IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 25, 2017, accepted February 2, 2018, date of publication February 22, 2018, date of current version May 16, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2805847

An Image Encryption Algorithm Based on Josephus Traversing and Mixed Chaotic Map

XINGYUAN WANG[1, 2], XIAOQIANG ZHU[2], AND YINGQIAN ZHANG[3]
[1]School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China
[2]School of Electronic and Information Engineering, Dalian University of Technology, Dalian 116024, China
[3]School of Information Science and Technology, Xiamen University Tan Kah Kee College, Zhangzhou 363105, China

Corresponding author: Xingyuan Wang (wangxy@dlut.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61672124, Grant 61370145, and Grant 61173183, in part by the Password Theory Project of the 13th Five-Year Plan National Cryptography Development Fund under Grant MMJJ20170203, and in part by the Program for New Century Excellent Talents in Fujian Province University.

ABSTRACT This paper proposes a new chaotic image encryption scheme, which employs Josephus traversing and mixed chaotic map. The scheme consists of three processes: key stream generation process; three-round scrambling process; and one-round diffusion process. The proposed mathematical model is applied for the key stream generator in the first process. The initial values and parameters are sensitive to both the secret keys in the new scheme and plain images. The second process employs the Josephus traversing in scrambling; then the rows and columns of pixels are exchanged. The third process can modify the pixel gray-level values and crack the strong correlations between adjacent pixels simultaneously. The initial conditions for chaotic systems are derived using external secret keys by applying some algebraic transformations to the key. Security analysis indicates that the new scheme is effective, which can resist common attacks.

INDEX TERMS Gray-scale, image analysis, cryptography, encryption, diffusion processes, chaos.

I. INTRODUCTION

Chaos is an interdisciplinary theory stating that within the apparent randomness of chaotic complex systems. Sequences are generated by chaotic system due to its initial value sensitivity, periodic and pseudo random, unpredictability for a long time and et al. So, it widely applied to the design and development of encryption algorithm. In recent years, a large number of encryption algorithms based on chaotic systems are used in image encryption [1]–[7].

A good cryptosystem should have a large enough key space and extreme sensitivity to plain and key. The histogram of cipher should be random and uniform as well as adjacent pixels are not relevant. In recent years, some literatures have analyzed the security of cryptosystems, some of which have been attacked. Traditional encryption technology is getting maturing, but its application in digital images [8], [9] does not match the idea results. Thus, there are some limitations where the traditional encryption technology is not suitable for directly applying in image encryptions. Image scrambling algorithm is a classical encryption method, such as Arnold transform, geometry transform, E curve transformation and so on. Although the results are different after scrambling, it still has certain regularity, which only changes the position of pixels without changing gray values. Arnold map has the characteristic of periodicity. After a certain number of iterations can be restored the original image; therefore, it brings potential flaws for the system [10]. The literature [11] was effective to decipher image encryption scheme based on Arnold map and Lü map.

This paper overcomes these weaknesses by designing a novel image encryption method with high security and high sensitivity. In order to get better encryption results, three-round scrambling process and one-round diffusion process are employed to modify the positions. Pixel values and their correlations between adjacent pixels of an image are broken simultaneously. Based on the chaotic sequence and correlating keys with a plaintext image, we proposed a new encryption scheme. These features strengthen the cryptosystem security. Experimental results and performance analysis verify the feasibility of this cryptography.

This paper is organized as follows. Section 2 gives a brief introduction of Josephus traversing and chaos system. Section 3 introduces the proposed encryption scheme and simulation results are presented in this section. Section 4 provides a detailed security study and various attacks to the proposed image encryption scheme. Section 5 reaches a conclusion.

II. JOSEPHUS TRAVERSING AND CHAOS SYSTEM

A. JOSEPHUS TRAVERSING

The Josephus problem is well-known in computer science and mathematics. It is a theoretical problem related to a certain counting-out game that works by having n people standing in a circle, with consecutive tags from 1 to n. Starting at a predetermined person, one counts around the circle. Once reached the mth person, take him out of the circle and have the remaining members to form a new circle. Then, repeat the process until only one person is left. The person left wins the game. If we record who have been taken out at each round as a sequence, this sequence is called Josephus permutation sequence.

It's clear that the Josephus problem involves three parameters. In other words, they are the initial total number of persons in a circle n, the starting position in the circle s, and the counting period m. Therefore, a Josephus permutation sequence can be denoted as follows [12] and [13]:

$$\text{josephus\_traver sin g}(\textit{total number}, \textit{start}, \textit{space}). \qquad (1)$$

For example, josephus_traver raversing $\sin g(8, 1, 4) = (4, 8, 5, 2, 1, 3, 7, 6)$.

Where *total number* is the size of plain image, *start* is the starting position, *space* is the counting period. Local random scrambling in the spatial domain of Josephus traversing method is lack of efficiency. If the step size is improper, it will be time-consuming. In addition, the next round is just starting from the next person whilst the step size is fixed; to a certain extent it reduces the randomness of the encryption results by using a fixed parameter. If the value of the step size is the average pixel value, therefore the plain information is effectively linked with the cryptosystem. In the scrambling, two Logistic chaotic sequences are used to generate the chaotic coordinate pairs for exchanging the positions of each pixel. Therefore, the rows and columns of pixels are exchanged well according to rules. Then, the above problems can be solved better.

B. CHAOTIC SYSTEM

A one-dimensional discrete-time nonlinear dynamic system is defined as follows [14]:

$$x_{n+1} = \tau(x_n), \qquad (2)$$

where $\tau_n \in V(n = 0, 1, 2, \ldots)$ is called the state, $\tau : V \to V$ is a map, x_n is the current state and x_{n+1} is the next state. If the function τiterates continuously with the initial value x_0, we can obtain a sequence x_n. This sequence is a trajectory of discrete-time nonlinear dynamic system.

The Logistic map is one of famous one dimension chaotic map. It's a kind of very simple equation which has been widely studied; its mathematical formula can be defined as follows:

$$x_{n+1} = \mu x_n(1 - x_n), \qquad (3)$$

where x_n is the output chaotic sequence with range of (0, 1). When $\mu \in (3.5699456, 4]$, the Logistic map is in chaoticbehaviors. the obtained sequence is non-periodic, non-convergence and sensitive to the initial value x_0. In the literature [4], Wang and Zhang proposed the ACLML system; and they discovered that the bifurcation diagram of traditional Logistic map system with periodic window. when $\mu > 3.63$, the system shows similar chaotic behaviors; when $\mu = 3.74$ and $\varepsilon = 0.2$, the system shows periodic behavior. In order to avoid the periodic behavior, this paper used the parameter μ with the range of $(3.87, 4]$.

III. ENCRYPTION SCHEME

The encryption scheme consists of three processes: key stream generation process, three-round scrambling process and one-round diffusion process, this section describe the encryption process in detail.

A. A NOVEL METHOD TO GENERATE THE INITIAL VALUES

In this paper, we propose a novel calculation method for the selection of the initial value x_0 for chaotic maps. For the original image P with the size $M \times N$, we calculate the sum of all the pixels of the plain image P and denoted as δ; then calculate the average of δ as defined by the following equation:

$$P_{\text{mean}} = floor(\delta/M \times N), \qquad (4)$$

where $floor(\cdot)$ function means the greatest integer less than or equal. Next, we computed a real value X_{01} and it's defined by the following equation:

$$X_{01} = \sum_{i=1}^{16} [\frac{2^{17-i}}{i!} \times |P_{mean} - a| + a]/2^{25}, \qquad (5)$$

where a is a control parameter, which can be used as the key and with range of $[50, 500]$. In order to be able to resist the chosen-plain attack, once the initial value of the chaotic sequence is selected, we employ Hash function, e.g. SHA-3 and other algorithms. Even if the pixel values of the plain images are 0 or 255, It doesn'twork. . Therefore, a novel method of selecting initial value is designed in this paper. It's dependent on both the new scheme and plain image, and carries out one-time pad [5] in encryption process. The purpose of setting the parameter a is to deal with a particular situation, such as the pixel values of the plain image are zero. Therefore, the new method can improve the efficiency of encryption system. We randomly selected 16 pixel values of the plain image P and they are recorded as $\{P_1, P_2, \ldots, P_{16}\}$; then we calculated another real value X_{02}:

$$X_{02} = \sum_{i=1}^{16} P_i/2^{16}. \qquad (6)$$

Finally, we calculated the X_0 by the following equation:

$$X_0 = (X_{01} + X_{02}) \bmod 1, \qquad (7)$$

where X_0 is used as the initial value of chaotic maps.

TABLE 1. **Chaotic system for generating diffusion sequences.**

Chaotic map	Representation	Parameter
Logistic map	$x_{n+1}=\mu_{3i}x_n(1-x_n)$	$\mu_{3i}\in(3.87,4]$
Chebyshev map	$x_{n+1}=\lvert\cos(\mu_4\operatorname{acos}(x_n))\rvert$	$\mu_4=20$
Sine map	$x_{n+1}=\mu_{5i}\sin(\pi x_n)$	$\mu_{5i}\in(0.87,1]$
Cosine map	$x_{n+1}=\mu_6\cos(\pi\lvert x_n-0.5\rvert)$	$\mu_6=0.98$

B. SCRAMBLING

Scrambling process is descripted as follows:

Step 1: First, the plain image P is converted into a one-dimensional sequence $B_i(i = 1, 2, 3, \ldots, M \times N)$ (the order is from left to right and up to down). We made $total\ number = M \times N$, $start = 2$, $space = P_{mean}$. Josephus traversing scrambles the plain image P for the first round. this scrambling method reduces the correlations between uplink and downlink adjacent elements. The scrambled image is denoted as P'. For better performance of scrambling, second and third round scrambling process can be applied for executions.

Step 2: The rows and columns of pixels are exchanged according to certain rules as second round scrambling process. Here, we agree on that images to be processed are noted as P'_{ij} with the size of $M \times N$, where $i = 1, 2, 3, \ldots, M$, $j = 1, 2, 3, \ldots, N$.

The entire row of pixels is exchanged. The 2nd row of pixels $P'_{\{2j\}}$ and the 256th row of pixels $P'_{\{256j\}}$ are exchanged. And, the $4th$ row of pixels $P'_{\{4j\}}$ are exchanged with the 254th row of pixels $P'_{\{254j\}}$, and so forth, until all the even number rows of pixels are exchanged. The position of the 128th row of pixels and all the odd number rows of pixels are unchanged.

The entire column of pixels is exchanged. The 1st column of pixels $P'_{\{i1\}}$ and the 255th column of pixels $P'_{\{i255\}}$ are exchanged, and the 3rd column of pixels $P'_{\{i3\}}$ are exchanged with the 253th column of pixels $P'_{\{i253\}}, \ldots$, until all the odd number columns of pixels are exchanged. The position of the 127th column of pixels and all the even number rows of pixels are unchanged.

Step 3: Used the chaos map (3) to produce two sequences x_i and y_j. We employed our proposed novel scheme to generate two new initial values X_0 and X'_0.

$$f : x_{n+1} = \mu_1 x_n(1 - x_n), \tag{8}$$

$$g : y_{n+1} = \mu_2 y_n(1 - y_n), \tag{9}$$

where X_0 is used for the Eq. (8) and X'_0 is used for the Eq. (9). (We didn't change the value of a, and selected 16 pixels of the plain image to calculate X_0, and then selected other 16 pixels to calculate X'_0. In other words, we have selected a total of 32 pixels.) They were iterated M times and N times respectively, then calculated two chaotic sequences and they were denoted as x_i and y_j. Sequence x_i and y_j were used to build the "out-of-order" coordinate sequences, sequence $x'_1x'_2\ldots x'_M$ and $y'_1y'_2\ldots y'_N$. The equations are as follows:

$$x'_i = sort(unique(M \times x_i)), \tag{10}$$

$$y'_j = sort(unique(N \times y_j)), \tag{11}$$

where $unique(\cdot)$ means it will delete repetitive elements of the sequences, and $sort(\cdot)$ means it will store the pseudo random sequences. Therefore, we can get a set of chaotic coordinate sequences (x'_i, y'_j). Here, we agree on that the $P(i, j)$ is used to indicate the position of pixels in plain image P. We built the map from $P(i, j)$ to $P(x'_i, y'_j)$, and exchanged their positions from $P(1, 1)$ to $P(M, N)$. At this point, three round scrambling process is completed. The scrambling image were denoted as P'.

C. DIFFUSION

We selected the four kinds of one-dimensional chaotic maps to use on the random chaos system for the image diffusion. They are the Logistic map, the Chebyshev map, the Sine map and the Cosine map. The dynamic behavior of the nonlinear system is decided by its parameters. When the parameter μ takes the value in the Table 1, the above 4 one-dimensional maps are chaotic [15].

In order to further enhance the effect of image diffusion, we applied some algebraic transformations to the parameter μ of the Logistic map and Sine map, which made the system in chaos. The generation process is as follows:

Step 4: We entered the external double-precision $key1, key2 \in (0, 1)$ as initial values. Where $key1$ is utilized for Eq. (8) and $key2$ is used for Eq. (9). They are iterated for a certain number of times respectively. In order to make the system full divergence, abandon their previous 500 values.

Step 5: We made their 501th values as the new initial values Xl_{10}, Yl_{20} of Eq. (8) and Eq. (9), and iterated them until generating length of the two double-precision arrays

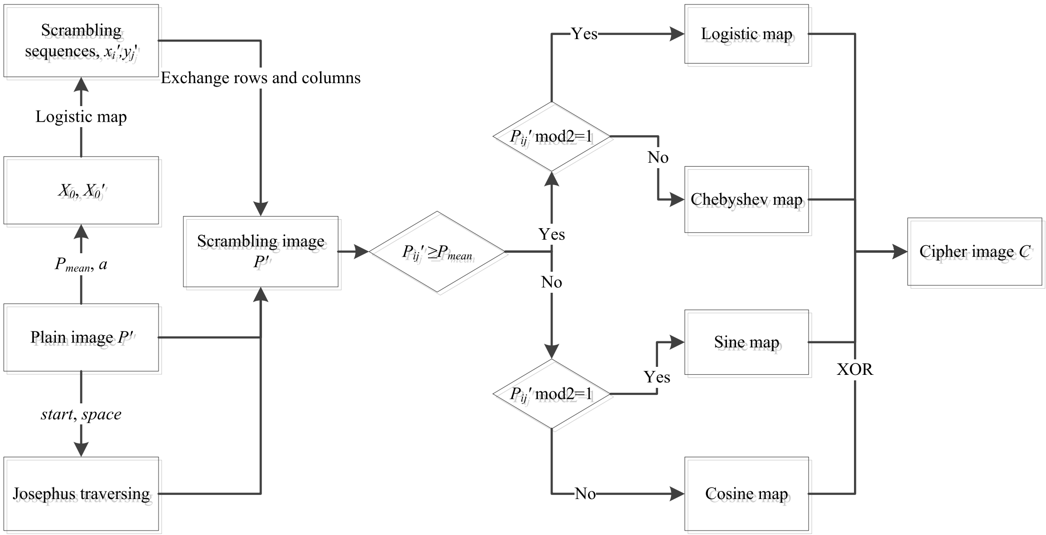


FIGURE 1. Flowchart of encryption process.

$\{Xl_{1i}\}$ and $\{Yl_{2i}\}$ are $odd1$ and $odd2$. The $odd1$ means that the total number of pixels satisfy the condition of $P'_{ij} \geq P_{mean}$ and P'_{ij} mod $2 = 1$; $odd2$ means the total number of pixels satisfy the condition of $P'_{ij} < P_{mean}$ and P'_{ij} mod $2 = 1$.

Step 6: Algebraic transformation of sequence $\{Xl_{1i}\}$ is $\{Xl'_{1i}\} = \{Xl_{1i}\} \times 0.13 + 3.87$, the control parameter $\{Xl'_{1i}\}$ of Logistic map is denoted as μ_{3i}, where $i = 1, 2, 3, \ldots, odd1$.

Step 7: Algebraic transformation of sequence $\{Yl_{2i}\}$ is $\{Yl'_{2i}\} = \{Yl_{2i}\} \times 0.13 + 0.87$, the control parameter $\{Yl'_{1i}\}$ of Sine map is denoted as μ_{5i}, where $i = 1, 2, 3, \ldots, odd2$.

Then parameters also contain the characteristics of chaos after processing.

Diffusion process is as follows:

Step 8: For the scrambling image P', choose the diffusion sequence can be described by the following equation:

$$Y(i) = \begin{cases} \mu_{3i}x(1-x), P'_{ij} \geq P_{mean}, P'_{ij} \bmod 2 = 1 \\ \cos(\mu_4 a \cos(x)), P'_{ij} \geq P_{mean}, P'_{ij} \bmod 2 = 0 \\ \mu_{5i}\sin(\pi x), P'_{ij} < P_{mean}, P'_{ij} \bmod 2 = 1 \\ \mu_6 \cos(\pi |x-0.5|), P'_{ij} < P_{mean}, P'_{ij} \bmod 2 = 0, \end{cases} \tag{12}$$

where $Y(i)$ is optional chaotic map.

Step 9: In order to modify the pixel gray-level values and crack the strong correlations between adjacent pixels of an image simultaneously, then adjacent pixels performed the XOR operation, it's described as follows:

$$\begin{cases} C_i = \text{floor}(P'_i \times Y(i) \times 1014) \text{mod} 256 \\ C'_1 = Y(1) \oplus C_1 \oplus C_{M \times N}, \quad i = 1 \\ C''_i = Y(i) \oplus C'_i \oplus C'_{i-1}, \quad i \neq 1, \end{cases} \tag{13}$$

where $i \in (1, 2, 3, \ldots, M \times N)$, C''_i is the ciphered image with the size $M \times N$ after encryption.

Decryption process is similar to the encryption process for the inverse process of the above steps. The flowchart of encryption process is shown in Fig. 1.

IV. EXPERIMENTS

In this section, we discuss the performance of the proposed algorithm. The computer configuration is 2 GHz CPU, 4 GB of memory and Microsoft Windows 10 operating system. We choose original plain images are Lena, Camera man and Peppers with the size 256 × 256. The keys are $\mu_1 = 3.96$, $\mu_2 = 3.98$, $key_1 = 0.2628$, $key_2 = 0.5$, $a = 50$, the initial values of diffusion sequences are $x_0 = 0.123$, $x_1 = 0.456$, $x_2 = 0.789$ and $x_3 = 0.666$ as keys. Fig. 2 shows the experimental results, and after decrypting we can get original plain images correctly.

The experimental results show that the performance of our proposed scheme is excellent, and the information of plain images has been completely hidden. And we can also utilize the correct key to decrypt and obtain the original plain images.

In addition, our proposed scheme can also be utilized to encrypt the color images. First, we need to decompose the color image into three grayscale images of the red, green, blue colors (R, G, B components). Next, we encrypt the three components by our algorithm with same or different keys, and get their corresponding cipher images. Finally, the three cipher images of components are recombined to get the color cipher image. We choose color plain image is Lena with the size of 256 × 256. The experimental results are also shown in Fig. 2.

V. SECURITY AND PERFORMANCE ANALYSIS

Common cryptosystem attacks include the cipher-only attack, known-plain attack, chosen-plain attack and chosen-cipher attack [25]–[29]. If a cryptosystem can resist the common four attacks, it shows good security. We analyze the security and performance of the cryptosystem, including the key space analysis, histogram analysis, correlation analysis. To evaluate the ability to resist common attacks, differential attack, known-plain and chosen-plain attacks, occlusion

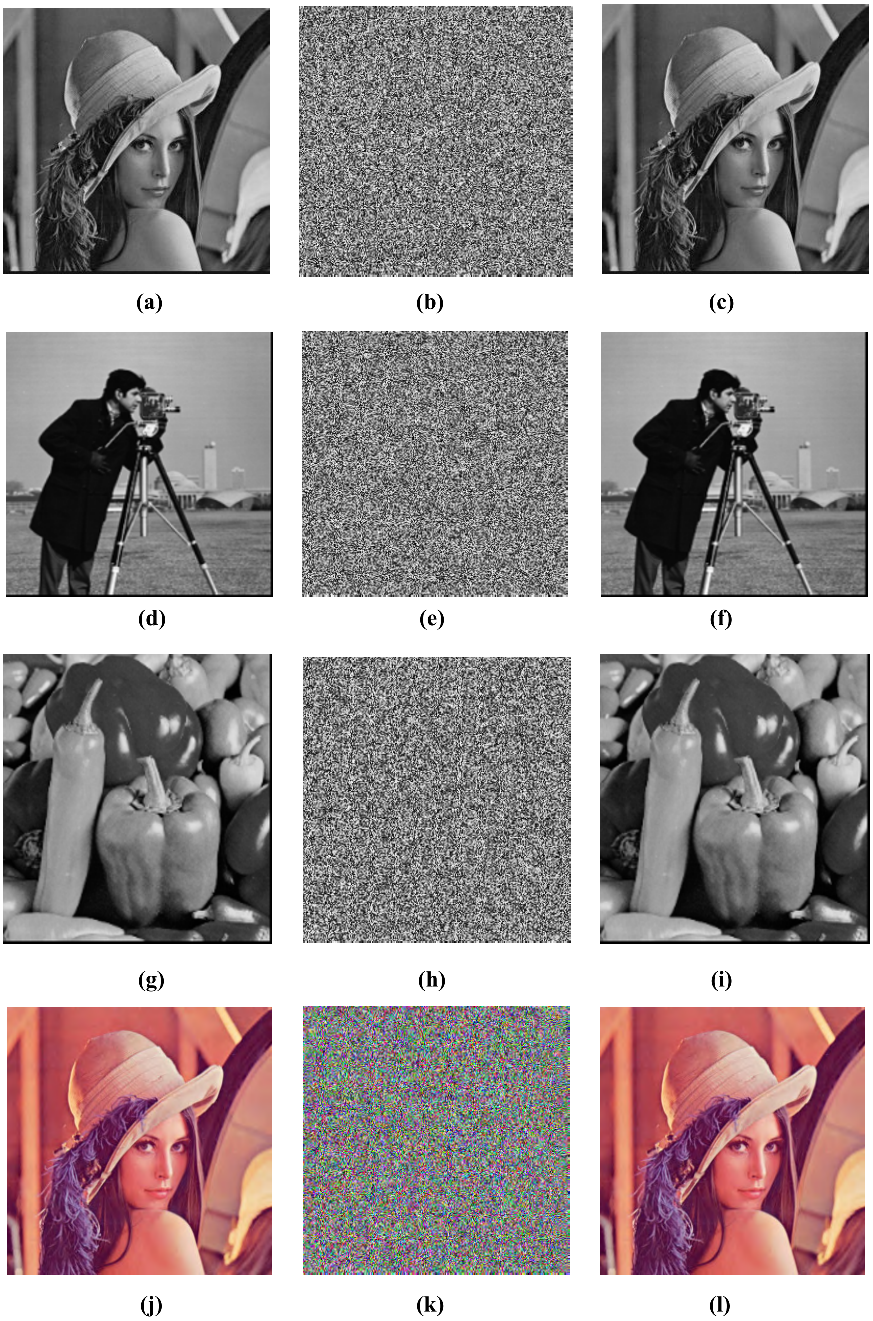
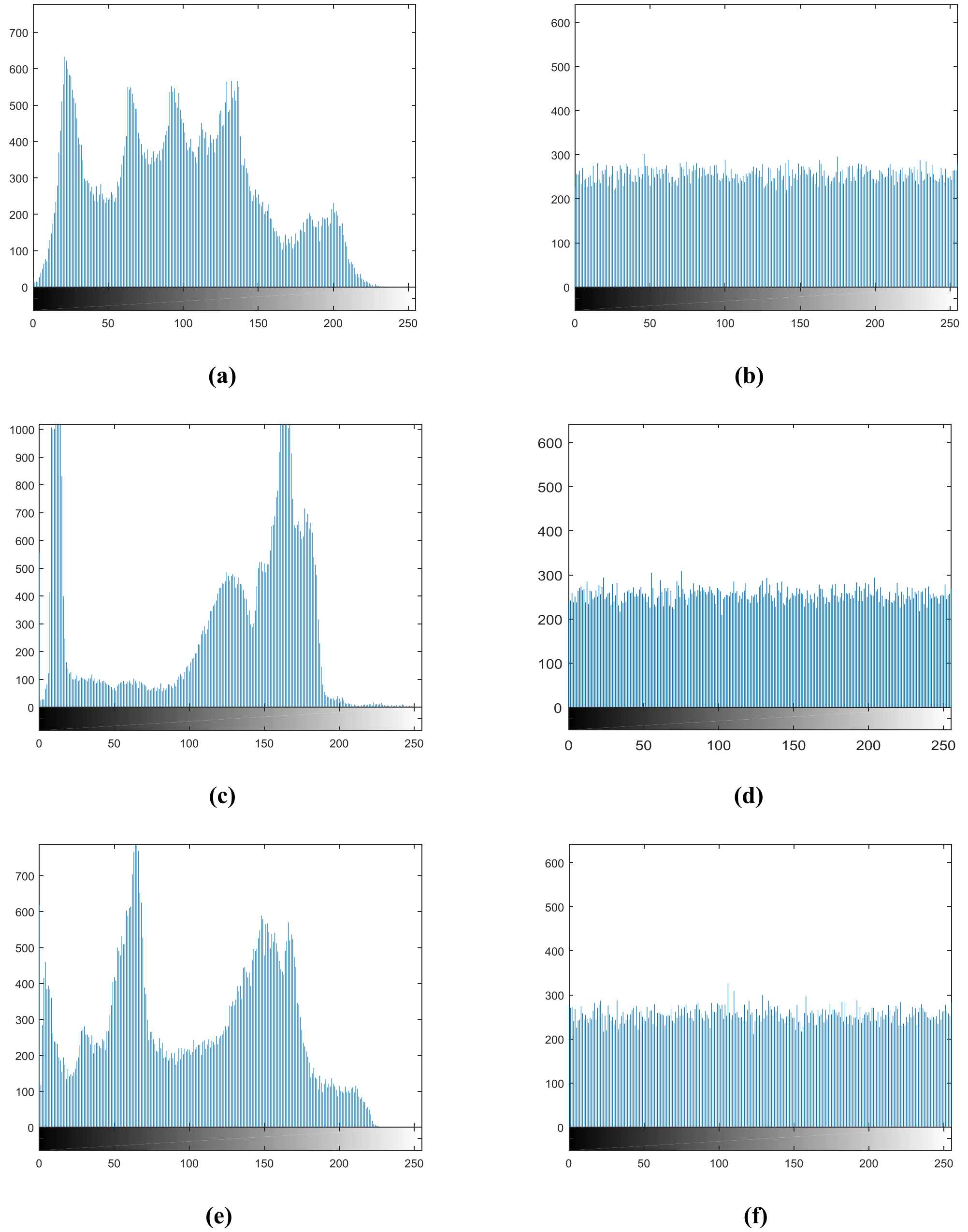


FIGURE 2. Experimental results of the proposed scheme, a plain image of Lena, b cipher image of Lena,
c decrypted image of Lena, d plain image of Camera man, e cipher image of Camera man,f decrypted image of Camera man, g plain image of Peppers, h cipher image of Peppers, i decrypted image of Peppers, j plain image of Lena, k cipher image of Lena, l decrypted image of Lena.

attack, noise attack are analyzed. in addition, sensitivity analysis and computation and complexity analysis are developed. Meanwhile, it is also accompanied by comparative experiments of other algorithms in [20]–[23].

A. KEY SPACE ANALYSIS

In order to effectively deal with all kinds of brute-force attacks, we should make the key space large enough. The size of the key space should be larger than 2^{100} to provide a high level of security [16]. The keys include: the parameter μ_1 and μ_2 of Logistic map in scrambling, their initial values key_1 and key_2, the control parameter a of Eq. (5), the initial values x_0, x_1, x_2 and x_3 of diffusion sequences. Assuming that the system accuracy is 10^{-14} and $a \in [50, 500]$, then the key space size is $4.5 \times 10^{114} \gg 2^{100}$. It's sufficiently large to resist brute-force attacks.



(a)

(b)

(c)

(d)

(e)

(f)

FIGURE 3. Histogram of plain images and cipher images, a histogram of Lena, b histogram of cipher image of Lena, c histogram of camera man, d histogram of cipher image of camera, e histogram of peppers,f histogram of cipher image of peppers.

B. HISTOGRAM ANALYSIS

The histogram of plain image has unique distribution regularity. For a good encryption scheme, the cipher image should try to erase the traces of plain image. In order to protect the information of the original image to withstand the statistical attacks, it's essential for the encrypted image to bear no statistical similarity to the original image. The histogram of the encrypted image should be uniform [17]. Then an attacker is difficult to extract statistical information from the cipher image; therefore, the algorithm can resist a chosen-plain or known-plain attack. Fig. 3 shows the histograms of plain images of Lena, camera man and peppers with the size of 256 × 256, and their corresponding histograms of cipher images. We can find that histograms of the cipher image are very uniform, and the regularity of the plain image is not obviously brought into the cipher image.

C. THE CORRELAIONS OF ADJACENT PIXELS

There is highly correlated with pixels of plain image in horizontal, vertical, or diagonal direction. So, it's necessary to crack the strong correlations between adjacent pixels of an image and improve the resistance against statistical analysis.

TABLE 2. The correlations of adjacent pixels on three directions.

Images	Plain image			Cipher image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena (256×256)	0.9721	0.9739	0.9705	-0.0029	-0.0017	0.0004
Camera man (256×256)	0.9634	0.9732	0.9449	0.0047	-0.0066	0.0031
Peppers (256×256)	0.9674	0.9710	0.9332	0.0021	0.0084	0.0007
Bird (512×512)	0.9939	0.9975	0.9936	-0.0049	-0.0005	0.0038
Finger (1024×1024)	0.9937	0.9943	0.9894	-0.0015	0.0032	0.0040

In order to test the correlations between adjacent pixels (including horizontal, vertical and diagonal), we randomly selected 10000 pairs of adjacent pixels from an image. Then we calculate the correlation of each pair using the following equations [18, 19]:

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{14}$$

where,

$$\begin{aligned}
\operatorname{cov}(x, y) &= \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)),\\
D(x) &= \frac{1}{N}\sum_{i+1}^{N}(x_i - E(x))^2,\\
E(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i.
\end{aligned} \tag{15}$$

Table 2 shows the correlations of plain and cipher image adjacent pixels of Lena for horizontal, vertical and diagonal directions. Both Table 2 and Fig. 4 show that our proposed scheme has effectively removed the correlation of adjacent pixels, therefore it has strong strength against statistical attacks.

D. DIFFERENTIAL ATTACK

The encryption scheme is based on one-time pad, which can make differential attack ineffective, for the keys are dynamically generated from the proposed scheme and plain image. The differential attack mechanism is to change one bit or one pixel in the plain image, and then to encrypt and to find out the difference two cipher images. It has two indicators: the number of pixels change rate (NPCR) and unified average changing intensity (UACI) [13], [24]. NPCR and UACI are usually applied to examine the performance of resisting against differential attack. They can be calculated as follows:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100, \tag{16}$$

$$UACI = \frac{1}{W \times H}[\sum_{i,j}\frac{|c_1(i,j) - c_2(i,j)|}{255}] \times 100. \tag{17}$$

Where c_1 and c_2 are two cipher images with the size $M \times N$. If $c_1(i, j) \neq c_2(i, j)$, then $D(i, j) = 1$; otherwise, $D(i, j) = 0$.

TABLE 3. NPCRs and UACIs of the cipher image.

Test images	NPCR(%)	UACI(%)
Lena (256×256)	99.5986	33.4561
Camera man (256×256)	99.5590	33.4439
Peppers (256×256)	99.5803	33.4324

TABLE 4. Information entropies.

Test image	Plain image	Cipher image
Lena (256×256)	7.5755	7.9971
Camera man (256×256)	7.0701	7.9971
Peppers (256×256)	7.5819	7.9968
Bird (512×512)	7.2319	7.9973
Finger (1024×1024)	6.3062	7.9970

Here we change one bit in Lena, Camera man and Peppers respectively, the results are shown in Table 3. In general, the values of NPCR and UACI must approach 99.6093% and 33.4635% respectively. We can found that their values are satisfactory. Therefore the new scheme is sensitive to plain image and it can make the differential attack ineffective.

E. INFORMATION ENTROPY

The information entropy is used to evaluate the randomness of an image. If an image has excellent random property, it means that the information entropy score is close to the maximum information entropy value [18]. Its value can be calculated by the following equation:

$$H(s) = \sum_{i=0}^{2^L-1} p(s_i)\log_2\frac{1}{p(s_i)}, \tag{18}$$

where L is the gray level, $p(s_i)$ denotes the probability of symbol s_i. For a gray-scale image with a data range of [0, 255],

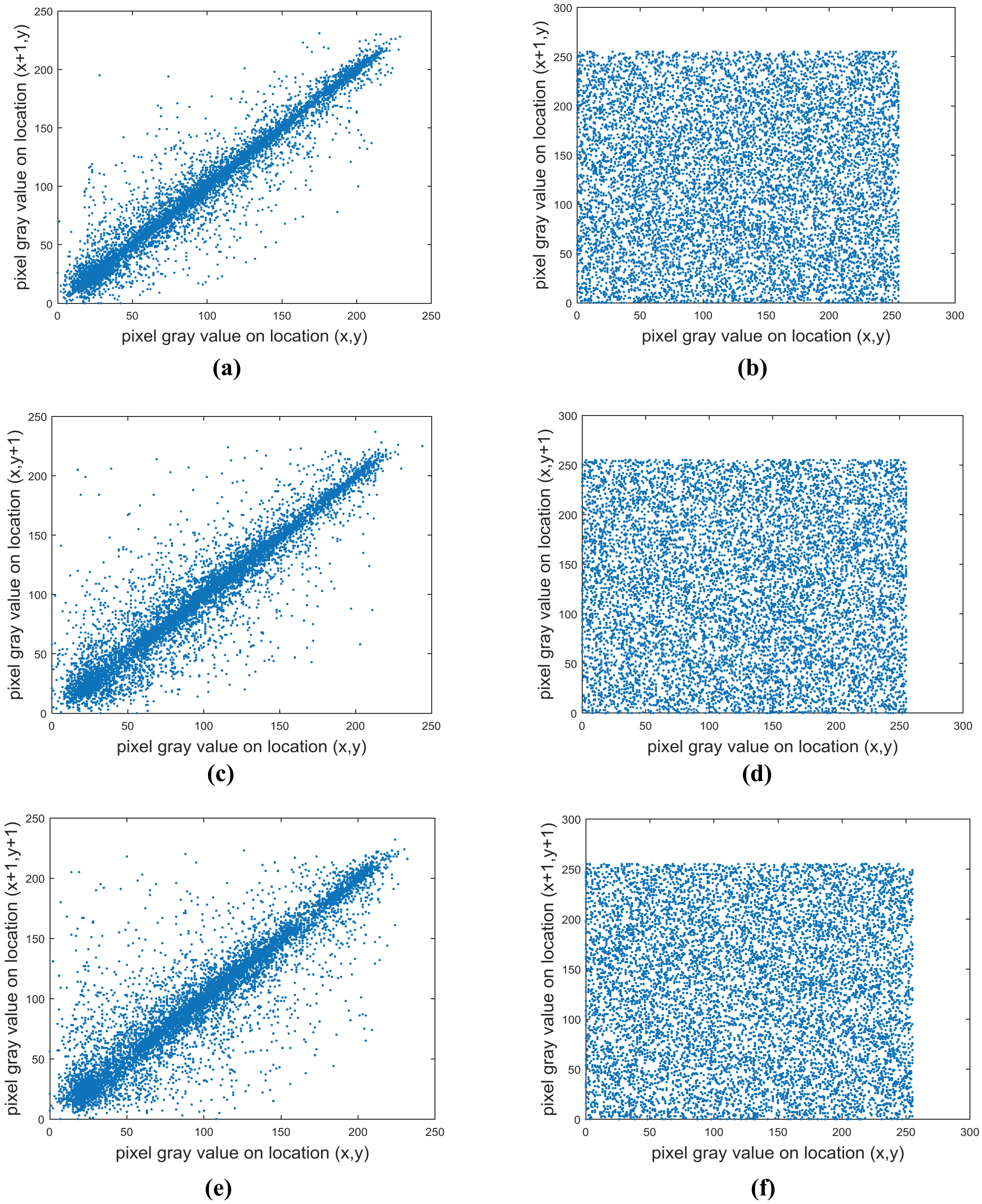


FIGURE 4. The correlations of two adjacent pixels, a horizontal correlation in plain image, b horizontal correlation in cipher image, c vertical correlation in plain image, d vertical correlation in cipher image, e diagonal correlation in plain image, f diagonal correlation in cipher image.

its theoretical of information entropy is 8, it means confused enough for the cipher image.

Table 4 lists the information entropies of the plain and cipher images. We can found that the information entropies are close to 8 after encryption. It means that our proposed scheme have better random distributions.

F. KNOWN-PLAIN AND CHOSEN-PLAIN ATTACKS

An excellent cryptosystem should be able to resist the known-plain and chosen-plain attacks. We discuss the performance of our algorithm to resist these attacks in this section. First, a novel method of selecting initial value is designed as described in Section 3.1; in order to achieve the same effect as hash functions, the choice of initial value depends on the parameter a and is also related to the plain images. If the plain image is changed, the initial value will be also changed; even for the same plain image, the initial value is different if the parameter is a changed. Thus, our proposed scheme has a high dependency to the plain image and can resist the known-plain and chosen-plain attacks.

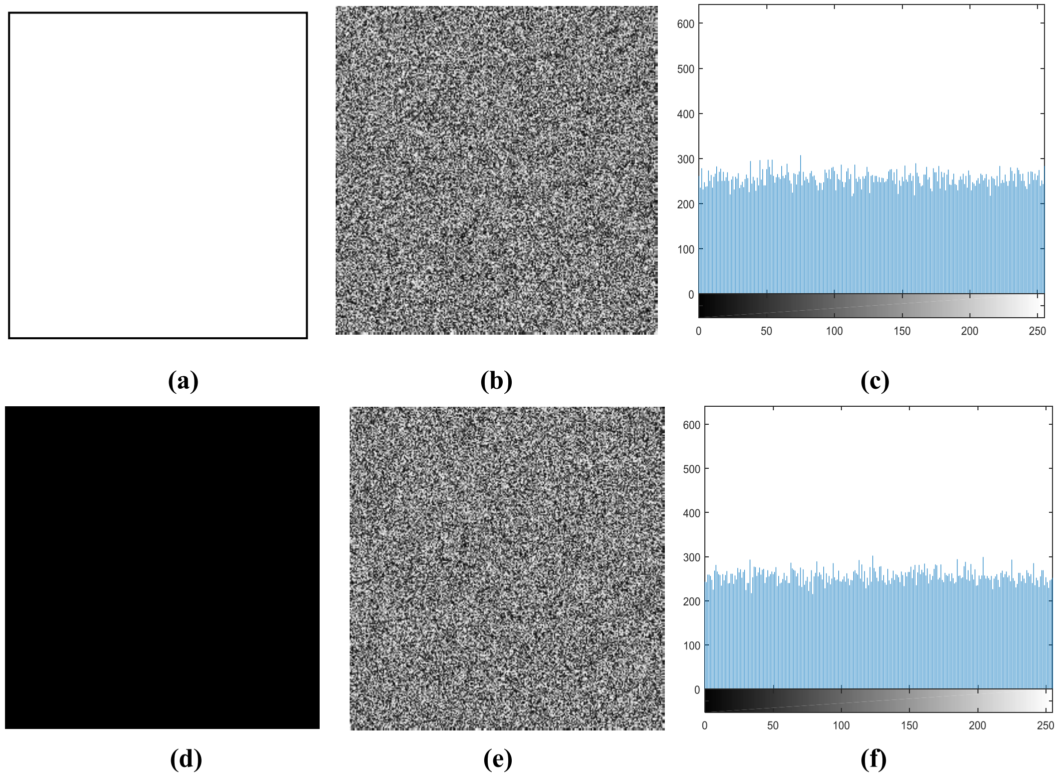


FIGURE 5. Experimental results of all black and white, a plain image of all black, b cipher image of all black, c histogram of the cipher image, d plain image of all white, e cipher image of all white, f histogram of the cipher image.

TABLE 5. The correlation coefficients and information entropies of the plain and cipher images of all black and white.

Images	Entropies	Correlation coefficients		
		Horizontal	Vertical	Diagonal
All black	0	--	--	--
Cipher of all black	7.9974	0.0055	-0.0009	-0.0039
All white	0	--	--	--
Cipher of all white	7.9970	0.0036	-0.0003	-0.0025

Sometimes, attackers choose some special plain images, such as all black or white images. Then, the equivalent keys of the algorithm are obtained, it makes cryptosystem insecurity. We utilize all black and all white images as plain images with the size 256 × 256, and corresponding cipher images and histograms are shown in Fig. 5. The correlation coefficients and information entropies of the plain and cipher images of all black and white are illustrated in Table 5. From the experimental results, we can conclude that our proposed scheme can resist the known-plain and chosen-plain attacks.

G. OCCLUSION ATTACK

When the images are transmitted in the network, it may bring data lost. In this section, we analyze the performance of our algorithm against occlusion attack. Occlusion attack is utilized to test the ability to recover from cipher images to plain images when the data is lost. Here, we also utilize the Peak Signal-to-Noise Ratio (PSNR) to test the quality of the attacked encrypted image. It can be described as follows:

$$PSNR = 10 \times \log_{10}(\frac{255 \times 255}{MSE})(dB), \tag{19}$$

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\|I_1(i,j) - I_2(i,j)\|^2 . \tag{20}$$

Where *MSE* is the mean square error value between the decrypted image $I_2(i, j)$ and the plain image $I_1(i, j)$. m and n represent the length and width of the image, respectively.

Fig. 6 shows the experimental results of data loss attacks to the cipher images of Lena with different occlusions and corresponding decrypted images. The cipher images are with

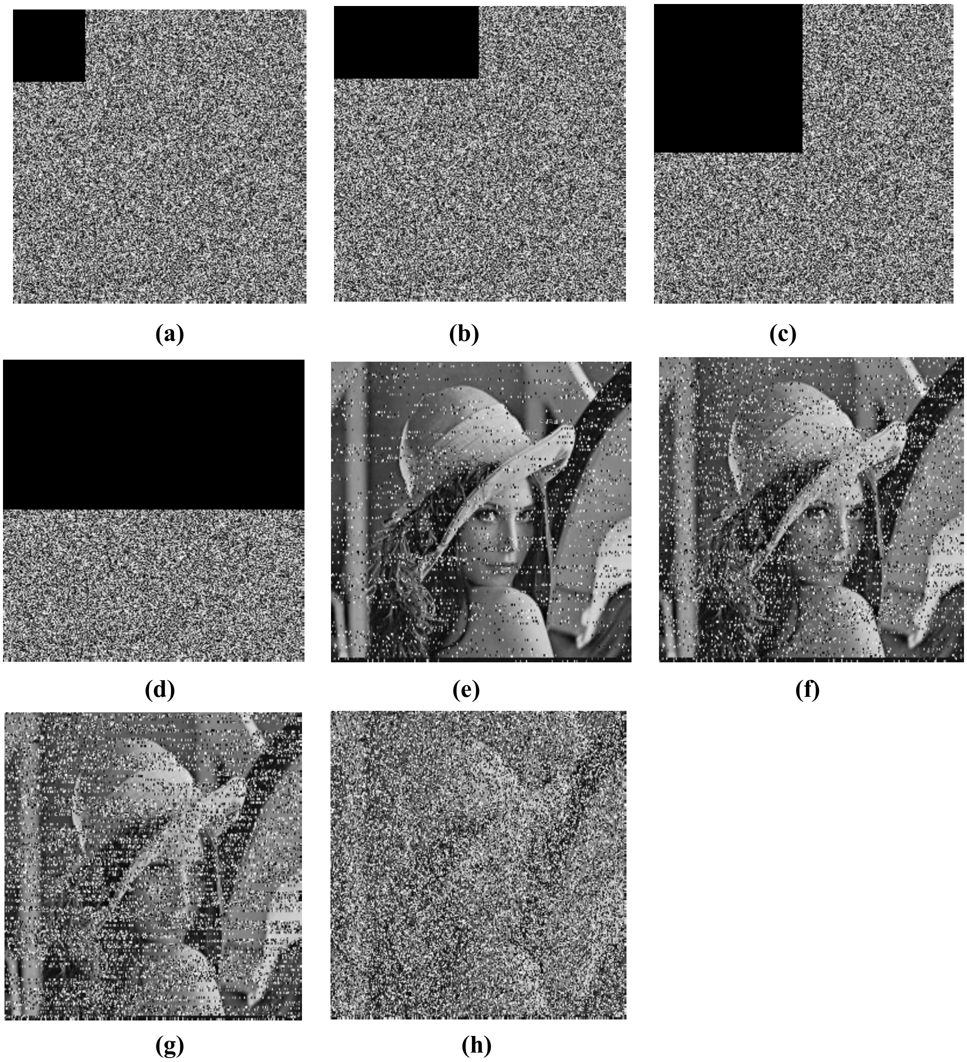


FIGURE 6. Occlusion attack analysis results, a cipher image with 1/16 occlusion, b cipher image with 1/8 occlusion, c cipher image with 1/4 occlusion, d cipher image with 1/2 occlusion; e,f, g and h are the corresponding decrypted images.

TABLE 6. The quantitative results of resisting occlusion attack.

Occlusion	MSE	PSNR	NPCR(%)	UACI(%)
1/16	10.21	38.04	12.08	3.752
1/8	20.07	35.11	23.33	7.157
1/4	37.26	32.42	43.58	13.42
1/2	65.45	29.97	74.63	22.97

1/16, 1/8, 1/4, 1/2 occlusion. And Table 6 lists the quantitative results of resisting occlusion attack. The quality of the decrypted images decreases as the occlusion size increases. Obviously, we can still identify the plain information from the decrypted image even if the data is lost. Therefore, our proposed scheme has high robustness against occlusion attack.

H. RESISTING NOISE ATTACK ANALYSIS

In real transmission channels, there are usually noise effects on plain images. Noise attack is also a method to verify the robustness of a cryptosystem. There are many kinds of noise, such as Gaussian noise, uniform noise and salt-and-pepper noise. In considering of the impact of noise on the plain image, this section utilizes Gaussian noise to test.

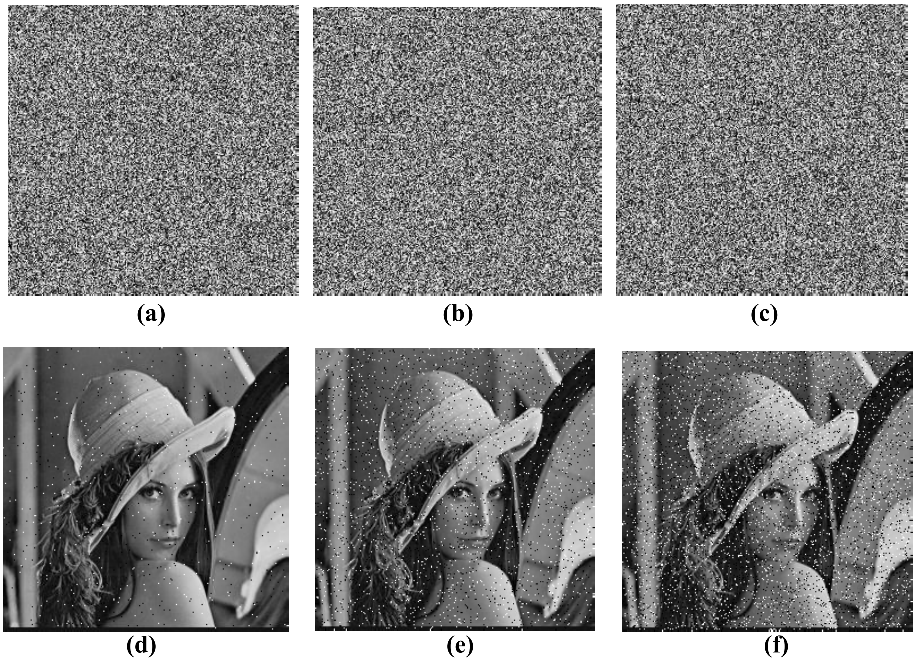


FIGURE 7. Noise attack analysis results, a cipher image under the intensity of 0.01, b cipher image under the intensity of 0.05, c cipher image under the intensity of 0.1; d, e and f are the corresponding decrypted images.

TABLE 7. The quantitative results of resisting noise attack.

Intensity	MSE	PSNR	NPCR(%)	UACI(%)
0.01	87.98	28.69	99.61	30.99
0.05	88.48	28.66	99.61	31.79
0.1	90.40	28.57	99.58	32.48

We add salt-and-pepper noises with different intensities into the plain images, and use correct keys to decrypt the images. Fig. 7 illustrates the experimental results that plain images of Lena with noise intensities of 0.01, 0.05 and 0.1 and corresponding decrypted images. And MSE, PSNR, NPCR and UACI are also listed in Table 7. From the figure and table, we can find that the decrypted images can still be identified despite some noise interference, even if the noise intensity reaches 0.1. It means that our proposed scheme can resist the noise attack.

I. SENSITIVITY ANALYSIS FOR KEYS AND THE PLAIN IMAGES

A good encryption algorithm should be sensitive to the key and plain image, even if just a bit of plain image has changed, the corresponding cipher image should become almost different completely. The sensitivity for plain images has been explained in Section 5.4, experimental results show that our algorithm is very sensitive to the plain image. We only discuss the sensitivity for keys in this section.

Fig. 8 shows the key sensitivity experimental results. We used primary keys (denoted as K_1) to encrypt the plain image of Lena in Fig. 8(a) to obtain the encrypted image (E_1) in Fig. 8(b). And then we made minor change to the key as $key1 = 0.2628 + 10^{-14}$, and others remain unchanged (they are denoted as K_2). The K_2 is used to encrypt the same plain image in Fig. 8(a), which will generate another encrypted image (E_2) in Fig. 8(c). The difference $|E_1 - E_2|$ of pixel-to-pixel in Fig. 8(d) shows that a minor change of the security key will lead to a significant change in the encrypted image.

We made minor change to the key as $x_0 = 0.123 + 10^{-14}$(denoted as K_3) in the decryption process. The K_1 and K_3 are used respectively to get the plain image from the encrypted image E_1 in Fig. 8(b). Fig. 8(e) and (f) show the decryption images. We can found that even there is a subtle change to the key will lead to the failure of decryption image. It's too difficult to get any useful information about plain image from the failure of decryption image. Thus, the proposed scheme is sensitive to the key in both the encryption and decryption processes.

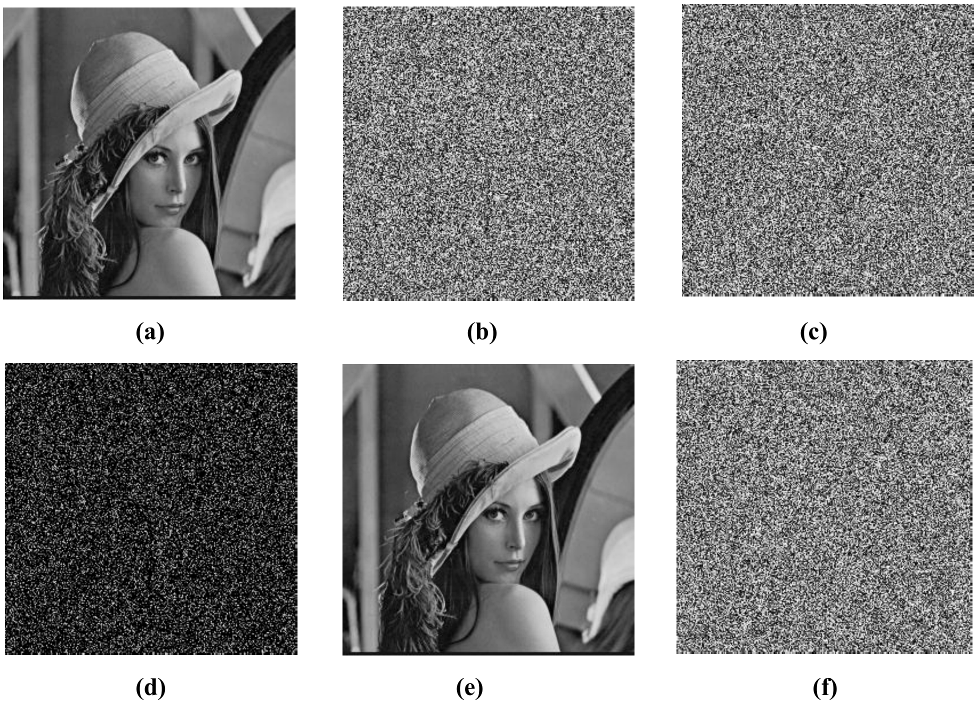


FIGURE 8. The key sensitivity experimental results for the encryption and decryption processes, a the plain image, b the encrypted image E_1 with the key set K_1, c the encrypted image E_2 with the key set K_2, d the pixel-to-pixel difference $|E_1 - E_2|$, e the decrypted image from E_1 using the correct key set K_1, f the decrypted image from E_1 using an incorrect key set K_3.

TABLE 8. Performance of the proposed scheme and other methods for Lena in size 256 × 256.

Schemes	Correlation coefficient			NPCR	UACI	Entropy
	Horizontal	Vertical	Diagonal			
Ours	-0.0029	-0.0017	0.0004	99.5986	33.4561	7.9971
Ref. [20]	-0.0074	0.0069	-0.0191	99.5040	31.6551	7.9963
Ref. [21]	0.0621	0.0031	0.0025	99.5064	32.2368	--
Ref. [22]	-0.0063	0.0095	0.0089	99.4602	37.6389	7.9974
Ref. [23]	0.0008	0.0016	0.0115	99.3011	34.5754	7.9970

J. COMPUTION AND COMPLEXITY ANALYSIS

The complexity of the proposed scheme is mainly dependent on computation of the floating point number of scrambling and diffusion. There are three-round scrambling process and one-round diffusion process. In the scrambling process, one-round Josephus traversing needs $\Theta(M \times N)$ iterations of pixel operations, two-round scrambling needs $\Theta(2 \times M \times N)$ iterations of chaotic sequences to move pixels; as for the diffusion process, it needs $\Theta(M \times N)$ iterations of multiplying floating point numbers. Thus, the computational complexity of our proposed scheme is $\Theta(4 \times M \times N)$. The method in [22] needs $\Theta(18 \times M \times N)$ iterations to encrypt image.

Regardless of the security considerations, some other aspects on image encryption are also important, such as the running speed for the real-time internet applications. Encryption speed can reflect the practicability of the scheme. The environment of development is Windows 10 operating system, 4.00GB RAM, Intel (R) Core (TM) i5-2410M CPU @ 2.30GHz and utilizing MATLAB R2015b. Test image with size of 256 × 256 is adopted to conduct the experiments. Mean execution time is 1.243s and mean speed is 0.051 MB/s. This paper is to propose a more secure image encryption algorithm, rather than the specific implementation. Thus, this result doesn't violate the original intention.

K. PERFORMANCE COMPARISONS WITH OTHER SCHEMES

Table 8 shows the performance of our proposed scheme and other schemes for Lena with the size 256 × 256. Comparison analysis of correlation coefficient, NPCR, UACI and entropy are listed in this table. From the above analysis, our scheme achieves low correlation values, better NPCR, UACI and entropy than other schemes in [20]–[23]. It has high sensitive to keys and plain images, and can also resist known-plain and chosen-plain attacks, occlusion attack and noise attack. Therefore, our scheme has better performance than other images encryption schemes.

VI. CONCLUSION

We proposes a novel chaotic image encryption scheme based on Josephus traversing and mixed chaotic map in this paper, which consists of three processes. The first part is a key stream generator based on a new proposed scheme of chaotic systems. The initial values and parameters are dependent on both the new scheme and plain image. The second process employed the Josephus traversing in scrambling, then the rows and columns of pixels are exchanged according to certain rules; finally, we used chaotic coordinates to exchange the positions of each pixel, which are generated by two logistic maps. The third process employed the image data and four chaotic maps in order to modify the pixel gray-level values and crack the strong correlations between adjacent pixels of an image simultaneously. Experiential results and security analysis show that the proposed scheme has better performance and can be applied for image encryption and transmission.

REFERENCES

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

[2] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Process.*, vol. 97, no. 7, pp. 172–182, Apr. 2014.

[3] X. Wang and H.-L. Zhang, "A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems," *Nonlinear Dyn.*, vol. 83, nos. 1–2, pp. 333–346, Jan. 2016.

[4] X.-Y. Wang and Y.-Q. Zhang, "A new image encryption algorithm based on non-adjacent coupled map lattices," *Appl. Soft Comput.*, vol. 26, no. 1, pp. 10–20, Jan. 2015.

[5] 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.

[6] M. J. Rostami, S. Saryazdi, H. Nezamabadi-pour, and A. Shahba, "Chaos-based image encryption using sum operation modulo 4 and 256," *IETE J. Res.*, vol. 62, no. 2, pp. 179–188, Mar. 2016.

[7] H. Khanzadi, M. Eshghi, and S. E. Borujeni, "Design and FPGA implementation of a *pseudo* random bit generator using chaotic maps," *IETE J. Res.*, vol. 59, no. 1, pp. 63–73, Jan./Feb. 2013.

[8] D. Coppersmith, "The data encryption standard (DES) and its strength against attacks," *IBM J. Res. Develop.*, vol. 38, no. 3, pp. 243–250, May 1994.

[9] H. C. Williams, "A modification of the RSA public-key encryption procedure," *IEEE Trans. Inf. Theory*, vol. IT-26, no. 6, pp. 726–729, Nov. 1980.

[10] X.-Y. Wang and Y.-Q. Zhang, "Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation," *Nonlinear Dyn.*, vol. 77, no. 3, pp. 687–698, Aug. 2014.

[11] J.-S. Guo and C.-H. Jin, "An attack with known image to an image cryptosystem based on general cat map," *J. China Inst. Commun.*, vol. 26, no. 2, pp. 131–135, Apr. 2005.

[12] J. Wu and L. Tu, "An image encryption algorithm based on Josephus traversing and position disordering," in *Proc. Int. Conf. Cybern. Inform.*, vol. 163. New York, NY, USA, Apr. 2013, pp. 1941–1946.

[13] G. Yang, H. Jin, and N. Bai, "Image encryption using the chaotic Josephus matrix," *Math. Problems Eng.*, vol. 2014, no. 1, pp. 1–13, Mar. 2014.

[14] J. A. Koupaei, S. M. M. Hosseini, and F. M. M. Ghaini, "A new optimization algorithm based on chaotic maps and golden section search method," *Eng. Appl. Artif. Intell.*, vol. 50, pp. 201–214, Apr. 2016.

[15] J. Scharinger, "Fast encryption of image data using chaotic Kolmogorov flows," *Electron Imag.*, vol. 7, no. 2, pp. 318–325, Apr. 1998.

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

[17] B. Norouzi and S. Mirzakuchaki, "A fast color image encryption algorithm based on hyper-chaotic systems," *Nonlinear Dyn.*, vol. 78, no. 2, pp. 995–1015, Oct. 2014.

[18] M. Brindha and N. A. Gounden, "A chaos based image encryption and lossless compression algorithm using hash table and Chinese Remainder Theorem," *Appl. Soft Comput.*, vol. 40, pp. 379–390, Mar. 2016.

[19] M. Ghebleh, A. Kanso, and H. Noura, "An image encryption scheme based on irregularly decimated chaotic maps," *Signal Process. Image Commun.*, vol. 29, no. 5, pp. 618–627, May 2014.

[20] Y. Guo, L.-P. Shao, and L. Yang, "Bit-level image encryption algorithm based on Josephus and Henon chaotic map," *Appl. Res. Comput.*, vol. 32, no. 4, pp. 1131–1137, Apr. 2015.

[21] Z.-L. Zhu, W. Zhang, K.-W. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Inf. Sci.*, vol. 181, no. 6, pp. 1171–1186, Mar. 2011.

[22] A. Bakhshandeh and Z. Eslami, "An authenticated image encryption scheme based on chaotic maps and memory cellular automata," *Opt. Lasers Eng.*, vol. 51, no. 6, pp. 665–673, Jun. 2013.

[23] R. S. Ye, "A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism," *Opt. Commun.*, vol. 284, no. 22, pp. 5290–5298, Oct. 2011.

[24] W. Ochs and W. Bayer, "Quantum States with Maximum Information Entropy. I.," *Zeitschrift Naturforschung A*, vol. 28, no. 5, pp. 693–701, 2014.

[25] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Appl. Soft Comput.*, vol. 11, no. 1, pp. 514–522, Jan. 2011.

[26] Y. Zhang and Y. Tang, "A plaintext-related image encryption algorithm based on chaos," *Multimedia Tools Appl.*, vol. 77, no. 6, pp. 6647–6669, Mar. 2018.

[27] K. Zhan, D. Wei, J. Shi, and J. Yu, "Cross-utilizing hyperchaotic and DNA sequences for image encryption," *J. Electron. Imag.*, vol. 26, no. 1, p. 013021, Jan. 2017.

[28] B. Ramalingam, D. Ravichandran, A. A. Annadurai, A. Rengarajan, and J. B. B. Rayappan, "Chaos triggered image encryption—A reconfigurable security solution," in *Multimedia Tools & Applications*. 2017, pp. 1–24.

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

XINGYUAN WANG received the Ph.D. degree in computer software and theory from Northeast University, China, in 1999. From 1999 to 2001, he was a Post-Doctoral Researcher with Northeast University. He is currently a Professor with Dalian Maritime University and the Dalian University of Technology, China. He has authored or co-authored over 410 papers indexed by SCI, his SCI papers have been cited over 6000 times (H-index of 58), two papers and 12 papers, respectively, are selected as the hot papers and highly cited papers of the ESI. His research interests include image processing and complex networks. He was selected as an Elsevier Chinese Highly Cited Scholar from 2014 to 2017. His eight international invention patents are authorized. He was a recipient of the Liaoning Province Natural Science First Prize 1 item (The only complete person) and the Ministry of Education of Natural Science Second Prize 1 item (first complete person).

XIAOQIANG ZHU received the M.E. degree from the School of Electronic and Information Engineering, Dalian University of Technology, Dalian, where he is currently pursuing the B.S. degree. His research interest includes image encryption.

YINGQIAN ZHANG received the Ph.D. degree from the School of Electronic and Information Engineering, Dalian University of Technology, Dalian, China, where he received another Ph.D. degree in computer application in 2014. From 2014 to 2016, he was a Professor with the City Institue, Dalian University of Technology. He is currently a Professor with the Xiamen University Tan Kah Kee College, China. He has authored or co-authored over 30 scientific papers in journals and proceedings. His research interests include nonlinear dynamics, cryptography, and image processing.