Hindawi
Security and Communication Networks
Volume 2021, Article ID 6627005, 16 pages
https://doi.org/10.1155/2021/6627005

Research Article

Image Encryption Scheme Based on Block Scrambling, Closed-Loop Diffusion, and DNA Molecular Mutation

Li-Hua Gong, Jin Du, Jing Wan, and Nan-Run Zhou

Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China

Correspondence should be addressed to Nan-Run Zhou; nrzhou@ncu.edu.cn

Received 24 November 2020; Revised 15 January 2021; Accepted 1 February 2021; Published 22 February 2021

Academic Editor: Angel M. Del Rey

A new image encryption scheme is proposed with a combination of block scrambling, closed-loop diffusion, and DNA molecular mutation. The new chaotic block scrambling mechanism is put forward to replace the traditional swapping rule by combining the rectangular-ambulatory-plane cyclic shift with the bidirectional random disorganization. The closed-loop diffusion strategy is designed to form a feedback system, which improves the anti-interference capacity of the algorithm. To further destroy the blocks characteristics and eliminate the correlations among adjacent blocks, two efficient methods of DNA molecular mutation are adopted in the mutation stage. Moreover, the proposed algorithm possesses a large key space and the keys are highly related with the plaintext image. Experimental results demonstrate that the suggested image encryption strategy is practicable and has strong ability against a variety of common attacks.

1. Introduction

Lots of images travel over the Internet due to the shareability and the openness of network transmission, which may threaten the security of private image information. To tackle this problem, various image encryption algorithms have been put forward successively [1–4]. The main purpose of these algorithms is to encrypt the serviceable image information into a noise-like one. For example, Li devised an image encryption algorithm with a chaotic tent map, since the key stream generated with the modified chaotic sequence was more suitable for encryption [5]. To achieve lower computing consumption and increase efficiency on scrambling, Wang provided a fast color image encryption with correlated logistic map [6]. Nevertheless, the key distribution of the low-dimensional chaos is nonuniform, and the generated sequence is also unstable. Thus, some high-dimensional chaotic systems emerged [7, 8] and a new hyperchaotic system was explored [9]. It is capable of generating chaotic attractors with multiring and multiwing, which enables it to have complex dynamic behavior. Besides, hyperchaotic systems have a wider chaotic range and better ergodicity, which are extremely profitable for image encryption. It might be an ideal strategy to adopt multiple chaotic systems on a single image encryption system [10–12]. To effectively apply the advantages of composite chaotic systems and inherit their randomness, it is necessary to design the frameworks of confusion and diffusion carefully.

Scrambling could destroy the strong correlation among adjacent pixels. Quite a few image encryption algorithms sorted the random sequences generated from chaotic systems, and then the positions of the image pixels are rearranged with a group of index numbers. However, simply mapping the index into the ciphertext image pixels one by one might ignore some fixed points [13]. Furthermore, it has been pointed out that the periodicity and the inefficiency of traditional permutation architecture may not meet the security requirements [14–16]. Consequently, it is necessary to further study scrambling strategy. Shahna gave a permutation strategy on both pixel level and bit level, which makes the encryption algorithm complicated and realizes high-performance random permutation [17]. Xian constructed a fractal sorting matrix to perturb the elements in the plaintext image [18]. The disordered sorting matrix could be flexibly derived from an initial block to any size, and it was safer in image encryption. To complicate the scrambling process,

Wang split the plaintext image into four sub-blocks and executed various degrees of Arnold transform [19]. In addition, the statistical law of pixel values could be changed by an effective diffusion algorithm [20, 21]. Gong adopted the chaotic sequences to XOR the compressed plaintext directly [22]. The image might be partially revealed because the decryption between unrelated pixels would not affect each other [23]. Thus, Mirzaei suggested a new diffusion method in the cryptosystem, where the plaintext image was split into 4 subimages. Each encrypted pixel of the previous subimage participated in the operation of the next subimage pixel [24]. To hide the statistical structure of plaintext more effectively, Sheela alternately employed the two-level diffusion operations and the pixels transform in image encryption system. In the first diffusion level, each pixel was processed by two points relative to its position in the chaos matrix, while the next level was handled by the former ciphered pixel [25]. Although the diffusion operations were more complex, a tiny alteration of the pixel could only affect the latter ones [14, 26]. Once the diffusion sequence was obtained, the ciphered pixels could be decrypted in a reverse order.

There were also numerous image encryption algorithms combining chaos theory with DNA computing [27–32]. The kernel of these image encryption algorithms was to encode the image pixels with the DNA encoding rules and then to perform biological and algebraic manipulations on the encoded sequence. These manipulations include DNA addition and subtraction and base complementation rules. For instance, Jian encoded the plaintext image and the generated mask by the logistic map, and then they were added up with a DNA addition rule. Subsequently, a complement matrix was utilized to execute the base complementation rule, and the final encryption image was obtained with a DNA decoding rule [27]. It might be more beneficial to combine DNA with Chen's hyperchaotic system in an image composite encryption mechanism [28]. Nevertheless, the DNA computing rules used in the image encryption algorithm were not well designed. Even if the algorithm was very sensitive, its security would still be questionable under the passive attack, and the cryptanalyses discussed in [29, 30] proved that the algorithm in [28] was vulnerable to the chosen-plaintext attack. There are two main security issues with generally used manipulations. One is that all DNA manipulations are based on the binary calculation, and the coding results might be easily predicted with four DNA bases. The other is that DNA coding rules are fixed, which is not conducive to the security of image encryption algorithms. Thus, Yu expatiated the deletion and insertion operations of DNA-based image encryption to update the computational pattern [31], and two images were regarded as keys to each other, which strengthens the image cryptosystem security. Yang explained three DNA mutation operations on the 12 layers of DNA molecules [32]. The improved Lorenz sequences were employed to operate the interlayer and intramolecular mutations, so that the final mutation results are random and unpredictable.

In this paper, a new chaotic block scrambling mechanism will be investigated, which contains rectangular-ambulatory-plane cyclic shift and bidirectional random disorganization. The rings of each sub-block could be dynamically managed during cyclic shift, and pixels could be randomly selected and inserted during bidirectional random disorganization. In addition, the closed-loop diffusion strategy could form a feedback mechanism among the key block, the plaintext image, and the ciphertext image. To further alter the features of the ciphertext blocks, two kinds of DNA molecular mutation rules based on the theory of biological variation are adopted.

The structure of the remaining parts in this paper is as follows: some fundamental tools are explained in Section 2. In Section 3, the key generation, the block scrambling and the closed-loop diffusion algorithm, and the entire image encryption process are dwelled on. Section 4 provides simulation results and performance evaluations. A brief conclusion is drawn in Section 5.

2. Fundamental Knowledge

2.1. Affine Transform. Affine transform is a linear transform in the two-dimensional coordinates, which can extend/retract the image to any angle and direction. The general type of affine transform is

$$\begin{cases} x' = a_1 x + a_2 y + b_1, \\ y' = a_3 x + a_4 y + b_2, \end{cases} \tag{1}$$

where (x, y) is the initial coordinate, and (x', y') is the coordinate after transform. a_1, a_2, a_3, .., b_1, and b_2 are the parameters of affine transform.

2.2. Chaotic Systems. 2D logistic-sine-coupling map (2D-LSCM) was designed by combining logistic map with sine map to enhance the complexity of the chaotic behavior, where the control parameter δ belongs to $[0, 1]$ and the original position at (x_n, y_n) is updated to the new position at (x_{n+1}, y_{n+1}),

$$\begin{cases} x_{n+1} = \sin\left(\pi\left(4\delta x_n\left(1 - x_n\right) + (1 - \delta)\sin\left(\pi y_n\right)\right)\right), \\ y_{n+1} = \sin\left(\pi\left(4\delta y_n\left(1 - y_n\right) + (1 - \delta)\sin\left(\pi x_{n+1}\right)\right)\right). \end{cases} \tag{2}$$

2D logistic-adjusted-sine map (2D-LASM) is an integration of two 1D sine logistic modulation maps [33]. Its system parameter γ ranges from 0 to 1.

$$\begin{cases} x_{n+1} = \sin\left[\gamma\pi x_n\left(1 - x_n\right)\left(y_n + 3\right)\right], \\ y_{n+1} = \sin\left[\gamma\pi y_n\left(1 - y_n\right)\left(x_{n+1} + 3\right)\right]. \end{cases} \tag{3}$$

Henon map is a dynamical chaotic system in discrete-time, as described in equation (4). If the parameters λ_1 and λ_2 of Henon map are 1.4 and 0.3, respectively, it turns into a chaotic state,

$$\begin{cases} x_{n+1} = 1 - \lambda_1 x_n^2 + y_n, \\ y_{n+1} = \lambda_2 y_n. \end{cases} \tag{4}$$

2.3. Hilbert Curve. As a space filling curve, Hilbert curve could be utilized as a scan tool to scan the whole points on

the $2^n \times 2^n$ plane through quartering continuously [34]. The scan path starts from the right bottom, via the right top and the left top and ends at the left bottom of each square. Hilbert curve is a good shuffling tool to obtain a scrambled image. Figure 1 shows the Hilbert curves, which are drawn in the blocks of size 2^2, 4^2 and 8^2, respectively.

2.4. DNA Encoding Rules. The complementary pairing rule between the four nucleobases in DNA is analogous to the complementation of 0 and 1 in the binary system. If each nucleobase is represented by a two-digit binary, there will be 24 kinds of encoding rules. Since the limitations of DNA complementation rules should be taken into account, only 8 of them are acceptable. The 8 encoding rules are recorded in Table 1.

2.5. Mutation in DNA Molecules. Two kinds of DNA variation rules based on gene mutation are investigated to destroy the statistical law of images. The first one is the dynamic point substitution according to the rules of base transversion and base transition. A random sequence is employed to construct the mutation environment and the rule is listed in Table 2. The point substitution could only be performed when the random value is in the range from 0 to 3. The other DNA mutation is the cross mutation among adjacent chains, where the starting point of the exchange is random. Figure 2 illustrates the interchange pattern when the starting point is in the middle of the exchange chain.

3. Proposed Image Encryption Scheme

3.1. Generation of Random Sequences. To possess an excellent capacity against the differential attack, the original values of chaotic systems are restricted with both the MD5 hash values and the parity quantization values of the plaintext image. The 32-bit hexadecimal key stream M generated from the MD5 hash function is divided into 16 groups, represented as k_i, $i = 1, 2, \ldots, 16$,

$$k_i = h2d\left(M_{2(i-1)+1} + M_{2i}\right), \tag{5}$$

where $h2d(\cdot)$ converts a hexadecimal number into a decimal integer. The sum of k_i is denoted as $\mathrm{SUM} = \sum_{i=1}^{16} k_i$. The parity property of the plaintext image is

$$u = \mathrm{floor}\left[\mathrm{abs}\left(\frac{k_e - k_o}{\overline{e} - \overline{o}}\right)\right], \tag{6}$$

where the numbers of even and odd integers in the plaintext image are represented as k_e and k_o, respectively; $\overline{e}$ and $\overline{o}$ are the mean values of the even and odd numbers, respectively. Then, the initial values are computed as

$$\begin{aligned} x_j &= \frac{\left(\left(u + k_{4j}\right) \oplus k_{4j-2} \oplus \left(u + k_{4j-1}\right) \oplus k_{4j-3}\right)}{\mathrm{SUM}}, \\ j &= 1, 2, 3, 4, \\ y_1 &= \frac{\left(\sum_{j=1}^{6} k_j + u\right)}{\mathrm{SUM}}, \\ y_2 &= \frac{\left(\sum_{j=1}^{6} k_{2j} + u\right)}{\mathrm{SUM}}, \end{aligned} \tag{7}$$

where $A \oplus B$ means $\mathrm{bitxor}(A, B)$. x_1, x_2, x_3, x_4, y_1, and y_2 are the initial values. The three chaotic systems are iterated with corresponding times and the former 1000 iteration elements are discarded to avert the so-called transient effect. The specific parameter values are collected in Table 3.

3.2. Block Scrambling and Closed-Loop Diffusion. The mechanisms of block scrambling and closed-loop diffusion are constructed to shuffle the preprocessed blocks and to diffuse the scrambled blocks in a linkage system. The whole process can be represented as

$$B = \mathrm{SD}\left(P_H, X_{ls}, Y_{ls}, X_{la}, Y_{la}\right), \tag{8}$$

where $\mathrm{SD}(\cdot)$ is the block scrambling and closed-loop diffusion function; X_{ls}, Y_{ls}, X_{la}, and Y_{la} are four random sequences; P_H is the preprocessed plaintext block set and stored as a cell array of size $n \times n$, where n is set to 16. The $l-$th sub-block in the cell array can be labeled as $P_H(l)$. The flowchart of block scrambling and closed-loop diffusion is displayed in Figure 3. The specific process is given as follows:

Step 1. Rectangular-ambulatory-plane cutting: the rings of each sub-block $P_H(l)$ are extracted and stored in $O^{P_H(l)}$. The $x-$th ring in the sub-block $P_H(l)$ can be represented as $O_x^{P_H(l)}$, where x belongs to $\{1, 2, \ldots, 8\}$.

Step 2. Four sequences r_1, r_2, r_3, and r_4 of length n^2 are selected from X_{ls} and the elements in r_1, r_2, r_3, and r_4 are all converted into integers in $[0, 255]$. The control sequence f of length $8n^2$ is updated from X_{la}. When the number in X_{la} is less than 0.5, it is updated to -1; otherwise, it is updated to 1.

Step 3. The rectangular-ambulatory-plane cyclic shift operation is executed on each ring,

$$C_x^{P_H(l)} = \begin{cases} \mathrm{circshift}\left(O_x^{P_H(l)}, r_{(x+1)/2}, f\right), & x = 1, 3, 5, 7; \\ \mathrm{circshift}\left(O_x^{P_H(l)}, xr_{x/2}, f\right), & x = 2, 4, 6, 8, \end{cases} \tag{9}$$

where $\mathrm{circshift}(a', b', c')$ is a function for the bidirectional cyclic shift operation. a' is a ring to be operated, b' determines the shift times, and the ring $O_x^{P_H(l)}$ rotates clockwise when $c' < 0$. $C_x^{P_H(l)}$ is the

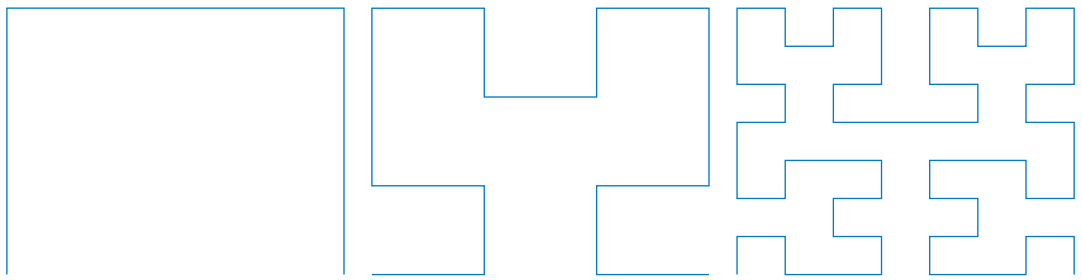


Figure 1: Hilbert curve of orders 1, 2, and 3, respectively. (a) Order 1. (b) Order 2. (c) Order 3.

Table 1: DNA encoding and decoding methods.

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: Points substitution rule.

Operation	Base transition		Base transversion		Fixed
Random sequence	0	1	2	3	Else
A	A	G	C	A	A
T	C	T	T	G	T
G	G	A	G	T	G
C	T	C	A	C	C

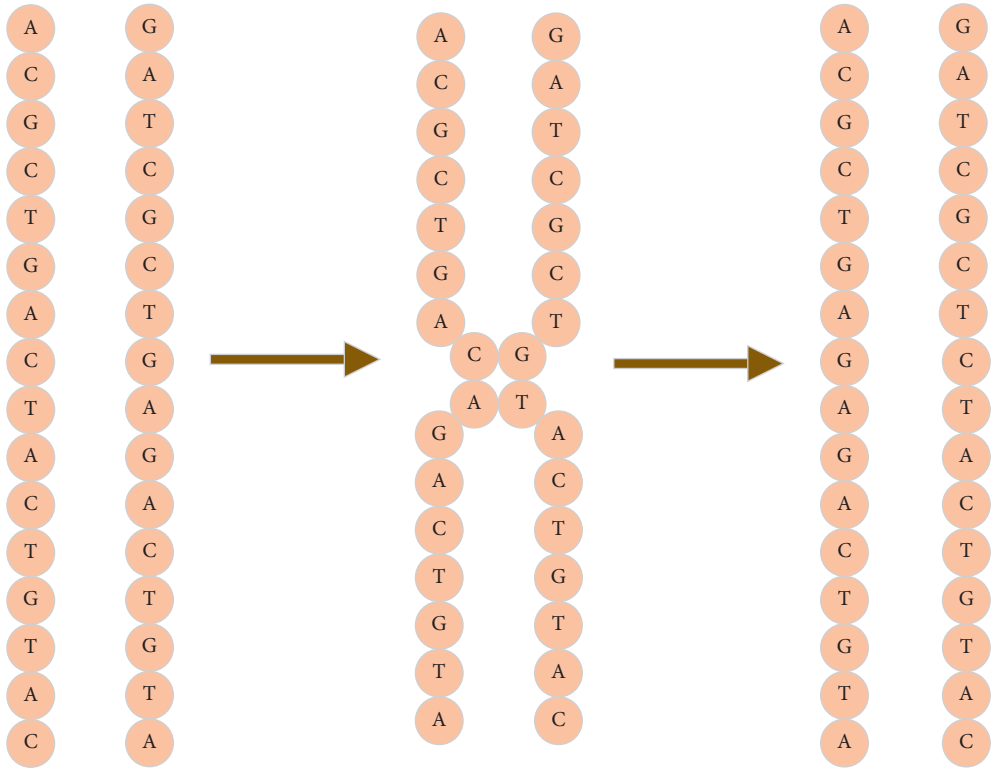


Figure 2: Cross-mutation among DNA chains.

Table 3: Parameter values of chaotic systems.

	2D-LSCM	2D-LASM	Henon map
Initial values	x_1, x_2	x_3, x_4	y_1, y_2
System parameters	$\delta = 0.8$	$\mu = 0.9$	$\lambda_1 = 1.4$, $\lambda_2 = 0.3$
Resulting random sequences	X_{ls}, Y_{ls}	X_{la}, Y_{la}	H_x, H_y

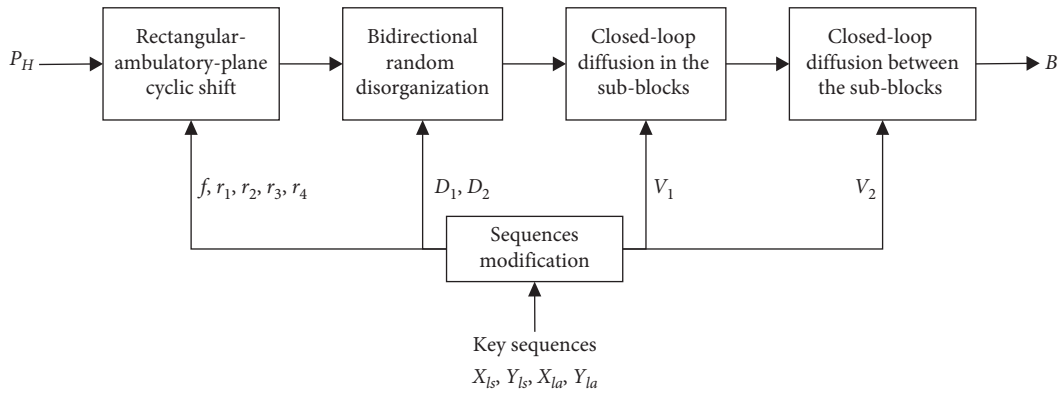


Figure 3: Block scrambling and closed-loop diffusion.

scrambled ring. After repeating the cyclic shift operation in each ring, a block set S is generated.

Step 4. Y_{ls} and Y_{la} are evenly divided into blocks, and then each sub-block of them is arranged in an ascending order to yield Y_{ls}' and Y_{la}', respectively. The corresponding index block sets are D_1 and D_2.

Step 5. Bidirectional random disorganization: each sub-block in S is scrambled by the double random block sets. The specific operation is

$$\begin{aligned} p' &= d_{\varphi}^{D_1(l)}, \\ p'' &= d_{\varphi}^{D_2(l)}, \\ k_{p''}^{K(l)} &= s_{p'}^{S(l)}, \end{aligned} \tag{10}$$

where $1 \le \varphi \le 256$; p' and p'' correspond to the φ − th pixels in $D_1(l)$ and $D_2(l)$, respectively; $s_{p'}^{S(l)}$ refers to the pixel extracted from the position p' of $S(l)$, and then all the extracted pixels are placed into a new block set K at a random position p''.

Step 6. Two key block sets V_1 and V_2 in the range of $[0, 255]$ are generated with Y_{ls}' and Y_{la}'. The overall ciphertext sub-blocks in K are diffused by

$$g_{\phi}^{G(l)} = \begin{cases} k_{\phi}^{K(l)} \oplus k_{n^2}^{K(l)} \oplus v_{\phi}^{V_1(l)}, & \phi = 1, \\ g_{\phi-1}^{G(l)} \oplus k_{\phi}^{K(l)} \oplus k_{\phi+1}^{K(l)} \oplus v_{\phi}^{V_1(l)}, & \phi = 2, 3, \ldots, n^2 - 1, \\ g_{\phi-1}^{G(l)} \oplus k_{\phi}^{K(l)} \oplus v_{\phi}^{V_1(l)}, & \phi = n^2, \end{cases} \tag{11}$$

where $G(l)$ is the sub-block when all the pixels in the sub-block $K(l)$ are updated.

Step 7. The diffusion operation between sub-blocks is subsequently executed. Then, the final ciphertext block set B is obtained after executing the closed-loop diffusion operation.

$$B(m) = \begin{cases} G(m) \oplus G\left(n^2\right) \oplus V_2(m), & m = 1, \\ B(m-1) \oplus G(m) \oplus G(m+1) \oplus V_2(m), & m = 2, 3, \ldots, n^2 - 1, \\ B(m-1) \oplus G(m) \oplus V_2(m), & m = n^2. \end{cases} \tag{12}$$

There exist some highlights in the above steps. First, the key blocks are associated with the plaintext image, and the proposed rectangular-ambulatory-plane cyclic shift takes full advantages of the chaotic sequences' randomness and scrambles each block efficiently. Also, the double random blocks mapping rule could attain the pixels extraction and insertion randomly at the same time. Ultimately, the blocks are related to each other after being diffused. The whole confusion and diffusion operations can strengthen the security of the block encryption process.

3.3. Image Encryption Scheme Based on Block Scrambling, Closed-Loop Diffusion, and DNA Molecular Mutation. In the proposed image encryption scheme, a global scrambling tool and a scanning method are adopted first. Subsequently, the strategy described in Section 2.5 will be executed and the ciphertext image will be obtained after mutation operations. The encryption steps are detailed as follows.

Step 1. The MD5 hash function and the parity formula are adopted on the plaintext image of size $N \times N$ to generate a key stream. The methods described in Section 3.1 are utilized to covert the key stream into several initial valves for the used chaotic systems. Six random sequences X_{ls}, Y_{ls}, X_{la}, Y_{la}, H_x, and H_y are generated according to the parameters in Table 3.

Step 2. Global scrambling: affine transform is exploited to scramble the plaintext image P for N times and generate a preliminary scrambled image P_A.

Step 3. P_A is evenly divided into $n \times n$ sub-blocks. These sub-blocks are treated as the points to be scanned, and then a shuffled block set P_H is obtained with the Hilbert matrix.

Step 4. Steps 1 to 7 in Section 3.2 are executed to accomplish block scrambling and closed-loop diffusion operations in the block set P_H and acquire a ciphered block set B.

Step 5. The key block h is randomly selected from D_1 to extract two sub-blocks located at $h(2z-1)$ and $h(2z)$ in B. Then, the extracted sub-blocks are converted into 8-bit blocks T_1 and T_2, respectively. They are subsequently spliced into Q,

$$\begin{aligned} Q(2\omega - 1) &= T_1(\omega), \\ Q(2\omega) &= T_2(\omega), \end{aligned} \tag{13}$$

where $1 \le \omega \le 8n^2$.

Step 6. The binary sequence Q is encoded into a DNA matrix E_1 of size $n \times 8n$, and the DNA encoding rule adopted in the DNA encoding operation is $R_c = \mathrm{mod}(h(2z-1) + h(2z), 8) + 1$.

Step 7. The random sequence f_1 utilized to construct the environment for point substitution could be calculated with equation (14), where $q \in [1, 4N^2]$. Then, the DNA molecules of E_1 are substituted by the DNA mutation rule listed in Table 2. After substitution, the DNA matrix is updated to ...

$$f_1(q) = \begin{cases} 1, & H_x(q) \in (0, 0.15], \\ 2, & H_x(q) \in (0.15, 0.35], \\ 3, & H_x(q) \in (0.35, 0.5], \\ 4, & H_x(q) \in (0.5, 0.65], \\ 5, & H_x(q) \in (0.65, 0.85], \\ 6, & H_x(q) \in (0.85, 1). \end{cases} \tag{14}$$

Step 8. The sequence f_2 calculated with equation (15) is in the set $\{1, 2, \ldots, n-1\}$ and is utilized to determine the starting point of cross-mutation,

$$\begin{aligned} f_2(q') = \mathrm{floor}\Big(\mathrm{mod}\Big(\big(\overline{H}_x(q') + H_y(q')\big) \\ \times 10^{14}, 15\Big) + 1\Big), \quad 1 \le q' \le 32N. \end{aligned} \tag{15}$$

The vertical adjacent DNA chains of E_2 would be exchanged randomly with f_2. For instance, W_1 and W_2 are the adjacent columns in E_2, and the molecules from points f_2 to n are exchanged. This process is expressed as

$$W' = \mathrm{exc}(W_1(f_2 : n), W_2(f_2 : n)), \tag{16}$$

where $\mathrm{exc}(a, b)$ is a function to exchange the values of a and b. After executing the cross-mutation operation on the whole adjacent columns in E_2, the DNA matrix E_3 is obtained.

Step 9. The DNA block set E_3 is converted into decimal numbers with the DNA decoding rule $R_d = \mathrm{mod}(h(2z-1) \times h(2z), 8) + 1$.

Step 10. Steps 5 to 9 are repeated until all the sub-blocks are traversed, and then the final ciphered image C is acquired after splicing the whole ciphered blocks.

The encryption image can be decrypted with the inverse process of the encryption algorithm, and the encryption and the decryption processes are summarized in Figure 4.

4. Simulation Results and Performance Analyses

To validate the reliability and the security of the proposed image encryption scheme based on block scrambling, closed-loop diffusion, and DNA molecular mutation, a series of numerical experiments with test images of size 256×256 are carried out in this section.

4.1. Encryption and Decryption Results and Quality Assessments. Figures 5(a)–5(c) show the plaintext images "Bridge," "Elaine," and "Bird," respectively. The corresponding encryption and decryption results are listed in Figures 5(d)–5(i). Visually, the ciphertext images reveal no information about the original ones, and Figures 5(g)–5(i) displayed that they can be decrypted intactly. To appraise the fidelity of the encryption and decryption images, the peak signal-to-noise ratio (PSNR) and the structural similarity index metric (SSIM) [35] are employed,

$$\mathrm{PSNR} = 10 \log_{10} \frac{S_1 \times S_2 \times 255^2}{\sum_{s_1=1}^{S_1} \sum_{s_2=1}^{S_2} [Q_1(s_1, s_2) - Q_2(s_1, s_2)]}, \tag{17}$$

where Q_1, Q_2 denote two contrast images and S_1, S_2 represent the image dimensions,

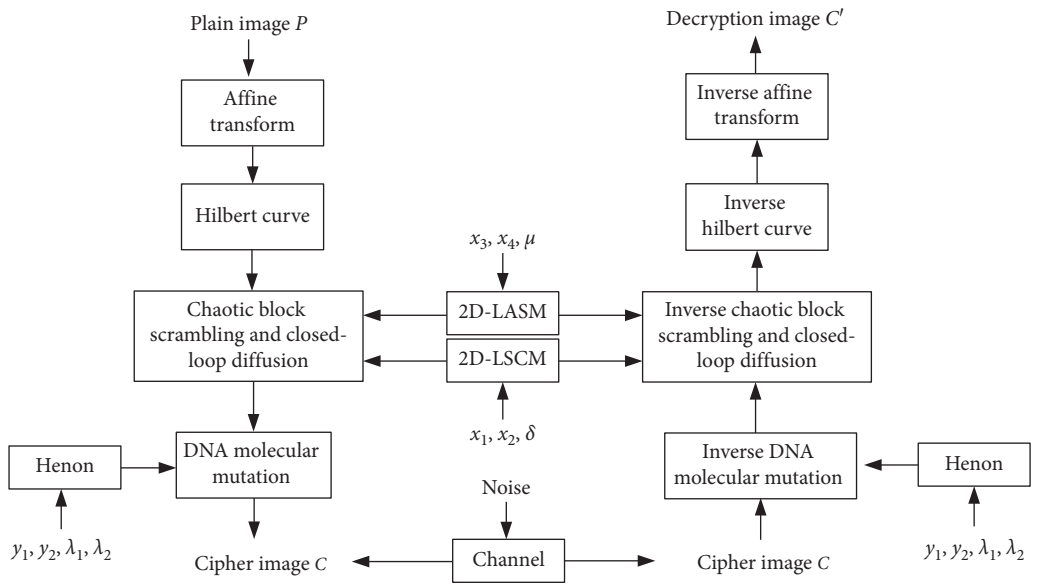


Figure 4: Encryption and decryption processes.

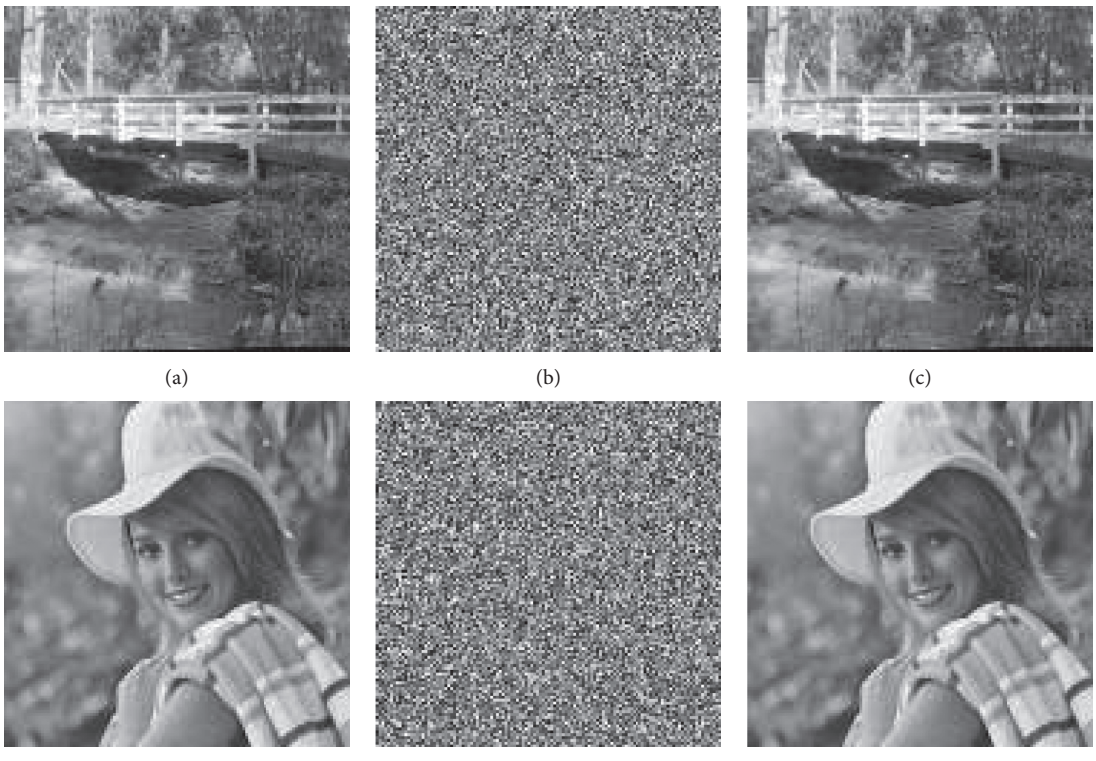
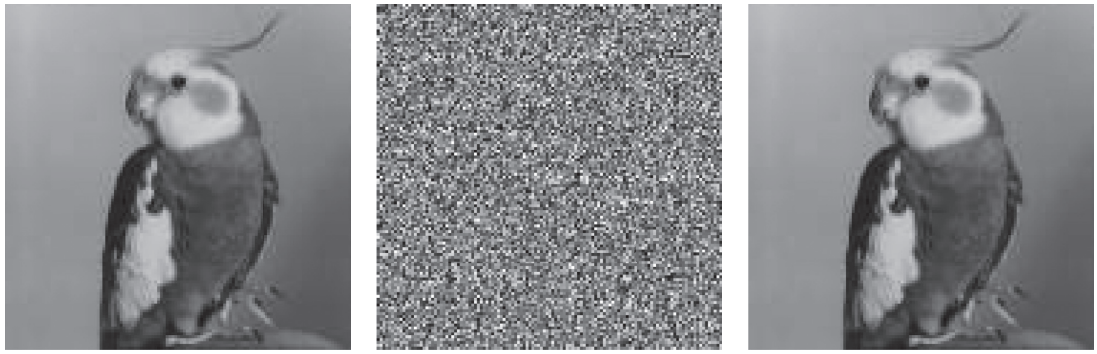


Figure 5: Continued.



(g) (h) (i)

Figure 5: Experiment results: (a)–(c) the plaintext images "Bridge," "Elaine," and "Bird," respectively; (d)–(f) the ciphertext images "Bridge," "Elaine," and "Bird," respectively; (g)–(i) correct decryption images (d)–(f).

$$\mathrm{SSIM}(m, m') = \frac{(2\mu_m\mu_{m'} + \zeta_1)(2\sigma_{mm'} + \zeta_2)}{(\mu_m^2 + \mu_{m'}^2 + \zeta_1)(\sigma_m^2 + \sigma_{m'}^2 + \zeta_2)}, \quad (18)$$

where $\mu_m = (1/\mathrm{ST}) \sum_{s=1}^{S} \sum_{s=1}^{T} m(s,t)$ and $\mu_{m'} = (1/\mathrm{ST}) \sum_{s=1}^{S} \sum_{t=1}^{T} m'(s,t)$ are the means for images m and m', respectively, σ_m^2 and $\sigma_{m'}^2$ are the images' variances, and $\sigma_{mm'}^2$ is their covariance. Constants $\zeta_1 = (v_1\ L)^2$ and $\zeta_2 = (v_2 L)^2$ can be obtained with $v_1 = 0.01$ and $v_2 = 0.03$ in the dynamic range L of an image. If the two images are nearly identical, the PSNR value would approach infinity and the SSIM value would approach 1. Thus, from the encryption results displayed in Table 4, the encryption images are severely disturbed, and the PSNR and the SSIM results for all the decryption images represent that there is no apparent data loss. In other words, the devised image encryption scheme based on block scrambling, closed-loop diffusion, and DNA molecular mutation could encrypt and decrypt images effectively.

4.2. Statistical Analyses

4.2.1. Histogram Analysis. The histograms of the plaintext images "Couple," "Camera," and "Peppers" are respectively presented in Figures 6(b)–6(j), while the histograms of their corresponding ciphertext images are exhibited in Figures 6(d)–6(l). The histograms after encryption are smoother with no raised spikes. This benefits from the devised close-loop block diffusion scheme and the mutation operation, which can distribute the pixel values uniformly in the range from 0 to 255. To further verify the histogram homogeneity, the chi-square test is adopted and the corresponding results are recorded in Table 5.

$$\chi^2 = \sum_{M=0}^{255} \frac{(k_s - o_s)^2}{o_s}, \quad (19)$$

where k_s is an observed frequency of the encryption image at level s and o_s represents the expected one. Theoretically, χ^2 should not be more than 293.2478 when the probability is 5%. Conclusively, it is impractical for an attacker to obtain the corresponding plaintext images with the histogram analysis attack, since the histograms of all test encryption images are smooth and featureless.

4.2.2. Correlation Coefficients of Adjacent Pixels. The high correlation among the adjacent pixels of a ciphertext image would increase the risk of being cracked [13]. To inspect the correlation between plaintext and ciphertext, 10,000 pairs of pixels are arbitrarily selected. As displayed in Figure 7, the scatter plots of the plaintext image seem like a linear distribution and the adjacent pixels are highly correlated. After executing the proposed strategies of confusion, diffusion, and DNA mutation, the positions and the values of the pixels are altered randomly and adequately. Therefore, the pixels of the corresponding ciphertext image are almost evenly dispersed on the plane. It can be seen from Tables 6 and 7 that our scheme is more effective in reducing the correlation and can stand up to the statistical analysis attack.

4.2.3. Information Entropy. Shannon entropy is a commonly used indicator to evaluate the randomness,

$$H(v) = \sum_{i=0}^{N-1} p(v) \log \frac{1}{p(v_i)}, \quad (20)$$

where $p(v_i)$ refers to the probability of the random gray value v_i. However, compared with the local entropy [41], the global Shannon entropy is insufficient in evaluating the uniformity. The local entropy is the sample average value of the global Shannon entropy of 1936 pixels taken from 30 nonoverlapping image blocks, which is more accurate, consistent, and efficient. The results of global and local entropies with our image encryption scheme are exhibited in Table 8, which are very close to 8 bits. Based on the above analysis, the information entropy analysis attack on our proposed image encryption scheme is ineffective.

4.3. Sensibility Analyses

4.3.1. Key Sensitivity Analysis. To rate the key sensitivity, simulation experiments are executed under a slight alteration of the correct keys. In Figure 8, the decryption images

Table 4: Quality assessments for different encryption and decryption images.

	Bridge		Elaine		Bird	
	PSNR (dB)	SSIM	PSNR (dB)	SSIM	PSNR (dB)	SSIM
Encryption image	8.7682	0.0104	9.2925	0.0096	9.3112	0.0090
Decryption image	∞	1	∞	1	∞	1

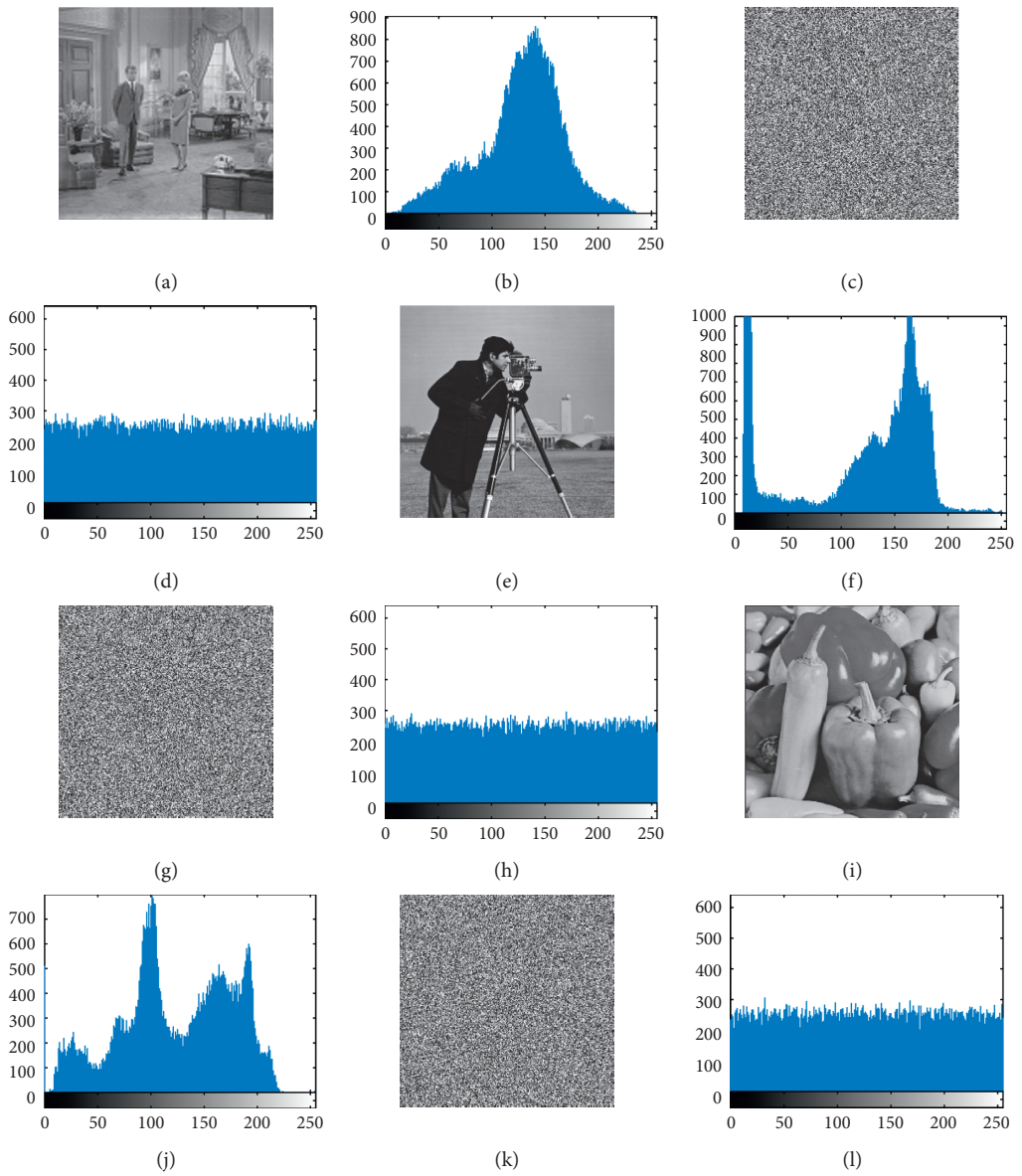


Figure 6: Histograms of several images: (b)–(j) the histograms for the plaintext images (a)–(i); (d)–(l) the histograms for the ciphertext images (c)–(k).

Table 5: Chi-square results for ciphertext images.

Image	Couple	Camera	Peppers
χ^2_{test}	226.6016	244.3672	240.0391
χ^2_{255}	293.2478	293.2478	293.2478
Decision	Accepted	Accepted	Accepted

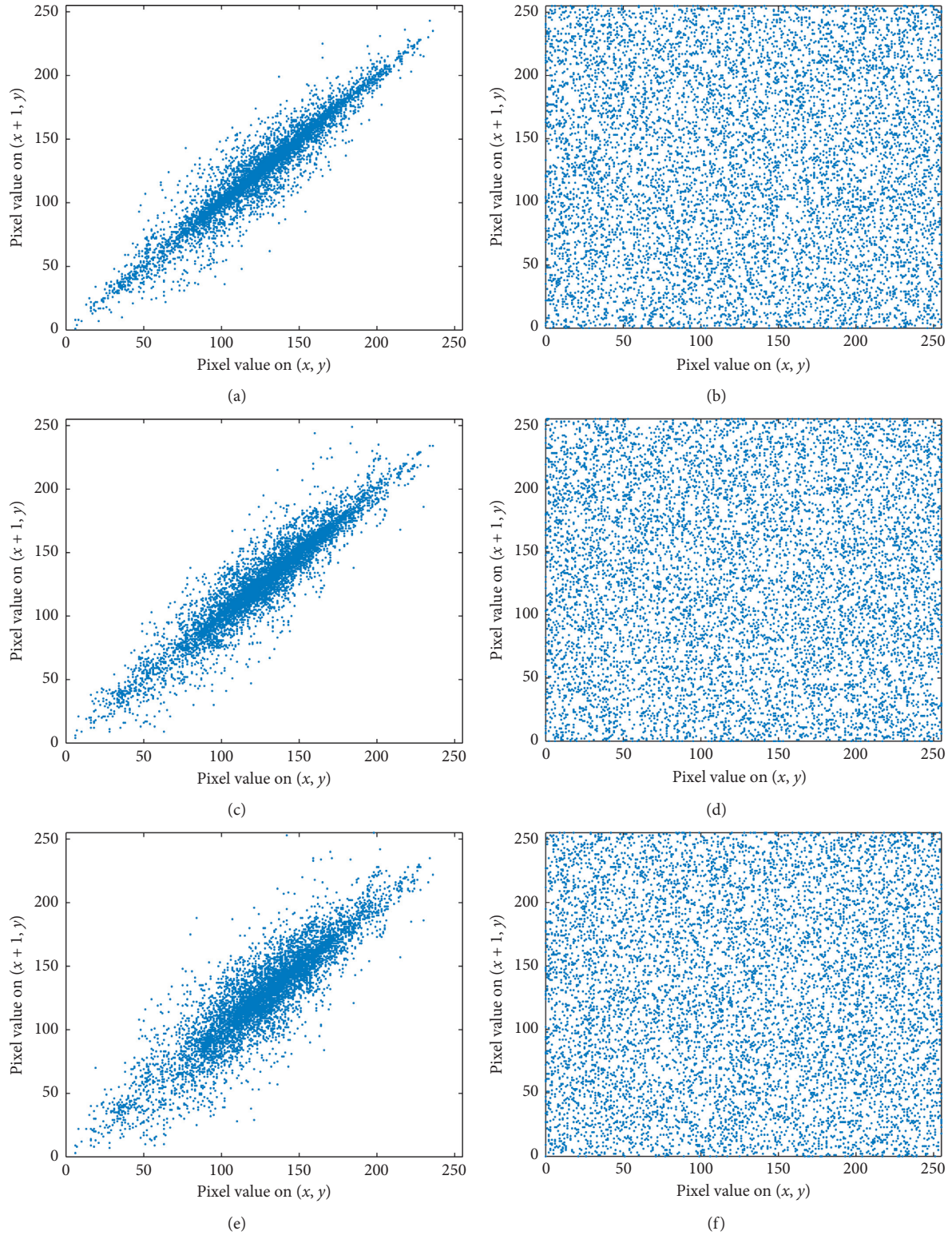


Figure 7: Correlation coefficients of the plaintext image "Couple" and the ciphertext one in three directions: (a) "Couple," vertical direction (VD). (b) "Couple," horizontal direction (HD). (c) "Couple," diagonal direction (DD). (d) Ciphertext image, VD. (e) Ciphertext image, HD. (f) Ciphertext image, DD.

are noise-like ones and will not reveal any meaningful information. The accuracy of the key would seriously affect the image decryption. Therefore, the proposed encryption scheme based on block scrambling, closed-loop diffusion, and DNA molecular mutation could withstand the brute-force attack successfully.

Table 6: Correlation coefficients of plaintext images and ciphertext ones.

Test image	Plaintext image			Ciphertext image		
	HD	VD	DD	HD	VD	DD
Bridge	0.8491	0.8869	0.8187	0.0026	0.0029	−0.0009
Elaine	0.9576	0.9483	0.9316	−0.0010	−0.0008	−0.0036
Bird	0.9908	0.9811	0.9711	0.0000	0.0035	0.0000
Couple	0.9439	0.9424	0.9150	−0.0015	−0.0016	−0.0004
Camera	0.9615	0.9321	0.9058	0.0002	−0.0018	0.0003
Peppers	0.9535	0.9439	0.8988	0.0021	0.0014	0.0002

Table 7: Correlation coefficients of image "Peppers" obtained by other encryption schemes.

Direction	Ref. [36]	Ref. [37]	Ref. [38]	Ref. [39]	Ref. [40]	Our scheme
HD	0.0057	−0.0056	0.0234	0.0068	−0.0160	0.0021
VD	0.0037	−0.0162	0.0121	−0.0022	0.0350	0.0014
DD	0.0043	−0.0202	0.0005	0.0005	−0.0097	0.0002

Table 8: Global and local Shannon entropies.

Image	Plaintext image entropy (bit)	Global Shannon entropy (bit)	Local Shannon entropy (bit)	Local entropy critical values (bit)		
				$h_{\text{left}}^{1*0.05} = 7.9019$ $h_{\text{right}}^{1*0.05} = 7.9030$	$h_{\text{left}}^{1*0.01} = 7.9017$ $h_{\text{left}}^{1*0.01} = 7.9032$	$h_{\text{left}}^{1*0.001} = 7.9015$ $h_{\text{left}}^{1*0.001} = 7.9034$
Couple	7.3021	7.9986	7.9025	Pass	Pass	Pass
Camera	7.0097	7.9990	7.9026	Pass	Pass	Pass
Peppers	7.5327	7.9983	7.9023	Pass	Pass	Pass

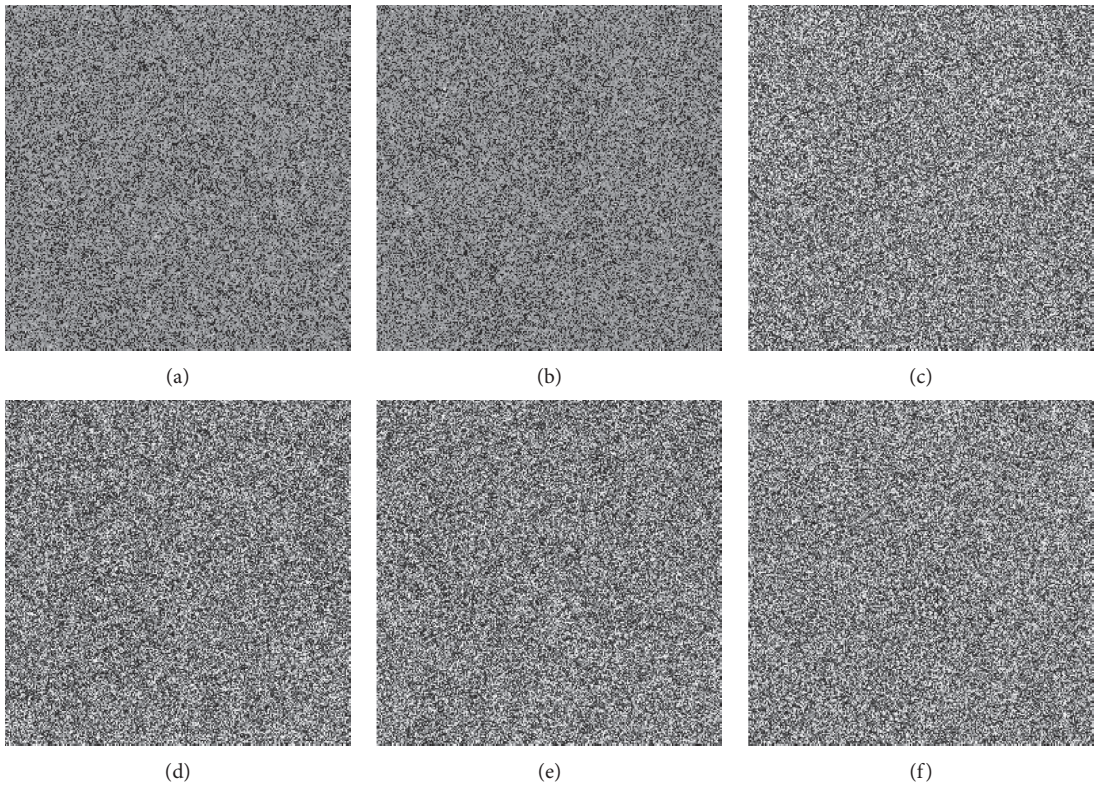


Figure 8: Decryption image "Camera" with incorrect keys: (a) $x_1 = 0.3623 \times 10^{-16}$, (b) $x_2 = 0.3281 + 10^{-16}$, (c) $x_3 = 0.3102 + 10^{-15}$, (d) $x_4 = 0.5263 + 10^{-15}$, (e) $y_1 = 0.7035 + 10^{-15}$, and (f) $y_2 = 0.5794 + 10^{-15}$.

4.3.2. Key Space Analysis. Exhaustive attack may threaten the cryptosystem security, but the key space expansion would make it harder to defeat the system. In the proposed algorithm, the initial values x_1, x_2, x_3 x_4, y_1, and y_2 for chaotic systems are the main keys. These initial values are all specified within $(-1, 1)$ and the simulation results demonstrate that the computational precision of the above key space are about 10^{-15} or 10^{-16}. Totally, the key space of the devised image encryption scheme is about 10^{92}, which is larger than the key space in [42]. Therefore, the brute-force attack is impracticable for the presented image encryption scheme based on block scrambling, closed-loop diffusion, and DNA molecular mutation.

4.3.3. Differential Attack Analysis. The number of pixel change rate (NPCR) and the unified average changing intensity (UACI) are applied to assess the sensitivity of the image encryption systems and the differential attack resistance,

$$\begin{aligned} \mathrm{NPCR}(\%) &= \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{G(i,j)}{M\times N}\times 100, \\ \mathrm{UACI}(\%) &= \sum_{i=1}^{M}\sum_{j=1}^{N}\left(\frac{\left|g(i,j)-g'(i,j)\right|}{255\times M\times N}\right)\times 100, \\ G(i,j) &= \begin{cases} 0, & g(i,j)=g'(i,j), \\ 1, & g(i,j)\neq g'(i,j), \end{cases} \end{aligned} \tag{21}$$

where g and g' are the ciphertext images of size $M \times N$ corresponding to the normal test image and the one pixel altered test image. The NPCR values and the UACI values of various test images are tabulated in Tables 9 and 10 compiles the results of other schemes with "Peppers." The results are close to their ideal values, indicating that the pixel change has a big impact on the encryption results. It substantiates that the proposed image encryption strategy could resist the differential attack.

4.4. Robustness Analyses under Attack

4.4.1. Chosen-Plaintext Attack. In our proposed scheme, the key stream is highly connected with the plaintext. It is composed of the MD5 hash values and the quantization values of the plaintext image. In other words, the slight change of the plaintext will have a great impact on the entire image encryption system, and in the designed closed-loop diffusion algorithm, the ciphertext blocks are interconnected with the key blocks and the plaintext blocks. Hence, a linkage system is formed that not only invalidates differential attack but also invalidates the chosen-plaintext. Besides, the mutations performed between two random selected sub-blocks are nonlinear operations, which render an attacker incapable of obtaining the correct keys. In brief, the presented image encryption system is nonlinear and the entire encryption blocks are highly interconnected, which make it immune to chosen-plaintext attack.

4.4.2. Gaussian Noise Attack. Assume the Gaussian noise attack is modeled as

$$E' = E + kN_G, \tag{22}$$

where E' is the encryption image affected by noise and E is the normal encryption one, N_G represents the white Gaussian noise with the standardized normal distribution, and k is the noise intensity. Figure 9 shows the simulation results when "Camera" is polluted by the white Gaussian noise of different intensities. Its primary information is still visible as the noise intensity increases, and the MSE curve in Figure 10 indicates that the proposed image encryption scheme is immune to the white Gaussian noise attack to a certain degree.

4.4.3. Salt and Pepper Noise Attack. The encryption "Camera" is added with Salt and Pepper noise of different variances 0.01, 0.05, 0.07, and 0.1, respectively. The test results are shown in Figures 11(a)–11(d), and it could verify that the proposed image encryption technology based on block scrambling, closed-loop diffusion, and DNA molecular mutation has a certain anti-interference ability under Salt and Pepper noise attack.

4.4.4. Occlusion Attack. Experiments with varying extents of data loss are executed on "Elaine," and the decryption images after cropping in different positions or sizes are shown in Figures 12(a)–12(d). The cropped pixels of the decryption images are replaced by 0. The devised operations, rectangular-ambulatory-plane cyclic shift and the bidirectional random disorganization, are controlled by the cascade chaotic systems. They would rearrange the image pixels stochastically, which makes the decryption results of the same size cropping in different positions similar. Visually, the encryption images in Figure 12 still contain general information as the cutting area increases. Thus, the proposed image encryption system has certain robustness against the cropping attack.

4.5. Computation Complexity and Execution Time. The computation complexity of an image encryption algorithm will greatly affect the execution time. To this end, complexity analysis is carried out for the main encryption modules in our algorithm. The total complexity is $O(2N^2)$ for the block scrambling and closed-loop diffusion module. Specifically, the rectangular-ambulatory-plane cyclic shift operation is executed in 8 rings and the complexity is $O(8N)$. The subsequent bidirectional random disorganization operation would traverse all of the image pixels, whose complexity is $O(N^2)$. The complexities of the intrablock diffusion and the outer-block diffusion are $O(N^2)$ and $O(N)$, respectively. The total complexity for the DNA mutation module is $O(17N^2)$. The complexity of encoding and decoding process is $O(8N^2)$. The complexities of the concatenation operations of binary sub-blocks and the conversion of the decimal matrices are $O(4N^2)$ and $O(N^2)$, respectively, and the complexity for the mutation processes in the sub-blocks is

Table 9: NPCR and UACI analyses of the proposed scheme.

Image	Bridge	Elaine	Bird	Couple	Camera	Peppers
NPCR	99.6263	99.6082	99.6107	99.6086	99.6124	99.6285
UACI	33.4248	33.4387	33.4013	33.4077	33.4170	33.3803

Table 10: NPCR and UACI results of other schemes with "Peppers."

Scheme	Ref. [36]	Ref. [37]	Ref. [38]	Ref. [39]	Ref. [40]	Our scheme
NPCR	99.5867	99.6319	99.4742	99.5538	99.6224	99.6285
UACI	36.6878	33.6923	33.1816	33.3541	33.5421	33.3803

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

Figure 9: Gaussian noise on "Camera" with different noise intensities: (a) $k = 1$, (b) $k = 10$, (c) $k = 20$, and (d) $k = 30$.

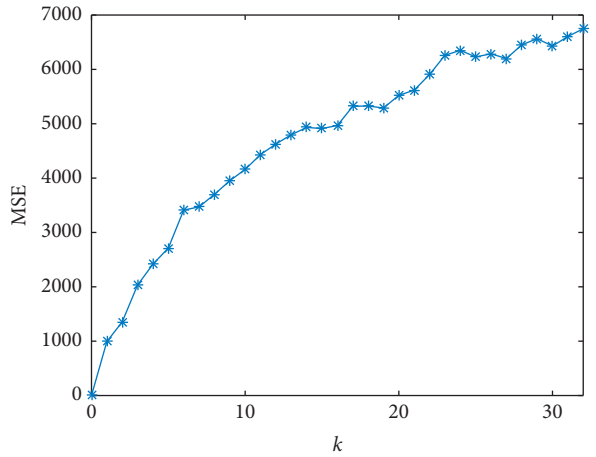


Figure 10: MSE curve with variation of noise intensity.

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

Figure 11: Salt and Pepper noise attack on image "Camera" with different variances: (a) 0.01; (b) 0.05; (c) 0.07; (d) 0.1.

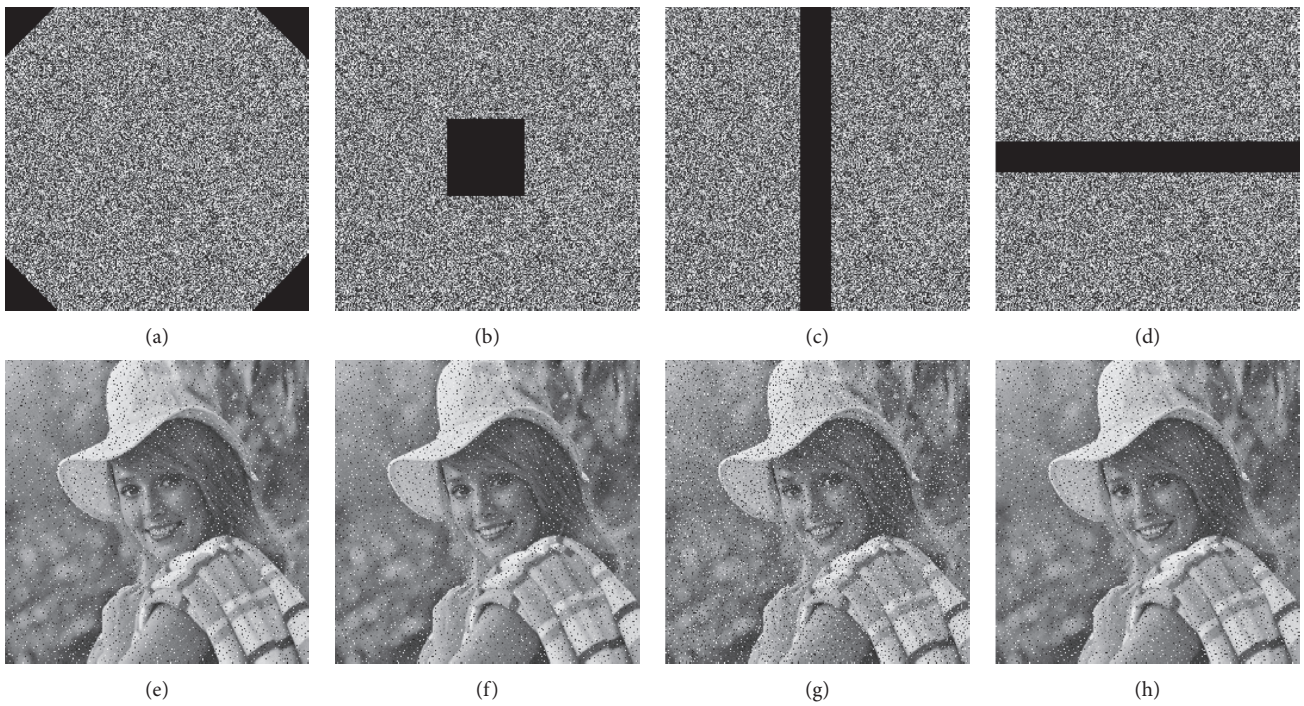


Figure 12: (a), (c)) The encryption "Elaine" with 6.5% cropped; ((b), (d))the corresponding decryption ones; ((e), (g)) the encryption "Elaine" with 10% cropped; ((f), (h)) the corresponding decryption ones.

$O(4N^2)$. The computation time of the algorithm is related to the program design, operating environment, and so on. The proposed image encryption algorithm is carried out under MATLAB (version R2016a) on the computer with 8 GB RAM and Windows 10. In our scheme, the operations of the block scrambling and closed-loop diffusion need one-round encryption only, which costs 0.200 s, and the DNA mutation process takes 14.147 s. Since the encoding and decoding rules for each selected sub-block are different, more iterations are involved, so it takes longer execution time. The complete encryption process needs 16.906 s, which is acceptable for most of the real-time image encryption schemes and also should be reduced for some cases.

5. Conclusion

A novel secure image encryption scheme with block scrambling, closed-loop diffusion, and the strategy of DNA molecular mutation is presented. During the block scrambling phase, the rectangular-ambulatory-plane cyclic shift and the bidirectional random disorganization are utilized to scramble the preprocessed blocks completely, and the results of the correlation coefficients demonstrate that our scheme inherits the randomness of chaotic sequences more effectively. The feedback mechanism in the diffusion phase is constructed with a new closed-loop block diffusion strategy, which improves the ability against the differential attack. The final encryption image is obtained with the DNA molecular mutation operations. Different types of simulation experiments and theoretical analyses demonstrate that the proposed image encryption scheme has strong reliability and high security.

Data Availability

The data can be available on request from the corresponding author.

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 Cultivation Plan of Applied Research of Jiangxi Province (Grant no. 20181BBE58022), and the Research Foundation of the Education Department of Jiangxi Province (Grant no. GJJ190203).

References

[1] C. Chen and K. Sun, "An improved image encryption algorithm with finite computing precision," *Signal Processing*, vol. 48, Article ID 102361, 2019.

[2] Z. J. Huang, S. Cheng, L. H. Gong, and N. R. Zhou, "Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform," *Optics and Lasers in Engineering*, vol. 124, Article ID 205821, 2020.

[3] Y. Xian, X. Wang, X. Yan, Q. Li, and X. Wang, "Image encryption based on chaotic sub-block scrambling and chaotic digit selection diffusion," *Optics and Lasers in Engineering*, vol. 134, Article ID 106202, 2020.

[4] 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.

[5] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 127–133, 2017.

[6] X. Wang and H.-l. Zhang, "A color image encryption with heterogeneous bit-permutation and correlated chaos," *Optics Communications*, vol. 342, pp. 51–60, 2015.

[7] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D logistic-sine-coupling map for image encryption," *Signal Processing*, vol. 149, pp. 148–161, 2018.

[8] Y. Xie, J. Yu, S. Guo, Q. Ding, and E. Wang, "Image encryption scheme with compressed sensing based on new three-dimensional chaotic system," *Entropy*, vol. 21, no. 9, p. 819, 2019.

[9] Z. B. Zhuang, J. Li, J. Y. Liu, and S. Q. Chen, "Image encryption algorithm based on new five-dimensional multi-ring multi-wing hyperchaotic system," *Acta Physica Sinica*, vol. 69, no. 4, Article ID 040502, 2020.

[10] Q. Cai, "A secure image encryption algorithm based on composite chaos theory," *Traitement Du Signal*, vol. 36, no. 1, pp. 31–36, 2019.

[11] Y. Abanda and A. Tiedeu, "Image encryption by chaos mixing," *IET Image Processing*, vol. 10, no. 10, pp. 742–750, 2016.

[12] X. Y. Wang, N. N. Guan, H. Y. Zhao, S. W. Wang, and Y. Q. Zhang, "A new image encryption scheme based on coupling map lattices with mixed multi-chaos," *Scientific Reports*, vol. 10, no. 1, p. 9784, 2020.

[13] Y. Wang, K.-W. Wong, X. Liao, T. Xiang, and G. Chen, "A chaos-based image encryption algorithm with variable control parameters," *Chaos, Solitons & Fractals*, vol. 41, no. 4, pp. 1773–1783, 2009.

[14] W. Zhang, H. Yu, Y.-l. Zhao, and Z.-l. Zhu, "Image encryption based on three-dimensional bit matrix permutation," *Signal Processing*, vol. 118, pp. 36–50, 2016.

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

[16] Z.-h. Gan, X.-l. Chai, D.-j. Han, and Y.-r. Chen, "A chaotic image encryption algorithm based on 3-D bit-plane permutation," *Neural Computing and Applications*, vol. 31, no. 11, pp. 7111–7130, 2019.

[17] K. Shahna and A. Mohamed, "A novel image encryption scheme using both pixel level and bit level permutation with chaotic map," *Applied Soft Computing*, vol. 90, Article ID 106162, 2020.

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

[19] X. Wang and S. Gao, "Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network," *Information Sciences*, vol. 539, pp. 195–214, 2020.

[20] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Processing*, vol. 144, pp. 134–144, 2018.

[21] X. Wang and S. Gao, "Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory," *Information Sciences*, vol. 507, pp. 16–36, 2020.

[22] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An image compression and encryption algorithm based on chaotic system and compressive sensing," *Optics & Laser Technology*, vol. 115, pp. 257–267, 2019.

[23] F. Y. Sun and Z. W. Lu, "Digital image encryption with chaotic map lattices," *Chinese Physics B*, vol. 20, no. 4, pp. 405–411, 2011.

[24] O. Mirzaei, M. Yaghoobi, and H. Irani, "A new image encryption method: parallel sub-image encryption with hyper chaos," *Nonlinear Dynamics*, vol. 67, no. 1, pp. 557–566, 2012.

[25] S. J. Sheela, K. V. Suresh, and D. Tandur, "Image encryption based on modified Henon map using hybrid chaotic shift transform," *Multimedia Tools and Applications*, vol. 77, no. 19, pp. 25223–25251, 2018.

[26] 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.

[27] A. Jian and N. Rajpal, "A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps," *Multimedia Tools and Applications*, vol. 75, no. 10, pp. 5455–5472, 2016.

[28] Q. Zhang, L. Guo, and X. Wei, "A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system," *Optik-International Journal for Light and Electron Optics*, vol. 124, no. 18, pp. 3596–3600, 2013.

[29] T. Xie, Y. Liu, and J. Tang, "Breaking a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system," *Optik*, vol. 125, no. 24, pp. 7166–7169, 2014.

[30] Y. Zhang, W. Wen, M. Su, and M. Li, "Cryptanalyzing a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system," *Optik*, vol. 125, no. 4, pp. 1562–1564, 2014.

[31] W. Yu, Y. Liu, L. Gong, M. Tian, and L. Tu, "Double-image encryption based on spatiotemporal chaos and DNA operations," *Multimedia Tools and Applications*, vol. 78, no. 14, pp. 20037–20064, 2019.

[32] Y. Liu and J. D. Zhang, "A multidimensional chaotic image encryption algorithm based on DNA coding," *Multimedia Tools and Applications*, vol. 79, no. 29-30, pp. 21579–21601, 2020.

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

[34] X. Zhang, L. Wang, Z. Zhou, and Y. Niu, "A chaos-based image encryption technique utilizing Hilbert curves and H-fractals," *IEEE Access*, vol. 7, pp. 74734–74746, 2019.

[35] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, 2004.

[36] M. Kar, M. K. Mandal, D. Nandi, A. Kumar, and S. Banik, "Bit-plane encrypted image cryptosystem using chaotic, quadratic, and cubic maps," *IETE Technical Review*, vol. 33, no. 6, pp. 651–661, 2016.

[37] A. Belazi, A. A. Abd El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, 2016.

[38] S. Q. Zhu, C. X. Zhu, Y. Fu, W. M. Zhang, and X. T. Wu, "A secure image encryption scheme with compression-confusion-diffusion structure," *Multimedia Tools and Applications*, vol. 19, no. 43-44, pp. 31957–31980, 2020.

[39] M. Ghazvini, M. Mirzadi, and N. Parvar, "A modified method for image encryption based on chaotic map and genetic

algorithm," *Multimedia Tools and Applications*, vol. 79, no. 37-38, pp. 26927–26950, 2020.

[40] M. A. B. Farah, A. Farah, and T. Farah, "An image encryption scheme based on a new hybrid chaotic map and optimized substitution box," *Nonlinear Dynamics*, vol. 99, no. 4, pp. 3041–3064, 2020.

[41] 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.

[42] D. D. Liu, W. Zhang, H. Yu, and Z. L. Zhu, "An image encryption scheme using self-adaptive selective permutation and inter-intra-block feedback diffusion," *Signal Processing*, vol. 151, pp. 130–143, 2020.