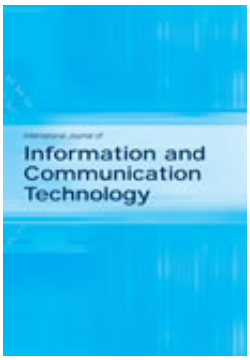
INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research



International Journal of Information and Communication Technology

ISSN online: 1741-8070 - ISSN print: 1466-6642
https://www.inderscience.com/ijict

Chaotic colour image encryption based on differential evolutionary deep learning

Zhengbao Cai

Article History:

Received:	30 August 2024
Last revised:	13 September 2024
Accepted:	13 September 2024
Published online:	10 October 2024

Chaotic colour image encryption based on differential evolutionary deep learning

Zhengbao Cai

College of Information Technology,
Anhui Vocational College of Defense Technology,
Lu'an 237000, China
Email: caizhengbao2024@163.com

Abstract: Traditional chaotic image encryption methods have certain limitations in terms of processing high-dimensional data, computational complexity and attack resistance, which limits their widespread promotion and use in practical applications. To solve these problems, this paper proposes a chaotic colour image encryption method based on differential evolutionary deep learning. Firstly, the security and stability of the image encryption algorithm is enhanced by introducing a six-dimensional cellular neural network (CNN). Secondly, the parameters of the six-dimensional CNN are optimised using differential evolutionary algorithms to improve the complexity and randomness of the chaotic sequences. The experimental results show that compared with the traditional CNN, AES and Chaotic Encryption Algorithm, this paper's method shows significant improvement in NPCR and UACI indicators.

Keywords: chaotic image encryption; differential evolutionary algorithm; six-dimensional cellular neural network; CNN; NPCR; unified average changing intensity; UACI.

Reference to this paper should be made as follows: Cai, Z. (2024) 'Chaotic colour image encryption based on differential evolutionary deep learning', *Int. J. Information and Communication Technology*, Vol. 25, No. 7, pp.57–74.

Biographical notes: Zhengbao Cai is currently an Associate Professor at the Anhui Vocational College of Defense Technology. His research interests include information security and artificial intelligence.

1 Introduction

Image encryption is a key technique for securing image data, especially in the process of information transmission and storage with important applications (Kaur and Kumar, 2020). With the wide application of digital images in the internet, cloud computing and internet of things, the demand for image encryption is increasing. With effective image encryption, unauthorised access to sensitive information can be prevented and personal privacy and trade secrets can be protected (Pareek et al., 2006; Gao et al., 2006). In addition, image encryption has a wide range of application prospects in fields such as medical images (Kumari et al., 2017; Guan et al., 2005), satellite images and military

images. In general, the research of image encryption technology not only improves data security, but also plays an important role in promoting the development of digital information technology.

Chaotic image encryption exploits the nonlinearity and initial condition sensitivity of chaotic systems to provide a highly secure solution for image encryption (Liu et al., 2014). Traditional chaotic image encryption methods have achieved some success, but there are still many challenges to overcome. Salleh et al. (2003) proposed an image encryption method based on chaotic mapping, which utilises Logistic mapping to generate encrypted sequences and achieves effective encryption of images. However, this method has high computational complexity when dealing with high resolution images. Liu (2008) proposed an image encryption algorithm based on the Lorenz chaotic system, and it was found that the algorithm was excellent in resisting statistical analysis attacks, but it was sensitive to the selection of initial conditions. Ye (2010) developed an image encryption method based on the chaotic sequences and disambiguation techniques, although the method achieved good results in improving the security of images. Method achieved significant results in improving image security, but it requires precise initial conditions in the decryption process and has high operational complexity.

In recent years, chaotic image encryption technology has been rapidly developed, and researchers have proposed a variety of improved and innovative methods. Lang (2015) proposed an image encryption method based on chaos and fractional-order Fourier transform, which improves the attack-resistant ability of encrypted images by introducing the fractional-order Fourier transform, but has higher requirements on computational resources in the implementation process. Zhang (2018) proposed an image encryption algorithm based on chaos and DNA coding, which was shown to significantly improve the security and complexity of image encryption, but there are some difficulties in hardware implementation. Tong et al. (2015) used high-dimensional chaotic systems for image encryption, and generated key streams through multi-dimensional chaotic mapping, which enhanced the security of encryption algorithms and the resistance to attacks, but further optimisation is needed in the selection of high-dimensional system parameters. Chen et al. (2018) proposed an image encryption method based on chaos and compressed sensing, which combines chaotic system and compressed sensing technology to improve the efficiency of the encryption algorithm, but the compressed sensing reconstruction accuracy needs to be solved in practical applications. Sang et al. (2022) developed an image encryption method that combines chaotic and deep learning combined image encryption method, which generates chaotic sequences through deep learning models and achieves efficient image encryption, but the limitations of data and computational resources need to be considered in the process of model training and deployment. Chen et al. (2023) proposed a graph convolutional self-encoder encryption algorithm.

Existing chaotic image encryption methods have achieved some success in improving the security of image encryption, but there are still some challenges in dealing with high-dimensional data, computational complexity and attack resistance. Traditional chaotic image encryption methods tend to have high computational complexity when dealing with high-resolution and multi-dimensional images, which makes it difficult to meet the real-time demand in practical applications. In addition, the anti-attack capability of the existing methods needs to be further improved when facing complex attack techniques (e.g., differential attack, statistical analysis attack). The parameter selection

and initial condition sensitivity in the chaotic sequence generation process also make the decryption process complex and unstable.

In order to solve the above problems, this paper proposes a chaotic colour image encryption method based on differential evolutionary deep learning, which aims to improve the security, computational efficiency and attack resistance of image encryption. The main innovations and contributions of this work include:

1 Aiming at the deficiencies of existing chaotic image encryption methods in terms of computational complexity and attack resistance, this paper proposes an image encryption method based on six-dimensional cellular neural network (CNN). The six-dimensional CNN is capable of generating more complex and unpredictable chaotic sequences, which enhances the security of the encryption algorithm and exhibits higher efficiency and stability in processing high-dimensional image data.

2 In this paper, the parameters of the six-dimensional CNN are optimised by differential evolution (DE) algorithm, which improves the complexity and randomness of the chaotic sequences. The DE algorithm effectively solves the problems of parameter selection and sensitivity of initial conditions in the traditional methods, which makes the generated chaotic sequences more resistant to attacks and more stable, and significantly improves the overall performance of image encryption. The experimental results show that the optimised method has significant improvement in both security and can effectively resist complex attack means.

The main difference between the DE-6DCNN method proposed in this paper and other deep learning encryption technologies is that it can generate more complex chaotic sequences and optimise the parameter selection through DE algorithm, thus significantly improving the security and efficiency of encryption. This method can effectively process high-dimensional data while maintaining high security.

2 Relevant technologies

2.1 Basic concepts of chaos

The core idea of chaotic systems is that even a small difference in the initial value can lead to a huge difference in the long-term evolution of the system, a property known as the 'butterfly effect' (Zhou et al., 2014). In image encryption, this extreme sensitivity to initial values can be effectively exploited to construct encryption algorithms with a high degree of security. This is because any small change to the encrypted image will lead to a huge deviation in the decryption process, thus making the original image unrecoverable and ensuring the security of the information.

The unpredictable long-term behaviour of chaotic systems is also an important reason why they are widely used in the field of image encryption. Traditional encryption algorithms often rely on fixed mathematical transformations and keys, which makes them a security risk in the face of strong computational power and advanced cracking techniques. Chaotic systems, on the other hand, due to their intrinsic complexity and uncertainty, make the encrypted sequences generated by them highly random and unpredictable, thus greatly improving the security of encrypted images.

Chaos describes the seemingly random and unpredictable behaviour exhibited by dynamic systems under deterministic nonlinear conditions (Gao et al., 2022). Key characteristics of chaotic systems include sensitive dependence on initial conditions, topological mixing, and fractal nature. The most notable property of chaotic systems is their high sensitivity to initial conditions, where even small changes can lead to significant differences in long-term behaviour (Lin et al., 2020). This property is usually quantified by the Lyapunov exponent, which indicates the sensitivity of the system state to changes in the initial conditions. For systems with a positive Lyapunov exponent, neighbouring orbits are separated exponentially with the expression:

$$\lambda = \lim_{t\to\infty} \frac{1}{t} \ln \frac{|\delta Z(t)|}{|\delta Z(0)|} \tag{1}$$

where λ is the Lyapunov exponent and $\delta Z(t)$ is the amount of change in the state at time t.

Topological hybridity describes the fact that a trajectory in any one region of a chaotic system is eventually able to enter any other region of the system. This property means that the state space of the system is fully explored, regardless of the initial state. The description of topological mixability is shown below:

$$\forall U, V \subset X, \exists N : \forall n \geq N, f^n(U) \cap V \neq \varnothing \tag{2}$$

where U and V are open sets in the state space X of the system; f^n is the state of the system after n iterations.

Many chaotic systems exhibit fractal attractors, which have non-integer dimensions called fractal or Hausdorff dimensions. The dimension of a fractal attractor can be approximated by the following relation:

$$D = \lim_{\partial\to 0} \frac{\log N(\partial)}{\log(1/\partial)} \tag{3}$$

where D is the Hausdorff dimension, ϵ is the size of the scale, and $N(\epsilon)$ is the minimum number of ϵ- spheres required to cover the attractor of the system.

The application of chaos theory in encryption algorithms is mainly based on its unpredictability and complex system behaviour, which makes the encryption methods based on chaotic systems have a natural advantage in security. By combining image encryption with chaos theory, the ability of encryption algorithms to resist external attacks can be greatly enhanced to ensure the security of transmitted information.

2.2 Cellular neural network

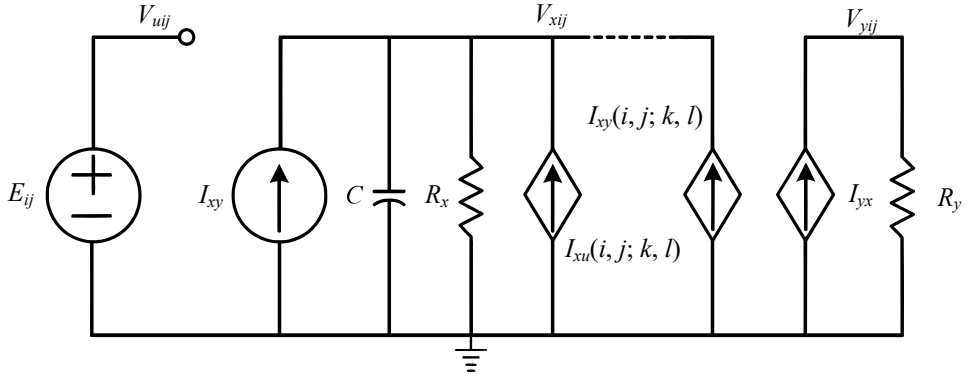
A CNN is a parallel computing architecture consisting of a number of simple processing units called cells, which transfer and process information through local interconnections (Chua and Yang, 1988). Each cell has inputs, outputs, and states, and changes in its state are described by nonlinear dynamic equations. CNNs are characterised by high-speed parallel processing, easy hardware implementation, and good fault tolerance, and therefore have been widely used in image processing, pattern recognition, etc. CNNs, with their unique structure and computational capabilities, have shown excellent. The design of CNN is inspired by the local connectivity and collective dynamics of biological neural systems, and its basic building blocks simulate the functions of biological neurons.

In the field of chaotic image encryption, the hyper chaotic nature of CNNs is used to generate key streams with a high degree of randomness and complexity. Fourth or higher order CNNs is capable of generating hyper chaotic behaviour which provides higher security during encryption. Using the hyper chaotic sequences generated by CNNs, the image can be disrupted and diffused at pixel level to achieve encryption.

CNN-based image encryption algorithms usually include two main steps: disruption and diffusion. In the disarrangement phase, the algorithm uses the parameters generated by the chaotic mapping to randomly rearrange the positions of the image pixels, breaking the pixel arrangement of the original image. In the diffusion phase, the algorithm uses the super chaotic sequence generated by the CNN to perform point-by-point dissimilarity or mode-addition operations on the pixel values of the disordered image, which further increases the degree of chaos and randomness of the image.

Cells are the basic units of CNNs, and each cell can contain a first-order circuit consisting of a linear capacitor, a nonlinear voltage-controlled current source, and some linear circuit elements (Aizenberg et al., 2001). The cellular elements also include linear resistors, where R_x and R_y are linear resistors, I_{xy} and I_{yx} are voltage-controlled current sources, E_{ij} is a linear power supply, C is a linear capacitor, $I_{xu}(i, j; k, l)$ and $I_{xy}(i, j; k, l)$ are linear circuit-connected current sources. The internal cellular units of each CNN have the same circuit basis and element structure. The cellular unit equivalent circuit is shown in Figure 1.

Figure 1 Cell unit circuit diagram

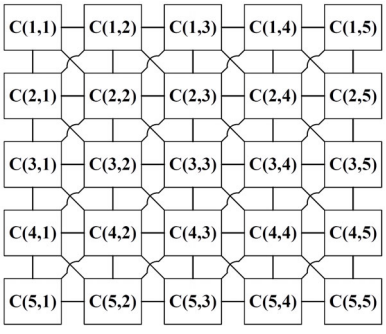


A CNN of size $M \times N$ is composed of M rows N columns totalling $M \times N$ cells. A CNN of size 5×5 is given in Figure 2. The $C(2, 2)$ is denoted as the cell in the 2nd row and 2nd column in the CNN. The neighbourhood $N_r(i, j)$ is defined as the set of all cells within r distance around cell (i, j).

$$N_r(i, j) = \left\{(k, l) \middle| \max\left(|k-i|, |l-j|\right) \le r, 1 \le k \le M, 1 \le l \le N\right\} 0 \tag{4}$$

This definition critically supports local interactions between cells that affect the overall behaviour and function of the network. For example, when $r = 1$, the neighbourhood includes all directly adjacent cells; when $r = 2$, the neighbourhood extends to all cells within two steps.

Figure 2 Structure of CNN at 5 × 5 scale



Based on the above circuit diagram of the cellular unit, the following dynamic behaviour of the cellular unit can be obtained by applying KCL and KVL as follows (Arena et al., 2000):

The representation of the state equation is shown below:

$$C\frac{dv_{ij}(t)}{dt} = -\frac{1}{R_x}v_{ij}(t) + \sum_{C(k,l)\in N_r(i,j)} A(i,\ j;\ k,\ l)v_{kl}(t) + \sum_{C(k,l)\in N_r(i,j)} B(i,\ j;\ k,\ l)u_{kl}(t) + I \tag{5}$$

where C denotes the capacitance of the cell, which determines the charge storage capacity; $v_{ij}(t)$ denotes the voltage of the cell (i, j) at time t; R_x denotes the resistance of the cell, which affects the flow of the current; $A(i, j; k, l)$ denotes the forward coupling coefficient from the cell (k, l) to the cell (i, j), which affects how the voltage of the neighbouring cell affects the current cell; $B(i, j; k, l)$ denotes the reverse coupling coefficient from cell (k, l) to cell (i, j) that affects how inputs from neighbouring cells affect the current cell; $u_{kl}(t)$ denotes the external inputs to cell (k, l) at time t; and I denotes the externally-applied currents, or bias, that regulate the active state of the entire network.

The output equation defines a threshold activation function as follows:

$$v_{ij}(t) = \frac{1}{2}\left(\left|v_{ij}(t)+1\right| - \left|v_{ij}(t)-1\right|\right), 1 \le i \le M; 1 \le j \le N \tag{6}$$

where $v_{ij}(t)$ denotes the voltage output of cell (i, j) at time t, and a threshold function is used here to simplify the conversion of the voltage state to a binary output.

The representation of the kinetic equations is shown below:

$$\begin{cases} \dfrac{dx_i}{dt} = -x_i + a_i f(x_i) + \sum_{k=1}^{n} A_{kf}(x_k) + \sum_{k=1}^{n} S_k x_k + I_i \\ f(x_i) = \dfrac{1}{2}\left(\left|x_i+1\right| - \left|x_i-1\right|\right) (i = 1, 2, ..., n) \end{cases} \tag{7}$$

where x_i denotes the internal state of cell i; a_i is used to regulate the strength of cell i's self-activation; $f(x_i)$ denotes the cell i's activation function, which is usually a nonlinear function; A_{kf} denotes the coupling coefficient, which regulates the effect of other cells k

on cell i; S_k denotes the self connection weights, describing how cell i is affected by its own previous state; I_i denotes the external inputs or biases to a given cell i.

These equations describe how each cell dynamically changes according to its state of charge and its interactions with its neighbouring cells, and these changes are the basis for realising the function of the CNN.

3 Six-dimensional CNN hyperchaotic systems

This paper proposes an image chaotic encryption algorithm based on a six-dimensional CNN. Chaotic sequences are generated by the six-dimensional CNN, and the chaotic sequences are processed and used in the encryption algorithm. The designed encryption method algorithm adopts the method of disruption-diffusion-disruption, and the diffusion process processes the image in chunks, respectively, using different diffusion methods. According to the above kinetic equations of CNN, the kinetic model of six-dimensional CNN proposed in this paper can be expressed as a set of six-dimensional nonlinear differential equations.

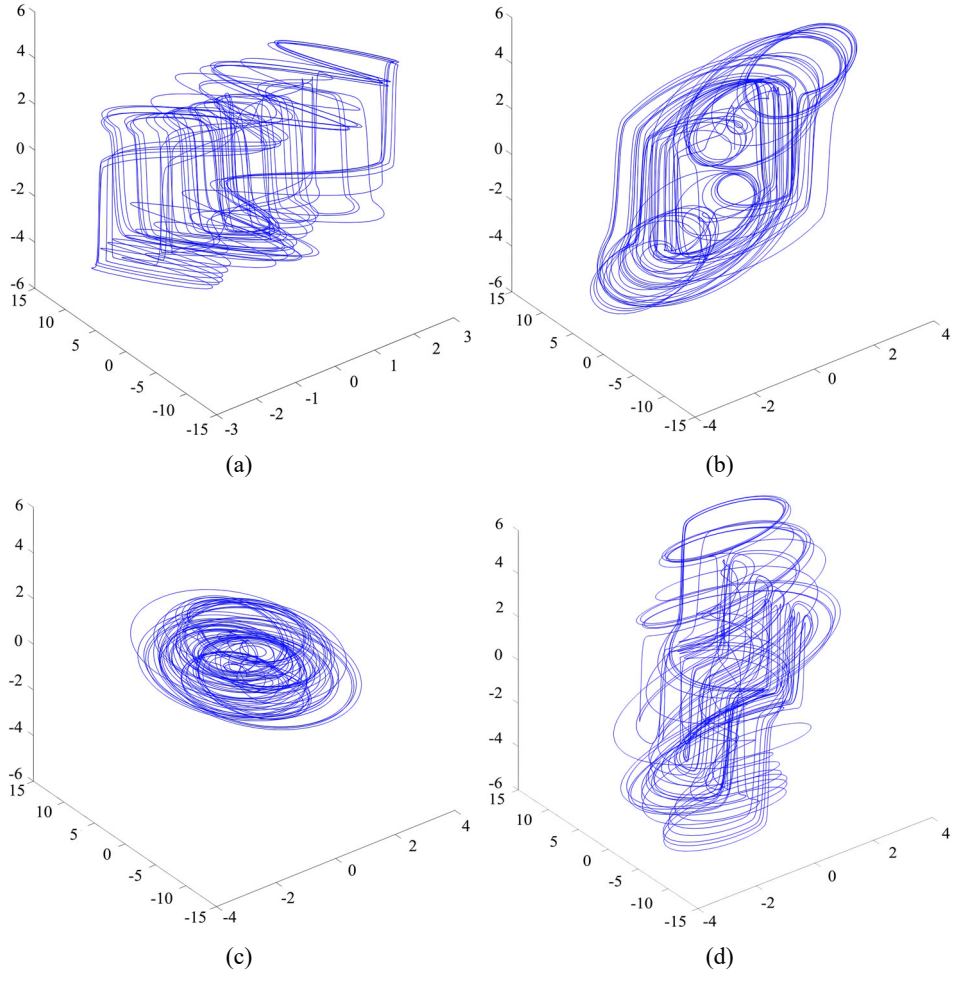
$$\begin{cases} \dot{x}_1 = -x_3 - x_4 \\ \dot{x}_2 = x_2 + x_3 \\ \dot{x}_3 = 4x_1 - 2x_2 \\ \dot{x}_4 = 11x_1 - 12x_4 + 200f(x_4) \\ \dot{x}_5 = 18x_2 + x_1 - x_5 \\ \dot{x}_6 = 4x_5 - 4x_6 + 100x_2 \end{cases} \tag{8}$$

$$f(x_4) = \frac{1}{2}\left(|x_4 + 1| - |x_4 - 1|\right) \tag{9}$$

The six-dimensional CNN consists of six interconnected cells, each of which is affected not only by its own state, but also by the states of the other five cells. This multidimensional interaction greatly increases the dynamic complexity of the system, enabling it to generate highly complex chaotic sequences.

Suppose the initial values are set as: $x_1(0) = 0$, $x_2(0) = 0.2$, $x_3(0) = 0.4$, $x_4(0) = 0.6$, $x_5(0) = 0.8$, $x_6(0) = 1$. The time step is set to $\Delta t = 0.02$. The numerical solution is computed using the Runge-Kutta method, which tracks the time evolution of each variable. Special attention is paid to the fact that x_4 is strongly influenced by the nonlinear function $f(x_4)$. The Benettin algorithm is used to estimate the global Lyapunov exponent of the system. Specifically, it is necessary to calculate the rate of divergence or convergence of the system from the initial state. Tracking the separation velocity of neighbouring trajectories usually requires calculations for multiple nearest-neighbour trajectories. The time evolution of the system is simulated by numerical methods (Runge-Kutta integrals) to see if the trajectories of the system state show behaviour that is sensitively dependent on the initial conditions. The trajectories of the system state after long time evolution are plotted in phase space to find the presence of strange attractors. The presence of strange attractors indicates that the nonlinear differential equation in the six dimensions proposed in this paper is a hyperchaotic system, as shown in Figure 3.

Figure 3 Partial chaotic attractor phase diagram, (a) y-z-w, (b) x-z-w, (c) x-y-z, (d) x-y-w (see online version for colours)



The main features of six-dimensional CNN include: high-dimensional interconnection structure, nonlinear dynamic equation and hyperchaotic behaviour. This structure can generate more complex and unpredictable chaotic sequences, thus enhancing the security of encryption algorithms.

4 Optimisation of six-dimensional CNN structure based on DE

For applications that require high security, such as encryption, chaotic properties are very important. DE algorithms can be used to adjust the network parameters so that the network exhibits stronger chaotic behaviour and improves security. Therefore, in order to improve the performance of six-dimensional CNNs in high-security applications such as image encryption, this study uses the DE algorithm to optimise the network parameters to enhance its chaotic properties. The enhancement of chaotic behaviour can increase the

unpredictability and complexity of the system, thus improving the security of the whole system.

4.1 Optimisation objective function definition

The goal of optimisation is to maximise the chaotic properties of the system, which is usually measured by the Lyapunov exponent. The larger the positive Lyapunov exponent, the more significant the chaotic behaviour of the system. Therefore, we define the fitness function F of the optimisation as the sum of the positive parts of the Lyapunov exponent of the system:

$$F(\theta) = \sum_{i=1}^{n} \max\left(0, \lambda_i(\theta)\right) \tag{10}$$

where θ denotes the parameter vector of the six-dimensional CNN and $\lambda_i(\theta)$ is the i^{th} Lyapunov exponent under the corresponding parameter.

4.2 Coding of differentially evolved individuals

In the DE algorithm, each individual is represented as a possible solution to the network parameters (Opara and Arabas, 2019). In a six-dimensional CNN, an individual can be encoded as a vector containing all the correlation coefficients and function parameters:

$$\theta = \left[c_1, c_2, \ldots, c_k, f_{params}\right] \tag{11}$$

where c_i denotes the coefficients in the network, e.g., 11, –12, 200 as well as other connection weights, and f_{params} denotes the activation function parameters, e.g., the coefficients in the nonlinear function $f(x_4)$.

4.3 Operation of DE

The DE operation consists of three main steps: mutation, crossover and selection. Each step can be specifically defined as follows:

1 Variants:

For each individual θ_i, three different individuals θ_a, θ_b, θ_c are randomly selected from the population and the variation vector is calculated:

$$\theta_{mut} = \theta_a + F \cdot (\theta_b - \theta_c) \tag{12}$$

where F is the difference weight, usually in the range [0.5, 2.0].

2 Cross-cutting:

The trial vector θ_{trial} is generated by a crossover operation:

$$\theta_{trial,j} = \begin{cases} \theta_{mut,j} & \text{if rand}(0,1) \le CR \text{ or } j = j_{rand} \\ \theta_{i,j} & \text{otherwise} \end{cases} \tag{13}$$

where CR is the crossover probability and j_{rand} is a randomly chosen index that ensures that at least one of the dimensions comes from the variation vector.

3 Selection:

Renewing populations through greedy selection:

$$\theta_i = \begin{cases} \theta_{trial} & \text{if } F(\theta_{trial}) > F(\theta_i) \\ \theta_i & \text{otherwise} \end{cases} \tag{14}$$

Through the above steps, the algorithm iterates until a stopping condition is met, such as reaching the maximum number of iterations or adaptation convergence.

After completing the optimisation, numerical simulations are required to assess the effect of the optimised network parameters, especially the change in Lyapunov exponent. By comparing the dynamic behaviour of the system before and after the optimisation, the degree of enhancement of the chaotic properties can be verified. By this method, the DE-based optimisation of the six-dimensional CNN structure can effectively enhance the performance of the network in security applications, making it more effective and reliable in dealing with applications with high security requirements.

5 Design of encryption algorithm for images

5.1 Generation of the chaos key

The key is the initial condition for generating a chaotic sequence. Generally, the key is input into the chaotic system as the initial value and parameters to generate the chaotic sequence. In order to make the ciphertext image more difficult to be deciphered, this paper adopts the key associated with the plaintext, which improves the security of the algorithm to a large extent. The image of size $M \times N$ is divided into six non-overlapping parts as shown in Figure 4, and each part is denoted as $I_i (i = 1, 2, \cdots, 6)$.

$$m_1 = (M - M \bmod 3)/3 \tag{15}$$

$$m_2 = \left\lfloor (M - m_1) + (M - m_1) \bmod 2 \right\rfloor / 2 \tag{16}$$

$$n_1 = (N + N \bmod 2)/2 \tag{17}$$

Calculate the sum of the pixel values in I_i separately, denoted as $SUM_i (i = 1, 2, \cdots, 6)$. Divide Y_i into three parts: SUM_1 and SUM_2, SUM_3 and SUM_4, SUM_5 and SUM_6. Compute the key $t_1 (t_1 \in (-4, 4))$, $t_2 (t_2 \in (-5, 5))$, $t_3 (t_3 \in (-13, 3))$. The values of t_1, t_2 and t_3 are assigned to the state variables y, z and w respectively in the CNN system, i.e., the key t_1, t_2, t_3 is used as the initial value of the CNN system. This method can dynamically generate the key by summing the pixel values of different images, thus dynamically updating the initial value of the system, and realising that the key is associated with the plaintext.

$$t_1 = (SUM_1 \oplus SUM_2) \bmod 5 - 4 \tag{18}$$

$$t_2 = (SUM_3 \oplus SUM_4) \bmod 7 - 5 \tag{19}$$

$$t_3 = (SUM_5 \oplus SUM_6) \bmod 23 - 13 \tag{20}$$

The highly complex chaotic sequence generated by six-dimensional CNN consists of six coupled nonlinear state variables, each of which is influenced by other variables. These sequences exhibit multiple positive Lyapunov index, which ensures the high unpredictability of the sequences. Specifically, the sequence contains chaotic characteristics in space and time, which makes it very suitable for image encryption applications.

5.2 Initial key generation process for the six-dimensional CNN

The specific steps of image encryption include three phases of disarrangement, diffusion and re-disarrangement. The purpose of the encryption process is to ensure the high security and complexity of the image information through multiple disarrangement and diffusion operations, making the encrypted image difficult to be cracked. The disarrangement stage is mainly to disrupt the original structure of the image by changing the position of the image pixels. The initial disruption sequence generation is performed first. Using the chaotic sequences generated by the six-dimensional CNN, two of these sequences are selected to perform the disruption operation. These sequences are generated by iterating the initial key.

5.3 Encryption process

The specific steps of image encryption include three phases of disarrangement, diffusion and re-disarrangement. The purpose of the encryption process is to ensure the high security and complexity of the image information through multiple disarrangement and diffusion operations, making the encrypted image difficult to be cracked. The disarrangement stage is mainly to disrupt the original structure of the image by changing the position of the image pixels. The initial disruption sequence generation is performed first. Using the chaotic sequences generated by the six-dimensional CNN, two of these sequences are selected to perform the disruption operation. These sequences are generated by iterating the initial key.

The new position of each pixel is obtained by calculating the chaotic sequence. Assuming that the chaotic sequence is $\{x_i\}$, the mapping relation can be expressed as.

$$\text{NewPos}(i, j) = (i + x_i) \bmod M, (j + x_j) \bmod N \tag{21}$$

where M and N are the number of rows and columns of the image, respectively.

The initial disarrangement operation is completed by rearranging the pixels in the image matrix according to the generated mapping rules.

The aim of the diffusion phase is to make a change in one pixel affect the grey values of multiple pixels by changing the grey values of the pixels. One of the remaining chaotic sequences is selected for the diffusion process. This sequence is used to adjust the grey value of each pixel. The operation to generate the diffused grey value using the chaotic sequence with the original grey value of the pixel is performed as:

$$I'(i, j) = (I(i, j) + x_k) \bmod 256 \tag{22}$$

where $I(i, j)$ is the original pixel value, x_k is the value of the diffusion sequence, and $I'(i, j)$ is the pixel value after diffusion.

Updating each pixel value in the image matrix causes a significant change in the statistical properties of the image, increasing the security of the encryption.

The re-disordering phase is designed to further disrupt the pixel positions after diffusion, increasing the complexity and randomness of the encryption. A new chaotic sequence is used to generate the mapping rule for the second disruption. Suppose the new chaotic sequence is $\{y_i\}$ and the mapping relation is:

$$\text{NewPos}'(i, j) = \left(i + y_i\right) \bmod M, \left(j + y_j\right) \bmod N \tag{23}$$

According to the new mapping rules, the pixels in the image matrix are rearranged again to complete the secondary disambiguation.

Through these three stages of processing, the pixel positions and grey values of the image are highly obfuscated, ensuring that the encrypted image is difficult to be restored to its original state. Each step relies on the initial key and chaotic sequence, ensuring a high degree of randomness and security in the encryption process. The encryption process includes three main steps: initial scrambling, diffusion and re-scrambling. Each step uses chaotic sequences generated by six-dimensional CNN. Initial scrambling changes the pixel position, diffusion changes the pixel value, and then scrambling further disrupts the pixel position to ensure high encryption security.

5.4 Decryption process

The decryption process is the inverse of the encryption process, and its purpose is to restore the encrypted image to the original plaintext image. In order to ensure the accuracy of decryption, it is necessary to strictly follow the reverse order of the encryption process. The decryption process is also divided into three stages: inverse scrambling, inverse diffusion and inverse scrambling again.

The inverse chaotic phase restores the pixel positions to the pre-encryption state by an inverse chaotic operation. Using the same initial key as the encryption process and the chaotic sequences generated by the six-dimensional CNN, the same two sequences as in the encryption phase are selected. The original position of each pixel is computed based on the chaotic sequences generating a mapping relation opposite to the encryption phase.

$$\text{OrigPos}(i, j) = \left(i - x_i + M\right) \bmod M, \left(j - x_j + N\right) \bmod N \tag{24}$$

According to the above inverse mapping rules, the pixels in the encrypted image matrix are rearranged back to their original positions to complete the initial inverse disarray operation. The purpose of the counter-diffusion stage is to restore the grey values of the pixels to their pre-encryption state by the counter-diffusion operation. The same chaotic sequence as in the encryption stage is used for the counter-diffusion operation. The original grey value is restored using the chaotic sequence with the encrypted pixel grey value by performing an inverse operation.

$$I(i, j) = \left(I'(i, j) - x_k + 256\right) \bmod 256 \tag{25}$$

where $I'(i, j)$ is the encrypted pixel value, x_k is the value of the diffusion sequence, and $I(i, j)$ is the recovered original pixel value. Each pixel value in the image matrix is updated to restore it to its pre-encryption state.

The again inverse chaotic stage further restores the diffused pixel positions to the original positions through an inverse chaotic operation. The same chaotic sequence as in the encryption phase is used to generate the mapping rules for the second inverse disarray.

$$\text{OrigPos}'(i, j) = \left(i - y_i + M\right) \bmod M, \left(j - y_j + N\right) \bmod N \tag{26}$$

According to the new inverse mapping rule, the pixels in the image matrix are rearranged back to their original positions to complete the secondary inverse disorder.

6 Simulation experiment results and analysis

6.1 Experimental set-up

The plaintext images chosen for the experiments are the commonly used standard test images 'Lena', 'mandrill' and 'peppers'. These images are widely used in image processing experiments to evaluate the effectiveness and performance of cryptographic algorithms. The size of both images is 256 × 256. The initial key of the six-dimensional CNN is {0.235, 0.350, 0.735, 0.680, 0.590, 0.472} for the 'Lena' image. The initial key of the six-dimensional CNN for 'mandrill' image is {0.267, 0.445, 0.782, 0.698, 0.567, 0.487}. The experimental platform parameters are shown in Table 1.

Table 1 Hardware and software configuration of the experiment

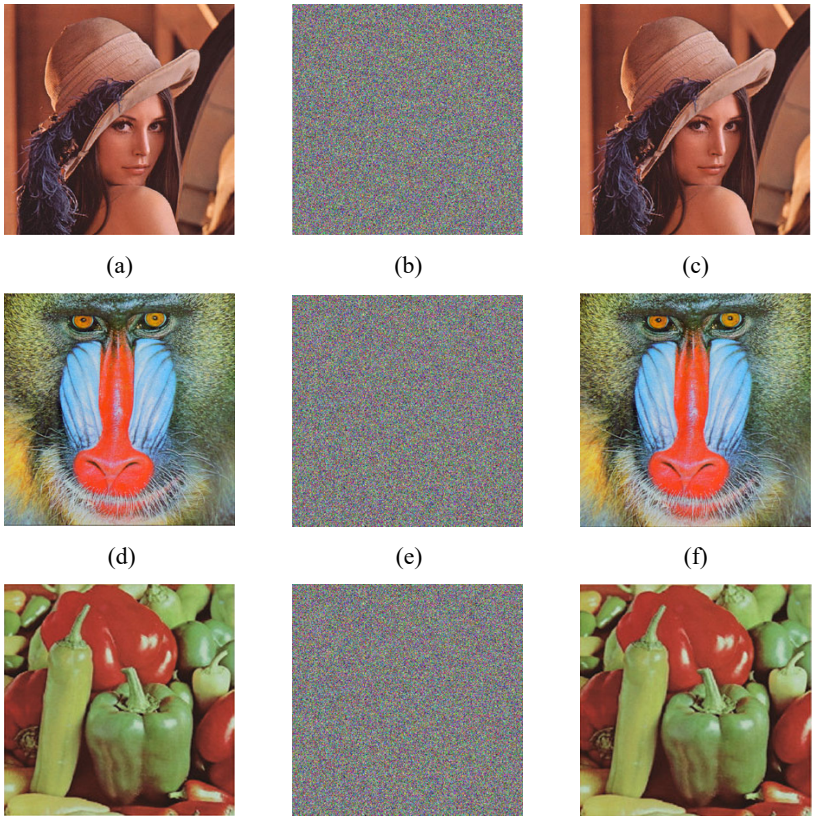
Assemblies	*Instructions*
CPU	Intel Core i7-9700K @ 3.60 GHz
RAM	16 GB DDR4
Stockpile	512 GB SSD
Operating system	Windows 10 Professional 64-bit
Hardware	MATLAB R2020a

To ensure the reproducibility of our experiments, we provide specific details about the parameters utilised in the DE algorithm. The population size was set to 50, which balances exploration and exploitation in the search space. The scaling factor F was chosen to be 0.8, which controls the amplification of differential variations, promoting diversity among the individuals in the population. The optimisation process of DE algorithm parameters is as follows: the population size is set to 50, the scaling factor F is 0.8, and the crossover rate CR is 0.9. These parameters are selected after balancing the convergence speed and the quality of the solution through many experiments and comparisons. The maximum algebra is set to 1,000 to ensure that the optimisation process has enough time to converge to the optimal or nearly optimal solution. These settings were chosen based on preliminary experiments and literature review, indicating that they provide a good balance between convergence speed and solution quality. Furthermore, the maximum number of generations was set to 1,000 to allow sufficient time for the optimisation process to converge to optimal or near-optimal solutions. The

choice of these parameters ensures that the optimisation process is efficient and effective, leading to highly complex and random chaotic sequences for secure image encryption.

The above experimental platform ensures sufficient processing power and environmental stability to accurately assess the performance and effectiveness of the encryption algorithm. The simulation results are shown in Figure 4.

Figure 4 Encryption and decryption simulation results, (a) plain text image Lena, (b) encrypted image Lena, (c) decrypted image Lena, (d) plain text image mandrill, (e) encrypted image mandrill, (f) decrypted image mandrill, (g) plain text image peppers, (h) encrypted image peppers, (i) decrypted image peppers (see online version for colours)



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

The main limitations encountered in the experiment include: the increase of computational overhead when processing high-resolution images, and the scalability problem on large-scale data sets. Future research directions include optimising algorithms to reduce computational complexity and exploring distributed computing methods to improve scalability.

6.2 Sensitivity analysis

In the field of image encryption, sensitivity analysis is an important tool to evaluate the sensitivity of encryption algorithms to input changes. This experiment evaluates the performance of the differential evolutionary six-dimensional CNN (DE-6DCNN) encryption algorithm proposed in this paper by calculating two metrics, number of pixels change rate (NPCR) and unified average changing intensity (UACI), and compares it with traditional CNN, AES and chaotic encryption algorithm are compared. The improvement of NPCR and UACI directly improves the security of image encryption in practical application. For example, in medical image transmission, a higher NPCR value means that patient data is more difficult to be accessed by unauthorised users. In satellite communication, improved UACI has strengthened its resistance to statistical analysis attacks.

NPCR and UACI are standard metrics for evaluating the responsiveness of image encryption algorithms to small changes in the initial image.

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,\ j)}{M \times N} \times 100\% \tag{27}$$

where $D(i, j)$ is a difference matrix, if the pixel values of the encrypted two images at position (i, j) are different, then $D(i, j) = 1$, otherwise $D(i, j) = 0$. M and N are the number of rows and columns of the image, respectively.

$$UACI = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{\left|C_1(i,\ j) - C_2(i,\ j)\right|}{255} \times 100\% \tag{28}$$

where C_1 and C_2 are the images generated by the two encryption processes, respectively; and $|C_1(i, j) – C_2(i, j)|$ is the absolute value of the difference in pixel values between these two images at the position (i, j).

In order to effectively test and compare the sensitivity of different encryption algorithms, ‘Lena’ and ‘mandrill’ were slightly modified, e.g., by changing the value of one pixel (plaintext sensitivity analysis), and the changes in the encryption results were observed. The sensitivity comparison of different encryption algorithms is shown in Table 2.

From the data in Table 2, it can be seen that DE-6DCNN shows higher NPCR and UACI values compared to conventional CNNs, AES and chaotic encryption when processing ‘Lena’ and ‘mandrill’ images NPCR and UACI values. Specifically, DE-6DCNN shows an NPCR value of 99.63% on the ‘Lena’ image, compared to 98.53% for traditional CNN, 99.51% for AES, and 99.59% for chaotic encryption, which shows 1.10%, 0.12%, and 0.04% improvement, respectively. On the ‘mandrill’ image, the NPCR value of DE-6DCNN is 99.60%, while that of conventional CNN is 98.41%, AES is 99.49%, and chaotic encryption is 99.57%, showing 1.19%, 0.11%, and 0.03% improvement, respectively.

Table 2 Sensitivity analysis of four image encryption algorithms

Encryption method	*Image*	*NPCR (%)*	*UACI (%)*
DE-6DCNN	Lena	99.63	33.5
	Mandrill	99.6	33.4
	Peppers	99.58	33.4
CNN	Lena	98.53	29.9
	Mandrill	98.41	29.8
	Peppers	98.32	29.7
AES	Lena	99.51	33.15
	Mandrill	99.49	33.09
	Peppers	99.36	33.06
Chaotic encryption	Lena	99.59	33.45
	Mandrill	99.57	33.35
	Peppers	99.55	33.42

In addition, DE-6DCNN also shows a significant advantage in UACI. On the 'Lena' image, the UACI value of DE-6DCNN is 33.50%, compared to 29.90% for conventional CNN, 33.15% for AES, and 33.45% for chaotic encryption, which show 3.60%, 0.35%, and 0.05% improvement, respectively. On the 'mandrill' image, the UACI value of DE-6DCNN is 33.40%, while that of conventional CNN is 29.80%, AES is 33.09%, and chaotic encryption is 33.35%, which shows 3.60%, 0.31%, and 0.05% improvement, respectively. It is obvious from these results that DE-6DCNN has a significant performance advantage in the sensitivity test of image encryption, proving its effectiveness in improving the sensitivity to changes in initial conditions, thus providing higher security for image encryption.

7 Conclusions

In this paper, an encryption method based on DE-6DCNN is proposed, which effectively solves the limitations of traditional chaotic image encryption methods in terms of processing high-dimensional data, computational complexity and attack resistance. By introducing a six-dimensional CNN, this method is able to generate more complex and unpredictable chaotic sequences, thus enhancing the security and stability of the encryption algorithm. In addition, the parameters of the six-dimensional CNN are optimised using the DE algorithm to improve the complexity and randomness of the chaotic sequences, which further enhances the overall performance of image encryption. The following conclusions can be drawn from the experiments on 'Lena' and 'mandrill' images:

1 The use of 6DCNN can significantly improve the security and efficiency of chaotic image encryption.

2 The DE algorithm performs well in optimising the parameters of the six-dimensional CNN, resulting in the generation of chaotic sequences with higher complexity and randomness.

3 Compared with traditional CNN, AES and chaotic encryption, the DE-6DCNN proposed in this paper shows significant improvement in both NPCR and UACI metrics, which verifies its efficiency and security in image encryption.

The experimental data in this paper were mainly selected from standard image sets, and although the results are satisfactory, the homogeneity of the dataset may limit the generalisation ability of the model. Future work should consider introducing more kinds of image datasets, including images with different resolutions and application scenarios, in order to verify the effectiveness of the model in a wider range of application scenarios.

Acknowledgements

This work is supported by the Key Project of Natural Science Research of Anhui Provincial Department of Education (No. 2022AH052515).

References

Aizenberg, I., Aizenberg, N., Hiltner, J. et al. (2001) 'Cellular neural networks and computational intelligence in medical image processing', *Image and Vision Computing*, Vol. 19, No. 4, pp.177–183.

Arena, P., Fortuna, L. and Porto, D. (2000) 'Chaotic behavior in noninteger-order cellular neural networks', *Physical Review E*, Vol. 61, No. 1, p.776.

Chen, C., Lu, H., Hong, H. et al. (2023) 'Deep self-supervised graph attention convolution autoencoder for networks clustering', *IEEE Transactions on Consumer Electronics*, Vol. 69, No. 4, pp.974–983.

Chen, J., Zhang, Y., Qi, L. et al. (2018) 'Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression', *Optics & Laser Technology*, Vol. 99, pp.238–248.

Chua, L.O. and Yang, L. (1988) 'Cellular neural networks: applications', *IEEE Transactions on Circuits and Systems*, Vol. 35, No. 10, pp.1273–1290.

Gao, H., Zhang, Y., Liang, S. et al. (2006) 'A new chaotic algorithm for image encryption', *Chaos, Solitons & Fractals*, Vol. 29, No. 2, pp.393–399.

Gao, X., Mou, J., Xiong, L. et al. (2022) 'A fast and efficient multiple images encryption based on single-channel encryption and chaotic system', *Nonlinear Dynamics*, Vol. 108, No. 1, pp.613—636.

Guan, Z-H., Huang, F. and Guan, W. (2005) 'Chaos-based image encryption algorithm', *Physics Letters A*, Vol. 346, Nos. 1–3, pp.153–157.

Kaur, M. and Kumar, V. (2020) 'A comprehensive review on image encryption techniques', *Archives of Computational Methods in Engineering*, Vol. 27, No. 1, pp.15–43.

Kumari, M., Gupta, S. and Sardana, P. (2017) 'A survey of image encryption algorithms', *3D Research*, Vol. 8, pp.1–35.

Lang, J. (2015) 'Color image encryption based on color blend and chaos permutation in the reality-preserving multiple-parameter fractional Fourier transform domain', *Optics Communications*, Vol. 338, pp.181–192.

Lin, H., Wang, C., Yu, F. et al. (2020) 'An extremely simple multiwing chaotic system: dynamics analysis, encryption application, and hardware implementation', *IEEE Transactions on Industrial Electronics*, Vol. 68, No. 12, pp.12708–12719.

Liu, S., Guo, C. and Sheridan, J.T. (2014) 'A review of optical image encryption techniques', *Optics & Laser Technology*, Vol. 57, pp.327–342.

Liu, Z-H. (2008) 'Image encryption algorithm based on Lorenz chaotic system', *Journal of Jishou University (Natural Sciences Edition)*, Vol. 29, No. 5, p.39.

Opara, K.R. and Arabas, J. (2019) 'Differential evolution: a survey of theoretical analyses', *Swarm and Evolutionary Computation*, Vol. 44, pp.546–558.

Pareek, N.K., Patidar, V. and Sud, K.K. (2006) 'Image encryption using chaotic logistic map', *Image and Vision Computing*, Vol. 24, No. 9, pp.926–934.

Salleh, M., Ibrahim, S. and Isnin, I.F. (2003) 'Image encryption algorithm based on chaotic mapping', *Jurnal Teknologi*, Vol. 39, pp.1–12.

Sang, Y., Sang, J. and Alam, M.S. (2022) 'Image encryption based on logistic chaotic systems and deep autoencoder', *Pattern Recognition Letters*, Vol. 153, pp.59–66.

Tong, X.J., Wang, Z., Zhang, M. et al. (2015) 'An image encryption algorithm based on the perturbed high-dimensional chaotic map', *Nonlinear Dynamics*, Vol. 80, pp.1493–1508.

Ye, G. (2010) 'Image scrambling encryption algorithm of pixel bit based on chaos map', *Pattern Recognition Letters*, Vol. 31, No. 5, pp.347–354.

Zhou, Y., Bao, L. and Chen, C.P. (2014) 'A new 1D chaotic system for image encryption', *Signal Processing*, Vol. 97, pp.172–182.