A Novel Color Image Encryption Scheme Based on Cellular Neural Network and Chen’s Chaotic System

Renxiu Zhang¹, Longfei Yu¹, Donghua Jiang², Wei Ding¹, Jian Song¹, Kuncheng He¹, and Qun Ding¹,*

¹Electronic Engineering College, Heilongjiang University, Harbin 150080, China
²School of Information Engineering, Chang’an University, Xi’an 710064, China
*qunding@aliyun.com

ABSTRACT

With the explosive development of communication technology, digital images are more widely stored and transmitted on the network as a medium of communication among people. At the same time, the security of the digital image has become the focus of people’s attention, and it is also the hotspot and difficulty of current research. Therefore, a novel color image encryption scheme is proposed in this paper by combining the 6-dimensional cellular neural network (CNN) and Chen’s hyperchaotic system. In the proposed scheme, the initial keys and switching function generated by the plaintext image are utilized to control the CNN to complete the scrambling operation. Then, using the Chen’s hyperchaotic system to diffuse the scrambled image for realizing higher security. Finally, the simulation tests and security performance analyses on the proposed encryption scheme are carried out. Experimental results demonstrate that the proposed scheme has an excellent encryption effect compared with other advanced image cryptography systems.

Introduction

With the rapid development of information technology, the importance of the network and its impact on society are also increasing. A large amount of information is stored and transmitted on the network in the form of short messages, videos, images, audio, etc. At the same time, the problem of information security has become increasingly serious. The digital image is widely used in communication for its vividness and clarity. Also, the continuous update of electronic equipment makes the transmission of images on the network more and more convenient, thus the image encryption technology is particularly important. The chaotic signal is suitable for secure communication technology especially because of its noise-like, initial value sensitivity, and long-term unpredictability1,2. And the algorithms based on chaos show outstanding characteristics in security, complexity, speed, and computing power3,4.

In recent years, the research of chaotic cryptography on image encryption has also attracted the attention of many scholars5-11. For instance, a novel image encryption approach based on the “permutation-substitution” network and the chaotic system is proposed in Ref.12. Liang et al.13 introduced a quantum algorithm based on quantum XOR operations generated with the logistic map to encrypt gray-level information, while the generalized affine transform is used to encode position information. In Ref.14, a 2-D Logistic map is used to generate the pseudorandom number generator (PRNG) to control the combination of position permutation and diffusion with XOR. Broumandnia15 generates an incoherent cryptographic image by harnessing modular chaotic maps, which hides any information about the original image. Chai et al.16 proposed a color image encryption algorithm based on dynamic DNA encryption and chaos, utilized the hash function and external parameters to calculate the initial value, which can effectively resist the known-plaintext attacks with better security. Wang et al.17 proposed an encryption scheme for color images that uses the 1-D and 2-D logistic map to generate a chaotic matrix. Then, these two chaotic maps are repeatedly replaced in sequence. The experimental results prove the security and applicability of the scheme. Fu et al.18 proposed a fast color image encryption scheme, which is based on permutation and substitution in the quantized sequence extracted from the orbit of Chen’s chaotic system. Sundari and Karthika19 presented an image encryption and decryption algorithm based on the concept of Logistic map. However, the encryption scheme of a single chaotic system can no longer meet the security and real-time requirements of modern life rhythm for image communication. Researchers have discovered that when CNN theory is applied to the chaotic encryption algorithm, hyperchaotic systems provide more complex dynamic behaviors, with strong randomness, unpredictability, and higher security performance20.

CNN is a nonlinear analog processor with locally interconnected, double-valued output signals, which was first proposed by Chua and Yang in 198821. It is an artificial neural network formed by the improvement of Hopfield neural network and cellular automata22, which adopts the local connection of cellular automata and at the same time resolves the difficulty of
Hopfield neural network on hardware. As a flexible and efficient local interconnection network, CNN not only has complex chaotic dynamics characteristics but also can be easily integrated on the very large scale integration (VLSI). Compared with the traditional chaotic system, CNN has a large key space and outstanding permutation and diffusion properties. Therefore, CNN is widely utilized in encryption systems, and has achieved good encryption effects on digital watermark technology, voice encryption, and image encryption. For example, Wang et al. proposed that using the cellular automata to perform the confusion and diffusion tasks suitable for parallel computing. Qing et al. analyzed the chaotic phenomenon of CNN model, then Peng et al. designed an image encryption algorithm based on the model of Ref. Besides, on the basis of the “scrambling-diffusion” mechanism, Kadir et al. applied the 6th-order CNN hyperchaotic system to generate a diffusion sequence to encrypt the color image. Meanwhile, a color image cryptography system based on hyperchaotic cellular neural network and chaotic control parameter was proposed in Ref., which adopted the compound “scrambling-diffusion” framework to encrypt the color image.

In order to further improve the security of the image encryption algorithm, obtain a larger key space, and better unpredictability, this paper proposes a new color image encryption scheme based on a 6-dimensional CNN and Chen’s hyperchaotic system. The plaintext image is utilized to generate the initial keys that are used as the initial value of the CNN, and the switching key is utilized to select the chaotic sequences. The selected chaotic sequence is used in the two stages of system scrambling and diffusion respectively to complete the encryption of the image. The proposed scheme can not only change the histogram of the image, but also break the high correlation between adjacent pixels. Meanwhile, associating the initial parameters of the CNN with the plaintext image can ensure that the proposed encryption scheme has sufficient sensitivity to the plaintext and has the advantages of resisting the known-plaintext attacks and chosen-plaintext attacks effectively. In addition, the proposed scheme adopts a 6-dimensional CNN chaotic system, which greatly increases the key space and makes it sufficient to resist the brute force attack. Experimental results show that the presented scheme is highly sensitive to both plaintext and ciphertext, greatly reduces the original high correlation between adjacent pixels in the plaintext image, has an almost ideal information entropy value and a key space sufficient to resist the brute force attack, which meets the security requirements of the encryption algorithm and has an excellent encryption effect.

The rest of the paper is organized as follows: Section 2 briefly introduces the preliminaries related to the encryption scheme proposed in this paper, including the mathematical model and chaotic characteristics of the CNN and Chen’s hyperchaotic system. Section 3 explains the design of the cryptosystem and the application of the proposed encryption scheme on the color image. And detailed experimental results and security analyses are presented in Section 4. Finally, the conclusions are drawn in Section 5.

Preliminaries

Cellular neural network

The basic component unit of CNN is called a cell. Besides, each cell can be equivalent to a nonlinear first-order circuit composed of the linear resistor, the linear capacitor, and the voltage-controlled current source as shown in Fig. 1. CNN is formed by the regular arrangement and connection of the same cell neurons in space. Each neuron is only connected with the adjacent 8 neurons and the cells that are not directly connected influence each other through continuous and dynamic propagation effect. Each neuron has the input and output states. A of size $M \times N$ is composed of $M$ rows and $N$ columns of cells. A $3 \times 3$ cellular neural network is constructed in Fig. 2, where $C(i, j)$ represents the cells in the $i$-th row and $j$-th column in the cellular neural network. The chaotic phenomenon of the 6-dimensional CNN hyperchaotic system is described in Ref. The state equation of the 6-order fully interconnected CNN is shown in Eq. (1):

$$
\frac{dx_i}{dt} = -x_i + a_i p_j + \sum_{k \neq j}^{6} a_{jk} p_k + \sum_{k=1}^{6} S_{jk} x_k + i_j,
$$

where $j = 1, 2, \ldots, 6$.

The system is in a chaotic state when the parameters are set as follows: $a_j = 0$ ($j = 1, 2, 3, 4, 5, 6$), $a_4 = 200$; $a_{jk} = 0$ ($j, k = 1, 2, \ldots, 6; j \neq k$); $S_{12} = S_{23} = S_{33} = S_{13} = 1$, $S_{14} = -1, S_{22} = 3, S_{31} = 14$, $S_{42} = -14, S_{41} = 100, S_{44} = -99$, $S_{52} = 18, S_{65} = 4, S_{66} = -3$. The mathematical model of 6th-order CNN is shown in Eq. (2), which can be obtained by
substituting the parameters into Eq. (1).

\[
\begin{align*}
\dot{x}_1 &= -x_3 - x_4 \\
\dot{x}_2 &= 2x_2 + x_3 \\
\dot{x}_3 &= 14x_1 - 14x_2 \\
\dot{x}_4 &= 100x_1 - 100x_4 + 200p_4 \\
\dot{x}_5 &= 18x_2 + x_1 - x_5 \\
\dot{x}_6 &= 4x_5 - 4x_6 + 100x_2
\end{align*}
\]

(2)

where \( p_4 = \frac{1}{2}(|x_4 + 1| - |x_4 - 1|) \).

The Lyapunov exponent of the 6th-order CNN can be calculated, \( \lambda_1 = 2.7481, \lambda_2 = -2.9844, \lambda_3 = 1.2411, \lambda_4 = -14.4549, \lambda_5 = -1.4123, \lambda_6 = -83.2282 \), when \( t \to \infty \). Two of them are positive, which indicates that the system is hyperchaotic. Since the initial values \( x_i(0) (i = 1, 2, 3, 4, 5, 6) \) can be arbitrary values of any length, this greatly increases the key space and security. The iteration step size \( h \) is set to 0.01, and the initial values are set as follows: \( x_1(0) = 0.1, x_2(0) = 0.3, x_3(0) = 0.5, x_4(0) = 0.7, x_5(0) = 0.9, x_6(0) = 1.1 \). The phase diagram of partial corresponding 6th-order CNN chaotic attractor obtained by Runge-Kutta method is plotted in Fig. 3.

**Chen’s hyperchaotic system**

In 1999, Chen discovered a system with more complex dynamic behaviors than Lorenz system when studying chaotic feedback control. The chaotic attractor of Chen’s system has more complex and abundant dynamic characteristics than that of Lorenz system. The mathematical model of Chen’s hyperchaotic system is expressed as follows.

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

(3)

where \( a, b \) and \( c \) are system parameters, when \( a = 35, b = 3, c = 28 \), the system is in a chaotic state. Eq. (3) is solved by the fourth-order Runge-Kutta method. The initial parameters are set as follows: \( x(0) = 0.1, y(0) = 0.2, z(0) = 0.3 \), step length \( h = 0.001 \), and 100000 iterations are performed. The chaotic attractor of this system are obtained as shown in the Fig. 4.
We calculate the sum of gray values of each cell respectively, and record them as $m$.

The function of switching key $d$ is to control the selection of dimensions. In the process of confusion, in order to facilitate the implementation, we choose one dimension in the 6-dimensional chaotic sequences generated by CNN to construct a matrix for the generation of the chaotic sequences, and the process of generation of the initial keys are as follows. A three-channel color plaintext image with a size of $M\times N\times 3$ is inputted and converted into a single-channel grayscale image. And as shown in Fig. 5, it is divided into 6 non-overlapping cells, and the size of each cell is $m\times n$, $m \times n_1$, $m \times n$, $m \times n_1$, $m_1 \times n$, and $m_1 \times n_1$, where $m = (M - \text{mod}(M, 3))/3$, $n = (N - \text{mod}(N, 2))/2$, $m_1 = M - 2 \times (M - \text{mod}(M, 3))/3$, and $n_1 = N - (N - \text{mod}(N, 2))/2$. We calculate the sum of gray values of each cell respectively, and record them as $\text{sum1}$, $\text{sum2}$, ..., $\text{sum6}$, then let $k_1$, $k_2$, ..., $k_6$ denote their sine values.

**Switching key**

The function of switching key $d$ is to control the selection of dimensions. In the process of confusion, in order to facilitate the implementation, we choose one dimension in the 6-dimensional chaotic sequences generated by CNN to construct a matrix for image confusion. As shown in Fig. 6, when the value of $d$ is 1, the switch $K_1$ is closed, that is, the first-dimensional chaotic...
sequence $D_1$ is selected. And when the value of $d$ is 2, the switch $K_2$ is closed, that is, the second-dimensional chaotic sequence $D_2$ is selected, and so on. We take the gray average value $a$ of the gray image and do the following operation (where fix is the rounding function and mod is the modulus function).

$$d = \text{mod}(\text{fix}(a), 6) + 1,$$

this ensured that the output value of $d$ is an integer within the range 1 to 6.

**Encryption scheme design**

**Scrambling**

We input the initial keys $k_1, k_2, ..., k_6$ and the control parameters into the CNN chaotic system, and at the same time, input the switching key $d$ which is used to select a sequence by controlling the opening and closing of the switch $K_1-K_6$. Then one sequence is selected from the generated 6-dimensional chaotic sequences. We discard the first 1000 elements of the selected sequence and then extract the remaining $M \times N$ elements. These elements are denoted as the sequence S. The quantitative formula of the sequence S is given as follow.

$$SQ = \text{mod}(\text{mod}(\text{abs}(S) \times 1000, 1000), 256),$$

Eq. (5) is equivalent to extracting the three digits after the decimal point of the chaotic sequence’s absolute value, and then converting it to a value between [0, 255]. The processed chaotic sequence is transformed into a two-dimensional matrix, and the elements in the matrix are traversed according to columns. After incremental sorting, the elements are put into the new empty matrix by columns, namely, the sorted chaotic matrix SCS. Besides, the original position of elements in SCS are recorded in another new empty matrix, namely, the position matrix ICS. If the elements in the increment sorting process are found equal, the element traversed first is placed first. Next, the plaintext pixel matrix is rearranged according to the position matrix ICS. That is to say that the scrambling transformation is completed. In order to better understand the proposed scrambling algorithm, an example of the scrambled process is demonstrated in Fig. 7, where $M = 3, N = 4$. Fig. 7 (a)-(b) represent a two-dimensional chaotic matrix CS and the corresponding sorted two-dimensional scrambling matrix SCS, respectively. Then the position matrix ICS that represents the original position of elements in sorted chaotic matrix is shown in Fig. 7 (c). Using the matrix ICS to scramble the plaintext matrix. Ultimately, the resulting scrambled matrix is displayed in Fig. 7 (e).

**Diffusion**

The 501st to 503rd values of the sequence selected in the scrambling process are taken as the initial values of the Chen’s hyperchaotic system, denoted as $x_1, x_2, x_3$. They are inputted into Chen’s system, and the fourth-order Runge Kutta method was
utilized to solve Chen’s system iteratively for $M \times N$ times. Then we perform the following operation on the generated chaotic sequence $C_1, C_2, C_3$ with a length of $M \times N$ in three dimensions.

$$C(i) = \frac{C_1(i) + C_2(i) + C_3(i)}{3}, \quad (6)$$

where $i = 1, 2, \ldots, M \times N$.

That is, we calculate the mean of the three sequences and define it as the new sequence $C$. Then the sequence $C$ is quantified according to Eq. (5). The quantized data is structured into a diffusion matrix $DM$ with the size of $M \times N$. The XOR operations are performed on it and the three components of the scrambled image SI respectively. And the ciphertext image CI in the form of RGB will be obtained after integration.

**Decryption scheme design**

**First decryption**

We input the initial keys $k_1, k_2, \ldots, k_6$ and control parameters into the CNN chaotic system, and at the same time input the switching key $d$. Extracting $M \times N$ elements from the resulting chaotic sequence produced by CNN to acquire the position matrix $ICS$ and the initial values $x_1, x_2, x_3$ of Chen’s hyperchaotic system. The initial values $x_1, x_2, x_3$ are inputted into Chen’s system. Then the sequence $C$ can be generated by averaging the 3-dimensional chaotic sequence acquired from Chen’s system. After processing, the diffusion matrix $DM$ is obtained, then we XOR the diffusion matrix $DM$ with the three components of the ciphertext image CI respectively. The first stage of the decryption process is completed after integration, and the scrambled image SI is obtained.
The block diagram of the encryption process is shown in Fig. 6, and the encryption effect is shown in Fig. 8 (c). It is obvious that the ciphertext images present a uniform carpet-like distribution, and no valuable information can be distinguished from it. It is indicated that the encryption scheme proposed in this paper can cover up the original image information successfully.

Reverse scrambling (second decryption)
The position matrix ICS obtained in the first stage of decryption process was utilized to reverse scramble the RGB components of the scrambled image SI and integrate the results into the RGB form, that is, the second stage of the decryption process was completed.

**Step to encrypt and decrypt color images**

**Steps to encrypt**
- Step 1: Initial keys $k_1, k_2, ..., k_6$, switching key $d$, and control parameters are inputted into the CNN hyperchaotic system, and the position matrix ICS will be obtained. Then the matrix ICS is utilized to scramble the plaintext image PI and complete the first encryption.
- Step 2: We input the initial values $x_1, x_2, x_3$ into Chen’s hyperchaotic system. Then the diffusion matrix DM can be obtained, which is XORed respectively with the three components matrices of the plaintext image obtained after the first encryption to complete the second encryption.
- Step 3: For higher security, the above steps can be repeated $n$ times.

The block diagram of the encryption process is shown in Fig. 6, and the encryption effect is shown in Fig. 8 (c). It is obvious that the ciphertext images present a uniform carpet-like distribution, and no valuable information can be distinguished from it. It is indicated that the encryption scheme proposed in this paper can cover up the original image information successfully.

**Steps to decrypt**
- Step 1: Initial keys $k_1, k_2, ..., k_6$, switching key $d$, and control parameters are inputted into the CNN hyperchaotic system, the position matrix ICS and the initial values $x_1, x_2, x_3$ of Chen’s system will be obtained.
- Step 2: Input the initial values $x_1, x_2, x_3$ into the Chen’s system, and the diffusion matrix DM will be obtained. The matrix DM is XORed respectively with the three components matrices of the ciphertext image CI. After the integration, the first decryption is completed and the scrambled image SI is obtained.
Figure 8. The experimental results of encryption and decryption algorithm: (a) The original plaintext image; (b) The scrambled image; (c) The encrypted ciphertext image; (d) The decrypted image.

• Step 3: The position matrix ICS in step1 is carried out the inverse scrambling on the RGB component of the scrambled image SI. Integrating it into the RGB form, the second stage of decryption process is completed.

The decryption effect is shown in Fig. 8 (d). It can be seen that there is almost no visual difference between the decrypted image and the original plaintext image, indicating that the scheme proposed in this paper can successfully decrypt the color image.

Experimental results and security analysis

In this section, we conduct simulation tests to evaluate the performance of the proposed encryption scheme. All simulation tests are carried out in the experimental environment of Matlab R2015b with a 2.90GHz CPU and 8GB memory. The parameters of the standard test images used in the experiments are as follows: the color Lena image with a size of $512 \times 512 \times 3$, the color Baboon image with a size of $512 \times 512 \times 3$, the color Peppers image with a size of $512 \times 512 \times 3$, the color Airplane image with a size of $512 \times 512 \times 3$, the color Barbara image with a size of $787 \times 576 \times 3$, and the color House image with a size of $256 \times 256 \times 3$.

Histogram analysis

The histogram is one of the indexes to measure the performance of encryption scheme. For encrypted information, if the histogram of the ciphertext information is unevenly distributed, it will be easily cracked by the ciphertext attack. The histogram comparisons of partial test images before and after encryption are shown in Fig. 9. It can be intuitively seen that the distributions of original images are uneven before encryption, that is, there is a significant difference in the probability of grayscale. After encryption, the histograms of ciphertext images become very uniform, with good statistical characteristics, which increases the difficulty of deciphering, and can effectively resist statistical attacks.

The variance of a histogram can also be used to describe quantitatively the distribution characteristics of the histogram. 

Figure 9. Histogram analysis: (a) The original plaintext image; (b) Histogram of the RGB component of the original plaintext image; (c) The encrypted ciphertext image; (d) Histogram of the RGB component of encrypted ciphertext image.

which is calculated by Eq. (7):

\[
\text{var}(Z) = \frac{1}{N^2} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \frac{1}{2} (z_i - z_j)^2,
\]

where \( N \) denotes the number of gray levels of an image. \( Z \) is a vector and \( z_i \) and \( z_j \) are the numbers of pixels with gray values equal to \( i \) and \( j \) respectively. The smaller the variance of a histogram is, the flatter the histogram is, and the number of each gray level pixel in the image tends to be equal. The ideal value of \( \text{var}(Z) \) is 0, which means \( z_i = z_j \) for all \( i \) and \( j \). The variances of histograms of the tested plaintext images and the corresponding ciphertext images are listed in Table 1. It can be seen that the variance of the cipher images encrypted by our scheme is greatly reduced. Thus, our scheme has good performance in resisting statistical attacks.

**Correlation of adjacent pixels**

One of the important features of an image is the high correlation between adjacent pixels. Attackers generally use it to decipher the ciphertext image, so in order to prevent the attacker from inferring the key or plaintext from the relationship between adjacent pixels, it is necessary to destroy the correlation of adjacent pixels. The encryption scheme is considered to be effective if the information of the encrypted image cannot be obtained through adjacent pixels. The correlation calculation formula of
adjacent pixels is as follows:

\[ E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i, \]  
\[ D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2, \]  
\[ \text{cov}(x,y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)), \]  
\[ r_{xy} = \frac{\text{cov}(x,y)}{\sqrt{D(x)D(y)}}, \]

where \( x \) and \( y \) are the gray values of two adjacent pixels in the image, \( \text{cov}(x,y) \) is the covariance, \( D(x) \) is the variance of the variable \( x \), and \( E(x) \) is the expectation of variable \( x \). The pixel distribution of plaintext image and ciphertext image in R, G, and B components of the scheme presented in this paper is shown in Fig. 10. It can be seen that the adjacent pixels of the original image are concentrated in the diagonal region, which is closely related, whereas the encrypted image pixels are distributed in the whole region irregularly, which means that the correlation of the encrypted image has been effectively reduced. Table 2 describes the correlation between the three components of the plaintext image and the ciphertext image in the horizontal, vertical, and diagonal directions. It can be seen that the two adjacent pixels in the plaintext image are highly correlated, whereas the correlation tends to zero in the encrypted image. Table 3 shows the correlation comparison between the scheme proposed in this paper and the scheme proposed in other references. It can be seen that the performance of the scheme proposed in this paper is better. In other words, it is not feasible for attackers to crack ciphertext images by using the correlation of pixels. Therefore, our scheme is security and free from statistical attacks.

### Table 1. The variance of histograms of the plaintext images and ciphertext images.

| Images          | Plaintext image | Ciphertext image |
|-----------------|-----------------|------------------|
|                 | R   | G   | B   | R   | G   | B   |
| Lena (512 × 512)| 991739.98 | 453157.22 | 1378183.53 | 1425.59 | 1304.59 | 1732.32 |
| Barbara (787 × 576) | 954873.52 | 1555262.50 | 1864604.11 | 2090.18 | 1841.38 | 2483.31 |
| Pepper (512 × 512) | 857051.13 | 201185.63 | 2351617.68 | 1219.48 | 1147.39 | 1415.58 |
| Baboon (512 × 512) | 351098.48 | 601865.98 | 413224.78 | 1085.59 | 1184.87 | 1227.58 |
| House (256 × 256) | 258651.73 | 300174.25 | 395652.48 | 272.55 | 273.96 | 321.41 |

### Table 2. Correlation of adjacent pixels of the plaintext image and the encrypted image in the direction of horizontal, vertical and diagonal of RGB component.

| Correlation coefficient | Horizontal | Vertical | Diagonal |
|-------------------------|------------|----------|----------|
|                         | R   | G   | B   | R   | G   | B   | R   | G   | B   |
| Lena (512 × 512)        | 0.9737 | 0.9740 | 0.8418 | 0.9963 | 0.9902 | 0.9555 | 0.9743 | 0.9615 | 0.9219 |
| Encrypted Lena          | 0.0073 | 0.0084 | 0.0072 | -0.0134 | -0.0133 | -0.0107 | 0.0034 | 0.0055 | 0.0035 |
| Baboon (512 × 512)      | 0.4301 | 0.4717 | 0.5558 | 0.8568 | 0.7619 | 0.8969 | 0.8588 | 0.7307 | 0.8461 |
| Encrypted Baboon        | 0.0019 | -0.0030 | -0.0117 | 0.0530 | -0.0115 | -0.0116 | 0.0051 | 0.0056 | 0.0043 |
| Peppers (512 × 512)     | 0.9727 | 0.9929 | 0.9847 | 0.9710 | 0.9927 | 0.9812 | 0.9587 | 0.9706 | 0.9467 |
| Encrypted Peppers       | 0.0069 | 0.0130 | 0.0041 | -0.0014 | 0.0076 | 0.0124 | 0.0069 | 0.0075 | 0.0067 |
| Airplane (512 × 512)    | 0.9851 | 0.9575 | 0.9575 | 0.9605 | 0.9941 | 0.9941 | 0.9355 | 0.9327 | 0.9327 |
| Encrypted Airplane      | 0.0062 | -0.0041 | -0.0016 | 0.0399 | 0.0446 | 0.0333 | 0.0013 | 0.0018 | 0.0003 |

### Information entropy

Information entropy is utilized to measure the randomness of a random variable, which is defined in Eq. (12).

\[ H(s) = - \sum_{i=0}^{L} P(m_i) \log_2 p(m_i) , \]
where \( m_i \) is the \( i \)-th grayscale value of the \( L \)-level grayscale image. Information entropy measures the distribution of grayscale values in the image. The pixel values are evenly distributed if the entropy value is close to 8, and the password is not vulnerable to statistical attacks\(^{30}\). Therefore, an effective encryption scheme should make the information entropy tend to 8. The entropy values of original plaintext images and the encrypted ciphertext images in the R, G, and B component are respectively calculated as shown in Table 4, which are very close to the theoretical value, indicating that the proposed scheme has good randomness and can effectively resist frequency analysis attack.

### Sensitivity analysis

#### Key sensitivity

Key sensitivity refers to the fact that encryption images and decryption images can vary greatly even if the key is only slightly changed. Fig. 11 shows the original image, the image encrypted with the correct key, the image encrypted with the wrong key (the key is changed by 1 bit), the difference between the two encrypted images, the image decrypted with the wrong key and the image decrypted with the correct key. It can be concluded that even if the key is only slightly changed, it will lead to incorrect encrypted images and decrypted images, which can indicate that the key sensitivity of the proposed scheme is excellent.
| Images          | Plaintext image |                | Ciphertext image |                |
|---------------|----------------|----------------|------------------|----------------|
|               | R             | G             | B                | R             | G             | B                |
| Lena (512 × 512) | 7.2510        | 7.5110        | 6.9403           | 7.9707        | 7.9437        | 7.9676           |
| Peppers (512 × 512) | 7.3255        | 7.3912        | 6.9169           | 7.9632        | 7.9324        | 7.9569           |
| Baboon (512 × 512)   | 7.6833        | 7.4466        | 6.7847           | 7.9541        | 7.9201        | 7.9438           |
| Airplane (512 × 512) | 6.7113        | 6.7853        | 6.2128           | 7.9633        | 7.9342        | 7.9594           |
| Barbara (787 × 576)  | 7.7581        | 7.6078        | 7.5774           | 7.9515        | 7.9230        | 7.9406           |

Table 4. Information entropy of the plaintext images and ciphertext images.

**Plaintext sensitivity**

The differential attack is a kind of chosen-plaintext attack. In the case of altering one or more pixels of the plaintext and encrypting the original plaintext and the slightly altered plaintext respectively. If the change of position or degree of the obtained two ciphertext pixels is not obvious or shows a regular pattern, then the attacker can use the differential attack to obtain the key. Therefore, a good encryption scheme should be highly sensitive to changes in the plaintext, so as to effectively resist differential attacks. The performance of resisting differential attacks is usually measured by the number of pixel change rate (NPCR) and the unified average changing intensity (UACI).

The NPCR obtains the difference between two images by evaluating the different number of pixels in the two images, which is defined in Eq. (13):

\[
\text{NPCR} = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} D(i, j)}{M \times N} \times 100\%,
\]

where \(M\) and \(N\) represent the height and width of an image, \(D(i, j)\) is the difference value of the pixels corresponding to the two encrypted images \(C_1\) and \(C_2\), which is defined in Eq. (14):

\[
D(i, j) = \begin{cases} 
1, & c_1(i, j) \neq c_2(i, j) \\
0, & c_1(i, j) = c_2(i, j)
\end{cases}
\]

The UACI measures the average intensity difference between two different images, which is defined in Eq. (15):

\[
\text{UACI} = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} |c_1(i, j) - c_2(i, j)|}{255} \times \frac{1}{M \times N}
\]

The closer the NPCR value is to 100% and the UACI value is to 33%, the better the encryption quality is. When the plaintext is changed by 1 bit, we respectively test the NPCR and UACI values of the scheme proposed in this paper, the test results are shown in Table 5. It can be seen that the NPCR and UACI values of this scheme are very close to the theoretical values. It shows that the encryption system proposed in this paper has good sensitivity to plaintext and has a strong ability to resist differential attacks.

| Images          | NPCR(%) | UACI(%) |
|-----------------|---------|---------|
|                 | R       | G       | B       | R       | G       | B       |
| Lena (512 × 512) | 99.5859 | 99.5525 | 99.5922 | 33.0865 | 33.1109 | 33.0458 |
| Peppers (512 × 512) | 99.6059 | 99.6124 | 99.6197 | 33.1151 | 33.1492 | 33.0812 |
| Baboon (512 × 512) | 99.6128 | 99.5903 | 99.5781 | 33.0810 | 33.1133 | 33.0467 |
| Airplane (512 × 512) | 99.6166 | 99.5796 | 99.6128 | 33.1021 | 33.1243 | 33.0585 |
| Barbara (787 × 576) | 99.6098 | 99.6042 | 99.5877 | 33.1288 | 33.1573 | 33.0858 |
| Ref.15          | 99.6338 | 99.6094 | 99.5795 | 33.2918 | 33.6839 | 33.3533 |
| Ref.16          | 99.6000 | 99.6100 | 99.6100 | 33.5600 | 33.4500 | 33.4900 |
| Ref.17          | 99.6300 | 99.5900 | 99.6700 | 33.4300 | 33.3900 | 33.5100 |
| Ref.47          | 99.3350 | -       | -       | 33.6000 | -       | -       |

Table 5. The NPCR and UACI of RGB component.
Figure 11. The test results of the key sensitivity analysis: (a) The plaintext image; (b) The correctly encrypted image; (c) The incorrectly encrypted image; (d) The difference between the two encrypted images; (e) The incorrectly decrypted image; (f) The correctly decrypted image.

**Key space**

In order to resist the brute force attacks, there must be a large enough key space. In the scheme of this paper, the key includes the switching key $d$ ranging from 1 to 6 and the initial values $k_1, k_2, ..., k_6$ generated by the plaintext image, it is declared as double-precision type, the key space of the encryption scheme is $6 \times 2^{192}$. Compared with other references, as shown in Table 6, the key space of the scheme proposed in this paper is huge, which is much larger than the theoretical requirement value $2^{128}$, which is enough to resist brute force attacks.

| Scheme | Ours | Ref.9 | Ref.10 | Ref.18 | Ref.30 | Ref.32 | Ref.48 | Ref.14 | Ref.49 | Ref.28 | Ref.47 |
|--------|------|-------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| Key space | $6 \times 2^{192}$ | $2^{18}$ | $2^{149}$ | $2^{159}$ | $10^{38}$ | $10^{56}$ | $10^{45}$ | $2^{128}$ | $2^{128}$ | $10^{37}$ |

Table 6. Comparison of the key space with other referenced schemes.

**Robustness analysis**

Robustness refers to the ability to decrypt the original image when the encrypted image is polluted or attacked by noise during transmission. We added Pepper & Salt noise and Gaussian noise with different noise densities to the cipher image respectively, and analyzed the robustness of the encrypted image when it is polluted. Figure 12 (a)-(c) shows that Pepper & Salt noise with noise densities of 0.1, 0.15 and 0.5 are added to the cipher image, respectively. The noise-contaminated ciphered images are then decrypted using the same key and the decrypted images are shown in Fig. 12 (d)-(f). Fig. 12 (g)-(i) shows that Gaussian white noise with noise densities of 0.01, 0.1 and 0.15 are added to the cipher image, and the corresponding decrypted images are shown in Fig. 12 (j)-(l). The experimental results show that the scheme is robust to Pepper & Salt noise and Gaussian noise added in ciphertext images.

In addition, we conducted a cropped attack test on the scheme proposed in this paper. We cropped and removed parts of the cipher image, and then applied the same key to test its decryption effect. Figure 13 (a)-(c) shows that 6.25%, 25% and 50% of the cipher image is removed where 255 is inserted to the cropped pixels. Fig. 13 (d)-(f) shows the decrypted image is obtained using the proposed scheme. We can easily observe that by cropping a reasonably area, such as 6.25% or 25% of the cipher,
Figure 12. Experimental results of adding noise: (a) Cipher House image with Pepper & Salt noise of 0.1; (b) Cipher House image with Pepper & Salt noise of 0.15; (c) Cipher House image with Pepper & Salt noise of 0.5; (d) Decrypted image from cipher with Pepper & Salt noise of 0.1; (e) Decrypted image from cipher with Pepper & Salt noise of 0.15; (f) Decrypted image from cipher with Pepper & Salt noise of 0.5; (g) Cipher House image with Gaussian white noise with mean value 0 and variance value 0.01; (h) Cipher House image with Gaussian white noise with mean value 0 and variance value 0.1; (i) Cipher House image with Gaussian white noise with mean value 0 and variance value 0.01; (j) Decrypted image from cipher with Gaussian white noise with mean value 0 and variance value 0.01; (k) Decrypted image from cipher with Gaussian white noise with mean value 0 and variance value 0.1; (l) Decrypted image from cipher with Gaussian white noise with mean value 0 and variance value 0.15.
Figure 13. Experimental results of decryption from cropped cipher images: (a) Cipher image with 6.25% cropped; (b) Cipher image with 25% cropped; (c) Cipher image with 50% cropped; (d) Decrypted image from 6.25% cropped cipher; (e) Decrypted image from 25% cropped cipher; (f) Decrypted image from 50% cropped cipher.

The quality of the reconstructed images are still recognizable and acceptable. Even if there is only a half of the cipher image remained, the deciphered image can still be recognized. Therefore, the scheme proposed in this paper has good robustness.

Randomness tests analysis

SP800-22 is a software package released by the national institute of standards and technology (NIST) for randomness testing, which includes 16 randomness tests. These tests are used to determine whether the data flow satisfies the characteristics of randomness. In this part, we will use SP800-22 to make a qualitative judgment on the randomness of color cipher images. The experimental results are shown in Table 7. By analyzing the data in Table 7, it can be seen that the generated color cipher images have successfully passed the test. Therefore, the color cipher images generated in this paper have good randomness.

Conclusion

In this paper, a novel color image encryption scheme based on the combination of the 6-dimensional CNN hyperchaotic system and Chen’s system was proposed. The advantages of the scheme are as follows:

- The key changes with the change of the plaintext image, so that it can resist the known plaintext or ciphertext attacks, and effectively overcome the shortcomings of traditional stream ciphers that are not sensitive to changes in the plaintext.

- The use of the 6-dimensional CNN hyperchaotic system increases the key space greatly, making the scheme sufficient to resist various brute force attacks.

- Compared with the traditional encryption scheme based on a single chaotic system, combining CNN with a high-dimensional chaotic system can achieve higher security.

Simulation tests and security analysis showed that the scheme proposed in this paper is highly sensitive and the degree of scrambling of the ciphertext image is relatively high. Moreover, in this paper, the correlation between adjacent pixels is effectively reduced. Also, the information entropy value is close to the ideal value and the key space is huge. Above all, the scheme can effectively resist various attacks and the encryption effect is excellent. It can not only be applied to the encryption and transmission of real-time images but also be widely used in other fields of information security.
| Tests                        | P-value  | Results |
|-----------------------------|----------|---------|
| Frequency test              | 0.441300 | Pass    |
| Block Frequency test        | 0.810465 | Pass    |
| Cusum-forward test          | 0.387693 | Pass    |
| Cusum-reverse test          | 0.832407 | Pass    |
| Runs test                   | 0.290305 | Pass    |
| Longest run test            | 0.644892 | Pass    |
| Rank test                   | 0.908125 | Pass    |
| FFT test                    | 0.720427 | Pass    |
| Non-Overlapping template test | 0.546890 | Pass  |
| Overlapping template test   | 0.577412 | Pass    |
| Universal test              | 0.911848 | Pass    |
| Approximate entropy test    | 0.276530 | Pass    |
| Random-excursions test (x = -1) | 0.672039 | Pass  |
| Random-excursions variant test (x = 1) | 0.643912 | Pass  |
| Serial1 test                | 0.380598 | Pass    |
| Serial2 test                | 0.117241 | Pass    |
| Linear complexity test      | 0.633098 | Pass    |

Table 7. Comparison of the key space with other referenced schemes.

References

1. Jiang, Z. A note on chaotic secure communication systems. *IEEE Trans. Circuits Syst. I* **49**, 92–96, DOI: https://doi.org/10.1109/81.974882 (2002).
2. Fan, C. & Ding, Q. Analysing the dynamics of digital chaotic maps via a new period search algorithm. *Nonlinear Dyn.* **97**, 831–841, DOI: https://doi.org/10.1007/s11071-019-05015-4 (2019).
3. Li, W., Yan, W., Zhang, R., Wang, C. & Ding, Q. A new 3D discrete hyperchaotic system and its application in secure transmission. *Int. J. Bifurc. & Chaos* **29**, DOI: https://doi.org/10.1142/S0218127419502067 (2019).
4. Kocarev, L. Chaos-based cryptography: A brief overview. *IEEE Circ. Syst. Mag.* **1**, 6–21, DOI: https://doi.org/10.1109/7384.963463 (2001).
5. Ramli, K., Suryanto, Y., Magfirawaty & Hayati, N. Novel image encryption using a pseudoset generated by chaotic permutation multicircular shrinking with a gradual deletion of the input set. *IEEE Access* **8**, 110351–110361, DOI: https://doi.org/10.1109/ACCESS.2020.3001949 (2020).
6. Özkaynak, F. Brief review on application of nonlinear dynamics in image encryption. *Nonlinear Dyn.* **92**, 305–313, DOI: https://doi.org/10.1007/s11071-018-4056-x (2018).
7. Musanna, F. & Kumar, S. Image encryption using quantum 3-D baker map and generalized gray code coupled with fractional chen’s chaotic system. *Quantum Inf. Process.* **19**, 1–31, DOI: https://doi.org/10.1007/s11128-020-02724-3 (2020).
8. Wang, X., Wang, X., Zhao, J. & Zhang, Z. Chaotic encryption algorithm based on alternant of stream cipher and block cipher. *Nonlinear Dyn.* **63**, 587–597, DOI: https://doi.org/10.1007/s11071-010-9821-4 (2011).
9. Chen, G., Mao, Y. & Chui, C. K. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos Soliton. Fract.* **21**, 749–761, DOI: https://doi.org/10.1016/j.chaos.2003.12.022 (2004).
10. Zhu, C. & Ouyang, W. A new image encryption algorithm based on general Chen’s chaotic system. *J. Cent. South Univ. (Science Technol.)* **37**, 1142–1148, DOI: https://doi.org/10.1016/j.physleta.2007.07.040 (2006).
11. Pak, C. & Huang, L. A new color image encryption using combination of the 1D chaotic map. *Signal Process.* **138**, 129–137, DOI: https://doi.org/10.1016/j.sigpro.2017.03.011 (2017).
12. Belazi, A., El-Latif, A. A. A. & Belghith, S. A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Process.* **128**, 155–170, DOI: https://doi.org/10.1016/j.sigpro.2016.03.021 (2016).

13. Liang, H. R., Tao, X. Y. & Zhou, N. R. Quantum image encryption based on generalized affine transform and logistic map. *Quantum Inf. Process.* **15**, 2701–2724, DOI: https://doi.org/10.1007/s11128-016-1304-1 (2016).

14. Huang, X. & Ye, G. An image encryption algorithm based on irregular wave representation. *Multimed. Tools & Appl.* **77**, 2611–2628, DOI: https://doi.org/10.1007/s11242-017-4455-x (2018).

15. Broumandnia, A. The 3D modular chaotic map to digital color image encryption. *Futur. Gener. Comput. Syst.* **99**, 489–499, DOI: https://doi.org/10.1016/j.future.2019.04.005 (2019).

16. Chai, X., Fu, X., Gan, Z., Lu, Y. & Chen, Y. A color image cryptosystem based on dynamic DNA encryption and chaos. *Signal Process.* **155**, 44–62, DOI: https://doi.org/10.1016/j.sigpro.2018.09.029 (2019).

17. Wang X. Z. H. G. K., Zhao Y. A novel color image encryption scheme using alternate chaotic mapping structure. *Opt. Lasers Eng.* **82**, 79–86, DOI: https://doi.org/10.1016/j.optlaseng.2015.12.006 (2016).

18. Fu, C., Chen, Z., Zhao, W. & Jiang, H. A new fast color image encryption scheme using Chen chaotic system. In 2017 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 121–126, DOI: https://doi.org/10.1109/SNPD.2017.8022710 (2017).

19. Sundari, T. J. V. & Karthika, K. Colour image encryption using chaotic mapping. *Res. J. Eng. Technol.* **8**, 301–305, DOI: https://doi.org/10.1016/j.sigpro.2011.10.023 (2017).

20. Kadir, A., Hamdulla, A. & Guo, W. Q. Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN. *Optik - Int. J. for Light. Electron Opt.* **125**, 1671–1675, DOI: https://doi.org/10.1016/j.ijleo.2013.09.040 (2014).

21. Chua, L. O. & Yang, L. Cellular neural networks: theory. In *IEEE International Workshop on Cellular Neural Networks and Their Applications*, vol. 35, 1257–1272, DOI: https://doi.org/10.1109/CNNA.1996.566545 (1988).

22. Döhler, F., Mormann, F., Weber, B., Elger, C. E. & Lehertz, K. A cellular neural network based method for classification of magnetic resonance images: towards an automated detection of hippocampal sclerosis. *J. Neuroence Methods* **170**, 324–331, DOI: https://doi.org/10.1016/j.jneumeth.2008.01.002 (2008).

23. Jamshidi, V. A VLSI majority-logic device based on spin transfer torque mechanism for brain-inspired computing architecture. *IEEE Transactions on Very Large Scale Integration (VLSI) Syst.* **28**, 1858–1866, DOI: https://doi.org/10.1109/TVLSI.2020.2997369 (2020).

24. Ratnavelu, K., Kalpana, M., Balasubramaniam, P., Wong, K. & Raveendran, P. Image encryption method based on chaotic fuzzy cellular neural networks. *Signal Process.* **140**, 87–96, DOI: https://doi.org/10.1016/j.sigpro.2017.05.002 (2017).

25. Jiao, S., Zhou, C., Shi, Y., Zou, W. & Li, X. Review on optical image hiding and watermarking techniques. *Opt. & Laser Technol.* **109**, 370–380, DOI: https://doi.org/10.13140/RG.2.2.33289.34400 (2018).

26. Huang, Q., Zhao, X. & Li, G. Research on the application of video encryption technology based on 7 dimensional CNN hyper chaos. In 2018 10th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), 448–451, DOI: https://doi.org/10.1109/ICMTMA.2018.00115 (2018).

27. Wang, J., Long, F. & Ou, W. CNN-based color image encryption algorithm using DNA sequence operations. In 2017 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC), 730–736, DOI: https://doi.org/10.1109/SPAC.2017.8304370 (2017).

28. Wang, Y., Zhao, Y., Zhou, Q. & Lin, Z. Image encryption using partitioned cellular automata. *Neurocomputing* **275**, 1318–1332, DOI: https://doi.org/10.1016/j.neucom.2017.09.068 (2018).

29. Qing, D., Xiao, S. & Fang, Y. Hyperchaos in a simple CNN. *Int. J. Bifurc. & Chaos* **16**, 2453–2457, DOI: https://doi.org/10.1142/S0218127406016197 (Aug, 2006).

30. Peng, J., Zhang, D. & Liao, X. A digital image encryption algorithm based on hyper-chaotic cellular neural network. *Fundamenta Informaticae* **90**, 269–282, DOI: https://doi.org/10.3233/FL-2009-0018 (2009).

31. Kadir, A., Hamdulla, A. & Guo, W. Q. Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN. *Optik - Int. J. for Light. Electron Opt.* **125**, 1671–1675, DOI: https://doi.org/10.1016/j.ijleo.2013.09.040 (2014).

32. Li, J., Bai, F. & Di, X. New color image encryption algorithm based on compound chaos mapping and hyperchaotic cellular neural network. *J. Electron. Imaging* **22**, 3036, DOI: https://doi.org/10.1117/1.JEI.22.1.013036 (2013).

33. Suykens, J. A. K. & Chua, L. O. n-double scroll hypercubes in 1-D CNNs. *Int. J. Bifurc. & Chaos* **7**, 1873–1885, DOI: https://doi.org/10.1142/S021812749700145X (1997).
34. Yen, J. C. & Guo, J. I. A new image encryption algorithm and its VLSI architecture. In IEEE Workshop on Signal Processing Systems. 430–437, DOI: https://doi.org/10.1109/SIPS.1999.822348 (1999).

35. Wang, X., Xu, B. & Zhang, H. A multi-ary number communication system based on hyperchaotic system of 6th-order cellular neural network. Commun. Nonlinear Sci. Numer. Simul. 15, 124–133, DOI: https://doi.org/10.1016/j.cnsns.2009.03.035 (2010).

36. Koçak, H. & Palmer, K. Lyapunov exponents and stability in interval maps. Semin J. 51, 79–82, DOI: https://doi.org/10.1007/BF03322557 (2010).

37. Chen, G. & Ueta, T. Yet another chaotic attractor. Int. J. Bifurc. & Chaos 9, 1465–1466, DOI: https://doi.org/10.1142/S0218127499001024 (1999).

38. Zhou, T., Yun, T. & Chen, G. Complex dynamical behaviors of the chaotic Chen’s system. Int. J. Bifurc. & Chaos 13, 2561–2574, DOI: https://doi.org/10.1142/S0218127403008089 (2003).

39. Zhu, C. & Sun, K. Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic Tent maps. IEEE Access 6, 18759–18770, DOI: https://doi.org/10.1109/ACCESS.2018.2817600 (2018).

40. Liu, L., Jiang, D., An, T. & Guan, Y. A plaintext-related dynamical image encryption algorithm based on permutation-combination-diffusion architecture. IEEE Access 8, 62785–62799, DOI: https://doi.org/10.1109/ACCESS.2020.2983716 (2020).

41. Shannon, C. E. Communication theory of secrecy systems. Bell Syst. Tech. J. 28, 656–715, DOI: https://doi.org/10.1002/j.1538-7305.1949.tb00928.x (1949).

42. Wei, X., Ling, G., Qiang, Z., Zhang, J. & Lian, S. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. J. Syst. Softw. 85, 290–299, DOI: https://doi.org/10.1016/j.jss.2011.08.017 (2014).

43. Tong, X. et al. A fast encryption algorithm of color image based on four-dimensional chaotic system. J. Vis. Commun. & Image Represent. 33, 219–234, DOI: https://doi.org/10.1016/j.jvcir.2015.09.014 (2015).

44. Nestor, T., Dieu, N. J. D., Jacques, K., Yves, E. J. & El-Latif, A. A. A. A multidimensional hyperjerk oscillator: Dynamics analysis, analogue and embedded systems implementation, and its application as a cryptosystem. Sensors 20, 83, DOI: https://doi.org/10.3390/s20010083 (2019).

45. Nestor, T., Kengne, J., Abd-El-Atty, B., Iliyasu, A. M. & El-Latif, A. A. A. Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption. Sensors 20, 83, DOI: https://doi.org/10.3390/s20010083 (2019).

46. Zhou, R. G., Sun, Y. J. & Fan, P. Quantum image gray-code and bit-plane scrambling. Quantum Inf. Process. 14, 1717–1734, DOI: https://doi.org/10.1007/s11128-015-0964-6 (2015).

47. Deng, J. et al. Image compression-encryption scheme combining 2D compressive sensing with discrete fractional random transform. Multimed. Tools & Appl. 76, 1–21, DOI: https://doi.org/10.1007/s11042-016-3600-2 (2017).

48. Wu, X., Wang, K., Wang, X., Kan, H. & Kurths, J. Color image DNA encryption using NCA map-based CML and one-time keys. Signal Process. The Off. Publ. Eur. Assoc. for Signal Process. (EURASIP) 148, 272–287, DOI: https://doi.org/10.1016/j.sigpro.2018.02.028 (2018).

49. Liu, L. & Miao, S. An image encryption algorithm based on baker map with varying parameter. Multimed. Tools & Appl. 76, 16511–16527, DOI: https://doi.org/10.1007/s11042-016-3925-x (2017).

Acknowledgements
This work was supported in part by the National Natural Science Foundation of China under Grant 61471158.

Author contributions
Q.D. provided ideas, design solutions, and the division of labor throughout the project. R.Z. conceived the experiments and wrote the main manuscript text and code. L.Y. participated in part of the experiments. D.J. supplemented the experiments based on previous work. W.D. is responsible for preparing image materials, experimental testing, and collating experimental data. J.S. and K.H. polished the language and modified the manuscript. All authors reviewed the manuscript.

Competing interests
The authors declare no competing interests.