IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 19, 2020, accepted April 15, 2020, date of publication April 20, 2020, date of current version May 6, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2988880

Image Encryption Based on Improved Lorenz System

CHENGYE ZOU[1], QIANG ZHANG[2,3], XIAOPENG WEI[3], AND CHANJUAN LIU[2], (Member, IEEE)

[1]School of Mathematics and Statistics, Anyang Normal University, Anyang 455000, China
[2]Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116024, China
[3]Key Laboratory of Advanced and Intelligent Computing, Dalian University, Ministry of Education, Dalian 116622, China

Corresponding author: Qiang Zhang (zhangq@dlut.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61425002, Grant 61751203, and Grant 61772100, in part by the Program for Changjiang Scholars and Innovative Research Team in University under Grant IRT_15R07, and in part by the Program for Liaoning Innovative Research Team in University under Grant LT2015002.

ABSTRACT This paper proposes a new method to strengthen the nonlinear kinetic complexity and ergodicity of Lorenz system. Through the analysis of auto-correlation, frequency distribution, approximate entropy and information entropy, the improved Lorenz system has better dynamical properties than Lorenz system. According to NIST-800-22 test results, the chaotic sequences generated from proposed system have passed all random tests, which denotes that the improved Lorenz system is applicable to chaotic encryption. Once the plaintext image is color, the size of scramble image is three times as big as plaintext image, so that a lot more pixel information participant in permutation and diffusion to get better encryption results. Simulation results show that the image encryption scheme provides good security and high capacity to resist common attacks.

INDEX TERMS Ergodicity, image encryption, NIST-800-22 test, Lorenz system, improved Lorenz system.

I. INTRODUCTION

Since Lorenz proposed the first two scrolls system in 1963 [1], chaotic systems have attracted attention of scientific community due to their vast applications in many areas such as physics, biology, complex networks, economics and so on [2]–[6]. Non-predictability, ergodicity, random-like behavior, and high sensitivity to initial conditions are the main characteristics of chaotic systems, which can be used in encryption and secure communication [7]–[20]. Generally, diffusion and permutation are two significant steps in chaotic image encryption. In permutation phase, strong correlations between adjacent pixels are masked. In the diffusion phase, pixel values are replaced by mutual diffusion among different pixels, so that the important and valid information of plaintext-image are concealed. In many proposed chaotic image encryption algorithms, Lorenz system as pseudo random number generator (PRNG) to generate chaotic sequences. Obaida *et al.* applied Lorenz system to digital image encryption, and embedded hash value of the plain image in the proposed cryptosystem to increase the security level [21]. Amir has proposed a robust image encryption scheme for low profile applications based on chaotic Lorenz system [22]. Younas and Khan combined inverse left almost semi group with Lorenz system in image encryption scheme to obtain better confusion and diffusion effect through a modern substitution-permutation network [23]. Hussain *et al.* have designed a cryptographically strong systems based on proposed S-boxes and Lorenz chaotic system [24]. Girdhar and Kumar hybridized Lorenz system and Rossler system to generate the random sequence, and applied the rules of DNA cryptosystem to encrypt image [25].

However, dimension, complexity and ergodicity of Lorenz system are limited, therefore the original Lorenz system is improved or modified in many investigations to achieve better encryption results. Kaur and Kumar generated six random sequences by Lorenz-like chaotic system with varying bifurcation parameter [26]. It is obvious that, hyper-chaotic systems possess more complex dynamical characteristics and higher randomness than low-dimensional chaotic systems, so that hyper-Lorenz system is more applicable to image encryption [27]–[29]. Usman *et al.* proposed Walsh

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

compressed quantum spinning chaotic Lorenz system to satisfy the need of fast computing and quantum encryption [27]. Ran *et al.* have coupled two Lorenz system and obtained hyper-Lorenz system, which is injected impulse during the iteration process in order to counter the degeneration of dynamics [30].

In this paper, the motivations of our work are included as follows:

(1) In order to strengthen the complexity and ergodicity of Lorenz system, we have added delay coupling and mod function to Lorenz system, and enhanced complexity and ergodicity of Lorenz system effectively according to the analysis of auto correlation, frequency distribution, approximate entropy and information entropy.

(2) To avoid attacker gain the random value of the proposed system through the selection of different plaintext images, the keys derive from plaintext image. Furthermore, the key space can be enlarged greatly by increase of key number.

(3) To make the information of plaintext image participant the permutation and diffusion more sufficiently, the scramble image has three times the size of plaintext image for color plaintext image. This permutation operation will not increase the burden of transmission or storage, because we just transfer the information of R, B, G components of plaintext image to the scramble image. If the the plaintext image is gray, scramble image has the same size as plaintext image. The experimental results showed that our proposed encryption scheme has high security.

The rest of the paper is organized as follows: Section II presents basic mechanism and analysis of improved Lorenz system. Our encryption and decryption algorithm are depicted in Section III. Simulation results and security analyses are provided in Section IV and V respectively. Section VI and VII present the statistical and robust analysis respectively. Finally, this paper is concluded in Section VIII.

II. IMPROVED LORENZ SYSTEM

A. BASIC MECHANISM

Lorenz system is one of the most widely used chaotic system, especially in image encryption. The mathematical model of Lorenz system can be described as follow:

$$\begin{cases} \dfrac{dx(t)}{dt} = a(y(t) - x(t)) \\ \dfrac{dy(t)}{dt} = bx(t) - x(t)z(t) - y(t) \\ \dfrac{dz(t)}{dt} = x(t)y(t) - cz(t) \end{cases} \tag{1}$$

where chaos of Eq. (1) is determined by the parameters a, b and c. As shown in Figure 1, we modified the form of Eq. (1) as:

$$\begin{cases} \dfrac{\mathrm{d}x(t)}{\mathrm{d}t} = a\left(\hat{y}(t) - \hat{x}(t)\right) \\ \dfrac{\mathrm{d}y(t)}{\mathrm{d}t} = b\hat{x}(t) - \hat{x}(t)\hat{z}(t) - \hat{y}(t) \\ \dfrac{\mathrm{d}z(t)}{\mathrm{d}t} = \hat{x}(t)\hat{y}(t) - c\hat{z}(t) \end{cases} \tag{2}$$

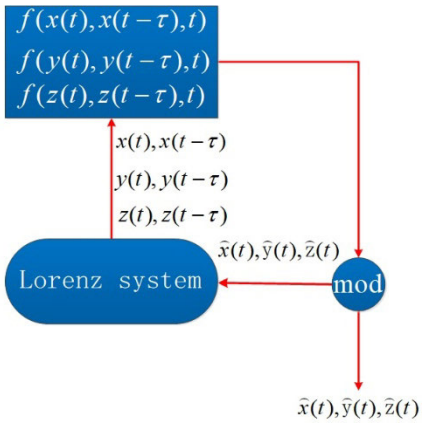


FIGURE 1. Mechanism of our proposed system.

The form of $\hat{x}(t)$, $\hat{y}(t)$ and $\hat{z}(t)$ is designed as

$$\begin{cases} \hat{x}(t) = (\bmod (f(x(t), x(t-\tau), t)), 1) \\ \hat{y}(t) = (\bmod (f(y(t), y(t-\tau), t)), 1) \\ \hat{z}(t) = (\bmod (f(z(t), z(t-\tau), t)), 1) \end{cases} \tag{3}$$

where the function $f(x(t), x(t-\tau), t)$, $f(y(t), y(t-\tau), t)$ and $f(z(t), z(t-\tau), t)$ are described as Eq. (4), and $\tau > 0$ is delayed time.

$$\begin{cases} f(x(t), x(t-\tau), t) = \dfrac{x(t) + x(t-\tau)}{2} + \sin(t) \\ f(y(t), y(t-\tau), t) = \dfrac{y(t) + y(t-\tau)}{2} + \sin(t) \\ f(z(t), z(t-\tau), t) = \dfrac{z(t) + z(t-\tau)}{2} + \sin(t) \end{cases} \tag{4}$$

where $\hat{x}(t)$, $\hat{y}(t)$ and $\hat{z}(t)$ are output sequences.

B. EXPERIMENT RESULTS

In experiment, the initial values of Lorenz system are fixed as $x_0 = 0.01$, $y_0 = 0.02$ and $z_0 = 0.02$. The initial values of improved system are the same as Lorenz system. Taking parameters $a = 20$, $b = 50$ and $c = 8$. Delayed time τ is fixed as $\tau = 1$. As shown in Figure 2, our proposed system can break the two scrolls attractor structure totally and make the attractor as the noise-like pattern, which denotes that proposed system has better ergodicity than Lorenz system. As shown in Figure 3, temporal evolution of proposed system oscillates more seriously than Lorenz system. The trajectories of improved system are random-like and ergodic with no apparent cycle in the phase space.

C. APPROXIMATE ENTROPY

The complexity of time series can be measured by approximate entropy (AE) [31], given a time-series of data $\{u(i), i = 1, 2, \cdots, N\}$, reconstruct this series as:

$$X_i = \{u(i), u(i+1), \cdots, u(i+m-1)\}, \quad i = 1, 2, \cdots, n, \ n = N - m + 1.$$

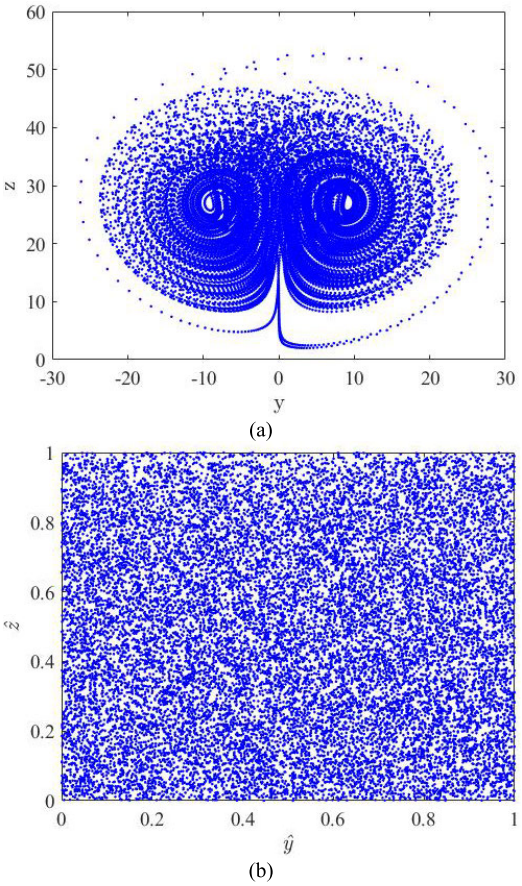


FIGURE 2. Phase diagram of Lorenz system and proposed system with the same initial value, (a) Lorenz system, (b) proposed system.

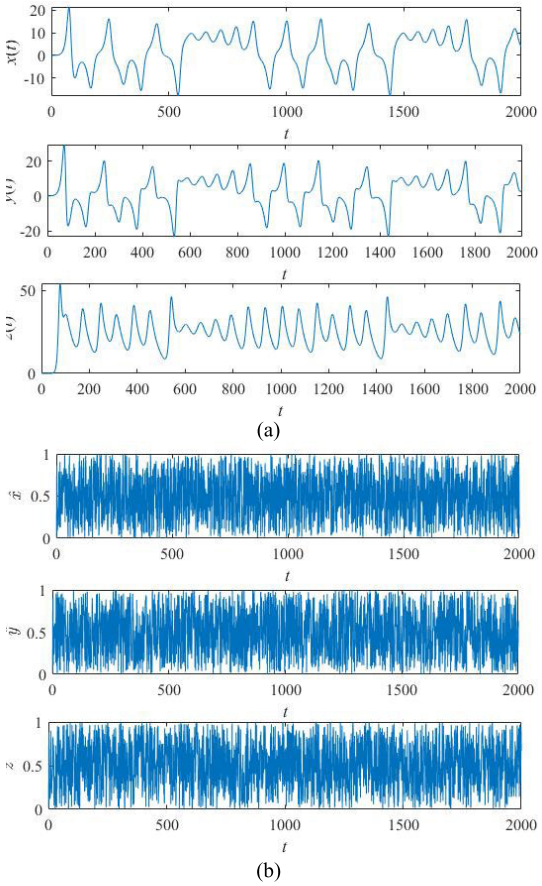


FIGURE 3. Temporal evolution of system: (a) Lorenz system; (b) proposed system.

where X_i is a m-dimentional vector. Calculate the distance between x_i and x_j as

$$d\left[x\left(i\right)-x(j)\right]=\max_{k=0,1,\cdots,m-1}\left(\left|u\left(i+k\right)-u(j+k)\right|\right) \tag{5}$$

Given a threshold $r \in [0.2, 0.3]$, Let K be the number satisfying the equation $d_{ij} \leq r \times \mathrm{SD}$, where SD is the standard value of the sequence, then we define

$$\phi^m\left(r\right)=\frac{1}{N-m+1}\sum_{i=1}^{N-m+1}\ln C_i^m\left(r\right) \tag{6}$$

where $C_i^m\left(r\right)=\frac{K}{N-m}$, then the AE of a sequence can be calculated as $\phi^m-\phi^{m+1}$.

As shown in Figure 4, the AE of proposed system is larger than Lorenz system, Lorenz-like system [26] and coupled Lorenz system [27] with different precisions, which demonstrates that proposed system can strengthen the complexity of Lorenz system greatly.

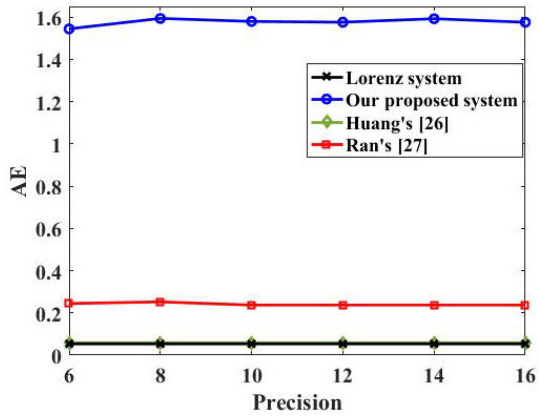


FIGURE 4. Approximate entropy analysis of Lorenz system, improved Lorenz system, Huang's system and Ran's system.

D. INFORMATION ENTROPY

Shannon proposed information entropy in 1948 [32], and the degree of confusion can be characterized by information entropy. The system is more ordered, information entropy is lower. It is defined as:

$$H\left(s\right)=-\sum_{i=1}^{N}P\left(s_i\right)\log_2\left(P\left(s_i\right)\right) \tag{7}$$

where s is information source, N demonstrates the number of states, $P\left(s_i\right)$ indicates the probability of occurrence of s_i. The sequences x, y, z, $\hat{x}$, $\hat{y}$ and $\hat{z}$ are hypothesized to 256 states, in

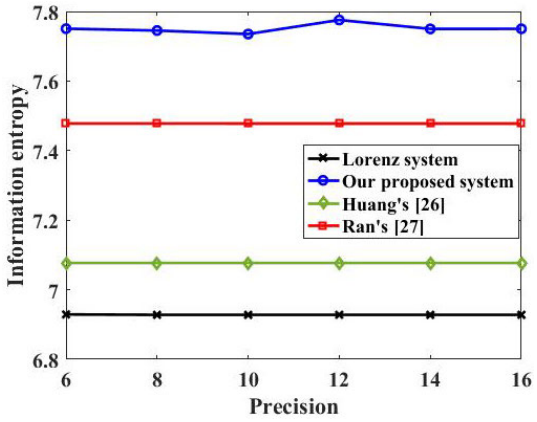


FIGURE 5. Analysis of information entropy of Lorenz system, improved Lorenz system, Huang's system and Ran's system.

theory the maximum information entropy of each sequence is $\log_2 256 = 8$. As shown in Figure 5, all entropy value of our proposed system is close to 7.8, which is bigger than the other systems.

E. AUTO CORRELATION

Auto correlation (AC) is also a significant factor used to evaluate the dynamical characteristics of a chaotic system. The correlation is defined as follow [33]:

$$\chi_{x,y} = \frac{\sum_{i=1}^{N} (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{N} (x_i - \bar{x})^2 (y_i - \bar{y})^2}} \tag{8}$$

where x_i and y_i represent the ith sequences, $\bar{x}$ and $\bar{y}$ are the average of sequence x and y respectively. Figure 6 (a), (b) and (c) show the auto-correlations of Lorenz system. As shown in Figure 6 (c), the auto-correlation of z is much stronger than x and y. As shown in Figure 6 (d), (e) and (f), the autocorrelation of adjacent orbits of the proposed system is weaker than the Lorenz system. Auto-correlation function of improved Lorenz system has a small main peak, and the side lobes are rarely low and even virtually invisible, which demonstrates that our proposed system are good random.

F. FREQUENCY DISTRIBUTION

Figure 7 depicts the frequency distribution of Lorenz system and proposed system, where the whole interval is divided into 500 equal sub-intervals. It can be seen that the distribution of proposed system is much more homogeneous than Lorenz system. Therefore, the proposed perturbation method can resist frequency attack effectively.

G. NIST-800-22 STATISTICAL TESTS

The NIST-800-22 test was designed to assess the performance of Pseudo Random Number Generator (PRBG) [34]. We can judge whether or not a chaotic binary sequence is suitable to cryptographic algorithm based on the results of NIST test. The NIST-800-22 test is made up of 15 test methods, including frequency test, run test, approximate entropy test, random excursions test, etc. Randomness of test sequence can be measured by p value. If $p \geq 0.01$, the sequence is random. If $p < 0.01$, the sequence is not random. If $p = 1$, the sequence is completely random. If $p = 0$, the sequence is not at all random. Moreover, p value is bigger, the randomness of the sequence is better. Table 1 shows NIST tests of PRNG, which can be found sequence of improved Lorenz system passes all random tests.

TABLE 1. Test results by NIST test suite.

Test Item	Means of p-Value	Result
Approximate Entropy	0.48636	Passed
Block Frequency	0.55117	Passed
Cumulative Sums	0.49226	Passed
FFt	0.51597	Passed
Frequency	0.50321	Passed
Linear Complexity	0.40560	Passed
Longest Run	0.51564	Passed
Nonoverlapping Template	0.50127	Passed
Overlapping Template	0.48756	Passed
Random Excursions	0.52112	Passed
Random Excursions Variant	0.50540	Passed
Ranks	0.48194	Passed
Runs	0.56419	Passed
Serial Test	0.52448	Passed
Maurer's Universal	0.67773	Passed

III. ENCRYPTION AND DECRYPTION ALGORITHMS

A. ENCRYPTION ALGORITHM

Suppose that a plaintext image P with a size of $M \times N$ is given. If plaintext image is a color image, P is converted into R, G and B components, and we can obtain three matrixes P^{r}, P^{g} and P^{b}, the size of each color's matrix is $M \times N$, where the pixel values range from 0 to 255. The encryption process is as follows.

Step 1. When plaintext image is color, construct a big matrix $S = [P^{\mathrm{r}}, P^{\mathrm{g}}, P^{\mathrm{b}}]$, so that the information of P^{r}, P^{g} and P^{b} is transferred to a big matrix S; when plaintext image is gray, the matrix S is built as $S = P$ to avoid additional burdens of transmission or storage.

We apply sequencing index function to S as follow:

$$[H, q] = \mathrm{sort}(S) \tag{9}$$

where $[\cdot, \cdot] = \mathrm{sort}(\cdot)$ is the sequencing index function, $H = [h_1, h_2, \cdots, h_{M\times 3N}]$ is the new sequence after ascending to S, and $q = [q_1, q_2, \cdots, q_{M\times 3N}]$ is the index value of H.

Then, we have

$$\mathrm{sum} = \sum_{m=1}^{M\times 3N} h_m \times q_m \tag{10}$$

We utilize Eq. (11) to generate K keys as

$$d_k = \mathrm{mod}\ (\mathrm{sum}, k + 0.1) \tag{11}$$

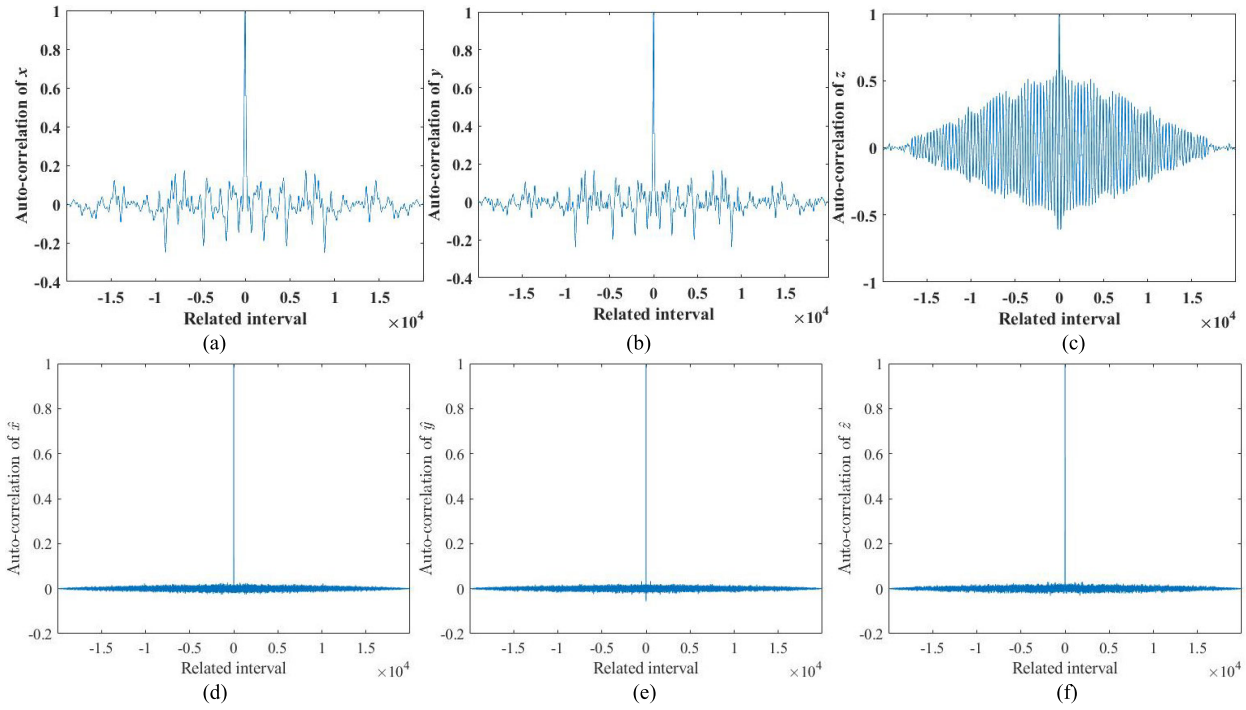


FIGURE 6. Auto-correlation functions of Lorenz system and proposed system: (a), (d) and (c) Lorenz system; (d), (e) and (f) proposed system.

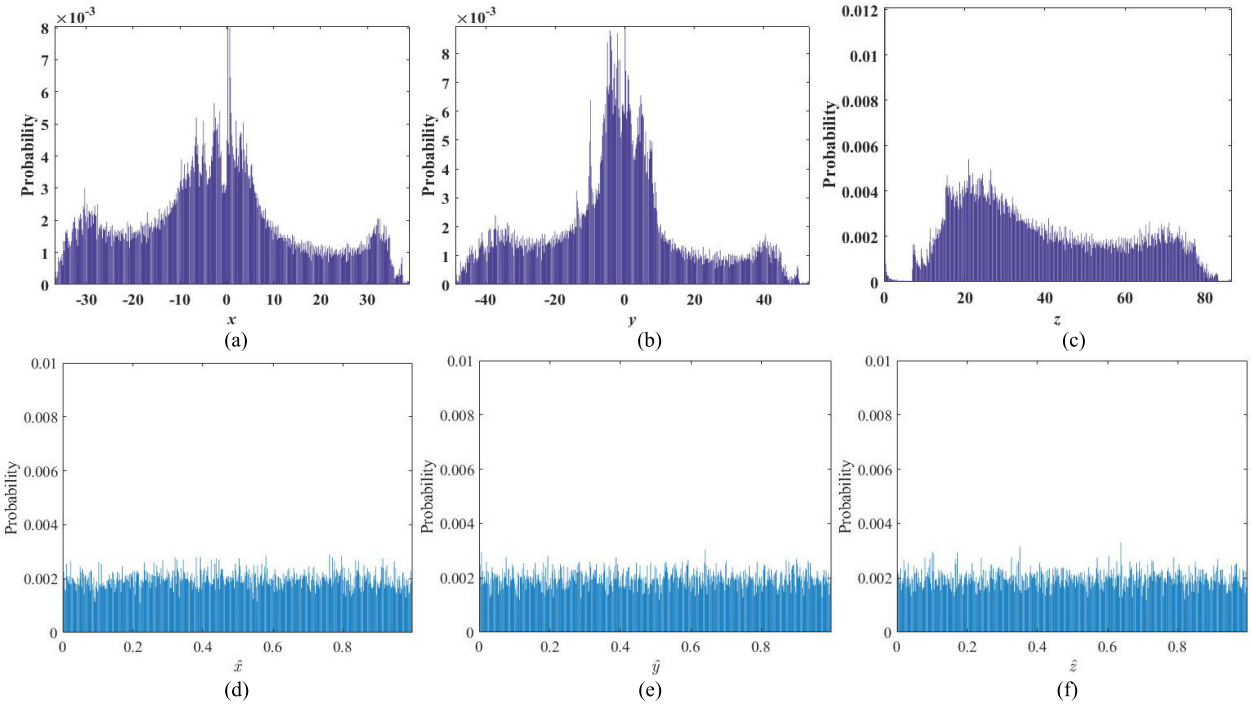


FIGURE 7. Frequency distributions: (a), (d) and (c) Lorenz system; (d), (e) and (f) proposed system.

where $k \in [1, 2, \cdots, K]$, and average value $\overline{d} = \sum_{k=1}^{K} d_k/K$ is obtained, K is assumed as $K \geq 3$ to satisfy the inequality $10^{14K} > 2^{100}$.

In this article, the keys are associated with plaintext images, if plaintext images are different, the keys will be updated. The update of keys may bring encryption inconvenience, but which will improve security of algorithm, because the attacker cannot obtain the random value of the improved system by selecting different plaintext images [35].

The initial values, and parameter a, b and c of the Eq. (2) can be calculated by the follows:

$$\begin{cases} x_0 = d_1 \bmod 1 \\ y_0 = d_2 \bmod 1 \\ z_0 = d_3 \bmod 1 \\ a = 20 + d_1 \bmod 0.1 \\ b = 50 + d_2 \bmod 0.1 \\ c = 8 + d_3 \bmod 0.1 \end{cases}$$

If plaintext image is gray, $H = [h_1, h_2, \cdots, h_{M\times N}]$, $q = [q_1, q_2, \cdots, q_{M\times N}]$, and sum is calculated as

$$\text{sum} = \sum_{m=1}^{M\times N} h_m \times q_m$$

Step 2. Generate three sequences $\hat{x}$, $\hat{y}$ and $\hat{z}$ with the length of $M \times N$ and reshape $\hat{x}$, $\hat{y}$ and $\hat{z}$ as Eq. (12), then spliced them together into two big matrixes W_1 and W_2 as Eq. (13):

$$\begin{cases} X_1 = \text{reshape}(\hat{x} \times 10^2, [M, N]) \\ X_2 = \text{reshape}(\hat{y} \times 10^2, [M, N]) \\ X_3 = \text{reshape}(\hat{z} \times 10^2, [M, N]) \end{cases} \tag{12}$$

$$\begin{cases} W_1 = [X_1, X_2, X_3] \\ W_2 = [X_2, X_3, X_1] \end{cases} \tag{13}$$

If plaintext image is gray, matrixes W_1 and W_2 are built as:

$$\begin{cases} W_1 = [X_1] \\ W_2 = [X_2] \end{cases}$$

Step 3. Create a new matrix by using the following method:

$$W\{i, j\} \leftarrow W_1\{i, j\} \times W_2\{i, j\} \tag{14}$$

where $i = 1, 2, \cdots, M$ and $j = 1, 2, \cdots, 3N$. If plaintext image is gray, $j = 1, 2, \cdots, N$.

Step 4. Replace the values of the first column of W with D, and obtain a new matrix Ψ, where D is calculated as:

$$D = (d \times 10^{14}) \bmod \xi \tag{15}$$

and

$$d = \sqrt{\frac{\sum_{k=1}^{K} (d_k - \overline{d})^2}{K}}$$
$$\xi = \min\{|X_1|_{\max}, |X_2|_{\max}, |X_3|_{\max}\}$$

Step 5. Apply sequencing index function to each row of Ψ according to Eq. (9), and obtain the index matrix U, then select the pixels of S according to the follow law:

$$T_1\{i, j\} \leftarrow \{Si, U_{i,j}\} \tag{16}$$

Step 6. Replace the values of the first row of W with D, and obtain a new matrix Φ.

Step 7. Apply sequencing index function to each column of Φ according to Eq. (9), and obtain the index matrix V, then select the pixels of T_1 according to Eq. (17):

$$T\{i, j\} \leftarrow T_1\{V_{i,j}, j\} \tag{17}$$

As shown in Figure 8, an example with the color image size of 3×4 is used to better explain the process of permutation.

A good diffusion property of encryption should make cipher-text image sensitive to the change of plaintext. Usually, XOR operation is a manipulation on the level of bit, but addition operation is a manipulation on the level of pixel. We combine XOR operation with addition operation to enhance the effectiveness of diffusion.

Step 8. We generated three chaotic sequences as:

$$\begin{cases} \tilde{X}_1 = \left\lfloor \left(\frac{\hat{x}}{d} \times 10^{14} \right) \bmod \theta \right\rfloor \\ \tilde{X}_2 = \left\lfloor \left(\frac{\hat{y}}{d} \times 10^{14} \right) \bmod \theta \right\rfloor \\ \tilde{X}_3 = \left\lfloor \left(\frac{\hat{z}}{d} \times 10^{14} \right) \bmod \theta \right\rfloor \end{cases} \tag{18}$$

then reshape three matrixes $\tilde{X}_1$, $\tilde{X}_2$ and $\tilde{X}_3$ as

$$\begin{cases} \tilde{X}_1 = \text{reshape}(\tilde{X}_1, [M, N]) \\ \tilde{X}_2 = \text{reshape}(\tilde{X}_2, [M, N]) \\ \tilde{X}_3 = \text{reshape}(\tilde{X}_3, [M, N]) \end{cases} \tag{19}$$

Step 9. We build two big matrixes $\tilde{W}_1$ and $\tilde{W}_2$ according to Eq. (13) by $\tilde{X}_1$, $\tilde{X}_2$ and $\tilde{X}_3$, and regenerate the matrix $\tilde{W}$ as:

$$\tilde{W}\{i, j\} \leftarrow \left(\tilde{W}_1\{i, j\} \times \tilde{W}_2\{i, j\} \right) \bmod \theta. \tag{20}$$

The manipulation diffusion is defined as

$$\begin{cases} C_i = (T_i \oplus T_{M\times 3N} + \tilde{W}_i) \bmod \theta & \text{if } i = 1 \\ C_i = T_i \oplus T_{i+1} \oplus C_{i-1} \oplus \tilde{W}_i & \text{if } 1 < i < M \times 3N \\ C_i = (T_i \oplus C_{i-1} + \tilde{W}_i) \bmod \theta & \text{if } i = M \times 3N \end{cases} \tag{21}$$

If plaintext image is gray, the diffusion operation is defined as

$$\begin{cases} C_i = (T_i \oplus T_{M\times 3N} + \tilde{W}_i) \bmod \theta & \text{if } i = 1 \\ C_i = T_i \oplus T_{i+1} \oplus C_{i-1} \oplus \tilde{W}_i & \text{if } 1 < i < M \times N \\ C_i = (T_i \oplus C_{i-1} + \tilde{W}_i) \bmod \theta & \text{if } i = M \times N \end{cases}$$

where $\oplus$ is the bit wise XOR operation, and θ is the maximum value of pixel in plaintext-image.

Step 10. Let $C = \text{reshape}(C, [M, 3N])$, and split the matrix C into three equal-sized small matrixes as R, G and B components. Combine R, G and B components into an image, and cipher-image is obtained. If plaintext image is gray, let $C = \text{reshape}(C, [M, N])$, and obtain the cipher-image.

The image encryption scheme is shown by Figure 9.

B. DECRYPTION ALGORITHM

The decryption procedure is a reverse process of encryption procedure.

Step 1. We remove the diffusion effect from the last pixel to the first pixel using the following formulae.

$$\begin{cases} T_i = C_{i-1} \oplus (C_i - \tilde{W}_i) \bmod \theta & \text{if } i = M' \times N' \\ T_i = T_{i+1} \oplus C_{i-1} \oplus C_i \oplus \tilde{W}_i & \text{if } 1 < i < M' \times N' \\ T_i = T_{M\times 3N} \oplus (C_i - \tilde{W}_i) \bmod \theta & \text{if } i = 1 \end{cases} \tag{22}$$

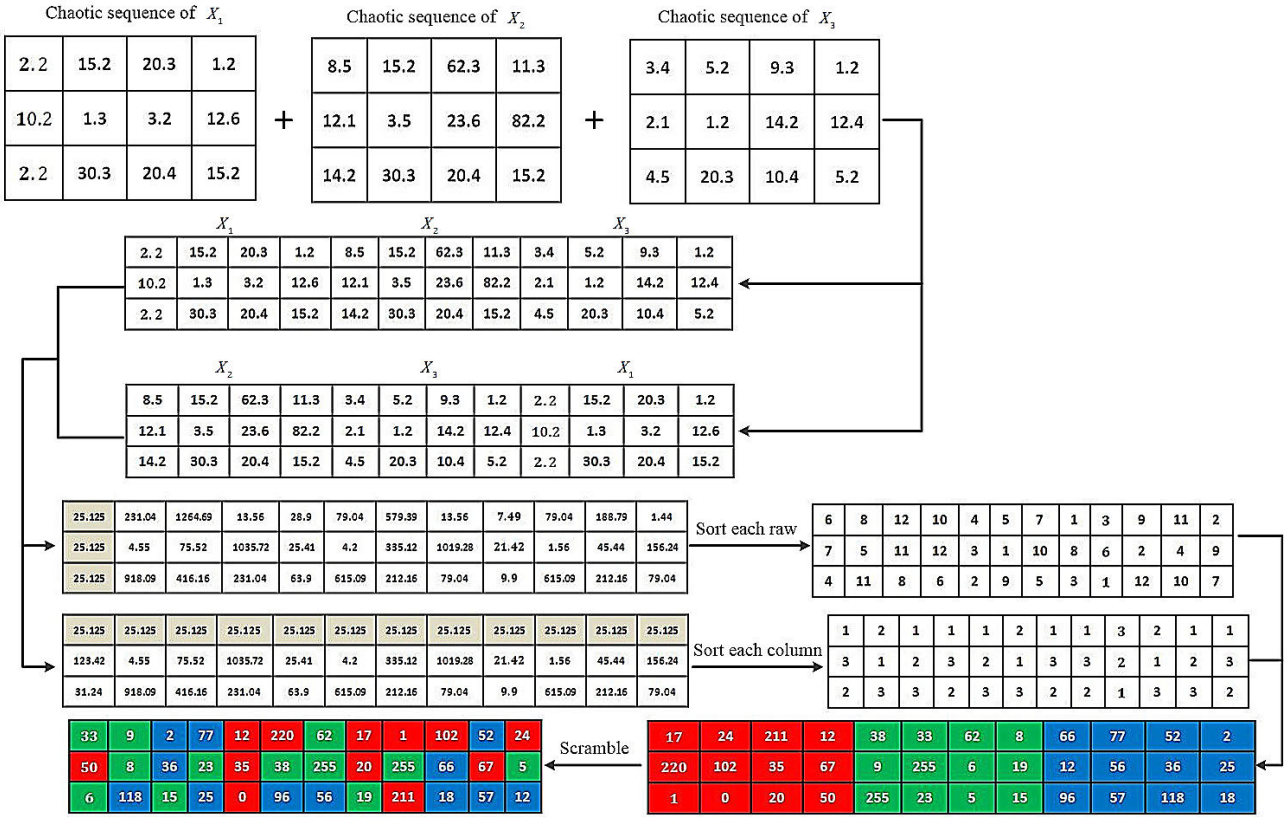


FIGURE 8. An example of permutation through the color image of size 3 × 4.

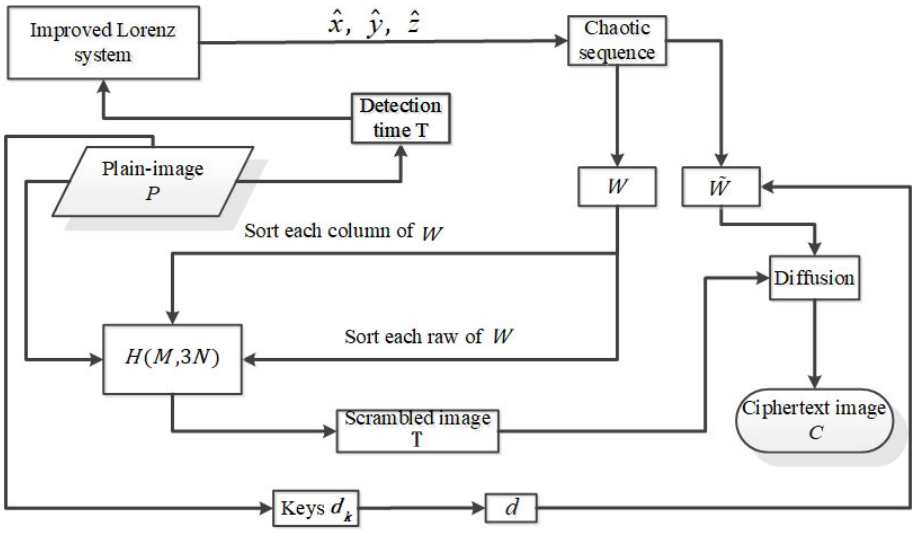


FIGURE 9. Flowchart of the encryption process.

where $M' \times N'$ is the size of of cipher-image C.

Step 2. Eliminate the column confusion effect as follow:

$$T_1\{V_{i,j}, j\} \leftarrow T\{i, j\} \tag{23}$$

where $i = 1, 2, \cdots, M'$ and $j = 1, 2, \cdots, N'$.

Step 3. Eliminate the row confusion effect as follow:

$$S\{i, U_{i,j}\} \leftarrow T_1\{i, j\} \tag{24}$$

Step 4. If cipher-image is color, split the matrix S into three small matrixes with the same size as the three components of a color image, which are combined together, and a color

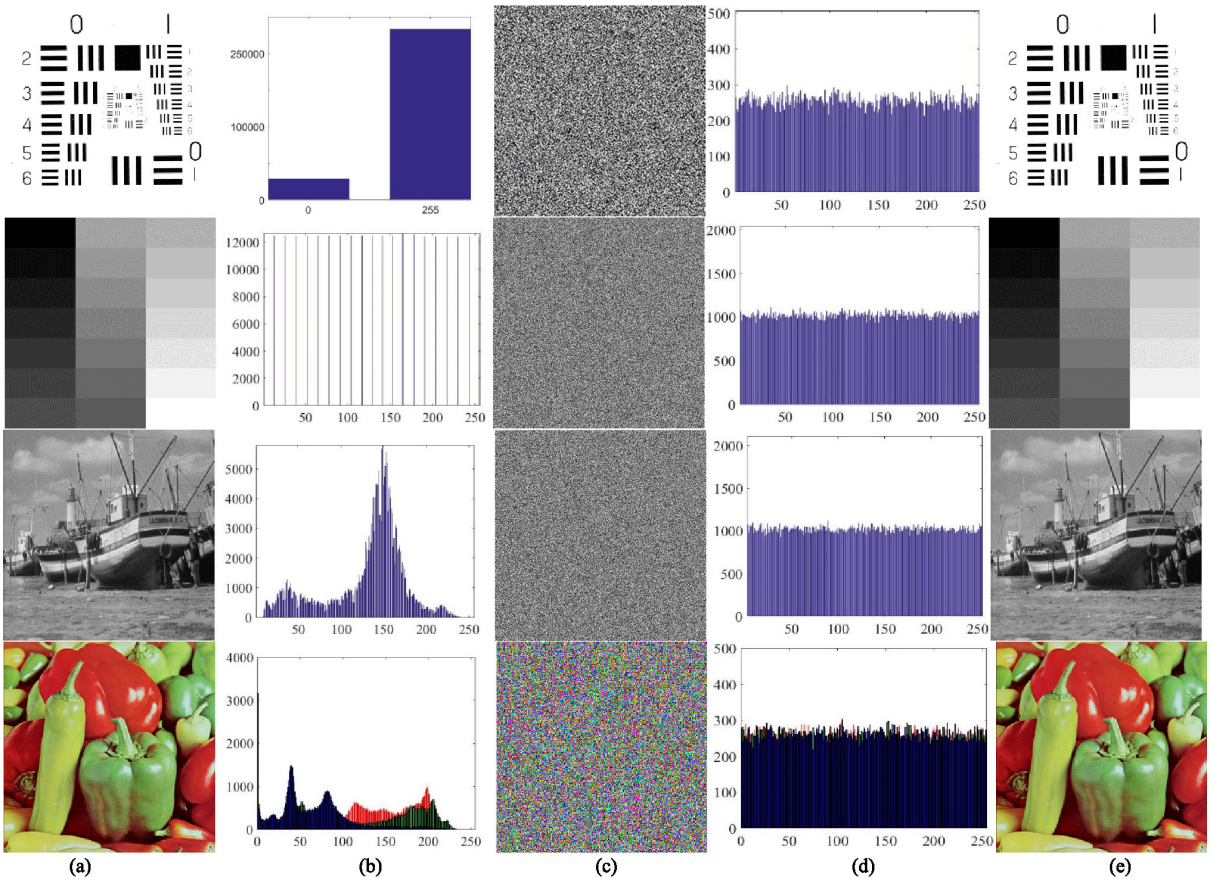


FIGURE 10. Experimental results obtained using the proposed scheme: (a) Four different kinds of plaintext images; (b) histograms of (a); (c) encrypted image of (a); (d) histograms of (c); (e) decrypted image of (c).

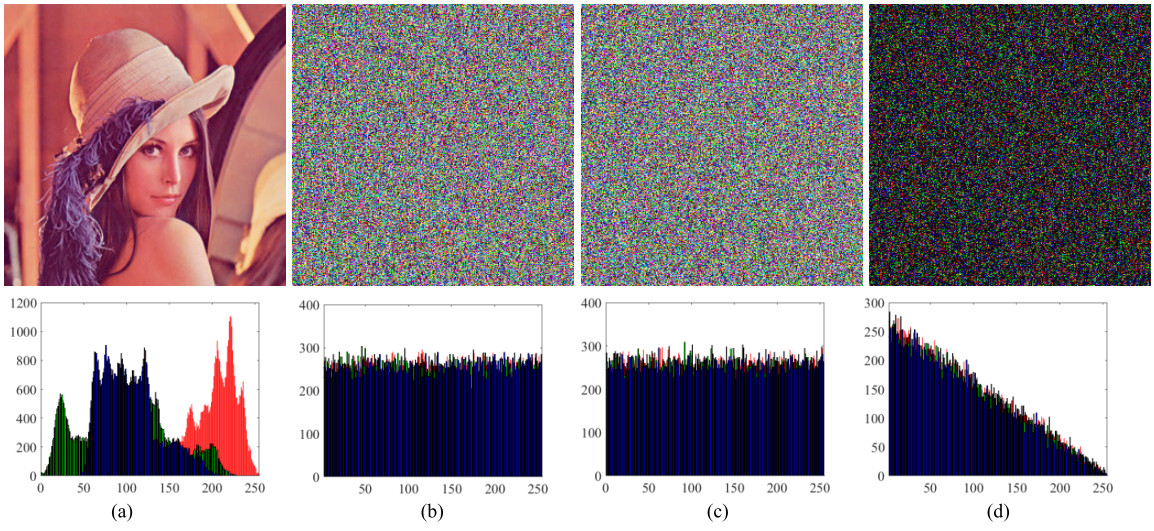


FIGURE 11. Key sensitivity tests in encryption. (a) plaintext-image of Lena (b) cipher-image c_1 with $d_1 + 10^{-14}$; (c) cipher-image c_2 with $d_2 - 10^{-14}$; (d) the difference between c_1 and c_2.

plaintext-image is obtained; If cipher-image is gray, S is equal to P, and gray plaintext-image is obtained.

IV. EXPERIMENTAL RESULTS

A good image encryption algorithm should encrypt different kinds of image into unrecognized cipher-image. As shown in Figure 10 (b), the four types of plaintext-image have different properties of histograms, but their cipher-images are all random-like. As shown in Figure 10 (d), the distribution of pixel values of cipher-images is harmonious, and attracters can't obtain useful information from histograms of cipher-images.

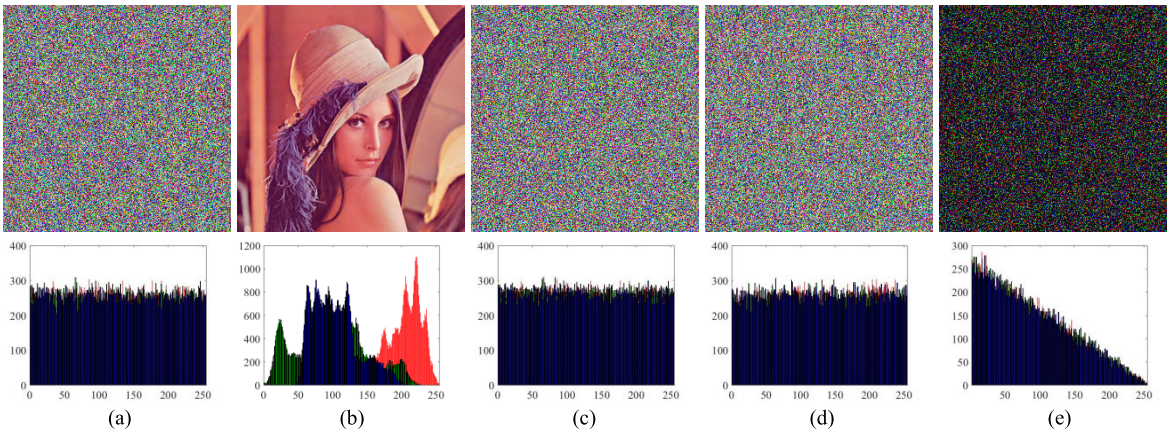


FIGURE 12. Key sensitivity tests in decryption. (a) cipher-image (b) plaintext-image of Lena (c) decrypted image D_1 with $d_1 + 10^{-14}$; (d) decrypted image D_2 with $d_2 - 10^{-14}$; (d) the difference between D_1 and D_2.

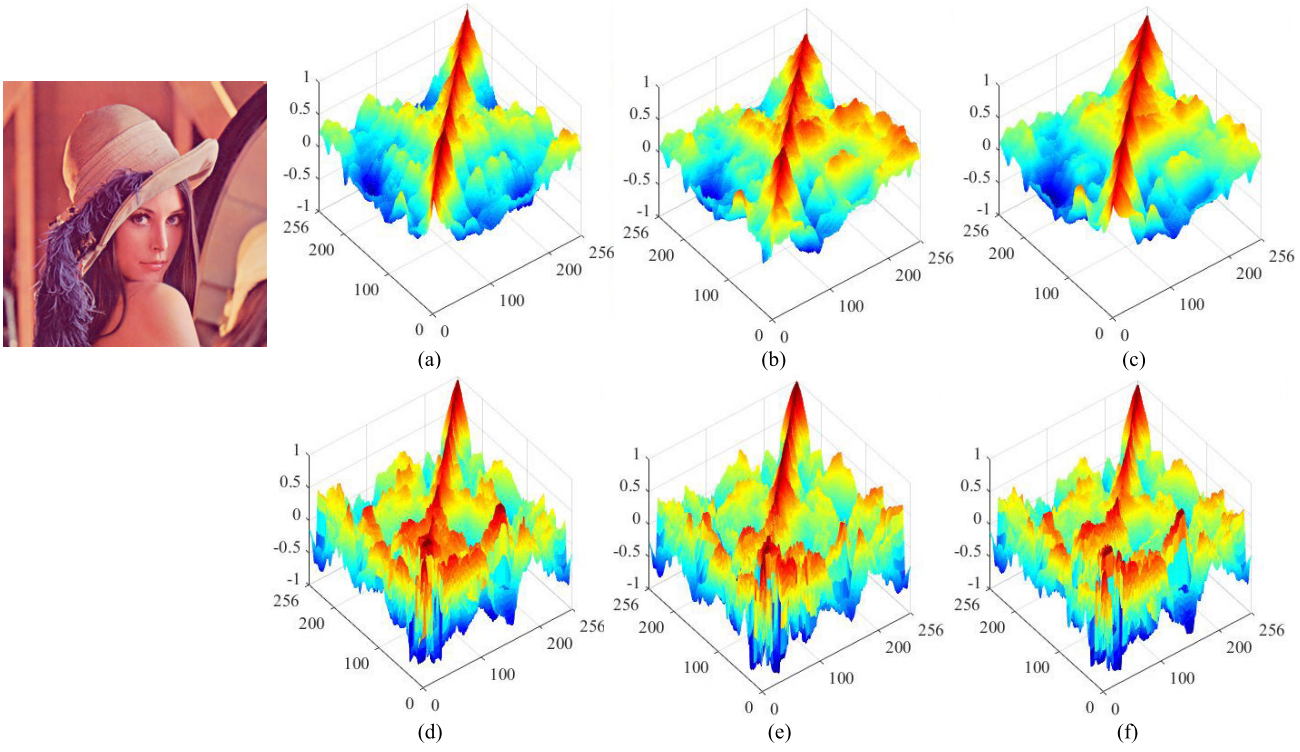


FIGURE 13. AC between R, G and B components of the plain color image Lena, (a) correlation between row pixels of R and G components of the plaintext-image; (b) correlation between row pixels of G and B components of the plaintext-image; (c) correlation between row pixels of R and B components of the plaintext-image; (d) correlation between column pixels of R and G components of the plaintext-image; (e) correlation between column pixels of G and B components of the plaintext-image; (f) correlation between column pixels of R and B components of the plaintext-image.

V. SECURITY ANALYSIS

A. KEY SECURITY

A sensitivity test was performed based on the color plaintext-image of "Lena" and the results are shown in Figure 11 and 12. When $K = 5$, through Eq. (11), we can obtain five keys as $d_1 = 0.799826060252032$, $d_2 = 0.89908888703445$, $d_3 = 2.799938279444270$, $d_4 = 3.800186667046599$, $d_5 = 4.500150065664913$. As shown in Figure 11 (d), the cipher-images are completely different even if the change in the keys is very slight. As Figure 12 (b) demonstrates, the decrypted image was exactly the same as the original plaintext image with the correct keys d_k, where $k = 1, 2, \cdots, 5$. The decrypted images are random-like although the change of keys is slight as shown in Figure 12 (c), (d) and (e).

B. KEY SPACE

The key space should be large enough to resist exhaustive attacks. According to Figure 11 and 12, the operational precision of d_k was fixed as 10^{-14}. When we considered the precision of d_k, the key space size was $10^{14K} (K = 5)$, it is approximately 2^{232} and much larger than the security

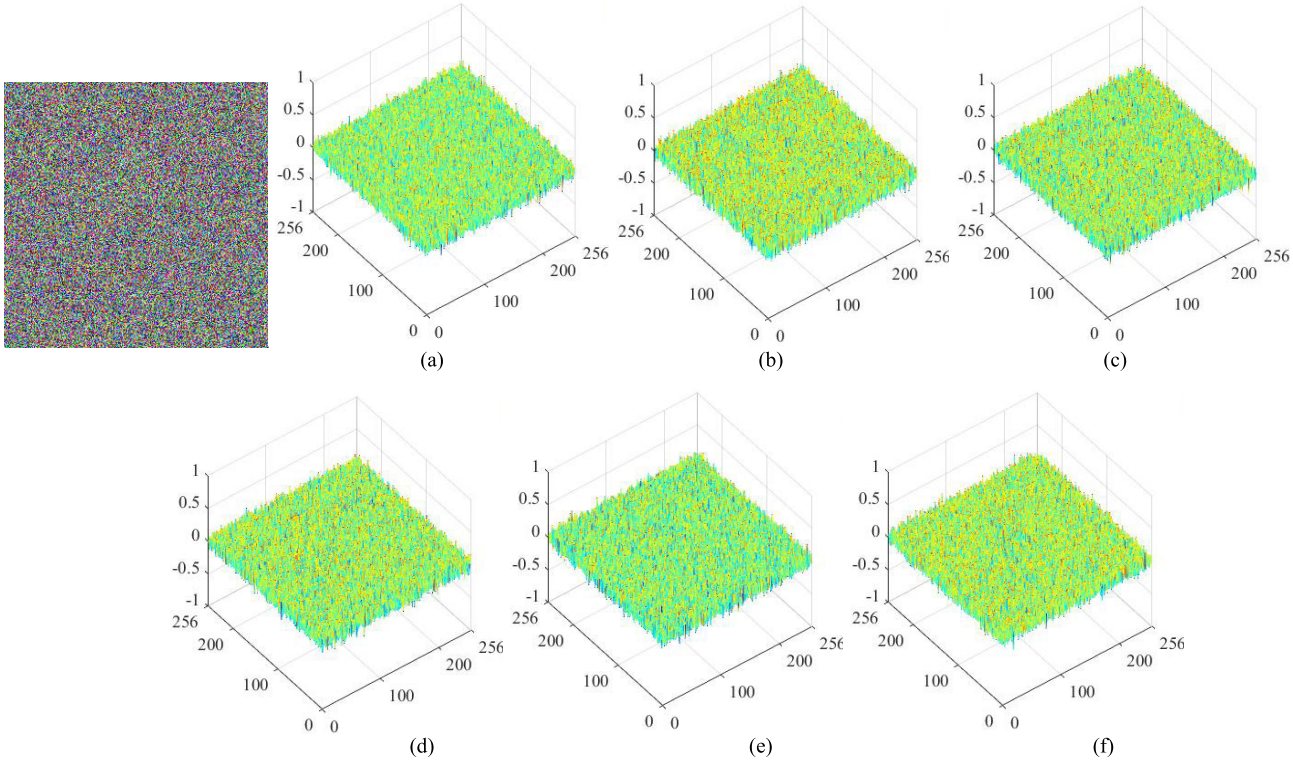


FIGURE 14. AC between R, G and B components of the cipher-image, (a) correlation between row pixels of R and G components of the cipher-image; (b) correlation between row pixels of G and B components of the cipher-image; (c) correlation between row pixels of R and B components of the cipher-image; (d) correlation between column pixels of R and G components of the cipher-image; (e) correlation between column pixels of G and B components of the cipher-image; (f) correlation between column pixels of R and B components of the cipher-image.

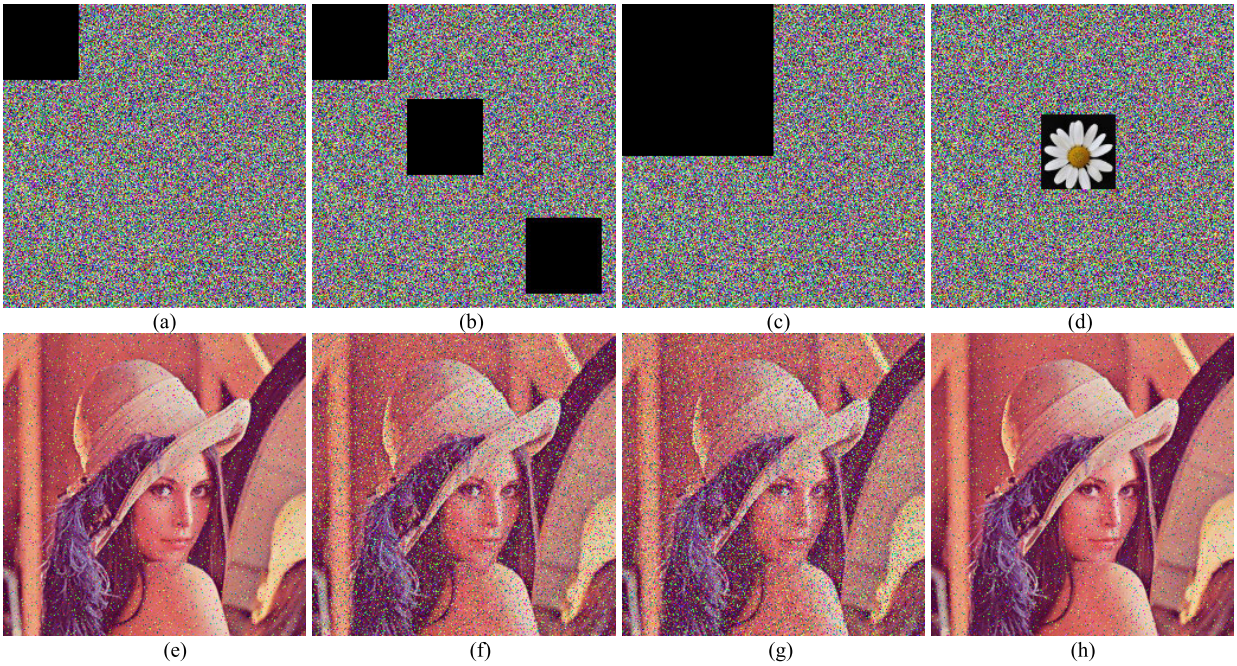


FIGURE 15. Experimental results for cipher-image of Lena with different kinds of data loss. (a) 1/16 data loss; (b) 3/16 data loss; (c) 1/4 data loss (d) 1/16 data modification with a square; (e), (f), (g) and (h) are the corresponding decrypted images.

requirement for a key space of 2^{100} [36]. It's obvious that, brute-force attacks on our encryption algorithm is infeasible. Furthermore, the key space can be enlarged greatly by increase of K.

VI. STATISTICAL ANALYSIS

A. CORRELATION COEFFICIENT

In general, there are strong correlations between adjacent pixels in a plaintext image, the correlations between two adjacent

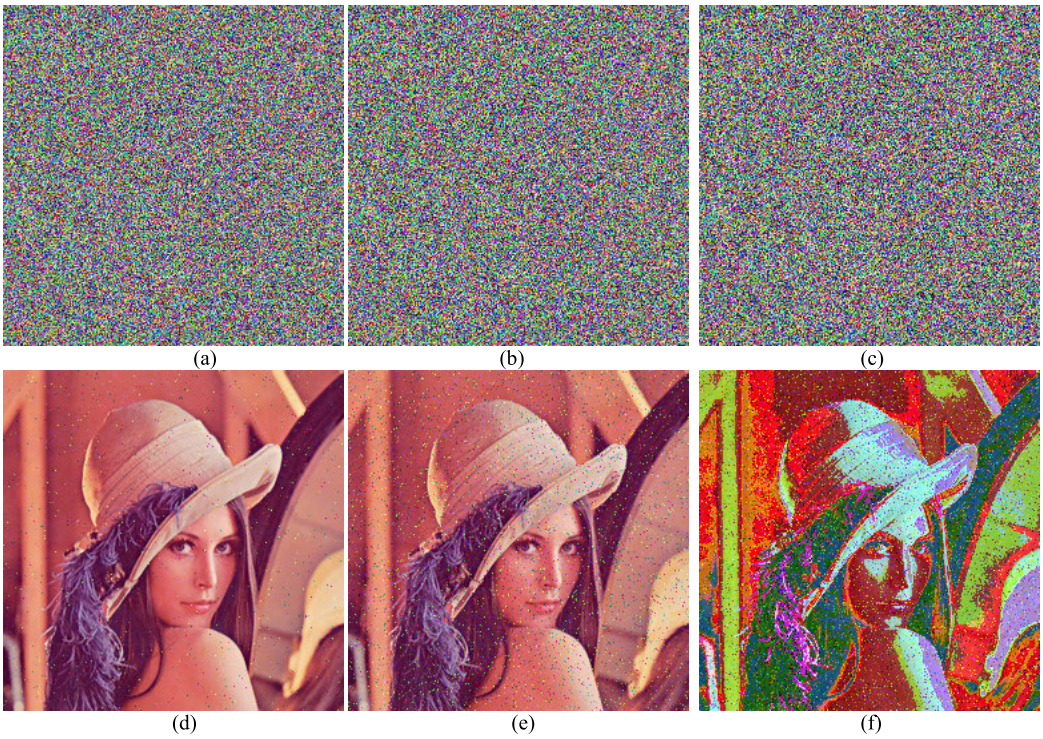


FIGURE 16. Experimental results for a noise attack. (a) 0.01 intensity salted pepper noise; (b) 0.05 intensity salted pepper noise; (c) 0.1 intensity salted pepper noise; (d), (e) and (f) are the corresponding decrypted images.

TABLE 2. Correlations between adjacent pixels in the "Lena" plaintext and ciphertexts.

Direction	Plaintext	Ciphertext	Ref. [38]	Ref. [40]	Ref. [41]	Ref. [42]	Ref. [43]
Horizontal	0.9765	0.0032	0.0013	−0.0047	−0.0226	−0.0001	0.0019
Vertical	0.9606	−0.0004	0.0006	0.0015	0.0041	0.0089	0.0012
Diagonal	0.9356	0.0059	0.0019	0.0030	0.0368	0.0091	0.0009

pixels need to be decreased in the ciphered image to resist statistical attacks. The correlations between the horizontal, vertical, and diagonal adjacent pixels can be calculated by 3000 randomly selected pairs of adjacent pixels from the plaintext image and encrypted image as follows [37]:

$$\lambda_{xy} = \frac{\mathrm{cov}(\alpha, \beta)}{\sqrt{\varphi(\alpha)}\sqrt{\varphi(\beta)}} \tag{25}$$

where

$$\mathrm{cov}(\alpha, \beta) = \frac{1}{N}\sum_{i=1}^{N}(\alpha_i - \Phi(\alpha))(\beta_i - \Phi(\beta))$$

$$\varphi(\alpha) = \frac{1}{N}\sum_{i=1}^{N}(\alpha_i - \Phi(\alpha))^2, \quad \Phi(\alpha) = \frac{1}{N}\sum_{i=1}^{N}\alpha_i$$

The correlations between adjacent pixels in the plaintext image and encrypted image are shown in Table 2, which demonstrates that the correlations of ciphered image were much smaller than the plain image of "Lena".

The correlation between R, G, B components of an image can be measured intuitively and amply by AC [38]. Similar to Eq. (8), it is defined as:

$$AC = \frac{E[(x_i - E[X_i]) - (x_{i+1} - E[X_i])]}{E\left[(x_i - E[X_i])^2\right]} \tag{26}$$

where X_i and X_{i+1} is a pixel sequence and another pixel sequence from different components respectively, $E[\cdot]$ is the mathematical expectation.

Figure 13 and 14 depicts the correlations between R, G, B components of the plain color image Lena and its cipher-image respectively. It's obvious that, the correlation values between R, G, B components of cipher-image is much smaller than plaintext-image, it means that the proposed encryption algorithm can mask the correlations between R, G, B components effectively.

B. INFORMATION ENTROPY

Randomness of an image is measured by information entropy. Similar to Eq. (7), it can be calculated as follows:

$$H(s) = \sum_{i=0}^{2^N-1} v(s_i)\log_2\frac{1}{v(s_i)} \tag{27}$$

TABLE 3. The comparison of information entropy.

Text images	Entropy
Lena (256 × 256)	7.9991
Pepper (256 × 256)	7.9991
Baboon (256 × 256)	7.9991
Ref. [40] (Lena)	7.9991
Ref. [41] (Lena)	7.9973
Ref. [42] (Lena)	7.9973
Ref. [43] (Lena)	7.9912
Ref. [44] (Lena)	7.9963

TABLE 4. NPCR and UACI values for the encrypted images.

Text images	NPCR(%)	UACI(%)
Lena(256 × 256)	99.6246	33.5118
Pepper(256 × 256)	99.6048	33.3828
Baboon(256 × 256)	99.5885	33.4590
Ref. [40] (Lena)	99.6253	33.4807
Ref. [41] (Lena)	99.6100	33.5300
Ref. [42] (Lena)	99.6096	33.4574
Ref. [43] (Lena)	100	33.47
Ref. [44] (Lena)	99.6228	33.7041

where $v(s_i)$ is the probability of symbol s_i and N is the bit depth of the image. The information entropies for the encrypted "Lena", "Pepper" and "Baboon" images are listed in Table 3. The experimental results showed that the information entropies of the encrypted images were close to 8.

C. DIFFERENCE ATTACK ANALYSIS

An excellent image encryption tactics should differential attacks sensitively, which can be measured based on NPCR and NPCR as follows [39]:

$$\text{NPCR} = \frac{\sum_{ij} \omega(i,j)}{F \times G} \times 100\% \tag{28}$$

$$\text{UACI} = \frac{1}{F \times G}[\sum_{i,j} \frac{E(i,j) - E'(i,j)|}{255}] \times 100\% \tag{29}$$

where the width and height of the image is represented by F and G respectively, $E(i,j)$ and $E'(i,j)$ are the ith row and jth pixel values from ciphered images before and after one pixel of the plain image been changed respectively, and $\omega(i,j)$ is determined as

$$\omega(i,j) = \begin{cases} 0 & E(i,j) = E'(i,j) \\ 1 & E(i,j) \neq E'(i,j) \end{cases} \tag{30}$$

The keys of our proposed encryption scheme are based on the plaintext image, so even if only one pixel of plaintext image is changed, the change in the ciphered image is significant, which can make differential attacks ineffective. Table 4 shows the NPCR and UACI results for "Lena", "Pepper" and "Baboon" where all the NPCR and UACI scores are close to the expected values, where the expected values of NPCR and UACI are as NPCR = 99.6094%, UACI = 33.4635% [37].

VII. ROBUSTNESS ANALYSIS

Figure 15 denotes the experimental results of data loss attack to the encrypted images. The quality of the decrypted images decreases as the data loss size increases as shown in Figure 15 (e)-(g). As shown in Figure 15 (h), the main information of the plaintext images can be recognized despite of some date modification, because there are correlations between loss data and reserved data.

In order to test the resistance of noise attack, we add salted pepper noise to the encrypted images. As the Figure 16 shown, quality of the decrypted images is degraded with the increase of noise intensity, but the decrypted images still be identified. Therefore, the proposed encryption scheme can highly robust against noise and loss attacks.

VIII. CONCLUSION

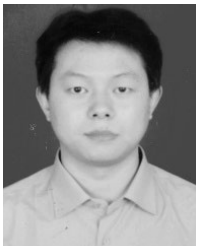
In this study, we have proposed an image encryption scheme based on improved Lorenz system. The proposed system has more complex kinetic properties than Lorenz system, therefore it is more suitable to encrypt image. In encryption algorithm, the keys are associated with plaintext-image to update the keys with the change of plaintext image, and key space is large enough to resist attacks of brute-force. Through the analysis of key security, protection against differential attack, information entropy and correlation, we can see that our proposed system can encrypt different kinds of images into random-like cipher-images with high security level.

REFERENCES

[1] E. Lorenz, "Deterministic nonperiodic flow," *J. Atmos. Sci.*, vol. 20, no. 2, pp. 130–141, 1963.
[2] S. Nazari, M. Ataei, and A. Tamizi, "Improving diagnosis of some brain disease by analysing chaotic indices of EEG signals," *Int. J. Biomed. Eng. Technol.*, vol. 22, no. 4, pp. 349–369, 2016.
[3] K. Zare and S. Chesley, "Order and chaos in the planar isosceles three-body problem," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 8, no. 2, pp. 475–494, Jun. 1998.
[4] Y. Jun-Zhong and Z. Mei, "Chaos synchronization in complex networks," *Chin. Phys. Lett.*, vol. 22, no. 9, pp. 2183–2185, Sep. 2005.
[5] Y. Gong, B. Xu, Q. Xu, C. Yang, T. Ren, Z. Hou, and H. Xin, "Ordering spatiotemporal chaos in complex thermosensitive neuron networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 73, no. 4, Apr. 2006, Art. no. 046137.
[6] C. H. Hommes, H. E. Nusse, and A. Simonovits, "Cycles and chaos in a socialist economy," *J. Econ. Dyn. Control*, vol. 19, nos. 1–2, pp. 155–179, Jan. 1995.
[7] X. Ge, B. Lu, F. Liu, and X. Luo, "Cryptanalyzing an image encryption algorithm with compound chaotic stream cipher based on perturbation," *Nonlinear Dyn.*, vol. 90, no. 2, pp. 1141–1150, Oct. 2017.
[8] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Process.*, vol. 138, pp. 129–137, Sep. 2017.
[9] J. Zhou and O. C. Au, "On the security of chaotic convolutional coder," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 58, no. 3, pp. 595–606, Mar. 2011.
[10] H. Liu, H. Wan, C. K. Tse, and J. Lu, "An encryption scheme based on synchronization of two-layered complex dynamical networks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 63, no. 11, pp. 2010–2021, Nov. 2016.
[11] K.-Z. Li, M.-C. Zhao, and X.-C. Fu, "Projective synchronization of driving-response stems and its application to secure communication," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 56, no. 10, pp. 2280–2291, Oct. 2009.
[12] X.-Y. Wang, P. Li, Y.-Q. Zhang, L.-Y. Liu, H. Zhang, and X. Wang, "A novel color image encryption scheme using DNA permutation based on the lorenz system," *Multimedia Tools Appl.*, vol. 77, no. 5, pp. 6243–6265, Mar. 2018.

[13] M. J. Rostami, A. Shahba, S. Saryazdi, and H. Nezamabadi-pour, "A novel parallel image encryption with chaotic windows based on logistic map," *Comput. Electr. Eng.*, vol. 62, pp. 384–400, Aug. 2017.
[14] R. Bansal, S. Gupta, and G. Sharma, "An innovative image encryption scheme based on chaotic map and Vigenère scheme," *Multimedia Tools Appl.*, vol. 76, no. 15, pp. 16529–16562, Aug. 2017.
[15] M. Kanafchian and B. Fathi-Vajargah, "A novel image encryption scheme based on clifford attractor and noisy logistic map for secure transferring images in navy," *Int. J. e-Navigat. Maritime Economy*, vol. 6, pp. 53–63, Apr. 2017.
[16] H. Liu, A. Kadir, and Y. Niu, "Chaos-based color image block encryption scheme using S-box," *AEU-Int. J. Electron. Commun.*, vol. 68, no. 7, pp. 676–686, Jul. 2014.
[17] J.-X. Chen, Z.-L. Zhu, C. Fu, H. Yu, and L.-B. Zhang, "A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 20, no. 3, pp. 846–860, Mar. 2015.
[18] R. Guesmi, M. A. Ben Farah, A. Kachouri, and M. Samet, "Hash key-based image encryption using crossover operator and chaos," *Multimedia Tools Appl.*, vol. 75, no. 8, pp. 4753–4769, Apr. 2016.
[19] C. Song and Y. Qiao, "A novel image encryption algorithm based on DNA encoding and spatiotemporal chaos," *Entropy*, vol. 17, no. 12, pp. 6954–6968, 2015.
[20] 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.
[21] O. M. Al-Hazaimeh, M. F. Al-Jamal, N. Alhindawi, and A. Omari, "Image encryption algorithm based on lorenz chaotic map with dynamic secret keys," *Neural Comput. Appl.*, vol. 31, no. 7, pp. 2395–2405, Jul. 2019.
[22] A. Anees, "An image encryption scheme based on lorenz system for low profile applications," *3D Res.*, vol. 6, no. 3, pl. 24, Sep. 2015.
[23] I. Younas and M. Khan, "A new efficient digital image encryption based on inverse left almost semi group and lorenz chaotic system," *Entropy*, vol. 20, no. 12, p. 913, 2018.
[24] I. Hussain, A. Anees, A. H. AlKhaldi, A. Algarni, and M. Aslam, "Construction of chaotic quantum magnets and matrix lorenz systems S-boxes and their applications," *Chin. J. Phys.*, vol. 56, no. 4, pp. 1609–1621, Aug. 2018.
[25] A. Girdhar and V. Kumar, "A RGB image encryption technique using lorenz and Rossler chaotic system on DNA sequences," *Multimedia Tools Appl.*, vol. 77, no. 20, pp. 27017–27039, Oct. 2018.
[26] M. Kaur and V. Kumar, "Efficient image encryption method based on improved lorenz chaotic system," *Electron. Lett.*, vol. 54, no. 9, pp. 562–564, May 2018.
[27] U. Arshad, S. I. Batool, and M. Amin, "A novel image encryption scheme based on Walsh compressed quantum spinning chaotic lorenz system," *Int. J. Theor. Phys.*, vol. 58, no. 10, pp. 3565–3588, Oct. 2019.
[28] H. Bouslehi and H. Seddik, "Innovative image encryption scheme based on a new rapid hyperchaotic system and random iterative permutation," *Multimedia Tools Appl.*, vol. 77, no. 23, pp. 30841–30863, Dec. 2018.
[29] Z. Li, C. Peng, L. Li, and X. Zhu, "A novel plaintext-related image encryption scheme using hyper-chaotic system," *Nonlinear Dyn.*, vol. 94, no. 2, pp. 1319–1333, Oct. 2018.
[30] Q. Ran, L. Wang, J. Ma, L. Tan, and S. Yu, "A quantum color image encryption scheme based on coupled hyper-chaotic lorenz system with three impulse injections," *Quantum Inf. Process.*, vol. 17, no. 8, p. 188, Aug. 2018.
[31] S. M. Pincus, "Approximate entropy as a measure of system complexity," *Proc. Nat. Acad. Sci. USA*, vol. 88, no. 6, pp. 2297–2301, 1991.
[32] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 4, pp. 623–656, 1948.
[33] C. Chen, K. Sun, Y. Peng, and A. O. A. Alamodi, "A novel control method to counteract the dynamical degradation of a digital chaotic sequence," *Eur. Phys. J. Plus*, vol. 134, no. 1, pp. 1–16, Jan. 2019.
[34] C. Fan, Q. Ding, and C. K. Tse, "Counteracting the dynamical degradation of digital chaos by applying stochastic jump of chaotic orbits," *Int. J. Bifurcation Chaos*, vol. 29, no. 8, Jul. 2019, Art. no. 1930023.
[35] X. Wang, Y. Wang, X. Zhu, and C. Luo, "A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level," *Opt. Lasers Eng.*, vol. 125, Feb. 2020, Art. no. 105851.
[36] X. Wang, X. Zhu, X. Wu, and Y. Zhang, "Image encryption algorithm based on multiple mixed hash functions and cyclic shift," *Opt. Lasers Eng.*, vol. 107, pp. 370–379, Aug. 2018.
[37] 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, 2019.
[38] Z. Hua and Y. Zhou, "Image encryption using 2D logistic-adjusted-sine map," *Inf. Sci.*, vol. 339, pp. 237–253, Apr. 2016.
[39] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations," *Signal Process., Image Commun.*, vol. 52, pp. 6–19, Mar. 2017.
[40] R. Zahmoul, R. Ejbali, and M. Zaied, "Image encryption based on new beta chaotic maps," *Opt. Lasers Eng.*, vol. 96, pp. 39–49, Sep. 2017.
[41] L. Xu, X. Gou, Z. Li, and J. Li, "A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion," *Opt. Lasers Eng.*, vol. 91, pp. 41–52, Apr. 2017.
[42] C. Cao, K. Sun, and W. Liu, "A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map," *Signal Process.*, vol. 143, pp. 122–133, Feb. 2018.
[43] J. Wu, X. Liao, and B. Yang, "Color image encryption based on chaotic systems and elliptic curve ElGamal scheme," *Signal Process.*, vol. 141, pp. 109–124, Dec. 2017.
[44] A. Belazi, A. A. Abd El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Process.*, vol. 128, pp. 155–170, Nov. 2016.

CHENGYE ZOU received the B.S. degree in physics and the M.E. degree in theoretical physics from Liaoning Normal University, Dalian, China, and the Ph.D. degree in computer application technology from the Dalian University of Technology, Dalian. He is currently a Lecturer with Anyang Normal University, Anyang, China. His research interests include complex networks, biological computing, and chaotic image encryption.



QIANG ZHANG received the Ph.D. degree from Xidian University, Xi'an, China, in 2002. He is a Professor with the Dalian University of Technology, Dalian, China. He is also a Professor with Dalian University, Dalian. His research interests include intelligent computing and intelligent robots. He is currently serving on editorial boards of seven international journals and has edited special issues in journals, such as *Neurocomputing* and the *International Journal of Computer Applications in Technology*.

XIAOPENG WEI is a Professor with the Dalian University of Technology, Dalian, China. He has (co)authored about 160 articles published. His research interests include computer animation and intelligent CAD.

CHANJUAN LIU (Member, IEEE) received the B.Eng. degree in computer science from Jinan University, Guangzhou, China, in 2010, and the Ph.D. degree in computer science from Peking University, Beijing, China, in 2016. She is currently a Lecturer with the Dalian University of Technology, Dalian, China. Her research interests include logic and game theory.