maps. *Math. Comput. Model.* **2010**, *52*, 2028–2035. [CrossRef]
12. Yunpeng, Z.; Yu, Z.; Zhong, W.; Sinnott, R.O. Index-Based Symmetric DNA Encryption Algorithm. In Proceedings of the 4th International Congress on Image and Signal Processing, CISP 2011, Shanghai, China, 15–17 October 2011; pp. 2290–2294.
13. Zhang, Q.; Zhang, J.; Lian, S.; Guo, L.; Wei, X. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. *J. Syst. Softw.* **2011**, *85*, 290–299.
14. Enayatifar, R.; Abdullah, A.H.; Isnin, I.F. Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. *Opt. Lasers Eng.* **2014**, *56*, 83–93. [CrossRef]
15. Liu, H.; Wang, X.; Kadir, A. Image encryption using DNA complementary rule and chaotic maps. *Appl. Soft Comput. J.* **2012**, *12*, 1457–1466. [CrossRef]
16. Liu, H.; Wang, X. Color image encryption based on one-time keys and robust chaotic maps. *Comput. Math. Appl.* **2010**, *59*, 3320–3327. [CrossRef]
17. Zhang, Q.; Guo, L.; Wei, X. Cryptanalyzing a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. *Optik* **2013**, *124*, 3596–3600. [CrossRef]
18. Zhu, J.C.Z.; Fu, C.; Zhang, L.Z.Y. An efficient image encryption scheme using lookup table-based confusion and diffusion. *Nonlinear Dyn.* **2015**, *81*, 1151–1165.

19. Chen, J.; Zhu, Z.; Zhang, L.; Zhang, Y.; Yang, B. Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption Exploiting self-adaptive permutation—Diffusion and DNA random encoding for secure and efficient image encryption. *Signal Process. J.* **2018**, *142*, 340–353. [CrossRef]
20. Al-Mashhadi, H.M.; Abduljaleel, I.Q. Color Image Encryption Using Chaotic Maps, Triangular Scrambling, with DNA Sequences. In Proceedings of the International Conference on Current Research in Computer Science and Information Technology, ICCIT 2017, Dhaka, Bangladesh, 22–24 December 2017; pp. 93–98.
21. Liu, H.; Wang, X. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. *Opt. Commun.* **2011**, *284*, 3895–3903. [CrossRef]
22. Hua, Z.; Xu, B.; Jin, F.; Huang, H. Image encryption using Josephus problem and filtering diffusion. *IEEE Access* **2019**, *7*, 8660–8674. [CrossRef]
23. Li, C.; Zhang, Y.; Xie, E.Y. When an attacker meets a cipher-image in 2018: A Year in Review. *Inf. Secur. Appl.* **2019**, *48*. [CrossRef]
24. Chai, X.; Fu, X.; Gan, Z.; Lu, Y.; Chen, Y. A color image cryptosystem based on dynamic DNA encryption and chaos. *Signal Process.* **2019**, *155*, 44–62. [CrossRef]
25. Özkaynak, F. Brief review on application of nonlinear dynamics in image. *Nonlinear Dyn.* **2018**, *92*, 305–313. [CrossRef]
26. Matthews, R. On the derivation of a 'chaotic' encryption algorithm. *Cryptologia* **1989**, *13*, 29–42. [CrossRef]
27. Zhu, C.; Chen, Z.; Ouyang, W. A New Image Encryption Algorithm Based on General Chen's Chaotic System. *J. Cent. South Univ. Technol.* **2006**, *37*, 1142–1148.
28. Khan, M.; Shah, T. A construction of novel chaos base nonlinear component of block cipher. *Nonlinear Dyn.* **2014**, *76*, 377–382. [CrossRef]
29. Fu, X.Q.; Liu, B.C.; Xie, Y.Y.; Li, W.; Liu, Y. Image encryption-then-transmission using DNA encryption algorithm and the double chaos. *IEEE Photonics J.* **2018**, *10*, 1–16. [CrossRef]
30. Lorenz, E. Deterministic Nonperiodic Flow. *J. Atmos. Sci.* **1963**, *20*, 130–141. [CrossRef]
31. LÜ, J.; Chen, G. A New Chaotic Attractor Coined. *Int. J. Bifurc. Chaos* **2002**, *12*, 659–661. [CrossRef]
32. Liu, C.; Liu, T.; Liu, L.; Liu, K. A new chaotic attractor. *Chaos Solitons Fractals* **2004**, *22*, 1031–1038. [CrossRef]
33. Park, J.H. Intuitionistic fuzzy metric spaces. *Chaos Solitons Fractals* **2004**, *22*, 1039–1046. [CrossRef]
34. Dai, H.; Jia, L.X.; Zhang, Y.B.; Shang, J. A new four-dimensional hyperchaotic L system and its adaptive control. *Chin. Phys. B* **2011**, *20*, 1–9.
35. Wang, X.-Y.; Yang, L.; Liu, R.; Kadir, A. A chaotic image encryption algorithm based on perceptron model. *Nonlinear Dyn.* **2010**, *62*, 615–621. [CrossRef]
36. Wang, X.; Wang, M. A hyperchaos generated from Lorenz system. *Phys. A Stat. Mech. Appl.* **2008**, *387*, 3751–3758. [CrossRef]
37. Zhang, F.; Zhang, G. Dynamical Analysis of the Hyperchaos Lorenz System. *Complexity* **2016**, *21*, 440–445. [CrossRef]
38. Zhang, Y. A chaotic system based image encryption scheme with identical encryption and decryption algorithm. *Chin. J. Electron.* **2017**, *26*, 1022–1031. [CrossRef]
39. Srividhya, N.; Vino, T. Genome Based Highly Secured Image Using DNA Cryptography and Trellis Algorithm. In Proceedings of the IEEE International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2016, Chennai, India, 23–25 March 2016; pp. 1658–1662.
40. Zhang, Y. Plaintext Related Image Encryption Scheme Using Chaotic Map. *Telkomnika Indones. J. Electr. Eng.* **2013**, *12*, 635–643. [CrossRef]
41. Arab, A.; Rostami, M.J.; Ghavami, B. An image encryption method based on chaos system and AES algorithm. *J. Supercomput.* **2019**, *75*, 6663. [CrossRef]
42. Zhu, C.; Hu, Y.; Sun, K. New Image Encryption Algorithm Based on Hyperchaotic System and Ciphertext Diffusion in Crisscross Pattern. *J. Electron. Inf. Technol.* **2013**, *34*, 1735–1743. [CrossRef]
43. Zhu, C.; Sun, K. Cryptanalysis and improvement of a class of hyperchaos based image encryption algorithms. *Acta Phys. Sin.* **2012**, *61*, 1–12.
44. Wang, X.; Liu, C. A novel and effective image encryption algorithm based on chaos and DNA encoding. *Multimed. Tools Appl.* **2017**, *76*, 6229–6245. [CrossRef]
45. Zhan, K.; Wei, D.; Shi, J.; Yu, J. Cross-utilizing hyperchaotic and DNA sequences for image encryption. *J. Electron. Imaging* **2017**, *26*, 1–11. [CrossRef]

46. Ravichandran, D.; Praveenkumar, P.; Rayappan, J.B.B.; Amirtharajan, R. Chaos based crossover and mutation for securing DICOM image. *Comput. Biol. Med.* **2016**, *72*, 170–184. [CrossRef] [PubMed]
47. Ravichandran, D.; Praveenkumar, P.; Rayappan, J.B.B.; Amirtharajan, R. DNA Chaos Blend to Secure Medical Privacy. *IEEE Trans. NanoBiosci.* **2017**, *16*, 850–858. [CrossRef] [PubMed]
48. Liu, Y.; Yu, L.; Wong, Y.Z.K.; Wang, J. Chosen-plaintext attack of an image encryption scheme based on modified permutation—Diffusion structure. *Nonlinear Dyn.* **2016**, *84*, 2241–2250. [CrossRef]
49. Zhang, Y.; Xiao, D.; Wen, W.; Li, M. Cryptanalyzing a novel image cipher based on mixed transformed logistic maps. *Multimed. Tools Appl.* **2014**, *73*, 1885–1896. [CrossRef]
50. Wu, Y.; Zhou, Y.; Saveriades, G.; Agaian, S.; Noonan, J.P.; Natarajan, P. Local Shannon entropy measure with statistical tests for image randomness. *Inf. Sci.* **2013**, *222*, 323–342. [CrossRef]
51. Zhu, H.; Zhao, C.; Zhang, X. A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem. *Signal Process. Image Commun.* **2013**, *28*, 670–680. [CrossRef]
52. Zhu, Z.; Zhang, W.; Wong, K.W.; Yu, H. A chaos-based symmetric image encryption scheme using a bit-level permutation. *Inf. Sci.* **2011**, *181*, 1171–1186. [CrossRef]
53. Zhou, Y.; Bao, L.; Philip Chen, C.L. Image encryption using a new parametric switching chaotic system. *Signal Process.* **2013**, *93*, 3039–3052. [CrossRef]
54. Zhu, H.; Zhao, C.; Zhang, X.; Yang, L. An image encryption scheme using generalized Arnold map and affine cipher. *Optik* **2014**, *125*, 6672–6677. [CrossRef]