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

PENGFEI FANG, HAN LIU, (Member, IEEE), AND CHENGMAO WU

1School of Automation and Information Engineering, Xi’an University of Technology, Xi’an 710048, China
2School 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]...
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 image 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 hyperchaotic 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 Lorenz 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):

\[
\begin{align*}
\dot{x} &= a(x - y), \\
\dot{y} &= cx - xz - y, \\
\dot{z} &= xy - bz,
\end{align*}
\]

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, defined as in (2):

\[
\begin{align*}
\dot{x} &= ax - y^2, \\
\dot{y} &= b(z - y) - (x + w), \\
\dot{z} &= xy + (c - b)y + cz, \\
\dot{w} &= xy + z + w,
\end{align*}
\]

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 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 $$(x, y, z, w) \rightarrow (-x, -y, z, -w)$$ 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
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):

\[
\begin{align*}
ax - y^2 &= 0, \\
b(z - y) - (x + w) &= 0, \\
xy + (c - b)y + cz &= 0, \\
xy + z + w &= 0.
\end{align*}
\]

(4)

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

\[
\begin{bmatrix}
a & -2y & 0 & 0 \\
-1 & -b & b & -1 \\
y & x & -16 & c \\
y & x & 1 & 1
\end{bmatrix}
\]

(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 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.

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.
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.

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

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

where $\phi^n(r)$, $\phi^{n+1}(r)$ 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:

$$ K_c = \frac{\text{cov}(i, D_c(i))}{\text{var}(i)\text{var}(D_c(i))} $$

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.
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. 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.

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 \( \{x_1, x_2, x_3, x_4\} \) and \( \{y_1, y_2, y_3, y_4\} \) are mixed via the fusion sequence generator (FSG) according to equation (9-12) to generate the four-dimensional pseudo-random sequence \( \{z_{i1}, z_{i2}, z_{i3}, z_{i4}\} \) with \( i = 1, 2, 3, 4 \) and \( j = 1, 2, 3, 4 \).

\[
\begin{align*}
    z_{i1} &= \left\lfloor \left( y_{i1} + y_{i2} \right) \times 10^8 \mod 256 \right\rfloor, \\
    z_{i2} &= \left\lfloor \left( y_{i2} + y_{i3} \right) \times 10^8 \mod 256 \right\rfloor, \\
    z_{i3} &= \left\lfloor \left( y_{i3} + y_{i4} \right) \times 10^8 \mod 256 \right\rfloor, \\
    z_{i4} &= \left\lfloor \left( y_{i1} + y_{i2} + y_{i3} + y_{i4} \right) \times 10^8 \mod 256 \right\rfloor.
\end{align*}
\]

where mod is the modulo operation. According to Section II regarding the approximate entropy and Z1 test, the results of the sequence \( \{z_{i1}\} \) 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

---

Some tables are shown in the document, but the text is not clear enough to transcribe them accurately. The code listings are also not transcribed.
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:

$$x(1) = \left( \sum_{i=1}^{M \times N} R_i / 2^{32} \right)^{2^3 + 256^2} \quad (13)$$

$$x(2) = \left( \sum_{i=1}^{M \times N} G_i / 2^{32} \right)^{2^3 + 256^2} \quad (14)$$

$$x(3) = \left( \sum_{i=1}^{M \times N} B_i / 2^{32} \right)^{2^3 + 256^2} \quad (15)$$

$$x(4) = \text{mod}(\left( x(3) \times 10^8 \right), 1) \quad (16)$$

**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 $\{z_i\}, \{z_{i'}\}, \{z_{i''}\}$ and $\{z_{i'''}\}, i = 1, 2, \ldots, M \times N$ 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:

$$q = w + xi + yj + zk \quad (17)$$

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 $\{z_i\}, \{z_{i'}\}, \{z_{i''}\}$ and $\{z_{i'''}\}$, 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:

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

$$R_i^{j+1} = L_i^j \oplus F \quad (22)$$

$$L_i^{j+1} = \text{mod}(R_i^j + R_i^{j+1}, 256) \quad (23)$$

The single-round decryption process is as follows:

$$R_i^j = \text{mod}(L_i^{j+1} - R_i^{j+1}, 256) \quad (24)$$

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

$$L_i^j = R_i^{j+1} \oplus F \quad (26)$$

where mod(·) 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 $i = 1, 2, \ldots, M \times (3 \times N)$.
is as follows:

$$\text{sum} = \left( \sum_{i=1}^{M \times N} d_1^i + \sum_{i=1}^{M \times N} d_2^i + \sum_{i=1}^{M \times N} d_3^i \right)$$  \hspace{1cm} (28)$$

$$\beta = \text{sum} - (d_1^1 + d_2^1 + d_3^1)$$  \hspace{1cm} (29)$$

$$CR_i = \text{bitxor}((d_1^1 + CR_{i-1} + CG_{i-1}) \mod 256, z_1^1)$$  \hspace{1cm} (30)$$

$$CG_i = \text{bitxor}((d_2^1 + CG_{i-1} + CB_{i-1}) \mod 256, z_2^1)$$  \hspace{1cm} (31)$$

$$CB_i = \text{bitxor}((d_3^1 + CB_{i-1} + CR_{i-1}) \mod 256, z_3^1)$$  \hspace{1cm} (32)$$

where \( \text{mod}(\cdot) \) is the modular operation, \text{bitxor}(\cdot)\) is the xor operation, and \( CR_i, CG_i \) and \( CB_i \) are the final ciphertext sequences.

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

$$C = CR_i || CG_i || CB_i \quad i = 1, 2, \ldots, M \times N$$  \hspace{1cm} (33)

\section{B. DECRYPTION PROCESS}

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

\textbf{Step 1:} According to Section III, generate the fusion sequence \( \{z_i'\} \), key stream block \( K_i \).

\textbf{Step 2:} Perform pixel inverse diffusion on the ciphertext image \( C \) by using the fusion sequence \( \{z_i'\} \), according to formulas (35), (36), (37), to obtain matrices \( d_1^i, d_2^i \) and \( d_3^i \).

\begin{align*}
    d_1^i &= \text{bitxor}(CR_i, z_1'^1 - CR_{i-1} - CG_{i-1}) \mod 256 \quad (37) \\
    d_2^i &= \text{bitxor}(CG_i, z_2'^1 - CG_{i-1} - CB_{i-1}) \mod 256 \quad (38) \\
    d_3^i &= \text{bitxor}(CB_i, z_3'^1 - CB_{i-1} - CR_{i-1}) \mod 256 \quad (39)
\end{align*}

\textbf{Step 3:} Convert \( d_1^i, d_2^i \) and \( d_3^i \) into the matrix \( W' \) with a size of \( M \times (3 \times N) \) and conduct the pixel inverse overall scrambling to obtain.

\begin{align*}
    T(q) &= \begin{bmatrix}
        w^2 + x^2 + y^2 - z^2 & 2xy - 2wz & 2x^2 + 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}  \
    & \quad \text{for } i = 1, 2, 3, 4 \\
    K_i &= \begin{bmatrix}
        (z_1'^1)^2 + (z_2'^1)^2 - (z_3'^1)^2 & 2(z_1'^1)(z_2'^1) - 2(z_1'^1)(z_3'^1) & 2(z_1'^1)(z_2'^1) + 2(z_2'^1)(z_3'^1) \\
        2(z_1'^1)(z_2'^1) + 2(z_1'^1)(z_3'^1) & (z_1'^1)^2 - (z_2'^1)^2 + (z_3'^1)^2 & 2(z_1'^1)(z_3'^1) - 2(z_3'^1)(z_3'^1) \\
        2(z_1'^1)(z_3'^1) - 2(z_2'^1)(z_3'^1) & 2(z_2'^1)(z_3'^1) + 2(z_2'^1)(z_3'^1) & (z_2'^1)^2 - (z_3'^1)^2 - (z_2'^1)^2 + (z_3'^1)^2
    \end{bmatrix} \quad (19) \\
    K_i &= [K_i \mod 257] \quad i = 1, 2, \ldots, M \times (N/2)  \
\end{align*}
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 $M \times (N/2)$
$R_{i-1} = \text{mod}(L_i - R_i, 256)$
$L_{i-1} = R_i \oplus (\text{mod}(KR_{i-1}, 256))$
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 $(256 \times 256)$ were selected as plaintext images for encryption. The control parameters ($a, b,$ and $c$) of hyper-chaotic 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 $(256 \times 256)$. 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.
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:

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

(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 $X^2_{255,0.01} = 310.457$, respectively.
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:
\[
M_D = \frac{D_0 + D_{n-1}}{2} + \sum_{i=1}^{m-2} D_g \tag{42}
\]
\[
I_D = \sum_{i=0}^{N-1} |H_{Dg} - A_h| \tag{43}
\]
\[
H_{Dg} = |H_g - A_h| \tag{44}
\]
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 | \( I_o \) |
|-----------------|---------|----------|
| CT              | Red     | 38023    |
|                 | 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    |

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):

\[
\rho_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)D(y)}} \tag{45}
\]

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

\[
\text{cov}(x, y) = \frac{1}{N} \sum_{j=1}^{N} (x_j - \frac{1}{N} \sum_{i=1}^{N} x_i)(y_j - \frac{1}{N} \sum_{i=1}^{N} y_i) \tag{47}
\]

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 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 | 0.0353 |
|                 | Green   | 0.1196 | 0.6695 | 0.0717 |
|                 | Blue    | 0.0253 | 0.6889 | 0.0293 |
| Ref. [51] (Lena)| Red     | -0.1054 | 0.0008 | -0.157 |
|                 | 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 | 0.0020 |
|                 | 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 |

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:

\[
H = \frac{1}{N} \sum_{j=1}^{N} H(B_j)
\]

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 \(32 \times 32\) are tested. At this time, the corresponding theoretical value of local entropy is 7.8087. Table 12 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] 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 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:

\[
\text{Contrast} = \sum_{i} \sum_{j} P(i,j)^2
\]

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:

\[
\text{Correlation} = \frac{\sum_{i} \sum_{j} (ij)P(i,j) - \mu_x \mu_y}{\sigma_x \sigma_y}
\]

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:

\[
\text{Energy} = \sum_{i} \sum_{j} P(i,j) \log P(i,j)
\]

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:

\[ \text{Homogeneity} = \frac{\sum M \sum N P(i, j)/(1 + |(i - j)|)}{\sum N} \]  \hspace{1cm} (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  | 0.6551   | 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 |

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.

\[
H(i,j) = \begin{cases} 
0 & \text{if } C_1(i,j) = C_2(i,j) \\
1 & \text{if } C_1(i,j) \neq C_2(i,j)
\end{cases}
\]  

\[
NPCR = \frac{\sum_{i,j} H(i,j)}{MN} \times 100\% 
\]  

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

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 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.
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.

\[
x(1) = \frac{\sum_{i=1}^{M\times N} R_i + 256^2}{2^{23} + 256^2} \quad (57)
\]

\[
x(2) = \frac{\sum_{i=1}^{M\times N} G_i + 256^2}{2^{23} + 256^2} \quad (58)
\]

\[
x(3) = \frac{\sum_{i=1}^{M\times N} B_i + 256^2}{2^{23} + 256^2} \quad (59)
\]

\[
x(4) = \text{mod}(x(3)^*10^8, 1) \quad (60)
\]

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:

\[
F = \text{mod}(K_0, 256) \quad (61)
\]

\[
R_{i+1}^j = L_i^j \oplus F \quad (62)
\]

\[
L_{i+1}^j = \text{mod}(R_i^j + R_{i+1}^j, 256) \quad (63)
\]

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 \(C_R, C_G, \) and \(C_B\) are image pixel values after the Feistel change, and no plaintext leakage occurs. The attacker cannot obtain some characteristic information related to the key matrix.
to the original plaintext from the ciphertext analysis; thus, this encryption process has high security.

\[ CR_i = \text{bitxor}(d_i^1 + CR_{i-1} + CG_{i-1}) \mod 256, z_i^1) \] (64)

\[ CG_i = \text{bitxor}(d_i^2 + CG_{i-1} + CB_{i-1}) \mod 256, z_i^2) \] (65)

\[ CB_i = \text{bitxor}(d_i^3 + CB_{i-1} + CR_{i-1}) \mod 256, z_i^3) \] (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.

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

| Encryption algorithm | Execution time(s) | Calculation amount (\( \Theta() \)) |
|----------------------|-------------------|-----------------------------------|
| 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).
The author would like to sincerely thank the teachers in the field of key stream generation and an encryption algorithm to propose a new encryption algorithm, which provides new ways and ideas at the same time, the deep learning mechanism is introduced into the proposed encryption algorithm provides very competitive 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, AES 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. Chéze, “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.2019.29141886.
[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-Mustansiryah 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.2010.07.023.
[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/s11422-018-7639-1.
[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 hyperchaos,” 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. ElKhamchouchi, and K. H. Moussa, “A novel color image encryption algorithm based on hyperchaotic DNA sequences,” Multimedia Tools Appl., vol. 79, no. 1, pp. 1497–1518, Jan. 2020, doi: 10.1007/s11284-019-08247-z.
[28] 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.
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.

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.

J. Y. Liang, X. Yue, 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.

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.

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.

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.

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.

M. Zabibi, S. Kiranyaz, A. B. Rad, A. K. Katsaggelos, M. M. Gabouj, 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.

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.

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.

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.

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.

M. Dzvonkovski, M. Papaj, and R. Ryzakiewicz, “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.

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.

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, no. 12, Mar. 2020, doi: 10.1155/2020/7913061.

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.

A. K. Farhan, N. M. G. Al-Saied, A. T. Maoolod, 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.

A. Belazi, M. Talha, S. Kharbeck, 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.

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.

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/s1144-020-09595-x.

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.

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 shuffling,” PLoS ONE, vol. 15, no. 7, Jul. 2020, Art. no. e0236015, doi: 10.1371/journal.pone.0236015.

P. Fang et al.: Novel Chaotic Block Image Encryption Algorithm Based on Deep Convolutional Generative Adversarial Networks

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, China. His current research interests include image processing, computer vision, pattern recognition, intelligent information processing, and nonlinear system control.

CHENMAO WU received the B.S. degree in computer science 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.