IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 24, 2020, accepted November 9, 2020, date of publication November 25, 2020, date of current version February 2, 2021.

Digital Object Identifier 10.1109/ACCESS.2020.3040573

A Novel Chaotic Block Image Encryption Algorithm Based on Deep Convolutional Generative Adversarial Networks

PENGFEI FANG[1], HAN LIU[1], (Member, IEEE), AND CHENGMAO WU[2]
[1]School of Automation and Information Engineering, Xi'an University of Technology, Xi'an 710048, China
[2]School of Electronic Engineering, Xi'an University of Posts and Telecommunications, Xi'an 710061, China

Corresponding author: Han Liu (liuhan@xaut.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61973248, and in part by the Key Project of Shaanxi Key Research and Development Program under Grant 2018ZDXM-GY-089.

ABSTRACT This paper proposes a novel chaotic block image encryption algorithm based on deep convolutional generative adversarial networks (DCGANs), quaternions, an improved Feistel network, and an overall scrambling and diffusion mechanism. First, a new hyperchaotic system is introduced and combined with DCGANs to generate a random sequence with better randomness and complexity as a key stream. This sequence is then combined with a quaternion and an improved Feistel network encryption of a colour plaintext image by utilizing the key block matrix to ultimately achieve overall scrambling and diffusion of the cipher image. Finally, the security of this algorithm is quantitatively and qualitatively analysed. The simulation results show that the proposed hyperchaotic system has a large key space and good random characteristics and that the new algorithm yields adequate security and can resist brute-force attacks and chosen-plaintext attacks. Therefore, this approach provides a new way to achieve secure transmission and protection of image information.

INDEX TERMS Image encryption, chaotic system, deep convolutional generative adversarial networks.

I. INTRODUCTION

With the rapid development of the computer industry, a large amount of image information is transmitted on networks, which may be stolen by illegal users in the process of storage or transmission, resulting in information leakage. Since images contain large amounts of information, possess strong correlation and include pixels with high redundancy, traditional data encryption standard (DES) and advanced encryption standard (AES) algorithms are unsuitable; among other shortcomings, they require high computational consumption and achieve low efficiency and poor real-time performance. Thus, they do not satisfy the security requirements of current image information. Therefore, the development of efficient, high-security image encryption algorithms is urgently needed. Such algorithms would be of very high research and practical value.

Many image encryption algorithms have been proposed [1]–[4], which are mainly based on four common image encryption algorithms: (1) Modern cryptosystem-based encryption [5]. Due to the large amount of data associated with images, the encryption efficiency of this algorithm is low. (2) Matrix transformation. In this algorithm, the order of the input plaintext is disordered, and the plaintext information is masked by the elementary matrix transformation of the image for finite times [4]. Typical scrambling algorithms include Arnold transformation, Baker mapping, etc. However, this algorithm has low resistance to statistical attacks and periodicity. (3) Secret segmentation and sharing. This algorithm achieves safety but leads to the rapid expansion of data [6]. (4) Chaotic systems. To expand the key space and improve the security and encryption efficiency of the algorithm, the chaotic system was introduced to generate a key sequence for image encryption. There are many advantages of the chaotic system, such as randomness, control parameters, ergodicity, and sensitivity to the initial conditions. The initial value sensitivity of the chaotic system can improve the security of an encryption algorithm, and the range of initial values determines the key space [7], [8].

According to their dimensions, existing chaotic systems can be divided into low-dimensional chaotic systems and high-dimensional chaotic systems [9]–[15]. The author of [9]

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

presented a four-dimensional quadratic autonomous hyperchaotic system based on the Lorenz system, which has only one hyperchaotic attractor. The authors of [10] presented a four-wing hyperchaotic memristive system that generates a four-wing hyperchaotic attractor with the unusual feature of having a line equilibrium. The authors of [11] presented a new four-dimensional hyperchaotic system with coexisting attractors, which has several dynamic behaviours and utilizes a hyperchaotic system constructor state-error controller. The authors of [12] presented a new four-dimensional chaotic system with multi-wing and coexisting attractors and simulated its circuit. The authors of [13] presented a new four-dimensional hyperchaotic system and applied it to image encryption. The authors of [14], [15] presented an image encryption algorithm based on six-dimensional and seven-dimensional hyperchaotic systems, which has large secret key spaces. Low-dimensional chaotic systems are simple in structure and easy to implement. Therefore, the generation speed of a low-dimensional chaotic sequence is fast, and the encryption efficiency is high. However, questions remain regarding issues such as the bounded range of chaos, discontinuity and the non-uniform distribution of chaotic sequence. With the development of computer science technology since Lorenz discovered the first three-dimensional chaotic system, the high-dimensional chaotic system has rapidly developed. Compared with the low-dimensional chaotic system, it has stronger dynamic characteristics and randomness, better computational complexity and a larger key space; it also has two or more positive Lyapunov exponents. Overall, the high-dimensional chaotic system has good chaotic dynamics performance, which satisfies the safety requirement of an image encryption algorithm. Therefore, in this paper, we develop a new, four-dimensional hyperchaotic system. Analysis shows that the proposed hyperchaotic system has complex chaotic dynamic characteristics and a large key space, which is suitable for chaotic image encryption.

In 1979, Fridrich applied chaotic systems to image encryption. Since then, a large number of encryption algorithms based on chaotic systems have been proposed. These algorithms variously employ one-time keys [16], bit-level scrambling [17], [18], pixel-level scrambling [19], deoxyribonucleic acid (DNA) rule encoding [20], [27], [28], DNA dynamic encoding [21], [25], [26], complex mathematical network models [22],S-box [23], block encryption [24], etc. These encryption algorithms mainly perform two steps: image pixel position scrambling and image pixel value diffusion. The author of [16] presented an image encryption algorithm based on one-time key and robust chaotic map, which can solve the problems of short chaotic period and small key space while providing resistance against chosen-plaintext attack. The author of [17] presented a colour image encryption algorithm based bit-level scrambling and Chen's hyperchaotic system scrambling and diffusion that has a large key space. The authors of [18] presented an improved one-dimensional logistic chaotic system for scrambling the plaintext image pixel position and pixel value, which offers high security. The author of [19] presented an image encryption based on pixel-level scrambling and reversible mixed cellular automata model, which has higher security performance. The author of [20] presented an image encryption algorithm based on piecewise linear chaotic map (PWLCM) and DNA complementary rule, which are used for image scrambling and diffusion. The algorithm not only has a large key space but also can resist against common attacks. The authors of [21] combined the hyperchaotic and DNA operations to realize image encryption with high security performance. The author of [22] presented a new encryption algorithm that uses nonlinear characteristics of the complex mathematical network perceptron. The hyperchaotic system is combined with the perceptron of image encryption, which solves the short-cycle problem of chaos. The authors of [23] presented a new logistic-sine system (LSS) and constructed a new S-Box by using LSS; based on this S-Box and the chaotic key stream, the new image encryption algorithm performs a round of scrambling and two rounds of a substitution process. The authors of [24] presented an image encryption algorithm based on dynamic S-boxes and random blocks, in which a plaintext image is scrambled and diffused to implement an encrypted image. The authors of [25] presented a new 5D continuous hyperchaotic system that is combined with DNA dynamic encoding, scrambling and diffusion to encrypt an image; the algorithm can resist chosen-plaintext attack. The authors of [26] presented a novel colour image encryption algorithm based on dynamic DNA encoding and a chaotic system in which DNA encoding and diffusion are used to diffuse the image information. The authors of [27], [28] presented a hyperchaotic system combined with block encryption to realize image encryption.

The above described algorithms have problems of low complexity, imperfect security, small key space of the encryption algorithm, an inability to resist chosen-plaintext attack, etc. In addition, the scrambling process leads to high time complexity and poor scrambling performance and the diffusion process is slow due to the increasing volume of information in the image. Furthermore, the diffusion process is too simple thus makes it difficult to guarantee efficient algorithm operation. Therefore, in this paper, to reduce the correlation between image pixels, improve the security of the encryption algorithm, and increase the performance of scrambling and diffusion encryption, we construct a new encryption algorithm based on a scrambling and diffusion mechanism. The key stream, quaternion rotation and a block encryption mechanism are used to pixel-level image and scrambling and diffusion encryption are applied, which improves the parallel encryption efficiency of image channels, reduces the correlation between adjacent pixels of image, and realizes the image scrambling and diffusion encryption from the local block to the whole. Simulation results show that the proposed encryption algorithm can resist chosen-plaintext attack and has good robustness and efficient parallel image encryption.

Some new image encryption algorithms based on deep learning, matrix semi-tensor product theory and Boolean networks have been proposed in recent years, representing new directions in image encryption. By combining features of nonlinearity, controllability and logicality with the chaotic system, the scrambling and diffusion of an images are achieved. The author of [29] applied a combination of coupled map logistic lattice, double diffusion and cyclic shift to scramble and diffuse an image, which has high security. The author of [30] presented a two-dimensional chaotic system along with a Boolean network. Matrix semi-tensor product theory and random position transformation are used to scramble and diffuse an image to realize encryption, providing high encryption efficiency and security. The author of [31] presented image block scrambling algorithm followed by generation of the key stream by combining a Boolean network with a mixed linear-nonlinear coupled map; the image is encrypted by matrix semi-tensor and key stream. The algorithm is secure, effective, and suitable for colour image encryption. The author of [32] presented a new dispersion-keeping evaluation mechanism and two bi-objective memetic genetic programming algorithms, which have good regression characteristics and can be applied to image encryption. The author of [33] developed a Loren chaotic generation key stream matrix for image scrambling, and matrix semi-tensor product theory is applied to diffuse the image to generate a ciphertext image with improved encryption security. The author of [34] developed PWLCM to generate a key stream and combines it with the nonlinear characteristics of the McCulloch-Pitts model to encrypt an image, which has a large key space and can resist common attacks. In the above-described research, from the perspective of deep learning, matrix semi-tensor product theory and Boolean network theory are applied to image encryption, which has high security. In addition to the choice of algorithm, the structure of the key stream determines the performance of the encryption system. In this paper, from the point of key stream generation, we construct a fusion random sequence with high randomness and complexity based on a new hyperchaotic system combined with deep convolutional generative adversarial networks (DCGANs), which overcomes the periodicity of chaotic systems and are used as the key stream for scrambling and diffusion operations. This paper provides a new idea for the combination of chaotic systems and deep learning for image encryption.

To summarize, the new hyperchaotic system makes it possible to expand the key space, obtain larger positive Lyapunov exponents and achieve better chaotic dynamics performance. At the same time, it combines with the nonlinearity mechanism of deep convolutional generative adversarial networks and scrambling diffusion mechanism to apply image encryption to further improve the security algorithm of encryption. Therefore, a new block image encryption algorithm based on a four-dimensional hyperchaotic system is proposed, which combines the hyperchaotic concept with DCGANs, and a quaternion rotation matrix and an improved Feistel network are employed to realize overall scrambling and diffusion encryption of colour image pixels. The experimental result and security analysis show that the new hyperchaotic system has a large key space and a larger positive Lyapunov exponent, which means that the complexity of the chaotic sequence is better, and it combines with DCGANs to be applied to the new image encryption algorithm to reduce the pixel correlation of the obtained colour ciphertext image and increase its resistance to common attacks, thus improving security.

The rest of the paper is organized as follows: In Section II, a new four-dimensional hyperchaotic system is proposed. In Section III, a pseudo-random sequence generator based on the new hyperchaotic system and DCGANs is designed. A new image encryption and decryption algorithm is described in Section IV, and the encryption results are analysed in Section V. Finally, the conclusions are presented in Section VI.

II. NEW HYPERCHAOTIC SYSTEM

A. SOME EXTRA DETAILS

The Lorenz system is one of the classic three-dimensional chaotic systems [35]. It was discovered by Hendrik Antoon Lorentz and is defined as in (1):

$$\begin{cases} \dot{x} = a(x - y), \\ \dot{y} = cx - xz - y, \\ \dot{z} = xy - bz, \end{cases} \tag{1}$$

where a, b, and c are positive real numbers, with $a = 10$, $b = 8/3$ and $c = 28$, and the system represents a chaotic attractor.

1) NEW HYPERCHAOTIC SYSTEM

On the basis of the Lorenz chaotic system, a new four-dimensional hyperchaotic system is proposed, which includes the added variable$w$, defined as in (2):

$$\begin{cases} \dot{x} = ax - y^2, \\ \dot{y} = b(z - y) - (x + w), \\ \dot{z} = xy + (c - b)y + cz, \\ \dot{w} = xy + z + w, \end{cases} \tag{2}$$

where $a = -6$, $b = 59$, and $c = 43$ result in the new hyperchaotic attractor system with initial conditions of (1,1,1,1), which are the hyperchaotic attractors.

2) PHASE DIAGRAM

The phase diagrams of the new hyperchaotic system (2) and Ref. [9], Ref. [10], Ref [11], Ref [12], and Ref [13] as shown in Figure 1.

Figure 1 shows the phase diagram of the new hyperchaotic system (2) for different coordinates, in which a chaotic attractor exists.

3) BIFURCATION DIAGRAM

In the dynamic system, the phenomenon of topological structure change caused by the change of control parameters is bifurcation. The bifurcation can clearly reflect the whole

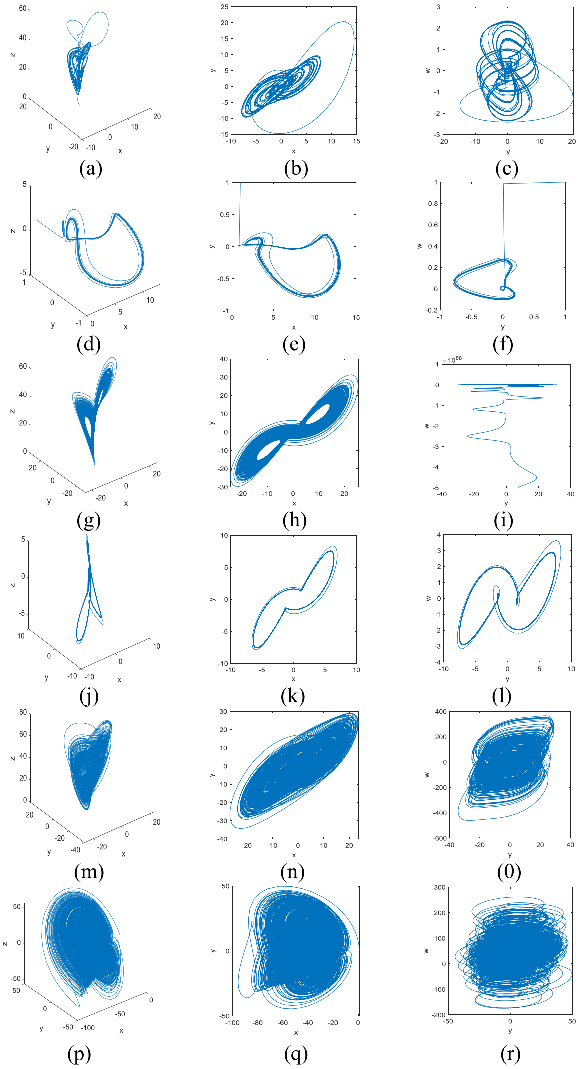


FIGURE 1. The phase diagrams of the system with the parameters and the initial values (1,1,1,1):(a),(b),(c):phase diagrams of Ref[9]; (d),(e),(f): phase diagrams of Ref[10];(g),(h),(i): phase diagrams of Ref[11];(j),(k),(l): phase diagrams of Ref[12];(m),(n),(0): phase diagrams of Ref[13];(p),(q),(r): phase diagrams of new hyperchaotic system(2).

process of the system from period to chaotic system. When a large number of irregular distribution points appear on the bifurcation diagram, it indicates that the system is in a chaotic state; when the bifurcation diagram is linear or some certain points, it indicates that the system is in a periodic state. The bifurcation diagrams of the new hyperchaotic system (2) and Ref. [9], Ref. [10], Ref. [11], Ref. [12], and Ref. [13] as shown in Figure 2.

It can be seen from the Figure 2 that the transition from periodic state to chaotic state appears of the new hyperchaotic system (2).

4) TIME SERIES DIAGRAM

A time series diagram of the new chaotic system in different phases, i.e., x, y, z, and w, is shown in Figure 3.

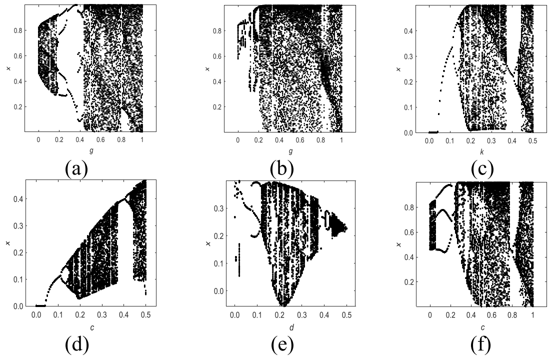


FIGURE 2. The bifurcation diagrams of the system with the parameters; (a): bifurcation diagrams of Ref [9]; bifurcation diagrams of Ref [10]; bifurcation diagrams of Ref [11]; bifurcation diagrams of Ref [12]; bifurcation diagrams of Ref [13]; bifurcation diagrams of new hyperchaotic system.

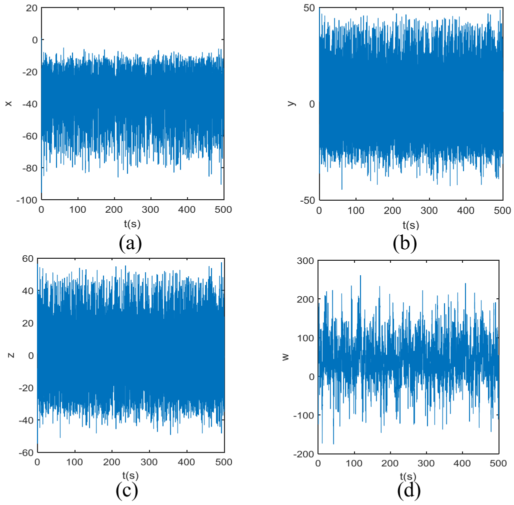


FIGURE 3. Time series diagrams of the new system (2) with parameters $a = -6$, $b = 59$, and $c = 43$ and the initial values (1,1,1,1): (a) time series x; (b) time series y; (c) time series z; (d) time series w.

Figure 3 shows that the time series of the proposed new hyperchaotic system has good randomness.

B. ANALYSIS OF THE NEW HYPERCHAOTIC DYNAMIC PROPERTIES

From the perspective of chaotic dynamics, we conducted an in depth study on the proposed hyperchaotic system (2) and compared it with the typical improved hyperchaotic system with some differences.

1) SYMMETRY AND DISSIPATIVITY OF THE HYPERCHAOTIC SYSTEM

The transformation $(x, y, z, w) \to (-x, -y, z.-w)$ of the proposed hyperchaotic system, which is invariant by calculation, is symmetrical about the z-axis. The dissipativity calculation of the system can be conducted by the gradient formula shown in (3):

$$\Delta\dot{V}=\frac{\partial\dot{x}}{x}+\frac{\partial\dot{y}}{y}+\frac{\partial\dot{z}}{z}+\frac{\partial\dot{w}}{w}=a-b+c+1=-21<0 \tag{3}$$

where $a=-6, b=59$, $c=43$, and $\Delta\dot{V}<0$. Therefore, the new hyperchaotic system (2) is dissipative such that all trajectories of the systems are limited to a set of limit points collected for a volume of 0, and its asymptotic dynamics behaviour is fixed onto an attractor, which proves the existence of chaotic attractors.

2) EQUILIBRIUM AND STABILITY

The equilibrium point of the new hyperchaotic system (2) can be obtained by solving the following equation (4):

$$\begin{cases} ax-y^2=0, \\ b(z-y)-(x+w)=0, \\ xy+(c-b)y+cz=0, \\ xy+z+w=0, \end{cases} \tag{4}$$

Given equation (4), the new hyperchaotic system (2) is shown to have only one equilibrium points$s=(0,0,0,0)$. Since system (2) has only one equilibrium point, the Jacobian matrix of the system is as follows:

$$\begin{bmatrix} a & -2y & 0 & 0 \\ -1 & -b & b & -1 \\ y & x-16 & c & 0 \\ y & x & 1 & 1 \end{bmatrix} \tag{5}$$

where $a=-6, b=59$, $c=43$ and $s=(0,0,0,0)$. When input into equation (4), four eigenvalues, namely, $\lambda_1=0.9898$, $\lambda_2=-48.7023$, $\lambda_3=32.7125$, and $\lambda_4=-6$, are obtained, which are not all positive or negative; thus, the equilibrium point $s=(0,0,0,0)$ is the unstable saddle point.

3) LYAPUNOV EXPONENT AND DIMENSION

The Lyapunov exponent [36] is an important index of the system dynamics, since it represents the system in terms of the phase space average exponential rate of convergence or divergence between adjacent orbits when $a=-6$, $b=59$, $c=43$ and the initial value is $(1,1,1,1)$ in new hyperchaotic system (2). The Lyapunov exponent spectrum is shown in Figure 4, in which the Lyapunov exponents of the new hyperchaotic system (2) are $LE_1=2.8747, LE_2=0.0523, LE_3=-0.0078$, and $LE_4=-23.9192$.

Figure 4 shows that the new system has two positive Lyapunov exponents; hence, the new system is hyperchaotic. The Lyapunov dimension is one of the effective means to judge chaotic motion, the formula of which is as follows:

$$d_j=j+\frac{\sum_{i=1}^{j}LE_i}{|LE_{j+1}|} \tag{6}$$

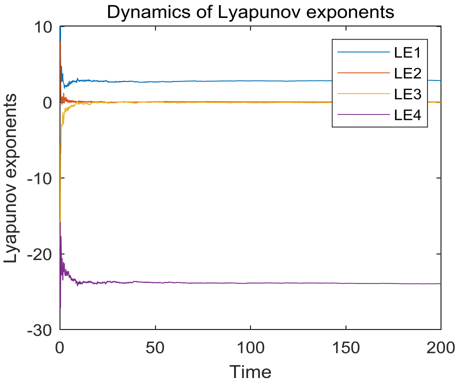


FIGURE 4. **Diagram of the Lyapunov exponents.**

TABLE 1. **Lyapunov exponents and dimensions of several chaotic systems.**

Chaotic	Lyapunov exponents	Lyapunov dimensions
Ref. [9]	0.4160, 0.1348, -0.0014, 14.2200	3.0386
Ref.[10]	0.0845, 0.0152, -0.0001, -1.9527	3.0510
Ref.[11]	0.4934, 0.4034, 0.0042, -23.9010	3.0377
Ref.[12]	0.5162, 0, -4.9208, -6.5954	2.3322
Ref.[13]	0, 2.5274, 2.1036, -16.3014	3.2814
Proposed	2.8069,0.1668, 0.0592, 23.9145	3.1219

The new hyperchaotic chaotic system is four-dimensional; thus, $j=3$, which utilizes the Lyapunov exponent of the chaotic system to calculate the dimensions. A comparison of the five systems is shown in Table 1.

Table 1 shows that the new hyperchaotic system (2) has relatively large positive Lyapunov exponents and dimensions, thus exhibiting its apparent advantages.

4) POINCARE SECTION

Poincare sections can be used to analyse the movement of multivariable autonomous systems [37]. When a Poincare section distributes point sets along a line segment or a line arc and discrete points are unevenly distributed data, the system is chaotic. When $a=-6$, $b=59c=43$ and the initial value is $(1,1,1,1)$, the Poincare section is as shown in Figure 5.

Figure 5 reveals that the Poincare section is a set of line arc distribution points, in which the distribution of discrete points is dense and different. Hence, the new hyperchaotic system (2) is in a chaotic state.

5) COMPLEXITY AND RANDOM ANALYSIS OF THE CHAOTIC SYSTEM

The complexity and randomness of the chaotic system sequence are necessary to test and determine whether the sequence meets the security standard of information encryption. At present, most testing software and standards are provided by the National Institute of Standards and Technology (NIST) [38]. The measure of sequence randomness is the p-value algorithm, which provides the probability that the randomness of the sequence is better than that of a truly random

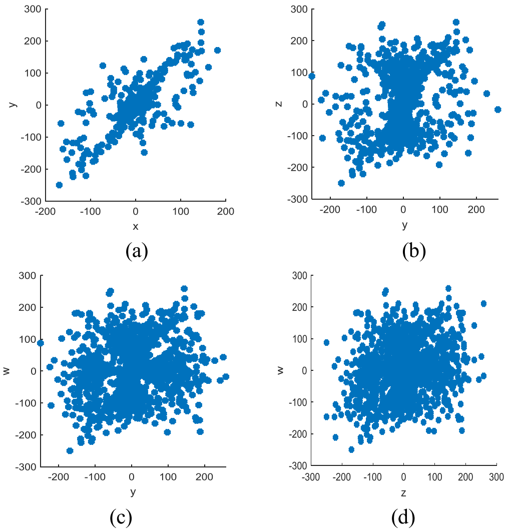


FIGURE 5. Poincare section of the new hyperchaotic system: (a) $x - y$ plane; (b) $y - z$ plane; (c) $y - w$ plane; (d) $z - w$ plane.

TABLE 2. NIST tests.

Test	x-phase	y-phase	z-phase	w-phase
Frequency	0.3504	0.2133	0.5341	0.3504
Frequency Test within a Block	0.3504	0.3564	0.7399	0.2133
Cumulative Sums	0.7399	0.3504	0.5341	0.7399
Runs	0.2133	0.0668	0.3504	0.3504
Test for the Longest Run of Ones in a Block	0.5314	0.3504	0.3562	0.5341
Binary Matrix Rank Test	0.5341	0.5341	0.2133	0.0668
Discrete Fourier Transform (Spectral)	0.0351	0.5341	0.7399	0.1223
Non-overlapping Template Matching	0.7399	0.9914	0.7399	0.5341
Overlapping Template Matching	0.7399	0.3504	0.7399	0.2133
Maurer's "Universal Statistical" Test	0.3504	0.3504	0.7399	0.7399
Approximate Entropy	0.5341	0.1223	0.2133	0.7399
Random Excursions	0.7926	0.5314	0.1992	0.4368
Random Excursions Variant	0.8054	0.5314	0.6200	0.2292
Linear Complexity	0.5341	0.5341	0.3504	0.1223
Serial	0.4063	0.9114	0.3504	0.9114

sequence. All test results are determined by the $P - value$; if $P < 0.01$, then the sequence is considered neither random nor complex. If $P \geq 0.01$, the sequence is considered random and complex. According to the requirements of the NIST test software, 10 groups of 10^6 bits of new hyperchaotic system (2) sequences are selected for testing. The test results are shown in Table 2.

Table 2 shows that the new hyperchaotic system (2) sequence has passed all NIST tests; therefore, it has good complexity and random characteristics.

TABLE 3. Approximate entropy (ApEn) of a random sequence generated by a chaotic system.

Chaotic	x-phase	y-phase	z-phase	w-phase
Ref. [9]	0.3901	0.3784	0.2198	0.3528
Ref. [10]	0.0220	0.0001	0.0163	0.0004
Ref. [11]	0.2961	0.3110	0.3127	0.0013
Ref. [12]	0.2728	0.1678	0.1354	0.3164
Ref. [13]	0.5508	0.5349	0.4022	0.3897
Proposed	0.3856	0.5915	0.5832	0.3508

TABLE 4. z1 test of a random sequence generated by a chaotic system.

Chaotic	x-phase	y-phase	z-phase	w-phase
Ref. [9]	0.0479	0.0164	0.0527	0.0726
Ref. [10]	0.0649	0.0036	0.0156	0.0607
Ref. [11]	0.0304	0.0412	0.1308	0.3171
Ref. [12]	0.0106	0.0508	0.0091	0.0039
Ref. [13]	0.0289	0.0314	0.1835	0.0667
Proposed	0.0045	0.0403	0.6250	0.0118

Many scholars utilize approximate entropy (ApEn) to describe the complexity of a chaotic sequence [23], which is calculated as follows:

$$ApEn = \sum_{i=1}^{N} [\varphi^{n}(r) - \varphi^{n+1}(r)] \tag{7}$$

where $\varphi^{n}(r)$, $\phi^{n+1}(r)$ is the average of the logarithm of the chaotic series, n is the dimension, r is the threshold, and N is the sequence length. The larger the ApEn value is, the more complex the chaotic series is. Given that $N = 2000$, $n = 2$, and $r = 0.15$, the calculation results of the complexity of the chaotic random sequences generated by the five chaotic systems are as shown in Table 3.

Table 3 shows that the approximate entropy of the sequence generated by the new system is relatively large, which reveals that the chaotic complexity of the new hyperchaotic system is higher. To summarize, the new hyperchaotic system (2) has more complex random characteristics, which means that it has a better security performance in image encryption.

6) Z1 TEST OF THE CHAOTIC SYSTEM

Gottwald and Melbourne proposed a reliable and effective binary test method called the Z1 test for determining whether a system is chaotic. The Z1 test method does not require phase space reconstruction and the value of the linear growth rate is directly calculated, which is to approach 1 or 0 to judge whether chaotic behavior exists. It is calculated as follows:

$$K(c) = \frac{\text{cov}(i, D_c(i))}{\sqrt{\text{var}(i)\text{var}(D_c(i))}} \tag{8}$$

where $i = 1, 2, \ldots, n, D_C(i)$ is the modified mean square displacement function, $\text{cov}(\cdot)$ is covariance function, and $\text{var}(\cdot)$ is Variance function. The chaotic sequence length is set to 2000, the values of the new hyperchaotic system is compared with Ref. [9], Ref. [10], Ref. [11], Ref. [12], and Ref. [13], as shown in Table 4.

Table 4 shows that all of the values are close to 0, and the value of the new hyperchaotic system (2) is larger than those of the other systems. Thus, the performance of the proposed hyperchaotic system is better.

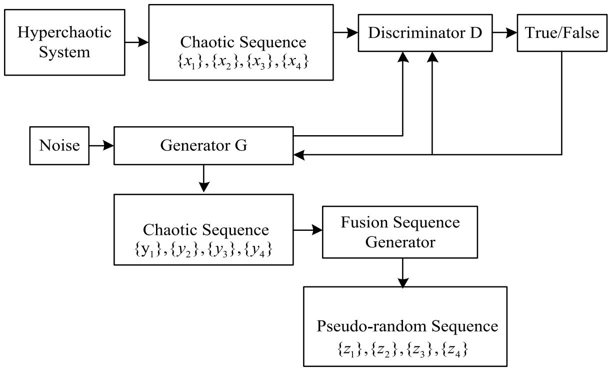

Hyperchaotic System
Chaotic Sequence $\{x_1\},\{x_2\},\{x_3\},\{x_4\}$
Discriminator D
True/False
Noise
Generator G
Chaotic Sequence $\{y_1\},\{y_2\},\{y_3\},\{y_4\}$
Fusion Sequence Generator
Pseudo-random Sequence $\{z_1\},\{z_2\},\{z_3\},\{z_4\}$

FIGURE 6. Pseudo-random sequence generator.

III. GENERATION OF THE KEY STREAM

In the recent years, the field of automatic generative modelling has mainly relied on the idea of generative adversarial networks (GANs) [39], which achieve balance by gaming the discriminator and the generator and capturing the internal distribution of the data. DCGANs [40], [41] introduce the convolutional neural network (CNN) into the generative model and the discriminative model. The advantages of DCGANs are as follows: (1) the pooling layer in the convolutional network is replaced with a convolutional layer with the corresponding step size; (2) the batch normalization layer is used in the generative model and the discriminative model; (3) the full connection layer in the network is removed; (4) the rectified linear unit (ReLu) activation function is used in the generative model; (5) the Leaky ReLu activation function is used in the discriminative model; and (6) the complex nonlinear characteristics of the deep convolutional generative adversarial networks are leveraged to improve the resistance to brute-force attacks of the encryption system and key;(7) Due to the limited precision effect, the chaotic sequence generated by chaotic system will show a certain degree of periodicity, however, DGANs can eliminate periodicity by training chaotic sequences, which is making the sequence more stochastic and complex to well meet the requirements of cryptography. At the same time, training DCGAN models is more stable and easier to carry out, which simplifies the generation of data.

The random sequence occupies an important role in cryptography, as almost all cryptographic algorithms use it as a key. Therefore, a high-quality random sequence is very important to ensure the information security of a system. A random sequence generator is divided into a pseudo-random generator and a physical random generator. However, with the development of computer technology, they do not meet the needs of information security. When the random sequence is a fusion operation in which cycling occurs, the sequence is unpredictable, exhibits non-reproducibility and can meet the requirements of an information security system regarding the uncertainty of the random sequence.

A new key stream sequence generator is proposed, which is a combination of the proposed new hyperchaotic system (2), and the DCGANs. It applies the above theory and generates a key stream sequence with a non-cyclical nature, stochastic characteristics and complexity. The block diagram is shown in Figure 6.

TABLE 5. Approximate entropy (ApEn) of the random sequence generated.

Sequence	z_i^1	z_i^2	z_i^3	z_i^4
Result	2.0229	2.0527	2.0228	2.0364

TABLE 6. Z1 test of the random sequence generated.

Sequence	z_i^1	z_i^2	z_i^3	z_i^4
Result	0.9959	0.9973	0.9955	0.9975

The steps of the key stream generator include the following:

Step 1: Using the new four-dimensional hyperchaotic system (2), four chaotic sequences $\{x_1\}$, $\{x_2\}$, $\{x_3\}$, $\{x_4\}$ are generated under the initial conditions.

Step 2: The above four chaotic sequences $\{x_1\}$, $\{x_2\}$, $\{x_3\}$ and $\{x_4\}$ are the real data, and a number in [0, 1] is the random noise. After training the DCGANs over multiple rounds, the sequences $\{y_1\}$, $\{y_2\}$, $\{y_3\}$ and $\{y_4\}$ are generated by the generator.

Step 3: The sequences $\{y_1\}$, $\{y_2\}$, $\{y_3\}$ and $\{y_4\}$ are mixed via the fusion sequence generator (FSG) according to equation (9-12) to generate the four-dimensional pseudo-random sequence $\{z_i^1\}$, $\{z_i^2\}$, $\{z_i^3\}$ and $\{z_i^4\} \in \{z_i^j\}$ with $j = 1, 2, 3, 4$ and $i = 1, 2, ...M \times N$,

$$z_i^1 = \left|\left\lfloor\left|y_i^1 + y_i^2\right| {}^*10^8 \bmod 256\right\rfloor\right| \tag{9}$$

$$z_i^2 = \left|\left\lfloor\left|y_i^2 + y_i^3\right| {}^*10^8 \bmod 256\right\rfloor\right| \tag{10}$$

$$z_i^3 = \left|\left\lfloor\left|y_i^3 + y_i^4\right| {}^*10^8 \bmod 256\right\rfloor\right| \tag{11}$$

$$z_i^4 = \left|\left\lfloor\left|y_i^1 + y_i^2 + y_i^3 + y_i^4\right| {}^*10^8 \bmod 256\right\rfloor\right| \tag{12}$$

where mod is the modulo operation. According to Section II regarding the approximate entropy and Z1 test, the results of the sequence $\{z_i^j\}$ are as shown in Tables 5-6.

Table 5-6 shows that the approximate entropy and Z1 test of the sequence generated by the FSG is relatively large, which shows that the complexity and randomness of the fusion sequence is high.

IV. IMAGE ENCRYPTION AND DECRYPTION ALGORITHM

To improve the security and anti-attack ability of the colour image encryption system, a colour image encryption algorithm based on the Feistel network, image pixel scrambling and the diffusion mechanism is proposed. The encryption and decryption block diagram is shown in Figure 7.

A. ENCRYPTION PROCESS

The research on colour image cryptography has shown that the common encryption algorithm is more vulnerable to attack given its low sensitivity to plaintext images due to

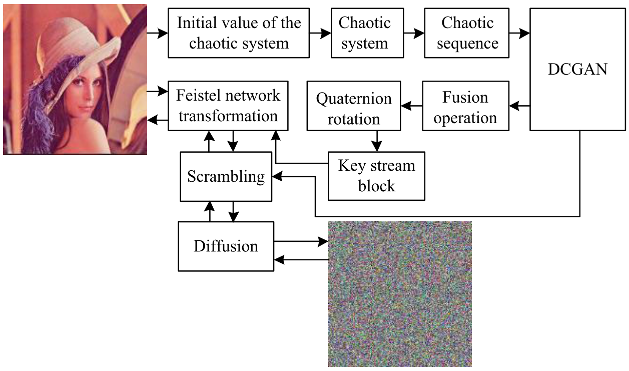


FIGURE 7. Block diagram of image encryption and decryption.

the strong correlation among the R, G and B channels in colour images, The Feistel network is a symmetric cipher processing architecture, and the processes of encrypting and decrypting information are very similar, often even the same, thus offering good security. Therefore, combining the key stream with the improved Feistel network and the overall scrambling and diffusion of image pixels is proposed. The encryption algorithm can reduce the correlation among the three channels of colour images and has high sensitivity to plaintext images since it is able to resist the known plaintext and chosen-plaintext attacks. This process consists of the following steps:

Step 1: We use plaintext image to generate the initial value of hyperchaotic system, which is controlled to generate chaotic sequence. It solves the problem that the key is not related to plaintext in image encryption algorithm based on chaotic system, and improves the security of key. The plaintext colour image P matrix of size $M \times N$, where M, N are the length of the column and row, respectively, in which every pixel is decomposed into R, G, and B channels. Then, the three-channel image pixels obtained above are converted into the 1D image pixel matrices $\{R_{1,}R_2, \ldots R_{M\times N}\}, \{G_{1,}G_2, \ldots G_{M\times N}\}$, and $\{B_{1,}B_2, \ldots B_{M\times N}\}$, which are used to calculate the initial values $x(1), x(2), x(3)$ and $x(4)$ of the new hyperchaotic system (2). The process is as follows:

$$x(1) = (\sum_{i=1}^{M\times N} R_i + 256^2)/(2^{23} + 256^2) \tag{13}$$

$$x(2) = (\sum_{i=1}^{M\times N} G_i + 256^2)/(2^{23} + 256^2) \tag{14}$$

$$x(3) = (\sum_{i=1}^{M\times N} B_i + 256^2)/(2^{23} + 256^2) \tag{15}$$

$$x(4) = \mathrm{mod}((x(3)^* 10^8), 1) \tag{16}$$

Step 2: The chaotic initial value is employed in the new hyperchaotic system, which involves $M \times (3 \times N)$ iterations; then, the chaotic sequence $\{x_1\}, \{x_2\}, \{x_3\}$ and $\{x_4\}$ can be calculated. It is sent to the DCGAN model as real data, and model training is performed, in which the sequence generated $\{y_1\}, \{y_2\}, \{y_3\}$ and $\{y_4\}$ by the generator is utilized for the fusion operation to generate a pseudo-random sequence $\{z_i^1\}, \{z_i^2\}, \{z_i^3\}$ and $\{z_i^4\}, i = 1, 2, \ldots, M \times N$ with higher complexity at the end of model training.

Quaternions, which are also known as hypercomplex numbers [42], were first proposed in 1843 and consists of real numbers and three imaginary numbers: i, j and k. The equation is defined as follows:

$$q = w + xi + yj + zk \tag{17}$$

where w, x, y and z are real numbers, and the matrix of quaternion rotation can be expressed as follows:
After a quaternion rotation transformation is performed, the key block matrix is generated by iterating the chaotic sequence generated by the chaotic system, which is applied to image encryption. Utilization of the one-time pad algorithm increases the difficulty of key cracking and ensures the security of the system.

The key stream block is generated iteratively by using the random sequences $\{z_i^1\}, \{z_i^2\}, \{z_i^3\}$ and $\{z_i^4\}$, according to the quaternion rotation transformation expression (18), as shown at the bottom of the next page, into the form of equation (19), as shown at the bottom of the next page.
where mod is modulo operation, and N is the sequence length. So the pseudo-random sequence is then converted to a key stream block K_i for encryption algorithm.

Step 3: The three channels $R_{M\times N}, G_{M\times N}$ and $B_{M\times N}$ of each image pixel are divided into the left sub-block $L_i^j(i = 1, 2, \ldots M \times (N/2), j = R, G, B)$ and the right sub-block $R_i^j(i = 1, 2, \ldots M \times (N/2), j = R, G, B)$, where K_i is the key stream block. A single round of the improved Feistel network encryption and decryption process is as follows:

$$F = \mathrm{mod}(K_i R_i^j, 256) \tag{21}$$

$$R_{i+1}^j = L_i^j \oplus F \tag{22}$$

$$L_{i+1}^j = \mathrm{mod}(R_i^j + R_{i+1}^j, 256) \tag{23}$$

The single-round decryption process is as follows:

$$R_i^j = \mathrm{mod}(L_{i+1}^j - R_{i+1}^j, 256) \tag{24}$$

$$F = \mathrm{mod}(K_i R_i^j, 256) \tag{25}$$

$$L_i^j = R_{i+1}^j \oplus F \tag{26}$$

where mod($\cdot$) is the modular operation, $\oplus$ is the xor operation, and $F(\cdot)$ is the round function. The block diagram of the improved encryption algorithm for the Feistel network is shown in Figure 8.

Step 4: Two blocks L_i^j and R_i^j are merged and spliced after 30 rounds of iterations to obtain the ciphertext image M_i^j, with $i = 1, 2, \ldots, M \times N$ and $j = R, G, B$.

The improved Feistel network of the 30-round encryption process is shown in Algorithm 1.

Step 5: The ciphertext image M_i^j obtained above is converted into the one-dimensional image pixel matrix $W = \{w_i\}$, with $i = 1, 2, \ldots, M \times (3 \times N)$.

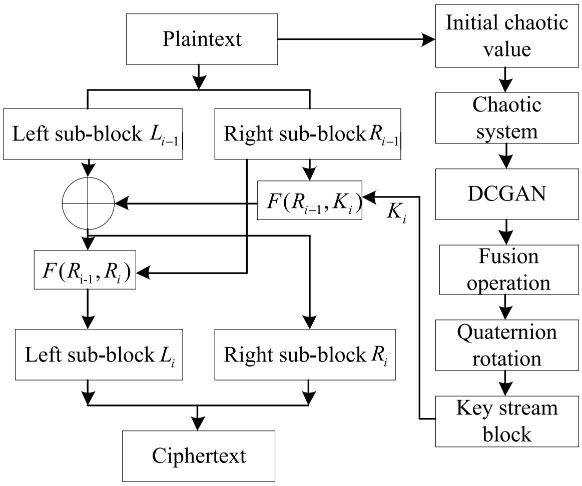


FIGURE 8. **Encryption block diagram of the improved Feistel network.**

Algorithm 1 Encryption Process

```
Read $P$, $K_i$
  $L_1 = $ Left half of $P$
  $R_1 = $ Right half of $P$
for $j = 1$ to 30
  for $i = 1$ to $M \times (N/2)$
      $R_i = L_{i-1} \oplus (\mathrm{mod}(KR_{i-1}, 256))$
      $L_i = \mathrm{mod}(R_{i-1} + R_i, 256)$
  end
end
  $C = L_i||R_i$, where || is the connection symbol
```

Step 6: Obtain the permutation position matrix $Z = \{z_i\}$, with $i = 1, 2, \ldots, M \times (3 \times N)$ by sorting the fusion sequence $\{z_i^j\}$, in ascending order.

Step 7: Obtain the overall pixel scrambling matrix W' by using the permutation position matrix and the image pixel matrix W. The process is as follows:

$$W_i' = W(Z_i) \tag{27}$$

Step 8: Convert W' into the W_i^j matrix with a size of $i = M \times N, j = 1, 2, 3, 4$ and convert W_i^j into one-dimensional matrices d_i^1, d_i^2, and d_i^3. Then, the pixel diffusion operation is as follows:

$$sum = (\sum_{i=1}^{M\times N} d_i^1 + \sum_{i=1}^{M\times N} d_i^2 + \sum_{i=1}^{M\times N} d_i^3) \tag{28}$$

$$\beta = sum - (d_1^1 + d_1^2 + d_1^3) \tag{29}$$

$$CR_0 = \left|\beta/(256^5)^*(10^{10}) \bmod 256\right| \tag{30}$$

$$CG_0 = \left|\beta/(256^6)^*(10^{10}) \bmod 256\right| \tag{31}$$

$$CB_0 = \left|\beta/(256^7)^*(10^{10}) \bmod 256\right| \tag{32}$$

$$CR_i = \mathrm{bitxor}((d_i^1 + CR_{i-1} + CG_{i-1}) \bmod 256, z_i^1) \tag{33}$$

$$CG_i = \mathrm{bitxor}((d_i^2 + CG_{i-1} + CB_{i-1}) \bmod 256, z_i^2) \tag{34}$$

$$CB_i = \mathrm{bitxor}((d_i^3 + CB_{i-1} + CR_{i-1}) \bmod 256, z_i^3) \quad i = 1, 2, \ldots, M \times N \tag{35}$$

where mod(·) is the modular operation, bitxor(·) is the xor operation, and CR_i, CG_i and CB_i are the final ciphertext sequences.

Step 9: Convert CR_i, CG_i and CB_i into the ciphertext image matrix c with a size of $M \times N$.

$$C = CR_i||CG_i||CB_i \quad i = 1, 2, \ldots, M \times N \tag{36}$$

B. DECRYPTION PROCESS

The decryption algorithm involves the inverse of the above process and consists of the following steps:

Step 1: According to Section III, generate the fusion sequence $\{z_i^j\}$, key stream block K_i.

Step 2: Perform pixel inverse diffusion on the ciphertext image C by using the fusion sequence $\{z_i^j\}$, according to formulas (35), (36), (37), to obtain matrices d_i^1, d_i^2 and d_i^3.

$$d_i^1 = (\mathrm{bitxor}(CR_i, z_i^1) - CR_{i-1} - CG_{i-1}) \bmod 256 \tag{37}$$

$$d_i^2 = (\mathrm{bitxor}(CG_i, z_i^2) - CG_{i-1} - CB_{i-1}) \bmod 256 \tag{38}$$

$$d_i^3 = (\mathrm{bitxor}(CB_i, z_i^3) - CB_{i-1} - CR_{i-1}) \bmod 256 \quad i = 1, 2, \ldots, M \times N \tag{39}$$

Step 3: Convert d_i^1, d_i^2 and d_i^3 into the matrix W' with a size of $M \times (3 \times N)$ and conduct the pixel inverse overall scrambling to obtain.

$$T(q) = \begin{bmatrix} w^2 + x^2 + y^2 - z^2 & 2xy - 2wz & 2xz + 2wy \\ 2wz + 2xy & w^2 - x^2 + y^2 - z^2 & 2yz - 2wx \\ 2xz - 2wy & 2yz + 2wz & w^2 - x^2 - y^2 + z^2 \end{bmatrix} \tag{18}$$

$$K_i = \begin{bmatrix} (z_4^i)^2 + (z_1^i)^2 - (z_2^i)^2 - (z_3^i)^2 & 2(z_1^i)(z_2^i) - 2(z_4^i)(z_3^i) & 2(z_1^i)(z_3^i) + 2(z_4^i)(z_2^i) \\ 2(z_4^i)(z_3^i) + 2(z_1^i)(z_2^i) & (z_4^i)^2 - (z_1^i)^2 + (z_2^i)^2 - (z_3^i)^2 & 2(z_2^i)(z_3^i) - 2(z_4^i)(z_1^i) \\ 2(z_1^i)(z_3^i) - 2(z_4^i)(z_2^i) & 2(z_2^i)(z_3^i) + 2(z_4^i)(z_3^i) & (z_4^i)^2 - (z_1^i)^2 - (z_2^i)^2 + (z_3^i)^2 \end{bmatrix} \tag{19}$$

$$K_i = |K_i \bmod 257| \quad i = 1, 2, \ldots M \times (N/2) \tag{20}$$

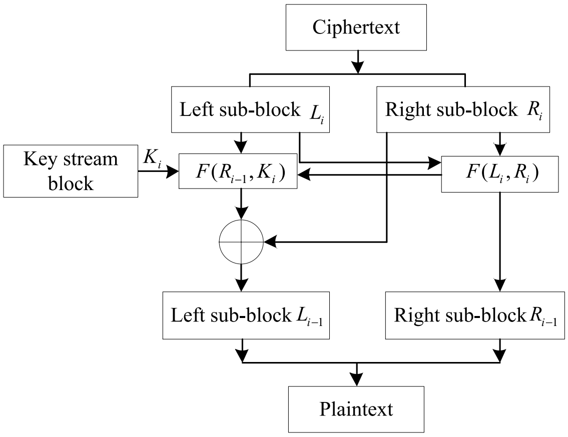


FIGURE 9. **The decryption block diagram of the improved Feistel network.**

Step 4: Convert W into the matrix M_i^j, with $i = 1, 2, \ldots, M \times N$ and $j = R, G, B$, and combine key stream block K_i with the decryption process of the improved Feistel network, obtain the plaintext image P. The block diagram of the improved decryption algorithm for the Feistel network is shown in Figure 9.

The improved Feistel network of the 30-round decryption process is shown in Algorithm 2.

Algorithm 2 Decryption Process

```
Read $C, K_i$
  $L_i$ = Left half of $C$
  $R_i$ = right half of $C$
for $j = 1$ to $30$
  for $i = 1$ to $M \times (N/2)$
      $R_{i-1} = \mathrm{mod}(L_i - R_i, 256)$
      $L_{i-1} = R_i \oplus (\mathrm{mod}(KR_{i-1}, 256))$
  end
end
  $P = L_1 || R_1$ where || is the connection symbol
```

V. ENCRYPTION RESULTS AND SECURITY ANALYSIS

In the experiment, the Lena, Ship, Fruits, and Tulips images of size (256 × 256) were selected as plaintext images for encryption. The control parameters (a, b, and c) of hyperchaotic system (2) were fixed at $(-6, 59, 43)$, and the initial value was calculated according to the input plaintext image, for example, from the Lena image as $x(1) = 1.3991$, $x(2) = 0.7729$, $x(3) = 0.8212$, and $x(4) = 0.5740$. In the DCGAN model with 10 rounds of training, the learning rate was 0.0001, and each round of training sent 50 batches of data, the size of which was (256 × 256). Python 3.5 and MATLAB 2018b were used on a computer with an Intel Core i-7, 2.3 GHz CPU, 8 GB of memory and a 250-GB hard disk running the Windows 10 Professional operating system. The encryption and decryption results are shown in Figure 10.

Figure 10 shows that the encryption effect of the algorithm is good and that it cannot obtain any plaintext information

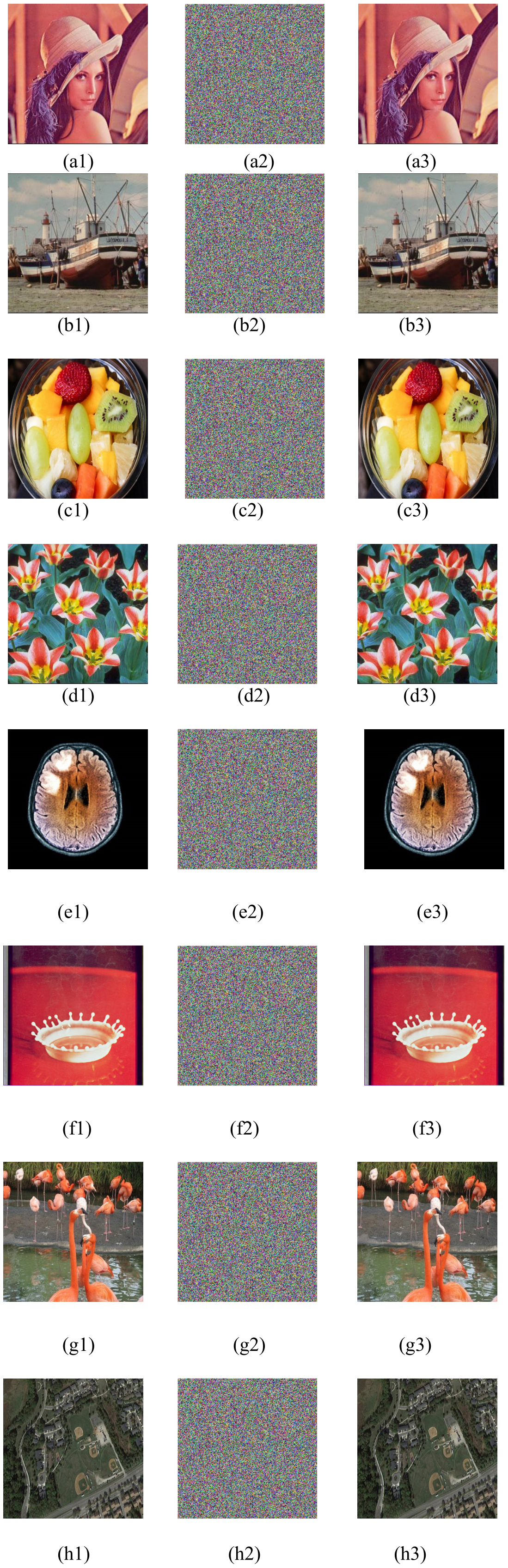


FIGURE 10. **Plain images and their encrypted results. (a1, b1, c1, d1, e1, f1, g1, h1, i1, j1): plaintext; (a2, b2, c2, d2, e2, f2, g2, h2, j2): ciphertext; (a3, b3, c3, d3, e3, f3, g3, h3, i3, j3): decrypted image.**

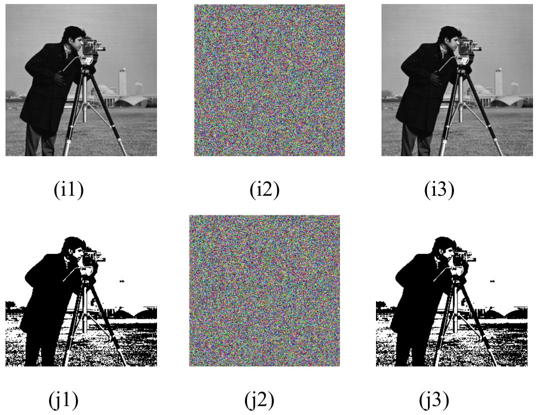


FIGURE 10. ***(Continued.)*** **Plain images and their encrypted results. (a1, b1, c1, d1, e1, f1, g1, h1, i1, j1): plaintext; (a2, b2, c2, d2, e2, f2, g2, h2, j2): ciphertext; (a3, b3, c3, d3, e3, f3, g3, h3, i3, j3): decrypted image.**

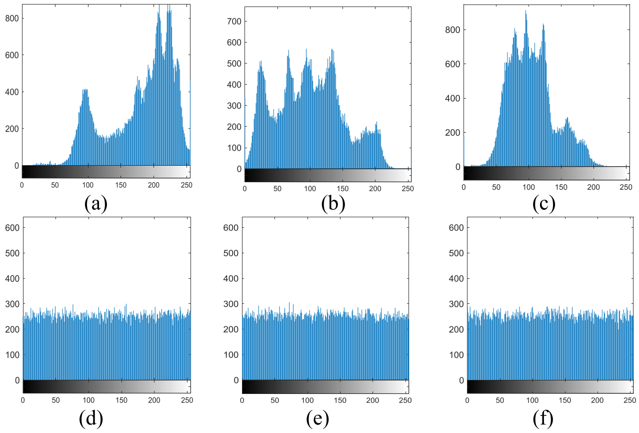


FIGURE 11. **Histograms of the Lena plaintext and ciphertext images. (a, b, c): The histograms of the plaintext image encryption in the red, green and blue channels, respectively; (d, e, f): the histograms of the ciphertext image encryption in the red, green and blue channels, respectively.**

from the ciphertext image, which shows the effectiveness of the proposed encryption algorithm.

A. HISTOGRAM ANALYSIS

Histograms reflect the statistical characteristics of the relationship between the grey level and frequency of an image, and good encryption algorithms can more evenly distribute ciphertext image pixels. The histograms of the Lena image are shown in Figure 11.

Figure 10 shows that the histogram of the ciphertext image is uniform, which is obviously different from that of the original image; thus, the proposed encryption algorithm is good at protecting the information of the image against statistical attacks.

To analyse the distribution of pixel values of ciphertext images, the variance of the histogram is used to evaluate the uniformity of ciphertext image [43]. The variance of the histogram is defined as follows:

TABLE 7. **Variance of histogram.**

Image/Algorithm	Channel	Variance
CT	Red	222.3281
	Green	213.8047
	Blue	228.0938
Composite	Red	219.7813
	Green	231.9375
	Blue	202.4766
Remote sensing	Red	226.2266
	Green	209.9609
	Blue	234.7031
Proposed (Lena)	Red	213.2422
	Green	221.4609
	Blue	232.8125
Ref. [52] (Lena)	Red	250.6819
	Green	243.1290
	Blue	236.3140
Ref. [49] (Lena)	Red	259.3906
	Green	232.2188
	Blue	245.2500
Ref. [27] (Lena)	Red	231.5703
	Green	232.1641
	Blue	281.3047
Ref. [28] (Lena)	Red	248.5313
	Green	216.9375
	Blue	277.1016
Ref. [48] (Lena)	Red	266.2734
	Green	238.0625
	Blue	238.2109

$$\mathrm{var} = \frac{1}{n^2}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{1}{2}(P_i - P_j)^2 \qquad (40)$$

where P_i and P_j are the pixel values of the image. When the variance is smaller, the pixel distribution of the encrypted image will appear more uniform. To assess the uniformity of the pixels in the ciphertext image, the Lena ciphertext image, CT ciphertext image, composite ciphertext image, and remote sensing ciphertext image are evaluated using the variance of the histogram. The proposed encryption algorithm is compared with the algorithms in Ref. [52], Ref. [49], Ref. [27], Ref. [28], and Ref. [48], as shown in Table 7.

From the results, we can see that the variance of the histogram of the Lena ciphertext image obtained by the proposed encryption algorithm is lower than the variances obtained with the other algorithms. Therefore, the proposed encryption algorithm is secure.

Chi-square test can be used to test the uniformity of histogram of ciphertext image. Low chi-square value indicates that the uniformity of histogram is better. For chi-square test results, at the 5% and 1% significance levels, the chi-square value was $x^2_{255.0.05} = 293.2478$ and $x^2_{255.0.01} = 310.457$,

TABLE 8. Chi-squar of histogram.

Image/Algorithm	Channel	x^2
CT	Red	236.4658
	Green	229.8015
	Blue	234.4376
Composite	Red	277.4675
	Green	265.9762
	Blue	238.7922
Remote sensing	Red	215.6421
	Green	229.8015
	Blue	212.0252
Proposed (Lena)	Red	213.2422
	Green	221.4609
	Blue	232.8125
Ref. [52] (Lena)	Red	250.6819
	Green	243.1290
	Blue	236.3140
Ref. [49] (Lena)	Red	259.3906
	Green	232.2188
	Blue	245.2500
Ref. [27] (Lena)	Red	231.5703
	Green	232.1641
	Blue	281.3047
Ref. [28] (Lena)	Red	248.5313
	Green	216.9375
	Blue	277.1016
Ref. [48] (Lena)	Red	266.2734
	Green	238.0625
	Blue	238.2109

which are defined as follows:

$$x^2 = \sum_{k=1}^{256} \frac{(v_k - 256)^2}{256} \tag{41}$$

where v_k is the frequency of each gray level. In order to test the histogram uniformity of ciphertext image, the Lena ciphertext image, CT ciphertext image, composite ciphertext image and remote sensing ciphertext image are evaluated using the chi-square test. The proposed encryption algorithm is compared with the algorithms in Ref. [52], Ref. [49], Ref. [27], Ref. [28], and Ref. [48], as shown in Table 8.

From the results, we can see that the chi-square test of the Lena ciphertext image obtained by the proposed encryption algorithm is lower than the variances obtained with the other algorithms. Therefore, the proposed encryption algorithm is secure.

B. MAXIMUM DEVIATION AND IRREGULAR DEVIATION ANALYSIS

The maximum deviation (M_D) and irregular deviation (I_D) measure the security of encryption algorithm by calculating the pixel deviation of plaintext image and ciphertext image, which is defined as follows:

$$M_D = (\frac{D_0 + D_{n-1}}{2}) + \sum_{i=1}^{m-2} D_g \tag{42}$$

TABLE 9. Maximun deviation OF ciphertext image.

Image/Algorithm	Channel	M_D
CT	Red	58317
	Green	56392
	Blue	54255
Composite	Red	51975
	Green	51272
	Blue	46940
Remote sensing	Red	44829
	Green	50967
	Blue	54800
Proposed (Lena)	Red	53624
	Green	44606
	Blue	50688
Ref. [52] (Lena)	Red	55142
	Green	58746
	Blue	51092
Ref. [49] (Lena)	Red	44278
	Green	48809
	Blue	47176
Ref. [27] (Lena)	Red	39083
	Green	38757
	Blue	36159
Ref. [28] (Lena)	Red	48070
	Green	44537
	Blue	41218
Ref. [48] (Lena)	Red	57718
	Green	58732
	Blue	49914

$$I_D = \sum_{i=0}^{N-1} H_{D_g} \tag{43}$$

$$H_{D_g} = \left| H_g - A_h \right| \tag{44}$$

where D_g is the amplitude difference of histogram between plaintext image and ciphertext image at index g. M, N are the number of pixels. H_i is the amplitude of histogram at index i, A_h is the average sum of histogram values. The larger the maximum deviation is, the more uniform the distribution of image pixels is. The smaller the irregular bias value is, the more uniform the pixel distribution of the image could be. The results of maximum deviation and irregular deviation of the proposed algorithm are compared to the encryption results in Ref. [52], Ref. [49], Ref. [27], Ref. [28], and Ref. [48] shown in Table 9-10.

From the results, we can see that the maximum deviation and irregular deviation of the proposed encryption algorithm is better than the other encryption algorithms. Therefore, the proposed encryption algorithm is secure.

C. KEY SPACE ANALYSIS

To prevent violent attacks, a good encryption system must contain a large key space. The key space of the proposed encryption algorithm consists of the initial values and control parameters of the hyperchaotic system. The hyperchaotic

TABLE 10. **Irregular deviation OF ciphertext image.**

Image/Algorithm	Channel	I_D
CT	Red	38623
	Green	48439
	Blue	44264
Composite	Red	41268
	Green	40947
	Blue	44971
Remote sensing	Red	41268
	Green	44764
	Blue	44126
Proposed (Lena)	Red	38188
	Green	36292
	Blue	37282
Ref. [52] (Lena)	Red	53253
	Green	56722
	Blue	53606
Ref. [49] (Lena)	Red	54982
	Green	49011
	Blue	41497
Ref. [27] (Lena)	Red	54982
	Green	55719
	Blue	48370
Ref. [28] (Lena)	Red	45445
	Green	41805
	Blue	43606
Ref. [48] (Lena)	Red	55884
	Green	56722
	Blue	54710

system proposed in this paper has three control parameters and four initial values. If dual-precision representation is used up to 14 digits after the decimal point, the total key space can reach 10^{98}, that is, the key length is approximately $\log_2(10^{98}) \approx 326 bits$. Generally, an algorithm key length of 128 bits is considered safe [44]; hence, the key space of the proposed encryption algorithm is secure against brute-force attacks.

D. CORRELATION ANALYSIS

A good encryption algorithm should significantly destroy the correlation of adjacent pixels [45]. The correlation coefficient is calculated as follows in (45), (46), and (47):

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{45}$$

$$D(x) = \frac{1}{N}\sum_{j=1}^{N}(x_j - \frac{1}{N}\sum_{i=1}^{N}x_i)^2 \tag{46}$$

$$\operatorname{cov}(x, y) = \frac{1}{N}\sum_{j=1}^{N}(x_j - \frac{1}{N}\sum_{j=1}^{N}x_i)(y_i-\frac{1}{N}\sum_{i=1}^{N}y_i) \tag{47}$$

where x_i and y_i are the pixel value sizes of the corresponding positions in the image. When the correlation coefficient of adjacent pixels in a ciphertext image is close to 0, the encryption algorithm is safer. In the horizontal, vertical and diagonal directions of the plaintext image and ciphertext image, 10,000 pairs of adjacent pixels are randomly selected for the test. To visually illustrate the correlation of adjacent pixels, the correlations of the Lena plaintext image and ciphertext image in the horizontal, vertical and diagonal directions by the proposed encryption algorithm are shown in Figure 12. The correlation coefficients of adjacent pixels in the horizontal, vertical and diagonal directions for the CT, composite and remote sensing ciphertext images by the proposed encryption algorithm are shown. For comparison, the correlation coefficients of adjacent pixel results in Ref. [49], Ref. [40], Ref. [51], Ref. [52], Ref. [18], Ref. [21], Ref. [27], Ref. [28], and Ref. [48] are shown in Table 11.

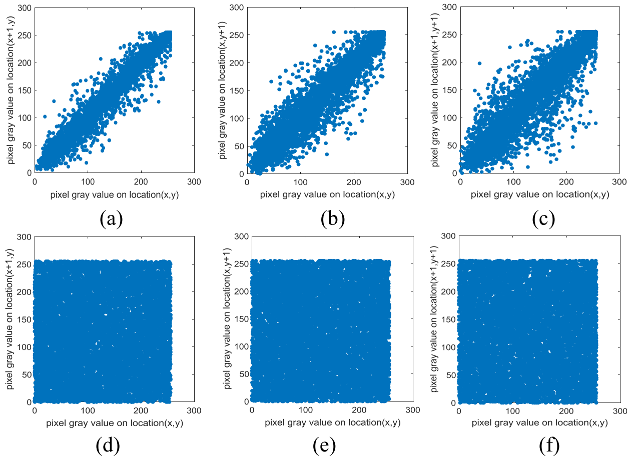


FIGURE 12. **Red spectrum correlation distribution results of adjacent pixels in the Lena plaintext and ciphertext images: (a), (b), (c) horizontal, vertical, and diagonal correlation distribution results of the Lena plaintext image, respectively; (d), (e), (f) horizontal, vertical, and diagonal correlation distribution results of the Lena ciphertext image, respectively.**

Figure 12 and Table 11 show that there is almost no relationship between the adjacent points in the ciphertext image, and the correlation coefficient of adjacent pixels in the plaintext image is close to 1, while that of the ciphertext image is close to 0. Therefore, the ciphertext image obtained by the proposed encryption algorithm has an excellent confusion diffusion ability, and the strong correlation among adjacent pixels is reduced in the ciphertext image produced by the proposed algorithm.

E. ENTROPY ANALYSIS

Global entropy is an important measure to reflect the randomness of information. The more uniform the image grey value distribution is, the greater the global entropy [46]. The formula used to calculate the global entropy is as follows:

$$H = -\sum_{i-1}^{L} P_i \log P_i \tag{48}$$

where P_i is the pixel probability, denoting the grey value, and L is the grey image pixel level. The cipher image information entropy is near 8, which it means the more uniform the grey

TABLE 11. Pixel correlation coefficient of ciphertext images.

Image/Algorithm	Channel	H	V	D
CT	Red	-0.0019	-0.0047	0.0037
	Green	0.0000	0.0071	-0.0008
	Blue	-0.0175	0.0189	0.0162
Composite	Red	-0.0079	0.0076	-0.0098
	Green	-0.0102	0.0020	0.0044
	Blue	0.0106	0.0054	-0.0174
Remote sensing	Red	0.0063	-0.0029	0.0237
	Green	0.0040	0.0046	0.0003
	Blue	-0.0138	-0.0083	-0.0210
Lena plaintext	Red	0.9581	0.9303	0.9073
	Green	0.9626	0.9356	0.9050
	Blue	0.9204	0.8742	0.8273
Proposed(Lena)	Red	0.0069	-0.0109	-0.0049
	Green	-0.0055	-0.0032	0.0110
	Blue	-0.0057	-0.0093	-0.0003
Ref. [49] (Lena)	Red	-0.0180	-0.0170	-0.0056
	Green	-0.0066	0.0140	-0.0063
	Blue	0.0157	-0.0011	0.0081
Ref. [40] (Lena)	Red	0.0831	0.2877	0.0335
	Green	0.1196	0.6695	0.0717
	Blue	0.0253	0.6889	0.0293
Ref. [51] (Lena)	Red	-0.1054	0.0008	-0.0157
	Green	-0.0611	-0.0071	0.0101
	Blue	0.0436	0.0126	-0.0040
Ref. [52] (Lena)	Red	0.0298	0.0083	-0.0110
	Green	0.0979	-0.0054	0.0049
	Blue	0.0173	0.0003	0.0099
Ref. [18] (Lena)	Red	-0.0104	0.0115	0.0080
	Green	0.0156	0.0048	-0.0106
	Blue	-0.0057	0.0042	-0.0185
Ref. [21] (Lena)	Red	0.0490	0.0476	0.0476
	Green	0.0464	0.0428	0.0336
	Blue	0.0356	0.0288	0.0217
Ref. [27] (Lena)	Red	0.0015	-0.0084	-0.0117
	Green	0.0004	0.0051	0.0202
	Blue	0.0219	0.0025	0.0078
Ref. [28] (Lena)	Red	0.0090	0.0064	-0.0148
	Green	0.0019	-0.0061	0.0027
	Blue	-0.0048	0.0079	-0.0014
Ref. [48] (Lena)	Red	-0.0001	-0.0148	0.0164
	Green	0.0011	-0.0023	-0.0134
	Blue	0.0152	0.0069	-0.0087

value distribution of the ciphertext image is, the better the ability to resist statistical attacks is. Table 7 lists the global entropy test results of different ciphertext images, and the proposed encryption algorithm is used to encrypt the Lena image to obtain the cipher image global entropy. The results are compared to the encryption results in Ref. [51], Ref. [52], Ref. [18], Ref. [21], Ref. [27], Ref. [28], and Ref. [48] shown in Table 12.

Table 12 shows that the global entropy of the ciphertext image based on the proposed encryption algorithm is near 8; thus, the ciphertext image is difficult to decrypt.

TABLE 12. Entropy of the ciphertext image.

Image/Algorithm	Channel		
	Red	Green	Blue
CT	7.9888	7.9892	7.9896
Composite	7.9884	7.9894	7.9893
Remote sensing	7.9893	7.9893	7.9891
Proposed(Lena)	7.9894	7.9896	7.9892
Ref. [51] (Lena)	7.9884	7.9876	7.9877
Ref. [52] (Lena)	7.9072	7.8402	7.9192
Ref. [18] (Lena)	7.9800	7.9894	7.8800
Ref. [21] (Lena)	7.9784	7.9771	7.9347
Ref. [27] (Lena)	7.9897	7.9899	7.9890
Ref. [28] (Lena)	7.9901	7.9900	7.9885
Ref. [48](Lean)	7.9892	7.9893	7.9895

TABLE 13. Local Entropy of the ciphertext image.

Image/Algorithm	Channel		
	Red	Green	Blue
CT	7.8127	7.8121	7.8165
Composite	7.8054	7.8105	7.8075
Remote sensing	7.8083	7.8126	7.8054
Proposed (Lena)	7.8091	7.8121	7.8165
Ref. [49] (Lena)	7.0923	7.4332	7.0117
Ref. [51] (Lena)	7.7963	7.7781	7.7966
Ref. [52] (Lena)	7.7266	7.6454	7.7329
Ref. [18] (Lena)	7.8043	7.8104	7.8075
Ref. [21] (Lena)	7.7248	7.7324	7.6788
Ref. [27] (Lena)	7.8039	7.8082	7.8060
Ref. [28] (Lena)	7.8123	7.8073	7.8080
Ref. [48] (Lena)	7.8068	7.8060	7.8150

The image grey value is 256, while the theoretical value of global entropy is 8; moreover, Wu y et al. proposed a calculation algorithm for local entropy based on the global entropy, which overcomes the shortcomings of global entropy [47]. The formula used to calculate the local Shannon entropy is as follows:

$$\overline{H} = \frac{1}{N}\sum_{j=1}^{N} H(B_j) \tag{49}$$

where B_j is a non-overlapping image block, and N is the number of sub-blocks. Local entropy is an improvement of global entropy. According to the algorithm described in the literature, 40 non-overlapping blocks with the size of 32×32 are tested. At this time, the corresponding theoretical value of local entropy is 7.8087. Table 13 lists the local entropy test results of different ciphertext images, and the proposed encryption algorithm is used to encrypt the Lena image to obtain the cipher image entropy. The results are compared to the encryption results in Ref. [49], Ref. [51], Ref. [52], Ref. [18], Ref. [21], Ref. [27], Ref. [28], and Ref. [48].

TABLE 14. Keys.

Key	$x(1)$	$x(2)$
Key 1	1.3991	0.7729
Key 2	$1.3991+10^{-15}$	0.7729
Key 3	1.3991	$0.7729+10^{-15}$
Key 4	1.3991	0.7729
Key 5	1.3991	0.7729

TABLE 15. Keys.

Key	$x(3)$	$x(4)$
Key 1	0.8212	0.5740
Key 2	0.8212	0.5740
Key 3	0.8212	0.5740
Key 4	0.8212	0.5740
Key 5	$0.8212+10^{-15}$	$0.5740+10^{-15}$

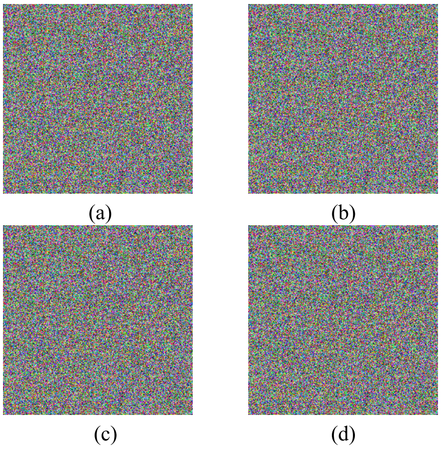


FIGURE 13. Key sensitivity analysis. (a): Decryption image by key 2; (b): decryption image by key 3; (c) decryption image by key 4; (d) decryption image by key 5.

Table 13 shows that the local entropy of the ciphertext image based on the proposed encryption algorithm is near 7.8087; thus, the ciphertext image is difficult to decrypt.

F. KEY SENSITIVITY ANALYSIS

Key sensitivity analysis refers to testing the sensitivity of an encryption system to the security key. A good encryption algorithm should ensure that the same plaintext is encrypted even with a slightly different security key, which can obtain completely different ciphertext images, and the plaintext image cannot be obtained. For example, the encryption key obtained from the Lena plaintext image is shown in Tables 14-15. The key stream is generated by the encryption key. On decryption, Key 2, Key 3, Key 4, and Key 5 in Table 9-10 are obtained by fine-tuning the initial value of the Lena plaintext image, which is carried out to generate fusion pseudo-random sequences as the key stream to decrypt the ciphertext image. The result is shown in Figure 13.

Figure 13 reveals that even if a difference exists between the initial values, the correct decryption image cannot be obtained. Therefore, the proposed encryption algorithm has high security.

G. GREY-LEVEL CO-OCCURRENCE MATRIX

The grey level co-occurrence matrix (GLCM) is used to study the spatial distribution uniformity of adjacent pixels in the ciphertext image. The matrix is constructed from pairwise values of grey level co-occurrence of pixels across the image [48]. In this paper, the contrast, correlation, energy and homogeneity of the co-occurrence matrix are used to study the spatial distribution uniformity of encryption image adjacent pixels, and the specific definitions are as follows.

1) CONTRAST

Contrast is used to describe the depth and clarity of the encryption image texture, and higher values of contrast reflect higher security of a ciphertext image. Contrast is defined as follows:

$$Contrast = \sum_{i}^{M}\sum_{j}^{N} P(i,j)^2 \tag{50}$$

where $P(i,j)$ denotes the coordinate values in the grey-level co-occurrence matrix.

2) CORRELATION

Correlation is used to measure the similarity of adjacent pixels in a given direction of an encryption image, and smaller values of correlation reflect higher security of a ciphertext image. Correlation is defined as follows:

$$Correlation = \left[\sum_{i}^{M}\sum_{j}^{N}((ij)P(i,j)) - \mu_x\mu_y\right]/\sigma_x\sigma_y \tag{51}$$

where $P(i,j)$ denotes the coordinate values in the grey-level co-occurrence matrix.

3) ENERGY

Energy is used to describe the texture, thickness and uniformity of an encrypted image, and smaller values of energy reflect higher security of a ciphertext image. Energy is defined as follows:

$$Energy = -\sum_{i}^{M}\sum_{j}^{N} P(i,j)\log P(i,j) \tag{52}$$

where $P(i,j)$ denotes the coordinate values in the grey-level co-occurrence matrix and is the logarithmic operation.

4) HOMOGENEITY

Homogeneity reflects how closely the elements in the GLCM are distributed along the GLCM diagonal, and smaller values of homogeneity reflect higher security of a ciphertext image.

TABLE 16. Contrast of the co-occurrence matrix for the ciphertext image.

Image	Channel	Contrast
Lena	Red	10.4936
	Green	10.4762
	Blue	10.5296
CT	Red	10.4744
	Green	10.5609
	Blue	10.4135
Composite	Red	10.4882
	Green	10.5022
	Blue	10.4509
Remote sensing	Red	10.5450
	Green	10.4859
	Blue	10.3715

TABLE 17. Correlation of the co-occurrence matrix for the ciphertext image.

Image	Channel	Correlation
Lena	Red	0.0003
	Green	0.0009
	Blue	-0.0040
CT	Red	0.0013
	Green	-0.0050
	Blue	0.0029
Composite	Red	-0.0013
	Green	0.0012
	Blue	0.0025
Remote sensing	Red	-0.0064
	Green	0.0016
	Blue	0.0065

TABLE 18. Energy of the co-occurrence matrix for the ciphertext image.

Image	Channel	Energy
Lena	Red	0.0156
	Green	0.0156
	Blue	0.0156
CT	Red	0.0156
	Green	0.0156
	Blue	0.0156
Composite	Red	0.0156
	Green	0.0156
	Blue	0.0156
Remote sensing	Red	0.0156
	Green	0.0156
	Blue	0.0156

TABLE 19. Homogeneity of the co-occurrence matrix for the ciphertext image.

Image	Channel	Homogeneity
Lena	Red	0.3897
	Green	0.3886
	Blue	0.3886
CT	Red	0.3901
	Green	0.3891
	Blue	0.3894
Composite	Red	0.3915
	Green	0.3890
	Blue	0.3893
Remote sensing	Red	0.3891
	Green	0.3890
	Blue	0.3909

Homogeneity is defined as follows:

$$Homogeneity = \sum_{i}^{M}\sum_{j}^{N} P(i,j)/(1+|(i-j)|) \tag{53}$$

where $P(i,j)$ denotes the coordinate values in the grey-level co-occurrence matrix.

The uniformity of the spatial distribution of adjacent pixels in the ciphertext image is assessed with the texture feature contrast of the grey-level co-occurrence matrix of the Lena, CT, composite, and remote sensing ciphertext images, as shown in Tables 16-19. The Lena ciphertext image values based on the proposed algorithm are compared with the values obtained in Ref. [50], Ref. [51], Ref. [52], Ref. [18], Ref. [21], Ref. [27], Ref. [28], and Ref. [48], which are shown in Tables 20.

Tables 16-20 show that the texture features of the grey-level co-occurrence matrix of the Lena, CT, composite, and remote sensing ciphertext images of the eighteen encryption algorithms are very similar, but the proposed encryption algorithm yields a low correlation and a better image encryption effect.

In addition, the two-dimensional histograms of the grey-level co-occurrence matrix of adjacent pixels in four different directions for the Lena plaintext image and ciphertext image obtained by the proposed algorithm are shown in Figures 14-15.

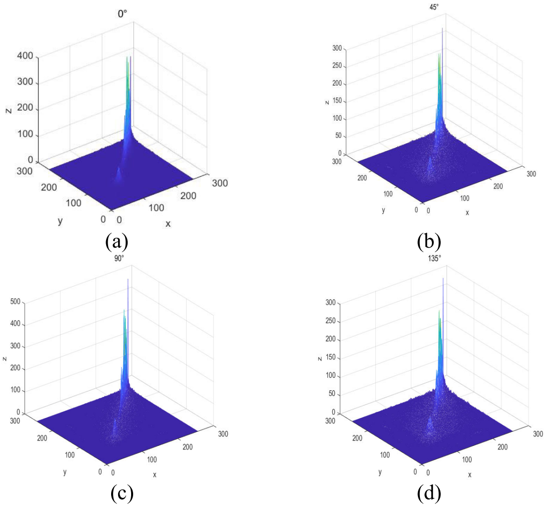
Figures 14-15 show that the ciphertext image and the two-dimensional histogram of the ciphertext image indicate the uniformity of the spatial distribution of adjacent pixels in the encrypted image; therefore, the proposed encryption algorithm yields adjacent pixels that have sufficient random characteristics

H. DIFFERENTIAL ANALYSIS

According to the principle of cryptography, a good encryption algorithm should be resistant to the differential attack. Therefore, the number of pixels change rate (NPCR) and the unified average changing intensity (UACI) have become important indicators to measure the image encryption algorithm's resistance to differential attacks. They represent the degree of change after randomly changing a certain pixel value of the plaintext image and indicate the proportion of the number of changes in the pixel values of the encrypted image

TABLE 20. The co-occurrence matrix for the ciphertext image.

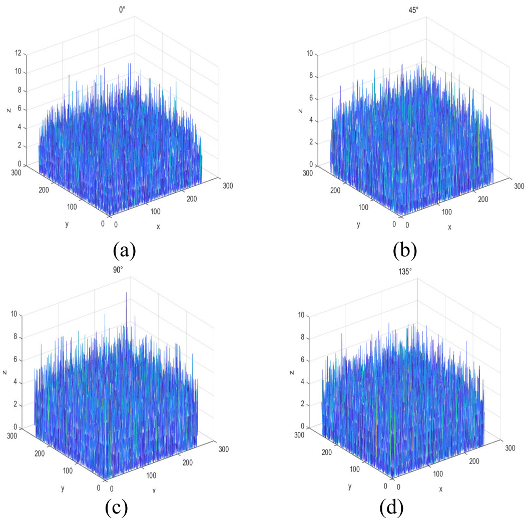
Algorithm	Channel	Contrast	Correlation	Energy	Homogeneity
Proposed	Red	10.4936	0.0003	0.0156	0.3897
	Green	10.4762	0.0009	0.0156	0.3896
	Blue	10.5296	-0.0019	0.0156	0.3896
Ref. [50]	Red	4.3317	0.2300	0.3382	0.7253
	Green	1.9958	0.6607	0.3986	0.8158
	Blue	1.9676	0.6651	0.3660	0.7847
Ref. [51]	Red	10.5063	-0.0019	0.0156	0.3897
	Green	10.5540	-0.0065	0.0156	0.3885
	Blue	10.4942	0.0019	0.0156	0.3909
Ref. [52]	Red	10.5705	0.0027	0.0157	0.3885
	Green	10.6283	0.0019	0.0160	0.3889
	Blue	10.6129	-0.0016	0.0156	0.3893
Ref. [18]	Red	10.4878	0.0001	0.0156	0.3887
	Green	10.4988	0.0027	0.0156	0.3897
	Blue	10.4370	0.0014	0.0156	0.3893
Ref. [21]	Red	10.1457	0.0601	0.0171	0.4189
	Green	10.1006	0.0558	0.0166	0.4162
	Blue	10.9830	0.0344	0.0185	0.4106
Ref. [27]	Red	10.4477	0.0072	0.0156	0.3894
	Green	10.3969	0.0062	0.0156	0.3914
	Blue	10.5112	0.0085	0.0156	0.3896
Ref. [28]	Red	10.4567	0.0045	0.0156	0.3900
	Green	10.4269	0.0001	0.0156	0.3916
	Blue	10.4545	-0.0017	0.0156	0.3888
Ref. [48]	Red	10.5438	-0.0038	0.0156	0.3897
	Green	10.5157	-0.0019	0.0156	0.3896
	Blue	10.5215	-0.0001	0.0156	0.3886



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

FIGURE 14. Two-dimensional histogram of the plaintext image in the red channel. (a) 0°; (b) 45°; (c) 90°; (d) 135°.

and the change degree. If the change of a pixel value of the plaintext image can change the ciphertext image to a great extent, it shows that the encryption algorithm has a strong ability to resist differential attacks [53], [54]. Values of the UACI $> 33.4\%$ and of the NPCR $> 99.6\%$ ensure that an image encryption algorithm is immune to differential attacks.



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

FIGURE 15. Two-dimensional histogram of the ciphertext image in the red channel. (a) 0°; (b) 45°; (c) 90°; (d) 135°.

Images with only one pixel value difference are tested with the encryption algorithm. The number of changed image pixels is a percentage of the total number of pixels, which is represented by the NPCR. For two images with only one pixel value difference, after the same encryption algorithm is run, the degree of image pixel change is represented by the UACI. Two images with only one pixel value difference are encrypted as C_1 and C_2, where $H(i, j)$ represents the difference in image pixel values and M, N is the image size.

$$H(i,j) = \begin{cases} 0 & C_1(i,j) = C_2(i,j) \\ 1 & C_1(i,j) \neq C_2(i,j) \end{cases} \tag{54}$$

$$NPCR = \frac{\sum_{i,j} H(i,j)}{MN} \times 100\% \tag{55}$$

$$UACI = \frac{\sum_{i,j} \frac{|C_1(i,j)-C_2(i,j)|}{255}}{MN} \times 100\% \tag{56}$$

Tables 16-18 list the NPCR and UACI test results obtained when the value of one pixel is changed using the different ciphertext images. For comparison, the NPCR and UACI values of the Lena ciphertext image attained by the proposed algorithm are presented with the values from Ref. [49], Ref. [50], Ref. [51], Ref. [52], Ref. [18], Ref. [21], Ref. [27], Ref. [28], and Ref. [48] in Tables 21-22.

Tables 21-22 reveal that compared with the algorithms in the literature, the proposed encryption algorithm achieves high performance, exhibiting values very close to their notional amounts.

I. CHOSEN-PLAINTEXT ATTACK ANALYSIS

According to the basic principles of modern cryptography, cryptanalysis refers to the study of ciphertext, keys and cipher systems, aiming to understand the principle of the encryption mechanisms and determine the loopholes of encryption

TABLE 21. The NPCR performance (%).

Image/Algorithm	Channel		
	Red	Green	Blue
CT	99.72	99.75	99.69
Composite	99.71	99.72	99.69
Remote sensing	99.53	99.62	99.61
Proposed (Lena)	99.72	99.66	99.69
Ref.[49](Lena)	99.58	99.62	99.61
Ref.[50](Lena)	99.61	99.61	99.60
Ref.[51](Lena)	99.63	99.61	99.63
Ref.[52] (Lena)	99.58	99.61	99.58
Ref. [18] (Lena)	99.61	99.62	99.63
Ref. [21] (Lena)	99.60	99.59	99.64
Ref. [27] (Lena)	99.61	99.62	99.61
Ref. [28] (Lena)	99.56	99.51	99.56
Ref. [48] (Lena)	99.62	99.62	99.63

TABLE 22. the UACI performance (%).

Image/Algorithm	Channel		
	Red	Green	Blue
CT	33.39	33.39	33.44
Composite	33.42	33.43	33.58
Remote sensing	33.40	33.39	33.34
Proposed (Lena)	33.39	33.43	33.57
Ref. [49] (Lena)	33.70	33.35	33.45
Ref. [50] (Lena)	33.48	33.42	33.41
Ref. [51] (Lena)	33.45	33.43	33.45
Ref. [52] (Lena)	33.30	33.42	33.53
Ref. [18] (Lena)	33.57	33.33	33.40
Ref. [21] (Lena)	33.06	30.59	27.60
Ref. [27] (Lena)	33.47	33.34	33.00
Ref. [28] (Lena)	33.31	33.41	33.44
Ref. [48] (Lena)	33.63	33.51	33.47

mechanisms. The common cryptanalysis techniques include ciphertext-only attacks, chosen-plaintext attacks, chosen ciphertext attacks, and known plaintext attacks, and the chosen-plaintext attack is the strongest attack. Therefore, if the encryption algorithm can resist the chosen-plaintext attack, then it can resist the other three attacks. The chosen-plaintext attack is thus used to analyse the security of the proposed encryption algorithm in this paper.

1) THE ASSOCIATION BETWEEN THE KEY AND PLAINTEXT

One of the most important advantages of combining the chaotic system and encryption algorithm is that the chaotic system can generate an infinite-length random sequence through a small number of initial values and control parameters and that the security of the image chaotic encryption mechanism can be greatly improved by key association plaintext. Therefore, it can effectively encrypt images with a large amount of data and ensure the security of the algorithm. In this paper, the initial value of system (2) is calculated by using different plaintexts (the calculation process is shown in (57), (58), (59), and (60)), and chaotic sequences are obtained to fuse and generate the key stream.

$$x(1) = (\sum_{i=1}^{M\times N} R_i + 256^2)/(2^{23} + 256^2) \tag{57}$$

$$x(2) = (\sum_{i=1}^{M\times N} G_i + 256^2)/(2^{23} + 256^2) \tag{58}$$

$$x(3) = (\sum_{i=1}^{M\times N} B_i + 256^2)/(2^{23} + 256^2) \tag{59}$$

$$x(4) = \mathrm{mod}((x(3)^{*}10^8), 1) \tag{60}$$

From the above formula, different plaintexts will produce different initial values of the new chaotic systems, and different initial values of the chaotic systems will produce different fusion pseudo-random sequences for image encryption, which do not leak plaintext information regardless of whether using the ciphertext or the encryption algorithm. Therefore, different plaintexts that produce different key matrices can resist the chosen-plaintext attacks in the proposed encryption approach.

2) SECURITY ANALYSIS OF THE ENCRYPTION PROCESS

Key association plaintext can greatly improve the security of the image chaotic encryption mechanism, but it cannot guarantee that the encryption algorithm is safe from all attacks. If we can find some knowledge related to the characteristics of plaintext in ciphertext, we can use the chosen-plaintext attack under limited conditions to make the chosen-plaintext and the plaintext that corresponds to the ciphertext under attack have a certain correspondence. Then, the equivalent key matrix (based on the initial key, i.e., the initial value and control of the chaotic system and the random number matrix obtained by iterating the chaotic system) can be used to decrypt the ciphertext. The flowchart of the proposed encryption and decryption algorithm is shown in Figure 7. If the pixel values of the plaintext image are all zero, according to equations (61), (62) and (63), in the process of the Feistel transformation, the following equation is used:

$$F = \mathrm{mod}(K_i 0, 256) \tag{61}$$

$$R_{i+1}^{j} = L_i^j \oplus F \tag{62}$$

$$L_{i+1}^{j} = \mathrm{mod}(R_i^j + R_{i+1}^j, 256) \tag{63}$$

From the above equation, the plaintext and key matrix will be completely hidden after multiple iterations, which means that the attacker cannot obtain the key matrix information.

To reduce the correlation among three-channel pixels of the colour image, considering the scrambling and diffusion of image pixels after the Feistel transformation, the process of encryption of scrambling and diffusion is shown in (64), (65) and (66), where CR_i, CG_i, and CB_i are image pixel values after the Feistel change, and no plaintext leakage occurs. The attacker cannot obtain some characteristic information related

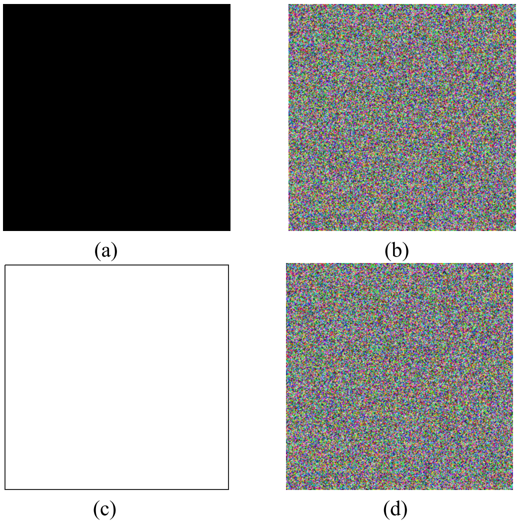


FIGURE 16. The results of special image encryption. (a): The plaintext image of the all-zero case; (b) the ciphertext image of the all-zero case; (c) the plaintext image of the all-255 case; (d) the ciphertext image of the all 255 case.

to the original plaintext from the ciphertext analysis; thus, this encryption process has high security.

$$CR_i = \text{bitxor}((d_i^1 + CR_{i-1} + CG_{i-1}) \bmod 256,\, z_i^1) \quad (64)$$

$$CG_i = \text{bitxor}((d_i^2 + CG_{i-1} + CB_{i-1}) \bmod 256,\, z_i^2) \quad (65)$$

$$CB_i = \text{bitxor}((d_i^3 + CB_{i-1} + CR_{i-1}) \bmod 256,\, z_i^3) \quad (66)$$

A similar analysis process occurs for plaintext images when all values are 255. The all-zero or all-255 cases are considered to obtain ciphertext images through the proposed encryption algorithm, as shown in Figure 16.

Figure 16 shows that the ciphertext image obtained by encrypting a special plaintext image is still a noisy image, and no useful information may be obtained from it; thus, the proposed encryption algorithm is secure.

J. COMPLEXITY ANALYSIS OF ENCRYPTION ALGORITHM

In general, we use time complexity and space complexity to refer to runtime and space requirements; when complexity is used without qualifier, it usually refers to time complexity [55]. The time complexity analysis of an encryption algorithm is an important index of encryption performance, and the computational complexity is used to analyse the computer resources needed to run the algorithm. The experimental environment consists of an Intel Core i-7, 2.3 GHz CPU, 8 GB of memory and a 250-GB hard disk running the Windows 10 Professional operating system. For the Lena plaintext image of size $M \times N$, the execution times of the encryption algorithms from the literature are shown in Table 19. When judging the advantages and disadvantages of an algorithm, the software and hardware factors can be avoided, and only the calculation amount of the algorithm can be considered. For the Lena plaintext image of size $M \times N$, the calculation amount ($\Theta()$) values of encryption algorithms from the literature are shown in Table 23.

TABLE 23. Time complexity.

Encryption algorithm	Execution time(s)	Calculation amount Θ()
Ref. [49]	1.0860	8*MN
Ref. [50]	1.0800	4*MN
Ref. [51]	3.2100	6*MN
Ref. [52]	1.0800	28*MN
Ref. [18]	3.9620	30*MN
Ref. [21]	2.7620	4*MN
Ref. [27]	0.3850	11*MN
Ref. [28]	9.9410	6*MN
Ref. [48]	6.7700	130*MN
Proposed	1.8220	4*MN

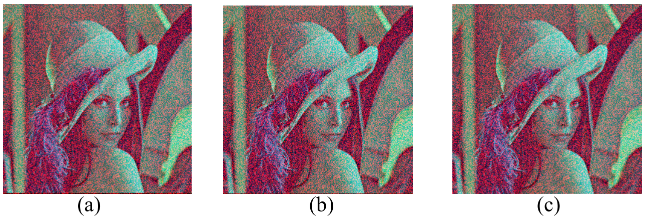


FIGURE 17. Salt and pepper noise attack. (a) 0.1% salt & pepper noise; (b): 0.5% salt & pepper noise; (c): 1% salt & pepper noise.

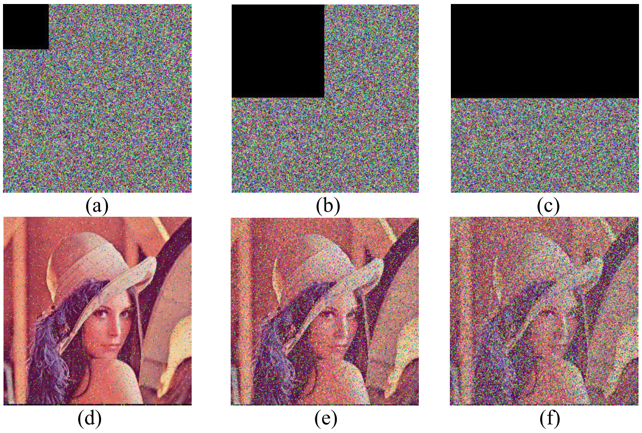


FIGURE 18. Crop attack. (a) full encryption 1/16 block attack; (b): full encryption 1/4 block attack; (c): full encryption 1/2 block attack; (d): decrypted image of (a); (e): decrypted image of (b); (f): decrypted image of (c).

It can be seen from Table 23 that the proposed hyperchaotic system and encryption algorithm has lower complexity than other algorithms in the literature.

K. ROBUSTNESS ANALYSIS

To prevent the image from being destroyed maliciously in the transmission process, the image encryption algorithm should have strong robustness, allowing the ciphertext image to be decrypted correctly following its attack by noise or cropping [56]. We use the ciphertext image obtained by the proposed algorithm for robustness analysis. Figure 17 shows the results of adding salt & pepper noise to the ciphertext image and then decrypting the image with the same decryption algorithm and secret key. Figure 18 shows different cropped parts of the ciphertext image and the resulting decrypted image with the same decryption algorithm and secret key.

Figure 17-18 shows that the proposed algorithm can decrypt the image outline correctly, thereby resisting noise and cropping attack.

VI. CONCLUSION

A new block encryption algorithm for images based on the hyperchaotic system and deep convolutional generative adversarial networks (DCGANs) is proposed in this paper. First, the new four-dimensional hyperchaotic system and DCGANs are combined to generate more complex and better pseudo-random sequences, which are used to iteratively generate the rotation matrix as the key stream. Then, the colour image is divided into two blocks, which are combined with the key stream and the improved Feistel network to generate the matrix. Third, according to the scrambling and diffusion mechanism, the transformation generation matrix obtains the ciphertext image. The experimental results show that the proposed encryption algorithm provides very competitive security performance and can resist common attacks. At the same time, the deep learning mechanism is introduced into the encryption algorithm, which provides new ways and ideas for image information security protection.

In future work, we plan to construct the parallel mechanism of key stream generation and an encryption algorithm to improve the overall efficiency of the encryption system.

ACKNOWLEDGMENT

The author would like to sincerely thank the teachers in the research group.

REFERENCES

[1] G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map," *Pattern Recognit. Lett.*, vol. 31, no. 5, pp. 347–354, Apr. 2010, doi: 10.1016/j.patrec.2009.11.008.

[2] A. Y. Niyat, M. H. Moattar, and M. N. Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Opt. Lasers Eng.*, vol. 90, pp. 225–237, Mar. 2017, doi: 10.1016/j.optlaseng.2016.10.019.

[3] G. Hu, D. Xiao, Y. Wang, and T. Xiang, "An image coding scheme using parallel compressive sensing for simultaneous compression encryption applications," *J. Vis. Commun. Image Represent.*, vol. 44, pp. 116–127, Apr. 2017, doi: 10.1016/j.jvcir.2017.01.022.

[4] G. Singh and S. Supriya, "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security," *Int. J. Comput. Appl.*, vol. 67, no. 19, pp. 33–38, Apr. 2013, doi: 10.5120/11507-7224.

[5] S. P. Raja, "Secured medical image compression using DES encryption technique in bandelet multiscale transform," *Int. J. Wavelets Multiresolution Inf. Process.*, vol. 16, no. 4, Jul. 2018, Art. no. 1850028, doi: 10.1142/S0219691318500285.

[6] G. Chèze, "How to share a cake with a secret agent," *Math. Social Sci.*, vol. 100, pp. 13–15, Jul. 2019, doi: 10.1016/j.mathsocsci.2019.04.001.

[7] Y. D. Xia, J. Wang, B. Meng, and X. Y. Chen, "Further results on fuzzy sampled-data stabilization of chaotic nonlinear systems," *Appl. Math. Comput.*, vol. 379, Aug. 2020, Art. no. 125225, doi: 10.1016/j.amc.2020.125225.

[8] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An image compression and encryption algorithm based on chaotic system and compressive sensing," *Opt. Laser Technol.*, vol. 115, pp. 257–267, Jul. 2019, doi: 10.1016/j.optlastec.2019.01.039.

[9] A. Zarei and S. Tavakoli, "Hopf bifurcation analysis and ultimate bound estimation of a new 4-D quadratic autonomous hyper-chaotic system," *Appl. Math. Comput.*, vol. 291, pp. 323–339, Dec. 2016, doi: 10.1016/j.amc.2016.07.023.

[10] J. Ma, Z. Chen, Z. Wang, and Q. Zhang, "A four-wing hyper-chaotic attractor generated from a 4-D memristive system with a line equilibrium," *Nonlinear Dyn.*, vol. 81, no. 3, pp. 1275–1288, Aug. 2015, doi: 10.1007/s11071-015-2067-4.

[11] C. Zhou, C. Yang, D. Xu, and C.-Y. Chen, "Dynamic analysis and finite-time synchronization of a new hyperchaotic system with coexisting attractors," *IEEE Access*, vol. 7, pp. 52896–52902, 2019, doi: 10.1109/access.2019.2911486.

[12] L. Huang, Z. Zhang, J. Xiang, and S. Wang, "A new 4D chaotic system with two-wing, four-wing, and coexisting attractors and its circuit simulation," *Complexity*, vol. 2019, pp. 1–13, Oct. 2019, doi: 10.1155/2019/5803506.

[13] L. Ding and Q. Ding, "The establishment and dynamic properties of a new 4D hyperchaotic system with its application and statistical tests in gray images," *Entropy*, vol. 22, no. 3, p. 310, Mar. 2020, doi: 10.3390/e22030310.

[14] S. A. Mehdi and Z. L. Ali, "Image encryption algorithm based on a novel six-dimensional Hyper- chaotic system," *Al-Mustansiriyah J. Sci.*, vol. 31, no. 1, p. 54, Mar. 2020, doi: 10.23851/mjs.v31i1.739.

[15] S. Sun, Y. Guo, and R. Wu, "A novel image encryption scheme based on 7D hyperchaotic system and row-column simultaneous swapping," *IEEE Access*, vol. 7, pp. 28539–28547, 2019, doi: 10.1109/access.2019.2901870.

[16] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Comput. Math. Appl.*, vol. 59, no. 10, pp. 3320–3327, May 2010, doi: 10.1016/j.camwa.2010.03.017.

[17] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Opt. Commun.*, vol. 284, nos. 16–17, pp. 3895–3903, Aug. 2011, doi: 10.1016/j.optcom.2011.04.001.

[18] C. Pak, K. An, P. Jang, J. Kim, and S. Kim, "A novel bit-level color image encryption using improved 1D chaotic map," *Multimedia Tools Appl.*, vol. 78, no. 9, pp. 12027–12042, May 2019, doi: 10.1007/s11042-018-6739-1.

[19] X. Wang and N. Guan, "Chaotic image encryption algorithm based on block theory and reversible mixed cellular automata," *Opt. Laser Technol.*, vol. 132, Dec. 2020, Art. no. 106501, doi: 10.1016/j.optlastec.2020.106501.

[20] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," *Appl. Soft. Comput.*, vol. 12, no. 5, pp. 1457–1466, May 2012, doi: 10.1016/j.asoc.2012.01.016.

[21] Z. Liu, C. Wu, J. Wang, and Y. Hu, "A color image encryption using dynamic DNA and 4-D memristive hyper-chaos," *IEEE Access*, vol. 7, pp. 78367–78378, 2019, doi: 10.1109/access.2019.2922376.

[22] 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, doi: 10.1007/s11071-010-9749-8.

[23] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the LSS chaotic map and single S-box," *IEEE Access*, vol. 8, pp. 25664–25678, 2020, doi: 10.1109/ACCESS.2020.2970806.

[24] X. Wang and J. Yang, "A novel image encryption scheme of dynamic S-boxes and random blocks based on spatiotemporal chaotic system," *Optik*, vol. 217, Sep. 2020, Art. no. 164884, doi: 10.1016/j.ijleo.2020.164884.

[25] S. Zhu and C. Zhu, "Secure image encryption algorithm based on hyperchaos and dynamic DNA coding," *Entropy*, vol. 22, no. 7, p. 772, Jul. 2020, doi: 10.3390/e22070772.

[26] L.-P. Chen, H. Yin, L.-G. Yuan, A. M. Lopes, J. A. T. Machado, and R.-C. Wu, "A novel color image encryption algorithm based on a fractional-order discrete chaotic neural network and DNA sequence operations," *Frontiers Inf. Technol. Electron. Eng.*, vol. 21, no. 6, pp. 866–879, Jun. 2020, doi: 10.1631/FITEE.1900709.

[27] H. G. Mohamed, D. H. ElKamchouchi, and K. H. Moussa, "A novel color image encryption algorithm based on hyperchaotic maps and mitochondrial DNA sequences," *Entropy*, vol. 22, no. 2, p. 158, Jan. 2020, doi: 10.3390/e22020158.

[28] A. Y. Niyat and M. H. Moattar, "Color image encryption based on hybrid chaotic system and DNA sequences," *Multimedia Tools Appl.*, vol. 79, no. 1, pp. 1497–1518, Jan. 2020, doi: 10.1007/s11042-019-08247-z.

[29] X. Wang, L. Feng, and H. Zhou, "Fast image encryption algorithm based on parallel computing system," *Inf. Sci.*, vol. 486, pp. 340–358, Jun. 2019, doi: 10.1016/j.ins.2019.02.049.

[30] X. Wang and S. Gao, "Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network," *Inf. Sci.*, vol. 539, pp. 195–214, Oct. 2020, doi: 10.1016/j.ins.2020.06.030.

[31] 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, doi: 10.1016/j.ins.2019.08.041.

[32] J. Y. Liang, Y. Xue, and J. M. Wang, "Bi-objective memetic GP with dispersion-keeping Pareto evaluation for real-world regression," *Inf. Sci.*, vol. 539, pp. 16–35, Oct. 2020, doi: 10.1016/j.ins.2020.05.136.

[33] X. Y. Wang and S. Gao, "Application of matrix semi-tensor product in chaotic image encryption," *J. Franklin Inst.-Eng. Appl. Math.*, vol. 356, no. 18, pp. 11638–11667, Dec. 2019, doi: 10.1016/j.jfranklin.2019.10.006.

[34] Y. Zhang, A. G. Chen, Y. J. Tang, J. W. Dang, and G. P. Wang, "Plaintext-related image encryption algorithm based on perceptron-like network," *Inf. Sci.*, vol. 526, pp. 180–202, Jul. 2020, doi: 10.1016/j.ins.2020.03.054.

[35] L. Bougoffa, A. Saud, and S. Bougoffa, "A complete and partial integrability technique of the Lorenz system," *Results Phys.*, vol. 9, pp. 712–716, Jun. 2018, doi: 10.1016/j.rinp.2018.03.031.

[36] H. Bao, "Dimension, recurrence via entropy and Lyapunov exponents for C-1 map with singularities," *Ergodic Theory Dyn. Syst.*, vol. 38, no. 3, pp. 801–831, May 2018, doi: 10.1017/etds.2016.61.

[37] M. Zabihi, S. Kiranyaz, A. B. Rad, A. K. Katsaggelos, M. M. Gabbouj, and T. Ince, "Analysis of high-dimensional phase space via poincare section for patient-specific seizure detection," *IEEE Trans. Neural Syst. Rehabil. Eng.*, vol. 24, no. 3, pp. 386–398, Mar. 2016, doi: 10.1109/TNSRE.2015.2505238.

[38] L. Gong, R. Wu, and N. Zhou, "A new 4D chaotic system with coexisting hidden chaotic attractors," *Int. J. Bifurcation Chaos*, vol. 30, no. 10, Aug. 2020, Art. no. 2050142, doi: 10.1142/S0218127420501424.

[39] U. Mutlu and E. Alpaydın, "Training bidirectional generative adversarial networks with hints," *Pattern Recognit.*, vol. 103, Jul. 2020, Art. no. 107320, doi: 10.1016/j.patcog.2020.107320.

[40] M. Cheng, F. Fang, C. C. Pain, and I. M. Navon, "Data-driven modelling of nonlinear spatio-temporal fluid flows using a deep convolutional generative adversarial network," *Comput. Methods Appl. Mech. Eng.*, vol. 365, Jun. 2020, Art. no. 113000, doi: 10.1016/j.cma.2020.113000.

[41] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," *Commun. ACM*, vol. 60, no. 6, pp. 84–90, May 2017, doi: 10.1145/3065386.

[42] M. Dzwonkowski, M. Papaj, and R. Rykaczewski, "A new quaternion-based encryption method for DICOM images," *IEEE Trans. Image Process.*, vol. 24, no. 11, pp. 4614–4622, Nov. 2015, doi: 10.1109/TIP.2015.2467317.

[43] C. Zhu and K. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps," *IEEE Access*, vol. 6, pp. 18759–18770, 2018, doi: 10.1109/ACCESS.2018.2817600.

[44] S. Xiao, Z. Yu, and Y. Deng, "Design and analysis of a novel chaos-based image encryption algorithm via switch control mechanism," *Secur. Commun. Netw.*, vol. 2020, pp. 1–12, Mar. 2020, doi: 10.1155/2020/7913061.

[45] X. Wang and L. Liu, "Image encryption based on hash table scrambling and DNA substitution," *IEEE Access*, vol. 8, pp. 68533–68547, 2020, doi: 10.1109/ACCESS.2020.2986831.

[46] A. K. Farhan, N. M. G. Al-Saidi, A. T. Maolood, F. Nazarimehr, and I. Hussain, "Entropy analysis and image encryption application based on a new chaotic system crossing a cylinder," *Entropy*, vol. 21, no. 10, p. 958, Sep. 2019, doi: 10.3390/e21100958.

[47] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, "Novel medical image encryption scheme based on chaos and DNA encoding," *IEEE Access*, vol. 7, pp. 36667–36681, 2019, doi: 10.1109/ACCESS.2019.2906292.

[48] S. Q. Zhu and C. X. Zhu, "Plaintext-related image encryption algorithm based on block structure and five-dimensional chaotic map," *IEEE Access*, vol. 7, pp. 147106–147118, 2019, doi: 10.1109/ACCESS.2019.2946208.

[49] H. Xiang and L. Liu, "An improved digital logistic map and its application in image encryption," *Multimedia Tools Appl.*, vol. 79, nos. 41–42, pp. 30329–30355, Nov. 2020, doi: 10.1007/s11042-020-09595-x.

[50] C. Cheng, K. Sun, and Q. Xu, "A color image encryption algorithm based on 2D-CIMM chaotic map," *China Commun.*, vol. 17, no. 5, pp. 12–20, May 2020, doi: 10.23919/JCC.2020.05.002.

[51] X. Wang, Y. Su, C. Luo, and C. Wang, "A novel image encryption algorithm based on fractional order 5D cellular neural network and Fisher-yates scrambling," *PLoS ONE*, vol. 15, no. 7, Jul. 2020, Art. no. e0236015, doi: 10.1371/journal.pone.0236015.

[52] Y. J. Niu, X. M. Sun, C. Zhang, and H. J. Liu, "Anticontrol of a fractional-or der chaotic system and its application in color image encryption," *Math. Problems Eng.*, vol. 2020, Mar. 2020, Art. no. 6795964, doi: 10.1155/2020/6795964.

[53] M. Jiang, L. Shen, L. Zheng, M. Zhao, and X. H. Jiang, "Tone-mapped image quality assessment for electronics displays by combining luminance partition and colorfulness index," *IEEE Trans. Consum. Eletron.*, vol. 66, no. 2, pp. 153–162, May 2020, doi: 10.1109/TCE.2020.2985742.

[54] W.-S. Yap, C.-W. Phan, W.-C. Yau, and S.-H. Heng, "Cryptanalysis of a new image alternate encryption algorithm based on chaotic map," *Nonlinear Dyn.*, vol. 80, no. 3, pp. 1483–1491, May 2015, doi: 10.1007/s11071-015-1956-x.

[55] B. Zhang, B. Rahmatullah, S. L. Wang, A. A. Zaidan, B. B. Zaidan, and P. Liu, "A review of research on medical image confidentiality related technology coherent taxonomy, motivations open challenges and recommendations," *Multimed Tools Appl.*, pp. 1–40, Aug. 2020, doi: 10.1007/s11042-020-09629-4.

[56] 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, doi: 10.1016/j.sigpro.2020.107629.

PENGFEI FANG received the B.S. degree in communication engineering from the School of Communication Engineering, Xi'an University of Posts and Telecommunications, China, in 2010, and the M.S. degree in electronics and communication engineering from the School of Electronic Engineering, Xi'an University of Posts and Telecommunications, in 2014. He is currently pursuing the Ph.D. degree in pattern recognition and intelligent system with the School of Automation and Information Engineering, Xi'an University of Technology, China. His current research interests include image processing, deep learning, and information security.

HAN LIU (Member, IEEE) received the Ph.D. degree in control science and engineering from the School of Automation and Information Engineering, Xi'an University of Technology, China, in 2003. He is currently a Professor with the School of Automation and Information Engineering, Xi'an University of Technology. His current research interests include industrial artificial intelligence, machine learning, pattern recognition, intelligent information processing, and nonlinear system control.

CHENGMAO WU received the B.S. degree in computer applications from the School of Computer Science, Xi'an Technological University, China, in 1992. He is currently a Senior Engineer with the School of Electronic Engineering, Xi'an University of Posts and Telecommunications, China. His research interests include digital image processing, circuit systems, and fuzzy intelligent information process systems.