IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 23, 2021, accepted March 9, 2021, date of publication March 10, 2021, date of current version March 19, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3065453

A Novel Double-Image Encryption Algorithm Based on Rossler Hyperchaotic System and Compressive Sensing

WEI HUANG[1], **DONGHUA JIANG**[1], **YISHENG AN**[1], **LIDONG LIU**[1], **AND XINGYUAN WANG**[2]

[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

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 Key Research Program under Grant 2019GY-070, in part by the Shaanxi Province Science and Technology Program under Grant 2020JM-220 and Grant 2020JQ-351, and in part by the Fundamental Research Funds for the Central Universities of China under Grant 300102240205.

ABSTRACT In this paper, a novel double-image compression-encryption algorithm is proposed by combining Rossler hyperchaos and compressive sensing. In the proposed scheme, the sparse matrixes obtained by performing two-dimensional discrete wavelet transform on two plain images are first scrambled and compressed by index confusion and compressive sensing. Next, the compressed matrixes are linearly quantized, and then variable step length Josephus confusion and bitwise exclusive-OR operation are performed on them. The final noise-like cipher image is generated by hiding half of the encrypted image into the alpha channel of the other half of encrypted image. In order to realize ''One cipher image corresponds to one key'', a novel key generation mechanism is designed. Finally, the simulation analyses indicate that the proposed double-image encryption scheme has high transmission efficiency. Meanwhile, the average local information entropy of the cipher image is about 0.902 and the decryption quality is as high as 30 dB.

INDEX TERMS Double-image encryption, Rossler system, compressive sensing, Josephus confusion.

I. INTRODUCTION

With the advent of the era ''Big Data'', the amount of multimedia information in the network also grows exponentially. As one of the mainstream forms of information transmission, digital images are widely used in various fields. Meanwhile, with continually increasing security requirements for storing and transmitting digital image, how to efficiently and securely protect the information carried by digital image has attracted more and more scholars' attention.

Because of its noise-like, long-term unpredictability and sensitivity to initial values [1]–[4], chaotic system is a good choice to design the image cryptosystem. Such as Ref [5], Teng *et al.* used a one-dimensional segmented chaotic map (Skew tent map) to encrypt the color plain images on the bit plane. However, the low dimensional chaotic system is easy to be attacked by signal estimation algorithm [6] because of its simple chaotic trajectory. At the same time, it has a small key space, which makes it vulnerable to violent attacks. Subsequently, many improved chaotic systems have been proposed [7]–[11]. For example, in Ref [12], Hua *et al.* proposed an exponential chaotic model framework to generate robust and secure chaotic system. Moreover, Wang *et al.* [13] also proposed an improved cross coupled map lattice with wider chaotic range and higher information entropy, and applied it to the field of image encryption. Additionally, in order to improve security, some image encryption schemes combining chaotic system with other technologies [14]–[17] are proposed. Brahim *et al.* [18] used the measurement matrix generated by Lorentz chaotic system to simultaneously encrypt and comp-rests the plain image. And in Ref [19], a four-wing hyper-chaotic system is used to dynamically generate DNA sequence to diffuse the image. However, the above-mentioned image encryption schemes can only encrypt one image at a time, which cannot meet the requirements of efficient information transmission.

Simultaneously encrypting multiple images is an inevitable trend. At present, many chaotic multi-image encryption algorithms have been proposed [20]–[24]. In Ref [25],

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

Liu *et al.* proposed a dynamic triple-image compression-encryption algorithm based on chaos, S-box and interpolation technology, which can realize "Multiple cipher image corresponds to one key". Moreover, a multi-color image encryption algorithm through multi-level scrambling operation was introduced by Patro *et al.* [26]. In addition, in his scheme, the hash value of the plain image is associated with the cross-coupled PWLCM system to improve the high security of the encryption algorithm-hm. Although Patro's scheme improves encryption efficiency to some extent, it does not consider compressing multi-plain images to reduce storage space and transmission costs. And there are similar deficiencies in the Ref [27]–[28].

In recent years, the emergence of compressive sensing (CS) technology has made it possible to conduct non-uniform sampling, compression and encryption on the plain image simultaneously. Besides, the CS-based compression-encryption framework has been studied in Ref [29]–[32]. For example, Huang *et al.* [29] introduced a compression-diffusion-scrambling strategy and applied it to image security. In his scheme, only a few keys are needed to generate the measurement matrix, thus reducing the space for storing keys. Moreover, in Ref [30], Jiang *et al.* proposed a novel dual-image encryption scheme conjugating compressive sensing, double random phase encoding and Josephus scrambling to improve the information transmission efficiency. Huo *et al.* [31] also presented an optical multi-image encryption scheme via CS. In these schemes, chaotic sequence is used to generate the measure-mint matrix to reduce transmission costs, compression and encryption performance are also improved. However, the encryption operations are not related to the natural image. The same key stream is applied to different plain images. There-fore, it is easy to be broken by the chosen-plaintext attacks.

In this paper, a double-image compression-encryption algorithm based on Rossler hyperchaos and compressive sensing technology is proposed. Different from the existing multi-image encryption algorithms, in our scheme, half of encrypted image is hidden into the alpha channel of remaining encrypted image to improve the security level of the proposed encryption scheme. Additionally, in order to resist chosen-plaintext attacks, a novel key generation mechanism is designed to realize "One cipher image corresponds to one key".

The remaining sections of this paper are organized as follows. The second section introduces the basic knowledge related to the proposed algorithm. And the proposed encrypt-ton scheme and the corresponding decryption scheme will be described in detail in the third section. Meanwhile, the fourth section gives the simulation results and performance analyses. The last section briefly summarizes our work.

II. FUNDAMENTAL KNOWLEDGE

A. CHAOTIC SYSTEMS

To save storage space, the measurement matrix is generated by the improved Sine-exponent-Logistic map. Meanwhile, the Rolsser hyperchaotic system will be used to generate the scrambling and diffusion matrix. The detailed introduction of these two chaotic systems is shown below.

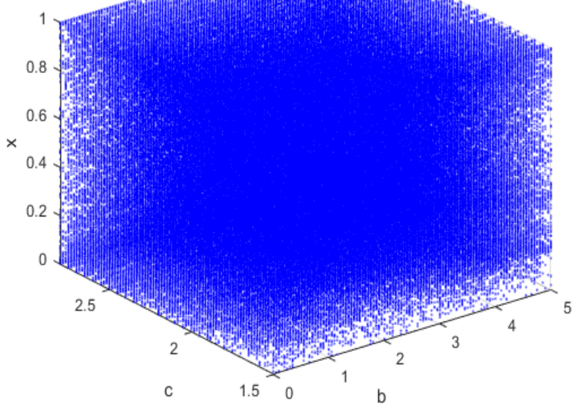


FIGURE 1. The bifurcation diagram for ISEL map (a = 1).

1) THE IMPROVED SINE-EXPONENT-LOGISTIC MAP

The improved Sine-exponent-Logistic (ISEL) map is obtained by combining the Sine map and the Logistic map through exponential operation. Additionally, the corresponding mathematical definition [33] is shown in Eq.(1).

$$v_{i+1} = (\sin(\pi v_i))^{a\ln\,(4bv_i(1-v_i)+c)} \tag{1}$$

When $a \in [0, 1]$, $b \in [0, 5]$ and $c \in [1.5, 2.8]$, this improved map is in chaotic state. The corresponding bifurcation diagram of the ISEL map is ploted in Fig. 1. It can be seen from the figure that the output values of the ISEL map is almost uniformly distributed over the whole parameter range, showing complex chaotic performance.

2) ROSSLER HYPERCHAOTIC SYSTEM

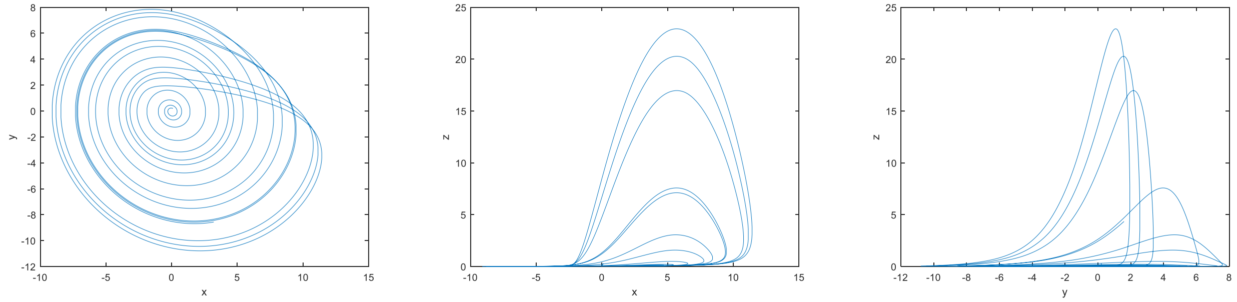
The Rossler hyperchaos is one of the most famous chaotic systems, which was proposed by Otto in 1976 [34]. The differential equation is shown in Eq.(2).

$$\begin{cases} \dfrac{dx}{dt} = -(y+z) \\ \dfrac{dy}{dt} = x+\alpha y \\ \dfrac{dz}{dt} = \beta + r(x-\gamma) \end{cases} \tag{2}$$

When $\alpha = \beta = 0.2$ and $\gamma = 5.7$, the attractors of this hyperchaos generated by the Runge-Kutta method are plotted in Fig. 2. And its initial state variable is set to $[0.1, 0.2, 0.3]^{\mathrm{T}}$.

B. COMPRESSIVE SENSING

Compressive sensing refers to randomly sampling the sparse signal under condition of far below the Nyquist sampling rate. And using the optimal solution algorithm to recover the



(a) (b) (c)

FIGURE 2. The attractor diagram of Rossler hyperchaotic system. (a) the x-y plane; (b) the x-z plane; (c) the y-z plane.

original signal with high probability [35]–[36]. Specifically, for the real signal $\boldsymbol{x} \in \mathbb{R}^N$, if it is K-sparse under a certain $N \times N$ orthogonal basis $\boldsymbol{\Psi}$, that is.

$$\mathbf{x} = \boldsymbol{\Psi}\mathbf{s} \tag{3}$$

In Eq.(3), there are K ($K \ll N$) non-zero elements in s. A one-dimensional compressed signal $\mathbf{y} \in \mathbb{R}^M$ can be obtained by using the measurement matrix Φ with size of $M \times N$ ($M < N$) to observe the signal x. This process can be represented by Eq.(4).

$$\mathbf{y} = \boldsymbol{\Phi}\mathbf{x} = \boldsymbol{\Phi}\boldsymbol{\Psi}\mathbf{s} = \boldsymbol{\Theta}\mathbf{s} \tag{4}$$

where the matrix $\boldsymbol{\Theta} = \boldsymbol{\Phi}\boldsymbol{\Psi}$ is called the perception matrix. Since the Eq.(4) belongs to an underdetermined equation system, other regular constraint condition need to be added to recover the original signal **x**, namely RIP condition [37]. It says that the original signal **x** can be reconstructed with high probability, when the measurement matrix $\boldsymbol{\Phi}$ and the orthogonal basis matrix $\boldsymbol{\Psi}$ are not correlated. Moreover, reconstructing the sparse signal**x** can be expressed as solving the l_1 norm problem, that is.

$$\min \|s\|_1 \quad s.t.\mathbf{y} = \boldsymbol{\Phi}\mathbf{x} \tag{5}$$

where $\|\cdot\|_1$ represents the l_1 norm. Additionally, the orthogonal matching pursuit (OMP) and the smoothed l_0 norm (SL$_0$) are two commonly used algorithms to reconstruct the original signal **x**.

C. VARIABLE STEP LENGTH JOSEPHUS CONFUSION

Variable step length Josephus confusion originates from the Josephus ring problem [38]–[39] which says that there are n people (denoted as 1, 2, …, n) sitting around a large round table. Later, the s-th ($s < n$) person starts counting from one. And the person counting to g (the count length) will be automatically shifted out. Then his next person starts counting from one again. Similarly, the person counting to g will be automatically shifted out. And so on until the people at the round table are all shifted out.

Fig. 3 demonstrates an example of the variable step length Josephus confusion. The original sequence is [26], [17], [58], [24], [70], [84]. Additionally, the step length sequence is set to [4], [7], [6], [8], [3]. First, 17 is selected as the initial position to start counting clockwise. Then the element counting to 4 that is 70 is automatically shifted out. Its next element starts counting again. And so on until the element at the ring are all shifted out. The final scrambled sequence is [70], [26], [58], [84], [17], [24].

III. ALGORITHM DESCRIPTIONS

A. THE ENCRYPTION PROCESS

The proposed encryption procedure is illustrated in Fig. 4. As can be seen from this figure, there are three stages in the encryption process. In the first stage, the internal keys are scrambled with the hash value of two plain images to generate the initial states of chaotic systems. The second stage is to utilize the measurement matrix to compress the two plain images after sparse and threshold processing. In the last stage, the quantized matrix is encrypted by variable step length Josephus confusion and bitwise exclusive-OR operation to generate the noise-like cipher image. Addition-ally, in order to improve security, half of the cipher image is hidden in the alpha channel of the other half of cipher image. Assuming that the two plain images (**P1**, **P2**) are all sized of $M \times N$. The detailed double-image encryption steps are as follows.

1) GENERATING THE INITIAL KEYS

In order to realize ‘‘One cipher image corresponds to one key’’, a novel key generation mechanism is proposed in this paper. That is, the internal keys are scrambled though the scrambling sequence generated by the hash value of plain image to obtain the initial states of the chaotic systems. The generation steps are shown below.

Step 1. Perform the hash operate on two plain images, and two hash values sized of 256-bit are obtained, denoted as *KS1* and *KS2*.

Step 2. Bitwise xor operation is carried out on *KS1* and *KS2* to obtain *KS3*. Then, *KS3* is partitioned to generate *KE1* sized of 8-byte and *KE2* sized of 24-byte.

Step 3. Respectively, *KE1* and *KE2* are divided into several single bytes and sorted to obtain two index sequences **IK1** and **IK2**. This process can be represented by Eq.(6)-Eq.(7), where $KE1^i$ stands for the

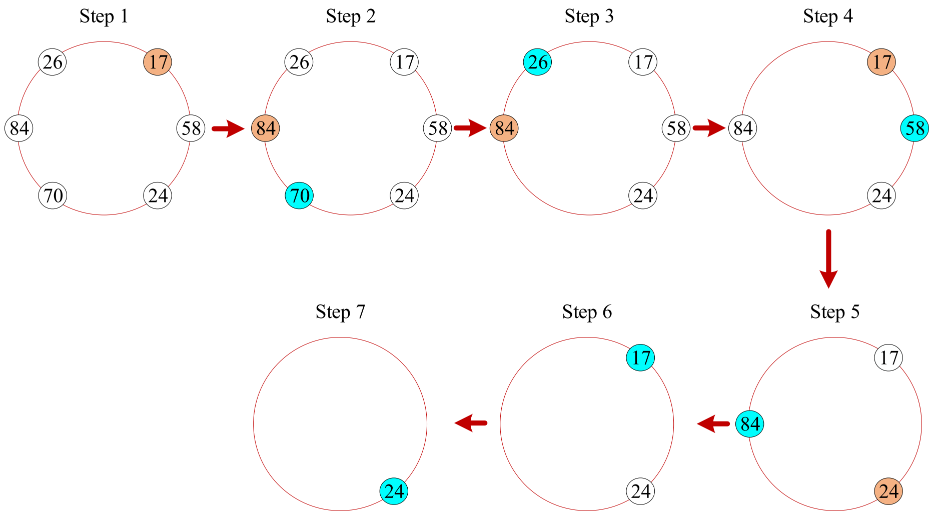


FIGURE 3. An example of variable step length Josephus confusion.

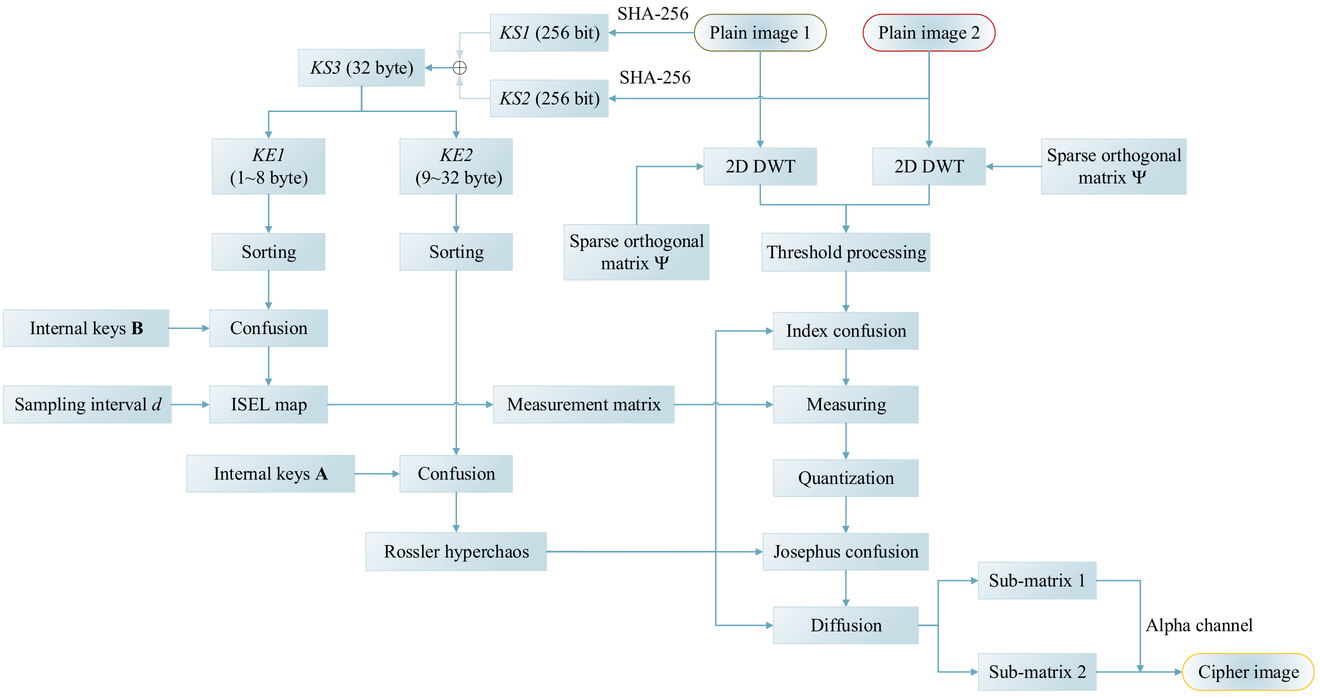


FIGURE 4. The proposed encryption procedure.

i-th byte of *KE1*.

$$[\sim, \mathbf{IK1}] = \mathrm{sort}(KE1^{i}) \quad i = 1, 2, 3, \ldots, 8 \tag{6}$$

$$[\sim, \mathbf{IK2}] = \mathrm{sort}(KE2^{j}) \quad j = 1, 2, 3, \ldots, 24 \tag{7}$$

Step 4. **A**’ and **B**’ are generated by scrambling two groups of internal keys **A** and **B** though the index sequences, according to Eq.(8)-Eq.(9).

$$\mathbf{A}'_i = \mathbf{A}_{\mathbf{IK2}^i} \tag{8}$$

$$\mathbf{B}'_i = \mathbf{B}_{\mathbf{IK1}^i} \tag{9}$$

Step 5. By dividing **A**’ into three parts and multiplied by 10^{-8}, the initial states x_0, y_0 and z_0 of the Rossler hyperchaotic system can be obtained. In addition, **B**’ is multiplied by 10^{-8} to generate the initial state v_0 of the ISEL map.

2) COMPRESSING THE PLAIN IMAGES

In the compression process, the ISEL map is utilized to generate the measurement matric to reduce storage space. Additionally, it is worth mentioning that compared with hyperchaotic systems with high complexity and implementation cost, the one-dimensional discrete chaotic maps are more suitable for generating the measurement matrix. The corresponding steps are as follows.

Step 1. The ISEL map is iterated $500 + Mnd$ times with the initial value v_0. Then, discarding the former 500 values, the chaotic sequence $\mathbf{V} \in \mathbb{R}^{Mnd}$ is obtained, where d is the sampling distance. In addition, $n = CR \times N$ and CR represents the preset compression rate.

Step 2. According to Eq.(10), the chaotic sequence $\mathbf{V}$ is processed to obtain $\mathbf{V}$'.

$$\mathbf{V}'_i = 1 - 2\mathbf{V}_{1+id}, \quad i = 0, 1, 2, \ldots, Mn - 1 \quad (10)$$

Step 3. The measurement matrix can be obtained by converting the sequence $\mathbf{V}$' into the matrix sized of $n \times M$ and performing normalization processing. This process can be represented by Eq.(11).

$$\mathbf{\Phi} = \sqrt{\frac{2}{M}} \begin{bmatrix} V'_{11} & V'_{12} & \cdots & V'_{1M} \\ V'_{21} & V'_{22} & \cdots & V'_{2M} \\ \vdots & \vdots & \vdots & \vdots \\ V'_{n1} & V'_{n2} & \cdots & V'_{nM} \end{bmatrix} \quad (11)$$

Step 4. Construct a sparse orthogonal matrix $\mathbf{\Psi}$ though DB3 wavelet. Then the two plain images are sparse as follows:

$$\begin{cases} \mathbf{P3} = \mathbf{\Psi} \times \boldsymbol{P1} \times \mathbf{\Psi}^{\mathrm{T}} \\ \mathbf{P4} = \mathbf{\Psi} \times \boldsymbol{P2} \times \mathbf{\Psi}^{\mathrm{T}} \end{cases} \quad (12)$$

where the symbol T represents the transpose operation performed on the matrix.

Step 5. Assign all elements in the matrixes **P3** and **P4** whose absolute value is less than the preset threshold TS to zero, in order to achieve higher sparsity. Later, the matrixes after threshold processing are denoted as **P5**and **P6**, respectively.

Step 6. The Rossler hyperchaos is iterated $500 + MN$ times by Runge-Kutta method and the initial value is set to $[x_0, y_0, z_0]^{\mathrm{T}}$. Then, discarding the former 500 values, the chaotic sequence **X**, **Y** and **Z** are obtained as follows.

$$\begin{cases} \mathbf{X} = \{x_1, x_2, \ldots, x_{MN}\} \\ \mathbf{Y} = \{y_1, y_2, \ldots, y_{MN}\} \\ \mathbf{Z} = \{z_1, z_2, \ldots, z_{MN}\} \end{cases} \quad (13)$$

Step 7. The chaotic sequences **X** and **Y** are spliced together, and then sorted to obtain the index sequence **Ixy**. It is used to scramble the matrix **P7** generated by combining the matrixes **P5** and **P6**. The scrambling equation is shown in Eq.(14).

$$\mathbf{P8}_i = \mathbf{P7}_{\mathbf{Ixy}(i)} \quad i = 1, 2, \ldots, 2MN \quad (14)$$

Step 8. Compress the $\mathbf{P8} \in \mathbb{R}^{M \times 2N}$ through the measurement matrix $\mathbf{\Phi}$. And the corresponding compression equation is described as follows.

$$\mathbf{P9} = \mathbf{\Phi} \times \mathbf{P8} \quad (15)$$

Step 9. The compressed image $\mathbf{P10} \in N^{n \times 2N}$ can be obtained by quantizing the matrix **P9**, as shown in Eq.(16).

$$\mathbf{P10} = \mathrm{round}(255 \times \frac{\mathbf{P9} - min}{max - min}) \quad (16)$$

where the quantization parameters max and min represent the maximum and minimum values of the matrix **P9** respectively. Additionally, round $(\cdot)$ means to round off the element in parentheses to the nearest integer.

3) ENCRYPTING THE COMPRESSED IMAGE

The plain image can be compressed linearly and encrypted at the same time though the compressive sensing technology. But it cannot conceal the statistical characteristics of the image. Therefore, it is necessary to diffuse the compressed image. In addition, in order to improve security, variable step length Josephus confusion is utilized to scramble the compressed image before the diffusion operation. The detailed encryption steps are shown below.

Step 1. The step length sequence of Josephus confusion can be generated by chaotic sequence **Y** according to Eq.(17).

$$\mathbf{sy} = \mathrm{mod}(\mathrm{floor}(\mathbf{Y} \times 10^{10}), nN : -1 : 1) \quad (17)$$

Step 2. Then, using the method described in section 2.2, perform Josephus confusion on the compressed image **P10** though the step length sequence **sy**. And the scram-bled image is denoted as **P11**.

Step 3. The chaotic sequence **Z** is used to generate the diffusion sequence. The generation process is shown in Eq.(18).

$$\mathbf{KS} = \mathrm{mod}(\mathrm{floor}(\mathbf{Z} \times 10^{10}), 256) \quad (18)$$

Step 4. Perform bitwise xor operation on the scrambled image **P11**, as shown in Eq.(19).

$$\mathbf{P12}_i = \mathbf{P11}_i \oplus \mathbf{KS}_i \quad (19)$$

Step 5. Then, the image **P12** is divided into two sub-images **PS1** and **PS2**. And the alpha channel of **PS2** is replaced by **PS1** to obtain the final noise-like cipher image **P13**.

B. THE DECRYPTION PROCESS

The double-image encryption algorithm proposed in this paper belongs to the symmetric encryption domain. Hence, the decryption process corresponds to the inverse process of corresponding encryption process. The detailed double-image decryption steps are as follows.

Step 1. First, the **KS3** is used to scramble the internal keys to generate the initial states of the chaotic systems. Then, the chaotic trajectories **X**, **Y** and **Z** of Rossler hyper-chaotic system are obtained by Runge-Kutta method with the initial value $[x_0, y_0, z_0]^{\mathrm{T}}$. At the same time, the measurement matrix $\mathbf{\Phi}$ is generated according to Eq.(11).

Step 2. The **PS1** is extracted from the alpha channel of cipher image **P13**. And the diffused image **P12** can be generated by combining **P13** and **PS1**.

Step 3. The diffusion sequence is generated by the chaotic sequence **Z** (as shown in Eq.(18)) to carry out inverse diffusion operation on **P12**. The inverse diffusion operation can be formulated by Eq.(20).

$$\mathbf{P11}_i = \mathbf{P12}_i \oplus \mathbf{KS}_i \tag{20}$$

Step 4. The step sequence generated by Eq.(17) is used to perform inverse variable step length Josephus confusion on **P11** to obtain the compressed image **P10**.

Step 5. Next, the inverse quantization operation is carried out on the **P10** and the matrix **P9** is gotten. This procedure can be formulated as follows.

$$\mathbf{P9} = \frac{\mathbf{P10} \times (max - min)}{255} + min \tag{21}$$

Step 6. The smoothed l_0 norm method is adopted to reconstruct **P8** from the compressed matrix **P9** with the measurement matrix $\mathbf{\Phi}$. This procedure can be denoted as Eq.(22).

$$\mathbf{P8} = \mathrm{SL}_0(\mathbf{P9}, \mathbf{\Phi}) \tag{22}$$

Step 7. According to Eq.(23), the inverse index confusion is performed on the coefficient matrix **P8**.

$$\mathbf{P7}_i = \mathbf{P8}_{\mathbf{Ixy}(i)} \; i = 1, 2, \ldots, 2MN \tag{23}$$

Step 8. The matrix **P7** obtained in the previous step is divided into two sub-matrices. And the inverse wavelet transform is performed on them to obtain the final decrypted image **D1** and **D2**.

IV. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

A. ENCRYPTION AND DECRYPTION RESULTS

The simulation results of the proposed double-image encryption algorithm are demonstrated in Fig. 5, which are provided by the PC platform with 16G RAM, 1.8 GHz CPU and MATLAB 2019a. Twelve plain images sized of 256 × 256 are selected for the test. In addition, the encryption keys **A** and **B** are set to {8991276369782740718261 04} and {78253967}, respectively. The remaining parameters are set as follows: $TS = 25$, $d = 25$, $a = 0.99$, $b = 3.89$, $c = 2.57$ and $CR = 0.5$.

It can be seen from the figure that the cipher image effectively conceals the information carried by plain image. Moreover, the total volume of two plain images is compressed to a quarter, which means the compression rate is as high as 400%. In other aspects, the decrypted images have a good visual effect, which are similar to the corresponding plain images. Additionally, it is worth mentioning that, unlike other existing image encryption algorithms, we hide half of cipher image generated by the proposed algorithm into the alpha channel of the other half of cipher image to control the transparency. To sum up, the double-image encryption algorithm proposed in this paper has very high transmission efficiency and security.

B. SECRET KEY ANALYSIS

The anti-violent attack ability of encryption algorithm depends on the key space and the key sensitivity. In this paper, the encryption keys are mainly composed of the *KS3* generated by performing exclusive or operation on the hash values of the two plain images and the internal keys. Therefore, the total key space is $2^{256} + 10^{32} > 2^{362}$, which is much larger than 2^{100} [40]. In addition, the control parameters of ISEL map can also be used as the encryption keys.

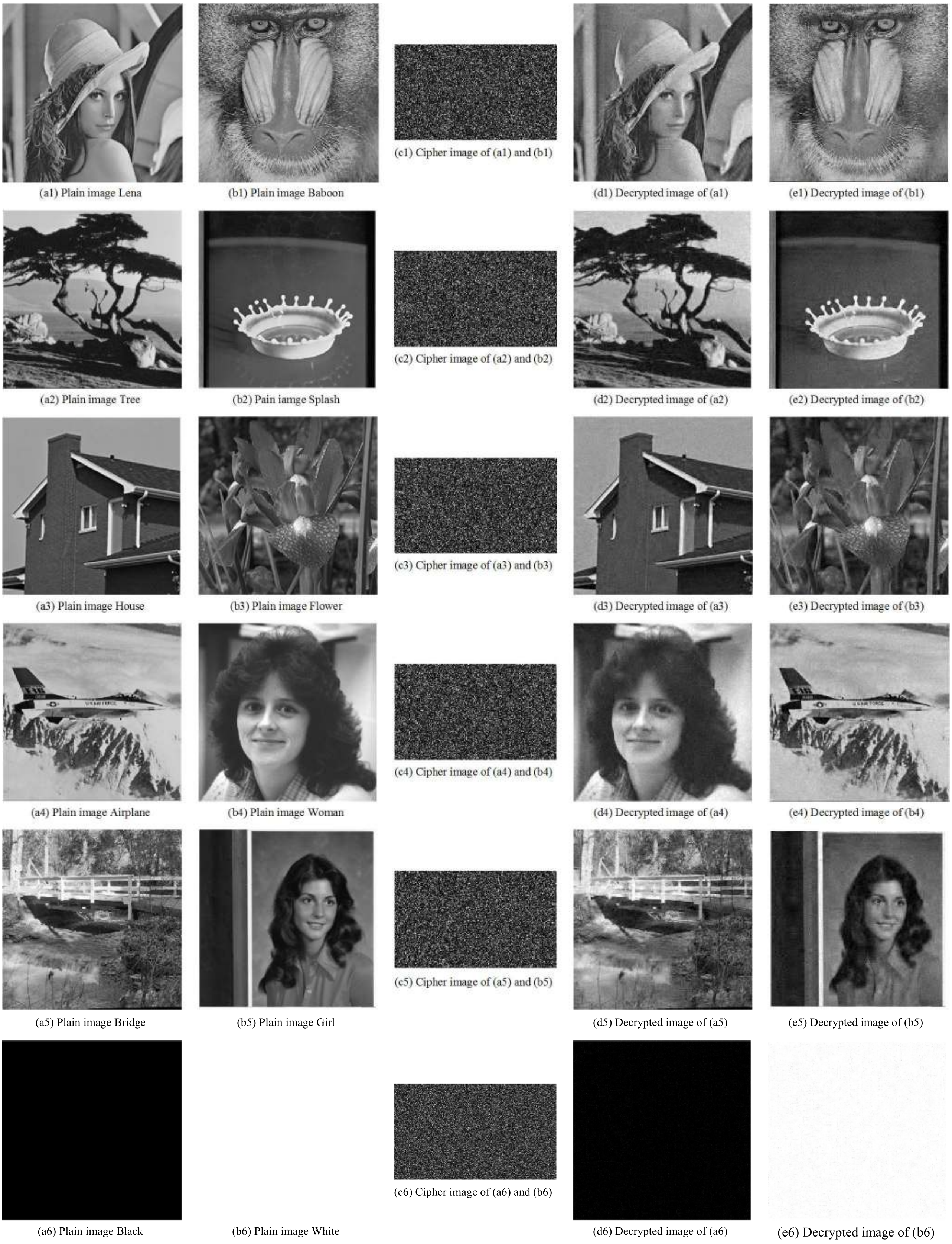
Fig. 6 demonstrates the decrypted image "Tree" obtained by decrypting with the wrong secret keys. As can be seen, when a slight perturbation is added to one of the decryption secret keys, the decrypted images have a big difference from the corresponding plain image. Visually, the decrypted images do not provide any useful information about the plain image, indicating that the proposed encryption scheme has very good key sensitivity. Through the above analysis, it shows that the proposed double-image encryption algorithm has a large enough key space and sensitivity to resist violent attacks.

C. HISTOGRAM ANALYSIS

The histogram reflects the distribution of each gray level in the image. In this sub-section, chi-square test [41] is used to quantitatively analyze the ability of proposed encryption scheme to resist statistical attacks, which is defined in Eq. (24). In addition, when the degree of freedom is 255 and the confidence is set to 5%, if the chi-square value of generated cipher image is lower than 293.2478, it indicates that the encryption algorithm has a strong ability to resist statistical attacks.

$$\chi^2 = \sum_{i=o}^{255} \frac{u_i - u_0}{u_0} \tag{24}$$

where u_i is the actual frequency of the gray levels $i(i = 0, 1, 2, \ldots, 255)$ appearing in the image, and u_0 is the expected frequency of gray levels which is equal to $(M \times N)/256$. Histograms of different images and corresponding chi-square values are provided in Fig. 7. As can be seen, the pixel distribution of plain image is uneven. At the same time, its distribution has a certain statistical rule. In other aspects, the pixel distribution of cipher image generated-ed in this paper is very uniform, and its corresponding chi-square value is also lower than 293.2478. Tab. 1 lists the chi-square values of different encryption algorithms. It can be seen from the table that the cipher images generated in this paper have lower chi-square value, indicating that our scheme-me has a stronger ability to resist statistical attacks.



(a1) Plain image Lena (b1) Plain image Baboon (c1) Cipher image of (a1) and (b1) (d1) Decrypted image of (a1) (e1) Decrypted image of (b1)

(a2) Plain image Tree (b2) Pain iamge Splash (c2) Cipher image of (a2) and (b2) (d2) Decrypted image of (a2) (e2) Decrypted image of (b2)

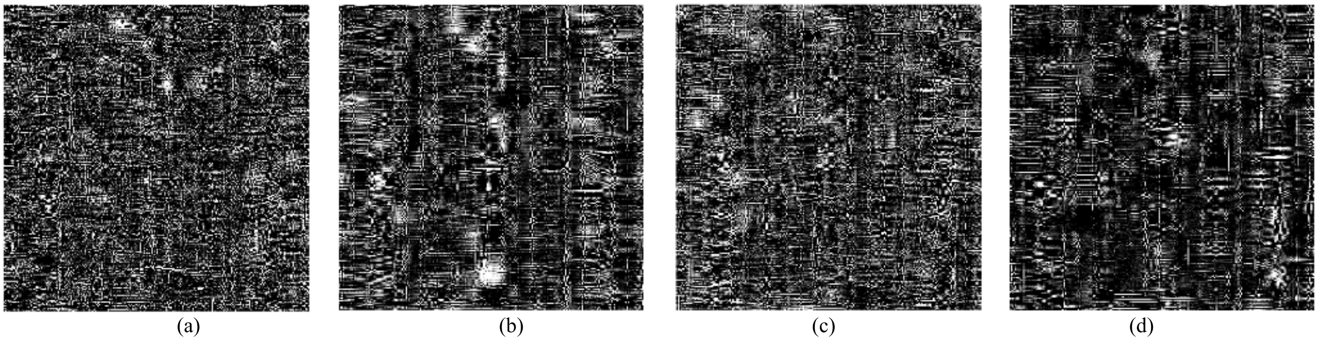
(a3) Plain image House (b3) Plain image Flower (c3) Cipher image of (a3) and (b3) (d3) Decrypted image of (a3) (e3) Decrypted image of (b3)

(a4) Plain image Airplane (b4) Plain image Woman (c4) Cipher image of (a4) and (b4) (d4) Decrypted image of (a4) (e4) Decrypted image of (b4)

(a5) Plain image Bridge (b5) Plain image Girl (c5) Cipher image of (a5) and (b5) (d5) Decrypted image of (a5) (e5) Decrypted image of (b5)

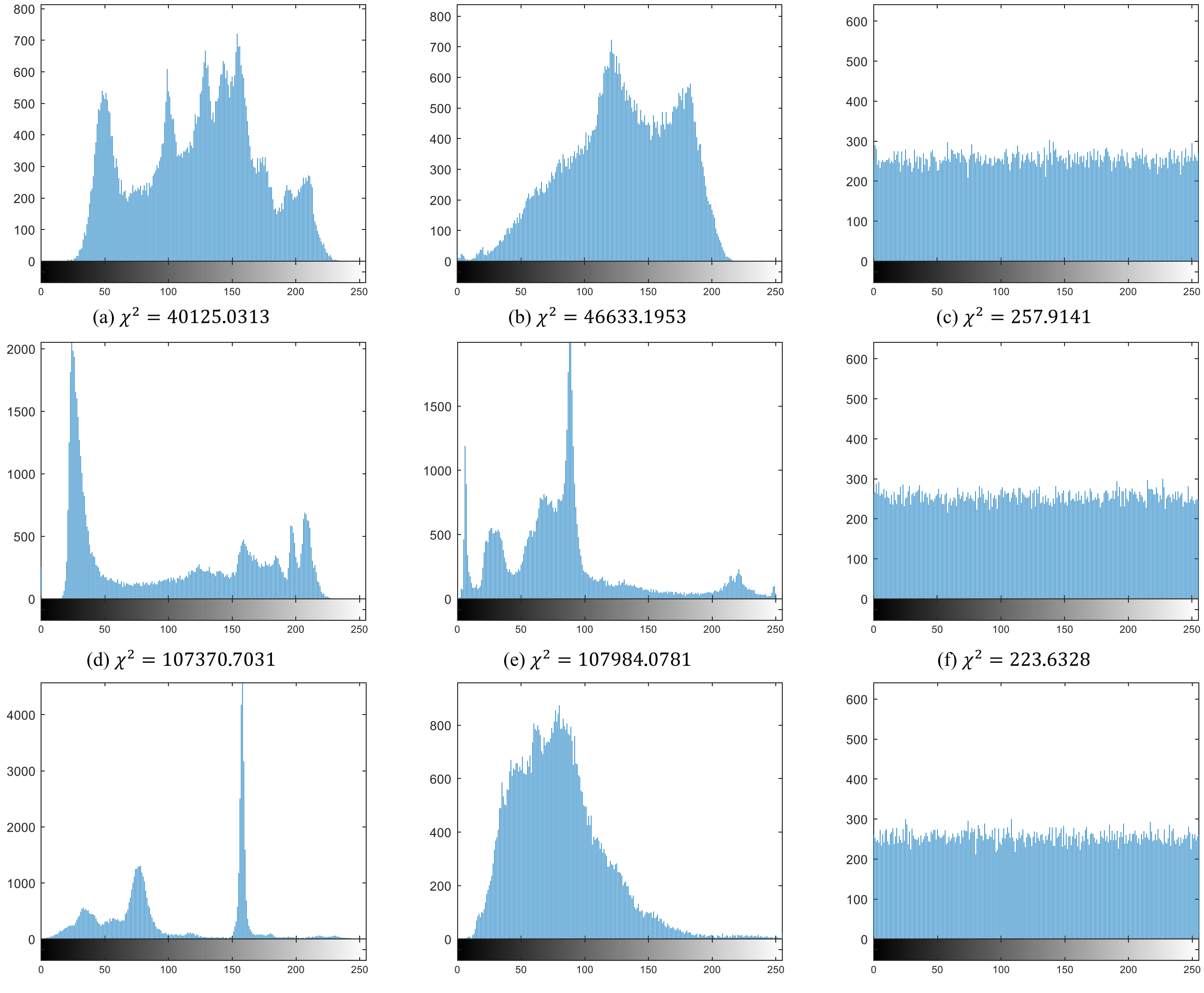
(a6) Plain image Black (b6) Plain image White (c6) Cipher image of (a6) and (b6) (d6) Decrypted image of (a6) (e6) Decrypted image of (b6)

FIGURE 5. Simulation results (resolution 256 × 256).



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

FIGURE 6. Decrypted "Tree" using incorrect keys. (a) $x_0 + 10^{-14}$; (b) $y_0 + 10^{-14}$; (c) $z_0 + 10^{-14}$; (d) $v_0 + 10^{-14}$.



(a) $\chi^2 = 40125.0313$ (b) $\chi^2 = 46633.1953$ (c) $\chi^2 = 257.9141$

(d) $\chi^2 = 107370.7031$ (e) $\chi^2 = 107984.0781$ (f) $\chi^2 = 223.6328$

(g) $\chi^2 = 270021.5156$ (h) $\chi^2 = 81592.3359$ (i) $\chi^2 = 240.8984$

FIGURE 7. Histograms of different images. (a), (b) and (c) are the histograms of the image "Lena", "Baboon" and the corresponding cipher image. (d), (e) and (f) are the histograms of the image "Tree", "Splash" and the corresponding cipher image. (g), (h) and (i) are the histograms of the image "House", "Flower" and the corresponding cipher image.

D. CORRELATION ANALYSIS

For a noise-like cipher image, the correlation between adjacent pixels should tend to zero. Therefore, the Eq.(25) [44] is utilized to calculate the correlation coefficient between adjacent pixels in different images, where K is the number of randomly selected pixel pairs. Additionally, the expected

TABLE 1. Comparison of chi-square values of cipher images generated by different encryption algorithms.

	Our	Ref.[27]	Ref.[26]	Ref.[42]	Ref.[43]
Lena Baboon	257.91	281.47	262.69	254.68	265.57
Tree Splash	223.63	270.57	253.23	248.53	279.22
Average	240.77	276.02	257.96	251.61	272.40

TABLE 2. Comparison of correlation coefficients of cipher images generated by different encryption algorithms.

	Our	Ref.[27]	Ref.[26]	Ref.[43]	Ref.[42]
H	0.000871	0.005411	0.002171	0.002808	-0.000376
V	0.001932	0.004213	-0.005156	0.003260	0.008859
D	0.000493	0.000715	-0.003417	-0.001574	-0.001280

values of x and y are $\bar{x}$ and $\bar{y}$, respectively.

$$r_{xy} = \frac{\sum_{i=1}^{k}(x_i - \bar{x})(y_i - \bar{y})^2}{\sqrt{\sum_{i=1}^{k}(x_i - \bar{x})\sum_{i=1}^{k}(y_i - \bar{y})^2}} \tag{25}$$

The correlation distribution of images "Lena", "Baboon" and corresponding cipher image in horizontal, vertical and diagonal directions are plotted in Fig. 7. It can be seen from the figure that there is a strong positive correlation between the adjacent pixels in the two plain images. In addition, for the generated cipher image, the correlation between adjacent pixels is very low and uniformly distributed in the whole region. Tab. 2 lists the correlation coefficients of different encryption algorithms. By comparing the experimental data in the table, it can be seen that the cipher image generated in this paper have the lowest correlation.

E. PLAINTEXT SENSITIVITY ANALYSIS

Plaintext sensitivity analysis refers to encrypting two plain images with the same secret key, and comparing the differences between the two corresponding cipher images. The main indicators are NPCR and UACI [45]–[46]. If only the pixel values of (i, j) in the two plain images are different, the pixel values at (i, j) in their encrypted images are $\mathbf{P}_1(i, j)$ and $\mathbf{P}_2(i, j)$, respectively. Then the NPCR and UACI can be calculated by Eq.(26) and Eq.(27).

$$NPCR = \frac{1}{MN}|\text{Sign}(\mathbf{P}_1(i,j) - \mathbf{P}_2(i,j))| \times 100\% \tag{26}$$

$$UACI = \frac{1}{MN}(\frac{|\mathbf{P}_1(i,j) - \mathbf{P}_2(i,j)|}{255}) \times 100\% \tag{27}$$

From the above equations, if the difference between the two cipher images is larger, the value of NPCR and UACI will be larger. The test results of NPCR and UACI in the two groups of cipher images (Lena and Baboon, Tree and Splash) are listed in Tab. 2. Obviously, the NPCR and UACI of the proposed encryption algorithm are larger than that of Ref. [26-27, 42-43], which indicates that the proposed encryption scheme is very sensitive to plaintext attacks and has a strong ability to resist the differential attacks or the chosen-plaintext attacks.

TABLE 3. Comparison of plaintext sensitivity in different encryption algorithms.

	Our	Ref.[27]	Ref.[26]	Ref.[42]	Ref.[43]	
Lena	99.63	99.61	99.61	99.62	99.57	NPCR
Baboon	33.41	33.41	33.40	33.30	33.41	UACI
Airplane	99.68	99.64	99.60	99.59	99.55	NPCR
Woman	33.59	33.48	33.42	33.54	33.59	UACI

TABLE 4. Local Shannon entropy test for cipher images.

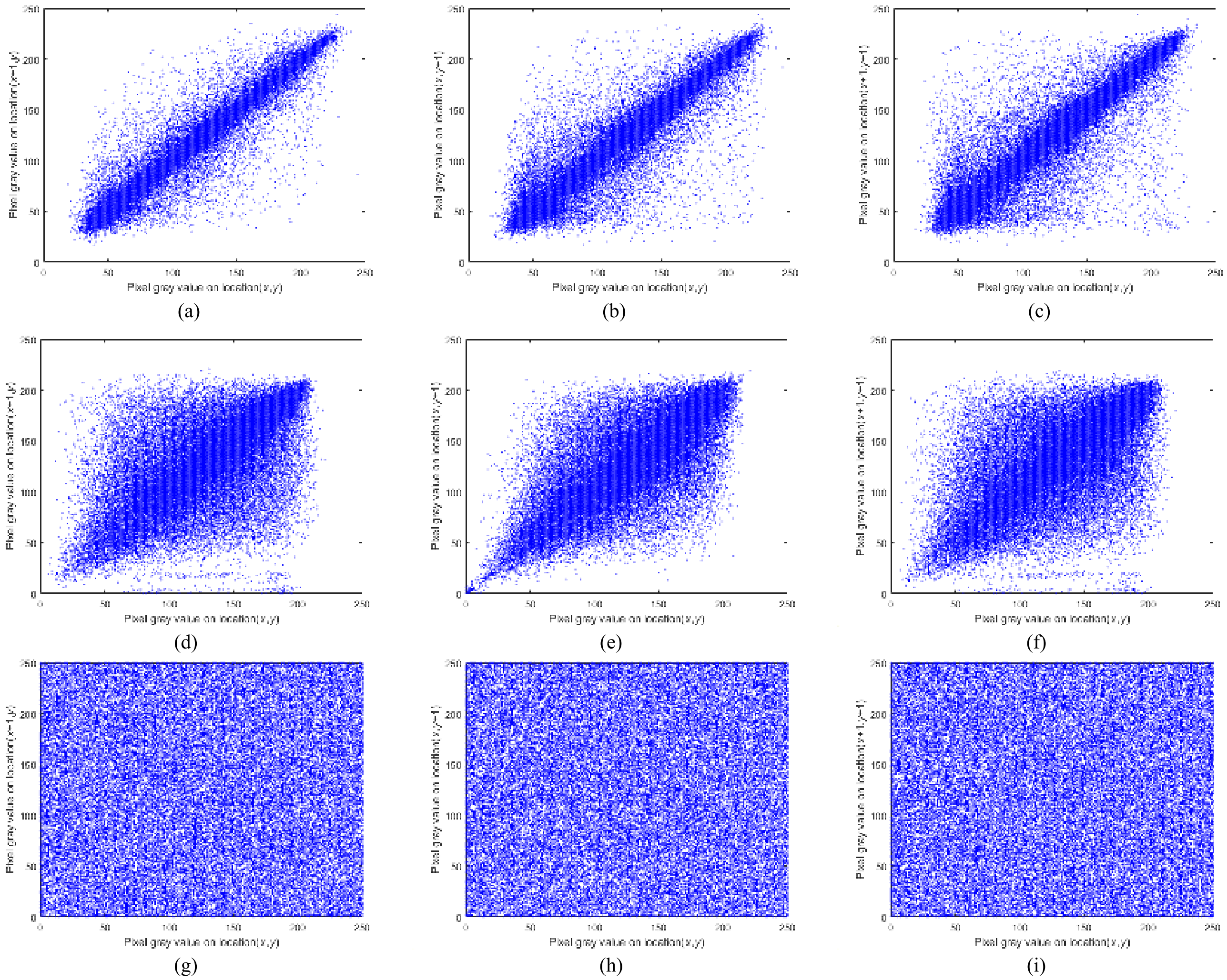
Plain image	Local information entropy	Result
Lena Baboon	7.90238032231388	Pass
Tree Splash	7.90255867309644	Pass
House Flower	7.90301774401962	Pass
Airplane Woman	7.90246463857135	Pass
Bridge Girl	7.90202973517702	Pass
Boat Fruit	7.90293118902876	Pass

F. LOCAL SHANNON INFORMATION ENTROPY ANALYSIS

Shannon information entropy reflects the overall randomness of the image. The higher Shannon information entropy of the image is, the stronger the overall randomness of the image is. In order to accurately evaluate the randomness of cipher images generated by the proposed encryption algorithm, the local Shannon information entropy [47] is adopted, which is defined as follows:

$$LH = \sum_{i=1}^{k}\frac{H(S_i)}{k} \tag{28}$$

where S_i represents the i-th non-overlapping sub-image in the cipher image. In addition, k is the number of segmented sub-image. Thirty cipher sub-images with size of 44 × 44 are adopted for the test. The corresponding experimental results are listed in Tab. 4. According to [48]–[49], when the confidence is 5%, the local information entropy LH should be between 7.901901305 and 7.903037329. It can be seen from



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

FIGURE 8. Correlation distribution of different images. (a)-(c) are the correlation distribution in horizontal, vertical and diagonal directions of image "Lena". (d)-(f) are the correlation distribution in horizontal, vertical and diagonal directions of image "Baboon". (g)-(i) are the correlation distribution in horizontal, vertical and diagonal directions of the corresponding cipher image.

the table that the values of local information entropy are all within this range, indicating that cipher images generated by the proposed encryption algorithm are very random.

G. DECRYPTION QUALITY ANALYSIS

Undeniably, the quality of the decrypted image is reduced by using lossy compression technology to compress the plain image. Therefore, it is necessary to analyze the decrypted image quality. In this sub-section, the peak signal-to-noise ratio (PSNR) [50]–[51] will be used to quantitatively measure the quality of the decrypted image. Its mathematical expression is shown in Eq.(29).

$$PSNR = 10 \times \log \frac{255^2}{\frac{1}{MN}\sum_{i=1}^{k}\sum_{i=1}^{k}(\mathbf{D}_{i,j}-\mathbf{I}_{i,j})^2}(\text{dB}) \qquad (29)$$

where **D** and **I** are the plain image and the corresponding decrypted image. The decryption quality of the different images is listed in Tab. 5. As can be seen, the quality of the decrypted images is greater than 30 dB. And visually, the decrypted images are similar to the corresponding plain images. For the encryption schemes proposed in Ref [26]–[27], [42]–[43], since the plain images are not compressed during the encryption process, the decrypted images

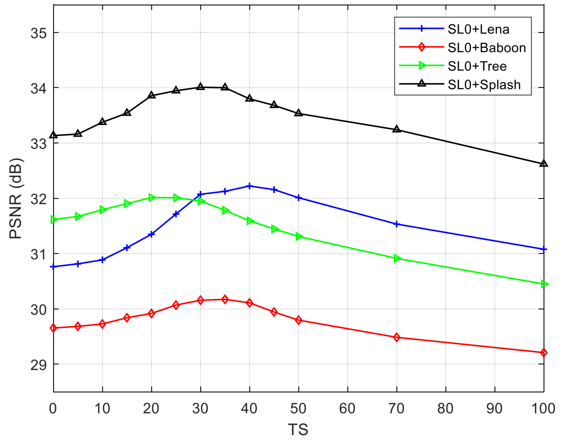
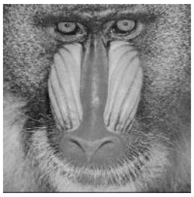
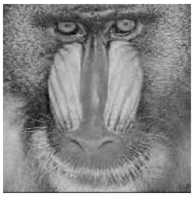


FIGURE 9. Impact of threshold value TS on decryption image quality.

TABLE 5. Decryption quality of different images.

Plain image	Decrypted image	PSNR (dB)	Plain image	Decrypted image	PSNR (dB)
		31.7164			32.0114
		30.0700			33.9456
		33.5155			31.3706
		32.7238			31.8926

are the same as the plain images. Although the decryption quality of proposed encryption scheme is lower than that of Ref [26]–[27], [42]–[43], our scheme requires less transmission cost and storage space.

As can be seen from Fig. 10, the GN has the greatest impact on the proposed encryption scheme, that is, with the increase of noise intensity, the quality of decrypted image decreases most obviously. In contrast, since the decryption quality has almost no change from the visual perspective, the impact of SPN is the least. Then, the impact of SN on the proposed encryption scheme is somewhere in between. In other aspects, as plotted in Fig. 11, the proposed scheme has a certain recovery ability when attacked by data loss. In general, our scheme has the strongest anti-interference ability against SPN attack, and can also resist SN, GN and cropping attacks to some extent.

It is worth mentioning that the threshold *TS* has a certain influence on the quality of decrypted image, which is plotted in Fig. 9. It can be seen that the impact of threshold on the quality of decrypted image is not simplex, and the optimal threshold is different for different images.

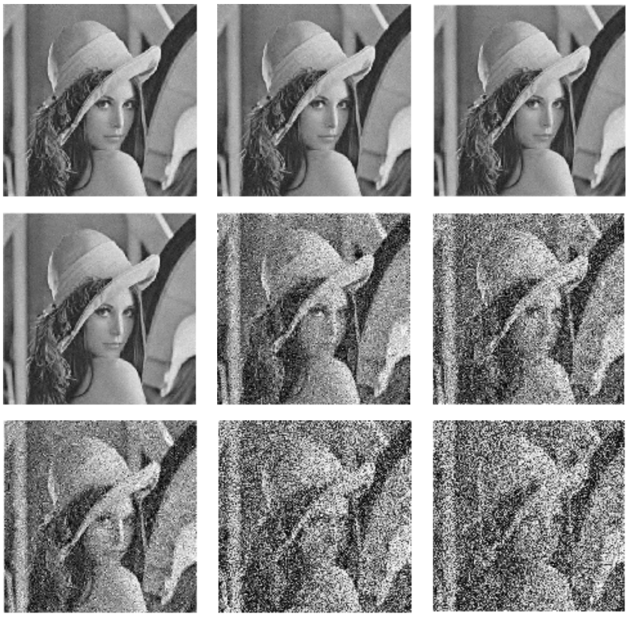
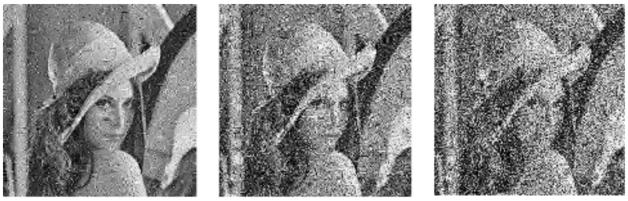


FIGURE 10. Noise attack analysis results.

H. NIST SP 800-22 ANALYSIS

The NIST SP 800-22 test suite is published by the National Institute of Standards and Technology to determine the randomness of sequences [52]. Thus, in this sub-section, we will adopt this suite to evaluate the uncertainty of the generated cipher image under the condition that the confidence value is set to 0.01. The results are listed in Tab. 6. As can be seen,



10×10 data loss 20×20 data loss 30×30 data loss

FIGURE 11. **Cropping attack analysis results.**

TABLE 6. **Test results of the cipher image with NIST SP800 suite.**

Test items	P-value	Results
Frequency test	0.314723686	Pass
Block Frequency test	0.546881519	Pass
Cusum-forward test	0.241886338	Pass
Cusum-reverse test	0.421761282	Pass
Runs test	0.605740699	Pass
Longest run test	0.157613081	Pass
Rank test	0.446881519	Pass
FFT test	0.800280468	Pass
Non-Overlapping template test	0.278498218	Pass
Overlapping template test	0.141886338	Pass
Universal test	0.381558457	Pass
Approximate entropy test	0.489764395	Pass
Random-excursions test (x = -1)	0.709364830	Pass
Random-excursions variant test (x = 1)	0.565477890	Pass
Serial1 test	0.171186687	Pass
Serial2 test	0.376922984	Pass
Linear complexity test	0.655477890	Pass

the obtained experimental data have all passed the random test, indicating that the generated cipher image has good randomness.

I. ROBUSTNESS ANALYSIS

To qualitatively evaluate the anti-interference ability of the proposed encryption scheme in various noise environments, we add three different types of noise to the cipher image, including Gaussian noise (GN), salt & pepper noise (SPN) and speckle noise (SN). And then their normalized noise intensity is set as 0.0001%, 0.0003% and 0.0005% in turn. Additionally, cropping attacks with different intensity are applied to the cipher image. The decrypted images obtained under different attacks are illustrated in Fig. 10 and Fig. 11, respectively.

J. TIME COMPLEXITY ANALYSIS

The time complexity is used to evaluate the execution time of an algorithm. In this paper, the proposed encryption scheme mainly includes exchange operation, four arithmetic operations and matrix multiplication. Assuming that the size of each plain image is $N \times N$. Therefore, the time complexity of generating chaotic sequences and measuring matrix is $\theta(N^2)$ and $\theta(CR \times N^2)$, respectively. Meanwhile, in encryption process, the time complexity of performing Josephus confusion and diffusion operation on the quantized image is $\theta(CR \times 2N^2)$. Additionally, before the compression process, the two sparse matrices need to be scrambled by the index confusion, and the time complexity of this part is $\theta(2N^2)$. Then the total time complexity of the proposed algorithm is calculated as $\theta(3(1+CR)N^2)$, which is larger than that of Ref [26] ($\theta(22N)$) and Ref [27] ($\theta(N^2/8)$).

V. CONCLUSION

In this paper, a novel double-image encryption algorithm is proposed by Rossler hyperchaotic system conjugated with compressive sensing to improve transmission efficiency and reduce storage space. In addition, the proposed key generation mechanism makes our scheme very sensitive to plain images. Finally, the simulation results and security performance analyses indicate that the proposed encryption algorithm can resist multiple attacks, and the quality of decrypted images is satisfactory. The major limitation of this paper is its high time complexity. In the future work, we will deeply study and design the algorithm that can encrypt plain image in parallel.

REFERENCES

[1] Y. Zhang, "A new unified image encryption algorithm based on a lifting transformation and chaos," *Inf. Sci.*, vol. 547, pp. 307–327, Feb. 2021.

[2] 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.

[3] Y. Xian and X. Wang, "Fractal sorting matrix and its application on chaotic image encryption," *Inf. Sci.*, vol. 547, pp. 1154–1169, Feb. 2021.

[4] 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.

[5] L. Teng, X. Wang, and J. Meng, "A chaotic color image encryption using integrated bit-level permutation," *Multimedia Tools Appl.*, vol. 77, no. 6, pp. 6883–6896, Mar. 2018.

[6] C. Li, D. Lin, J. Lü, and F. Hao, "Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography," *IEEE Multimedia*, vol. 25, no. 4, pp. 46–56, Oct. 2018.

[7] W. Cao, Y. Mao, and Y. Zhou, "Designing a 2D infinite collapse map for image encryption," *Signal Process.*, vol. 171, Jun. 2020, Art. no. 107457.

[8] Y. Liu, Z. Qin, X. Liao, and J. Wu, "A chaotic image encryption scheme based on Hénon—Chebyshev modulation map and genetic operations," *Int. J. Bifurcation Chaos*, vol. 30, no. 6, May 2020, Art. no. 2050090.

[9] 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.

[10] 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.

[11] F. Yu, S. Qian, X. Chen, Y. Huang, L. Liu, C. Shi, S. Cai, Y. Song, and C. Wang, "A new 4D four-wing memristive hyperchaotic system: Dynamical analysis, electronic circuit design, shape synchronization and secure communication," *Int. J. Bifurcation Chaos*, vol. 30, no. 10, Aug. 2020, Art. no. 2050147.

[12] Z. Hua and Y. Zhou, "Exponential chaotic model for generating robust chaos," *IEEE Trans. Syst., Man, Cybern., Syst.*, early access, Aug. 28, 2019, doi: 10.1109/TSMC.2019.2932616.

[13] M. Wang, X. Wang, T. Zhao, C. Zhang, Z. Xia, and N. Yao, ''Spatiotemporal chaos in improved cross coupled map lattice and its application in a bit-level image encryption scheme,'' *Inf. Sci.*, vol. 544, pp. 1–24, Jan. 2021.

[14] Y. Naseer, T. Shah, Attaullah, and A. Javeed, ''Advance image encryption technique utilizing compression, dynamical system and S-boxes,'' *Math. Comput. Simul.*, vol. 178, pp. 207–217, Dec. 2020.

[15] Y.-G. Yang, B.-W. Guan, Y.-H. Zhou, and W.-M. Shi, ''Double image compression-encryption algorithm based on fractional order hyper chaotic system and DNA approach,'' *Multimedia Tools Appl.*, vol. 80, no. 1, pp. 691–710, Jan. 2021, doi: 10.1007/s11042-020-09779-5.

[16] 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.

[17] 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.

[18] A. H. Brahim, A. A. Pacha, and N. H. Said, ''Image encryption based on compressive sensing and chaos systems,'' *Opt. Laser Technol.*, vol. 132, Dec. 2020, Art. no. 106489.

[19] 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.

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

[21] N. Zhou, H. Jiang, L. Gong, and X. Xie, ''Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging,'' *Opt. Lasers Eng.*, vol. 110, pp. 72–79, Nov. 2018.

[22] X. Yang, H. Wu, Y. Yin, X. Meng, and X. Peng, ''Multiple-image encryption base on compressed coded aperture imaging,'' *Opt. Lasers Eng.*, vol. 127, Apr. 2020, Art. no. 105976.

[23] X. Li, X. Meng, X. Yang, Y. Yin, Y. Wang, X. Peng, W. He, G. Dong, and H. Chen, ''Multiple-image encryption based on compressive ghost imaging and coordinate sampling,'' *IEEE Photon. J.*, vol. 8, no. 4, pp. 1–11, Aug. 2016.

[24] Z. Gan, X. Chai, M. Zhang, and Y. Lu, ''A double color image encryption scheme based on three-dimensional brownian motion,'' *Multimedia Tools Appl.*, vol. 77, no. 21, pp. 27919–27953, Nov. 2018.

[25] L. Lidong, D. Jiang, X. Wang, L. Zhang, and X. Rong, ''A dynamic triple-image encryption scheme based on chaos, S-box and image compressing,'' *IEEE Access*, vol. 8, pp. 210382–210399, 2020.

[26] 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.

[27] 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.

[28] X. Zhang and X. Wang, ''Multiple-image encryption algorithm based on mixed image element and chaos,'' *Comput. Electr. Eng.*, vol. 62, pp. 401–413, Aug. 2017.

[29] 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.

[30] H. Jiang, Z. Nie, N. Zhou, and W. Zhang, ''Compressive-sensing-based double-image encryption algorithm combining double random phase encoding with Josephus traversing operation,'' *Opt. Appl.*, vol. 49, no. 3, pp. 445–459, 2019.

[31] D. Huo, X. Zhou, L. Zhang, Y. Zhou, H. Li, and S. Yi, ''Multiple-image encryption scheme via compressive sensing and orthogonal encoding based on double random phase encoding,'' *J. Modern Opt.*, vol. 65, no. 18, pp. 2093–2102, Oct. 2018.

[32] N. Zhou, J. Yang, C. Tan, S. Pan, and Z. Zhou, ''Double-image encryption scheme combining DWT-based compressive sensing with discrete fractional random transform,'' *Opt. Commun.*, vol. 354, pp. 112–121, Nov. 2015.

[33] Y. Tan, C. Zhang, J. Qin, and X. Xiang, ''Image encryption algorithm based on exponential compound chaotic system,'' *J. Huazhong Univ. Sci. Technol., Natural Sci. Ed.*, vol. 49, no. 2, pp. 121–126, Jan. 2021.

[34] D. S. Malik and T. Shah, ''Color multiple image encryption scheme based on 3D-chaotic maps,'' *Math. Comput. Simul.*, vol. 178, pp. 646–666, Dec. 2020.

[35] D. L. Donoho, ''Compressed sensing,'' *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.

[36] L. Zhu, H. Song, X. Zhang, M. Yan, T. Zhang, X. Wang, and J. Xu, ''A robust meaningful image encryption scheme based on block compressive sensing and SVD embedding,'' *Signal Process.*, vol. 175, Oct. 2020, Art. no. 107629.

[37] R. G. Baraniuk, ''Compressive sensing,'' *IEEE Signal Process. Mag.*, vol. 24, no. 4, pp. 118–121, Jul. 2007.

[38] X. Wang and L. Liu, ''Application of chaotic Josephus scrambling and RNA computing in image encryption,'' *Multimedia Tools Appl.*, pp. 1–22, Jan. 2021, doi: 10.1007/s11042-020-10209-9.

[39] Z. Chai, S. Liang, G. Hu, L. Zhang, Y. Wu, and C. Cao, ''Periodic characteristics of the josephus ring and its application in image scrambling,'' *EURASIP J. Wireless Commun. Netw.*, vol. 2018, no. 1, pp. 1–11, Dec. 2018.

[40] G. Ye, C. Pan, Y. Dong, Y. Shi, and X. Huang, ''Image encryption and hiding algorithm based on compressive sensing and random numbers insertion,'' *Signal Process.*, vol. 172, Jul. 2020, Art. no. 107563.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] Z.-H. Gan, X.-L. Chai, D.-J. Han, and Y.-R. Chen, ''A chaotic image encryption algorithm based on 3-D bit-plane permutation,'' *Neural Comput. Appl.*, vol. 31, no. 11, pp. 7111–7130, Nov. 2019.

[46] N. Chidambaram, P. Raj, K. Thenmozhi, and R. Amirtharajan, ''Advanced framework for highly secure and cloud-based storage of colour images,'' *IET Image Process.*, vol. 14, no. 13, pp. 3143–3153, Nov. 2020.

[47] X. Chai, H. Wu, Z. Gan, Y. Zhang, and Y. Chen, ''Hiding cipher-images generated by 2-D compressive sensing with a multi-embedding strategy,'' *Signal Process.*, vol. 171, Jun. 2020, Art. no. 107525.

[48] X. Wang and N. Guan, ''A novel chaotic image encryption algorithm based on extended Zigzag confusion and RNA operation,'' *Opt. Laser Technol.*, vol. 131, Nov. 2020, Art. no. 106366.

[49] H. Ghazanfaripour and A. Broumandnia, ''Designing a digital image encryption scheme using chaotic maps with prime modular,'' *Opt. Laser Technol.*, vol. 131, Nov. 2020, Art. no. 106339.

[50] X. Chai, H. Wu, Z. Gan, D. Han, Y. Zhang, and Y. Chen, ''An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing,'' *Inf. Sci.*, vol. 556, pp. 305–340, May 2021, doi: 10.1016/j.ins.2020.10.007.

[51] Y.-G. Yang, B.-P. Wang, Y.-L. Yang, Y.-H. Zhou, and W.-M. Shi, ''Dual embedding model: A new framework for visually meaningful image encryption,'' *Multimedia Tools Appl.*, vol. 80, pp. 9055–9074, Nov. 2021, doi: 10.1007/s11042-020-10149-4.

[52] R. Sivaraman, S. Rajagopalan, J. B. B. Rayappan, and R. Amirtharajan, ''Ring oscillator as confusion–diffusion agent: A complete TRNG drove image security,'' *IET Image Process.*, vol. 14, no. 13, pp. 2987–2997, May 2020.