entropy

MDPI

Article

# A Novel Color Image Encryption Algorithm Based on Hyperchaotic Maps and Mitochondrial DNA Sequences

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

1 Electrical Department, College of Engineering, Princess Nourah Bint Abdulrahman University, Riyadh 11671, Saudi Arabia
2 Electrical Department, College of Engineering, Alexandria Higher Institute of Engineering and Technology, Alexandria 21421, Egypt
3 Information Technology, College of Computer and Information Sciences, 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 (H.G.M.); dhelkamchouchi@pnu.edu.sa (D.H.E.)

Received: 4 January 2020; Accepted: 27 January 2020; Published: 29 January 2020


**Abstract:** Multimedia encryption innovation is one of the primary ways of securely and privately guaranteeing the security of media transmission. There are many advantages when utilizing the attributes of chaos, for example, arbitrariness, consistency, ergodicity, and initial condition affectability, for any covert multimedia transmission. Additionally, many more benefits can be introduced with the exceptional space compliance, unique information, and processing capability of real mitochondrial deoxyribonucleic acid (mtDNA). In this article, color image encryption employs a confusion process based on a hybrid chaotic map, first to split each channel of color images into n-clusters; then to create global shuffling over the whole image; and finally, to apply intrapixel shuffling in each cluster, which results in very disordered pixels in the encrypted image. Then, it utilizes the rationale of human mitochondrial genome mtDNA to diffuse the previously confused pixel values. Hypothetical examination and trial results demonstrate that the anticipated scheme exhibits outstanding encryption, as well as successfully opposes chosen/known plain text, statistical, and differential attacks.

**Keywords:** hybrid chaotic; image; encryption; decryption; secured communications; DNA; mitochondrial genome

## 1. Introduction

Owing to vast development in the modern digital era, the world has grown to be a worldwide community sharing private information. Because of this, people use images instead of long texts for sharing this kind of information securely and privately [1]. Therefore, the protection of such images has become one of the vital concerns in medical, military, and many other areas. Recently, many cryptographic algorithms depending on chaotic systems have been used in image encryption [2]. One of the recognized methods employed before image transmission is to convert an image into an unintelligible form, so that the transmitted message of the distorted image will not be discovered if it has reached an unsought end [3,4]. The encryption process is done with the help of a key, which produces variation on the pixel values of the image and destroys the apparent image attribute. Another encryption process is the scrambling image technique. In this technique, all pixel values are repositioned between different pixels of the image to be different from the original plain image, for example, Arnold transform, exponential transformation, geometry transform, and so on. These

transformations have definite regularity, although the results of pixel distribution are different after scrambling, due to changes in only the position of pixels, without changing gray values. Arnold's map has the property of periodicity. After running the algorithm for a certain number of times, the original image can be restored. Therefore, it has a weakness for the system [5]. However, whilst [6] demonstrated the powerful recovery of an image encryption system based on an Arnold map and Lü map, their encryption system was susceptible to several attacks, such as plaintext and chosen-text attacks when it depended on only the permutation of pixel values [7]. As a result, these attack pixel values have to be rearranged and vary their position. Rearrangement of the values of pixels is called the confusion process, while changing the pixel values is known as the diffusion process. Chaos is a multi-disciplinary hypothesis which states that during the randomness of the chaotic complex technique, the chaotic system generates sequences due to its initial parameters' sensitivity, periodic and pseudo randomness, and long-term volatility [8], which encouraged us to employ the chaos theory in our new proposed scheme.

In recent years, several scientific papers have concentrated on researching chaotic image encryption. In 2015 [9], S. S. Askar, A. A. Karawia et al. presented an image encryption system based on a chaotic economic map, and the simulation outputs a display so that the proposed algorithm can utilize the same secret keys to encrypt and decrypt the images successfully. The security analysis shows that the encrypted images have a good performance, but cannot resist noise attacks. After one year, Abbas proposed a new image encryption technique based on unconventional element analysis and Arnold's Cat Map [10], which was easily achieved and afforded an efficient and secure approach for image encryption. However, the algorithm depends on the encryption of square images only, so the domain of application is remarkably restricted. Later, in 2017, Shaikh, Chapaneri et al. [11] proposed a color image encryption algorithm, which is a single round-based hyperchaotic system due to bi-directional pixel diffusion that contributes towards an increased security and improved efficiency. Recently, in 2019, Chenghai Li et al. used the "transforming-scrambling-diffusion" model to introduce a hyperchaotic color image encryption algorithm that depends on converting the pixel values into gray codes before scrambling [12]. In the same year, Priya Ramasamy et al. suggested an improved logistical map while using a chaotic maps function and uncomplicated encryption techniques, such as block scrambling and modified zigzag transformation, for encryption phases [13]. Recently, deoxyribonucleic acid (DNA) was applied to an image chaotic cryptosystem [14–22], as a result of its numerous superior characteristics, such as its enormous parallelism, vast storage, small power consumption, etc. In 2016, Kulsoom et al. extracted the most significant bits and the least significant bits for each pixel of an image and performed DNA computing for them. Kulsoom et al.'s algorithm has a low robustness against noise because most digits of each pixel are not changed [23]. After that, in 2018, Ran Wei et al. proposed an image cryptosystem that depends on the combination of DNA encoding and several chaotic maps [24]. The performance analysis illustrated that the system could greatly enhance the sensitivity of plain images and secret keys, but the algorithm was complex and the necessities for hardware were comparatively high. In 2020, J. Wu, J. Shi, T. Li, proposed a novel image encryption algorithm based on a hyperchaotic system and variable kernels for the confusion stage and a DNA technique for the diffusion stage [25].

Mitochondrial DNA (mtDNA) is a small part of the DNA of organelle cells within eukaryotic cells [26]. Eukaryotic cells are organisms that have a nucleus enclosed within membranes that are used to transform chemical energy into a formula that cells can use [27]. In humans, there are 16,569 base duos of mitochondrial DNA to code only 37 genes. The first major part of the human genome that can be sequenced is human mitochondrial DNA [28]. mtDNA is congenital and uniquely from the mother in several organisms, including humans. Since animal mtDNA develops more rapidly than nuclear genetic symbols [29,30], it signifies a mainstay of phylogenetic and evolutionary biology. mtDNA allows inspection of the kinship of inhabitants. Therefore, it has become vital in molecular biology and biotechnology.

In this article, a new image cryptosystem is presented to encrypt a color image using identical encryption and decryption schemes. Both of these processes consist of confusion stages employing a hyperchaotic system, diffusion stage, and mtDNA. The proposed encryption algorithm was applied on three channels of a color plain image to increase uncertainty in the plain image. From the numerical analysis, the proposed algorithm was seen to be robust against various attacks, for example, chosen/known plain text attacks, brute force attacks, differential cipher image attacks, and entropy attacks. It has a large key space and is sensitive to minimal change in the chosen secret key. The encryption scheme was also compared with newly developed encryption techniques. The rest of the article is organized as follows. Section 2 details a brief description of the hyperchaotic system, mtDNA, and DNA encoding. The explanation and argument of the proposed encryption/decryption algorithm are introduced in Section 3. Section 4 gives the numerical simulation results, while the security act of the proposed scheme is analyzed in Section 5. Finally, Section 6 concludes the article.

## 2. Preliminaries

### *2.1. Hyperchaotic System*

A hyperchaos system, technologically, advanced from chaos. Its dynamical structure is more complicated compared with other chaotic systems. In addition, hyperchaos enhances a higher level of randomization and uncertainty. By adding two or more positive Lyapunov exponents, the hyperchaotic system can be distinguished from chaos. Hyperchaos exists in four-dimension nonlinear systems. Owing to its simpler formula and higher effectiveness, the chaotic system has a smaller key space and lower complexity. Consequently, the chaotic system has lower security protection. On the contrary, the hyperchaotic system has more state variables, a larger key space, and complex nonlinear behavior, resulting in higher security protection. The hyperchaotic system can be determined as follows [31]:

$$\begin{aligned} \dot{x_1} &= \alpha(x_2 - x_1) + \lambda_1 x_4, \\ \dot{x_2} &= \xi x_1 - x_1 x_3 + \lambda_2 x_4, \\ \dot{x_3} &= -\beta x_3 + x_1 x_2 + \lambda_3 x_4, \\ \dot{x_4} &= -\tau x_1, \end{aligned} \tag{1}$$

where $\alpha, \beta, \xi, \tau, \lambda_1, \lambda_2$, and $\lambda_3$ are the control parameters of the 4-D hyperchaotic system. The system presents hyperchaotic behavior when the control parameters are $\alpha = 35, \beta = 3, \xi = 35, \tau = 5, \lambda_1 = 1, \lambda_2 = 0.2$, and $\lambda_3 = 0.3$

### *2.2. Fundamentals of Mitochondrial DNA*

Mitochondrial DNA is a type of DNA and is a small chromosome in a circular form found inside organelles known as mitochondria. Mitochondria are found in cells and have been determined in all unpredictable or eukaryotic cells, as well as plants, creatures, growths, and single-celled protists, which include their own mtDNA genome. In several creatures, mtDNA is a two-fold stranded particle that is shaped around the genome. Every mitochondrion can have several duplicates of the mtDNA genome. In human embryonic advancement, the variety of mitochondria and the substance of mtDNA in every mitochondrion have an impact on the creation of oocytes, preparation of the oocytes, and early embryonic development and enchantment [32].

For example, a simple sequence for the human mitochondrial genome is as follows:

"GATCACAGGTCTATCACCCTATTAACCACTCACGGGAGCTCTCCATGCAT
TTGGTATTTTCGTCTGGGGGGTGTGCACGCGATAGCATTGCGAGACGCTG
GAGCCGGAGCACCCTATGTCGCAGTATCTGTCTTTGATTCCTGCCTCATT
CTATTATTTATCGCACCTACGTTCAATATTACAGGCGAACATACCTACTAAAGT ... "

### 2.3. DNA Encoding

DNA encoding has a huge data capacity, so it can be used in cryptography [33]. In the transmission process, DNA can also be used to store data in image encryption. DNA computing depends on the DNA logic word, and only two digits are used to create four nucleic acid bases. Therefore, the information is stored in the form of these bases, which are Adenine (A), Cytosine (C), Guanine (G), and Thymine (T) [34]. In DNA cryptography, the four bases are used to capture the information. "A" and "T" are paired duos and the same is true for "C" and "G". Table 1 displays the rubrics for DNA encoding.

**Table 1.** Rubrics for DNA encoding [35].

| Rule No. | DNA Nucleic Acids | | | |
|---|---|---|---|---|
| | A | T | G | C |
| Rb1 | 00 | 11 | 01 | 10 |
| Rb2 | 00 | 11 | 10 | 01 |
| Rb3 | 11 | 00 | 01 | 10 |
| Rb4 | 11 | 00 | 10 | 01 |
| Rb5 | 10 | 01 | 11 | 00 |
| Rb6 | 01 | 10 | 11 | 00 |
| Rb7 | 10 | 01 | 00 | 11 |
| Rb8 | 01 | 10 | 00 | 11 |

## 3. Proposed Cryptosystem

The structure of the proposed cryptosystem is demonstrated in Figure 1, and involves two main phases. In the first phase, the confusion phase, the image pixels are shuffled based on the generated hyperchaotic sequence discussed in the first part of Section 2. For more unpredictability and to increase the efficiency of encryption, the pixels' positions are scrambled over the entire image, without changing the significance of the pixels, and the image becomes unknown. Hence, the primary and control factors of utilized chaotic maps serve as the employed undisclosed key. To improve the security further, the second stage, the diffusion stage, aims to diffuse the images' pixel values with the decimal converted values of the mtDNA sequence using the Exclusive OR (XOR) operation.

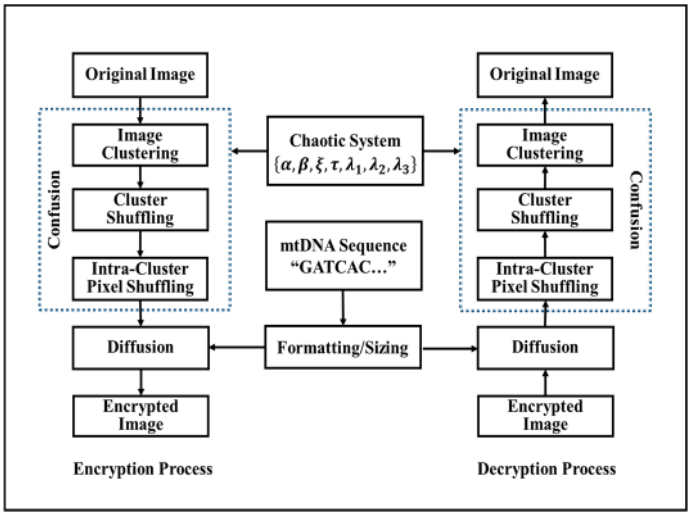



**Figure 1.** The proposed algorithm.

### *3.1. Hyperchaotic Sequence Generation*

We can use the hyperchaotic system discussed in Section 2.1 to generate the pseudorandom sequence. This is necessary for the field of cryptography, as both non-linearity and random performances make chaotic systems able to generate pseudorandom sequences. The following steps describe the sequence generation:

1. To reduce the cross effects and raise the security, pre-iterate the hyperchaotic system $N_0$ times;
2. The system is iterated another $M \times N$ times after $N_0$ iteration times. In each iteration $j$, four state values $\left\{x_1^j, x_2^j, x_3^j, x_4^j\right\}$ are sorted, where $j$ denotes the iteration index;
3. During each iteration, each state value of the four-state values $\left\{x_1^j, x_2^j, x_3^j, x_4^j\right\}$ is used to generate two different key values $((v_i^1)^j \in [0, 255]$, $i = 1, 2, 3, 4$ and $(v_i^2)^j \in [0, 255],)$, which are calculated by

$$(v_i^1)^j = \mathrm{mod}\left\{floor([(\left|x_i^j\right| - floor(\left|x_i^j\right|)) \times 10^{15}]/10^8), 256\right\}, \quad i = 1, \ldots, 4, \tag{2}$$

$$(v_i^2)^j = \mathrm{mod}(floor(\mathrm{mod}\left\{[(\left|x_i^j\right| - floor(\left|x_i^j\right|)) \times 10^{15}]/10^8\right\}), 256), \quad i = 1, \ldots, 4, \tag{3}$$

   where mod $(\cdot)$ indicates the modulo process;
4. Concatenate Equation (2) with Equation (3) to get $v^j$:

$$v^j = [(v_1^1)^j, (v_2^1)^j, (v_3^1)^j, (v_4^1)^j, (v_1^2)^j, (v_2^2)^j, (v_3^2)^j, (v_4^2)^j]; \tag{4}$$

5. These sequences are concatenated after the whole iteration with Equation (5) to obtain $K$:

$$K = [v^1, v^2, \ldots\ldots, v^{M \times N}]. \tag{5}$$

   One component in $K$ can be represented by $K_i, i \in [1, 8MN]$.

### *3.2. Image Encryption*

1. Let $M \times N \times 3$ represent the whole dimension of the contribution color image **P**, as displayed in Figure 2a;
2. Obtain the three channels R, G, and B from the input image;
3. Divide each channel for both the row and column into $p \times q$ clusters, where $p = 2, 4, 8, 16$ and $q = 2, 4, 8, 16$ randomly depend on the generated chaotic sequence. For example, when $p = 2$ and $q = 4$ the resulting image is split into eight clusters, as shown in Figure 2b;
4. Shuffle all the clusters using the generated chaotic sequence $K$, as illustrated in Figure 2c;
5. Apply a chaotic sequence for each cluster to shuffle the pixels within every cluster, as clarified in Figure 2d;
6. Concatenate these permuted clusters to formulate the shuffled image with the same size of the novel colored image illustrated in Figure 2e;
7. To get new values of pixels, apply the diffusion process as follows:

   - Read the first $64 \times 64 \times 4$ mitochondrial DNA sequence "gatcacaggtctatcaccctattaaccactca ... ... ";
   - Convert it to a binary sequence using the rule discussed in Table 1: "{00011011011101000010111001101101111111100110100101111110 ... ... }";
   - Divide the sequence into 8-bit slices: {00011011 01110100 00101110 01101101 11111110 ... };
   - Convert each slice into its decimal representation: [27 116 46 109 254 105 125 ... ];
   - Formulate a $64 \times 64$ rdDNAstring matrix with the above decimal sequences;

- Generate a $3 \times 64 \times 64$ matrix for the three channels R, G, and B, as in

$$DMat(:,:,i) = mod[i \times mod[sum(sum\{sum(Image)\}), 256] \times rdDNAstring, 256] \quad for\ i = 1, 2, 3; \tag{6}$$

- Generate $128 \times 128 \times 3$ using

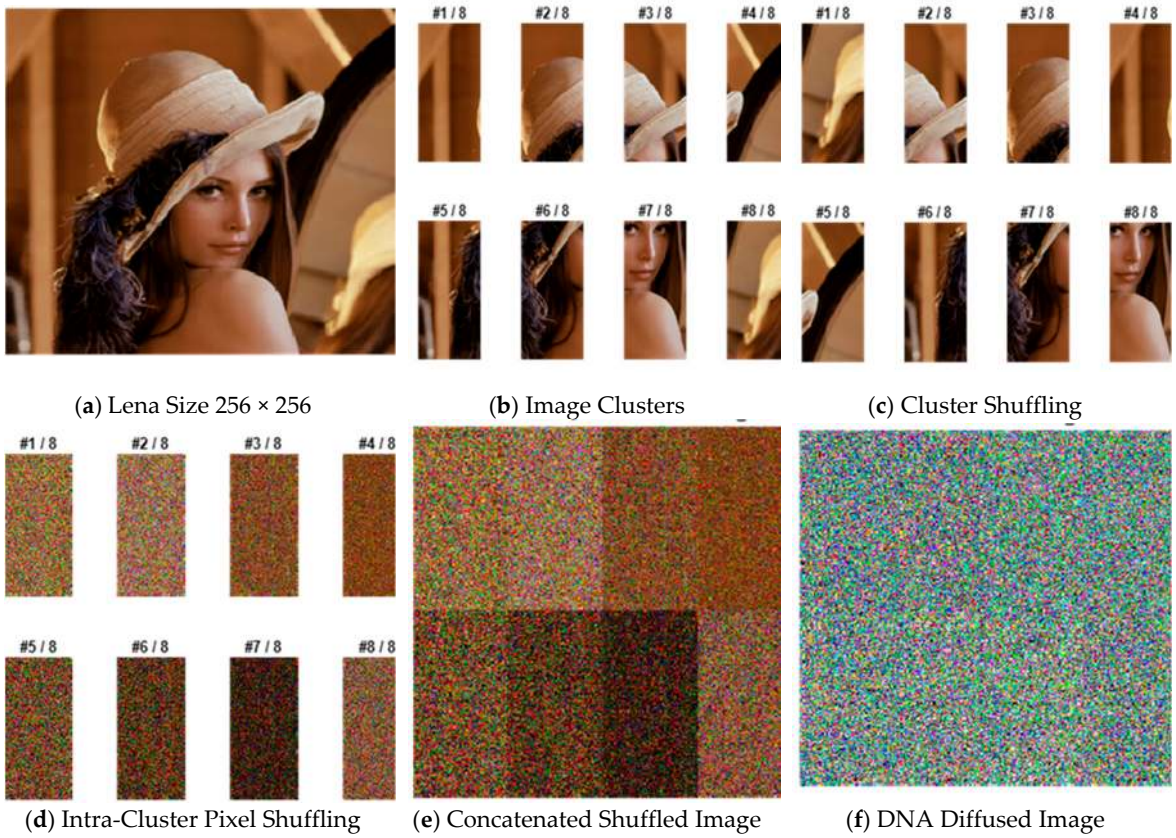
$$\text{lDMat}(:,:,i) = [\text{DMat}(:,:,i)\ \text{DMat}(:,:,i)\prime; \text{DMat}(:,:,i)\prime\ \text{DMat}(:,:,i)\prime] \quad for\ i = 1, 2, 3, \tag{7}$$

where [ ]′ is the transpose of the matrix;

- Generate $256 \times 256 \times 3$ using

$$\text{llDMat}(:,:,i) = [\text{lDMat}(:,:,i)\ \text{lDMat}(:,:,i)\prime; \text{lDMat}(:,:,i)\prime\ \text{lDMat}(:,:,i)\prime] \quad for\ i = 1, 2, 3; \tag{8}$$

- Resize the generated matrix to the same size of the concatenated image;
- Apply the XOR operation between the concatenated shuffled pixel values and the decimal converted values of mtDNA classification r1 and r2 to get the diffused encrypted image, as shown in Figure 2f.




(**a**) Lena Size 256 × 256 (**b**) Image Clusters (**c**) Cluster Shuffling

(**d**) Intra-Cluster Pixel Shuffling (**e**) Concatenated Shuffled Image (**f**) DNA Diffused Image

**Figure 2.** Simulation results of a Lena image.

## 4. Simulation Results

Experimentation was carried out on Lena and baboon images. The Matlab (R2015a) software (MathWorks, Natick, MA, USA) was used to apply the proposed algorithm. In the hyperchaotic map, the control parameters $\alpha = 35, \beta = 3, \xi = 35, \tau = 5, \lambda_1 = 1, \lambda_2 = 0.2$, and $\lambda_3 = 0.3$ were used to produce a chaotic sequence. The hyperchaotic sequences were arranged and the position of arranged sequences was used to split the plain image into n-clusters, shuffle the whole clusters, and scramble the

pixels of each cluster. The utilized colored plain images were Lena, with dimensions of $256 \times 256$ pixels, as shown in Figure 3a, and Baboon, with dimensions of $512 \times 512$ pixels, as shown in Figure 3d. The corresponding cipher image was generated using the encryption algorithm and is shown in Figure 3b,e. Then, we decrypted the cipher image, as presented in Figure 3b,e, with correct undisclosed key $\boldsymbol{K}$ to get the perfectly reconstructed image shown in Figure 3c,f.

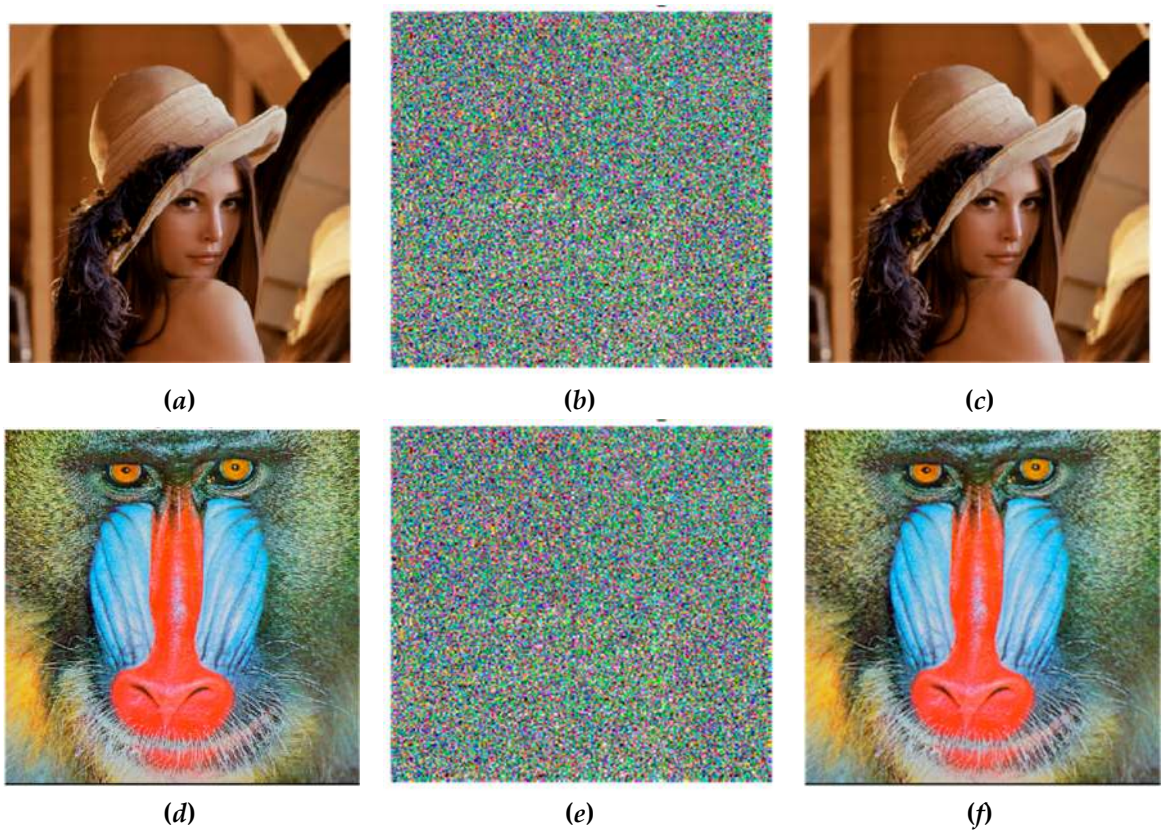



**Figure 3.** Simulation results. (**a**,**d**) Plain images; (**b**,**e**) generated cipher images of (**a**,**d**), respectively; and (**c**,**f**) recovered images.

## 5. Performance and Security Analysis

### *5.1. Key Space*

The key space of our new encryption algorithm consisted of the initial conditions of hyper-chaotic systems $x_1, x_2, x_3, x_4, r_1$, and $r_2$. The value ranges were $x_1 \in (-40, 40)$, $x_2 \in (-40, 40)$, and $x_3 \in (1, 80)$, each with a step size of $10^{-13}$, while the value range was $x_4 \in (-250, 250)$, with a step size of $10^{-12}$. $r_1$ and $r_2$ are two 8-bit random numbers whose value range is [0, 255] with a single step size. These factors were used as undisclosed keys for both the encryption and decryption process. Therefore, the key space of the proposed algorithm is $1.6777 \times 10^{64}$. The key space must be very large to restrict brute-force attacks; hence, it would take $2.03451 \times 10^{52}$ days to crack the system. Therefore, the proposed cryptosystem is able to protect against brute-force attacks.

### *5.2. Histogram Analysis*

Histogram analysis is an important statistical feature for estimating the enactment of an image encryption cryptosystem. The histograms for the three channels of original images of Lena and Baboon and their corresponding generated cipher images are presented in Figure 4. The original image's histogram is non-uniform and the characteristic peak is clear, and most of the image data were achieved smoothly. On the other hand, the recovered image is a perfectly reconstructed form of the

original image, and the cipher image is noise-like and not correlated with the original plain image. The recovered image is a perfectly reconstructed version of the original image. In the cipher image, the histogram is very stable and smooth, which proves that no statistical data from the original plain image was included. Therefore, the proposed system can counterattack statistical and cipher image attacks.

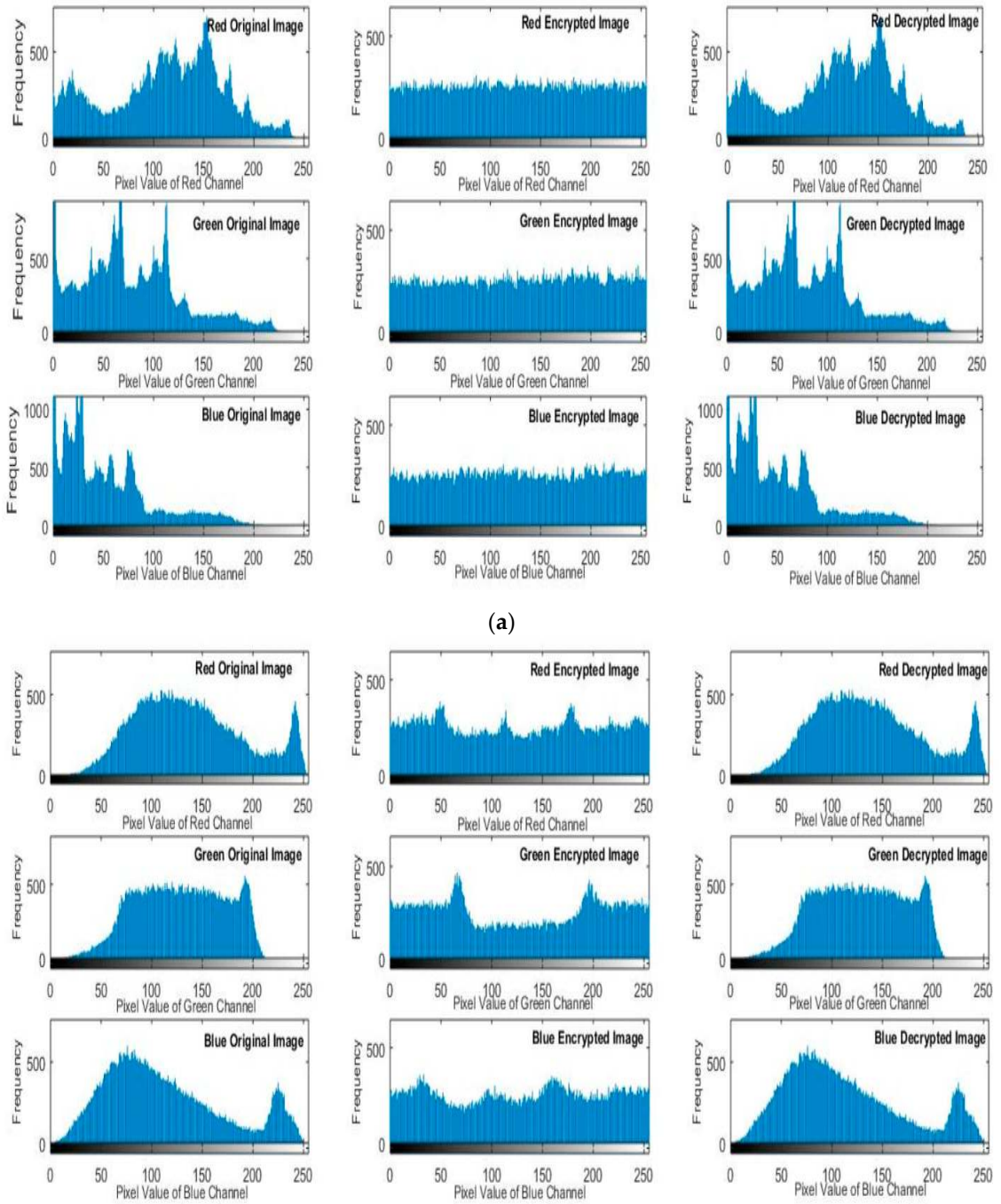



**Figure 4.** Histograms of colored plain images. (**a**) Histograms of Lena. (**b**) Histograms of baboon. The first column includes histograms of the original image, the second column includes histograms of the corresponding cipher image, and the third column includes histograms of the recovered colored image.

### *5.3. Correlation Factor Analysis*

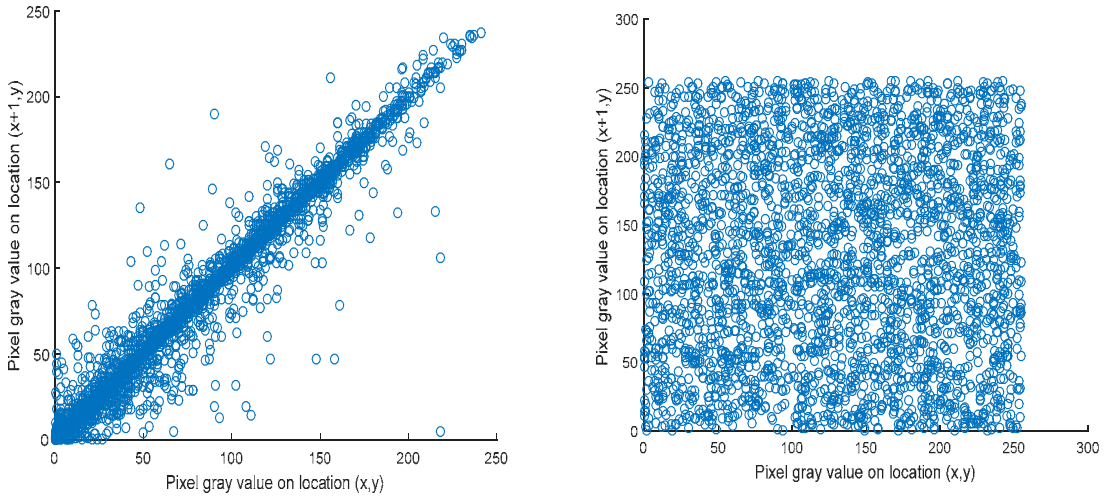
The correlation factor (CF) is an important metric for calculating two adjacent pixels in the three directions of horizontal, vertical, and diagonal. $N$ pairs of neighboring pixels are selected, and $x, y$ are two neighboring pixels. Then, the calculation formula of the correlation factor can be given by

$$CF = \frac{\sum_{i=1}^{N}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{N}(x_i - \overline{x})^2}\sqrt{\sum_{i=1}^{N}(y_i - \overline{y})^2}}. \quad (9)$$

Now, let $N = 2000$. The results of the correlation of the original and cipher images were computed and are presented in Table 2. The low value of the correlation factor for neighboring pixels in the three directions indicates that the neighboring pixels are uncorrelated. Figures 5 and 6 display the correlation distribution of each pair of horizontally neighboring pixels. The correlation factor of the original image is high and close to 1. In contrast, the correlation factor calculated for the cipher image is low and close to 0. Therefore, these results verify the strength of the proposed cryptosystem.

**Table 2.** The various calculated correlation factors.

| Correlation Factors | Direction of Adjacent Pixels | | |
|---|---|---|---|
| | **Horizontal** | **Vertical** | **Diagonal** |
| Plain | 0.9706 | 0.9841 | 0.9639 |
| Cipher | 0.0058 | 0.0033 | 0.0010 |
| Plain | 0.9195 | 0.9005 | 0.8696 |
| Cipher | 0.0013 | 0.0025 | 0.0010 |




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

**Figure 5.** Simulation of the correlation factor. (**a**) Correlation in the horizontal direction for the Lena plain image; (**b**) correlation in the horizontal direction for the Lena cipher image.

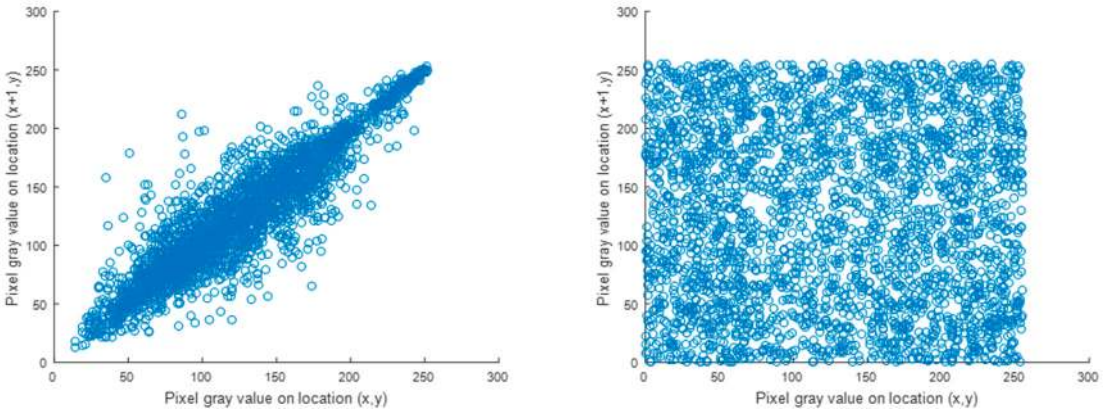



**Figure 6.** Simulation of the correlation factor. (**a**) Correlation in the horizontal direction for baboon plain images; (**b**) correlation in the horizontal direction for baboon cipher images.

### *5.4. Key Sensitivity Analysis*

We can observe in the proposed algorithm the sensitivity of the generated secret key $x_1, x_2, x_3, x_4, r_1$, and $r_2$ by modifying and changing one bit in it. The wrong key can be generated by changing any element of secret key $x_1, x_2, x_3$ by $10^{-13}$ or $x_4$ by $10^{-12}$, or any value of $r_1$ and $r_2$ by 1. This small change leads to a totally different ciphered image. Therefore, the ciphered image will be wholly dissimilar from the original input image. In the proposed cryptosystem, we encrypted the original plain images twice to exhibit the sensitivity of the generated secret key. In the first encryption process, the plain images were encrypted with the original secret key, while in the second encryption process, the plain images were encrypted with the wrong key. The wrong key was generated from the original key. We ran the algorithm on the images of Lena and the baboon, and the effects are displayed in Figures 7 and 8. As can be seen in the figures, the encrypted images with the wrong key are totally different from those encrypted with the exact key, which proves that the encryption algorithm has a high sensitivity to secret keys.

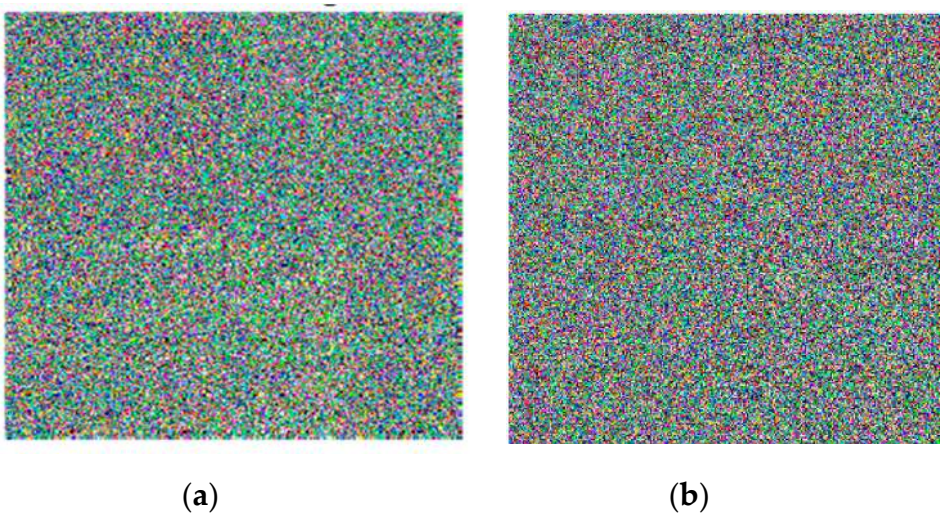
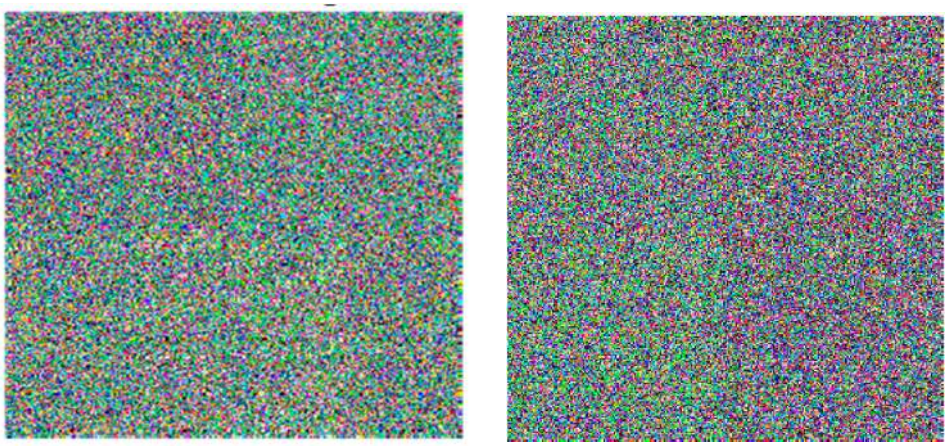



**Figure 7.** Key sensitivity analysis. (**a**) Encrypted Lena image using the exact secret key; (**b**) encrypted Lena image using the wrong key.



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

**Figure 8.** Key sensitivity analysis. (**a**) Encrypted baboon image using the exact secret key; (**b**) encrypted baboon image using the wrong key.

### *5.5. Differential Attack*

An opponent can get valuable information by altering several pixels of the original plain image. The number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI) are usually employed to evaluate the resistance of the encrypted plain image against differential raids. We utilized the presented encryption scheme to encrypt $\mathbf{P}_1$ and $\mathbf{P}_2$ to obtain their corresponding encrypted images, indicated by $\mathbf{C}_1$ and $\mathbf{C}_2$, with a unify secret key, where $\mathbf{P}_2$ is the change in one pixel of the original plain image $\mathbf{P}_1$. Then, the NPCR and UACI could be given by

$$\text{NPCR} = \frac{1}{W}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|Sign(\mathbf{C}_1(i,j) - \mathbf{C}_2(i,j))\right| \times 100\%, \tag{10}$$

$$\text{UACI} = \frac{1}{W}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\left|Sign(\mathbf{C}_1(i,j) - \mathbf{C}_2(i,j))\right|}{256} \times 100\%. \tag{11}$$

We chose randomly, changed the value of one pixel of the original input images 10 times, and calculated the NPCR and UACI of Lena and the baboon, respectively. The outputs are summarized in Tables 3 and 4, which clarify that our new cryptosystem is very sensitive to variation arising in only one pixel value of the original image. In [36–38], NPCR and UACI are close to theoretical values, but they have a reduced noise attack performance. Compared with the proposed cryptosystem, it is clear that the proposed system achieves a high performance by exhibiting average performances very close to their notional amount.

**Table 3.** Average performance of NPCR (number of changing pixel rate) (%).

| Images | Lena Image | | | Baboon Image | | |
|---|---|---|---|---|---|---|
| | **R** | **G** | **B** | **R** | **G** | **B** |
| Proposed System | 99.615 | 99.62 | 99.617 | 99.6140 | 99.6073 | 99.6292 |
| [36] | 99.60 | 99.61 | 99.61 | 99.6083 | 99.6065 | 99.6094 |
| [37] | 99.60 | 99.60 | 99.60 | 99.6138 | 99.6053 | 99.6182 |
| [38] | 99.6119 | 99.6097 | 99.6136 | 99.5864 | 99.5864 | 99.5864 |

**Table 4.** Average performance of UACI (unified averaged changed intensity) (%).

| Images | Lena Image | | | Baboon Image | | |
|---|---|---|---|---|---|---|
| | **R** | **G** | **B** | **R** | **G** | **B** |
| Proposed System | 33.4732 | 33.3428 | 33.4647 | 33.4843 | 33.4690 | 33.4965 |
| [36] | 33.56 | 33.45 | 33.49 | 33.4939 | 33.4295 | 33.4856 |
| [37] | 33.369 | 33.43 | 33.37 | 33.4712 | 33.4265 | 33.4705 |
| [38] | 33.4811 | 33.4652 | 33.4907 | 33.4834 | 33.4639 | 33.2689 |

### *5.6. Information Entropy*

The information entropy, which reflects the insecurity of image data, was denoted by $E(m)$ of matrix $m$, and evaluated by

$$E(m) = -\sum_{i=0}^{255} P_b(m_i) \log_2(P_b(m_i)), \tag{12}$$

where $P_b(m_i)$ denotes the probability of $m_i$. An accurate random image would yield 256-pixel values with an identical probability. Therefore, the theoretical value of the information entropy is closer to 8. Table 5 illustrates that the entropy values of cipher images of Lena and baboon are close to the theoretical value. Therefore, the outcomes prove that the proposed cryptosystem can efficiently counterattack the information entropy.

**Table 5.** Information entropy.

| Images | Lena Image | | | Baboon Image | | |
|---|---|---|---|---|---|---|
| | **R** | **G** | **B** | **R** | **G** | **B** |
| Proposed System | 7.9973 | 7.9975 | 7.9975 | 7.9970 | 7.9978 | 7.9987 |
| [36] | 7.9971 | 7.9971 | 7.9971 | 7.9926 | 7.9926 | 7.9926 |
| [37] | 7.9819 | 7.9814 | 7.9829 | 7.9881 | 7.9871 | 7.9863 |
| [38] | 7.9973 | 7.9973 | 7.9973 | 7.9896 | 7.9896 | 7.9896 |

### *5.7. Avalanche Effect*

When minor variation in the plain image or the secret key occurs, it will influence variation in the ciphered image. This influence is defined as the avalanche effect. To evaluate the avalanche effect of the proposed cryptosystem, the mean square error was evaluated for the two different cipher images $\mathbf{C}_1$ and $\mathbf{C}_2$ obtained from a slight change in the secret keys. The MSE can be given by

$$\text{MSE} = \frac{1}{W} \sum_{i=1}^{M} \sum_{j=1}^{N} ((\mathbf{C}_1(i,j) - \mathbf{C}_2(i,j))^2, \tag{13}$$

where $W = M \times N$ is the dimension of cipher images.

From Equation (13), the MSE of the proposed encryption algorithm can be evaluated for cipher images using the original secret key and cipher images obtained by changing each element in the original secret key, as cited in Tables 6 and 7, for both the Lena and baboon images, respectively. Cipher $\mathbf{C}_1$ is obtained by changing only key $x_1$ and maintaining the other keys' values. Similarly, ciphers $\mathbf{C}_2$, $\mathbf{C}_3$, and $\mathbf{C}_4$ are generated by changing $x_2$, $x_3$, and $x_4$, respectively. The large values of MSE in Tables 6 and 7 indicate that the proposed cryptosystem has a strong avalanche effect.

**Table 6.** Mean square error (MSE) between cipher images of Lena.

| Images | $x_1$ | $x_2$ | $x_3$ | $x_4$ | MSE |
|---|---|---|---|---|---|
| Cipher $\mathbf{C}_1$ | $0.12 + 10^{-15}$ | 0.23 | 0.34 | 0.45 | 9.758 |
| Cipher $\mathbf{C}_2$ | 0.12 | $0.23 \times 10^{-15}$ | 0.34 | 0.45 | 9.614 |
| Cipher $\mathbf{C}_3$ | 0.12 | 0.23 | $0.34 \times 10^{-15}$ | 0.45 | 9.520 |
| Cipher $\mathbf{C}_4$ | 0.12 | 0.23 | 0.34 | $0.45 \times 10^{-15}$ | 9.6729 |

**Table 7.** MSE between cipher images of the baboon.

| Images | $x_1$ | $x_2$ | $x_3$ | $x_4$ | MSE |
|---|---|---|---|---|---|
| Cipher $\mathbf{C}_1$ | $0.12 \times 10^{-15}$ | 0.23 | 0.34 | 0.45 | 10.869 |
| Cipher $\mathbf{C}_2$ | 0.12 | $0.23 \times 10^{-15}$ | 0.34 | 0.45 | 10.725 |
| Cipher $\mathbf{C}_3$ | 0.12 | 0.23 | $0.34 \times 10^{-15}$ | 0.45 | 10.8432 |
| Cipher $\mathbf{C}_4$ | 0.12 | 0.23 | 0.34 | $0.45 \times 10^{-15}$ | 10.631 |

## 6. Conclusions

This article has presented a novel encryption and decryption algorithm for the purpose of verifying picture transmission over information correspondence frameworks. Both of them are indistinguishable with hybrid chaotic confusion procedures and the mtDNA diffusion process that diminish the equipment usage intricacy and improve framework security. The exhibited algorithm was shown to be powerful against chosen/known plain text attacks. The numerical investigations demonstrated that the proposed cryptosystem has a very large key space for opposing brute-force attacks and scrambled pixels appropriated haphazardly through the figured picture. Likewise, the proposed framework is sensitive to insignificant changes in the covert encryption key and can oppose the known plaintext, chosen plaintext, differential figure picture, and entropy attacks.

Finally, in terms of future research, we suggest additional simulation analysis of the chaotic performance by using a cosine chaotic model and another confusion technique to generate a robust chaotic image encryption technique with the addition of digital signature technology, for the sake of achieving more secure authenticated data transmission.

**Author Contributions:** Conceptualization, H.G.M. and K.H.M.; Methodology, D.H.E.; Software, K.H.M.; Validation, H.G.M., D.H.E. and K.H.M.; Formal Analysis, H.G.M.; Investigation, D.H.E.; Resources, K.H.M.; Data Curation, H.G.M.; Writing-Original Draft Preparation, H.G.M.; Writing-Review & Editing, D.H.E.; Visualization, D.H.E.; Supervision, K.H.M.; Project Administration, H.G.M. All authors have read and agreed to the published version of the manuscript.

**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. Liu, Z.; Guo, Q.; Xu, L.; Ahmad, M.A.; Liu, S. Double image encryption by using iterative random binary encoding in gyrator domains. *Opt. Express* **2010**, *18*. [CrossRef]
2. Wang, X.; Zhang, H.-L. A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems. *Nonlinear Dyn.* **2016**, *83*, 333–346. [CrossRef]
3. Ahmad, J.; Hwang, S.O. A secure image encryption scheme based on chaotic maps and affine transformation. *Multimed. Tools Appl.* **2016**, *75*, 13951–13976. [CrossRef]
4. Ahmad, J.; Khan, M.A.; Hwang, S.O.; Khan, J.S. A compression sensing and noise-tolerant image encryption scheme based on chaotic maps and orthogonal matrices. *Neural Comput. Appl.* **2017**, *28*, 953–967. [CrossRef]
5. Wang, X.-Y.; Zhang, Y.-Q. Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation. *Nonlinear Dyn.* **2014**, *77*, 687–698.
6. Guo, J.-S.; Jin, C.-H. An attack with known image to an image cryptosystem based on general cat map. *J. China Inst. Commun.* **2005**, *26*, 131–135.

7. Jolfaei, A.; Wu, X.-W.; Muthukkumarasamy, V. On the security of permutation-only image encryption schemes. *IEEE Trans. Inf. Forensics Secur.* **2015**, *11*, 235–246. [CrossRef]
8. Wang, X.; Zhu, X.; Zhang, Y. An image encryption algorithm based on Josephus traversing and mixed chaotic map. *IEEE Access* **2018**, *6*, 23733–23746. [CrossRef]
9. Askar, S.; Karawia, A.; Alshamrani, A. Image encryption algorithm based on chaotic economic model. *Math. Prob. Eng.* **2015**, *2015*, 341729. [CrossRef]
10. Abbas, N.A. Image encryption based on independent component analysis and arnold's cat map. *Egypt. Inform. J.* **2016**, *17*, 139–146. [CrossRef]
11. Shaikh, N.; Chapaneri, S.; Jayaswal, D. Hyper chaotic color image cryptosystem. In Proceedings of the 2016 IEEE International Conference on Advances in Computer Applications (ICACA), Coimbatore, India, 24–24 October 2016.
12. Li, C.; Zhao, F.; Liu, C.; Lei, L.; Zhang, J. A Hyperchaotic Color Image Encryption Algorithm and Security Analysis. *Secur. Commun. Netw.* **2019**, *2019*, 8132547. [CrossRef]
13. Ramasamy, P.; Ranganathan, V.; Kadry, S.; Damaševičius, R.; Blažauskas, T. An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic—Tent map. *Entropy* **2019**, *21*, 656. [CrossRef]
14. Watson, J.D.; Crick, F.H. Molecular structure of nucleic acids. *Nature* **1953**, *171*, 737–738. [CrossRef] [PubMed]
15. Ning, K. A pseudo DNA cryptography method. *arXiv* **2009**, arXiv:0903.2693.
16. Zhang, Q.; Guo, L.; Wei, X. Image encryption using DNA addition combining with chaotic maps. *Math. Comput. Modell.* **2010**, *52*, 2028–2035. [CrossRef]
17. Liu, H.; Wang, X. Image encryption using DNA complementary rule and chaotic maps. *Appl. Soft Comput.* **2012**, *12*, 1457–1466. [CrossRef]
18. Wei, X.; Guo, L.; Zhang, Q.; Zhang, J.; Lian, S. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. *J. Syst. Softw.* **2012**, *85*, 290–299. [CrossRef]
19. Zhang, Q.; Guo, L.; Wei, X. A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. *Opt. -Int. J. Light Electron Opt.* **2013**, *124*, 3596–3600. [CrossRef]
20. Huang, X.; Ye, G. An image encryption algorithm based on hyper-chaos and DNA sequence. *Multimed. Tools Appl.* **2014**, *72*, 57–70. [CrossRef]
21. Ur Rehman, A.; Liao, X.; Kulsoom, A.; Abbas, S.A. Selective encryption for gray images based on chaos and DNA complementary rules. *Multimed. Tools Appl.* **2015**, *74*, 4655–4677. [CrossRef]
22. Zhan, K.; Wei, D.; Shi, J.; Yu, J. Cross-utilizing hyperchaotic and DNA sequences for image encryption. *J. Electron. Imaging* **2017**, *26*, 013021. [CrossRef]
23. Kulsoom, A.; Xiao, D.; Abbas, S.A. An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules. *Multimed. Tools Appl.* **2016**, *75*, 1–23. [CrossRef]
24. Ran, W.; Wei, P.; Duan, A. Image encryption algorithm based on multi-chaotic mapping and DNA coding. *Comput. Eng. Des.* **2018**, *7*.
25. Wu, J.; Shi, J.; Li, T. A novel image encryption approach based on a hyperchaotic system, pixel-level filtering with variable kernels, and DNA-level diffusion. *Entropy* **2020**, *22*, 5. [CrossRef]
26. Sykes B (10 September 2003). "Mitochondrial DNA and Human History". The Human Genome. Well Come Trust. Available online: http://genome.wellcome.ac.uk/doc_WTD020876.html (accessed on 7 September 2015).
27. Johnston, I.G.; Williams, B.P. Evolutionary inference across eukaryotes identifies specific pressures favoring mitochondrial gene retention. *Cell Syst.* **2016**, *2*, 101–111. [CrossRef] [PubMed]
28. Anderson, S.; Bankier, A.T.; Barrell, B.G.; de Bruijn, M.H.; Coulson, A.R.; Drouin, J.; Eperon, I.C.; Nierlich, D.P.; Roe, B.A.; Sanger, F. Sequence and organization of the human mitochondrial genome. *Nature* **1981**, *290*, 457–465. [CrossRef] [PubMed]
29. Delsuc, F.; Stanhope, M.J.; Douzery, E.J. Molecular systematics of armadillos (Xenarthra, Dasypodidae): Contribution of maximum likelihood and Bayesian analyses of mitochondrial and nuclear genes. *Mol. Phylogenet. Evol.* **2003**, *28*, 261–275. [CrossRef]
30. Hassanin, A.; An, J.; Ropiquet, A.; Nguyen, T.T.; Couloux, A. Combining multiple autosomal introns for studying shallow phylogeny and taxonomy of Laurasiatherian mammals: Application to the tribe Bovini (Cetartiodactyla, Bovidae). *Mol. Phylogenet. Evol.* **2013**, *66*, 766–775. [CrossRef]

31. Li, C.-L.; Yu, S.-M. A new hyperchaotic system and its adaptive tracking control. *Acta Phys. Sin.* **2012**, *61*, 22–28.
32. Haskett, D.R. Mitochondrial DNA (mtDNA). Embryo Project Encyclopedia (2014-12-19). Available online: http://embryo.asu.edu/handle/10776/8269 (accessed on 28 January 2020).
33. Wang, Q.; Zhang, Q.; Zhou, C. A multilevel image encryption algorithm based on chaos and DNA coding. In Proceedings of the 2009 Fourth International on Conference on Bio-Inspired Computing (BICTA' 09), Beijing, China, 16–19 October 2009; pp. 70–74.
34. Sebastian, A.; Delson, T. Secure magnetic resonance image transmission and tumor detection techniques. In Proceedings of the 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT), Nagercoil, India, 18–19 March 2016.
35. 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]
36. 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]
37. Ur Rehman, A.; Liao, X.; Ashraf, R.; Ullah, S.; Wang, H. A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2. *Optik* **2018**, *159*, 348–367. [CrossRef]
38. Wu, X.; Wang, K.; Wang, X.; Kan, H.; Kurths, J. Color image DNA encryption using NCA map-based CML and one-time keys. *Signal Process.* **2018**, *148*, 272–287. [CrossRef]