IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 6, 2020, accepted November 19, 2020, date of publication November 24, 2020,
date of current version December 7, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3039891

A Dynamic Triple-Image Encryption Scheme Based on Chaos, S-Box and Image Compressing

LIU LIDONG[1], **DONGHUA JIANG**[1], **XINGYUAN WANG**[2], **LINLIN ZHANG**[1], **AND XIANWEI RONG**[3], **(Member, IEEE)**

[1]School of Information Engineering, Chang'an University, Xi'an 710064, China
[2]School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China
[3]Physics and Electronic Engineering School, Harbin Normal University, Harbin 150025, China

Corresponding author: Donghua Jiang (jiangdonghua@chd.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61701043 and Grant 41874140, in part by the Shaanxi Province Science and Technology Program under Grant 2020JM-220 and Grant 2020JQ-351, in part by the Fundamental Research Funds for the Central Universities of China under Grant 300102240205, and in part by the Natural Science Foundation of Heilongjiang Province under Grant F2018022.

ABSTRACT To guarantee the security and high-efficiency of image transmission, a novel triple-image encryption scheme based on chaotic system, S-box and image compressing is proposed in this paper. Firstly, the combination process is performed by compressing three plain images to 25% and combining the compressed images with a stochastic matrix generated by the 2D-LSCM system to construct a new image. This process makes the proposed image encryption scheme have higher image transmission efficiency comparing to that of the state-of-the-art methods. Then, Z-scan and the proposed coded lock scrambling algorithm with low time complexity is used to randomly scramble the positions of pixels in the new construct image. Next, a cipher image is obtained by performing the diffusion operation on the scrambled image through S-box and chaotic sequences. In addition, the added stochastic matrix in the combination process makes the cipher image dynamic. In other words, the generated cipher images are always different to each other even when they are generated by the proposed encrypt scheme with identical plain images under the same secret keys, which can resist chosen-plaintext attacks. Finally, experimental results and simulation analysis are performed, which shows the proposed scheme can effectively resist common kinds of attacks.

INDEX TERMS Information security, image encryption, image compressing, chaos.

I. INTRODUCTION

Recently, with the amount of image information transmitted in the public network, it is necessary to design security and high-efficiency digital image encryption schemes in order to relieve the channel transmission burden and reduce storage space. The conventional encryption schemes designed for pure text infor-mation, such as AES, DES and RSA, can no longer meet the requirements of digital image encryption. One reason is that the pure text information is fundamentally different from digital image information [1]. Another reason is that the conventional encryption schemes for pure text information have a high computational complexity [2]. Later, with the maturity of chaos theory, it has been found that the chaotic systems have noise-like characteristics and extremely sensitive to initial values [3], [4], which are very suitable for secure communication. The emer-gence of chaos theory provides a new direction for image encryption.

At present, researchers have designed lots of chaotic image encryption schemes [5]–[23] based on the classical scrambling-diffusion architecture proposed by Fridrich in 1998 [5]. These image encryption schemes can be divided into the following four categories. (1) The first category is new architecture schemes for image encryption, such as the permutation-modulation-diffusion architecture [6], the permutation-diffusion-linear transformation architecture [7] and permutation-rewriting-diffusion architecture [8]. These encryption schemes aim to address the shortcomings of the classical scrambling-diffusion encryption architecture, which enhances the relationship between pixel scrambling

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

and diffusion. (2) The second category is to improve the chaotic systems and to apply them to image encryption. There are some defects in the classical one-dimensional chaotic system, such as small key space, blank windows and weak chaotic behavior. As a result, some image encryption schemes based on the improved chaotic systems were proposed. For example, Parvaz and Zarebnia [9] created a new chaotic system by combining Logistic, Sine and Tent chaotic systems, which eliminated the influence of blank windows and made the improved chaotic system have a very large key space. And then, the authors proposed a robust image encryption scheme based on the improved one-dimensional chaotic system. Similarly, a chaos improvement method was proposed by Hua *et al.* [10], and the defects of the seed chaotic systems can be solved perfectly through the cosine transform. (3) The third category is to add new technologies into chaotic image encryption schemes, for instance, DNA coding technology [11], Boolean network and matrix semi-tensor product theory [12]. DNA coding is characterized by parallel processing, massive storage and ultra-low power consumption. Chai *et al.* [11] combined chaos theory and DNA coding technology to encrypt the plain images. In their encryption scheme, the RGB com-ponents of the color plain image is extracted separately, and then a simultaneous intra-inter-component permutation mechanism is used for randomly scrambling the three components, and the cipher image can be obtained by diffusing the matrix encoded by DNA. The advantage of this scheme is that it can realize a dynamic DNA coding mechanism according to different plain images. Recently, Wang and Gao [12] combined Boolean network, matrix semi-tensor product theory and chaos theory to proposed a high-security image encryption scheme, which also can be used to encrypt other complex networks. (4) The fourth category is to enhance the speed of image encryption. Some encryption sche-mes have complex processes and high time complexity during the encryption, which cannot meet the requirements of real-time communication. Therefore, fast image encryption schemes emerged. In order to reduce the computational complexity, the most common method is to merge the scrambling operation with the diffusion operation. Another advantage of performing this is that it can resist separate attacks. Such as [13] and [14], both of them follow this rule to enhance the encryption speed. In [13], the initial value of the 2D Hénon-Sine system is generated according to the secret keys and plain image. Then the chaotic sequences are used to simultaneously scramble and diffuse the rows and columns to enhance the time speed. In [14], a cross-cyclic shift algorithm which is also a kind of simultaneous scrambling and diffusion scheme, is proposed for fast encryp-tion. The above-mentioned encryption schemes all have splendid security performance. However, the transmission efficiency of these schemes is not high. That is to say that only one cipher image is transmitted at a time.

Multi-plain image encryption is a research hotspot in the field of image encryption, and many scholars have also proposed lots of related encryption algorithms [24]–[29]. For example, Patro *et al.* [24] proposed that using the cross-coupled chaotic system to scramble and diffuse multiple plain images in pixel-level. In addition, Zhang and Wang [25] also proposed a set of multiple plain image encryption scheme based Deoxyribonucleic acid encoding and chaos. However, these proposed algorithms that encrypt multiple images simultaneously have the same transmission efficiency as that of encrypting one plain image at a time. One way to enhance the image transmission efficiency is to compress several plain images into one image for transmission.

The common method for image compression in image encryption is the compressive sensing (CS) technology [30]–[42]. It can simultaneously sample and compress signals to reduce the transmission burden and storage space. For example, in [30], color plain images were compressed by CS and Arnold chaotic system, which can release transmission space. However, the measurement matrices used to compress the color plain image in [30] were randomly generated, which caused the decryption end should obtain these random matrices as secret keys. This increased the storage space of the secret keys and the transmission channel burden. To solve this problem, in [31], Zhou *et al.* proposed a hybrid image compression-encryption algorithm based on compressive sensing which can encrypt and compress the plain images simultaneously without generating extra secret keys. Subsequently, [32] used 2D compressive sensing technology to compress the plain images so that the data capacity of the cipher images can be further reduced. In [33], Chai *et al.* proposed a plain related image encryption scheme by combining the memristive chaotic system, the elementary cellular automata and the compressive sensing technology. The permutated sparse coefficient matrix was compressed by a circular measurement matrix generated by the memristive chaotic system to decrease data transmission. In [34], Xu *et al.* proposed a fast and high-efficiency image encryption scheme by the improved chaotic system and compressive sensing. in which the plain images were compressed by two circular measurement matrices from two directions. Note that, although the application of CS technology to image encryption can improve the trans-mission efficiency, there are still some disadvantages. (a) Though plain images can be compressed by the compressive sensing to any size, the decrypted image has large distortions when the compression rate is lower than 0.5, such as that in [35]. (b) In the decryption process, the decryption algorithm needs the maximum value and the minimum value of the observation matrix besides the secret keys. Subtle differences of plain images can result in the observation matrices being different to each other, which caused the extreme value of observation matrices should be transmitted to the decryption end for decrypting. (c) The ability to resist the occlusion attack is limited. It is very difficult to identify the decrypted image when a certain amount of cipher image information is lost during transmitted in the public channel.

In order to enhance the security and transmission efficiency for image encryption, a novel triple image encryption scheme based on chaotic systems, S-box and image compressing is proposed in this paper. The proposed encryption scheme consists of three processes: combination, scrambling and diffusion. In the combination process, three plain images are compressed and then combined with a stochastic matrix generated by the 2D-LSCM system to construct the combined image. In the scramb-ling process, the combined image is transformed into the 1D sequence by Z-scan. Then the coded lock scrambling algorithm is adopted to randomly scramble the positions of the 1D sequence. Finally, in the diffusion process, the S-box generated by the Sin-Tent piecewise chaotic system (STS) system and the chaotic sequence generated by the 2D-LSCM system are used to diffuse the scrambled image to obtain the cipher image. More-over, the proposed encryption scheme is not a one-time pad. Batches of cipher images can be decrypted with a group of fixed secret keys. It does not need to manage huge secret keys like one-time pad schemes. The proposed encryption scheme has the following four advantages.

(1) The generated cipher image has the dynamic characteristic (see in section V.A). Every time the cipher image is different even when they are generated by the proposed encrypt scheme with the identical plain image under the same secret keys. So, it is unavailable to construct the special images like [43], [44] to attack the proposed encryption scheme.

(2) It has high efficiency, which can encrypt three images at a time. And its efficiency is higher than that of in [33], [36].

(3) It is robust against noise attacks and occlusion attacks. Even the cipher image is cut off 50% or suffer 30% salt and pepper noise attacks, the decrypted image is still visible (see in Section V.H).

(4) The proposed encryption scheme has low time complexity (see in section V.J), which benefits from the proposed coded lock scrambling (the detailed analysis of this scrambling algorithm is shown in section III).

The rest of this paper consists of the following sections. The second section briefly introduces the required theoretical knowl-edge. The third and the fourth section elaborate on the proposed encryption and the corresponding decryption algorithm. The security performance analyses of the encryption algorithm are presented in the fifth section. The last section summarizes our research work.

II. FUNDAMENTAL KNOWLEDGE

In general, the classical one-dimensional chaotic systems, such as Logistic system, Sine system, Tent system, have some drawbacks like simple structure, small key space and weak chaotic characteristics. This causes these chaotic systems are easy to be attacked by the signal estimation algorithm [45] in the encryption scheme. Therefore, we should try to use the system with complex chaotic characteristics to devise the encryption rules when designing the image encryption scheme. In this paper, the two-dimensional chaotic system [46] and the improved one-dimensional chaotic system [47] are adopted to design the encryption rules.

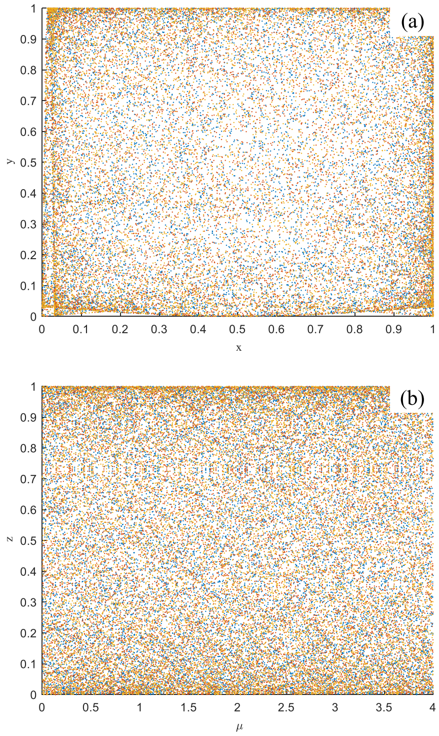


FIGURE 1. Performance analysis chart of chaotic systems. (a) the trajectory chart of the 2D Logistic-Sine-coupling map; (b) the bifurcation chart of the Sine-Tent system.

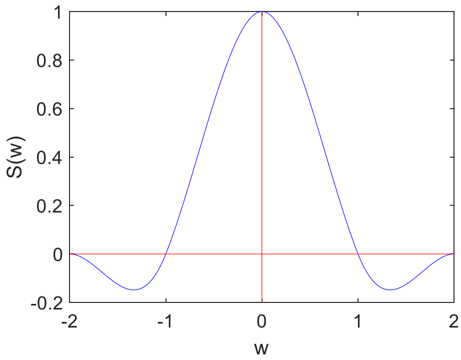


FIGURE 2. The basis function of the bicubic interpolation.

A. THE 2D LOGISTIC-SINE-COUPLING MAP

The 2D chaotic system (2D-LSCM) used in the paper is obtained by coupling the Logistic system and the Sine system. The mathematical iterative formula [46] is expressed in Eq.(1).

$$\begin{cases} x_{i+1} = \sin(\pi(4\theta x_i(1-x_i)) + (1-\theta)\sin(\pi y_i))) \\ y_{i+1} = \sin(\pi(4\theta y_i(1-y_i)) + (1-\theta)\sin(\pi x_{i+1}))) \end{cases} \tag{1}$$

where, θ is the control parameter of this 2D chaotic system, which belongs to [0, 1], **x** and **y** are the generated pseudo-random sequences. As shown in Fig.1, (a) is the trajectory chart generated by 2D-LSCM (parameters: $x_0 = 0.8$, $y_0 = 0.5$, $\theta = 0.99123675342$). It can be seen from the figure that

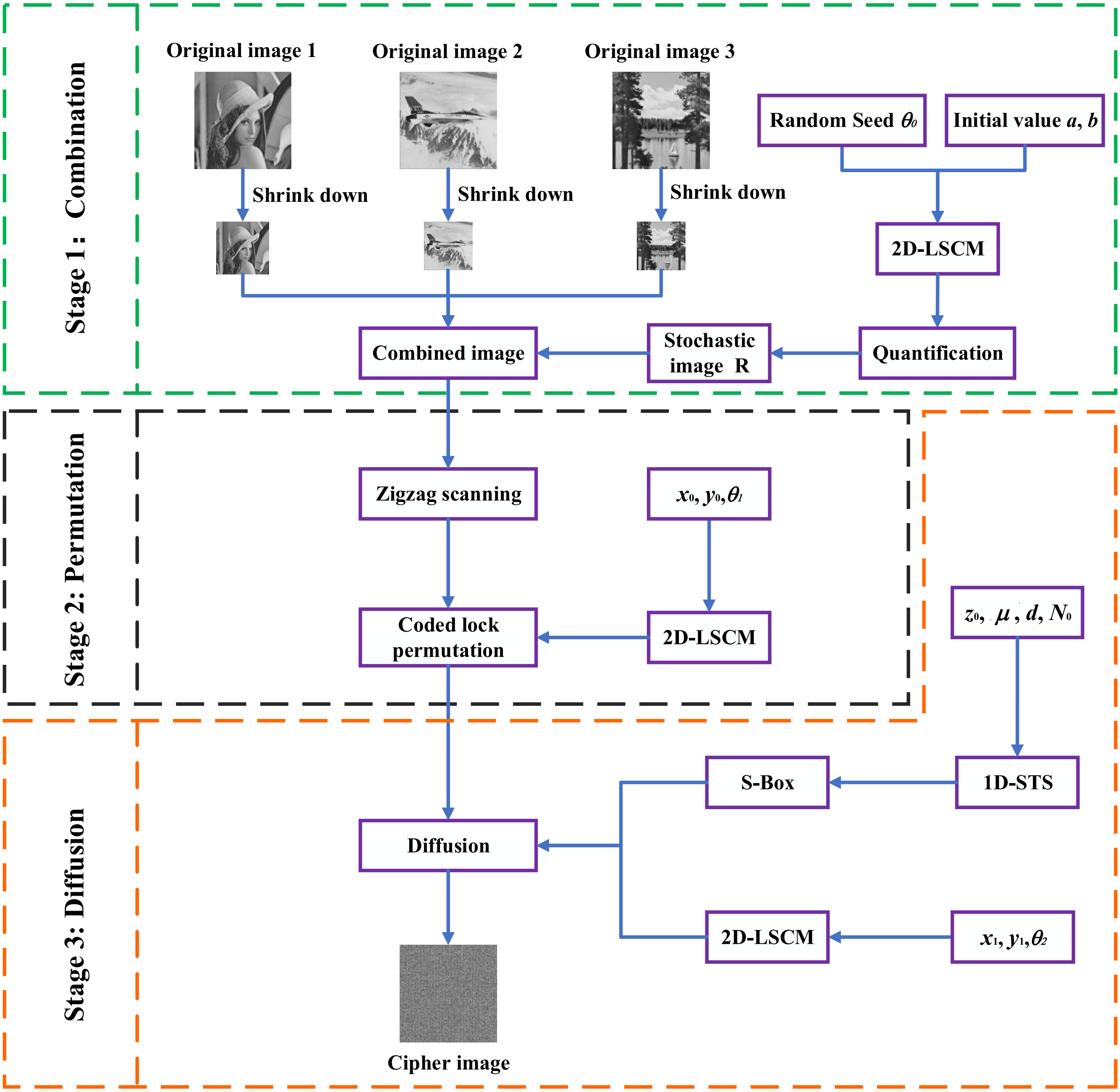


FIGURE 3. The flow chart of the proposed encryption algorithm.

the trajectories of this 2D coupled chaotic system can occupy all phase plane and distribute uniform.

B. THE SINE-TENT SYSTEM

The second chaotic system used in this paper is the Sin-Tent piecewise chaotic system (STS) proposed in [37]. The mathematical model of STS is shown in Eq.(2).

$$z_i = \begin{cases} \frac{4-\mu}{4} \times \sin(\pi z_i) + \frac{\mu}{2} \times z_i & z_i < 0.5 \\ \frac{4-\mu}{4} \times \sin(\pi z_i) + \frac{\mu}{2} \times (1 - z_i) & z_i \geq 0.5 \end{cases} \tag{2}$$

where, μ is the control parameter of the Sin-Tent piecewise chaotic system. When μ is evaluated between [0, 4], this system is in a chaotic state. Fig.1.b is the bifurcation chart of this improved chaotic system (parameters: $z_0 = 0.21$, $\mu = 3.9982789374626$). It indicates that compared with the Sine system and Tent system, the STS chaotic system has a wider chaotic range and eliminates the blank windows. Therefore, the generated chaotic sequence has better randomness and is more difficult to predict.

C. THE BICUBIC INTERPOLATION

The bicubic interpolation is also called cubic convolution interpolation, which is first proposed in [48]. This interpolation algorithm adopts sixteen-pixel points around the sampled point for interpolation operation, which not only takes into account the gray values of four directly adjacent pixels, but also takes into account the gray value change rate between the adjacent pixel points [49]. Thus, we can obtain a high resolution enlarge-ed image by using the bicubic interpolation algorithm. In the interpolation process, it is necessary to select the appropriate basis function $S(w)$ to fit the sampled data. The most common interpolation basis function is represented in Eq.(3). Fig.2 shows the functional image of the interpolation basis function $S(w)$. The method of enlarging the sampled image by using the bicubic interpolation algorithm is shown in Eq.(4).

$$S(w) = \begin{cases} 1 - 2\left|w|^2\right| + \left|w|^3\right| & |w| < 1 \\ 4 - 8|w| + 5|w|^2 - |w|^3 & 1 \leq |w| < 2 \\ 0 & |w| \geq 2 \end{cases} \tag{3}$$

$$f(x,y) = \sum_{i=0}^{3}\sum_{j=0}^{3} f(x_i, y_i) \times S(x - x_i) \times S(y - y_i) \tag{4}$$

where, $f(x, y)$ represents the pixel value of the interpolated point (x, y). Similarly, $f(x_i,y_i)$ is the pixel value of the neighborhood (x_i,y_i) near the interpolated point.

III. THE PROPOSED ENCRYPTION ALGORITHM

In this paper, we propose a dynamic triple image encryption scheme based on the chaotic system, S-box and image compr-essing technology. The proposed encryption scheme can be divided into three stages: combination, scrambling and diffusion. The flowchart of the proposed encryption scheme is shown in Fig.3. In the combination stage, three plain images are compressed by the image compressing technology. Then, the three compressed images are combined with a stochastic matrix generated by a two-dimensional chaotic system. This makes the cipher image dynamic since the parameter θ of the two-dimensional chaotic system is a dynamic variable (θ is not the secret in combination process, and it is randomly selected in [0, 1] each time) which causes the stochastic matrix generat-ed by the chaotic system is different each time. In other words, the generated cipher is different even when it is generated by the proposed encrypt scheme with the identical plain images under the same secret keys, which can resist chosen-plaintext attacks. In the scrambling stage, a novel fast scrambling algorithm named coded lock scrambling is proposed to improve the processing speed. The pseudo-code of the proposed scrambling algorithm is demonstrated in Tab.11 (shown in Appendices). In the last stage, we introduce a nonlinear component S-box of which the pseudo-code is demonstrated in Tab.12 (shown in Appendices) to participate in the diffusion process. Next, we will describe the encryption process of the proposed scheme in detail. For the sake of description, we assume that the three plain images are $\mathbf{P1} \in \mathbb{N}^{M\times N}$, $\mathbf{P2} \in \mathbb{N}^{M\times N}$ and $\mathbf{P3} \in \mathbb{N}^{M\times N}$ respectively.

Step 1. Input three different plain images **P1**, **P2** and **P3**. Compress these plain images according to Eq.(5)-Eq.(7), where $i = 1, 2, 3, \ldots, M/2$, $j = 1, 2, 3, \ldots, N/2$. Denote these compressed images as **SP1**, **SP2** and **SP3**, respectively. It can be seen from the Eq.(5)-Eq.(7) that the size of the compressed images is a quarter that of the plain images.

$$\mathbf{SP1} = \frac{\boldsymbol{P1}_{2i-1,2j-1} + \boldsymbol{P1}_{2i,2j-1} + \boldsymbol{P1}_{2i-1,2j} + \boldsymbol{P1}_{2i,2j}}{2\times 2} \tag{5}$$

$$\mathbf{SP2} = \frac{\boldsymbol{P2}_{2i-1,2j-1} + \boldsymbol{P2}_{2i,2j-1} + \boldsymbol{P2}_{2i-1,2j} + \boldsymbol{P2}_{2i,2j}}{2\times 2} \tag{6}$$

$$\mathbf{SP3} = \frac{\boldsymbol{P3}_{2i-1,2j-1} + \boldsymbol{P3}_{2i,2j-1} + \boldsymbol{P3}_{2i-1,2j} + \boldsymbol{P3}_{2i,2j}}{2\times 2} \tag{7}$$

Step 2. Input the initial value a, b and the control parameter θ_0 (the probability density of θ_0 is defined in Eq.(9)) of 2D-LSCM to generate two chaotic sequences $\mathbf{sx} \in \mathbb{R}^{1\times MN/4}$ and $\mathbf{sy} \in \mathbb{R}^{1\times MN/4}$. Then, two stochastic matrices $\mathbf{R1} \in \mathbb{R}^{M/2\times N/2}$ and $\mathbf{R2} \in \mathbb{R}^{M/2\times N/2}$ are generated by Eq.(8). Note that, parameter θ_0 is randomly selected in [0, 1] each time for image encryption. That is, for the ith and jth ($i \neq j$) encryption process, we have $\theta_0^{(i)} \neq \theta_0^{(j)}$. This causes matrices **R1**, **R2** to be dynamic changing ($\mathbf{R1}^{(i)} \neq \mathbf{R1}^{(j)}, \mathbf{R2}^{(i)} \neq \mathbf{R2}^{(j)}$) even for encrypting the identical plain images under the same secret keys.

$$\begin{cases} \mathbf{R1} = \begin{bmatrix} sx_1 & sx_{\frac{M}{2}+1} & \cdots & sx_{\frac{(MN-2M)}{4}+1} \\ sx_2 & sx_{\frac{M}{2}+2} & \cdots & sx_{\frac{(MN-2M)}{4}+2} \\ \cdots & \cdots & \cdots & \cdots \\ sx_{\frac{M}{2}} & sx_M & \cdots & sx_{\frac{MN}{4}} \end{bmatrix} \\ \mathbf{R2} = \begin{bmatrix} sy_1 & sy_{\frac{M}{2}+1} & \cdots & sy_{\frac{(MN-2M)}{4}+1} \\ sy_2 & sy_{\frac{M}{2}+2} & \cdots & sy_{\frac{(MN-2M)}{4}+2} \\ \cdots & \cdots & \cdots & \cdots \\ sy_{\frac{M}{2}} & sy_M & \cdots & sy_{\frac{MN}{4}} \end{bmatrix} \end{cases} \tag{8}$$

$$f(\theta_0) = \begin{cases} 1, & 0 \leq \theta_0 \leq 1 \\ 0, & \text{otherwise} \end{cases} \tag{9}$$

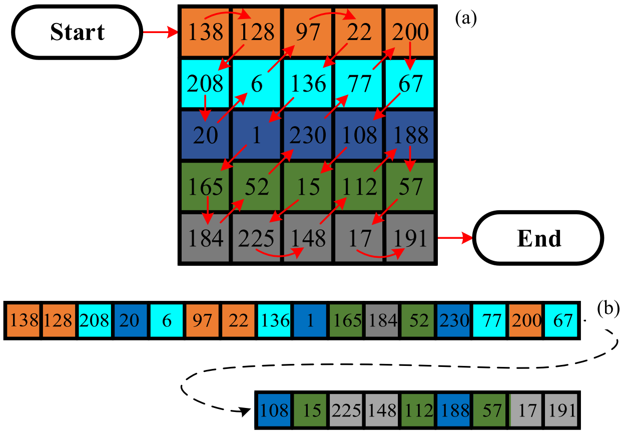
Step 3. Obtain the quantized matrices **QR1**, **QR2** by Eq.(10), where, mod(·) represents the remainder operation performed on the two elements in parentheses, floor(·) performs rounding the element in parentheses to the negative infinity direction. Then, the matrix **R** which is used to combine with the three compressed images is obtained by Eq.(11), where bitxor(·) performs bitwise xor operation on the two elem-ents in parentheses. **R** is also dynamics changing each time for encryption, since **R1** and **R2** are dynamics matrices.

$$\begin{cases} \mathbf{QR1} = \mathrm{mod}(\mathrm{floor}(\mathbf{R1}(:) \times 10^{10}), 256) \\ \mathbf{QR2} = \mathrm{mod}(\mathrm{floor}(\mathbf{R2}(:) \times 10^{10}), 256) \end{cases} \tag{10}$$

$$\mathbf{R} = \mathrm{bitxor}(\mathbf{QR1}, \mathbf{QR2}) \tag{11}$$

Step 4. Combine the three compressed images **SP1**, **SP2** and **SP3** with the stochastic matrix **R** by Eq.(12) and obtain the combined image **C** with the size $M \times N$.

$$\mathbf{C} = [\mathbf{SP1}, \mathbf{R}; \mathbf{SP2}, \mathbf{SP3}] \tag{12}$$



138	128	97	22	200
208	6	136	77	67
20	1	230	108	188
165	52	15	112	57
184	225	148	17	191

138	128	208	20	6	97	22	136	1	165	184	52	230	77	200	67

108	15	225	148	112	188	57	17	191

FIGURE 4. An example of zigzag scrambling. (a) schematic diagram of zigzag scan; (b) the generated sequence.

Step 5. Scan the combined image **C** like a Z-shape, and denote the obtained sequence as **ZC**. Then, **ZC** is divided into four equal sub-bocks that are denoted as **ZC1** $\in \mathbb{N}^{1\times(MN/4)}$, **ZC2** $\in \mathbb{N}^{1\times(MN/4)}$, **ZC3** $\in \mathbb{N}^{1\times(MN/4)}$ and **ZC4** $\in \mathbb{N}^{1\times(MN/4)}$ by Eq.(13). The schematic diagram of the Z-scan is shown in Fig.4.a, where the red arrow indicates the scanning direction. Fig.4.b shows the gener-ated sequence by Z-scanning. The variable i belongs to 1, 2, 3, 4} in Eq.(13).

$$\mathbf{ZC}i = \mathbf{ZC}(\frac{MN}{4}(i-1)+1 : \frac{MN}{4}i) \tag{13}$$

Step 6. Iterating the 2D-LSCM ($T0+MN/4$) times through the secret keys x_0, y_0 and θ_1 to obtain the chaotic sequences **u** and **v**. $T0$ is any positive integer greater than 100, which is used to eliminate the transient effects. Generating another two sets of chaotic sequences **w** ($\mathbf{w} = \mathbf{u}(:) + \mathbf{v}(:)$) and **z**($\mathbf{z} = \mathbf{u}(:) - \mathbf{v}(:)$).

Step 7. Sort the obtained four sets of chaotic sequences **u**, **v**, **w** and **z** by Eq.(14).

$$\begin{cases} [\sim, \mathbf{Tu}] = \text{sort}\,(\mathbf{u}\,(:)) \\ [\sim, \mathbf{Tv}] = \text{sort}\,(\mathbf{v}\,(:)) \\ [\sim, \mathbf{Tw}] = \text{sort}(\mathbf{w}(:)) \\ [\sim, \mathbf{Tz}] = \text{sort}(\mathbf{z}(:)) \end{cases} \tag{14}$$

where sort(**tmp**) indicates that the sequence **tmp** in parentheses is sorted in ascending order. The index sequence **Ttmp** is then returned.

Step 8. Scramble the sequence **ZC**x ($x = 1, 2, 3, 4$) through the four sets of index sequences by Eq.(15).

$$\begin{cases} \mathbf{img\_p}(4i-3) = \mathbf{ZC}1(\mathbf{Tu}(i)) \\ \mathbf{img\_p}(4i-2) = \mathbf{ZC}2(\mathbf{Tv}(i)) \\ \mathbf{img\_p}(4i-1) = \mathbf{ZC}3(\mathbf{Tw}(i)) \\ \mathbf{img\_p}(4i)= \mathbf{ZC}4(\mathbf{Tz}(i)) \end{cases} \tag{15}$$

Step 9. Iterate the two-dimensional chaotic system ($T0+256$) times through the secret keys x_1, y_1 and θ_2 to generate the chaotic sequence **m** $\in \mathbb{N}^{16\times16}$. Then, input another set of secret keys μ, z_0 and odd integer d which is greater than 0 to generate the S-box **S** $\in \mathbb{N}^{16\times16}$. Tab.12 (shown in Appendices) shows the pseudo-code used to generate a S-box.

Step 10. Generate a sequence **T** by Eq.(16). Then obtain a chaotic sequence $\mathbf{z} \in \mathbb{R}^{1\times256}$ by using μ, z_0 and N_0 to iterate the STS chaotic system (defined by Eq.(2) in section II.B). Next, the sequence **T** is scrambled by the index sequence **Tz** which is obtained by sorting the chaotic sequence **z**. Then the S-box used for diffusion can be obtained through Eq.(19).

$$\mathbf{T} = \text{mod}(d \times [1:256], 256) \tag{16}$$

$$[\sim, \mathbf{Tz}] = \text{sort}(\mathbf{z}) \tag{17}$$

$$\mathbf{Ts}(i) = \mathbf{T}(\mathbf{Tz}(i)), \quad i = 1, 2, 3, \ldots, 256 \tag{18}$$

$$\mathbf{S} = \text{reshape}(\mathbf{Ts}, 16, 16) \tag{19}$$

Step 11. The scrambled matrix **img_p** is divided into blocks with the size of 16 × 16. Then, use the chaotic sequence **m**(obtained in step 9 above) and the S-box **S** to diffuse all blocks by Eq.(20). Finally, all the diffused blocks are stitched to obtain the cipher image with the size of $M \times N$.

$$\mathbf{img\_d}(i,j) = \text{mod}(\mathbf{img\_p}(i,j) + \mathbf{m}(i,j), 256) \oplus \mathbf{S}(i,j) \tag{20}$$

where, i and j are integers and belong to [1], [16].

Note that, from the aforementioned descriptions, the proposed encryption scheme has the following advantages. (1) The generated cipher image has the dynamic characteristic. That is to say, the proposed encryption scheme can encrypt three identical plain images into different cipher images even under the same secret keys. The reason is that the parameter θ_0 in step 2 is randomly selected in [0,1] each time, which causes the 2D-LSCM chaotic system to generate different sequences each time. This makes the stochastic matrix **R** (in step 6) which is used to combine the three compressed plain images, to be dynamic changing. (2) It has high transmission efficiency which up to 300% compared to that of conventional image encryption schemes. The decrypted image also has a well visual effect under such high transmission efficiency (the peak signal-to-noise ratio is greater than 30 dB, shown in Section V.G). (3) The proposed scheme has low time complexity which benefit by the new scrambling algorithm named coded lock scrambling. Fig.5.a shows a scrambled image obtained by performing one round of coded lock scrambling on the Lena image with the time 0.02352s. Fig.5.b shows the scrambling time comparison, which illustrates the proposed scrambling algorithm has high time speed.

IV. THE PROPOSED DECRYPTION ALGORITHM

The specific steps for decryption are described as follows. Firstly, the reverse diffusion of the cipher image is performed according to the diffusion matrix and the S-box which are constructed based on the decryption secret keys. Eq.(21) shows the inverse diffusion process. The proposed coded lock scrambling algorithm in this paper is also reversible, so the obtained matrix after inverse diffusion operation is then performed by inversing scrambling by the pseudo-code in

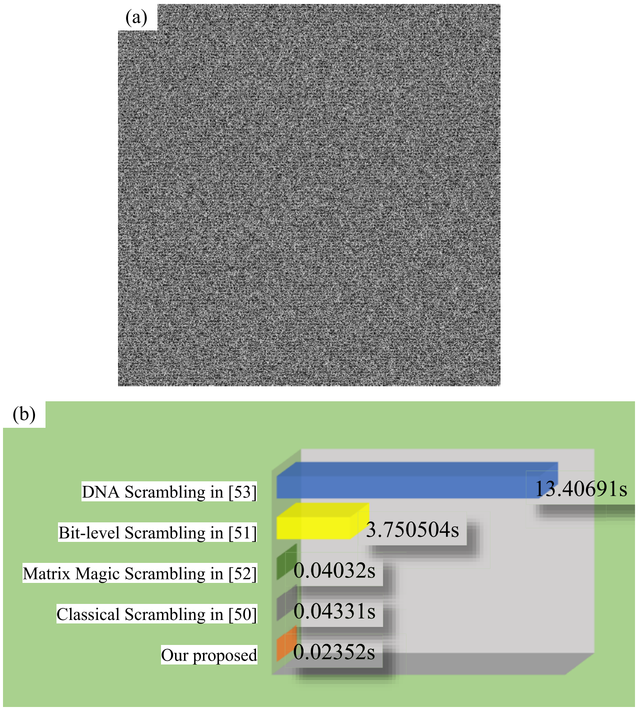


FIGURE 5. Experimental results of the new scrambling algorithm. (a) a scrambled image; (a) the scrambling time comparison.

Tab.11 (shown in Appendices). Finally, the combined image **C** generated in the previous operation is segmented into three compressed plain images and a stochastic image which is useless and will be discarded. The corresponding plain images are reconstructed at a high resolution by the bicubic interpolation algorithm to three compressed images (shown in Section II.C). Thus, the decryption process of the cipher image is completed.

$$\mathbf{img\_p}(i,j) = \text{mod}(\mathbf{img\_d}(i,j) \oplus \mathbf{S}(i,j) - \mathbf{m}(i,j), 256) \quad (21)$$

It is worth mentioning that although the generated cipher image changes dynamically, the encryption rules in the scrambling and diffusion process are controlled by the secret keys. So, when the encrypted image is transmitted to the receiver, the receiver can decrypt the cipher image according to the obtained secret keys and decryption scheme, since the dynamic stochastic image **R** is discarded, which does not affect the process of decryption.

V. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental simulation results of the proposed encryption scheme are demonstrated in this section. Nine selected plain images (Lena, Airplane, Sailboat, Barbara, Boat, Bridge, Couple, Crowd and Fruits) with size of 512 × 512 are divided into three groups for experiments. The encryption secret keys are set as $x_0 = 0.21$, $y_0 = 0.34$, $\theta_1 = 0.124$, $x_1 = 0.123$, $y_1 = 0.4$, $\theta_2 = 0.783$, $d = 124$, $\mu = 3.789$ and $z_0 = 0.127$. All simulation experiments are run in Matlab 2018b on the notebook (Intel(R) Core(TM) i7-8550U CPU 8G Memory and Windows 10 Enterprise). In addition, the proposed encry-ption algorithm is only suitable for the plain image whose length is equal to width. Fig.6 shows the results of the simulation experiments. In Fig.6, (A1)-(A3) are three plain images. (A4) is a stochastic image with the size of 256 × 256 generated during the encryption process. (A5) is the final generated cipher image with the size of 512 × 512. (A6)-(A8) are the corresponding decrypted images under the correct decryption secret keys. In the same way, the images of group B and group C can be obtained. It can be seen from the experiment results. (1) The cipher images generated by the proposed encryption scheme are disordered, and the related texture information of the plain images are completely covered up. (2) The proposed encryption scheme has good compression performance. Although the compression rate is as high as 33.33%, the decrypted image is basically the same as the plain image, which means that the decrypted images have well visual effect.

Next, we will analyze the security performance of the proposed encryption scheme and compare it with that of the state-of-the-art methods [33], [36], [39]–[41] published in recent years.

A. CHOSEN PLAINTEXT ATTACK ANALYSIS

Chosen-plaintext analysis on the encryption scheme is the most common and effective way of attacking. An excellent image encryption scheme should not only completely conceal the plain image information, but also resist the chosen-plaintext attacks. To address this issue, we propose a dynamic image encryption scheme. In other words, each time the generated cipher image is random and unpredictable. Tab.1 shows the experimental results of analyzing cipher images with the dynamic characteristic, where (A1)-(A3) are three plain images. Besides, (A4) and (A5) are the cipher images obtained by encrypting the three plain images two times with the same secret keys. The structural similarity of the two cipher images is 74.9062%, and the pixel change rate is 24.9134%, which can be seen from Tab. 1. This means that millions of different cipher images can be generated by the proposed scheme with the same secret keys for encrypting identical plain images. Therefore, the proposed encryption scheme can resist the chosen-plaintext attacks very well.

B. KEY SPACE ANALYSIS

The key space represents the total number of all different secret keys, and its size reflects the ability of the encryption scheme to resist brute-force attacks. From a security perspective, A keys pace greater than 2^{100} can satisfy a high level of security [54]. Assume that the calculation accuracy of the computer is 10^{-15}. In this paper, the secret keys of the encryption scheme are mainly composed of the following three parts. (a) The secret keys used to generate the scrambling sequence are x_0, y_0 and θ_1. The secret keys pace in this part is $10^{15} \times 10^{15} \times 10^{15}$. (b) The secret keys used to generate the diffusion sequence are x_1, y_1 and θ_2. The secret keyspace in this part is $10^{15} \times 10^{15} \times 10^{15}$(c) The secret keys used

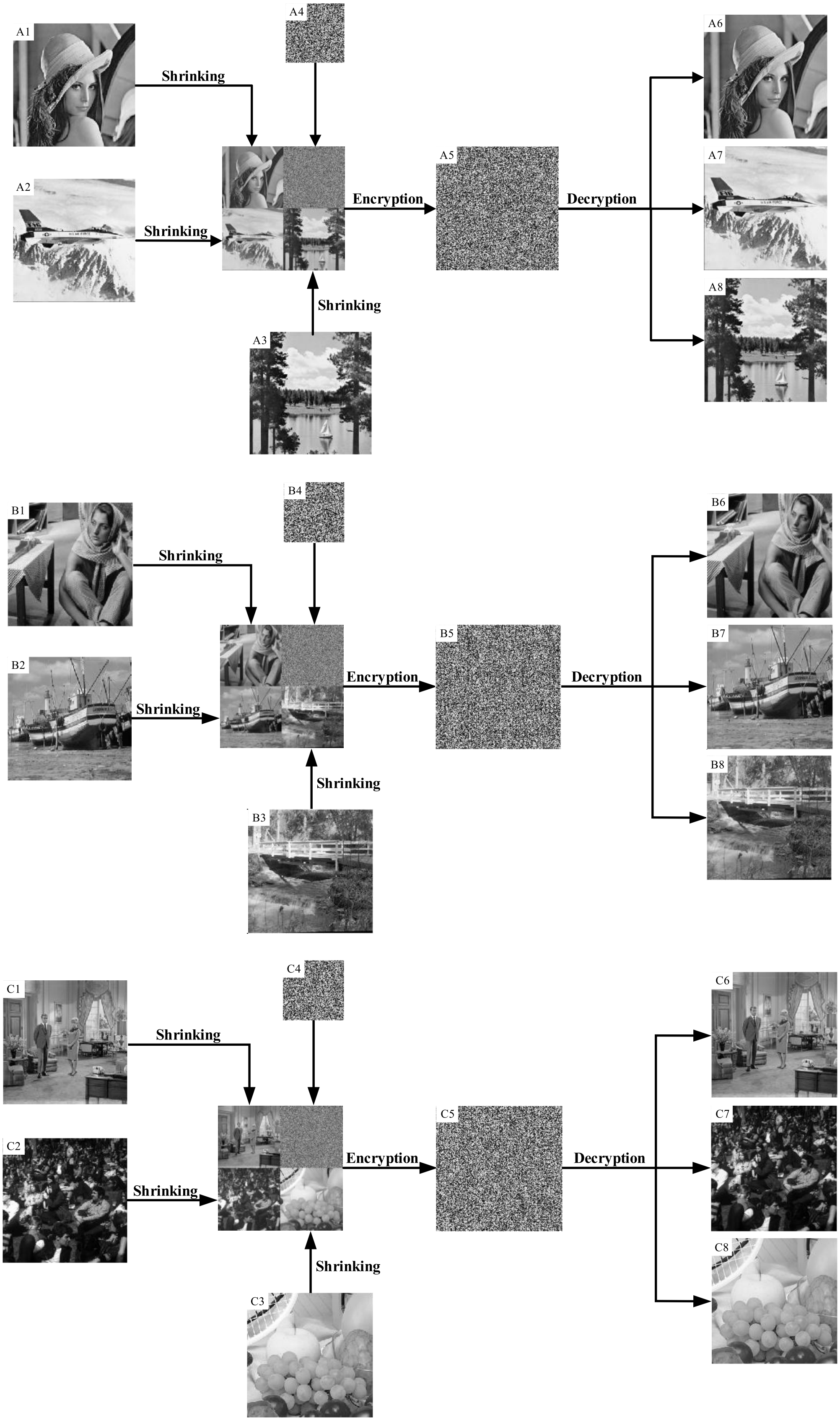


FIGURE 6. Simulation results of the proposed image encryption.

TABLE 1. Experimental results of dynamical cipher image test.

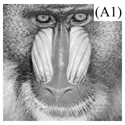
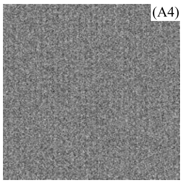
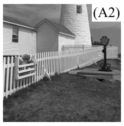
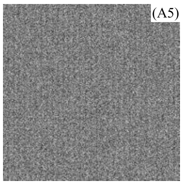
Plain image	Cipher image	SSIM	NPCR
 (A1)	 (A4)	0.7491	0.2491
 (A2)	 (A5)		
(A3)			

TABLE 2. Key space comparison with other algorithms.

Algorithm	Our	[33]	[36]	[39]	[40]	[41]
Key space	2^{561}	2^{232}	2^{504}	2^{176}	2^{149}	2^{448}

TABLE 3. Results of the histogram test on standard test images.

Image	histogram variance	
	Plain image	Cipher image
Lena	30665.703	297.862
Airplane	67829.394	
Sailboat	79401.053	
Barbara	37864.753	275.209
Boat	18369.607	
Bridge	15618.827	
Couple	63801.197	299.593
Crowd	27364.158	
Fruits	21983.516	

to generate the S box are d, μ and z_0. The key space in this part is $10^4 \times 10^{15} \times (10^{15})^4$ Then the complete secret key space of the encryption scheme is $(10^{15} \times 10^{15} \times 10^{15})^2 \times 10^4 \times 10^{15} \times (10^{15})^4 = 10^{169} \approx 2^{561}$ which is much larger than that of the references listed in Tab. 2. That is to say, the proposed encryption scheme has an outstanding ability to resist the brute-force attacks.

C. KEY SENSITIVITY ANALYSIS

Secret key sensitivity reflects the sensitivity of the encryption scheme to the secret keys, which means that the difference between the decrypted image and the plain image when the secret keys changed imperceptibly. Mean square error (MSE) is an indicator to measure the sensitivity of the encryption scheme to the secret keys. In this part, we also evaluate the secret key sensitivity of the encryption scheme through the MSE. The mathematical model of the MSE is

$$\text{MSE} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(\mathbf{P}_{i,j} - \mathbf{D}_{i,j})^2 \tag{22}$$

where, M and N represent the size of the image $\mathbf{P}$ or $\mathbf{D}$, respectively. (i, j) respectively represent the positions of pixels in the image. Fig.7 shows the Lena image obtained by decrypting with the incorrect secret keys. Fig. 8 shows the MSE curves of the secret keys $x_0, y_0, \theta_1, x_1, y_1, \theta_2, \mu$ and z_0. It is illustrated that when the correct secret keys are changed slightly, the cipher image cannot be decrypted correctly, and the decrypted image visually does not reveal any information of the plain image, which means the proposed encryption scheme has well secret key sensitivity.

D. HISTOGRAM ANALYSIS

The histogram describes the frequency of each gray level in the image, which reflects the gray level distribution of the image. In order to resist statistical attacks, it requires the histogram distribution of the cipher image to be uniform. According to [43], we can analyze the distribution of any image histogram by histogram variance through Eq.(23).

$$Var(U) = \frac{1}{N^2}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\frac{(u_i - u_j)^2}{2} \tag{23}$$

where $N = 256$, u_i and u_j respectively represent the number of pixel value i and j$(i, \mathrm{j} = 0, 1, 2, \ldots, 255)$ in image. Tab.3 is the histogram test results of the multiple plain images and corresponding cipher images. In addition, the Kolmogorov-Smirnov Goodness of Fit Test [55] is also applied to check the distribution of the cipher image. Firstly, constructing a completely uniform cipher image $\mathbf{X}$, and the library function *kstest2* provided by Matlab is used to verify whether the cipher images generated by the proposed encryption scheme are identically distributed with $\mathbf{X}$. Then, the results we get are all zero. That is to say, the histogram of the cipher image generated by the proposed encryption scheme is evenly distributed, which can block statistical attacks. Fig.9 shows the histograms of different plain images and the correspo-nding cipher images. It is shown that the encryption scheme can well cover the gray-scale distribution information of the plain image.

E. CORRELATION ANALYSIS

There is a very strong correlation between adjacent pixels in a plain image, which is an inherent property. Therefore, it requires that the image encryption algorithm to break this strong correlation. In order to test the correlation of the generated cipher image, we randomly select 100,000 pairs of adjacent pixels from multiple plain and cipher images. Then calculate the correlation coefficient between adjacent pixels by using Eq.(24). The results are shown in Tab.4.

$$r_{xy} = \frac{\sum_{i=1}^{K}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{K}(x_i - \bar{x})^2 \sum_{i=1}^{K}(y_i - \bar{y})^2}} \tag{24}$$

where, $i = 1, 2, 3, \ldots, K$. K is the number of selected pixels. $\bar{x}$,$\bar{y}$ are the expected values of x_i and y_i, respectively. Fig. 10

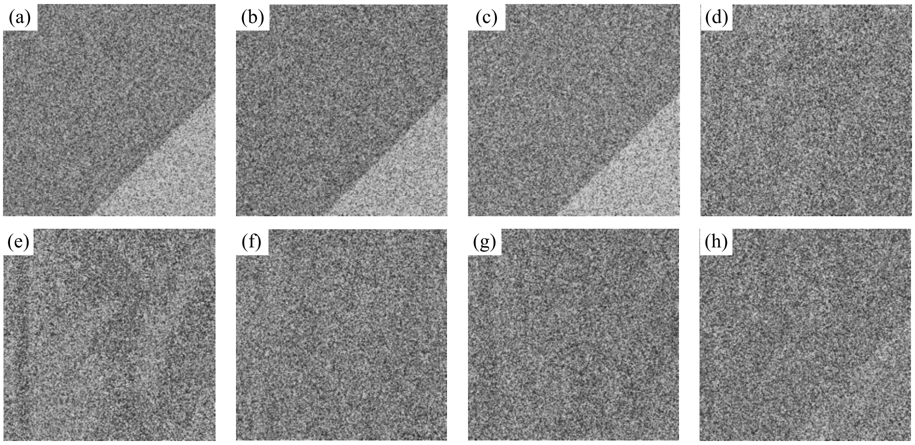


FIGURE 7. Decrypted "Lena" using incorrect keys (a) $x_0 + 10^{-14}$; (b) $y_0 + 10^{-14}$; (c) $\theta_1 + 10^{-14}$; (d) $x_1 + 10^{-14}$; (e) $y_1 + 10^{-14}$; (f) $\theta_2 + 10^{-14}$; (g) $\mu + 10^{-14}$; (h) $z_0 + 10^{-14}$.

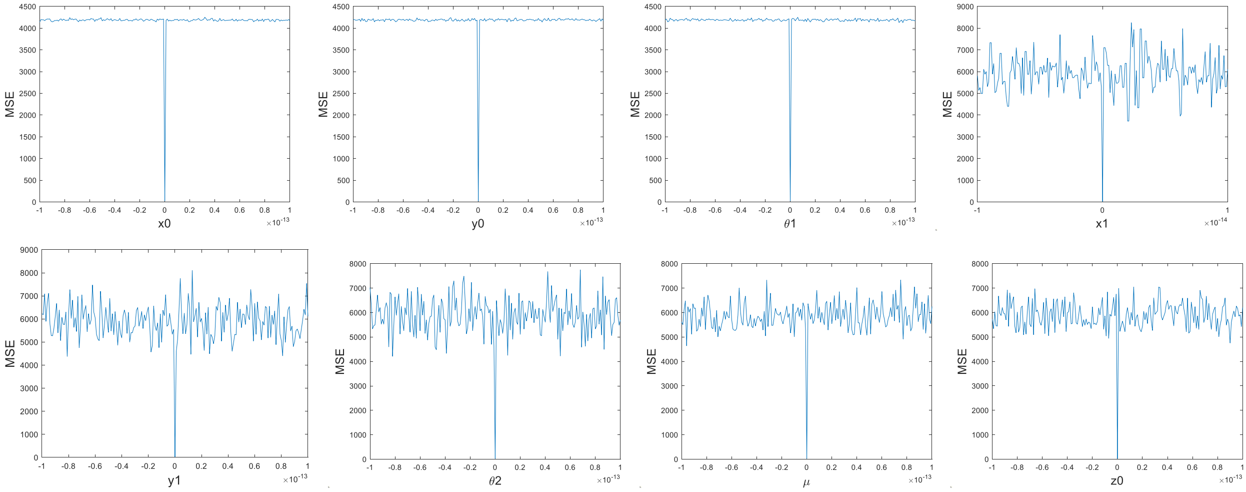


FIGURE 8. MSE curves.

TABLE 4. Correlation coefficients of two adjacent pixels of the plain and cipher.

Image	Horizontal		Vertical		Diagonal	
	Plain	Cipher	Plain	Cipher	Plain	Cipher
Lena	0.98478454	-0.0025189	0.97143965	0.00493738	0.96827090	-0.0010271
Airplane	0.96540434		0.96586019		0.93724986	
Sailboat	0.97174467		0.97445535		0.95665977	
Barbara	0.95888050	0.00131729	0.89508774	-0.0035582	0.90637378	-0.0081549
Boat	0.97140666		0.93636462		0.92631471	
Bridge	0.92836280		0.94027697		0.89858398	
Couple	0.95288329	0.00174277	0.94644740	0.00491952	0.91105603	-0.0014155
Crowd	0.96746869		0.97329348		0.94328315	
Fruits	0.97376092		0.97411959		0.95607927	

shows the correlation distribution of the Lena image and the corresponding cipher image in the horizontal direction, vertical direction and diagonal direction, respectively. It can be seen from (A1)-(A3) in Fig.10 that the adjacent pixels in the Lena image have a strong correlation and are distributed in a positive correlation. But (B1)-(B3) in Fig.10 shows that the correlation between adjacent pixels in the generated cipher image is very low, and it presents a disorderly distrib-ution. Especially compared with the cross-shaped distribution in [36], the pixel distribution of the produced

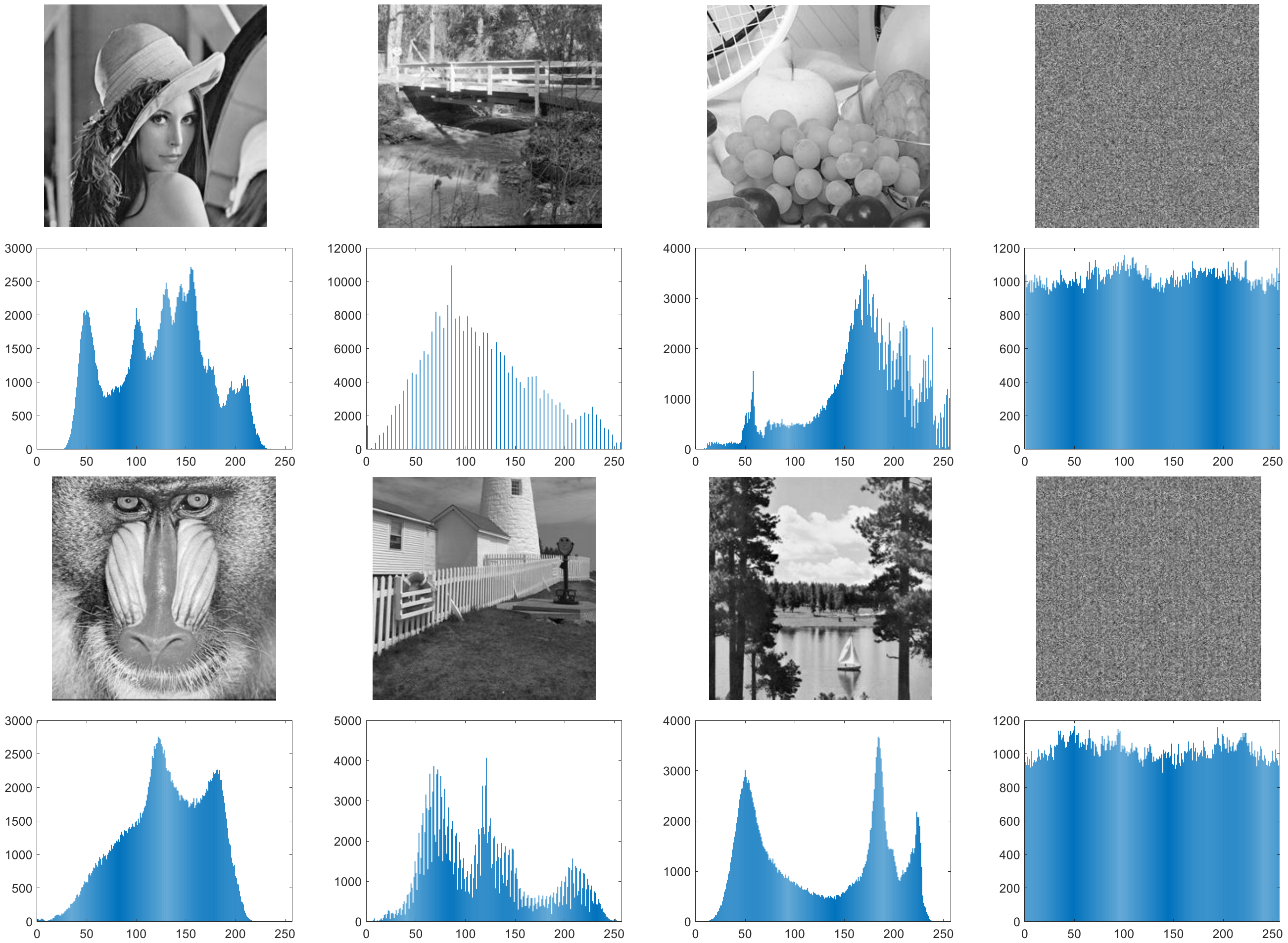


FIGURE 9. Histograms of the plain and cipher images.

TABLE 5. Correlation coefficients of the proposed method and other algorithms.

Algorithm	Horizontal	Vertical	Diagonal
Our	-0.0025189	0.00493738	-0.0010271
[33]	0.01613232	0.00782304	0.0027393
[36]	0.00430999	0.01371070	0.0022004
[39]	0.00564663	0.02554691	-0.0051870
[40]	0.00626483	0.01210758	-0.0025925
[41]	0.01367137	-0.01424386	-0.0037238

cipher image is more uniform. Tab.5 shows the comparison results of correl-ation coefficients with different encryption schemes [33], [36], [39]–[41], which shows that the proposed encryption scheme has a lower correlation between adjacent pixels than that of [33], [36], [39]–[41].

F. LOCAL INFORMATION ENTROPY ANALYSIS

Shannon information entropy reflects the overall randomness of an image. We use the local Shannon information entropy [56] to quantitatively measure this, which is calculated by Eq. (25).

$$\bar{H}_{(k,T_B)}(S) = \sum_{i=1}^{k} \frac{H(S_i)}{k} \tag{25}$$

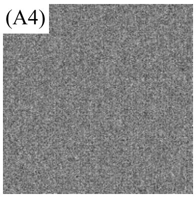
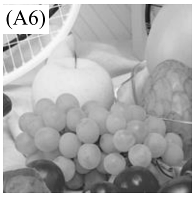
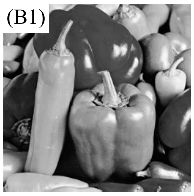
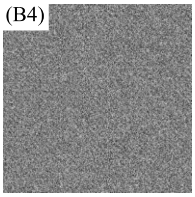
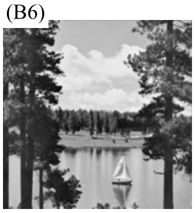
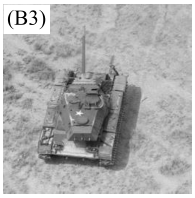
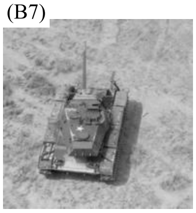
$$H(S_i) = -\sum_{i=0}^{255} p(S_{i,j}) \cdot \log_2 p(S_{i,j}) \tag{26}$$

where S_i is the randomly selected non-overlapping blocks containing T_B pixels in the cipher image. For $p(S_{i,j})$, it represents the probability of the pixel level j in the ith non-overlapping block. According to [57], we will set the confidence level α to 0.05, k to 30, and T_B to 1936. Then, the value of the local Shannon information entropy should fluctuate between [7.901901305, 7.903037329]. Tab.6 shows the local Shannon information entropy of encrypted images, which means that the distribution of pixels in the generated cipher image is random.

G. COMPRESSION PERFORMANCE ANALYSIS

In this part, the compression performance of the proposed encryption scheme is analyzed. As can be seen from Fig.5 in section III, the lossy compression algorithm is adopted in this paper and the compression rate reaches 1/3. Thus, there

TABLE 7. Experimental result of compression performance analysis.

Original image	Encrypted image	Decrypted image	PSNR (dB)	SSIM
(A1)		(A5)	34.1184	0.9945
(A2)	(A4) 	(A6) 	32.2166	0.9921
(A3)		(A7)	31.3655	0.9889
(B1) 		(B5)	32.0700	0.9939
(B2)	(B4) 	(B6) 	30.0969	0.9928
(B3) 		(B7) 	32.8731	0.9772

is some loss of pixel information in the final reconstructed image. Peak signal-to-noise ratio (PSNR) is often used as a measurement method for image reconstruction quality in the field of image compression. The calculation for the PSNR is shown in Eq.(27).

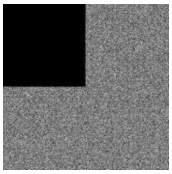
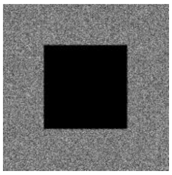
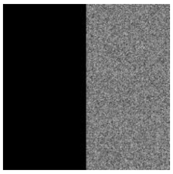
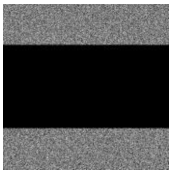
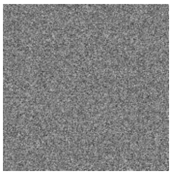
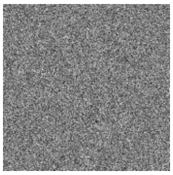
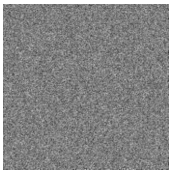
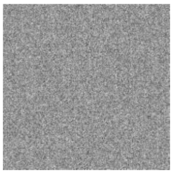
$$PSNR = 10\log\frac{255^2}{\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(\mathbf{D}_{i,j}-\mathbf{I}_{i,j})^2} \tag{27}$$

where, M and N represent the length and width of an image, respectively. $\mathbf{D}$ and $\mathbf{I}$ are expressed as plain image and its corresponding decrypted image, respectively. In addition, the structural similarity index measure (SSIM) which measures the similarity of two images from the brightness, contrast, and structure is also performed for analysis by Eq.(28)-Eq.(31).

$$\begin{cases} l(\mathbf{X},\mathbf{Y}) = \dfrac{2\mu_X\mu_Y + C1}{\mu_X^2+\mu_Y^2+C1} \\ C1 = (k1\times 255)^2 \end{cases} \tag{28}$$

$$\begin{cases} c\,(\mathbf{X},\mathbf{Y}) = \dfrac{2\sigma_X\sigma_Y + C2}{\sigma_X^2+\sigma_Y^2+C2} \\ C2 = (k2\times 255)^2 \end{cases} \tag{29}$$

TABLE 8. Experimental results of different occlusion attacks on cipher image.

Attack type & Intensity	Attacked cipher image	Decrypted image 1	PSNR (dB)	SSIM
Occlusion attack (0.25)			17.0364	0.7281
			17.0229	0.7275
Occlusion attack (0.5)			13.8874	0.4649
			13.9109	0.4693
Noise attack (0.1 SPN)			20.8376	0.8830
Noise attack (0.3 SPN)			16.0798	0.6663
Noise attack (0.01 GN)			16.2889	0.6857
Noise attack (0.1 GN)			14.6700	0.5722

$$\begin{cases} s(\mathbf{X},\mathbf{Y}) = \dfrac{\sigma_{XY} + C3}{\sigma_X \sigma_Y} \\ C3 = \dfrac{C2}{2} \end{cases} \tag{30}$$

$$SSIM(\mathbf{X},\mathbf{Y}) = l(\mathbf{X},\mathbf{Y}) \times c(\mathbf{X},\mathbf{Y}) \times s(\mathbf{X},\mathbf{Y}) \tag{31}$$

where, $k1 = 0.01$, $k2 = 0.03$, μ_X, σ_X are the expected and standard deviation of the image $\mathbf{X}$, respectively. μ_Y, σ_Y are the expected and standard deviation of the image $\mathbf{Y}$. σ_{XY} represents the covariance of the image $\mathbf{X}$ and $\mathbf{Y}$. Tab.7 shows the results of compressing performance analysis. In Tab.7 we

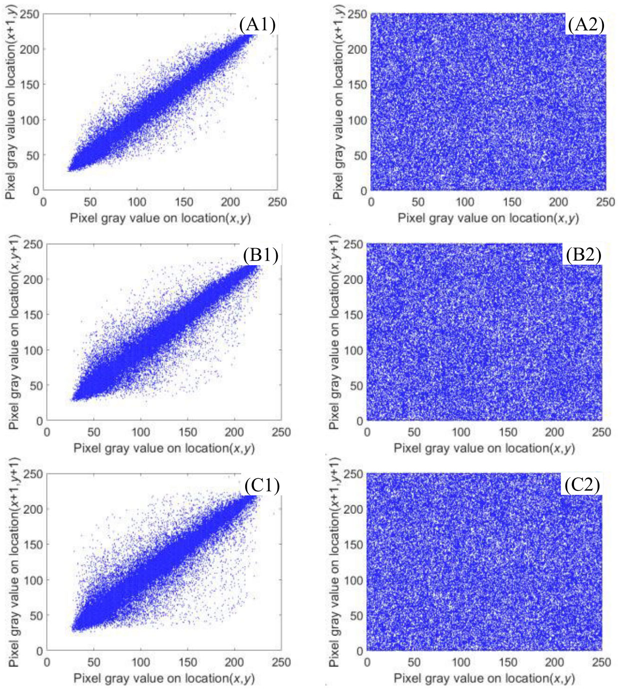


FIGURE 10. Correlation distribution of the plain image and the corresponding cipher image. (A1-A2) horizontal direction; (B1-B2) vertical direction; (C1-C2) diagonal direction.

TABLE 6. Local Shannon entropy test for cipher images.

Plain image	Local information entropy	Result
Lena Airplane Sailboat	7.90272455	Pass
Barbara Boat Bridge	7.90197353	pass
Couple Crowd Fruits	7.90280387	pass

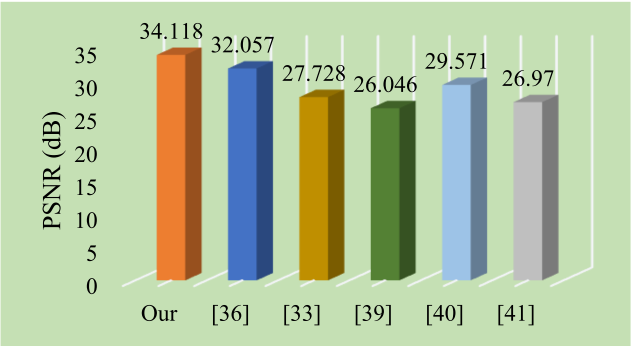


FIGURE 11. The PSNR values of the algorithms with CR = 1/3.

can see that when different images are encrypted, the PSNR of the corresponding decrypted images finally reconstructed are greater than 30 dB, and the SSIM is greater than 0.97, which indicates that the decrypted images are very close to their corresponding plain images. For comparison, PSNR of other encryption schemes with compressing ratio equaling to 1/3 are performed in Fig.11. As can be seen in Fig.11, PSNR in this paper is higher than that in [33], [36], [39]–[41].

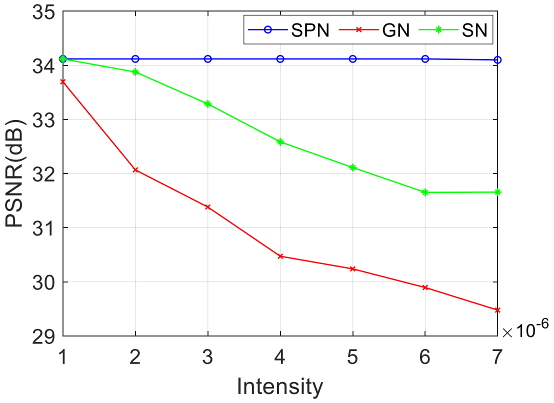


FIGURE 12. PSNR between plain and cipher image under the three noise attacks.

TABLE 9. Comparison with other algorithms under different noise.

Algorithm	Noise intensity	PSNR (dB)		
		SPN	GN	SN
Our	0.000001 0.000003 0.000005 0.000007	34.12 34.12 34.12 34.10	33.70 31.38 30.24 29.48	34.12 33.29 32.11 31.66
[36]	0.000001 0.000003 0.000005 0.000007	34.49 34.49 34.48 34.47	33.85 30.85 30.07 29.46	34.49 33.70 32.87 31.82
[33]	0.000001 0.000003 0.000005 0.000007	31.05 N/A N/A 27.93	30.10 N/A N/A 25.39	31.05 N/A N/A 30.99

TABLE 10. Experimental result of the encryption quality analysis.

Plain image	Homogeneity	Contrast	Energy
Lena Airplane Sailboat	0.3902	10.2895	0.0157
Barbara Boat Bridge	0.3913	10.5408	0.0157
Couple Crowd Fruits	0.3853	11.1523	0.0160

H. ROBUSTNESS ANALYSIS OF NOISE AND DATA LOSS

It will inevitably be affected by noise when the cipher image is transmitted through the public network, resulting in the loss of some pixel values. In this section, we artificially add interferences to cipher images to test the robustness of the encryption scheme. Tab.8 displays the experimental results of different intensity noise attacks and occlusion attacks on the

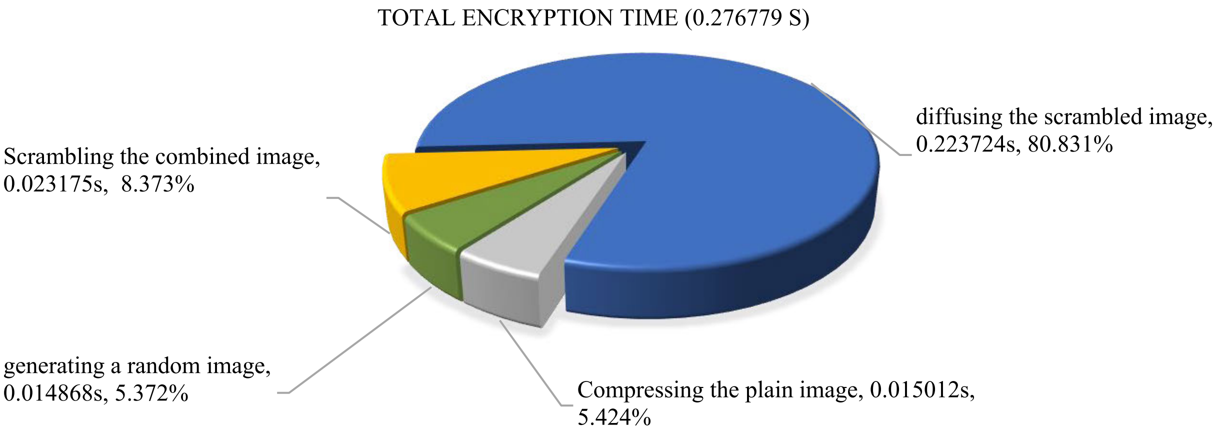


FIGURE 13. Total encryption time and time consumption percentage of each part.

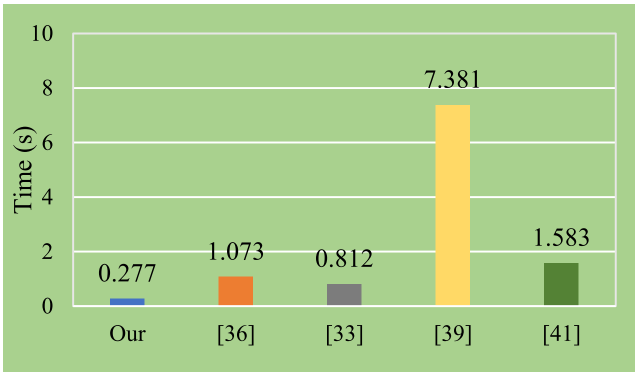


FIGURE 14. Time complexity of different methods.

cipher images. Tab.9 displays the comparative experimental results of the ability of three encryption schemes to resist noise attacks. From the result, it shows that the proposed encryption scheme in this paper is equivalent to that in [36], and is superior to that in [33]. Fig.12 shows the effect of three different kinds of noise attacks on the reconstructed and decrypted images. As can be seen from Tab.8 and Fig.12, the encryption algorithm not only has a high compression rate, but also has well robustness.

I. ENCRYPTION QUALITY ANALYSIS

In this subsection, we analyze the image encryption quality according to the Gray-level Co-occurrence Matrix (GLCM) [58], including its homogeneity, contrast and energy test. Homogeneity determines how closely the elements in the GLCM are distributed to its diagonal, defined in Eq.(32). And contrast, defined in Eq.(33), is used to measure the intensity of the difference between two adjacent pixels. In addition, energy reflects the evenness of GLCM distribution, which is defined in Eq.(34).

$$Hom = \sum_{a,b} \frac{p(a,b)}{1+|a-b|} \tag{32}$$

TABLE 11. Pseudo-code of the coded lock permutation.

```
Input: The plain image IMG and the secret keys Keys.
Output: A permutated matrix IMG_P.
[M, N] ⟵ size of (IMG)
[u, v] ⟵ LSCM (Keys, M/2, N/2)
w ⟵ u – v,  z ⟵ u + v,
Tu ⟵ sort(u), Tv ⟵ sort(v), Tw ⟵ sort(w), Tz ⟵ sort(z)
P ⟵ IMG(:)
P is divided into four non-overlapping blocks, denoted as P1, P2, P3, P4.
For i ⟵ 1 to M×N/4 do
    P_tmp(4i-3) ⟵ P1(Tu(i))
    P_tmp(4i-2) ⟵ P2(Tv(i))
    P_tmp(4i-1) ⟵ P3(Tw(i))
    P_tmp(4i) ⟵ P4(Tz(i))
End For
IMG_P ⟵ reshape(P_tmp, M, N)
```

Notes: The LSCM (~) in Tab.11 is a function that is used to generate two chaotic sequences through 2D-LSCM.

$$Con = \sum_{a,b} p(a,b)\,|a-b|^2 \tag{33}$$

$$Ene = \sum_{a,b} p(a,b)^2 \tag{34}$$

where $p(a, b)$ represent the gray-level co-occurrence matrix, and N is the total number of rows and columns. The experimental result of the encryption quality analysis is shown in Tab.10.

J. TIME COMPLEXITY ANALYSIS

The time complexity of the proposed encryption scheme is analyzed here. Assume the size of the three different plain images are all $N \times N$. The time complexity of the encryption scheme mainly depends on the three stages of image processing. Firstly, in the compression process, three plain images are compressed simultaneously, and the required time complexity is $\Theta(N^2/4)$. Then, the four sub-block images are simultaneously scrambled through the generated chaotic sequences

TABLE 12. **Pseudo-code of the S-box.**

```
Input: The secret keys: $d$, $\mu$, $z_0$ and $N_0$.
Output: A S-box: S.
T1 ⟵ [1 : 256]
T ⟵ mod($d$×T1(:), 256)
X ⟵ STS($\mu$,$z_0$,$N_0$)
Tx ⟵ sort(X)
For $i$ ⟵ 1 to 256 do
    S_tmp($i$) ⟵ T(Tx($i$))
End For
S ⟵ reshape(S_tmp, 16, 16)
```

Notes: The STS(~) in Tab.12 is a function that is used to generate a chaotic sequence through 1D-STS.

in the second process. The time complexity of this process is also $\Theta(N^2/4 + 3N/2)$. Next, each pixel of the combined image needs to be diffused, so its time complexity is $\Theta(N^2)$. Finally, the total time complexity of the proposed encryption scheme is $\Theta(3N(N + 1)/2)$.

Fig.13 shows the time distribution required for the proposed scheme to encrypt three plain text images with the size of 512 × 512. Fig.14 shows that of different schemes [33], [36], [39], [41] to encrypt a plain image with the size of 512 × 512. It can be seen from Fig.14 that the proposed encryption scheme takes much less time than that of other encryption schemes [33], [36], [39], [41].

VI. CONCLUSION

In this paper, a robust triple image encryption scheme based on chaos theory, S-box and image compressing is proposed, which consists of combination, scrambling and diffusion. In the combination process, three plain images are compressed into a quarter that of the original size, which makes the proposed scheme can transmit three plain images once a time. In addition, a stochastic matrix combined with the three compressed images makes the cipher image to be dynamic, which means the cipher images are different even when they are the output of the proposed scheme by encrypting the identical plain images with the same secret keys. In the scrambling process, a coded lock scrambling algorithm is proposed by randomly strike pixels in the combined image, which is used to reduce the time complexity. Next, the scrambled images are grouped and diffused by a S-box generated by STS chaotic system and a chaotic sequence generated by 2D-LSCM. Finally, the simulation results show that the encryption scheme has well compression perform-ance and can resist common attacks, noise attacks and occlusion attacks.

In the future, we will consider embedding the encrypted image into the host image adaptively in frequency domain, so as to achieve the double security of plain text and vision.

APPENDIX

See Tables. 11 and 12.

REFERENCES

[1] X. Li, Z. Xie, J. Wu, and T. Li, "Image encryption based on dynamic filtering and bit cuboid operations," *Complexity*, vol. 2019, pp. 1–16, Feb. 2019.

[2] S. Zhu and C. Zhu, "A new image compression-encryption scheme based on compressive sensing and cyclic shift," *Multimedia Tools Appl.*, vol. 78, no. 15, pp. 20855–20875, Aug. 2019.

[3] 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.

[4] Y.-J. Sun, H. Zhang, X.-Y. Wang, X.-Q. Wang, and P.-F. Yan, "2D non-adjacent coupled map lattice with q and its applications in image encryption," *Appl. Math. Comput.*, vol. 373, May 2020, Art. no. 125039.

[5] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation Chaos Appl. Sci. Eng.*, vol. 8, no. 6, pp. 1259–1284, 1998.

[6] G. Ye, C. Pan, X. Huang, Z. Zhao, and J. He, "A chaotic image encryption algorithm based on information entropy," *Int. J. Bifurcation Chaos*, vol. 28, no. 1, Jan. 2018, Art. no. 1850010.

[7] 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.

[8] 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.

[9] 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.

[10] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci.*, vol. 480, pp. 403–419, Apr. 2019.

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

[12] 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.

[13] L. Liu, Y. Lei, and D. Wang, "A fast chaotic image encryption scheme with simultaneous permutation-diffusion operation," *IEEE Access*, vol. 8, pp. 27361–27374, 2020.

[14] Y. Luo, L. Cao, S. Qiu, H. Lin, J. Harkin, and J. Liu, "A chaotic map-control-based and the plain image-related cryptosystem," *Nonlinear Dyn.*, vol. 83, no. 4, pp. 2293–2310, Mar. 2016.

[15] X.-Y. Wang and S.-X. Gu, "New chaotic encryption algorithm based on chaotic sequence and plain text," *IET Inf. Secur.*, vol. 8, no. 3, pp. 213–216, May 2014.

[16] G. Ye and X. Huang, "An efficient symmetric image encryption algorithm based on an intertwining logistic map," *Neurocomputing*, vol. 251, pp. 45–53, Aug. 2017.

[17] 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.

[18] X. Wang, L. Feng, R. Li, and F. Zhang, "A fast image encryption algorithm based on non-adjacent dynamically coupled map lattice model," *Nonlinear Dyn.*, vol. 95, no. 4, pp. 2797–2824, Mar. 2019.

[19] L. Liu, D. Jiang, T. An, and Y. Guan, "A plaintext-related dynamical image encryption algorithm based on permutation-combination-diffusion architecture," *IEEE Access*, vol. 8, pp. 62785–62799, 2020.

[20] C. Chen, K. Sun, and Q. Xu, "A color image encryption algorithm based on 2D-CIMM chaotic map," *China Commun.*, vol. 17, no. 5, pp. 12–20, May 2020.

[21] M. Kaur, D. Singh, K. Sun, and U. Rawat, "Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5D chaotic map," *Future Gener. Comput. Syst.*, vol. 107, pp. 333–350, Jun. 2020.

[22] F. Yang, J. Mou, K. Sun, and R. Chu, "Lossless image compression-encryption algorithm based on BP neural network and chaotic system," *Multimedia Tools Appl.*, vol. 79, nos. 27–28, pp. 19963–19992, Jul. 2020.

[23] Q. Xu, K. Sun, S. He, and C. Zhu, "An effective image encryption algorithm based on compressive sensing and 2D-SLIM," *Opt. Lasers Eng.*, vol. 134, Nov. 2020, Art. no. 106178.

[24] K. A. K. Patro, A. Soni, P. K. Netam, and B. Acharya, "Multiple grayscale image encryption using cross-coupled chaotic maps," *J. Inf. Secur. Appl.*, vol. 52, Jun. 2020, Art. no. 102470.

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

[26] K. A. K. Patro and B. Acharya, "A novel multi-dimensional multiple image encryption technique," *Multimedia Tools Appl.*, vol. 79, nos. 19–20, pp. 12959–12994, May 2020.

[27] R. Enayatifar, F. G. Guimarães, and P. Siarry, "Index-based permutation-diffusion in multiple-image encryption using DNA sequence," *Opt. Lasers Eng.*, vol. 115, pp. 131–140, Apr. 2019.

[28] K. A. K. Patro and B. Acharya, "Secure multi–level permutation operation based multiple colour image encryption," *J. Inf. Secur. Appl.*, vol. 40, pp. 111–133, Jun. 2018.

[29] L. Zhang and X. Zhang, "Multiple-image encryption algorithm based on bit planes and chaos," *Multimedia Tools Appl.*, vol. 79, nos. 29–30, pp. 20753–20771, Aug. 2020, doi: 10.1007/s11042-020-08835-4.

[30] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons Fractals*, vol. 21, no. 3, pp. 749–761, Jul. 2004.

[31] N. Zhou, A. Zhang, J. Wu, D. Pei, and Y. Yang, "Novel hybrid image compression–encryption algorithm based on compressive sensing," *Optik*, vol. 125, no. 18, pp. 5075–5080, Sep. 2014.

[32] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, "Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing," *Opt. Laser Technol.*, vol. 82, pp. 121–133, Aug. 2016.

[33] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, "An image encryption algorithm based on chaotic system and compressive sensing," *Signal Process.*, vol. 148, pp. 124–144, Jul. 2018.

[34] Q. Xu, K. Sun, C. Cao, and C. Zhu, "A fast image encryption algorithm based on compressive sensing and hyperchaotic map," *Opt. Lasers Eng.*, vol. 121, pp. 203–214, Oct. 2019.

[35] S. Yao, L. Chen, and Y. Zhong, "An encryption system for color image based on compressive sensing," *Opt. Laser Technol.*, vol. 120, Dec. 2019, Art. no. 105703.

[36] Y. Luo, J. Lin, J. Liu, D. Wei, L. Cao, R. Zhou, Y. Cao, and X. Ding, "A robust image encryption algorithm based on Chua's circuit and compressive sensing," *Signal Process.*, vol. 161, pp. 227–247, Aug. 2019.

[37] K. Zhou, J. Fan, H. Fan, and M. Li, "Secure image encryption scheme using double random-phase encoding and compressed sensing," *Opt. Laser Technol.*, vol. 121, Jan. 2020, Art. no. 105769.

[38] X. Chai, Z. Gan, Y. Chen, and Y. Zhang, "A visually secure image encryption scheme based on compressive sensing," *Signal Process.*, vol. 134, pp. 35–51, May 2017.

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

[40] J. Chen, Y. Zhang, L. Qi, C. Fu, and L. Xu, "Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression," *Opt. Laser Technol.*, vol. 99, pp. 238–248, Feb. 2018.

[41] H. Huang, X. He, Y. Xiang, W. Wen, and Y. Zhang, "A compression-diffusion-permutation strategy for securing image," *Signal Process.*, vol. 150, pp. 183–190, Sep. 2018.

[42] Y. Song, Z. Zhu, W. Zhang, L. Guo, X. Yang, and H. Yu, "Joint image compression–encryption scheme using entropy coding and compressive sensing," *Nonlinear Dyn.*, vol. 95, no. 3, pp. 2235–2261, Feb. 2019.

[43] K. A. K. Patro, B. Acharya, and V. Nath, "Various dimensional colour image encryption based on non-overlapping block-level diffusion operation," *Microsyst. Technol.*, vol. 26, no. 5, pp. 1437–1448, May 2020.

[44] M. Li, D. Lu, Y. Xiang, Y. Zhang, and H. Ren, "Cryptanalysis and improvement in a chaotic image cipher using two-round permutation and diffusion," *Nonlinear Dyn.*, vol. 96, no. 1, pp. 31–47, Apr. 2019.

[45] R. Ponuma and R. Amutha, "Compressive sensing based image compression-encryption using novel 1D-chaotic map," *Multimedia Tools Appl.*, vol. 77, no. 15, pp. 19209–19234, Aug. 2018.

[46] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D Logistic-Sine-coupling map for image encryption," *Signal Process.*, vol. 149, pp. 148–161, Aug. 2018.

[47] S. Zhu, G. Wang, and C. Zhu, "A secure and fast image encryption scheme based on double chaotic S-boxes," *Entropy*, vol. 21, no. 8, p. 790, Aug. 2019.

[48] H. Hou and H. Andrews, "Cubic splines for image interpolation and digital filtering," *IEEE Trans. Acoust., Speech, Signal Process.*, vol. 26, no. 6, pp. 508–517, Dec. 1978.

[49] F. Aràndiga, "A nonlinear algorithm for monotone piecewise bicubic interpolation," *Appl. Math. Comput.*, vol. 272, pp. 100–113, Jan. 2016.

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

[51] X. Wang and D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 18, no. 11, pp. 3075–3085, Nov. 2013.

[52] X. Wang, S. Lin, and Y. Li, "A chaotic image encryption scheme based on cat map and MMT permutation," *Modern Phys. Lett. B*, vol. 33, no. 27, Sep. 2019, Art. no. 1950326.

[53] X. Wu, K. Wang, X. Wang, and H. Kan, "Lossless chaotic color image cryptosystem based on DNA encryption and entropy," *Nonlinear Dyn.*, vol. 90, no. 2, pp. 855–875, Oct. 2017.

[54] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, Aug. 2006.

[55] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the LSS chaotic map and single S-Box," *IEEE Access*, vol. 8, pp. 25664–25678, 2020.

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

[57] X. Wang, C. Liu, D. Xu, and C. Liu, "Image encryption scheme using chaos and simulated annealing algorithm," *Nonlinear Dyn.*, vol. 84, no. 3, pp. 1417–1429, May 2016.

[58] S. Zhu and C. Zhu, "Plaintext-related image encryption algorithm based on block structure and five-dimensional chaotic map," *IEEE Access*, vol. 7, pp. 147106–147118, 2019.

LIU LIDONG 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 been involved with more than ten projects supported by the National Natural Science Foundation of China and the Natural Science Foundation of Shanxi province. He has authored or coauthored more than 40 papers in signal processing, control theory, and computational nonlinear journals and conferences. His current research interests include image encryption, secure communication, and nonlinear control systems.

DONGHUA JIANG received the B.S. degree in electronic information engineering from the College of Physical and Electrical Engineering, Harbin Normal University, China, in 2019. He is currently pursuing the degree with the College of Information Engineering, Chang'an University, China. His current research interests include image encryption, cryptanalysis, and image hiding technology.

XINGYUAN WANG received the Ph.D. degree in computer software and theory from Northeastern University, China, in 1999. From 1999 to 2001, he was a Postdoctoral Researcher with Northeastern University. He is currently a Professor of information science and technology with Dalian Maritime University, China. He has published three books and more than 400 scientific articles in refereed journals and proceedings. His research interests include nonlinear dynamics and control, image processing, chaos cryptography, systems biology, and complex networks.

LINLIN ZHANG received the B.S. degree in communication engineering from the College of Information Science and Technology, Chongqing Jiaotong University, China, in 2018. 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.

XIANWEI RONG (Member, IEEE) received the B.S. degree in physics and the M.S. degree in signal and information processing from Harbin Normal University, China, in 1996 and 2010, respectively. His current research interests include image processing and deep learning.