IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 15, 2020, accepted February 2, 2020, date of publication February 5, 2020, date of current version February 13, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2971759

A Fast Chaotic Image Encryption Scheme With Simultaneous Permutation-Diffusion Operation

LIDONG LIU, YUHANG LEI, AND DAN WANG
School of Information Engineering, Chang'an University, Xi'an 710064, China

Corresponding author: Yuhang Lei (1609647805@qq.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61701043 and Grant 41874140, and in part by the Fundamental Research Funds for the Central Universities of China under Grant 300102248103 and Grant 300102249318.

ABSTRACT In this paper, a secure and fast chaotic image encryption scheme with simultaneous permutation-diffusion operation is proposed. We combine permutation and diffusion processes into a whole, namely, simultaneous permutation and diffusion operation (SPDO). This can solve the problem of traditional encryption scheme in which the permutation and diffusion are two independent processes, that leads attackers to crack the two processes separately. In SPDO, the initial value of the current Sine-Sine chaotic map is related to the secret keys and the previous encrypted pixels' values. In this case, the proposed scheme can generate dynamic key streams and indexes that are related to plaintext, which improves the sensitivity to plaintext for the encryption scheme. In addition, the pixel values are processed by row and column (row-level and column-level) during the encryption procedure. Thus, the proposed scheme presents lower time complexity and faster running speed compared with bit-level or pixel-level image encryption schemes, which makes the proposed scheme be conducive to the batch transmission and real-time transmission of digital images. The simulation results and security analysis show that our scheme can resist common attacks, such as statistical attack, differential attack, chosen plaintext attack and other comprehensive attacks.

INDEX TERMS Permutation-diffusion operation, fast encryption, chaotic system, image encryption, security analysis.

I. INTRODUCTION

With the wide application of information technology, secure and efficient transmissions of digital images capture the attention of researchers. It is noted that images have some intrinsic features, such as high redundancy, bulk data capacity, and strong correlation. Therefore, the encryption effect of digital image is unsatisfactory by using traditional encryption technologies, such as DES and AES [1], [2]. When designing image encryption schemes, we must not only ensure the security of the transmission, but also take into account the encryption speed.

In recent years, a large number of image encryption schemes based on chaos [4]–[7], [15]–[32], [34]–[47] have been proposed, due to some inherent features of chaotic system such as noise-like, ergodicity and extreme sensitivity to initial parameters [3], [33], [48]–[50]. For example, Wang *et al.* [4] used the Logistic map in image encryption. Pak and Huang [5] constructed a new one-dimensional chaotic system to permute and diffuse the image pixels' value. Saljoughi and Mirvaziri [6] encrypted the values of the image pixels by applying three nonlinear chaotic sequences (three-dimensional Logistic maps). Luo *et al.* [7] used the piecewise linear chaotic map and four-dimensional hyper-chaotic map in their parallel image encryption scheme. The above encryption algorithms are traditional permutation-diffusion architecture (they are two separated stages and not related to the plaintext) as depicted in [8], which is vulnerable to be cracked by using chosen plaintext attack. For example, Tu *et al.* [9] and Wang *et al.* [10] cracked the diffusion process and the permutation process of the encryption schemes presented in [4], [5] respectively by developing chosen plaintext attack. Accordingly, in order to resist chosen plaintext attack, a lot of encryption schemes related to plaintext [11], [12], [28]–[32] are proposed. For example, in [11], the keystream is designed dependent upon the sum of pixels' squares of the plain image. In [12], the keystream of the permutation process is related to the sum of pixel values of the plain image, and the keystream

The associate editor coordinating the review of this manuscript and approving it for publication was Qiang Lai.

of the diffusion process is related to the selected nine pixel values of the permuted image in fixed positions. In [13], the secret matrix of the diffusion process is related to the pixel value of the plain image in secret location. However, the plaintext-related encryption schemes with the separated permutation-diffusion architecture can also be cracked by using chosen plaintext attack. For example, Liu *et al.* [14] cracked the scheme [12] by developing twice chosen plaintext attacks. They cracked the diffusion process by constructing a special image, and the nine-pixel values of the permuted image of the special image in fixed positions are identical with those in the cipher image. Then they cracked the permutation process by the obtained permuted image. Fan *et al.* [15] cracked the encryption scheme [13] by applying seven times chosen plaintext attacks. Firstly, they calculated the secret location by selecting two images with the same pixel sum. Secondly, they obtained the diffusion process by calculating the secret matrix. Finally, they cracked the permutation process by using the obtained secret matrix and the chosen special image and then recovered the plain image.

In order to resist the separated attack, image encryption schemes based on SPDO are presented in [16]–[18]. In [16], the permutation and diffusion processes are combined into one stage. Therefore, the attackers cannot crack the permutation and diffusion process independently and then the scheme can resist the separated attack. In addition, the encryption algorithm needs two rounds to achieve the desired encryption effect. In [17], the author permuted and diffused the pixel values simultaneously by using modified Logistic chaotic map. When a pixel value is processed, the chaotic map is iterated once again. If a size $M \times N$ image is encrypted, the chaotic map needs to be re-iterated $M \times N$ times. The encryption scheme can resist the separated attack and relieve the dynamic degradation problem [19], but it costs amounts of time for multi-image transmission. In [18], the pixels' values were encrypted by being converted into a pixel-cube. The scheme provides a single permutation-diffusion operation, in which the pixels' indexes are determined by the chaotic map, and the current encrypting pixel's value is related to the previous ciphertext. The encryption scheme has excellent security capacity and can resist the separated attack. However, the scheme has high time complexity and its encryption speed may not meet the requirements of real-time transmission. In addition, the first selected encrypted pixel value depends on the sum of pixel values of the plain image and chaotic maps, which prevents the first selected encrypted pixel value from being restored to its original value in decryption process.

In this paper, in order to overcome the above problems, especially in the security and speed, we proposed a new image encryption scheme. The contributions and novelties of the proposed scheme are as follows: **(1)** Our scheme can resist the separated attack and chosen plaintext attack, such as the attack methods in [9], [10], [14]. The reason is the permutation and diffusion operations are implemented simultaneously by using Sine-Sine chaotic map. In addition, the initial value of the current Sine-Sine chaotic map is related to the previous encrypted pixels (details can be seen in step 2 of Section III.B and III.C), which leads to the generation of dynamic keystreams related to the plaintext. **(2)** The proposed scheme has low time complexity and fast encryption speed. Since the pixel values are processed by row and column (row-level or column-level) during the whole encryption process, the proposed algorithm has better performance in speed than that of some existing simultaneous mechanism of scrambling and diffusion to implement fast image encryption algorithms such as [17] and [18] in which the pixel values are processed by pixel-level. The test results in IV show that our scheme is superior to other image encryption schemes (such as the scheme in [7], [11], [17], [18]) with regard to security performance, encryption effect and speed.

The rest of our paper is arranged as follows: In Section II, we introduce the applied chaotic maps. Section III presents the proposed scheme in detail. The simulation results and the security analysis of the proposed encryption scheme are discussed in Section IV. Finally, we make a comprehensive summary for the article in Section V.

II. PRELIMINARY WORK

In this part, two chaotic maps employed in the proposed encryption scheme are described in detail. Since classical one-dimensional chaotic maps such as Logistic map [4], Hénon map [20], Lorenz system [21] and Tent map [22] have several flaws such as small key spaces and limited chaotic ranges, we employ the 2D Hénon-Sine map proposed in [23] and the Sine-Sine map proposed in [5] for generating the random sequences in the proposed scheme.

A. 2D HÉNON-SINE MAP

2D Hénon -Sine map (2D-HSM) was proposed by Wu *et al.* [23], which can be described by Eq. (1):

$$\begin{cases} x_{n+1} = \left[1 - asin^2\left(x_n\right) + y_n\right] \text{mod} 1 \\ y_{n+1} = \left(bx_n\right) \text{mod} 1 \end{cases} \tag{1}$$

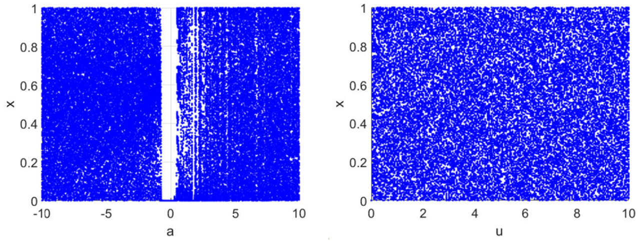
where the ranges of parameters a and b are both expanded to $(-\infty, +\infty)$, and the initial values of the 2D-HSM map $x_0, y_0 \in (0, 1)$. From the bifurcation diagram presented in Figure 1 (a), 2D-HSM has wider chaotic range. In addition, it has been proved in [23] that 2D-HSM has better ergodicity and randomness than Hénon map and Sine map. Therefore, 2D-HSM possesses complex trajectories and more unpredictable output results.

B. SINE-SINE MAP

Pak [5] proposed the Sine-Sine map based on Sine map, which can be described by Eq. (2):

$$\begin{aligned} z_{n+1} = u \times \sin\left(\pi \times z_n\right) \times 2^{14} \\ - floor\left(u \times \sin\left(\pi \times z_n\right) \times 2^{14}\right) \end{aligned} \tag{2}$$

where parameter $u \in (0, 10)$, and the initial value of the Sine-Sine map $z_0 \in (0, 1)$. From the bifurcation diagram shown



(a) (b)

FIGURE 1. (a) Bifurcation diagram of 2D-HSM. (b) Bifurcation diagram of Sine-Sine map.

in Figure 1 (b), Sine-Sine map has wide chaotic range and random outputs.

The features of the 2D-HSM and Sine-Sine map can be summarized as:

(1) The chaotic ranges of the two maps are much larger than that of the common one-dimension maps, such as Logistic map, Hénon map, Sine map and so on, which makes the proposed encryption method have large secret keys space.

(2) The Lyapunov exponents of the two maps are approximate to 2 can match that of common hyperchaotic maps such as [20]. The two maps have good chaotic performance, complex trajectories and well randomness.

(3) The two chaotic maps have simple structures and they are easy to be implemented by software and hardware. In addition, they have less execution time than that of hyperchaotic maps, which is suitable for fast encryption.

Therefore, we employ 2D-HSM and Sine-Sine map for image encryption.

III. ENCRYPTION ALGORITHM

In this section, our encryption process is described in detail. Ten parameters $(x_0, y_0, z_{01}, z_{02}, N_0, C_0, t_0, u, a, b)$ are the secret keys. The proposed encryption process includes three main parts: rewriting the plain image's pixel values by 2D-HSM, SPDO by row, and SPDO by column. The proposed architecture for image encryption is shown in Figure 2.

A. REWRITE PIXELS' VALUES OF THE PLAIN IMAGE P BY 2D-HSM

The rewriting steps are as follows.

Step 1: Iterate the 2D-HSM [23] by Eq.(1) (N_0+max(m, n)) times to get two chaotic sequences $(x_i, y_j : 1 \leq i \leq N_0 + \max(m, n))$. Note: $m \times n$ is the size of the plain image.

Step 2: The former N_0 elements are discarded to obtain two new random sequences (h_i, l_j : 1 $\leq i \leq$ n,1 $\leq j \leq$ m) according to Eq.(3):

$$\begin{cases} h_i = x(N_0 + i) \times 10^{14} \mathrm{mod} 256 \\ l_j = y(N_0 + j) \times 10^{14} \mathrm{mod} 256 \end{cases} \tag{3}$$

where the sequence h_i is used for row-rewriting with the length n and the sequence l_j is used for column-rewriting with the length m.

Step 3: Rewriting operation by Eq. (4):

$$\begin{cases} \boldsymbol{R} = (\boldsymbol{P} + h) \bmod 256 \\ \boldsymbol{Q} = (\boldsymbol{R} + l) \bmod 256 \end{cases} \tag{4}$$

where $\boldsymbol{R}$ represents the row-rewritten image and $\boldsymbol{Q}$ represents the column-rewritten image. In essence, each pixel' value of the plain image is added different numbers in two rounds during the rewriting operation, which makes the encryption results more random and unpredictable.

B. THE SPDO BY ROW

The diagram of SPDO by row is shown in Figure 3.

Step 1: Set $i = 1$.

Step 2: Iterate Sine-Sine map [5] by Eq.(2) $(N_0 + n)$ times and cut off the first N_0 elements to obtain a new random sequences with size of n. The initial value z_i of the Sine-Sine map is calculated according to Eq.(5)-Eq.(7).

$$z_i = \left(z_{01} + \frac{sum}{255 \times n}\right) \mathrm{mod} 1 \tag{5}$$

$$sum = \sum\nolimits_{j=1}^{n} C(T_i, j) \tag{6}$$

$$T_i = (m - i + 2) \mathrm{mod} (m + 1) \tag{7}$$

where z_{01}, C_0, N_0 are initial parameters, and ***sum*** is the sum of the previous cipher row-pixel values, which indicates that the initial value of the Sine-Sine map is influenced by the secret keys and the previous cipher pixels. Therefore, our scheme generates distinct keystreams for different plain images.

Step 3: The row index n_i of pixels to be processed is calculated by Eq.(8) and Eq.(9).

$$n_i = z\left(N_0 + t_i\right) \times 10^{14} \mathrm{mod} T_{i+1} + 1 \tag{8}$$

$$t_i = (t_0 + \mathrm{sum}) \bmod \mathrm{n} + 1 \tag{9}$$

where $t_i \in [1, n]$. When the chaotic system is re-iterated, a new n_i is obtained in Eq.(8). n_i is dynamically updated and distributed roughly uniformly from 1 to m. Namely, $n_1 \in [1, m], n_2 \in [1, m-1], \ldots, n_{m-1} \in [1, 2], n_m = 1$.

Step 4: Compute the sequence D_i for diffusion according to Eq.(10):

$$D_i = z\left(N_0 + j\right) \times 10^{14} \mathrm{mod}\ 256 \tag{10}$$

where $j \in (1, n)$. D_i is distinct for different plain images.

Step 5: Encrypt the n_i^{th} row pixels of the image according to Eq.(11):

$$C_{n_i} = \left(C_{n_i} + D_i\right) \mathrm{mod} 256 \oplus C(T_i, :) \tag{11}$$

where $C(T_i, :)$ are the previous encrypted and swapped row-pixel values.

Step 6: Swap the encrypted pixels C_{n_i} and pixels $C_{T_{i+1}}$ for permutation according to Eq.(12):

$$temp = C_{n_i}, C_{n_i} = C_{T_{i+1}}, C_{T_{i+1}} = temp \tag{12}$$

Step 7: Set $i = i + 1$ and repeat the above steps (in Section III.B) until all row-pixel values of the image are processed.

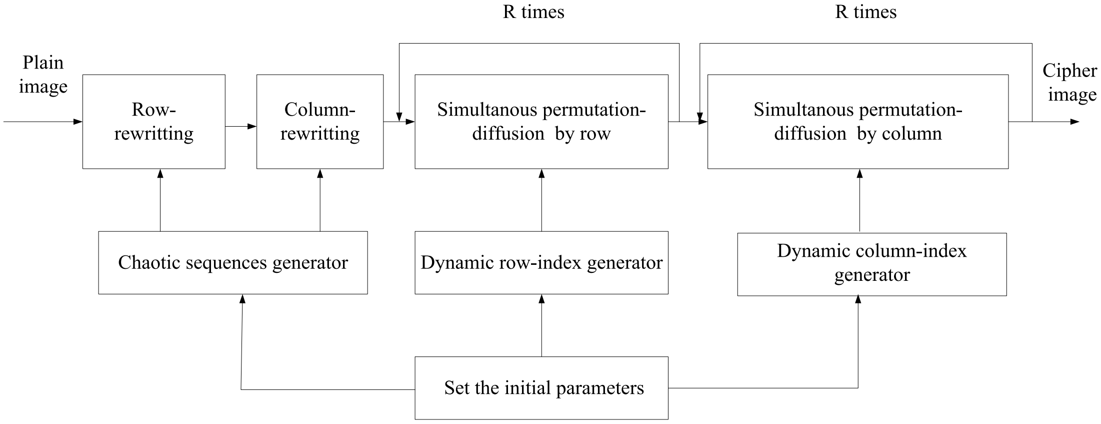

R times
R times
Plain image
Row-rewritting
Column-rewritting
Simultanous permutation-diffusion by row
Simultanous permutation-diffusion by column
Cipher image
Chaotic sequences generator
Dynamic row-index generator
Dynamic column-index generator
Set the initial parameters

FIGURE 2. **The flowchart of the proposed encryption scheme.**

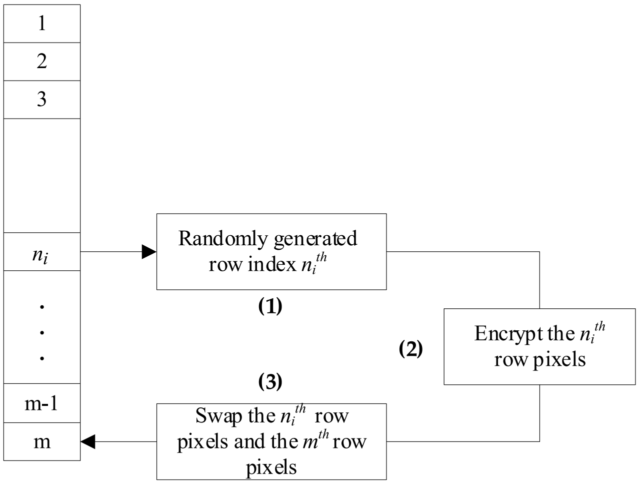

1
2
3
n_i
.
.
.
m-1
m
Randomly generated row index n_i^{th}
(1)
(2)
(3)
Encrypt the n_i^{th} row pixels
Swap the n_i^{th} row pixels and the m^{th} row pixels

FIGURE 3. **The diagram of the proposed simultaneous permutation-diffusion by row.**

C. THE SPDO BY COLUMN

The diagram of SPDO by column is shown in Figure 4.

Step 1: Set $j = 1$.

Step 2: Iterate Sine-Sine map [5] in Eq.(2) $(N_0 + n)$ times and cut off the first N_0 elements to obtain a new random sequences with size of m. The initial value z_j of the Sine-Sine map is calculated according to Eq.(13)-Eq.(15):

$$z_j = \left(z_{02} + \frac{sum}{255 \times m}\right) \text{mod} 1 \tag{13}$$

$$sum = \sum\nolimits_{i=1}^{m} C(i, T_j) \tag{14}$$

$$T_j = (\mathrm{n} - \mathrm{j} + 2)\text{mod}(\mathrm{n} + 1) \tag{15}$$

where z_{02} is initial parameter, and ***sum*** is the sum of the previous cipher column-pixel values. Eq. (13)-Eq. (15) state that the initial value of the Sine-Sine map depends on the secret key and the previous cipher pixels, which can generate distinct keystreams for different plain images.

Step 3: The column index n_j of pixels to be processed is calculated according to Eq.(16) and Eq.(17).

$$n_j = z\left(N_0 + t_j\right) \times 10^{14} \text{mod} T_{j+1} + 1 \tag{16}$$

$$t_j = (t_0 + \text{sum}) \text{ mod m} + 1 \tag{17}$$

where $t_j \in [1, m]$. When the chaotic system is re-iterated, a new n_j is obtained in Eq.(16). n_j is dynamically updated and distributed roughly uniformly from 1 to m. Namely, $n_1 \in [1, m], n_2 \in [1, m-1], \ldots, n_{m-1} \in [1, 2], n_m = 1$.

Step 4 is the same as *Step 4* in Section III.B above.

Step 5: Encrypt the n_j^{th} column pixels of the image according to Eq.(18):

$$C_{n_j} = \left(C_{n_j} + D_j\right) \text{mod} 256 \oplus C(:, T_j) \tag{18}$$

where $C(:,T_j)$ are the previous encrypted and swapped column-pixel values.

Step 6: Swap the encrypted pixels C_{n_j} and pixels $C_{T_{j+1}}$ for permutation according to Eq.(19):

$$temp = C_{n_j}, \quad C_{n_j} = C_{T_{j+1}}, \; C_{T_{j+1}} = temp \tag{19}$$

Step 7: Set $j = j + 1$ and repeat the above steps (in Section III.C) until all column-pixel values of the image are processed. Finally, the cipher image ***C*** can be obtained.

Similarly, the steps of decryption procedure are the inverse steps of the encryption procedure. The plain image can be completely restored by decryption operation with the same secret key.

The following characteristics of the proposed encryption scheme should be noticed.

(i) The information of the plain image can be completely hidden after rewriting operation, and then the pixel values of the n_1^{th} row (Section III.B) are covered before SPDO which is only related to the secret key, so that the attacker is failed to crack the proposed encryption scheme with all-zeroes image or other special images such as [9], [10].

(ii) Our scheme can resist chosen plaintext attack. In Section III.B and Section III.C, when $i = 1$ or $j = 1$, the initial value of the Sine-Sine map is only related to the

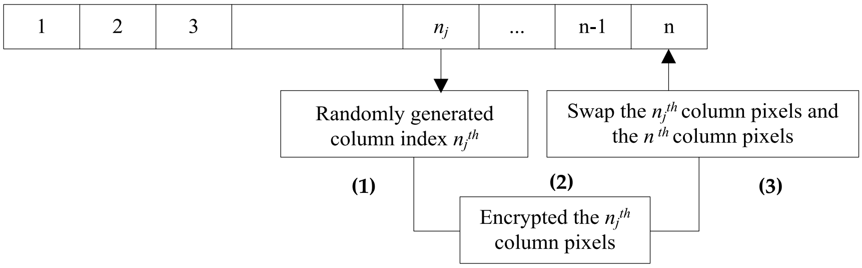

1
2
3
n_j
...
n-1
n
Randomly generated column index n_j^{th}
Swap the n_j^{th} column pixels and the n^{th} column pixels
(1)
(2)
(3)
Encrypted the n_j^{th} column pixels

FIGURE 4. The diagram of the proposed simultaneous permutation and diffusion by column.

secret keys. When $i \in [2, \mathrm{m}]$ or $j \in [2, \mathrm{n}]$, the initial value of the Sine-Sine map is set to be related to the initial key and the ciphertext information obtained from the previous encryption. Therefore, distinct row or column indexes of image pixels and the sequences for diffusion are generated for different plain images (step 3 and step 4 in Section III.B and III.C), which greatly improves the safety performance of the proposed scheme.

(iii) The proposed encryption process is reversible.

Because the new generated index n_i (step 3 in Section III.B) or n_j (step 3 in Section III.C) is smaller than the row index T_{i+1} (step 2 in Section III.B) or column index T_{j+1} (step 2 in Section III.C) of the swapped pixels, so the pixels' value will not change after permutation. Importantly, the sequences ***sum***(step 2 in Section III.B and III.C), which determine the initial value of the Sine-Sine map, will be equal in the encryption and decryption process. Therefore, the corresponding plain image can be recovered successfully by the decryption process.

(iv) The plain image is encrypted by row and column (row-level and column-level) in the proposed scheme, which is faster than that in bit-level [7], [24] and pixel-level [11], [25].

IV. SIMULATION RESULTS AND SECURITY ANALYSIS

In the section, ten gray-scale plain images (Lena, Mandril, Cameraman, Living-room, Pirate, Woman, Truck, Peppers, Resolution, Barbana) are tested. The proposed scheme is related to plaintext and based on SPDO, therefore, the following experiments compare the proposed scheme with four related schemes presented in Luo *et al.* [7], Ye *et al.* [11], Diab [17], Huang *et al.* [18].

The test images presented in the first column of Figure 5 are encrypted by our scheme and the corresponding cipher images are shown in the second column of Figure 5, which perfectly hide all the information of the plain images and present noise-like appearances. The decrypted images are displayed in the third column of Figure 5, which are exactly the same as the corresponding plain images. These results demonstrate the effectiveness and practicability of our scheme.

A. KEY SPACE ANALYSIS

The secret key of the proposed scheme consists of ten parameters $(x_0, y_0, z_{01}, z_{02}, N_0, C_0, t_0, u, a, b)$ shown in Table 1, where $x_0, y_0, z_{01}, z_{02} \in (0, 1]$, $u \in (0, 10]$, $C_0, t_0 \in [0, 255]$, $a, b \in (-\infty, +\infty)$, and $N_0 = 10^3$. Then the key space of the proposed scheme is $10^{98} \times 10^3 \times 256 \times 256 \approx 2^{351}$ with the accuracy of 10^{-14}. Therefore, our scheme can resist the brute-force attack.

B. STATISTICAL ANALYSIS

1) HISTOGRAM ANALYSIS

The results of the histogram test are shown in Figure 6. The second column images of Figure 6 are the histograms of the plain images, and the last column images of Figure 6 are the histograms of the corresponding cipher images which are well-distributed. Therefore, our scheme is enough to resist statistical attacks.

2) CHI-SQUARE ANALYSIS

To further illustrate the distribution of ciphertext pixel values, we calculate their chi-square values according to Eq. (20):

$$\chi^2_{test} = \sum\nolimits_{i=1}^{k} \frac{(o_i - e_i)^2}{e_i} \tag{20}$$

where $\boldsymbol{K} = \mathbf{256}$ for gray-scale image, $\boldsymbol{o_i}$ and $\boldsymbol{e_i}$ represent the occurrence frequency of each gray value obtained from the experiment and the expected occurrence frequency of each gray value respectively. The results shown in Table 2 indicate that the chi-square values of the ciphertext image obtained by the proposed scheme are all less than the theoretical value 293.24783. Therefore, the ciphertext has a uniform distribution, and our scheme passes the chi-square test successfully.

3) CORRELATION ANALYSIS OF TWO ADJACENT PIXELS

We randomly select 10,000 pairs of adjacent pixels from the plain images and cipher images at horizontal, vertical and diagonal directions. The correlation coefficient is calculated according to Eq. (21):

$$r_{xy} = \frac{cov\,(x, y)}{\sqrt{D\,(x)}\sqrt{D\,(y)}} \tag{21}$$

where $cov(x, y) = \frac{1}{\mathrm{N}} \sum_{i=1}^{\mathrm{N}} (x_i - E\,(x)\,(y_i - E\,(y))), D\,(x) = \frac{1}{N} \sum_{i=1}^{\mathrm{N}} (x_i - E\,(x))^2$ and $E\,(x) = \frac{1}{\mathrm{N}} \sum_{i=1}^{\mathrm{N}} x_i$.

The correlation distributions from Lena gray-scale image and the corresponding cipher image are presented in Figure 7. Evidently, there are no detectable correlation between adjacent pixels for the cipher image. In addition, the correlation coefficients of ten encrypted image using different encryption

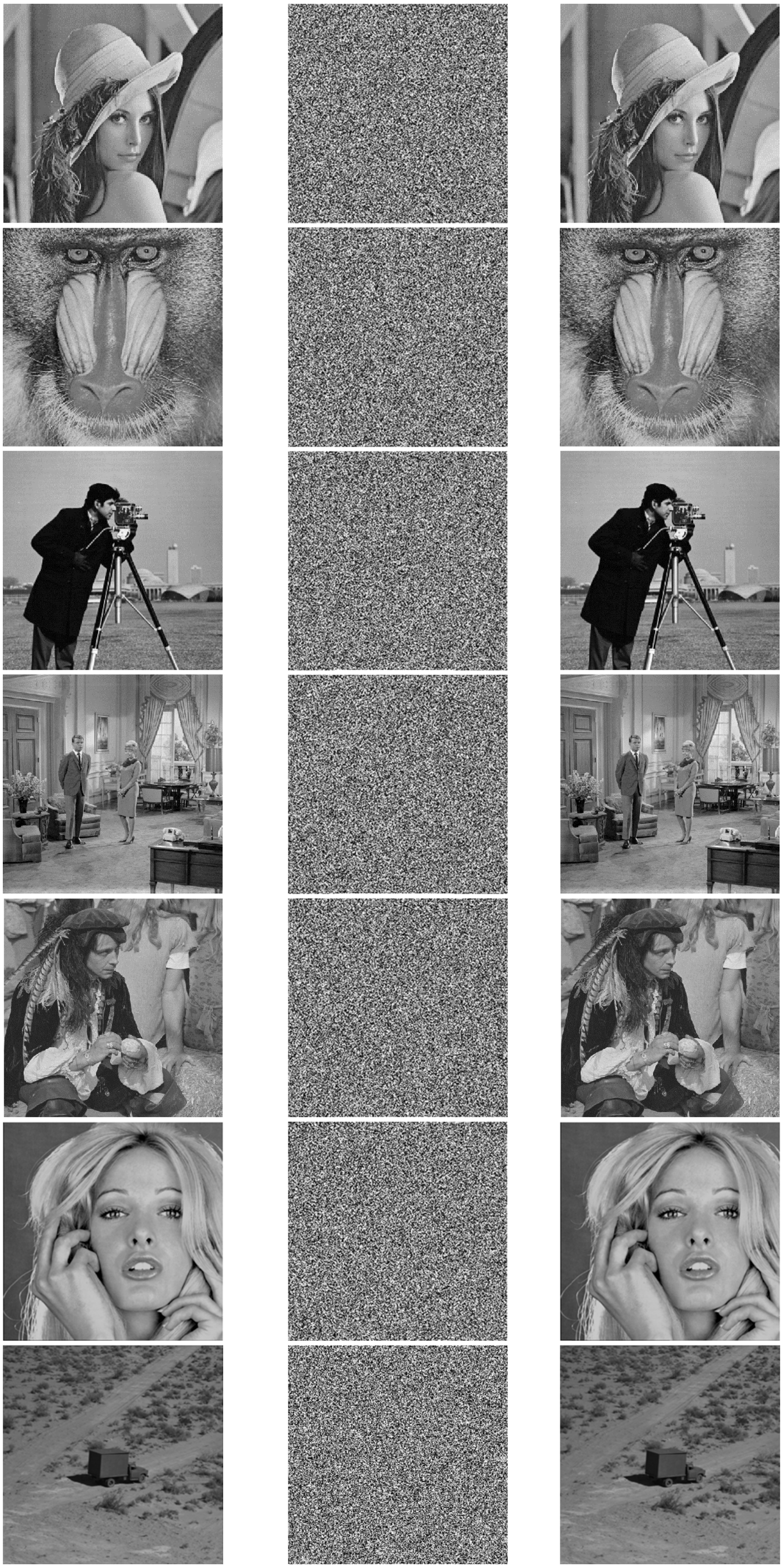


FIGURE 5. **The simulation results of the proposed cryptosystem. The first column images are plain images, the second column images are cipher images, and the last column images are decrypted images.**

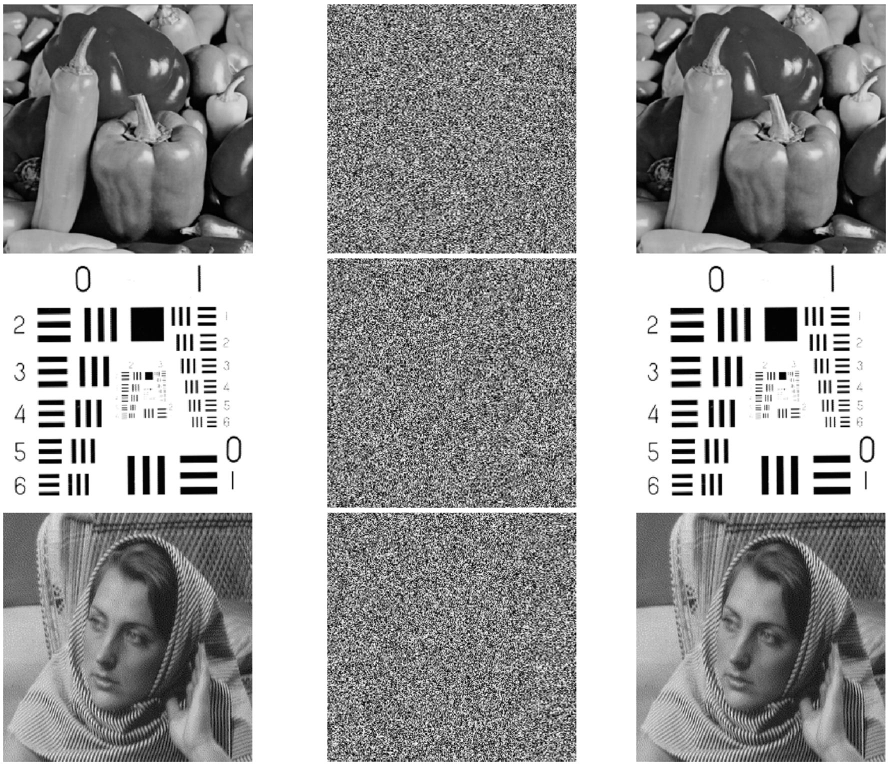


FIGURE 5. **(continued.) The simulation results of the proposed cryptosystem. The first column images are plain images, the second column images are cipher images, and the last column images are decrypted images.**

TABLE 1. **The description of the secret keys.**

The secret keys	The description
$x_{0,} y_0, a, b$	The initial values and parameters of 2D-HSM
z_{01}, z_{02}, u	The initial values and parameters of Sine-Sine map
C_0, t_0, N_0	seeds

TABLE 2. **Chi-square test.**

Images	$\chi^2_{Li's}$	$\chi^2_{Proposed}$	Result
Lena	293.24783	253.4844	Success
Mandril	293.24783	244.5859	Success
Cameraman	293.24783	251.8281	Success
Living-room	293.24783	261.0938	Success
Pirate	293.24783	230.0011	Success
Woman	293.24783	222.7266	Success
Truck	293.24783	224.9844	Success
Peppers	293.24783	265.2813	Success
Barbana	293.24783	282.5625	Success

schemes are listed in Table 3. These results show that our scheme can resist statistical attack.

C. KEY SENSITIVITY ANALYSIS

In this section, we encrypt plain image ‘Lena’ with size $\mathbf{256} \times \mathbf{256}$ by inputting the secret key ($\boldsymbol{x_0}, \boldsymbol{y_0}, \boldsymbol{z_{01}}, \boldsymbol{z_{02}}, \boldsymbol{N_0}, \boldsymbol{C_0}, \boldsymbol{t_0}, \boldsymbol{u}, \boldsymbol{a}, \boldsymbol{b}$), and decrypt the cipher image with the same secret key. In addition, we decrypt the cipher image with the modified secret keys respectively shown in Table 4. The corresponding recovered images are displayed in Figure 8. From the results, we can see the plain image cannot be recovered in the decryption process with slightly different secret keys. Therefore, the proposed scheme has strong key sensitivity.

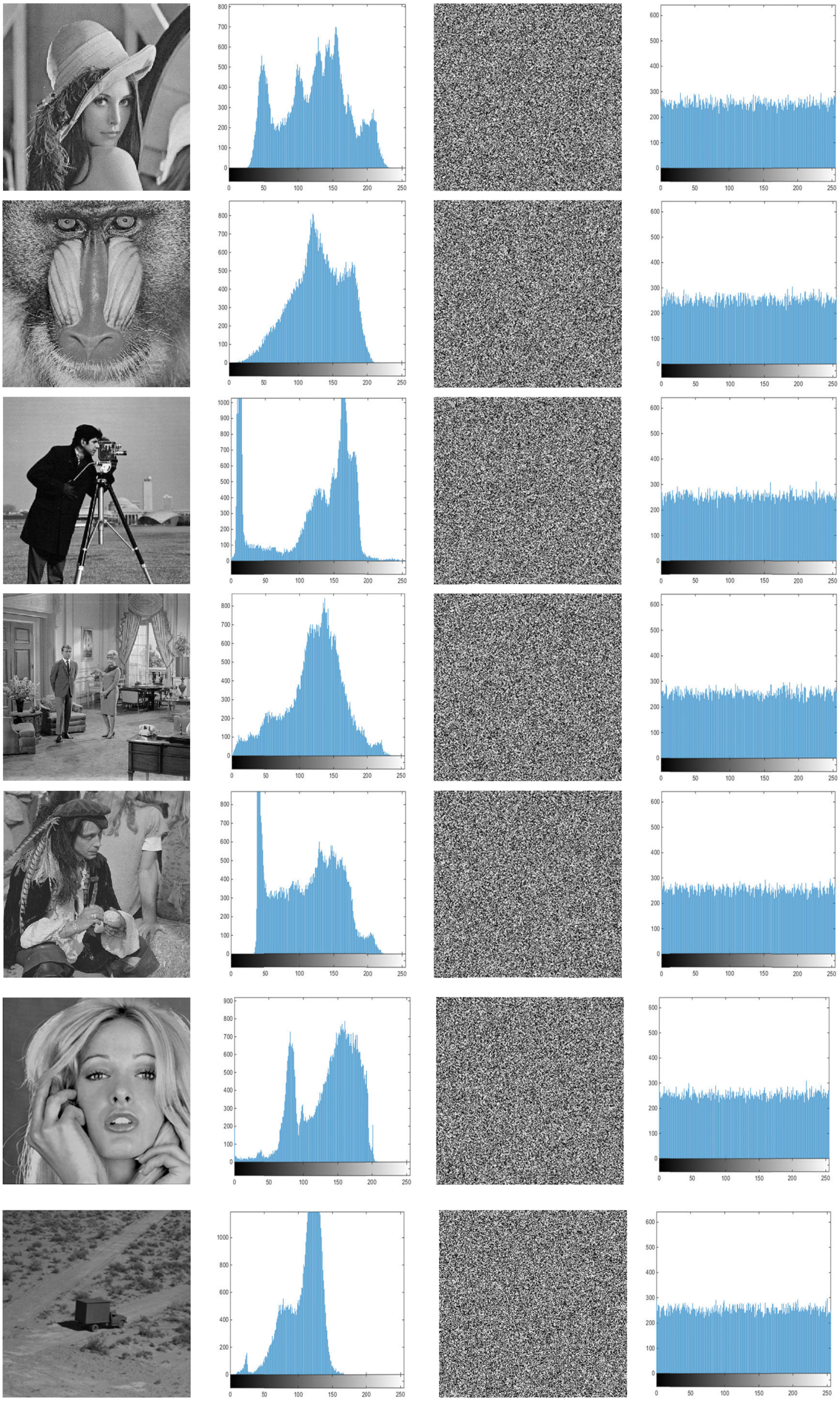


FIGURE 6. The results of the histogram test. The first column images are plain images. The second column images are histograms of corresponding plain images. The third column images are corresponding cipher images and the last column images are histograms of corresponding cipher images.

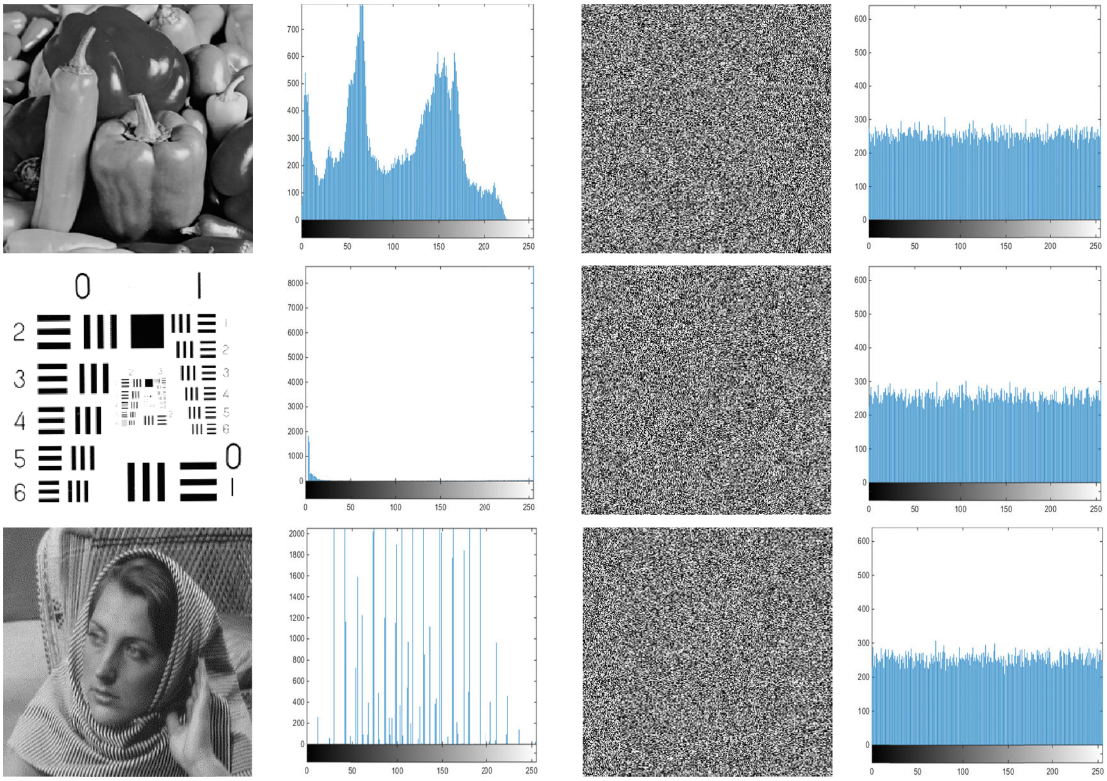
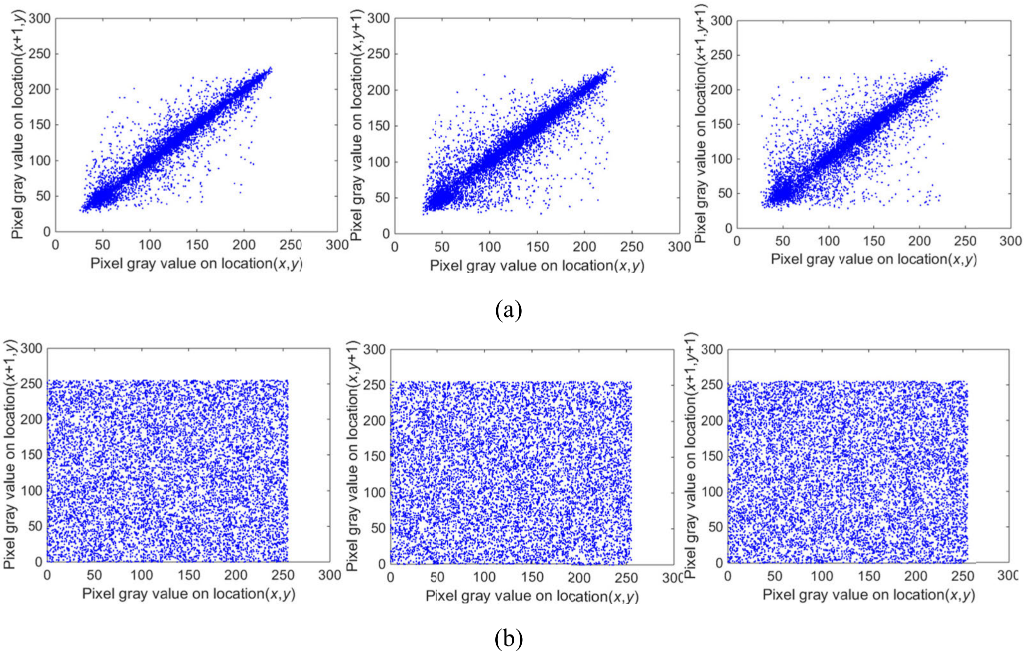


FIGURE 6. (continued.) The results of the histogram test. The first column images are plain images. The second column images are histograms of corresponding plain images. The third column images are corresponding cipher images and the last column images are histograms of corresponding cipher images.



(a)

(b)

FIGURE 7. Correlation of two horizontally, vertically and diagonally adjacent pixels of (a) Lena gray-image (256 × 256) and (b) Lena cipher image.

D. INFORMATION ENTROPY ANALYSIS

Information entropy is calculated according to Eq. (22):

$$W(s) = \sum_{i=0}^{2^k-1} f(s_i) log_2 \frac{1}{f(s_i)} \tag{22}$$

where k is the image bit depth, e.g., $k = 8$ for an 8-bit gray-scale image, and $f(s_i)$ is the probability of s_i.

In our scheme, the use of two chaotic maps increases the randomness of ciphertext images, so the information entropy is high. According to the Table 5, the information entropy of

TABLE 3. **Adjacent pixel correlation.**

Image	Direction	Plain image	Ciphered image			
			Proposed	Ref. [11]	Ref. [17]	Ref. [18]
Lena	H	0.9591	0.0106	0.0210	-0.0070	-0.0070
	V	0.9350	-0.0012	0.0038	-0.0054	0.0151
	D	0.9008	0.0009	-0.0042	0.0055	0.0003
Mandril	H	0.9102	0.0230	0.0042	0.0112	0.0064
	V	0.9337	0.0054	-0.0152	0.0006	-0.0138
	D	0.8638	-0.0168	-0.0051	-0.0019	0.0087
Cameraman	H	0.9903	0.0113	0.0157	-0.0003	0.0033
	V	0.9826	0.0169	-0.0139	0.0037	0.0027
	D	0.9724	0.0034	0.0064	-0.0048	0.0122
Living-room	H	0.9529	0.0100	-0.0043	0.0007	0.0350
	V	0.9433	0.0114	0.0157	-0.0079	0.0359
	D	0.9108	-0.0025	-0.0038	0.0003	0.0047
Pirate	H	0.9686	-0.0251	0.0144	0.0048	0.0315
	V	0.9615	-0.0108	0.0157	0.0033	0.0114
	D	0.9615	-0.0326	0.0054	0.0156	0.0174
Woman	H	0.9585	0.0172	0.0056	-0.0085	0.0245
	V	0.9365	0.0017	0.0080	0.0087	0.0070
	D	0.9182	0.0013	0.0036	0.0106	0.0118
Truck	H	0.9239	-0.0060	0.0083	-0.0046	0.1004
	V	0.9616	-0.0089	0.0043	-0.0088	0.0651
	D	0.9058	-0.0146	0.0049	0.0030	0.0452
Peppers	H	0.9821	-0.0024	0.0070	-0.0006	-0.0070
	V	0.9795	0.0142	0.0137	0.0114	0.0151
	D	0.9652	-0.0050	0.0039	0.0179	0.0003
Resolution	H	0.8745	0.0024	-0.0085	0.0040	0.0064
	V	0.8690	-0.0153	0.0064	-0.0079	-0.0138
	D	0.7600	0.0190	0.0004	0.0122	0.0087
Barbana	H	0.9055	0.0040	0.0058	0.0076	0.0033
	V	0.7566	0.0024	0.0004	0.0105	0.0027
	D	0.7098	0.0006	0.0027	0.0050	0.0122

all cipher images is close to the theoretical value 8. Therefore, the proposed scheme provides high randomness.

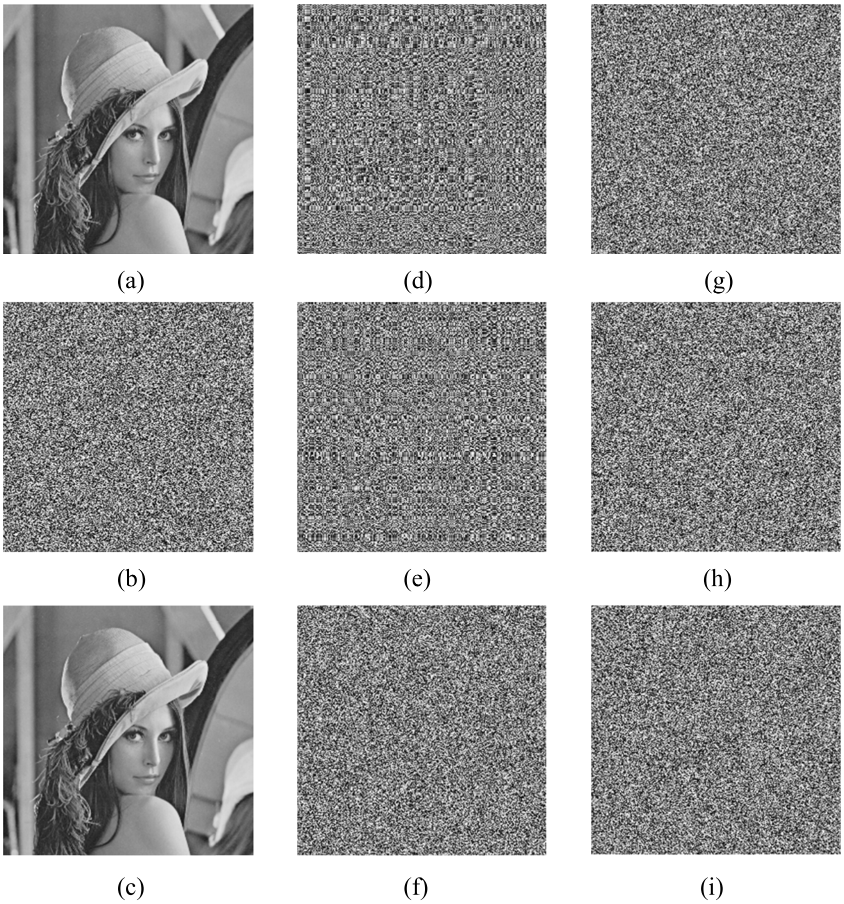
In addition, we calculate the local information entropy according to Eq. (23):

$$\overline{W_{k,T_b}}\left(C\right)=\sum\nolimits_{i=1}^{k}\frac{W\left(C_i\right)}{k} \tag{23}$$

where $\boldsymbol{W}\left(\boldsymbol{C_i}\right)$ is the information entropy for each block of randomly selected encrypted image and can be calculated by Eq.(22). As stated in [26], parameters k and $\boldsymbol{T_b}$ in this test are set to 30 and 1936. The local information entropy values for gray-scale images with size $\mathbf{512}\times\mathbf{512}$ and a significance level $\boldsymbol{\alpha}=\mathbf{0.05}$ are shown in Table 6. The results show that our scheme has better ability to resist the entropy attack [12].

E. DIFFERENTIAL ATTACK

To measure the ability of our scheme to resist differential attack, we calculate NPCR and UACI according to



(a) (d) (g)

(b) (e) (h)

(c) (f) (i)

FIGURE 8. The results of key sensitivity for the proposed cryptosystem. (a) Lena plain image. (b) Lena cipher image. (c) The recovered image with the same key. (d) The recovered image with the modified key: $x_0 + 10^{-14}$. (e) The recovered image with the modified key: $a + 10^{-14}$. (f) The recovered image with the modified key: $z_{01} + 10^{-14}$. (g) The recovered image with the modified key: $u + 10^{-14}$. (h) The recovered image with the modified key: $t_0 + 1$. (i) The recovered image with the modified key: $N_0 + 1$.

TABLE 4. Secret keys and the changed values.

Item	The changed values
x_0	$x_0 + 10^{-14}$
a	$a + 10^{-14}$
z_{01}	$z_{01} + 10^{-14}$
u	$u + 10^{-14}$
t_0	$t_0 + 1$
N_0	$N_0 + 1$

Eq. (24)-Eq. (26):

$$\mathrm{NPCR} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} D(i,j)}{m \times n} \times 100\% \tag{24}$$

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j) \\ 1, & C_1(i,j) \neq C_2(i,j) \end{cases} \tag{25}$$

$$\mathrm{UACI} = \frac{1}{m \times n}\left(\sum_{i=1}^{m}\sum_{j=1}^{n} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right) \times 100\% \tag{26}$$

where the image $\boldsymbol{C_1}$ is the cipher image of the plain image $\boldsymbol{P_1}$, and the image $\boldsymbol{C_2}$ is the cipher image of the plain image $\boldsymbol{P_2}$ differing in only one-bit from $\boldsymbol{P_1}$. We can see from the data in Table 7 that the NPCR and UACI values for the proposed scheme are very close to the ideal values 99.6094% and 33.4635% [25], [28] respectively, which shows that the proposed scheme is extremely sensitive to slight differences of the plain image and then can resist differential attack.

F. SPEED AND TIME COMPLEXITY ANALYSIS

In our scheme, the image pixel values are encrypted by row and column, which is faster than those are encrypted by bit-level [7], [24] or pixel-level [11], [25]. Accordingly, the time complexity in the rewriting process of our scheme is $\boldsymbol{\theta}(\mathbf{m}+\mathbf{n})$, and the time complexity in the SPDO is also $\boldsymbol{\theta}(\mathbf{m}+\mathbf{n})$. So the complexity of the proposed scheme is $\boldsymbol{\theta}(\mathbf{2}(\mathbf{m}+\mathbf{n}))$. For other related encryption schemes such as [7], [11], [17],

TABLE 5. Global information entropy test.

Image	Plain image	Ciphered image				
		Proposed	Ref. [7]	Ref. [11]	Ref. [17]	Ref. [18]
Lena	7.4429	7.9972	7.9969	7.9973	7.9967	7.8963
Mandril	7.2925	7.9967	7.9966	7.9975	7.9972	7.9007
Cameraman	7.0480	7.9972	7.9970	7.9972	7.9973	7.8979
Living-room	7.2952	7.9971	7.9973	7.9975	7.9975	7.8973
Pirate	7.2367	7.9974	7.9974	7.9970	7.9973	7.8973
Woman	6.9542	7.9976	7.9973	7.9968	7.9968	7.8977
Truck	6.0274	7.9975	7.9969	7.9970	7.9969	7.8944
Peppers	7.5715	7.9971	7.9972	7.9972	7.9976	7.8992
Resolution	1.5483	7.9968	7.9968	7.9969	7.9975	7.6269
Barbana	5.0030	7.9969	7.9970	7.9973	7.9973	7.9003

TABLE 6. Local Shannon entropy test for cipher image ($k = 30$, $Tb = 1936$, $\alpha = 0.05$).

Image	Local Shannon entropy of cipher image	Pass or not
Lena	7.9002	Pass
Mandril	7.9031	Pass
Cameraman	7.9046	Pass
Living-room	7.9005	Pass
Pirate	7.9031	Pass
Woman	7.9012	Pass
Truck	7.9040	Pass
Peppers	7.9031	Pass
Resolution	7.9010	Pass
Barbana	7.9012	Pass

[18], the time complexity of them is more than $\boldsymbol{\theta}(\mathbf{2}\,(\mathbf{m}+\mathbf{n}))$. And the complexity of our scheme is the same as that of the scheme in [16]. These are shown in Table 8 (where $\boldsymbol{m} \times \boldsymbol{n}$ is the size of the plain image). The running time for different plain images and different schemes are list in Table 9. This shows that our scheme is faster than that of others [7], [11], [17], [18]. In addition, the average time of decryption process in our scheme is 0.238547 seconds, which is faster than the scheme [29] with 3.525617 seconds. The experimental environment is MATLAB R2014b with Intel Core i5-4590 CPU @ 3.30GHz and 4.00 G RAM on window 7 OS.

G. RESISTANCE TO CHOSEN/KNOWN PLAINTEXT ATTACK

The proposed encryption scheme is based on SPDO. Accordingly, the attacker cannot separate the two processes and crack the permutation and diffusion rules respectively. In addition, there is a rewriting operation before SPDO, which leads the attacker not to find proper special images in the attack plan. Moreover, our algorithm will generate a distinct key-stream for different plain image in SPDO, so even if the attacker selected some special images to obtain the permutation and diffusion rules, our scheme cannot be broken since these rules are different for different plain images. In conclusion, the proposed encryption scheme can resist chosen and known plaintext attack.

V. CONCLUSION

In this paper, we propose a fast image encryption scheme based on SPDO. First of all, we permute and diffuse the pixel values simultaneously by row and column through Sine-Sine map, which can resist the separated attack. What's more, in SPDO, the initial value of the Sine-Sine map is related to the image information and the secret key, which generates distinct keystreams and index sequences for different plain images. The experimental results and security analysis demonstrate that the proposed encryption scheme has strong robustness against statistical attack, differential attack, chosen and known plaintext attack and other comprehensive attacks. Besides, the running speed of the proposed image encryption scheme (row-level and column-level) is faster than the existing encryption schemes based on SPDO [17], [18] which is conducive to the batch transmission and real-time transmission of digital images. Therefore, our scheme can be well applied in digital image encryption. In future work, we focus on improving the proposed scheme to resist on noise and occlusion attack (in this paper we suppose the images are transmitted losslessly). When the cipher image is contaminated by noises or subtracted from a part of data in the process of transmission, the effective information (the sequences (*sum*) which determine the diffusion matrices and the row-index or column-index in SPDO) may be changed. In this case, we cannot perform inverse permutation and diffusion process correctly. In future work, we will focus on the design of image encryption algorithm which can resist noise

TABLE 7. NPCR and UACI results.

Image	NPCR (%)				UACI (%)			
	Proposed	Ref. [11]	Ref. [17]	Ref. [18]	Proposed	Ref. [11]	Ref. [17]	Ref. [18]
Lena	99.6216	99.6246	99.6262	99.6033	33.4994	33.4877	33.4010	33.3631
Mandril	99.6368	99.6246	99.6094	99.5697	33.4702	33.5104	33.4461	33.0921
Cameraman	99.6353	99.5926	99.6185	99.6185	33.4810	33.4269	33.4231	33.4112
Living-room	99.6414	99.6063	99.6475	99.6445	33.4871	33.5146	33.4581	33.5189
Pirate	99.5773	99.6643	99.6170	99.5926	33.5008	33.4994	33.4387	33.4509
Woman	99.6246	99.6155	99.6140	99.6170	33.5307	33.4664	33.4808	33.4536
Truck	99.6246	99.5926	99.6246	99.5514	33.4672	33.4964	33.5324	33.5881
Peppers	99.5865	99.6307	99.5834	99.6490	33.4815	33.5047	33.4827	33.3091
Resolution	99.6307	99.6246	99.6445	99.6338	33.4751	33.4253	33.4448	32.9088
Barbana	99.6078	99.6170	99.6231	99.6078	33.4894	33.4771	33.4643	33.6673

TABLE 8. Time complexity.

Algorithm	Proposed	Ref. [7]	Ref. [11]	Ref. [17]	Ref. [18]	Ref. [16]
Time complexity	2(m+n)	3mn+m+n	mn+2m+n	3mn	4mn	2(m+n)

TABLE 9. Execution time with the same operating environment (unit: s).

Image	Proposed	Ref. [7]	Ref. [11]	Ref. [17]	Ref. [18]
Lena	0.276775	4.230902	0.473963	1.682497	6.452408
Mandril	0.279391	4.341490	0.490740	1.748854	6.468644
Cameraman	0.277338	4.330022	0.473870	1.784329	6.329378
Living-room	0.281813	4.329517	0.624850	1.734043	6.365339
Pirate	0.283655	4.588864	0.706076	1.737501	6.434008
Woman	0.290106	4.321750	0.510382	1.688897	6.281263
Truck	0.297566	4.466211	0.513892	1.715132	6.367833
Peppers	0.351624	4.482100	0.560079	1.747320	6.060382
Resolution	0.285191	4.260617	0.500189	1.705734	6.200881
Barbana	0.341586	4.459589	0.552802	1.734761	6.273276

and cropping attacks. One way is we can set the sequences (*sum*) as secret keys, but how to manage the huge amounts of secret keys and synchronize these secret keys to different plaintext images are still under research.

REFERENCES

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

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

[3] S. Ma, Y. Zhang, Z. Yang, J. Hu, and X. Lei, "A new plaintext-related image encryption scheme based on chaotic sequence," *IEEE Access*, vol. 7, pp. 30344–30360, 2019.

[4] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based chaos," *Signal Process.*, vol. 92, no. 6, pp. 1101–1108, 2012.

[5] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Process.*, vol. 138, pp. 129–137, Sep. 2017.

[6] A. S. Saljoughi and H. Mirvaziri, "A new method for image encryption by 3D chaotic map," *Pattern Anal Appl.*, vol. 22, no. 1, pp. 243–257, Feb. 2019.

[7] Y. Luo, R. Zhou, J. Liu, Y. Cao, and X. Ding, "A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map," *Nonlinear Dyn.*, vol. 93, no. 3, pp. 1165–1181, Aug. 2018.

[8] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation Chaos*, vol. 08, no. 06, pp. 1259–1284, Jun. 1998.

[9] G. Tu, X. Liao, and T. Xiang, "Cryptanalysis of a color image encryption algorithm based on chaos," *Optik*, vol. 124, no. 22, pp. 5411–5415, Nov. 2013.

[10] H. Wang, D. Xiao, X. Chen, and H. Huang, "Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map," *Signal Process.*, vol. 144, pp. 444–452, Mar. 2018.

[11] G. Ye, C. Pan, X. Huang, and Q. Mei, "An efficient pixel-level chaotic image encryption algorithm," *Nonlinear Dyn.*, vol. 94, no. 1, pp. 745–756, Oct. 2018.

[12] Z. Li, C. Peng, L. Li, and X. Zhu, "A novel plaintext-related image encryption scheme using hyper-chaotic system," *Nonlinear Dyn.*, vol. 94, no. 2, pp. 1319–1333, Oct. 2018.

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

[14] L. Liu, Z. Zhang, and R. Chen, "Cryptanalysis and improvement in a plaintext-related image encryption scheme based on hyper chaos," *IEEE Access*, vol. 7, pp. 126450–126463, 2019.

[15] H. Fan, M. Li, D. Liu, and K. An, "Cryptanalysis of a plaintext-related chaotic RGB image encryption scheme using total plain image characteristics," *Multimed Tools Appl.*, vol. 77, no. 15, pp. 20103–20127, Aug. 2018.

[16] W. Liu, K. Sun, and C. Zhu, "A fast image encryption algorithm based on chaotic map," *Opt. Lasers Eng.*, vol. 84, pp. 26–36, Sep. 2016.

[17] H. Diab, "An efficient chaotic image cryptosystem based on simultaneous permutation and diffusion operations," *IEEE Access*, vol. 6, pp. 42227–42244, 2018.

[18] L. Huang, S. Cai, X. Xiong, and M. Xiao, "On symmetric color image encryption system with permutation-diffusion simultaneous operation," *Opt. Lasers Eng.*, vol. 115, pp. 7–20, Apr. 2019.

[19] H. Hu, Y. Deng, and L. Liu, "Counteracting the dynamical degradation of digital chaos via hybrid control," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 6, pp. 1970–1984, Jun. 2014.

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

[21] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dyn.*, vol. 62, no. 3, pp. 615–621, Nov. 2010.

[22] B. Mondal, S. Singh, and P. Kumar, "A secure image encryption scheme based on cellular automata and chaotic skew tent map," *J. Inf. Secur. Appl.*, vol. 45, pp. 117–130, Apr. 2019.

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

[24] C. Cao, K. Sun, and W. Liu, "A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map," *Signal Process.*, vol. 143, pp. 122–133, Feb. 2018.

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

[26] J. Chen, Z. Zhu, L. Zhang, Y. Zhang, and B. Yang, "Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption," *Signal Process.*, vol. 142, pp. 340–353, 2018.

[27] S. Hanis and R. Amutha, "A fast double-keyed authenticated image encryption scheme using an improved chaotic map and a butterfly-like structure," *Nonlinear Dyn.*, vol. 95, no. 1, pp. 421–432, Jan. 2019.

[28] M. Ghebleh, A. Kanso, and D. Stevanović, "A novel image encryption algorithm based on piecewise linear chaotic maps and least squares approximation," *Multimed Tools Appl.*, vol. 77, no. 6, pp. 7305–7326, Mar. 2018.

[29] M. Y. Valandar, M. J. Barani, and P. Ayubi, "A fast color image encryption technique based on three dimensional chaotic map," *Optik*, vol. 193, Sep. 2019, Art. no. 162921.

[30] Y. Luo, R. Zhou, J. Liu, S. Qiu, and Y. Cao, "An efficient and self-adapting colour-image encryption algorithm based on chaos and interactions among multiple layers," *Multimed Tools Appl.*, vol. 77, no. 20, pp. 26191–26217, Oct. 2018.

[31] X. Wu, B. Zhu, Y. Hu, and Y. Ran, "A novel color image encryption scheme using rectangular transform-enhance chaotic tent maps," *IEEE Access*, vol. 5, pp. 6429–6436, 2017.

[32] L. Liu, L. Zhang, D. Jiang, Y. Guan, and Z. Zhang, "A simultaneous scrambling and diffusion color image encryption algorithm based on Hopfield chaotic neural network," *IEEE Access*, vol. 7, pp. 185796–185810, 2019.

[33] L. Liu, Y. Wang, L. Hou, and X. Feng, "An easy encoding and low bit-error-rate chaos communication system based on reverse-time chaotic oscillator," *IET Signal Process.*, vol. 11, pp. 869–876, 2017.

[34] M. Wang, X. Wang, Y. Zhang, S. Zhou, T. Zhao, and N. Yao, "A novel chaotic system and its application in a color image cryptosystem," *Opt. Lasers Eng.*, vol. 121, pp. 479–494, Oct. 2019.

[35] A. Yaghouti Niyat, M. H. Moattar, and M. N. Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Opt. Lasers Eng.*, vol. 90, pp. 225–237, Mar. 2017.

[36] Y. Su, Y. Wo, and G. Han, "Reversible cellular automata image encryption for similarity search," *Signal Process., Image Commun.*, vol. 72, pp. 134–147, Mar. 2019.

[37] M. Ma, S. Mei, S. Wan, J. Hou, Z. Wang, and D. D. Feng, "Video summarization via block sparse dictionary selection," *Neurocomputing*, vol. 378, pp. 197–209, Feb. 2020.

[38] T. Gao, Z. Liu, J. Cao, and S. Liang, "Local difference ternary sequences descriptor based on unsupervised min redundancy mutual information feature selection," *Multidimensional Syst. Signal Process.*, to be published, doi: 10.1007/s11045-018-0595-z.

[39] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations," *Signal Process., Image Commun.*, vol. 52, pp. 6–19, Mar. 2017.

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

[41] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Comput. Mathematics Appl.*, vol. 59, no. 10, pp. 3320–3327, May 2010.

[42] X.-Y. Wang and Z.-M. Li, "A color image encryption algorithm based on Hopfield chaotic neural network," *Opt. Lasers Eng.*, vol. 115, pp. 107–118, Apr. 2019.

[43] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption," *Opt. Laser Technol.*, vol. 101, pp. 30–41, May 2018.

[44] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," *Multidimensional Syst. Signal Process.*, vol. 30, no. 2, pp. 943–961, Apr. 2019.

[45] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Opt. Lasers Eng.*, vol. 66, pp. 10–18, Mar. 2015.

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

[47] Q. Lai, B. Norouzi, and F. Liu, "Dynamic analysis, circuit realization, control design and image encryption application of an extended Lü system with coexisting attractors," *Chaos, Solitons Fractals*, vol. 114, pp. 230–245, Sep. 2018.

[48] L. Liu, Y. Wang, Y. Li, X. Feng, H. Song, Z. He, and C. Guo, "Noise robust method for analytically solvable chaotic signal reconstruction," *Circuits Syst. Signal Process.*, vol. 38, no. 9, pp. 4096–4114, Sep. 2019.

[49] Q. Lai and S. Chen, "Generating multiple chaotic attractors from Sprott B system," *Int. J. Bifurcation Chaos*, vol. 26, no. 11, Oct. 2016, Art. no. 1650177.

[50] Q. Lai, P. D. K. Kuate, F. Liu, and H. H.-C. Iu, "An extremely simple chaotic system with infinitely many coexisting attractors," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, to be published, doi: 10.1109/tcsii.2019.2927371.

LIDONG LIU received the B.S. and M.S. degrees in control theory and control engineering from Southwest Jiaotong University, in 2005 and 2008, respectively, and the Ph.D. degree in signal and information processing from the University of Electronics Science and Technology of China, in 2012. He is currently an Associate Professor with Chang'an University. He has authored and coauthored more than 40 articles in signal processing, control theory, and computational nonlinear journals and conferences. He has been involved with more than 10 projects supported by the National Natural Science Foundation of China and Natural Science Foundation of Shanxi province. His current research interests include image encryption, secure communication, and nonlinear control systems.

YUHANG LEI received the B.S. degree in communication engineering from the College of Electronic Information Engineering, Xi'an Technological University, China, in 2017. She is currently pursuing the degree with the College of Information Engineering, Chang'an University, China. Her current research interests include image encryption, cryptanalysis, and image privacy protection.

DAN WANG received the B.S. degree in measurement and control technology and instrument from the College of Information Engineering, Chang'an University, China, in 2018, where she is currently pursuing the degree with the College of Information Engineering. Her current research interests include image encryption, cryptanalysis, and image privacy protection.