Hindawi
Advances in Multimedia
Volume 2019, Article ID 7074264, 13 pages
https://doi.org/10.1155/2019/7074264

Research Article

A Color-Image Encryption Scheme Using a 2D Chaotic System and DNA Coding

Haidar Raad Shakir

University of Thi-Qar, Nasiriyah, Iraq

Correspondence should be addressed to Haidar Raad Shakir; haidar.raad@utq.edu.iq

Received 5 June 2019; Revised 26 September 2019; Accepted 8 November 2019; Published 25 November 2019

Academic Editor: Martin Reisslein

This paper proposes a method of encrypting images with password protection for secure sharing based on deoxyribonucleic acid (DNA) sequence operations and the tangent-delay ellipse reflecting the cavity-map system (TD-ERCS). The initial values of the TD-ERCS system are generated from a user's password, and the TD-ERCS system is used to scramble the pixel locations of the R, G, and B matrices of the original image. Next, three DNA-sequence matrices are generated by encoding the permuted color image such that it can be transformed into three matrices. Then, the TD-ERCS system is employed to generate three chaotic sequences before encoding the DNA into the three matrices. Thereafter, a DNA exclusive OR (XOR) operation is executed between the DNA sequences of the permuted image and the DNA sequences generated by the TD-ERCS system to produce three encrypted scrambled matrices. Finally, the matrices of the DNA sequences are decoded, and the R, G, and B channels are recombined to form an encrypted color image. The results of simulation and security tests reveal that the proposed algorithm offers robust encryption and demonstrates the ability to resist exhaustive, statistical, and differential attacks.

1. Introduction

With recent developments in technology and Internet-based activities, computer networks have fundamentally transformed human communication. Individuals can now join a variety of different networks to access and share various types of multimedia and data. However, online networks are not without risks, and due to the open nature of many networks, public concerns regarding the security and safety of data that is exchanged online are now higher than ever [1].

Digital images play a large role in multimedia communication, and thus, it is critical that appropriate mechanisms are in place to protect this information. Traditional block encryption approaches, such as AES, IDEA, and DES, can encrypt images effectively and ensure their safety to an extent. However, they cannot protect against transmission noise, which can be introduced to a digital image during the transmission process [2]. Therefore, research must be conducted to investigate algorithms that can provide increased protection via more comprehensive image encryption.

Developments in the field of chaos theory have created new opportunities for image-encryption techniques. Chaos-based image-encryption algorithms are fast and secure methods that offer many beneficial features, such as ergodicity, mixing, and strong sensitivity to initial conditions and system parameters [3]. Therefore, they represent promising encryption approaches that can potentially provide the protection required to enhance the security of images shared via digital networks.

Since the 1990s, scholars have observed a close correlation between cryptography and chaos [4], and chaos can potentially be employed within the permutation-diffusion architecture proposed by Mao, Guan, and Pareek et al. [5–7]. This architecture has attracted the interest of researchers worldwide and has led to the expansion of chaos-based encryption. Despite the fact that these procedures have demonstrated some advances, chaos-based encryption is still considered to be weak against known/chosen plaintext attacks [8]. A range of chaos-based innovations have emerged in this field, spanning various systems, including novel permutation techniques [9–13], new diffusion approaches

[14, 15], hyperchaotic map systems [16, 17], a simultaneous image encryption-compression scheme [18, 19], and novel transform domains [20, 21].

However, many of these image-encryption schemes have been deciphered without knowing the secret keys. For instance, the chaos-based encryption in [4] is still reported to be weak against known/chosen plaintext attacks [22]. In addition, a cryptographic analysis has been introduced in [23] to break a chaotic encryption scheme that employs autoblocking and electrocardiography, which produces a sequence of random numbers using a logistic map and a 2D Arnold map. Furthermore, another chaotic image cryptanalysis scheme based on image entropy has been proposed in [24]; however, it still retains the insecurity issues of the chaotic image cryptosystem.

One area of particular interest is deoxyribonucleic acid (DNA) coding-based cryptosystem. These revolutionary approaches to encryption exploit the vast storage space, immense parallelism, and ultralow power consumption of DNA computing [25]. Given the significant potential of this area, researchers have studied a range of cryptosystem that combine chaos theory with DNA encoding [26–37]. In [27, 30, 31, 33], a logistic map and its variants were employed as key stream generators, whereas hyperchaotic systems within a DNA coding collaboration are introduced in [26, 28, 29, 32, 35, 37]. The logistic map has some drawbacks for information encryptions, such as small key space, insufficient complexity, and low security, which allow easy decryption of the encryption schemes [38]. Hyperchaotic systems within a DNA coding method have proven to be insecure by proposing a chosen plaintext attack method by Feng and He [39].

To overcome this problem, this paper proposes a new image-encryption approach that employs secure image sharing based on DNA-sequence operations and tangent-delay ellipse reflecting cavity-map system (TD-ERCS) maps. The TD-ERCS system is used as chaotic map for its complexity and has proved to be immune against differential attacks [40]. The preliminary values for the TD-ERCS system are produced by calculating SHA-256 from a user's password. The encryption approach employs diffusion and confusion. The generated TD-ERCS system is used to permute the positions of the pixels in the original image, thereby confusing it. Subsequently, the permuted image is DNA encoded before the TD-ERCS system and DNA encoding are employed to generate a mask image. Next, DNA XOR is performed between the mask image and permuted image to generate the scrambled image. Finally, DNA decoding is applied to the scrambled image to generate an encrypted image and, in doing so, achieve diffusion.

The remainder of this paper is organized as follows: Section 2 provides preliminaries, while Section 3 introduces the encryption scheme. Section 4 presents the experimental results and discussion, and Section 5 concludes the paper.

2. Preliminaries

In this section, a brief discussion of the TD-ERCS system and DNA sequences is provided.

2.1. Tangent-Delay Ellipse Reflecting Cavity-Map System. In 2004, Ke-Hui and Chuan-Bing developed a novel chaotic system named TD-ERCS [41]. TD-ERCS is a special two-dimensional map based on a physical model of an elliptical reflecting cavity. The system fulfills certain criteria, such as a maximum Lyapunov exponent greater than zero, zero correlation over the entire field, and unchangeable equiprobability [42]. The TD-ERCS can be mathematically described as follows [43]:

$$
\begin{aligned}
X_n &= \frac{2K_{n-1}Y_{n-1} + X_{n-1}\left(\mu^2 - K_{n-1}^2\right)}{\mu^2 + K_{n-1}^2},\\
Y_n &= K_{n-1}\left(X_n - X_{n-1}\right) + Y_{n-1},\\
K_n &= \frac{K'_{n-m} - K_{n-1} + K_{i-1}\left(\left(K'_{n-m}\right)^2\right)}{1 + 2K'_{n-1}K_{n-1} - K\left(K'_{n-j}\right)^2},\\
K'_{i-j} &= \begin{cases} -\dfrac{X_{n-1}}{Y_{n-1}} \times \mu^2, & \text{if } n < m,\\ -\dfrac{X_{n-m}}{Y_{n-m}} \times \mu^2, & \text{if } n \geq m. \end{cases}\\
Y_0 &= \mu \times \sqrt{1 - X_0^2},\\
K'_0 &= \frac{X_0}{Y_0} \times \mu^2,\\
K_0 &= -\frac{\tan\alpha + K'_0}{1 - K'_0 \tan\alpha},
\end{aligned}
\tag{1}
$$

where x_0, μ, α, and j are the initial or seed parameters of the TD-ERCS. The seed parameters in the TD-ERCS are as follows: $\mu \in [0, 1]$, $x_0 \in [-1, 1]$, and $\alpha \in [0, \pi]$ and the tangent-delay parameters m ($m = 1, 2, 3, 4, 5, 6, \ldots$). Figure 1 illustrates the iterations of continuous chaotic systems. The plots are generated by the TD-ERCS with initial parameters $\mu = 0.3324$, $x_0 = 0.2456$, $\alpha = 2.143$, and $m = 2$ and with $n = 2{,}500$ iterations.

2.2. DNA-Sequence Operations

2.2.1. DNA Encoding and Decoding. DNA is a biological material present in nearly all living organisms. Parents' DNA is transmitted to a child, thus causing the child to inherit the parents' features. In humans, DNA is shaped like a twisted ladder and contains four nucleobases: adenine (A), cytosine (C), guanine (G), and thymine (T) [44]. Watson and Crick published an article in 1953 [45] that presented the DNA complementary rule. This rule states that adenine (A) bonds with thymine (T) and that guanine (G) bonds with cytosine (C). Figure 2 illustrates the structure of DNA.

A computer system deals with binary numbers and is composed of two numbers only: 0 and 1 that can be opposite or complementary. For instance, numbers 00 and 11 are complementary, as are 01 and 10. The four DNA bases A, C, G, and T are used to represent a binary sequence of 00, 11, 10, and 01, respectively, in the DNA sequence. Eight coding rules convert the binary sequence into DNA code, as demonstrated in Table 1 [46].

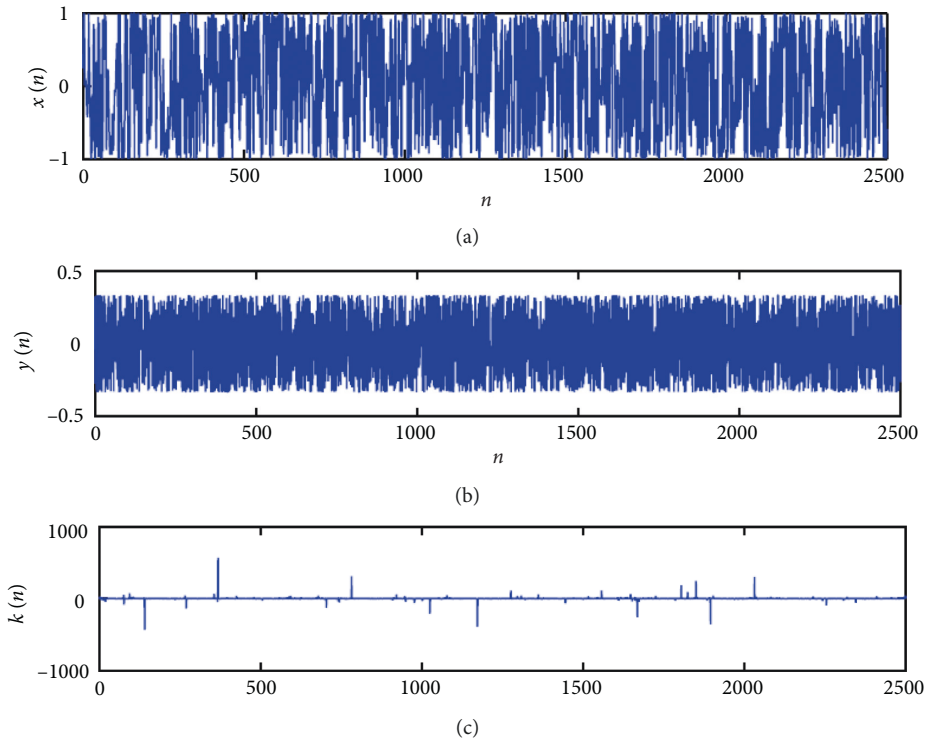


Figure 1: Time responses of TD-ERCS for initial parameters ($x_0 = 0.2456$, $\mu = 0.3324$, $\alpha = 2.143$, and $m = 2$).

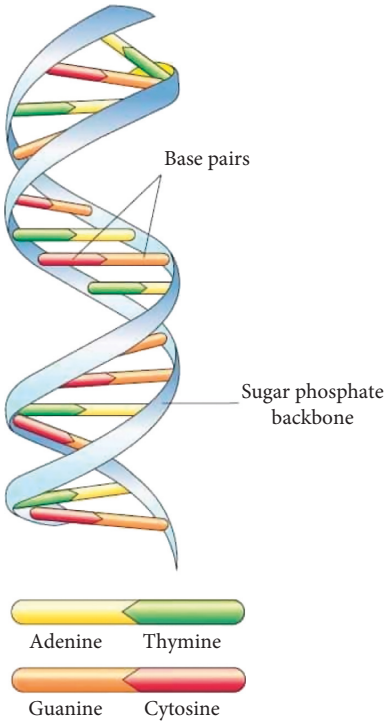


Figure 2: Structure of DNA (Image source: US National Library of Medicine).

A digital image comprises pixels of intensities in the range of 0 to 255. For an image pixel to be displayed, it is first transformed into a binary sequence of length 8 and then expressed as a DNA sequence of length 4. For instance, if the image pixel value is 89 (binary sequence: 01011001), it can be encoded into a DNA sequence (AATA) according to encoding rule #3.

Table 1: DNA encoding rules.

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

2.2.2. DNA Exclusive OR Operation. Due to the rapid development of DNA computing, several biological and algebraic operations have been proposed for DNA sequences, such as the XOR operation [47]. This operation is executed for a DNA sequence in the same way as a traditional XOR operation is executed in a binary sequence. Because there are eight DNA encoding rules, there are also eight DNA XOR rules. Table 2 presents the DNA XOR operations [48].

3. Proposed Algorithm

The encryption algorithm in this paper comprises two components: encryption and decryption. The algorithm has a pair of chaotic sequences (x, y) created by employing a TD-ERCS and three generated chaotic sequences: x, y, and z from a single map. In this study, x and y were used for position scrambling and x, y, and z were used for pixel

Table 2: DNA XOR operations.

XOR	A	G	C	T
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

scrambling via the DNA XOR method. Figure 3 illustrates the proposed encryption and decryption schemes.

3.1. Key Generation. The proposed encryption scheme employs a user's password to generate secret keys. First, SHA-256 is used to generate a message digest of 256 bits for the password. The 64 hash values of the message digest are then divided into eight hexadecimal groups: k_1, k_2, ..., k_8. Each group contains eight hexadecimal values and is converted into a floating decimal number via the following equation:

$$d_j = \frac{\text{hex 2dec}\,(k_1, k_2, \ldots, k_8)}{2\,\hat{}\,10}, \tag{2}$$

where $j = 1, 2, \ldots, 8$. The first set of the TD-ERCS initial values (μ, x_0, α, and m) is computed by

$$\begin{aligned} x_o &= \text{sign}\,(d_1 - d_2) \times d_1 \bmod 1, \\ \mu &= d_2 \bmod 1, \\ \alpha &= d_3 \bmod \pi, \\ m &= d_4 \bmod 10. \end{aligned} \tag{3}$$

The second set of initial values (μ, x_0, α, and m) for the TD-ERCS system is calculated as

$$\begin{aligned} x_o &= \text{sign}\,(d_1 - d_2) \times d_5 \bmod 1, \\ \mu &= d_6 \bmod 1, \\ \alpha &= d_7 \bmod \pi, \\ m &= d_8 \bmod 10. \end{aligned} \tag{4}$$

3.2. Image Encryption. The process of encryption involves the following steps:

Step 1. Conversion of the original color image to three matrices: R(m, n), G(m, n), and B(m, n).

Step 2. Generation of a pair of chaotic sequences, $x_{\text{new}} = (x_1, x_2, \ldots, x_{mn})$ and $y_{\text{new}} = (y_1, y_2, \ldots, y_{mn})$, via a TD-ERCS chaotic map. This uses the starting values μ, x_0, α, and m, as described in Section 3.1.

Step 3. Use of the method outlined below to prepare the x and y chaotic sequences:

$$\begin{aligned} [ly, fy] &= \text{sort}\,(X_{\text{new}}), \\ [ly, fy] &= \text{sort}\,(Y_{\text{new}}), \end{aligned} \tag{5}$$

where [•, •] = sort, (•) represents the type of index function, fx represents the new series of the X sequence, lx represents the index value of fx, and ly is equal to lx.

Step 4. Application of the combination (x_{new}, y_{new}) for scrambling R, G, and B positions using

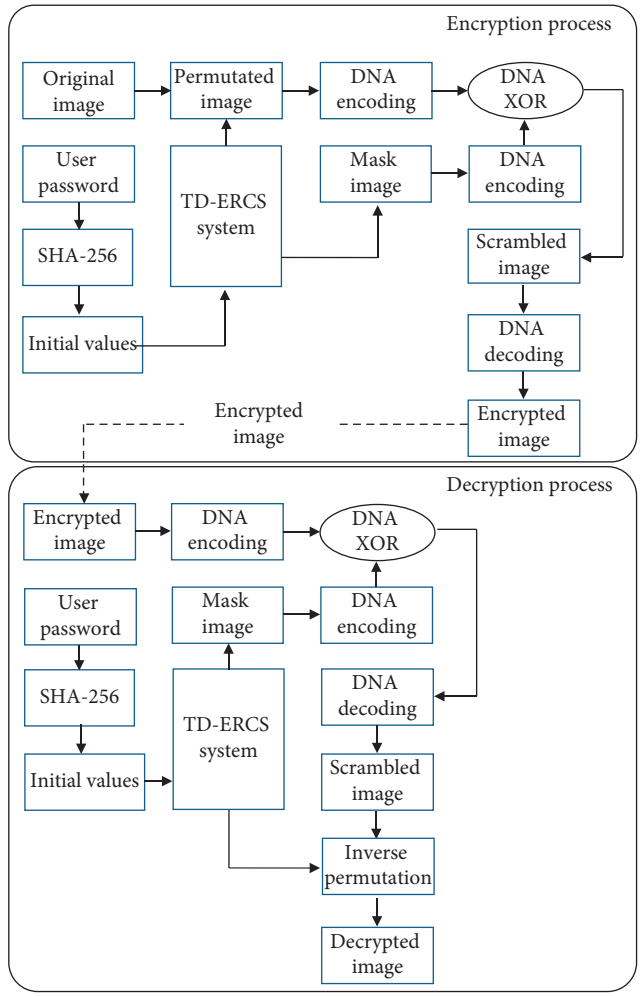


Figure 3: Encryption and decryption in the proposed scheme.

$$\begin{aligned} R_{\text{new}}(i, j) &\longleftrightarrow \text{R}(lx(i), ly(j)), \\ G_{\text{new}}(i, j) &\longleftrightarrow \text{G}(lx(i), ly(j)), \\ B_{\text{new}}(i, j) &\longleftrightarrow \text{B}(lx(i), ly(j)). \end{aligned} \tag{6}$$

Step 5. Conversion of R_{new}, G_{new}, and B_{new} to binary matrices. DNA encoding is then employed to encode these binary matrices, as detailed in Section 2.1. This results in three remodeled coding matrices: R_{dna}, G_{dna}, and B_{dna}, sized (m, $n \times 4$).

Step 6. Generation of three chaotic sequences $X_n = (x_1, x_2, \ldots, x_{mn})$, $Y_n = (y_1, y_2, \ldots, y_{mn})$, and $Z_n = (z_1, z_2, \ldots, z_{mn})$ via a TD-ERCS chaotic map. This uses the starting values of the second set, μ, x_0, α, and m, as detailed in Section 3.1. Then, these generated values are converted into a range from 0 to 256 according to

$$\begin{aligned} X_e(k) &= \text{round}\,(\text{abs}\,(X_i(k)) \times 1000 \bmod 256), \\ Y_e(k) &= \text{round}\,(\text{abs}\,(Y_i(k)) \times 500 \bmod 256), \\ Z_e(k) &= \text{round}\,(\text{abs}\,(Z_i(k)) \times 1000 \bmod 256), \end{aligned} \tag{7}$$

where k ranges from 0 to $M \times N$. Thus, the mask image is generated.

Step 7. Conversion of X_e, Y_e, and Z_e to binary matrices. DNA encoding is then employed to encode these matrices. This results in three remodeled coding matrices: X_{dna}, Y_{dna}, and Z_{dna}, sized (m, n ×4).

Step 8. Execution of the DNA XOR operation among (R_{dna} and X_{dna}), (G_{dna} and Y_{dna}), and (B_{new} and Z_{dna}). This results in three encrypted matrices: R_c, G_c, and B_c.

Step 9. Generation of the final encrypted image by performing a DNA decoding operation for R_c, G_c, and B_c. This results in three new matrices with values ranging from 0 to 255: R_{enc}, G_{enc}, and B_{enc}.

3.3. Image Decryption. The image decryption steps are as follows:

Step 1. Conversion of encrypted color image to three matrices: R(m, n), G(m, n), and B(m, n).

Step 2. Conversion of R, G, and B to binary matrices. DNA encoding is then employed to encode these binary matrices, as detailed in Section 2.1. This results in three remodeled coding matrices: R_{dna}, G_{dna}, and B_{dna}, sized (m, n ×4).

Step 3. Generation of three chaotic sequences $X_i = (x_1, x_2, \ldots, x_{mn})$, $Y_i = (y_1, y_2, \ldots, y_{mn})$, and $Z_i = (z_1, z_2, \ldots, z_{mn})$ via a TD-ERCS chaotic map. This employs the starting values of the second set, μ, x_0, α, and m, as discussed in Section 3.1. The generated values are then converted into range of 0 to 256 according to

$$\begin{aligned} X_e(k) &= \text{round}\left(\text{abs}\left(X_i(k)\right) \times 1000 \bmod 256\right), \\ Y_e(k) &= \text{round}\left(\text{abs}\left(Y_i(k)\right) \times 500 \bmod 256\right), \\ Z_e(k) &= \text{round}\left(\text{abs}\left(Z_i(k)\right) \times 1000 \bmod 256\right), \end{aligned} \tag{8}$$

where k ranges from 0 to $M \times N$. Thus, the mask image is generated.

Step 4. Conversion of X_e, Y_e, and Z_e to binary matrices. Then, DNA encoding is employed to encode these matrices. This results in three remodeled coding matrices: X_{dna}, Y_{dna}, and Z_{dna}, sized (m, n ×4).

Step 5. Execution of the DNA XOR operation among (R_{dna} and X_{dna}), (G_{dna} and Y_{dna}), and (B_{dna} and Z_{dna}). This results in three decrypted matrices: R_d, G_d, and B_d.

Step 6. Generation of a pair of chaotic sequences, $x_{\text{new}} = (x_1, x_2, \ldots, x_{mn})$ and $y_{\text{new}} = (y_1, y_2, \ldots, y_{mn})$, via a TD-ERCS chaotic map. This uses the first set of starting values, μ, x_0, α, and m, as detailed in Section 3.1.

Step 7. Use of the method outlined below to prepare the x and y chaotic sequences:

$$\begin{aligned} [lx, fx] &= \text{sort}\left(X_{\text{new}}\right), \\ [ly, fy] &= \text{sort}\left(Y_{\text{new}}\right), \end{aligned} \tag{9}$$

where [•, •] = sort, (•) represents the type of index function, fx represents the new series of the X sequence, lx represents the index value of fx, and ly is equal to lx.

Step 8. Application of the combination (x_{new}, y_{new}) for recovering R_d, G_d, and B_d positions using

$$\begin{aligned} \text{R}_{\text{dec}}(i, j) &\longleftrightarrow \text{R}_d(lx(i), ly(j)), \\ \text{G}_{\text{dec}}(i, j) &\longleftrightarrow \text{G}_d(lx(i), ly(j)), \\ \text{B}_{\text{dec}}(i, j) &\longleftrightarrow \text{B}_d(lx(i), ly(j)). \end{aligned} \tag{10}$$

Then, the final decrypted image is constructed by recombining these three matrices into a color image.

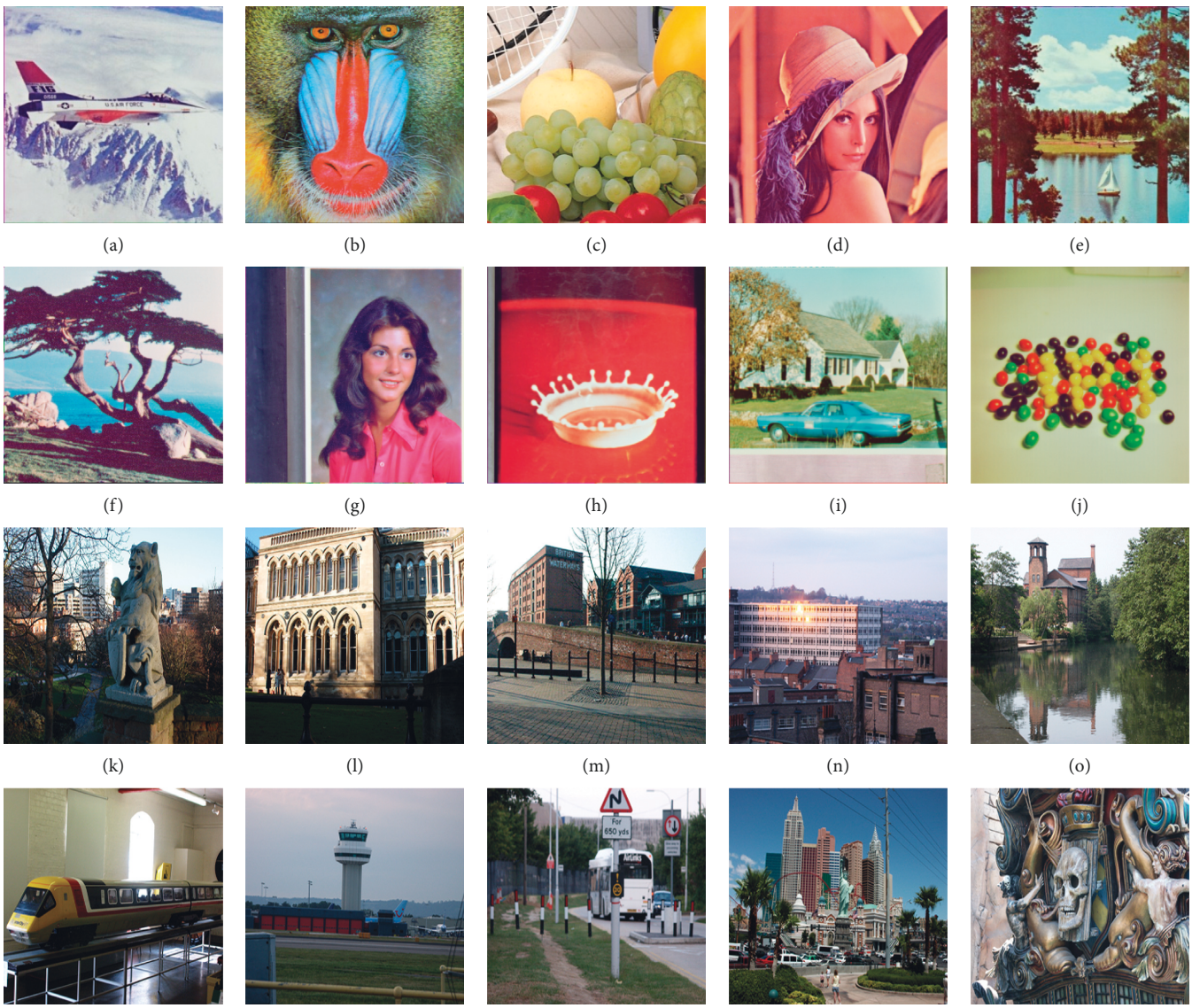
4. Simulation Results

Twenty color images of 512 × 512 pixels each were selected from the USC-SIPI image database (the USC-SIPI image database is available at http://sipi.usc.edu/services/database/Database.html) and UCID image database (the UCID image dataset is available at http://homepages.lboro.ac.uk/cogs/datasets/ucid/data/ucid.v2.tar.gz.) for testing. Figure 4 displays the images. The first two rows show the USC-SIPI images, and the next two rows show the UCID images. Performance analysis was performed for the proposed encryption scheme in terms of histogram analysis, correlation coefficient analysis, and differential attack resistance using the number of pixels change rate (NPCR) and the unified average changing intensity (UACI). Simulation experiments were performed on a personal computer with Intel Core i7-6500U, 3.0 GHz, 4 GB using Matlab R2017a and the Windows 10 operating system.

4.1. Key Space Analysis. For a secure cryptosystem, the key space must be large enough to withstand all kinds of brute-force attacks. Furthermore, the key space of the proposed encryption scheme is represented by the TD-ERCS seed parameters. If the precision is set to 10^{-15} for all the parameters, the key space size is 10^{90}. This key space is large enough to resist brute-force attacks.

4.2. Histogram Analysis. Histograms of an image are used to represent the pixel distribution for each color intensity level. An ideal image-encryption algorithm produces a histogram of the encrypted image with a uniform distribution. The histograms of the original and encrypted image (Lena) are displayed in Figures 5(a)–5(d) for the red, green, and blue components, respectively. It should be noted that the histograms of encrypted images are flat and thus differ from the original images. Therefore, the proposed encryption scheme can resist statistical attacks.

4.3. Mean-Square Errors and Peak Signal-to-Noise Ratio. The peak signal-to-noise ratio (PSNR) and mean-square error (MSE) are two error measures that are widely used for comparing image quality. The MSE refers to the cumulative square error between the original image and encrypted image. The higher the value of the MSE, the higher the probability that the encrypted images are distorted and noisy. The MSE can be calculated according to



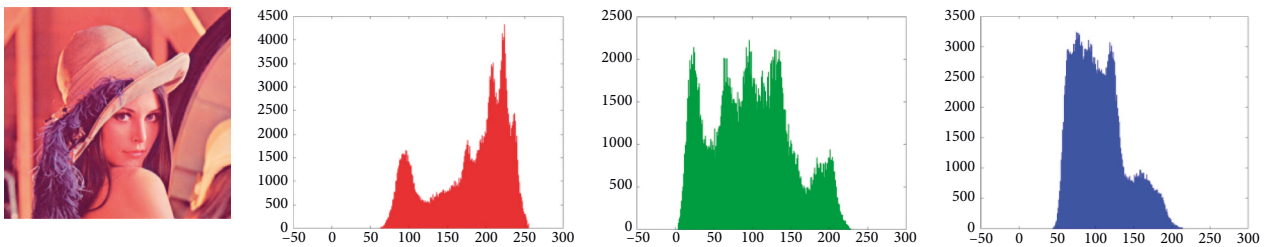
(a) (b) (c) (d) (e)

(f) (g) (h) (i) (j)

(k) (l) (m) (n) (o)

(p) (q) (r) (s) (t)

Figure 4: Image test set: (a) airplane; (b) baboon; (c) fruits; (d) Lena; (e) sailboat; (f) tree; (g) female; (h) splash; (i) house; (j) jelly beans; (k) ucid00010; (l) ucid00031; (m) ucid00182; (n) ucid00338; (o) ucid00463; (p) ucid00487; (q) ucid00586; (r) ucid00598; (s) ucid00779; (t) ucid00885.



(a) (b) (c) (d)

Figure 5: Continued.

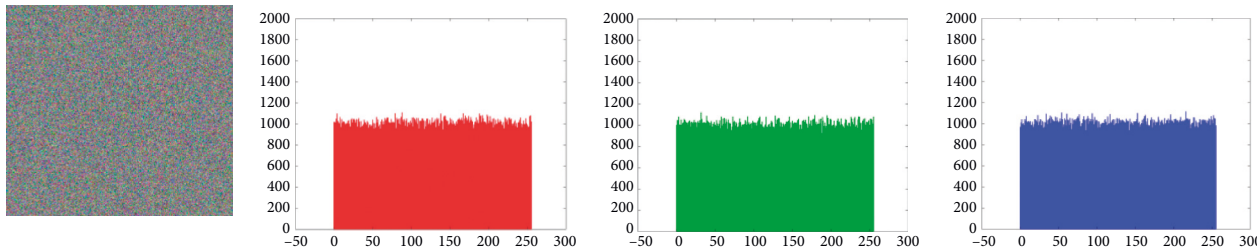


Figure 5: (a) Original image. (b–d) Histograms of the R, G, and B channels of the original image, respectively. (e) Encrypted image. (f–h) Histograms of the R, G, and B channels of the encrypted image, respectively.

$$\text{MSE} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} [x(i,j) - y(i,j)]^2, \tag{11}$$

where $x(i, j)$ refers to the original image, $y(i, j)$ refers to the encrypted image, and (i, j) refers to the coordinates of the image pixels of size $M \times N$.

The PSNR represents the noise ratio between the original image and the encrypted image and is measured in decibels (dB). Low PSNR values indicate that the encryption scheme results in high degradation of the encrypted images. Equation (12) is used to calculate the PSNR:

$$\text{PSNR} = 10 \log_{10} \left[\frac{(I_{\max})^2}{\text{MSE}} \right], \tag{12}$$

where $I_{\max}$ is the maximum intensity of the image. For an 8-bit image, $I_{\max}$ is set to 255. Table 3 displays the computed MSE and PSNR values for the test images.

These results demonstrate that the proposed encryption scheme can produce ciphered images with high degradation.

Table 3: PSNR and MSE test values.

Image	MSE	PSNR
Airplane	10344	7.9841
Baboon	8608	8.7816
Lena	8948	8.6133
Fruits	10053	8.1077
Sailboat	10053	8.1078
Tree	9917	8.1666
Female	8488	8.8425
Jelly beans	8879	8.6471
House	9218	8.4843
Splash	11245	7.6211
ucid00010	12725	7.0841
ucid00031	13282	6.8980
ucid00182	10910	7.7522
ucid00338	11402	7.5606
ucid00463	10584	7.8843
ucid00487	10878	7.7650
ucid00586	9285	8.4526
ucid00598	10008	8.1273
ucid00779	9051	8.5636
ucid00885	9108	8.5364

4.4. Correlation Coefficient Analysis. Correlation refers to the linear relation between two variables. For images, it is used to indicate the relation between two adjacent pixels. Normally, plain images possess a high correlation between adjacent pixels. Thus, a secure encryption scheme should reduce the correlation between adjacent encrypted image pixels to resist a statistical analysis attack. To evaluate the correlation between two adjacent pixels, 4,000 pairs of neighboring pixels in the vertical, horizontal, and diagonal directions were randomly selected from a plain image and corresponding encrypted image. The correlation coefficient was computed according to

$$\begin{aligned} r_{xy} &= \frac{|\text{cov}(x,y)|}{\sqrt{D(x)} \times \sqrt{D(y)}}, \\ \text{Cov}(x,y) &= \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)), \\ E(x) &= \frac{1}{N} \sum_{i=1}^{N} x_i, \\ D(x) &= \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2, \end{aligned} \tag{13}$$

where (r_{xy}) is the correlation coefficient, x and y are the gray-level values of two adjacent pixels, N is the number of pairs (x_i, y_i), $E(x)$ is the x_i mean, and $E(y)$ is the y_i mean. Figure 6 illustrates the correlation coefficient for the original image (airplane) and the corresponding encrypted image. The correlation coefficient was computed for all test images vertically, horizontally, and diagonally; Table 4 provides the results. The results reveal that the correlation coefficient of the encrypted images is close to zero or negative. Therefore, there is no correlation between adjacent image pixels.

Along with this analysis, the proposed scheme was compared to two representative methods from other schemes [34, 35, 49, 50]; Table 5 presents the correlation coefficient results for the encrypted Lena image. The proposed scheme obtained results superior to those of the reference methods, as the encrypted image correlation coefficient values were smaller than those obtained by the reference methods.

4.5. Entropy Information. In information theory, entropy information is defined as the uncertainty of information content and can be used to measure the randomness of a data sequence. It is expressed as follows:

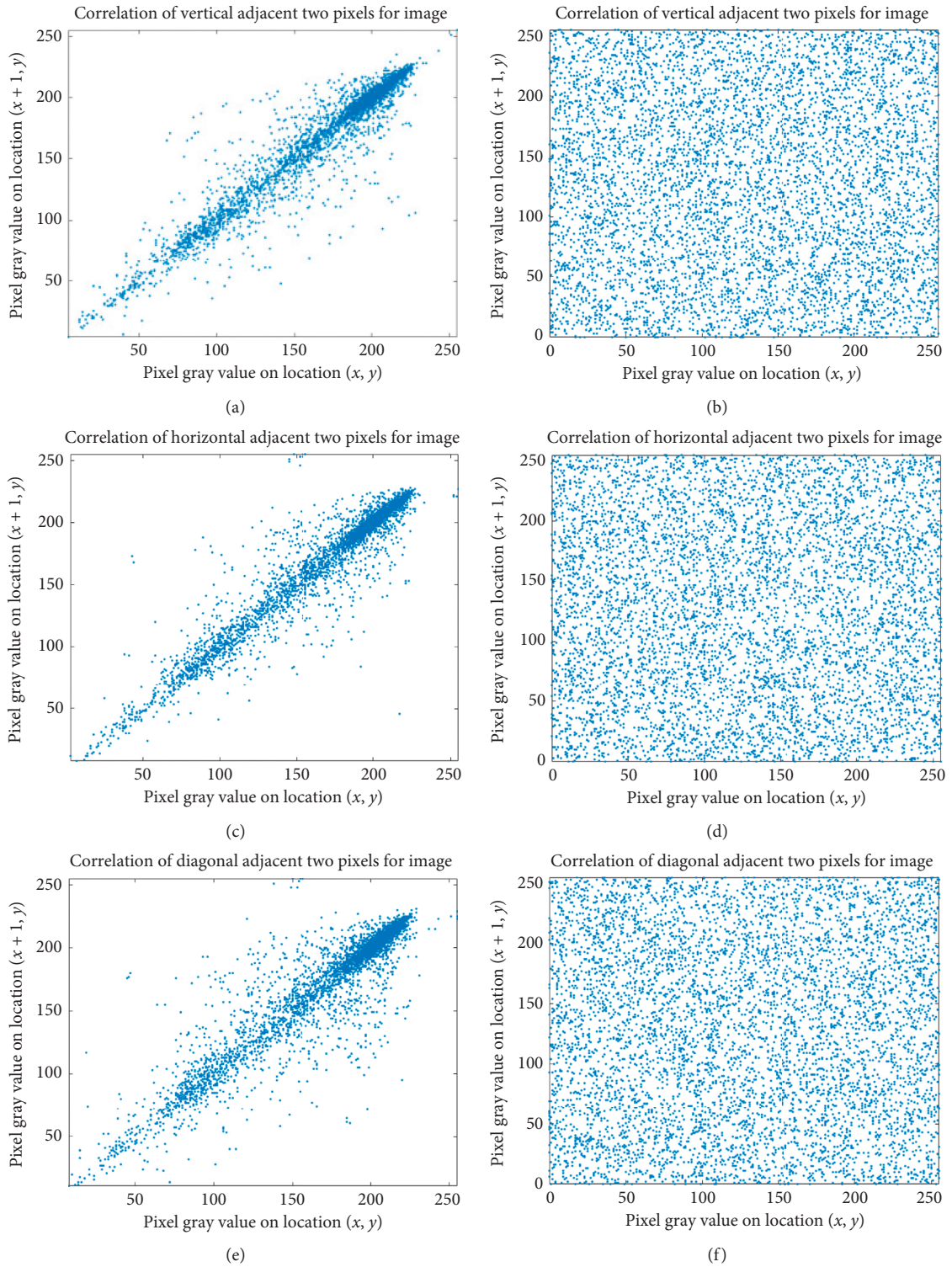


FIGURE 6: Correlation coefficient analysis. (a, c, e) Vertical, horizontal, and diagonal correlation coefficients for the original image, respectively. (b, d, f) Vertical, horizontal, and diagonal correlation coefficients for the encrypted image, respectively.

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i)\log_2\frac{1}{p(m_i)}, \tag{14}$$

where H is the image entropy and $p(m_i)$ refers to the probability of symbol m. For digital images with 2^8 pixels of, the maximum information entropy is 8. The higher the entropy value of the encrypted image, the more uniform the distribution. Table 6 presents the information entropy results. From these results, it is evident that the entropy values of the test images are very close to the ideal value. This indicates that the proposed encryption scheme is secure

Table 4: Correlation coefficients for original images and encrypted images.

Image name	Correlation for original image			Correlation for encrypted image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Airplane	0.96519	0.96099	0.93251	−0.00342	−0.00166	−0.00200
Baboon	0.92306	0.86595	0.85434	0.00266	−0.00242	−0.00250
Lena	0.97977	0.98931	0.96969	−0.00462	−0.00219	0.00201
Fruits	0.97260	0.97282	0.95225	0.00085	0.02700	−0.00509
Sailboat	0.95345	0.94605	0.92842	0.00109	0.00095	0.00130
Tree	0.96523	0.93955	0.92920	0.00144	−0.02213	−0.00419
Female	0.96279	0.98352	0.94419	−0.01329	0.00742	−0.00797
Jelly beans	0.97508	0.97863	0.95434	0.00287	0.01505	0.01359
House	0.95879	0.95913	0.92809	−0.01392	0.01166	−0.01338
Splash	0.99244	0.99398	0.98394	0.00230	0.02391	−0.02812
ucid00010	0.93665	0.94358	0.91250	−0.00403	−0.01216	0.00710
ucid00031	0.93081	0.95766	0.89533	0.00513	0.01206	−0.00590
ucid00182	0.94613	0.95460	0.92325	−0.02825	−0.00029	0.00553
ucid00338	0.97560	0.96944	0.95529	0.00681	−0.00466	−0.00789
ucid00463	0.96898	0.95896	0.94815	−0.00237	0.01745	−0.01583
ucid00487	0.98196	0.96627	0.94867	−0.00855	−0.00753	−0.00561
ucid00586	0.99514	0.98904	0.98802	0.01080	0.01380	−0.00716
ucid00598	0.98456	0.98680	0.96843	−0.00744	0.03222	0.01098
ucid00779	0.87867	0.87094	0.80665	0.00116	0.00311	−0.02112
ucid00885	0.93089	0.95192	0.90514	−0.00623	−0.01098	0.01196

Table 5: Correlation coefficient comparison for encrypted Lena image.

Correlation coefficient	Proposed scheme	Reference [34]	Reference [35]	Reference [49]	Reference [50]
Horizontal	−0.00462	0.0066	0.0082	0.0015	−0.0207
Vertical	−0.00219	0.0212	0.0032	0.0015	−0.0176
Diagonal	0.00201	0.0048	0.0150	0.0044	0.0168

Table 6: Entropy analysis for five images.

Image	Entropy		
	Red	Green	Blue
Airplane	7.999286	7.999365	7.999149
Baboon	7.999323	7.999323	7.999270
Lena	7.999282	7.999298	7.999352
Fruits	7.999246	7.999341	7.999371
Sailboat	7.999221	7.999214	7.999361
Tree	7.996742	7.997225	7.996865
Female	7.997256	7.997001	7.997404
Jelly beans	7.996850	7.997228	7.997331
House	7.999144	7.999349	7.999347
Splash	7.999128	7.999272	7.999319
ucid00010	7.997198	7.997213	7.996889
ucid00031	7.997182	7.997274	7.997245
ucid00182	7.997419	7.997017	7.997149
ucid00338	7.997002	7.997306	7.996904
ucid00463	7.996912	7.997032	7.997196
ucid00487	7.997106	7.997083	7.997457
ucid00586	7.997406	7.996624	7.996946
ucid00598	7.997462	7.997087	7.997495
ucid00779	7.997358	7.997134	7.996875
ucid00885	7.996809	7.996899	7.997134

against an entropy attack. In addition, Table 7 presents an average entropy analysis for the five images for the proposed method and the other reference methods from [36, 37, 43, 51]. The results indicate that the proposed scheme has superior performance, as demonstrated by its higher entropy values.

4.6. Differential Attack. Usually, the p attacker introduces a minor alteration (e.g., changing one pixel) to an unaltered image and, by doing so, creates a pair of cipher images that employ an identical encryption algorithm. The attacker then breaks into the cryptosystem by following the variations of this pair of encrypted images; this is referred to as a differential attack.

To examine what happens to an encrypted image when a single pixel is altered in the original image, the NPCR was calculated, as given in (15) and (16), and the UACI was computed, as given in (13):

$$\mathrm{NPCR}\left(C_1, C_2\right) = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{D\left(i,j\right)}{L} \times 100\%, \tag{15}$$

$$D\left(i,j\right) = \begin{cases} 0, & \text{if } C_1\left(i,j\right) = C_2\left(i,j\right), \\ 1, & \text{if } C_1\left(i,j\right) \neq C_2\left(i,j\right), \end{cases} \tag{16}$$

$$\mathrm{UACI}\left(C_1, C_2\right) = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\left|C_1\left(i,j\right) - C_2\left(i,j\right)\right|}{T \times L} \times 100\%, \tag{17}$$

where M represents the width of the encrypted image, N represents the height, L is the pixel number, and T is the

Table 7: Average entropy analysis for the proposed method and other reference methods.

Proposed scheme	Reference [36]	Reference [37]	Reference [43]	Reference [51]
7.999293	7.99718	7.99658	7.99325	7.999

Table 8: NPCR and UACI results.

Image	NPCR			UACI		
	Red (%)	Green (%)	Blue (%)	Red (%)	Green (%)	Blue (%)
Airplane	99.94	99.89	99.99	33.36	33.33	33.31
Baboon	99.97	99.99	99.95	33.20	33.19	33.11
Lena	99.70	99.71	99.69	33.20	33.25	33.27
Fruits	99.96	99.98	99.91	33.30	33.39	33.38
Sailboat	99.60	99.69	99.61	33.29	33.21	33.22
Tree	99.63	99.62	99.60	33.36	33.36	33.36
Female	99.79	99.75	99.77	33.31	33.37	33.38
Jelly beans	99.91	99.98	99.93	33.38	33.35	33.31
House	99.77	99.71	99.71	33.20	33.20	33.28
Splash	99.60	99.67	99.69	33.35	33.30	33.39
ucid00010	99.96	99.98	99.96	33.20	33.26	33.21
ucid00031	99.80	99.88	99.81	33.31	33.33	33.33
ucid00182	99.83	99.81	99.82	33.20	33.31	33.21
ucid00338	99.97	99.91	99.98	33.38	33.31	33.32
ucid00463	99.91	99.89	99.88	33.38	33.34	33.33
ucid00487	99.98	99.98	99.99	33.14	33.16	33.16
ucid00586	99.76	99.77	99.71	33.29	33.23	33.25
ucid00598	99.84	99.79	99.74	33.31	33.30	33.30
ucid00779	99.99	99.97	99.99	33.16	33.15	33.15
ucid00885	99.98	99.99	99.99	33.12	33.14	33.12

largest allowed pixel value for the image. The cipher images are represented by C_1 and C_2, which differ from the matching plain images by a single pixel. It is clear that if the differential attack is to be repelled via an effective cryptosystem, the UACI and NPCR values should be sizable.

In the numerical experiment that follows, the original image was encrypted. A single pixel was then selected at random from the image, and a small modification was performed. Then, the plain image was reencrypted with modifications employing identical means. The UACI RGB and NPCR RGB values were then calculated using a pair of cipher images. Table 8 presents the relevant data for these experiments. As Table 8 demonstrates, this methodology resulted in sizable UACI and NPCR levels. Thus, the proposed algorithm could detect minuscule alterations to the plaintext and was able to repel a differential attack.

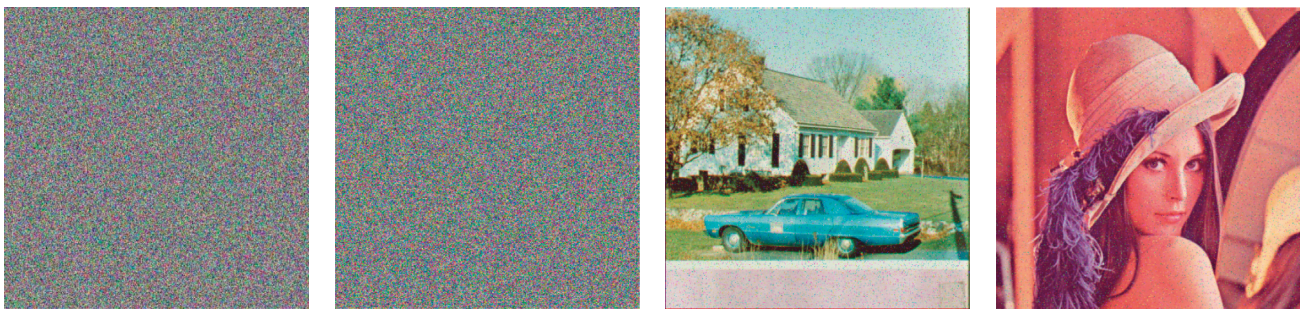
The proposed method was also compared with reference methods [36, 37, 43, 51] for the encrypted Lena image, as presented in Table 9. The NPCR and UACI values for the proposed method are superior, as they are higher than the values obtained using the reference methods.

Table 9: Comparison of NPCR and UACI between different schemes for the encrypted Lena image.

Scheme	NPCR (%)	UACI (%)
Reference [37]	99.61	33.32
Reference [36]	99.58	33.49
Reference [43]	99.65	33.44
Reference [51]	99.60	33.33
Proposed	99.70	33.24

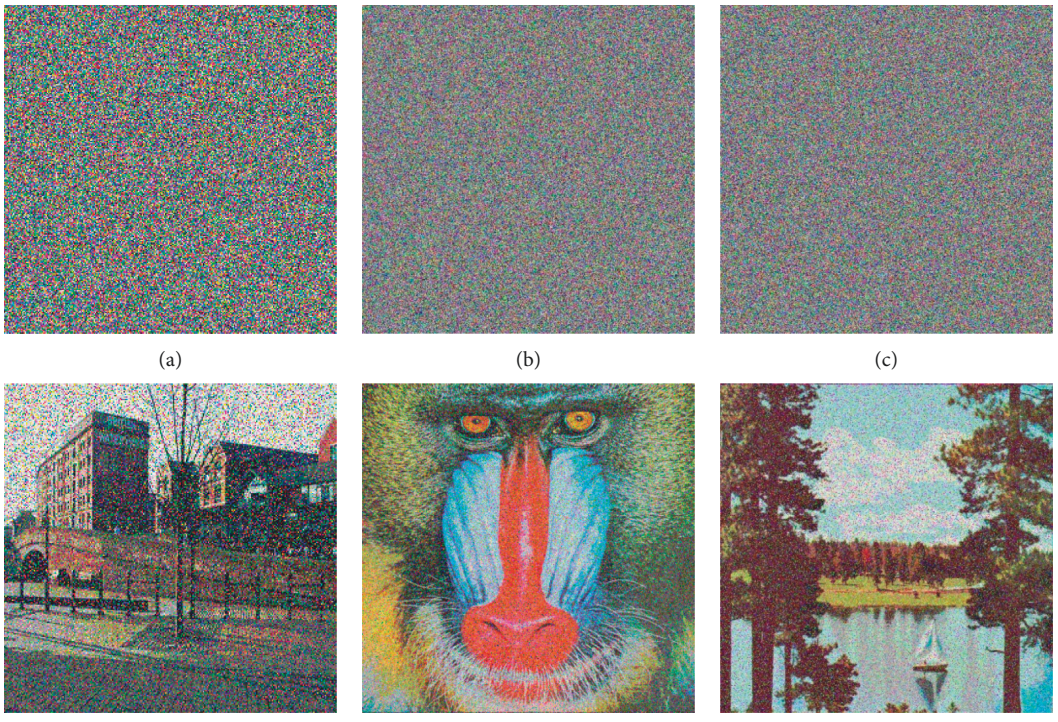
4.7. Analysis of Noise and Data Loss Attacks. There are several different types of noise existing in public multimedia channels such as Internet and wireless communication networks. Such noise belongs to a kind of attack that has no intentions; they decrease the image quality. Common types of noise include salt-and-pepper noise and Gaussian noise; they are different kinds of image noise. A wide range of noise is present in open interactive media channels such as wireless communication and the Internet. Such noise is a sort of attack that has no goals; it just distorts the image quality. Salt-and-pepper noise and Gaussian noise are the two types of image-noise attack. The experimental results in Figures 7 and 8 show the performance of the proposed algorithm after exposure to a noise attack. The experimental effect is illustrated in Figures 7 and 8; the top row shows the encrypted images after applying salt-and-pepper noise and Gaussian noise attacks on the test images. The bottom row shows the images reconstructed from the noisy images. Notably, the reconstructed images affected by the noise attack still retain most of the plain image information. These experimental outcomes prove that the proposed algorithm has excellent performance against noise attacks. The original images can be recovered even if the communication channel is noisy.

The test against a data loss attack is shown in Figure 9. The top rows show the encrypted images after cutting parts of them in different sizes and locations, and the bottom rows



(a) (b) (c) (d)

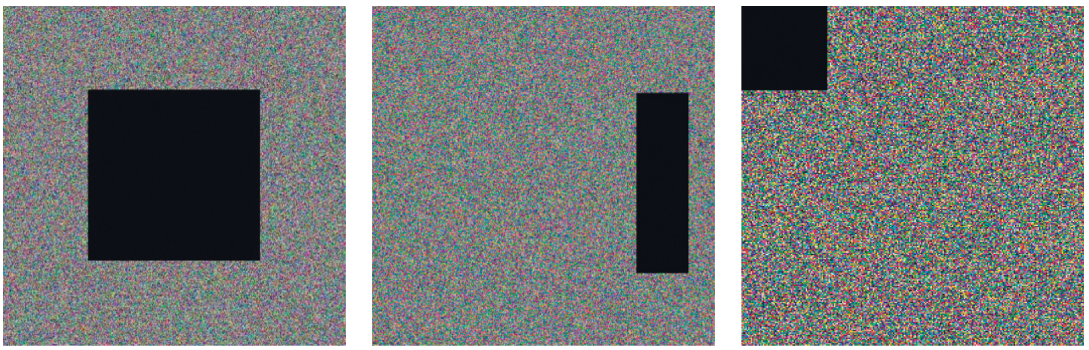
Figure 7: Salt-and-pepper noise attack.



(a) (b) (c)

(d) (e) (f)

Figure 8: Gaussian noise attack.



(a) (b) (c)

Figure 9: Continued.

(d) (e) (f)

Figure 9: Data loss attack.

show the reconstructed images after cropping. The reconstructed images after the attack obviously contain most of the original image data and can still be recognized.

5. Conclusion

In this paper, a new image-encryption algorithm is proposed using a TD-ERCS chaotic system, DNA-sequence operation, and Secure Hash SHA-256. From the above discussion, the positions of the image pixels are permuted by the TD-ERCS system, and the pixel gray values of the plain image are scrambled using DNA-sequence XOR operations. Based on the experimental results and security analysis, the efficiency of the algorithm encryption is found to be good. Furthermore, the proposed algorithm is able to resist most common attacks, such as statistical analysis, exhaustive attacks, differential attacks, and noise attacks. All these features make the algorithm efficient for secure digital image transmission.

Data Availability

The test image data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

References

[1] L. Y. Zhang, Y. Liu, F. Pareschi et al., "On the security of a class of diffusion mechanisms for image encryption," *IEEE Transactions on Cybernetics*, vol. 48, no. 4, pp. 1163–1175, 2018.

[2] G. Ye, "A block image encryption algorithm based on wave transmission and chaotic systems," *Nonlinear Dynamics*, vol. 75, no. 3, pp. 417–427, 2014.

[3] Y. Wu, J. P. Noonan, G. Yang, and H. Jin, "Image encryption using the two-dimensional logistic chaotic map," *Journal of Electronic Imaging*, vol. 21, no. 1, pp. 013014–013016, 2012.

[4] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and Chaos*, vol. 08, no. 6, pp. 1259–1284, 1998.

[5] Y. Mao, G. Chen, and S. Lian, "A novel fast image encryption scheme based on 3D chaotic baker maps," *International Journal of Bifurcation and Chaos*, vol. 14, no. 10, pp. 3613–3624, 2004.

[6] Z.-H. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," *Physics Letters A*, vol. 346, pp. 153–157, 2005.

[7] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, pp. 926–934, 2006.

[8] C. Li, Y. Zhang, and E. Y. Xie, "When an attacker meets a cipher-image in 2018: a year in review," *Journal of Information Security and Applications*, vol. 48, Article ID 102361, 2019.

[9] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Optics and Lasers in Engineering*, vol. 78, pp. 17–25, 2016.

[10] Z.-l. Zhu, W. Zhang, K.-w. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Information Sciences*, vol. 181, no. 6, pp. 1171–1186, 2011.

[11] V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, "A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption," *Optics Communications*, vol. 284, no. 19, pp. 4331–4339, 2011.

[12] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Optics and Lasers in Engineering*, vol. 90, pp. 238–246, 2017.

[13] J.-x. Chen, Z.-l. Zhu, C. Fu, H. Yu, and L.-b. Zhang, "An efficient image encryption scheme using gray code based permutation approach," *Optics and Lasers in Engineering*, vol. 67, pp. 191–204, 2015.

[14] N. K. Pareek, V. Patidar, and K. K. Sud, "Diffusion-substitution based gray image encryption scheme," *Digital Signal Processing*, vol. 23, no. 3, pp. 894–901, 2013.

[15] B. Norouzi, S. Mirzakuchaki, S. M. Seyedzadeh, and M. R. Mosavi, "A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process," *Multimedia Tools and Applications*, vol. 71, no. 3, pp. 1469–1497, 2014.

[16] B. Norouzi and S. Mirzakuchaki, "A fast color image encryption algorithm based on hyper-chaotic systems," *Nonlinear Dynamics*, vol. 78, no. 2, pp. 995–1015, 2014.

[17] H. Liu, A. Kadir, and Y. Li, "Asymmetric color pathological image encryption scheme based on complex hyper chaotic system," *Optik*, vol. 127, no. 15, pp. 5812–5819, 2016.

[18] H. Zhu, C. Zhao, and X. Zhang, "A novel image encryption-compression scheme using hyper-chaos and Chinese

remainder theorem," *Signal Processing: Image Communication*, vol. 28, no. 6, pp. 670–680, 2013.

[19] T. Zhang, S. Li, R. Ge, M. Yuan, and Y. Ma, "A novel 1D hybrid chaotic map-based image compression and encryption using compressed sensing and fibonacci-lucas transform," *Mathematical Problems in Engineering*, vol. 2016, Article ID 7683687, 15 pages, 2016.

[20] S. Liansheng, Z. Bei, N. Xiaojuan, and T. Ailing, "Optical multiple-image encryption based on the chaotic structured phase masks under the illumination of a vortex beam in the gyrator domain," *Optics Express*, vol. 24, no. 1, pp. 499–515, 2016.

[21] J. Lang, "Color image encryption based on color blend and chaos permutation in the reality-preserving multiple-parameter fractional fourier transform domain," *Optics Communications*, vol. 338, pp. 181–192, 2015.

[22] E. Y. Xie, C. Li, S. Yu, and J. Lü, "On the cryptanalysis of Fridrich's chaotic image encryption scheme," *Signal Processing*, vol. 132, pp. 150–154, 2017.

[23] C. Li, D. Lin, J. Lü, and F. Hao, "Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography," *IEEE MultiMedia*, vol. 25, pp. 46–56, 2018.

[24] C. Li, D. Lin, B. Feng, J. Lu, and F. Hao, "Cryptanalysis of a chaotic image encryption algorithm based on information entropy," *IEEE Access*, vol. 6, pp. 75834–75842, 2018.

[25] X. Zheng, J. Xu, and W. Li, "Parallel DNA arithmetic operation based on n-moduli set," *Applied Mathematics and Computation*, vol. 212, no. 1, pp. 177–184, 2009.

[26] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system," *Journal of Systems and Software*, vol. 85, no. 2, pp. 290–299, 2012.

[27] M. Babaei, "A novel text and image encryption method based on chaos theory and DNA computing," *Natural Computing*, vol. 12, no. 1, pp. 101–107, 2013.

[28] A. u. Rehman, X. Liao, R. Ashraf, S. Ullah, and H. Wang, "A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2," *Optik*, vol. 159, pp. 348–367, 2018.

[29] X. Chai, Z. Gan, Y. Lu, Y. Chen, and D. Han, "A novel image encryption algorithm based on the chaotic system and DNA computing," *International Journal of Modern Physics C*, vol. 28, no. 5, Article ID 1750069, 2017.

[30] A. Kulsoom, D. Xiao, A.-u. Rehman, and S. A. Abbas, "An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules," *Multimedia Tools and Applications*, vol. 75, no. 1, pp. 1–23, 2016.

[31] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," *Applied Soft Computing*, vol. 37, pp. 24–39, 2015.

[32] J. Kalpana and P. Murali, "An improved color image encryption based on multiple DNA sequence operations with DNA synthetic image and chaos," *Optik*, vol. 126, no. 24, pp. 5703–5709, 2015.

[33] M. T. Suryadi, Y. Satria, and M. Fauzi, "Implementation of digital image encryption algorithm using logistic function and DNA encoding," *Journal of Physics: Conference Series*, vol. 974, Article ID 012028, , 2018.

[34] L. Guo, J. Chen, and J. Li, "Chaos-Based color image encryption and compression scheme using DNA complementary rule and Chinese remainder theorem," in *Proceedings of the 2016 13th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, pp. 208–212, Chengdu, China, December 2016.

[35] X. Zhang, F. Han, and Y. Niu, "Chaotic image encryption algorithm based on bit permutation and dynamic DNA encoding," *Computational Intelligence and Neuroscience*, vol. 2017, Article ID 6919675, 11 pages, 2017.

[36] C. Song and Y. Qiao, "A novel image encryption algorithm based on DNA encoding and spatiotemporal chaos," *Entropy*, vol. 17, no. 12, pp. 6954–6968, 2015.

[37] S. Sun, "Chaotic image encryption scheme using two-by-two deoxyribonucleic acid complementary rules," *Optical Engineering*, vol. 56, Article ID 116117, 2017.

[38] C. Han, "An image encryption algorithm based on modified logistic chaotic map," *Optik*, vol. 181, pp. 779–785, 2019.

[39] W. Feng and Y.-G. He, "Cryptanalysis and improvement of the hyper-chaotic image encryption scheme based on DNA encoding and scrambling," *IEEE Photonics Journal*, vol. 10, no. 6, pp. 1–15, 2018.

[40] Y.-Y. Xiao, L.-Y. Sheng, J. Wen, and L.-L. Cao, "Differential cryptanalysis of TD-ERCS chaos," *Acta Physica Sinica*, vol. 56, pp. 78–83, 2007.

[41] S. L.-Y. S. Ke-Hui and L. Chuan-Bing, "Study of a discrete chaotic system based on tangent-delay for elliptic reflecting cavity and its properties," *Acta Physica Sinica*, vol. 9, p. 11, 2004.

[42] I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, "A novel image encryption algorithm based on chaotic maps and GF(28) exponent transformation," *Nonlinear Dynamics*, vol. 72, no. 1-2, pp. 399–406, 2013.

[43] J. S. Khan, J. Ahmad, and M. A. Khan, "Td-ercs map-based confusion and diffusion of autocorrelated data," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 93–107, 2017.

[44] S. Zhou, Q. Zhang, X. Wei, and C. Zhou, "A summarization on image encryption," *IETE Technical Review*, vol. 27, no. 6, pp. 503–510, 2010.

[45] J. D. Watson and F. H. C. Crick, "The structure of DNA," in *Cold Spring Harbor Symposia on Quantitative Biology*, pp. 123–131, Cold Spring Harbor Laboratory Press, Cold Spring Harbor, NY, USA, 1953.

[46] S. Som, A. Kotal, A. Chatterjee, S. Dey, and S. Palit, "A colour image encryption based on DNA coding and chaotic sequences," in *Proceeding of the 2013 1st International Conference on Emerging Trends and Applications in Computer Science*, pp. 108–114, Shillong, India, September 2013.

[47] A. ur Rehman, X. Liao, A. Kulsoom, and S. A. Abbas, "Selective encryption for gray images based on chaos and DNA complementary rules," *Multimedia Tools and Applications*, vol. 74, no. 13, pp. 4655–4677, 2015.

[48] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," *Optics and Lasers in Engineering*, vol. 56, pp. 83–93, 2014.

[49] H. Feng-ying and Z. Cong-xu, "An novel chaotic image encryption algorithm based on tangent-delay ellipse reflecting cavity map system," *Procedia Engineering*, vol. 23, pp. 186–191, 2011.

[50] Y. Niu, X. Zhang, and F. Han, "Image encryption algorithm based on hyperchaotic maps and nucleotide sequences database," *Computational Intelligence and Neuroscience*, vol. 2017, Article ID 4079793, 9 pages, 2017.

[51] L.-M. Zhang, K.-H. Sun, W.-H. Liu, and S.-B. He, "A novel color image encryption scheme using fractional-order hyperchaotic system and DNA sequence operations," *Chinese Physics B*, vol. 26, no. 10, Article ID 100504, 2017.