Hindawi
Security and Communication Networks
Volume 2021, Article ID 6650515, 18 pages
https://doi.org/10.1155/2021/6650515

Research Article

Nonlinear Multi-Image Encryption Scheme with the Reality-Preserving Discrete Fractional Angular Transform and DNA Sequences

Liang-Jia Tong,[1] Nan-Run Zhou ,[1] Zhi-Jing Huang,[1] Xin-Wen Xie ,[1,2,3] and Ya-Ru Liang[4]

[1]*Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China*
[2]*School of Electronic Engineering, Jiujiang University, Jiujiang 332005, China*
[3]*Xiexun Postdoctoral Practice Base, Xiexun Electronics Co., Ltd., Ji'an 343100, China*
[4]*School of Engineering, Jiangxi Agricultural University, Nanchang 330045, China*

Correspondence should be addressed to Xin-Wen Xie; xinwen.xie@jju.edu.cn

Received 2 December 2020; Revised 8 April 2021; Accepted 26 May 2021; Published 14 June 2021

Academic Editor: Zhiyuan Tan

A nonlinear multi-image encryption scheme is proposed by combining the reality-preserving discrete fractional angular transform with the deoxyribonucleic acid sequence operations. Four approximation coefficients of the four images are extracted by performing the two-dimensional lifting wavelet transform. Then, the four approximation coefficients are synthesized to generate a real-valued output with the reality-preserving discrete fractional angular transform. Finally, based on the deoxyribonucleic acid operation and the Logistic-sine system, the real-valued intermedium output will be encrypted to yield the final ciphertext image. To enhance the security of the image encryption algorithm, the initial value of the chaotic system is calculated by the 256-bit binary sequence, which is obtained by taking the statistics information of the plaintext images as the input of SHA-256. Deoxyribonucleic acid sequence operations, as nonlinear processes, could help to improve the robustness of the cryptosystem. Simulation results and security analysis demonstrate the effectiveness of the image encryption algorithm and the capability of withstanding various common attacks.

1. Introduction

Images can cover plentiful information and play an essential part in information transmission or processing. To enhance the security of private data in the rapidly developing digital age, more and more people focus on how to design an image encryption algorithm to prevent the leakage of original private information. In the past, many image encryption algorithms have been proposed with different techniques [1–11]. In the optical cryptosystem, since Refregier et al. first invented the double random phase encoding (DRPE) scheme, more DRPE-based algorithms have been developed [12–14]. Nevertheless, considering the inherent characteristic of linearity of these algorithms, DRPE-based cryptosystems still have the potential risk to be cracked with some special attacks [15–17]. In [18], based on the nonlinearity of phase-truncated Fourier transform (PTFT), Qin et al. explored an asymmetric cryptosystem to improve the weakness of linearity of the DRPE algorithms. The importance of the PTFT-based cryptosystem is undeniable. However, the encryption keys in this cryptosystem will be used as public keys and to encode plaintext. That is to say, known public keys and ciphertexts combined with an iterative amplitude-phase retrieval algorithm pose a great risk to this cryptosystem. Then, many nonlinear encryption schemes were applied to promote the reliability of the image cryptosystem [19–21].

In recent years, chaos-based image encryption algorithms have turned into one of the hot topics for their great dynamical performances. Image encryption algorithms combining mathematical transform with chaotic maps have been proposed successively for better security. Derived from one-dimensional (1D) chaotic maps, the Sine and Logistic maps, Hua et al. described the 2D Logistic-sine map and its

extension version, the 2D Logistic-adjusted-sine map, to encrypt images for higher robustness and lower time complexity [4, 22]. Besides, an image encryption algorithm that combined a 3D Logistic map with the electrocardiograph signal was presented by Ye et al. for a dynamic key [23]. In [24], Chen et al. proposed a single-channel optical asymmetric cryptosystem by encoding the RGB format of original images into the 2D format firstly and then employed the Ushiki chaotic system to generate the random phase mask in fractional Fourier transform (FrFT). In practice, given a situation with finite computing precision, the dynamical performance of the chaos-based cryptosystem will lower down. Thus, to reduce execution time on low-precision, Chen et al. proposed a new 2D hyperchaotic map, which was deduced from the Sine map, the Chebyshev map, and a linear function [25]. In addition, Wang et al. designed a method that conducts twice parallel diffusion in divided groups and bidirectional diffusion in the last two pixels of each group, which introduced a parallel model into diffusion operations [26]. Besides, for more efficient scrambling operation in chaos-based image encryption schemes, Xian and Wang explored a new square matrix with fractal properties in ordering (FSM), where the elements of this matrix can be generated iteratively and have a self-similar form [27].

Scrambling and diffusion operations in transform domains are effective tools for image encryption, such as the fractional Mellin transform (FrMT) [8], FrFT [9, 28], Fresnel transform [29, 30], and fractional angular transform (FrAT) [31, 32], in which the security of the key can be guaranteed with the use of additional parameters. The traditional Fourier transform is a special case of the FrFT, and Ozaktas et al. provided a detailed discussion about the FrFT in the book [33]. Based on the DRPE, Liu et al. explored the scrambling operation and the FrFT to compensate for possible plaintext attacks [28]. In the 2D-FrFT domain, Gao et al. proved the property of frequency shift-invariant, which presented in the magnitude of image restructuring from phase information. And this property is illustrated to enhance the robustness of image encryption [34]. Zhou et al. first introduced the FrMT into the field of image encryption to surmount the impuissance of linear cryptosystem [8]. In order to reduce the burden of calculation, Liu et al. conducted FrAT in the discrete domain and defined DFrAT with two parameters of angle and fractional order [31, 35]. Nevertheless, these schemes with fractional transforms are complex value transforms, which means the output values are complex numbers, which is inconvenient to transfer, display, and store. Venturini et al. presented a reality-preserving form of the fractional-order transform and provided a solution to real-valued image encryption [36]. Subsequently, a series of algorithms were improved based on the reality-preserving technique, such as the reality-preserving multiple parameters FrFT, the reality-preserving fractional Hartley transform, and the reality-preserving DFrAT [37–40].

However, image encryption schemes in [11, 23, 34, 40–43] are all applicable to encrypt a single image, which may not be efficient in the era of big data. Thus, to meet the demands of high image encryption efficiency, we proposed a scheme to encrypt multiple images simultaneously. By considering the convenience of real-valued output, the reality-preserving discrete fractional angular transform (RPDFrAT) is introduced in our proposed scheme. In addition, the DNA sequence operation and the Logistic-sine chaotic system are combined for the scrambling-diffusion operation to yield the final ciphertext image, which provides a high level of robustness.

The rest of this paper is arranged as follows. In Section 2, we retrospect the background knowledge of the algorithm. The details of the proposed encryption scheme are delineated in Section 3. Simulation results and security analysis of the cryptosystem are depicted in Section 4. Finally, a brief conclusion is drawn in Section 5.

2. Background Knowledge

2.1. The Logistic-Sine Chaotic System. The Logistic-sine system consisting of the Logistic map and the Sine map can be expressed as [44]

$$x_{n+1} = [\mu x_n(1 - x_n) + (4 - \mu)\sin \pi x_n] \bmod 1, \quad (1)$$

where x_n is the produced sequence, μ is the control parameter in the range of $(0, 4]$, and mod denotes the modulus operation.

2.2. Reality-Preserving Discrete Fractional Angular Transform. The DFrAT is derived from the discrete fractional Fourier transform and discrete fraction random transform [35]. The definition of the DFrAT is

$$L_N^{\alpha,\beta} = K_N^{\beta} D_N^{\alpha} \left(K_N^{\beta}\right)^T, \quad (2)$$

where T represents the transpose operation. K_N^{β} is defined by an angle β and consists of the eigenvectors of the DFrAT. $D_N^{\alpha} = \mathrm{diag}\{\lambda_k^{\alpha}\}_{k=0,1,\ldots,N-1}$ is a diagonal matrix, $\lambda_k^{\alpha} = \exp(-jk\alpha)$ is the eigenvalue of the DFrAT, and α is the fractional order.

The RPDFrAT is defined according to the method of deriving the reality-preserving forms from the fractional transform [6, 35]. The specific procedures are as follows.

(1) If $s = \{s_1, s_2, \ldots, s_N\}^T$ is a real signal with length N, then the signal is constructed as a complex vector $\widehat{s} = \{s_1 + j \times s_{N/2+1}, s_2 + j \times s_{N/2+2}, \ldots, s_{N/2} + j \times s_N\}^T$ of length $N/2$ (N is even). If N is odd, the first value of the original data is divided into two half-valued parts and one of them is taken as the last component.

(2) $\widetilde{L}_{N/2}^{\widetilde{\alpha},\beta}$ is expressed as a complex-valued DFrAT matrix of size $N/2$, and then $\widehat{w}$ is calculated as

$$\begin{aligned}\widehat{w} &= \widetilde{L}_{N/2}^{\overline{\alpha},\beta}\widehat{s} = \left\{\mathrm{Re}\left(\widetilde{L}_{N/2}^{\overline{\alpha},\beta}\right) + j\times \mathrm{Im}\left(\widetilde{L}_{N/2}^{\overline{\alpha},\beta}\right)\right\}\left\{\mathrm{Re}\left(\widehat{s}\right) + j\times \mathrm{Im}\left(\widehat{s}\right)\right\} \\ &= \left\{\mathrm{Re}\left(\widetilde{L}_{N/2}^{\overline{\alpha},\beta}\right)\mathrm{Re}\left(\widehat{s}\right) - \mathrm{Im}\left(\widetilde{L}_{N/2}^{\overline{\alpha},\beta}\right)\mathrm{Im}\left(\widehat{s}\right)\right\} + j\times\left\{\mathrm{Im}\left(\widetilde{L}_{N/2}^{\overline{\alpha},\beta}\right)\mathrm{Re}\left(\widehat{s}\right) + \mathrm{Re}\left(\widetilde{L}_{N/2}^{\overline{\alpha},\beta}\right)\mathrm{Im}\left(\widehat{s}\right)\right\},\end{aligned} \tag{3}$$

where $\mathrm{Re}(\cdot)$ and $\mathrm{Im}(\cdot)$ represent the operations to distill the real part and the imaginary part of the signal, respectively.

(3) The RPDFrAT is defined as

$$w = \left\{\mathrm{Re}\left(\widehat{w}\right), \mathrm{Im}\left(\widehat{w}\right)\right\}^T = \begin{bmatrix}\mathrm{Re}\left(\widetilde{L}_{N/2}^{\overline{\alpha},\beta}\right) & -\mathrm{Im}\left(\widetilde{L}_{N/2}^{\overline{\alpha},\beta}\right) \\ \mathrm{Im}\left(\widetilde{L}_{N/2}^{\overline{\alpha},\beta}\right) & \mathrm{Re}\left(\widetilde{L}_{N/2}^{\overline{\alpha},\beta}\right)\end{bmatrix}\begin{bmatrix}\mathrm{Re}\left(\widehat{s}\right) \\ \mathrm{Im}\left(\widehat{s}\right)\end{bmatrix}. \tag{4}$$

2.3. DNA Sequence

2.3.1. DNA Coding. There are four nucleobases in a DNA sequence: T (thymine), C (cytosine), A (adenine), and G (guanine). According to the principle of complementary bases pairing, A and *T* are complementary, so are C and G. Similarly, in the binary code, 0 and 1 are complementary, so are 01 and 10, 00 and 11. Each nucleobase is represented with a 2-bit binary and will produce 24 kinds of coding methods. However, only 8 of the 24 encoding rules satisfy the complementary rule [45]. Table 1 shows these 8 encoding rules.

2.3.2. DNA Sequence Operations. According to the binary operation rules, the addition, subtraction, and XOR operation rules of the DNA sequences can be realized. For DNA encoding rule 1, the three operation rules of DNA sequences are shown in Tables 2–4, respectively.

2.3.3. DNA Complementary Rules. Table 5 lists the six groups of DNA complementary rules, which satisfy the following equations.

$$\begin{cases} b_i \neq K(b_i) \neq K(K(b_i)) \neq K(K(K(b_i)));\\ b_i = K(K(K(K(b_i)))), \end{cases} \tag{5}$$

where b_i and $K(b_i)$ represent the nucleotide and the base pair of b_i, respectively.

3. Proposed Scheme

3.1. The Generation of the Key. For higher security, the SHA-256 algorithm is adopted to engender the keys related to the four plaintext images for the chaotic system. The detailed steps are as follows:

Step 1. The pixels of the reshaped image, which were obtained with the 2D LWT from four plaintext images, are used as inputs of SHA-256, resulting in a 256-bit hash value.

$$hv = h_1, h_2, \ldots, h_{255}, h_{256}, \tag{6}$$

Step 2. Divide the 256-bit hash value into two sequences $h1 = hv(1{:}\ 128)$ and $h2 = hv(129{:}\ 256)$, and then calculate the hamming distance [46].

$$hm = \mathrm{HM}(h1, h2), \tag{7}$$

where $\mathrm{HM}(\cdot)$ represents the Hamming distance function.

Step 3. Generate the initial values ζ_1 and ζ_2 of the Logistic-sine system with the following mathematical expressions:

$$\begin{aligned}\zeta_0 &= \mathrm{mod}\left(\frac{hm}{256}, 1\right) + 1,\\ \zeta_1 &= \mathrm{mod}\left(\zeta_0 \times \frac{10^6}{256}, 1\right),\\ \zeta_2 &= \mathrm{mod}\left(\zeta_1 \times \frac{10^6}{256}, 1\right) + 0.4,\end{aligned} \tag{8}$$

where ζ_0 is a normalized result and $\mathrm{mod}(\cdot)$ denotes the modulus operation.

3.2. Encryption Algorithm Based on the RPDFrAT. The proposed image encryption process is shown in Figure 1. And the detail is as follows:

Step 1. The four grayscale images of size $N \times N$ are decomposed by the 2D LWT, and then the four subimages of size $(N/2) \times (N/2)$ can be obtained by extracting the approximation coefficients.

Step 2. The pixels of the four subimages of size $(N/2) \times (N/2)$ are united into one matrix F of size $N \times N$ by reshaping the approximation coefficients of the four real images extracted from Step 1. And then, F is encrypted by the RPDFrAT to obtain a real-value image H_0, as shown in equations (2)–(4).

Step 3. Elements in matrix H_0 are mapped into integers ranging from 0 to 255 as

$$H_1 = \mathrm{round}\left[255 \times \frac{H_0 - H_{\min}}{H_{\max} - H_{\min}}\right], \tag{9}$$

where $\mathrm{round}[k]$ denotes the nearest integer to k, matrix H_1 is obtained with the mapping operation, and $H_{\max}$ and $H_{\min}$ represent the maximal value and the minimal one in H_0, separately.

Step 4. The real-value image H_1 and the integer sequence generated with the Logistic-sine system are encrypted by the DNA sequence operations.

Table 1: DNA encoding rules.

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

Table 2: DNA addition rule for the DNA encoding rule 1.

+	T	A	C	G
T	G	T	A	C
A	T	A	C	G
C	A	C	G	T
G	C	G	T	A

Table 3: DNA subtraction rule for the DNA encoding rule 1.

–	T	A	C	G
T	A	T	G	C
A	C	A	T	G
C	G	C	A	T
G	T	G	C	A

Table 4: DNA XOR rule for DNA encoding rule 1.

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

Table 5: DNA complementary rules.

Rule 1	$K_1(A) = T, K_1(T) = G, K_1(G) = C, K_1(C) = A$
Rule 2	$K_2(A) = G, K_2(G) = C, K_2(C) = T, K_2(T) = A$
Rule 3	$K_3(A) = G, K_3(G) = T, K_3(T) = C, K_3(C) = A$
Rule 4	$K_4(A) = T, K_4(T) = C, K_4(C) = G, K_4(G) = A$
Rule 5	$K_5(A) = C, K_5(C) = T, K_5(T) = G, K_5(G) = A$
Rule 6	$K_6(A) = C, K_6(C) = G, K_6(G) = T, K_6(T) = A$

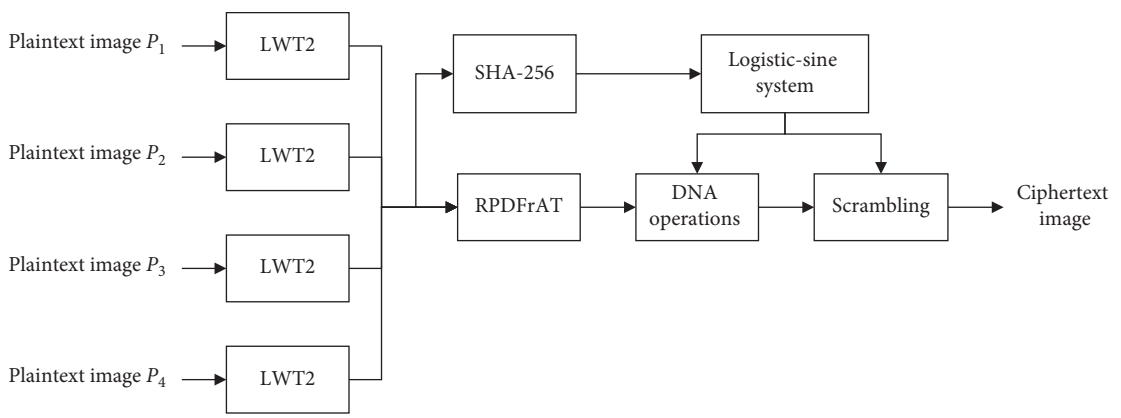


Figure 1: The proposed nonlinear multi-image encryption scheme.

$$d(l) = \begin{cases} R_{q_1}[H_2(l)], S_3(l) = A; \\ R_{q_2}[H_2(l)], S_3(l) = G; \\ R_{q_3}[H_2(l)], S_3(l) = C; \\ R_{q_4}[H_2(l)], S_3(l) = T, \end{cases} \quad (10)$$

(1) The integer sequence produced by the Logistic-sine system with the initial input ζ_1 is divided into S_1 and S_2 of length $N \times N$.

(2) The elements in image H_1, sequence S_1, and sequence S_2 are converted into 8-bit binary sequences, respectively. Next, the three 8-bit binary sequences are encrypted into associated DNA sequences H_2, S_3, and S_4 of length $4N^2$ according to DNA encoding rule 1.

(3) The DNA sequence H_2 is encrypted with the DNA complementary rules as

where $q_1, q_2, q_3, q_4 \in \{1, 2, 3, 4, 5, 6\}$, $l = 1, 2, \ldots, 4N^2$, A, G, C, and T are the nucleobases, and $R_q(\cdot)$ represents the q-th DNA complementary rule.

$$M(l) = S_4(l) \otimes d(l), \quad (11)$$

(4) The encrypted DNA sequence $M(l)$ is generated with the DNA XOR principle shown in Table 4,

where $l = 1, 2, \ldots, 4N^2$ and "$\otimes$" denotes the XOR operation.

(5) Decode the DNA sequence $M(l)$ with the DNA decoding Rule 5. Then, convert the results into decimal numbers to acquire image P. Moreover, the image P is processed to yield a new image P_1 through $P_1 = (P \times [H_{\max} - H_{\min}]/255) + H_{\min}$.

Step 5. The final encrypted image is acquired by confusing the output image P_1 with the Logistic-sine system under controlling the initial value ζ_2. The scrambling method is as follows:

(1) Generate a sequence λ_1 of length $N \times N$ by the Logistic-sine system under the control of the initial value ζ_2. Next, the sequence λ_1 is sorted in an ascending order to generate an index sequence g_1, which represents the corresponding index value sequence of the sorted λ_1.

(2) The index sequence g_1, whose elements are integers and spread between 1 and $N \times N$, can be used to confuse the positions of pixels in image P_1.

$$E(g_1(i)) = P_1(i), \quad (12)$$

where $i = 1, 2, \ldots, N^2$, $P_1(i)$ is the i-th pixel in image P_1, $g_1(i)$ represents the i-th elements in the index sequence g_1, and E denotes the scrambled image.

3.3. Decryption Algorithm. In this paper, the proposed encryption algorithm is symmetric; in a simple way, image decryption is a reverse process of encryption one. Since the keys of encryption and decryption algorithm are consistent and the DNA coding is a reversible process according to relevant rules, the encrypted image can be decrypted with a series of reverse processes. Through inverse scrambling, DNA decoding, inverse RPDFrAT, and inverse 2D LWT, one can recover four plaintext images from the encrypted image.

4. Simulation Results and Security Analysis

A series of experiments are implemented on MATLAB (version R2016a) to verify the security and effectiveness of the proposed scheme. Three groups of grayscale images of size 256×256 are selected as the test images, where images "Peppers," "House," "Elaine," and "Bridge" are referred to test group 1, "Baboon," "Lax," "Woman," and "Barbara" are referred to test group 2, and "Couple," "Airfield," "Flowers," and "Lake" are referred to test group 3.

4.1. Encryption and Decryption Results. The initial values of the Logistic-sine system are calculated as $\zeta_1 = 0.5762$, $\mu_1 = 3.99$, $\zeta_2 = 1.0714$, and $\mu_2 = 3.89$. The parameter α of the RPDFrAT is set as 0.2. The original images of test group 1 with 256×256 pixels are shown in Figures 2(a)–2(d). The encrypted image is given in Figure 2(e), and the corresponding decryption images with the correct keys are displayed in Figures 2(f)–2(i), respectively. From the encryption and decryption results shown in Figure 2, it is obvious that one cannot intuitively capture any valuable information from the encrypted images. And compared with the plaintext images, the corresponding decryption images show no significant differences.

2D LWT needs less memory space, has time-frequency localization capability, and can be calculated more efficiently. In the proposed scheme, four detail components including approximation coefficient LL, horizontal detail component HL, vertical detail component LH, and diagonal detail component HH are extracted from test images with the 2D LWT. Calculably, the sizes of the suiting detail components are 128×128 for the original images of size 256×256. To evaluate the decryption results of the three test groups, the values of the peak signal-to-noise ratio (PSNR) for decrypted images with different detail components were calculated with the mean square error (MSE).

$$\text{MSE} = \frac{1}{N^2} \sum_{m=1}^{N} \sum_{n=1}^{N} [R(m,n) - B(m,n)]^2, \text{PSNR} = 10\log_{10}\left[\frac{255^2}{\text{MSE}}\right], \quad (13)$$

where N^2 denotes the size of test images, and $R(m,n)$ and $B(m,n)$ represent the pixel values of the plaintext image and decrypted one at position (m,n), severally. From Tables 6–8, by comparing the value of the PSNR, the more the detailed components are contained in encrypted images, the higher the quality decryption images are recovered. Besides, for more components, the size of the encrypted image is expanded from 256×256 to 512×512. It can be concluded that the proposed scheme can meliorate the efficiency of encryption and has a good performance in encryption and decryption.

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

(e) (f) (g) (h)

(i)

Figure 2: Encrypted and decrypted images for test group 1: (a) Peppers, (b) House, (c) Elaine, (d) Bridge, (e) encrypted image, (f) decrypted "Peppers," (g) decrypted "House," (h) decrypted "Elaine," and (i) decrypted "Bridge".

Table 6: PSNR values for different subimages in test group 1.

Image	PSNR (dB)				Resolution ratio
	Peppers	House	Elaine	Bridge	
LL	23.8991	28.0304	24.7152	24.8944	256 × 256
LL + HL	24.5692	29.7437	27.3227	28.2862	
LL + LH	28.2129	29.0744	28.1203	26.6629	
LL + HH	23.5328	28.2238	25.2936	25.4404	
LL + HL + LH	24.801	31.7226	28.7284	32.4214	512 × 512
LL + HL + HH	20.4607	30.3214	26.8095	28.8676	
LL + LH + HH	23.4738	29.5268	28.4828	26.9537	
LL + HL + LH + HH	44.819	32.0278	35.0628	46.598	

Table 7: PSNR values for different subimages in test group 2.

Image	PSNR (dB)				Resolution ratio
	Baboon	Lax	Woman	Barbara	
LL	18.0353	22.4549	17.3189	23.0936	256 × 256
LL + HL	20.0236	24.0307	18.4896	24.6340	
LL + LH	18.4570	25.3754	20.1867	25.5969	
LL + HH	18.5045	23.2808	18.3846	24.2337	

Table 7: Continued.

Image	PSNR (dB)				Resolution ratio
	Baboon	Lax	Woman	Barbara	
LL + HL + LH	23.3347	27.9507	20.4353	23.7978	512 × 512
LL + HL + HH	21.9994	24.9871	17.5307	25.2391	
LL + LH + HH	20.0223	26.7670	20.4971	25.8953	
LL + HL + LH + HH	21.7028	44.8666	23.4088	42.3084	

Table 8: PSNR values for different subimages in test group 3.

Image	PSNR (dB)				Resolution ratio
	Couple	Airfield	Flowers	Lake	
LL	23.7612	21.2786	21.2690	22.9572	256 × 256
LL + HL	26.7980	23.8957	23.1842	25.1712	
LL + LH	27.1773	23.9516	23.9700	24.5594	
LL + HH	24.7250	22.5693	21.9644	23.4695	
LL + HL + LH	27.7772	21.7138	19.9242	31.5062	512 × 512
LL + HL + HH	26.2791	21.7087	19.0926	27.0977	
LL + LH + HH	27.0403	21.1431	19.4538	26.6705	
LL + HL + LH + HH	38.9034	43.1816	36.8264	29.8761	

4.2. Histogram Analysis and Chi-Square Test. The histogram is one of the important statistical assessment tools for cryptosystem. By comparing the characteristics of the plaintext image histograms and the ciphertext histograms, one can analyze the ability of the proposed scheme to homogenize encrypted image histograms. Figures 3(a)–3(l) are the histograms of the original images, which are distributed differently and disorganized. Figures 4(a)–4(c) are the histograms for the corresponding encrypted images, and they exhibit quite flat distributions. In the proposed scheme, the XOR operation based on DNA coding rules can make the pixel values of the test images distributed in the range of 0 to 255 evenly. It means that the statistical attack on this scheme is impracticable.

Besides, the chi-square (χ^2) test was introduced to further verify the homogeneity of the encrypted image histograms. The mathematical expression is as follows.

$$\chi^2 = \sum_{j=0}^{255} \frac{\left(\sigma_j - e\right)^2}{e}, \tag{14}$$

where j represents the pixel value of 8 grayscale levels and σ_j and e denote actual and theoretical frequencies of each gray value, respectively. When the χ^2 test follows 255 degrees of freedom and significance level of 0.05 and 0.01, $\chi^2_{0.05}(255) = 293.24783$ and $\chi^2_{0.01}(255) = 310.45739$ [47]. The results of the chi-square test for the proposed image encryption algorithm are shown in Table 9. It is obvious that the χ^2-value of the three test groups is lower than $\chi^2_{0.05}(255)$ and $\chi^2_{0.01}(255)$. Thus, one can conclude that there is no significant difference between the encrypted image and the uniform distribution. In other words, the encrypted images produced by our proposed nonlinear multi-image encryption scheme passed the chi-square test under 0.05 and 0.01 significance level and could resist the statistical attack effectively.

4.3. Correlation Analysis. In this part, we will discuss the ability of the proposed scheme to eliminate the correlation among adjacent points in images. To calculate the correlation coefficient, 1000 pairs of adjacent pixels in horizontal, vertical, and diagonal directions are extracted casually from the three test groups' images and their corresponding encrypted ones, respectively. The correlation distributions of test group 1 in the horizontal direction are shown in Figure 5. One can intuitively observe the correlation intensity of adjacent pixel points where the adjacent pixels are linearly distributed in plaintext images, while randomly distributed in encrypted images. And the correlation coefficients in directions HD, VD, and DD for the test images and corresponding encrypted images are compiled in Table 10. It is apparent that the correlation distributions of the original images in the three directions are highly correlated, totally different from the ones of the encrypted images with almost uniform distributions.

In the proposed scheme, the DNA operation and the chaotic system are utilized to scramble the pixels of the test images and change the value of pixels, which contribute to providing a lower correlation between any two adjacent pixels. Besides, compared with the schemes in [48, 49], the correlation coefficients of the encrypted images in our scheme are either smaller than these schemes or close to 0. It means that our proposed nonlinear multi-image encryption scheme could provide one noise-like encrypted image, which has strong resistivity of statistical attack.

4.4. Information Entropy. If the input variable confirms the uniform distribution, the global Shannon entropy will reach the maximal value, which represents a great uncertainty. The entropy of an image with $p(m_i)$ representing the probability of a pixel is

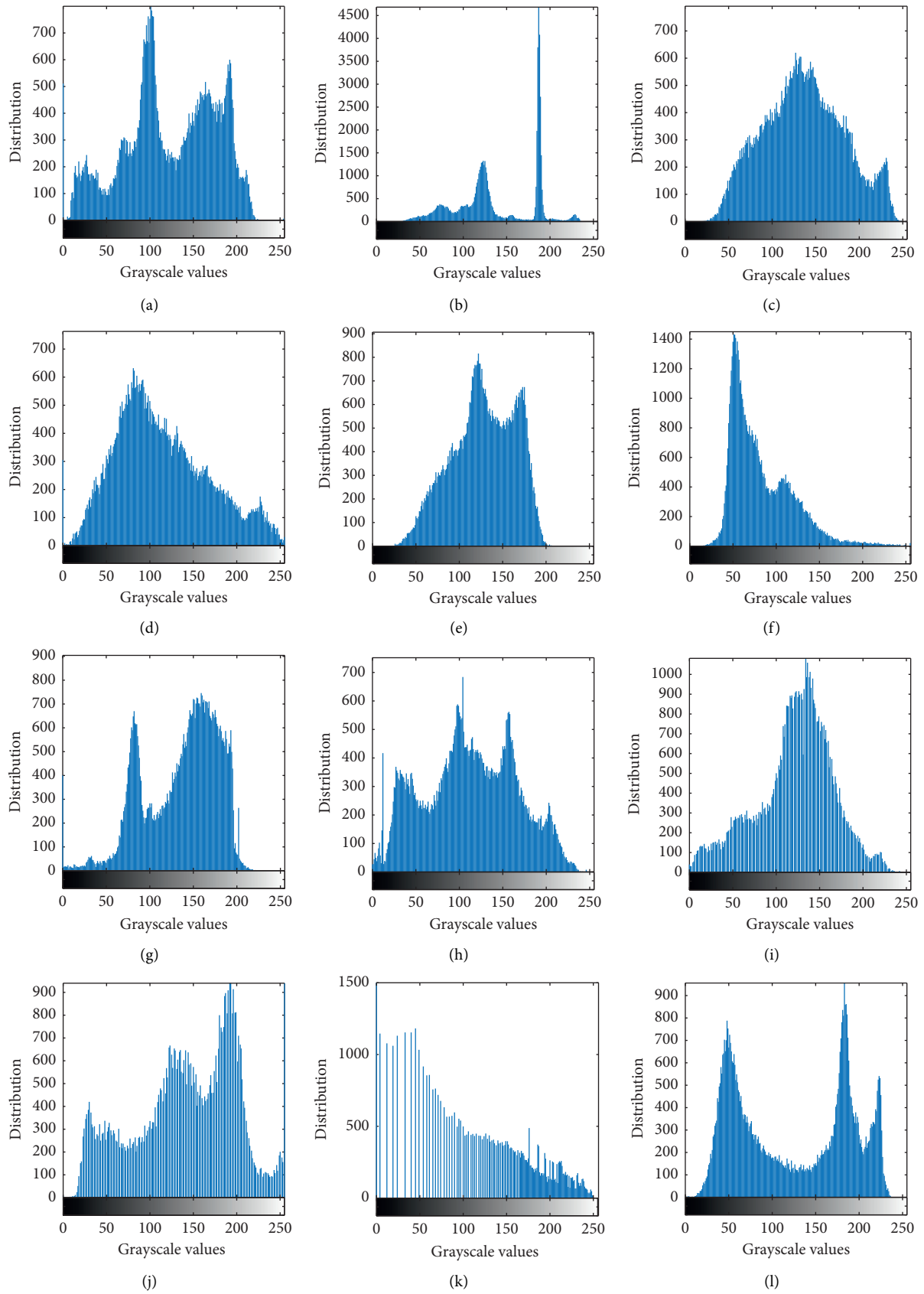


Figure 3: Histograms for three test groups' images: (a) "Peppers," (b) "House," (c) "Elaine," (d) "Bridge," (e) "Baboon," (f) "Lax," (g) "Woman," (h) "Barbara," (i) "Couple," (j) "Airfield," (k) "Flower," and (l) "Lake".

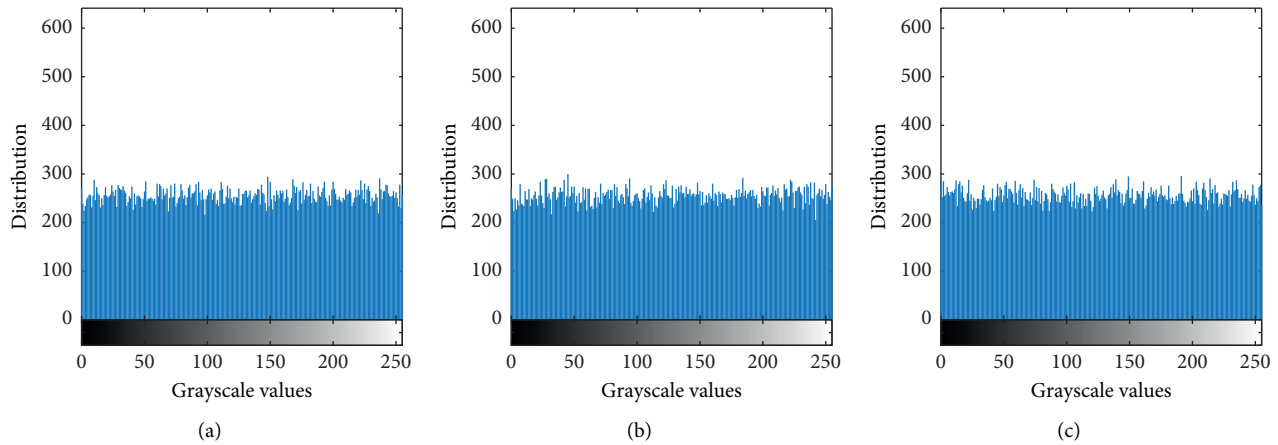


Figure 4: Histogram for encrypted images: (a) encrypted image of test group 1, (b) encrypted image of test group 2, and (c) encrypted image of test group 3.

Table 9: Chi-square test result.

Test group	χ^2-value	$\chi^2_{0.05}(255)$	$\chi^2_{0.01}(255)$	Decision
1	218.7031			Pass
2	271.3438	293.24783	310.45739	Pass
3	250.125			Pass

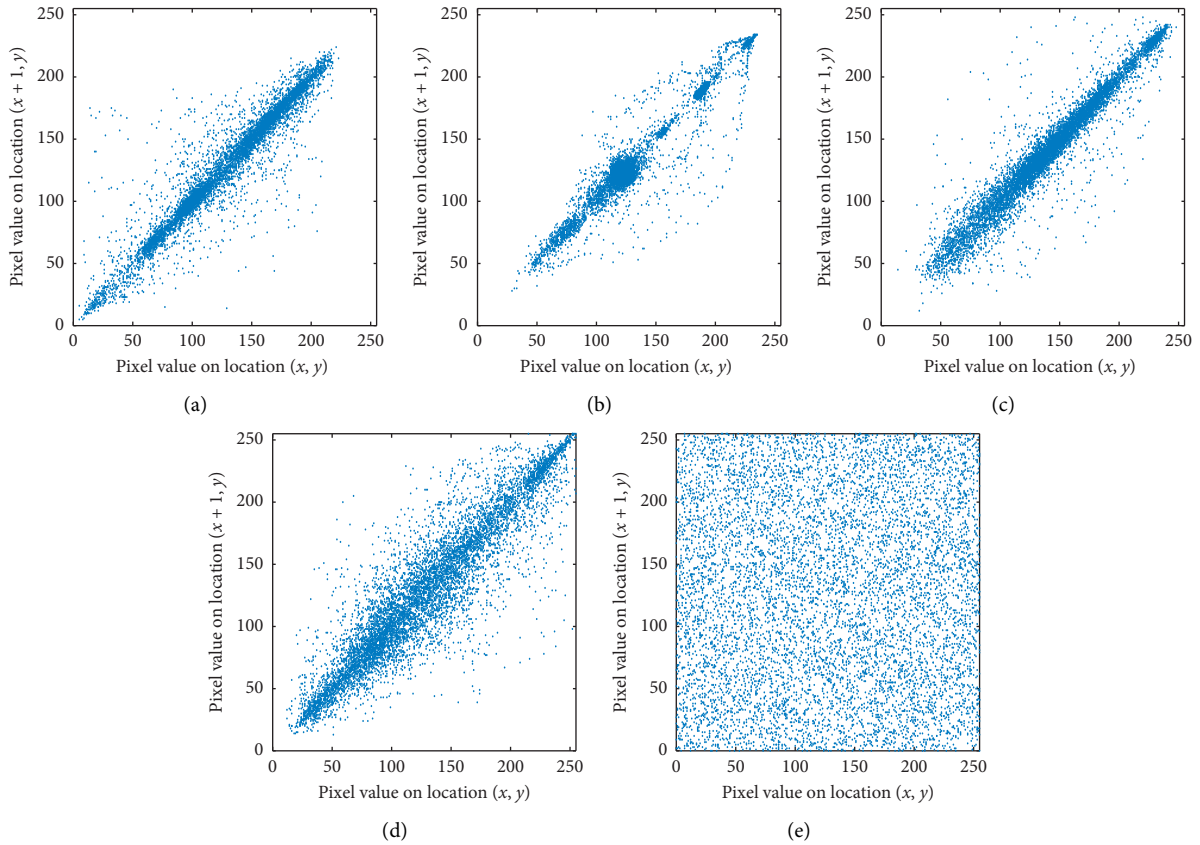


Figure 5: Correlation distribution results in the horizontal direction for test group 1: (a) "Peppers," (b) "House," (c) "Elaine," (d) "Bridge," and (e) encrypted image of test group 1.

Table 10: Correlation coefficients of adjacent pixels.

	Image	HD	VD	DD
	Peppers	0.9470	0.9489	0.9045
	House	0.9647	0.9768	0.9457
	Elaine	0.9564	0.9541	0.9389
	Bridge	0.9036	0.9286	0.8776
Proposed scheme	Encrypted image	−0.0043	−0.0011	0.0052
Ref. [48]	Encrypted image	0.0187	0.0495	−0.0246
Ref. [49]	Encrypted image	−0.0142	−0.0092	0.0157
	Baboon	0.7079	0.8365	0.6947
	Lax	0.7250	0.5911	0.5719
	Woman	0.9217	0.8801	0.8507
	Barbara	0.9070	0.8567	0.8100
Proposed scheme	Encrypted image	−0.0024	−0.0034	−0.0070
Ref. [48]	Encrypted image	−0.2044	0.0392	−0.0143
Ref. [49]	Encrypted image	−0.0011	−0.0039	−0.0136
	Couple	0.9421	0.9106	0.8758
	Airfield	0.9360	0.9249	0.9008
	Flowers	0.9826	0.9697	0.9580
	Lake	0.9330	0.9370	0.9046
Proposed scheme	Encrypted image	−0.0023	0.0015	−0.0063
Ref. [48]	Encrypted image	−0.0132	0.0142	0.0110
Ref. [49]	Encrypted image	0.0114	0.0126	−0.0021

$$H(m) = -\sum_{i=1}^{N} p(m_i)\log_2 p(m_i). \tag{15}$$

The maximal global Shannon entropy for a grayscale image of 256-level is 8 bits. However, considering the weakness of the global Shannon entropy including inaccuracy, inconsistency, and low efficiency, Wu et al. introduced another indicator, namely, local Shannon entropy [50]. With significance levels of 0.05, 0.01, and 0.001, the critical values of local Shannon entropy are presented in Table 11. Besides, the local Shannon entropy results are expected to be within the limits. In this analysis, we randomly selected thirty nonoverlapping image blocks with 16×121 pixels from the encrypted image; then, global and local Shannon entropies were calculated and listed in Table 11.

The DNA sequence operation based on Logistic-sine chaotic system in our proposed scheme can randomly change the pixel intensity value as well as contribute to uniform distributions of the encrypted images. As the results shown in Table 11, the global Shannon entropy of the encrypted images is very close to 8 bits, and the local ones meet the critical values. The results demonstrate that the pixels of the encrypted images are highly random and the provided cryptosystem is robust to the entropy attack.

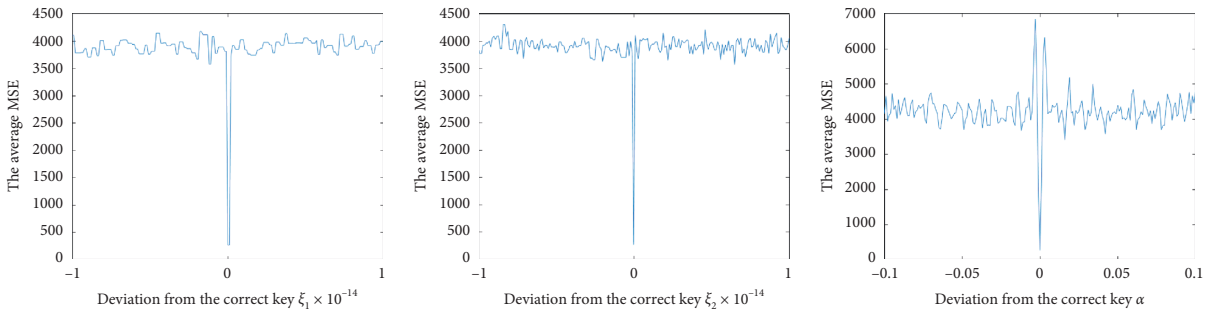
4.5. Key Space Analysis. In this segment, we will evaluate the ability of this presented scheme to resist brute-force attacks [44]. In the nonlinear multi-image encryption scheme, the secret key mainly includes ζ_1, ζ_2, and α. According to the simulation results, one can consider that the Key Space for ζ_1 or ζ_2 is about 10^{16} while that for α is 10^3. What is more, the 256-bit hash value of SHA-256 also amplifies the Key Space. Thus, the total Key Space is $10^{16} \times 10^{16} \times 10^3 \times 2^{128} = 10^{35} \times 2^{128} \approx 1.2037 \times 2^{244}$, large to resist the brute-force attack.

4.6. Key Sensitivity Analysis. In our proposed scheme, the keys are composed of ζ_1, ζ_2, and α, where the keys ζ_1 and ζ_2 are the initial values of the chaotic system and the key α is the fractional order of the RPDFrAT. Theoretically, our proposed scheme is highly sensitive towards keys, which depends on the high sensitivity to initial conditions of the chaos-based cryptosystem. Besides, the fractional-order α of the RPDFrAT is also contributed to key sensitivity. The MSE curves of keys ζ_1, ζ_2, and α are presented in Figure 6, respectively. It shows that a little deviation of the correct keys will necessarily cause a drastic change in the MSE values. Figure 7 illustrates the decrypted results when one of the keys slightly deviates from the exact value. Figure 7(a) is the decryption image when the keys ζ_2 and α are correct while the key ζ_1 has a deviation 10^{-16}. Figure 7(b) is the decryption image when the keys ζ_1 and α are correct while the key ζ_2 has a deviation 10^{-16}. Figure 7(c) is the decryption image when the keys ζ_1 and ζ_2 keep intact while the key α deviates 10^{-3}. The decryption images generated with the incorrect keys unable to be recognized indicate that the proposed nonlinear multi-image encryption scheme has a high sensitivity to the keys and the aggressors cannot crack the cryptosystem without knowing the exact keys.

4.7. Differential Attack Analysis. To measure whether this image encryption scheme can be against differential attacks or not, the number of pixels change rate (NPCR) and the uniform average change intensity (UACI) are employed as usual [44]. The mathematical expressions of the NPCR and the UACI are as follows:

Table 11: Global and local Shannon entropy analysis for the encrypted images.

Test group	Global Shannon entropy (bits)	Local Shannon entropy (bits)	Local Shannon entropy critical values (bits)		
			$h_{\text{left}}^{1*0.05} = 7.9019$ $h_{\text{right}}^{1*0.05} = 7.9030$	$h_{\text{left}}^{1*0.01} = 7.9017$ $h_{\text{right}}^{1*0.01} = 7.9032$	$h_{\text{left}}^{1*0.001} = 7.9015$ $h_{\text{right}}^{1*0.001} = 7.9034$
1	7.9978	7.9030	Pass	Pass	Pass
2	7.9972	7.9026	Pass	Pass	Pass
3	7.9973	7.9029	Pass	Pass	Pass



(a) (b) (c)

Figure 6: MSE curve of the key: (a) ζ_1, (b) ζ_2, and (c) α.

(a) (b) (c)

Figure 7: Decrypted images with deviated keys: (a) $\zeta_1 = 0.5762 + 10^{-16}$, (b) $\zeta_2 = 1.0714 + 10^{-16}$, and (c) $\alpha = 0.2 + 10^{-3}$.

$$\text{NPCR} = \frac{1}{X \times Y} \sum_{i=1}^{X} \sum_{j=1}^{Y} K(i,j) \times 100\%,$$

$$\text{UACI} = \sum_{i=1}^{X} \sum_{j=1}^{Y} \left(\frac{\left| f(i,j) - f'(i,j) \right|}{255 \times X \times Y} \right) \times 100\%, \tag{16}$$

$$K(i,j) = \begin{cases} 0, & f(i,j) = f'(i,j); \\ 1, & f(i,j) \neq f'(i,j), \end{cases}$$

where $X \times Y$ represents the size of the encrypted image and $f(i,j)$ and $f'(i,j)$ are corresponding encryption results where only one pixel is changed in plaintext image. Since our proposed scheme is a plaintext-related image cryptosystem by employing the SHA-256 algorithm, the encrypted image will drastically different when any pixel is changed.

Tables 12 and 13, respectively, list the NPCR and the UACI values of the encrypted images. $N_{0.05}^{*}$, $N_{0.01}^{*}$, and $N_{0.001}^{*}$ denote the critical values for NPCR test with significance levels of 0.05, 0.01, and 0.001, respectively. If the NPCR test results are higher than these critical values, the encrypted images are random-like with corresponding

significance levels. Similarly, the critical values of the UACI test are composed of U_{η}^{*-} and U_{η}^{*+}, where η represents significance level. For the UACI test, the results are expected to be kept between U_{η}^{*-} and U_{η}^{*+} with an η-level of significance. From Tables 12 and 13, both of the tests have high coincidence rates under different significance levels. It can be inferred that the proposed nonlinear multi-image encryption scheme is helpful in defeating the differential attack.

4.8. Noise Attack Analysis and Occlusion Attack Analysis. The white Gaussian noise (WGN) with zero-mean and unit standard deviation is added to the encrypted image as

$$C_1 = C_0 + kG, \tag{17}$$

where C_1 is the encrypted image with the WGN, C_0 is the encrypted image without noise, G represents the WGN, and k denotes the noise intensity. And the corresponding decrypted images of test group 1 under different noise attacks are shown in Figure 8. Besides, the values of the MSE and the PSNR are listed in Table 14 to describe the quality of decrypted results mathematically. It can be observed that the decryption images of test group 1 are still visually recognizable since there exist rough features the same as the original ones. Though the decryption performances decrease when the noise strength increases, the values of the MSE and the PSNR indicate the similarity between the original images and recovered ones. Therefore, our proposed nonlinear multi-image encryption scheme is competent to some robustness against noise attacks.

Moreover, considering a practical situation that the encrypted image may be deliberately occluded by unaccredited attackers in transmission, the encrypted image is partially cropped with different sizes to analyze the ability to resist the occlusion attacks. The corresponding decryption images are shown in Figure 9, and the results of the MSE and the PSNR are listed in Table 15. The higher the values of the PSNR are, the more similar the decrypted images are to original images. In the results, we can see that the major characteristics of the decryption images are still preserved, though they have become blurry. That is because the main features of the multiple original images have been spread over the entire encrypted image by the 2D LWT and chaos-based scramble-diffuse operations. Deductively, the proposed scheme has a certain degree of survivability against occlusion attacks.

4.9. Analysis of Withstanding Four Typical Attacks. The four classical attacks are ciphertext-only attack, chosen-ciphertext attack, known-plaintext attack, and chosen-plaintext attack (CPA). Among them, CPA is the most forceful attack; thus, if the proposed image encryption scheme can resist CPA, it can also perform well in withstanding the other three typical attacks [1]. The proposed scheme is a plaintext-related image cryptosystem where the keys are associated with multiple plaintext images. Therefore, any pixel changes in the plaintext images will cause the generated chaotic sequences to change correspondingly, as well as the encrypted image. In addition, with the DNA sequence operations, it is more difficult for attackers to deduce the exact keys. Therefore, attackers with CPA will only get a scrambled matrix and cannot obtain beneficial information between the plaintext images and the corresponding encrypted image. It indicates that the proposed nonlinear multi-image cryptosystem has the competence to protest CPA and the other three typical attacks.

4.10. Computation Complexity Analysis. The execution efficiency of one image cryptosystem is an important practical issue that needs to be considered. In this part, we will give the computation complexity analysis. In the proposed nonlinear multi-image cryptosystem, the computation complexity is mainly related to the scrambling and diffusion operations. One real-valued intermediate encrypted image from RPDFrAT will be scrambled and diffused by the DNA sequence operation and chaotic system, so the first time-consuming part in computation is the operation of multiplying floating point numbers for the generation of chaotic sequences. Hence, the time complexity is $\Theta(2 \times N \times N)$ for the image of size $N \times N$. For the DNA sequence operations, the second time-consuming part is the number of the DNA complementary and XOR operations. The time complexity is $\Theta(24 \times N \times N)$. In addition, for the scrambling process at the pixel level, the time complexity is $\Theta(N \times N)$. Therefore, the total time complexity of the proposed nonlinear multi-image cryptosystem is $\Theta(24 \times N \times N)$, which is similar to the results in [1, 51] but less efficient than the scheme in [52]. Obviously, the DNA encoding and decoding operations take a lot of time. However, considering the advent of DNA computers, the DNA sequence operations may be implemented faster, also for the proposed scheme.

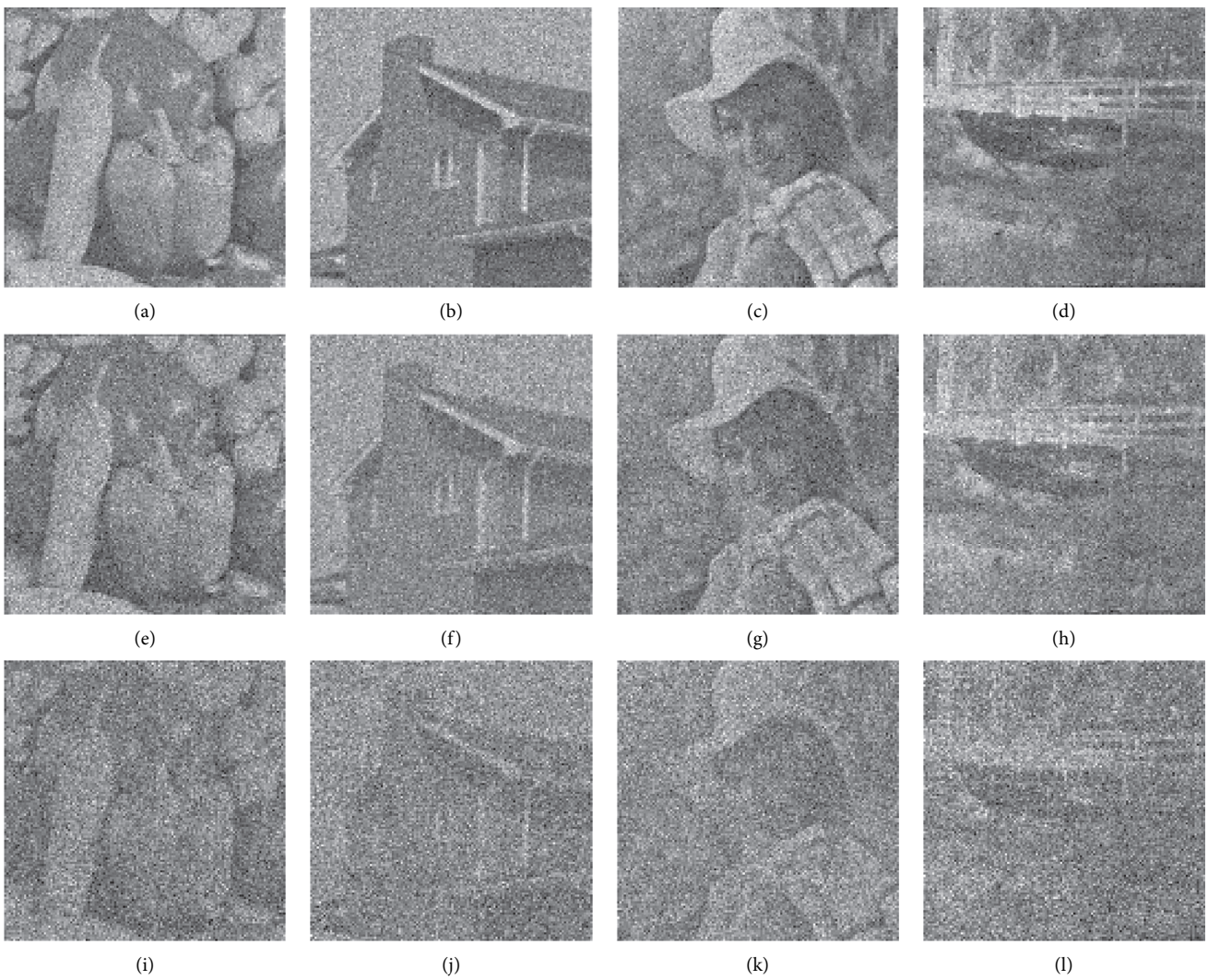
4.11. Comparison with Existing Works. The proposed nonlinear multi-image encryption scheme has been compared with the preexisting chaos-based schemes [52–57] in Table 16. Firstly, the proposed algorithm can encrypt and decrypt four grayscale images at the same time, while the schemes presented in [52, 53] are only suitable for a single image. Therefore, compared with [52, 53], this proposed multi-image encryption scheme is more efficient. Moreover, the Logistic-sine chaotic system is employed for better performance in pseudorandomness and ergodicity. The DNA sequence operations combined with the Logistic-sine chaotic map are used to hide plaintext information for higher security. Compared with algorithms in [54–56], the proposed scheme is highly resistant to various security attacks with the DNA encoding operation. In Table 17, the proposed scheme is compared with [49, 58–60] from several security analysis indicators. The results of information entropy are obtained from the encrypted image of "Elaine", which was encrypted by the corresponding scheme. The comparison of information entropy serves to show that the result of our scheme is either better or very near to the entropies of other schemes. The UACI and the NPCR test results of the proposed scheme are similar to the results of [49, 58–60] and close to the ideal values; they

Table 12: NPCR test results.

Theoretical NPCR critical values	NPCR(%)		
	Test group 1	Test group 2	Test group 3
$N^*_{0.05} = 99.5693\%$ $N^*_{0.01} = 99.5527\%$ $N^*_{0.001} = 99.5341\%$	99.65	99.68	99.66

Table 13: UACI test result.

Theoretical UACI critical values	UACI(%)		
	Test group 1	Test group 2	Test group 3
$U^{*-}_{0.05} = 33.2824\%$ $U^{*+}_{0.05} = 33.6447\%$ $U^{*-}_{0.01} = 33.2255\%$ $U^{*+}_{0.01} = 33.7016\%$ $U^{*-}_{0.001} = 33.1594\%$ $U^{*+}_{0.001} = 33.7677\%$	33.55	33.58	33.54

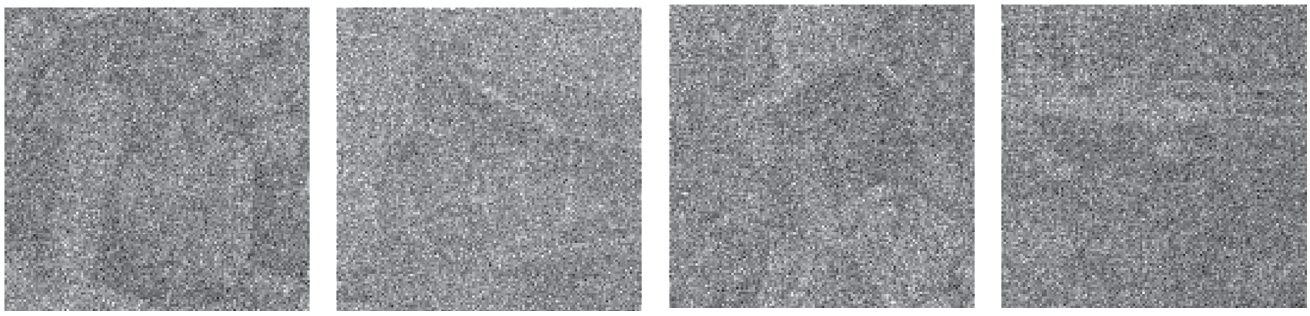


(a) (b) (c) (d)

(e) (f) (g) (h)

(i) (j) (k) (l)

Figure 8: Continued.

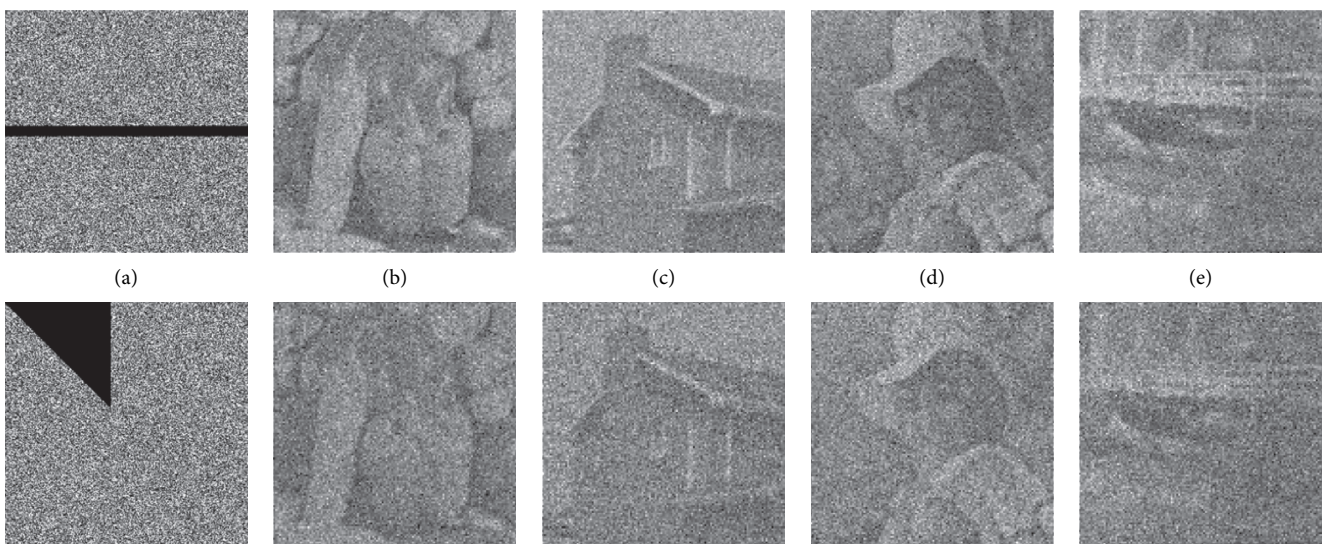


(m) (n) (o) (p)

Figure 8: Noise attacks analysis in the encrypted image of test group 1: (a–d) decrypted images of "Peppers," "House," "Elaine," and "Bridge," respectively, with the noise intensity $k = 0.5$, (e–h) decrypted results with the noise intensity $k = 1$, (i–l) decrypted results with the noise intensity $k = 5$, and (m–p) decrypted results with the noise intensity $k = 10$.

Table 14: The MSE and PSNR values of test group 1 with the white Gaussian noise.

The intensity of the white Gaussian noise	Image	MSE	PSNR (dB)
$k = 0.5$	Decrypted "Peppers"	1152.9237	17.5128
	Decrypted "House"	848.3636	18.8450
	Decrypted "Elaine"	830.1441	18.9393
	Decrypted "Bridge"	1128.4652	17.6059
$k = 1$	Decrypted "Peppers"	1672.5266	15.8971
	Decrypted "House"	1287.4921	17.0334
	Decrypted "Elaine"	1203.8451	17.3251
	Decrypted "Bridge"	1687.9173	15.8573
$k = 5$	Decrypted "Peppers"	2329.1915	14.4588
	Decrypted "House"	2106.6591	14.8949
	Decrypted "Elaine"	2074.7117	14.9612
	Decrypted "Bridge"	2486.3427	14.1752
$k = 10$	Decrypted "Peppers"	2848.1021	13.5852
	Decrypted "House"	2562.9442	14.0434
	Decrypted "Elaine"	2379.4283	14.3661
	Decrypted "Bridge"	3111.0023	13.2018



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

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

Figure 9: Continued.

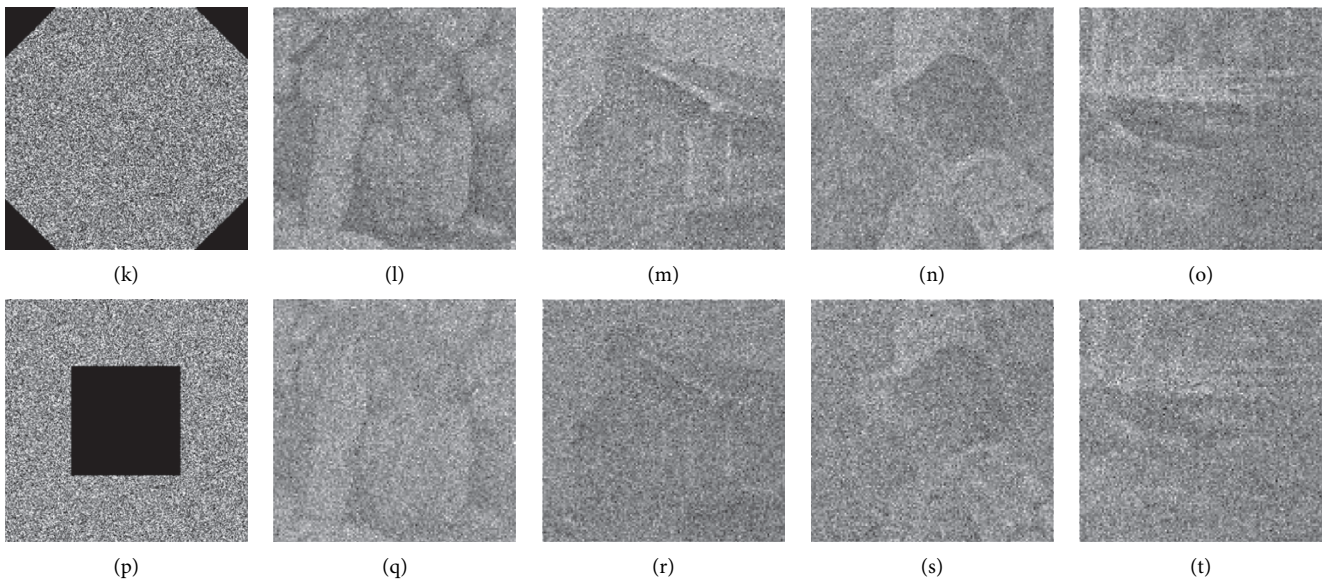


Figure 9: Occlusion attack results.

Table 15: The MSE and PSNR values of test group 1 with data loss.

Data loss in cipher	Image	MSE	PSNR (dB)
Figure 9(a)	Decrypted "Peppers"	1631.2076	16.0057
	Decrypted "House"	1370.5680	16.7618
	Decrypted "Elaine"	1635.5325	15.9942
	Decrypted "Bridge"	1864.8458	15.4244
Figure 9(f)	Decrypted "Peppers"	2244.3347	14.6199
	Decrypted "House"	2024.8464	15.0669
	Decrypted "Elaine"	1945.2161	15.2411
	Decrypted "Bridge"	2267.7465	14.5739
Figure 9(k)	Decrypted "Peppers"	2288.5194	14.5353
	Decrypted "House"	1838.9888	15.4850
	Decrypted "Elaine"	1810.6396	15.5525
	Decrypted "Bridge"	2441.6336	14.2540
Figure 9(p)	Decrypted "Peppers"	2775.3518	13.6976
	Decrypted "House"	2400.4469	14.3279
	Decrypted "Elaine"	2252.1406	14.6048
	Decrypted "Bridge"	3011.6712	13.3427

Table 16: Comparison of different image encryption algorithms.

Algorithms	Types of encryption	Chaotic maps	DNA sequence operation
Proposed scheme	Multi-image	Logistic-sine chaotic map	Yes
Reference [54]	Multi-image	Henon map, logistic map	No
Reference [55]	Multi-image	PWLCM system	No
Reference [56]	Multi-image	PWLCM system	No
Reference [57]	Multi-image	PWLCM system	Yes
Reference [52]	Single image	2D logistic chaotic map	Yes
Reference [53]	Single image	3D Lorenz chaotic system, Chen's 4D hyperchaotic system	Yes

prove that the proposed encryption scheme forcefully resists differential attacks. Table 18 listed the Key Space of [49, 52, 55, 60, 61]. The Key Space of our proposed scheme has value more than 2^{128}, which is sufficient to defeat the brute-force attack.

Reference [62] proposed a multi-grayscale-image encryption scheme in a cross-coupled manner. Multiple grayscale images will be reconstructed into one image, and then two piecewise linear chaotic maps (PWLCM) are cross-coupled to carry out the permutation-diffusion operation in

Table 17: Comparison results for encrypted single "Elaine" of size 256×256.

Algorithms	Information entropy (bits)	NPCR(%)	UACI(%)
Proposed scheme	7.9978	99.63	33.52
Reference [58]	7.9974	99.61	33.46
Reference [59]	7.9976	99.62	33.41
Reference [49]	7.9992	99.63	33.54
Reference [60]	7.7196	99.59	33.43

Table 18: Comparison of key space results.

Algorithms	Proposed scheme	Ref. [49]	Ref. [52]	Ref. [55]	Ref. [60]	Ref. [61]
Key Space	1.2037×2^{244}	2^{180}	9.2094×2^{265}	1.0195×2^{186}	2^{49}	1.2446×2^{199}

this reshaped image. The encrypted image will be separated to yield the final multiple cipher images. However, the security of this scheme is insufficient in some cases. Thus, [63] proposed an improved scheme, which employed two different layers of cross-coupled PWLCM systems and flip operations. Both our proposed scheme and schemes in [62, 63] are plaintext-related cryptosystems and encrypt multiple grayscale images with scrambling-diffusion operations. However, in our proposed algorithm, transform domain operations and DNA sequence operations are utilized for higher security compared with [62, 63]. In [56], the cryptosystem also uses the PWLCM only to encrypt multiple images. Besides, Chen et al. put a self-adaptive permutation and diffusion architecture to yield cipher from a single grayscale image, which only performs scrambling operation once time with DNA coding [64]. However, in addition to the DNA sequence operation and chaotic map, our proposed scheme introduced transform domain operation to encrypt multi-images as well.

5. Conclusion

A nonlinear multi-image encryption scheme is presented. The main features of multiple original images are extracted with the 2D lifting wavelet transform, and the information of original images is compressed into a small amount of data as well. Next, the reality-preserving discrete fractional angular transform is employed to produce a real-valued intermediate output, which is convenient to transfer, display, and store. Ultimately, the scrambling-diffusion operations are conducted with the combination of the deoxyribonucleic acid sequence operations and Logistic-sine chaotic system, which promises a bright prospect with the development of DNA computer. The proposed lossy multi-image encryption scheme could greatly improve the encryption efficiency at the cost of the quality of decryption images. Moreover, the lossy multi-image encryption scheme is robust and secure against various attacks where the deoxyribonucleic acid sequence operations are nonlinear and the main keys are associated with the original images.

Data Availability

The raw/processed data required to reproduce these findings can be available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant nos. 62041106 and 61861029), the Major Academic Discipline and Technical Leader of Jiangxi Province (Grant no. 20162BCB22011), the Cultivation Plan of Applied Research of Jiangxi Province (Grant no. 20181BBE58022), the Foundation of Jiujiang University (Grant no. 2015LGYB03), and the foundation of the Education Department of Jiangxi Province (Grant no. GJJ190203).

References

[1] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Processing*, vol. 155, pp. 44–62, 2019.

[2] W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," *Advances in Optics and Photonics*, vol. 6, no. 2, pp. 120–155, 2014.

[3] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, "A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2," *Nonlinear Dynamics*, vol. 83, no. 3, pp. 1123–1136, 2016.

[4] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D Sine Logistic modulation map for image encryption," *Information Sciences*, vol. 297, pp. 80–94, 2015.

[5] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R. M. López-Gutiérrez, and O. R. Acosta Del Campo, "A RGB image encryption algorithm based on total plain image characteristics and chaos," *Signal Processing*, vol. 109, pp. 119–131, 2015.

[6] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letters*, vol. 20, no. 7, pp. 767–769, 1995.

[7] S. Mohammad Seyedzadeh and S. Mirzakuchaki, "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map," *Signal Processing*, vol. 92, no. 5, pp. 1202–1215, 2012.

[8] N. Zhou, Y. Wang, and L. Gong, "Novel optical image encryption scheme based on fractional Mellin transform," *Optics Communications*, vol. 284, no. 13, pp. 3234–3242, 2011.

[9] N. Zhou, Y. Wang, L. Gong, H. He, and J. Wu, "Novel single-channel color image encryption algorithm based on chaos and

fractional Fourier transform," *Optics Communications*, vol. 284, no. 12, pp. 2789–2796, 2011.

[10] A. Belazi, A. A. Abd El-Latif, A.-V. Diaconu, R. Rhouma, and S. Belghith, "Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms," *Optics and Lasers in Engineering*, vol. 88, pp. 37–50, 2017.

[11] K. Jiao, G. Ye, Y. Dong et al., "Image encryption scheme based on a generalized Arnold map and RSA algorithm," *Security and Communication Networks*, vol. 2020, Article ID 9721675, 16 pages, 2020.

[12] K. Nakano, M. Takeda, H. Suzuki, and M. Yamaguchi, "Generalized model of double random phase encoding based on linear algebra," *Optics Communications*, vol. 286, pp. 91–94, 2013.

[13] I.-H. Lee and M. Cho, "Double random phase encryption based orthogonal encoding technique for color images," *Journal of the Optical Society of Korea*, vol. 18, no. 2, pp. 129–133, 2014.

[14] H. Singh, A. K. Yadav, S. Vashisth, and K. Singh, "Double phase-image encryption using gyrator transforms, and structured phase mask in the frequency plane," *Optics and Lasers in Engineering*, vol. 67, pp. 145–156, 2015.

[15] H. Tashima, M. Takeda, H. Suzuki, T. Obi, M. Yamaguchi, and N. Ohyama, "Known plaintext attack on double random phase encoding using fingerprint as key and a method for avoiding the attack," *Optics Express*, vol. 18, no. 13, pp. 13772–13781, 2010.

[16] X. Liu, J. Wu, W. He, M. Liao, C. Zhang, and X. Peng, "Vulnerability to ciphertext-only attack of optical encryption scheme based on double random phase encoding," *Optics Express*, vol. 23, no. 15, pp. 18955–18968, 2015.

[17] G. Li, W. Yang, D. Li, and G. Situ, "Cyphertext-only attack on the double random-phase encryption: experimental demonstration," *Optics Express*, vol. 25, no. 8, pp. 8690–8697, 2017.

[18] W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated fourier transforms," *Optics Letters*, vol. 35, no. 2, pp. 118–120, 2010.

[19] W. Chen and X. Chen, "Double random phase encoding using phase reservation and compression," *Journal of Optics*, vol. 16, no. 2, Article ID 25402, 2014.

[20] Y. Wang, C. Quan, and C. J. Tay, "Asymmetric optical image encryption based on an improved amplitude-phase retrieval algorithm," *Optics and Lasers in Engineering*, vol. 78, pp. 8–16, 2016.

[21] Z. Shao, Y. Shang, X. Fu, H. Yuan, and H. Shu, "Double-image cryptosystem using chaotic map and mixture amplitude-phase retrieval in gyrator domain," *Multimedia Tools and Applications*, vol. 77, no. 1, pp. 1285–1298, 2018.

[22] Z. Hua and Y. Zhou, "Image encryption using 2D logistic-adjusted-sine map," *Information Sciences*, vol. 339, pp. 237–253, 2016.

[23] G. Ye, K. Jiao, C. Pan et al., "An effective framework for chaotic image encryption based on 3D Logistic map," *Security and Communication Networks*, vol. 2018, Article ID 8402578, 17 pages, 2018.

[24] H. Chen, Z. Liu, L. Zhu, C. Tanougast, and W. Blondel, "Asymmetric color cryptosystem using chaotic Ushiki map and equal modulus decomposition in fractional fourier transform domains," *Optics and Lasers in Engineering*, vol. 112, pp. 7–15, 2019.

[25] C. Chen, K. Sun, and S. He, "An improved image encryption algorithm with finite computing precision," *Signal Processing*, vol. 168, Article ID 107340, 2020.

[26] X. Wang, L. Feng, and H. Zhao, "Fast image encryption algorithm based on parallel computing system," *Information Sciences*, vol. 486, pp. 340–358, 2019.

[27] Y. Xian and X. Wang, "Fractal sorting matrix and its application on chaotic image encryption," *Information Sciences*, vol. 547, pp. 1154–1169, 2021.

[28] Z. Liu, S. Li, W. Liu, Y. Wang, and S. Liu, "Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding," *Optics and Lasers in Engineering*, vol. 51, no. 1, pp. 8–14, 2013.

[29] C. Yu, J. Li, X. Li, X. Ren, and B. B. Gupta, "Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer generated hologram," *Multimedia Tools and Applications*, vol. 77, no. 4, pp. 4585–4608, 2018.

[30] S.-S. Yu, N.-R. Zhou, L.-H. Gong, and Z. Nie, "Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system," *Optics and Lasers in Engineering*, vol. 124, Article ID 105816, 2020.

[31] Z. Liu, M. Gong, Y. Dou et al., "Double image encryption by using Arnold transform and discrete fractional angular transform," *Optics and Lasers in Engineering*, vol. 50, no. 2, pp. 248–255, 2012.

[32] L. Sui, K. Duan, and J. Liang, "A secure double-image sharing scheme based on Shamir's three-pass protocol and 2D Sine Logistic modulation map in discrete multiple-parameter fractional angular transform domain," *Optics and Lasers in Engineering*, vol. 80, pp. 52–62, 2016.

[33] H. M. Ozaktas, M. Kutayalper, and Z. Zalevsky, *The Fractional Fourier Transform: with Applications in Optics and Signal Processing*, John Wiley & Sons, Hoboken, NJ, USA, 1995.

[34] L. Gao, L. Qi, and L. Guan, "The property of frequency shift in 2D-FRFT domain with application to image encryption," *IEEE Signal Processing Letters*, vol. 28, pp. 185–189, 2021.

[35] Z. Liu, M. A. Ahmad, and S. Liu, "A discrete fractional angular transform," *Optics Communications*, vol. 281, no. 6, pp. 1424–1429, 2008.

[36] I. Venturini and P. Duhamel, "Reality preserving fractional transforms signal processing applications," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, pp. 205–208, Montreal, Canada, May 2004.

[37] J. Lang, "Image encryption based on the reality-preserving multiple-parameter fractional fourier transform and chaos permutation," *Optics and Lasers in Engineering*, vol. 50, no. 7, pp. 929–937, 2012.

[38] X. Kang, Z. Han, A. Yu et al., "Double random scrambling encoding in the RPMPFrHT domain," in *Proceedings of the 24th IEEE International Conference on Image Processing*, pp. 4362–4366, Anchorage, AL, USA., September 2017.

[39] 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.

[40] X. Kang, A. Ming, and R. Tao, "Reality-preserving multiple parameter discrete fractional angular transform and its application to color image encryption," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 29, no. 6, pp. 1595–1607, 2019.

[41] O. S. Faragallah, H. S. El-Sayed, A. Afifi et al., "Efficient and secure opto-cryptosystem for color images using 2D logistic-based fractional Fourier transform," *Optics and Lasers in Engineering*, vol. 137, 2021.

[42] S. Kumar, B. Panna, and R. K. Jha, "Medical image encryption using fractional discrete cosine transform with chaotic function," *Medical & Biological Engineering & Computing*, vol. 57, no. 11, pp. 2517–2533, 2019.

[43] Y.-Q. Zhang, X.-Y. Wang, J. Liu, and Z.-L. Chi, "An image encryption scheme based on the MLNCML system using DNA sequences," *Optics and Lasers in Engineering*, vol. 82, pp. 95–103, 2016.

[44] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An optical image compression and encryption scheme based on compressive sensing and RSA algorithm," *Optics and Lasers in Engineering*, vol. 121, pp. 169–180, 2019.

[45] J. D. Watson and F. H. C. Crick, "Molecular structure of nucleic acids: a structure for deoxyribose nucleic acid," *Nature*, vol. 171, no. 4356, pp. 737-738, 1953.

[46] L. Wang, H. Song, and P. Liu, "A novel hybrid color image encryption algorithm using two complex chaotic systems," *Optics and Lasers in Engineering*, vol. 77, pp. 118–125, 2016.

[47] N. D. Gagunashvili, "Chi-square tests for comparing weighted histograms," *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment*, vol. 614, no. 2, pp. 287–296, 2010.

[48] X.-D. Chen, Q. Liu, J. Wang, and Q.-H. Wang, "Asymmetric encryption of multi-image based on compressed sensing and feature fusion with high quality image reconstruction," *Optics & Laser Technology*, vol. 107, pp. 302–312, 2018.

[49] H.-S. Ye, N.-R. Zhou, and L.-H. Gong, "Multi-image compression-encryption scheme based on quaternion discrete fractional hartley transform and improved pixel adaptive diffusion," *Signal Processing*, vol. 175, Article ID 107652, 2020.

[50] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness," *Information Sciences*, vol. 222, pp. 323–342, 2013.

[51] 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.

[52] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Optics and Lasers in Engineering*, vol. 88, pp. 197–213, 2017.

[53] T. Hu, Y. Liu, L.-H. Gong, and C.-J. Ouyang, "An image encryption scheme combining chaos with cycle operation for DNA sequences," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 51–66, 2017.

[54] Z. Tang, J. Song, X. Zhang, and R. Sun, "Multiple-image encryption with bit-plane decomposition and chaotic maps," *Optics and Lasers in Engineering*, vol. 80, pp. 1–11, 2016.

[55] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on mixed image element and chaos," *Computers & Electrical Engineering*, vol. 62, pp. 401–413, 2017.

[56] K. A. K. Patro and B. Acharya, "A novel multi-dimensional multiple image encryption technique," *Multimedia Tools and Applications*, vol. 79, no. 19-20, pp. 12959–12994, 2020.

[57] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on DNA encoding and chaotic system," *Multimedia Tools and Applications*, vol. 78, no. 6, pp. 7841–7869, 2019.

[58] A. Rehman, D. Xiao, A. Kulsoom, M. A. Hashmi, and S. A. Abbas, "Block mode image encryption technique using two-fold operations based on chaos, MD5 and DNA rules," *Multimedia Tools and Applications*, vol. 78, no. 7, pp. 9355–9382, 2019.

[59] J. Wu, X. Liao, and B. Yang, "Image encryption using 2D Hénon-Sine map and DNA approach," *Signal Processing*, vol. 153, pp. 11–23, 2018.

[60] S. M. Pan, R. H. Wen, Z. H. Zhou, and N. R. Zhou, "Optical multi-image encryption scheme based on discrete cosine transform and nonlinear fractional Mellin transform," *Multimedia Tools and Applications*, vol. 76, no. 2, pp. 2933–2953, 2017.

[61] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on mixed image element and permutation," *Optics and Lasers in Engineering*, vol. 92, pp. 6–16, 2017.

[62] K. A. K. Patro, A. Soni, P. K. Netam, and B. Acharya, "Multiple grayscale image encryption using cross-coupled chaotic maps," *Journal of Information Security and Applications*, vol. 52, Article ID 102470, 2020.

[63] K. K. Patro and B. Acharya, "An efficient dual-layer cross-coupled chaotic map security-based multi-image encryption system," *Nonlinear Dynamics*, vol. 23, no. 3, 2021.

[64] J. Chen, Z. Zhu, L. Zhang et al., "Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption," *Signal Processing*, vol. 142, pp. 340–353, 2017.