Article

A Novel Plaintext-Related Color Image Encryption Scheme Based on Cellular Neural Network and Chen's Chaotic System

Renxiu Zhang ¹ , Longfei Yu ¹, Donghua Jiang ² , Wei Ding ¹, Jian Song ¹, Kuncheng He ¹ and Qun Ding ^{1,*}

¹ Electronic Engineering College, Heilongjiang University, Harbin 150080, China; 2191297@s.hljy.edu.cn (R.Z.); 2181222@s.hljy.edu.cn (L.Y.); 2191266@s.hljy.edu.cn (W.D.); 2191351@s.hljy.edu.cn (J.S.); 2191359@s.hljy.edu.cn (K.H.)

² School of Information Engineering, Chang'an University, Xi'an 710064, China; jiangdonghua@chd.edu.cn

* Correspondence: 1984008@s.hljy.edu.cn

Abstract: To address the problem that traditional stream ciphers are not sensitive to changes in the plaintext, a novel plaintext-related color image encryption scheme is proposed in this paper, which combines the 6-dimensional cellular neural network (CNN) and Chen's chaotic system. This encryption scheme belongs to symmetric cryptography. In the proposed scheme, the initial key and switching function generated by the plaintext image are first utilized to control the CNN to complete the scrambling process. Then, Chen's chaotic system is used to diffuse the scrambled image for realizing higher security. Finally, extensive performance evaluation is undertaken to validate the proposed scheme's ability to offer the necessary security. Furthermore, the scheme is compared alongside state-of-the-art algorithms to establish its efficiency.

Keywords: image encryption; symmetric cryptography; cellular neural network; chaotic system

Citation: Zhang, R.; Yu, L.; Jiang, D.; Ding, W.; Song, J.; He, K.; Ding, Q. A Novel Plaintext-Related Color Image Encryption Scheme Based on Cellular Neural Network and Chen's Chaotic System. *Symmetry* **2021**, *13*, 393. <https://doi.org/10.3390/sym13030393>

Academic Editor: Juan Alberto Rodríguez Velázquez

Received: 9 February 2021

Accepted: 24 February 2021

Published: 28 February 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The Internet's impact on society is increasing due to the explosive development of information technology. A large amount of information is transmitted on the network by short messages, videos, images, audio, etc. Especially, the continuous update of electronic equipment makes the transmission of images on the network increasingly more convenient. Nevertheless, some of the images spreading across networks that are widely used in various communication systems such as telemedicine, military imaging, and video conferencing are secret, and the owner does not want others to access them without authorization. Thus, it is extremely important to protect the contents of these secret images.

The chaotic signal is suitable for secure communication technology because of its long-term unpredictability, initial value sensitivity, and noise-like [1,2]. Moreover, the chaos-based algorithms show outstanding characteristics in terms of security, complexity, speed, and computing power [3,4]. In recent years, the research of chaotic cryptography on image encryption has received a lot of attention from scholars [5–9]. For instance, on the basis of the permutation-substitution, an image encryption algorithm is presented in [10]. Meanwhile, Wang et al. [11] presented an encryption algorithm of images that uses the 1-dimensional and 2-dimensional logistic map to generate the chaotic matrix. Moreover, the 1-dimensional and 2-dimensional chaotic maps are repeatedly replaced in sequence. The results of the experiment demonstrate the reliability and applicability of the algorithm. Further, in [12] a pseudorandom number generator (PRNG) is generated using the 2-dimensional Logistic map to control the confusion and diffusion of pixels by XOR operation. Broumandnia [13] generates an incoherent cryptographic image by harnessing modular chaotic maps, which hides the information of original images. Then, Chai et al. [14] proposed a dynamic DNA and chaos-based encryption scheme for images and calculated initial values by using the hash function and extrinsic parameters. Moreover, Sundari and Karthika [15] presented an image encryption method associated with 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 performance [16].

CNN is a nonlinear analog processor with locally interconnected, double-valued output signals [17]. It is an artificial neural network formed by the improvement of Hopfield neural network and cellular automata [18], 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) [19]. Compared with traditional chaotic systems, CNN has more extensive key space and outstanding permutation and diffusion properties. Therefore, CNN is widely utilized in encryption systems [20], and has achieved good encryption effects on digital watermark technology [21], voice encryption [22], and image encryption [23]. For example, Wang et al. [24] proposed the use of cellular automata (CA) to deal with the problems that match parallel computing. Furthermore, Qing et al. [25] analyzed the chaotic phenomenon of CNN model, then Peng et al. [26] conceived an encryption scheme for the image based on the theoretical model in [25]. Further, on the basis of the “scrambling-diffusion” mechanism, Kadir et al. [16] applied the CNN hyperchaotic system to construct the diffusion sequence to encrypt images. Meanwhile, a color image cryptography system based on hyperchaotic CNN and chaotic control parameter was proposed in [27], which adopted the compound “scrambling-diffusion” framework to encrypt the color image.

To overcome the shortcoming of traditional stream ciphers that is insensitive to the changes in the plaintext and further improve the security of the image encryption algorithm, obtain a larger key space, and better unpredictability, this paper proposes a new plaintext-related color image encryption scheme based on a 6-dimensional CNN and Chen’s chaotic system. First, the plaintext image is utilized to generate the initial key that is used as initial values of CNN, and the switching key is then utilized to select the chaotic sequences. Finally, the selected chaotic sequences are used in the two stages of scrambling and diffusion, respectively, to complete the image encryption. Consequently, 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 contributes to obtaining unique keystreams for each image, which ensures that the encryption scheme proposed in this paper is sufficiently sensitive to plaintext and has the advantages of resisting the known-plaintext attacks and chosen-plaintext attacks effectively. Additionally, the proposed scheme adopts a 6-dimensional CNN hyperchaotic system, which greatly expands the key space and makes it sufficient to resist the brute force attack. Extensive experimental results including histogram, correlation of adjacent pixels, entropy, sensitivity, key space, robustness, randomness, and known- and chosen-plaintext attacks show that the presented scheme meets the security requirements of the encryption algorithm and has a satisfactory encryption effect.

Based on the aforementioned, the main contributions of this study are threefold: (i) the proposed scheme that combines CNN with a high-dimensional chaotic system manifests higher security than the traditional encryption scheme based on a single chaotic system. (ii) We exploit the original image to generate one-time-key streams, which could be equated to signatures reflecting the respective pixel states of each input image. This enhances the sensitivity of both the input images and secret keys to small alterations to their respective contents, which helps to disable known or chosen plaintext attacks and overcomes the shortcomings of traditional stream ciphers that are not sensitive to changes in the plaintext. (iii) We utilize the 6-dimensional CNN hyperchaotic system, which increases the key space greatly and makes the scheme sufficient to resist various brute force attacks.

The rest of the paper is organized as follows. Section 2 briefly introduces the preliminaries related to the proposed encryption scheme, including the mathematical model and

chaotic characteristics of the CNN and Chen's chaotic system. Section 3 explains the design of the cryptosystem and the application of the proposed encryption scheme on the color image. The experimental results and security analysis are presented in Section 4. Finally, the conclusions are drawn in Section 5.

2. Preliminaries

2.1. Cellular Neural Network

The cell is the basic component unit of CNN. Besides, each cell can be equivalent to a nonlinear 1-order circuit as shown in Figure 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 eight neurons and the cells that are not directly connected influence each other through continuous and dynamic propagation effect [28]. Each neuron has the input and output states. A 3×3 CNN is constructed in Figure 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 [29]. The state equation of the 6-order fully interconnected CNN is shown in Equation (1):

$$\frac{dx_i}{dt} = -x_j + a_j p_j + \sum_{\substack{k=1 \\ k \neq j}}^6 a_{jk} p_k + \sum_{k=1}^6 s_{jk} x_k + i_j, \quad (1)$$

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

Figure 1. Cellular neural network structure of 3×3 .

Figure 2. Equivalent circuit diagram of each cell.

The system is in a chaotic state when the parameters are set as follows [30]: $a_j = 0$ ($j = 1, 2, 3, 5, 6$), $a_4 = 200$; $a_{jk} = 0$ ($j, k = 1, 2, \dots, 6; j \neq k$); $S_{12} = S_{23} = S_{33} = S_{51} = 1$, $S_{13} = S_{14} = -1$, $S_{22} = 3$, $S_{31} = 14$, $S_{32} = -14$, $S_{41} = S_{62} = 100$, $S_{44} = -99$, $S_{52} = 18$, $S_{65} = 4$, $S_{66} = -3$. The mathematical model of 6-order CNN is shown in Equation (2), which can be obtained by substituting the parameters into Equation (1).

$$\begin{cases} \dot{x}_1 = -x_3 - x_4 \\ \dot{x}_2 = 2x_2 + x_3 \\ \dot{x}_3 = 14x_1 - 14x_2 \\ \dot{x}_4 = 100x_1 - 100x_4 + 200p_4 \\ \dot{x}_5 = 18x_2 + x_1 - x_5 \\ \dot{x}_6 = 4x_5 - 4x_6 + 100x_2 \end{cases} \quad (2)$$

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

The Lyapunov exponent of the 6-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 $t \rightarrow \infty$. Two of them are positive, which indicates that the system is hyperchaotic [31]. As 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 6-order CNN hyperchaotic attractor obtained by Runge–Kutta method is plotted in Figure 3.

Figure 3. Partial 6-order CNN hyperchaotic attractor distribution: (a) Distribution in the direction of x_3 - x_6 - x_4 . (b) Distribution in the direction of x_1 - x_3 - x_4 . (c) Distribution in the direction of x_5 - x_4 - x_3 . (d) Distribution in the direction of x_2 - x_4 - x_6 . (e) Distribution in the direction of x_2 - x_3 - x_4 . (f) Distribution in the direction of x_4 - x_5 - x_6 . (g) Distribution in the direction of x_1 - x_3 - x_5 . (h) Distribution in the direction of x_1 - x_2 - x_3 .

2.2. Chen's Chaotic System

In 1999, the authors of [32] discovered a system with more complex dynamic behaviors than Lorenz system when studying chaotic feedback control. The chaotic attractors of Chen's system had more complex and abundant dynamic characteristics than that of Lorenz system. The mathematical model of Chen's chaotic system is expressed as

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = (c - a)x - xz + cy \\ \dot{z} = xy - bz \end{cases} \quad (3)$$

where a , b , and c are system parameters, when $a = 35$, $b = 3$, and $c = 28$, the system is in a chaotic state [33]. The 4-order Runge–Kutta algorithm is used to calculate Equation (3). The initial parameters are set as $x(0) = 0.1$, $y(0) = 0.2$, $z(0) = 0.3$, and step length $h = 0.001$, and 100,000 iterations are performed. The chaotic attractors of this system are obtained as shown in Figure 4.

Figure 4. Chaotic attractors of Chen's system: (a) Distribution in the direction of x - y - z . (b) Distribution in the direction of x - y . (c) Distribution in the direction of y - z . (d) Distribution in the direction of x - z .

3. Encryption and Decryption on Color Images

Having outlined CNN and Chen's chaotic system and established their superior properties, in this part, we outline the design process of the proposed plaintext-related color image encryption scheme, which is based on the classical "Scrambling-Diffusion" framework. For the sake of generality, it is assumed that the plaintext image **PI** with the size of $M \times N$. In addition, the ciphertext image is **CI** with the size of $M \times N$. The specific encryption steps and corresponding decryption steps are shown below.

3.1. Key Generation

Key generation is defined as the process of generating keys used in cryptography. In this study, key generation includes two parts: the initial key and the switching key. Outcomes of them depend on the plaintext, which leads to a unique key for each different output.

3.1.1. Initial Key

Initial key is inputted into the CNN hyperchaotic system as initial values, which is an integral part of the initial conditions for generating chaotic sequences. As shown in Figure 5, a three-channel color plaintext image with the size of $M \times N$ is converted into a single-channel grayscale image, it is then divided into six 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 $m = (M - M \bmod 3)/3$, $n = (N - N \bmod 2)/2$, $m_1 = M - 2 \times m$, and $n_1 = N - n$. We calculate the sum of gray values of each cell, respectively, and record them as $sum1$, $sum2$, ..., $sum6$, then let $k_1, k_2, \dots, k_6$ denote their sine values. That is, the initial key is dynamically updated by means of the sine values of the sum of the pixels of an image. Thus, one-time chaotic sequences are produced for the image, which results in high sensitivity to the slightest alternations in the corresponding input image. This is a veritable property for good immunity against chosen or known-plaintext attacks.

Figure 5. Key generation.

3.1.2. Switching Key

The function of switching key d in Figure 5 is to control the selection of dimensions. In the process of confusion, 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 Figure 6, when the extracted eigenvalue d is 1, the switch K_1 is closed, that is, the first dimensional chaotic sequence D_1 is selected. Moreover, 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 image and transcode it to an integer within the range of 1 to 6 according to Equation (4).

$$d = \text{mod}(\text{fix}(a), 6) + 1. \quad (4)$$

Figure 6. Flow chart of encryption scheme.

3.2. Encryption Scheme Design

3.2.1. Scrambling

Input the initial key and control parameters into the CNN hyperchaotic system. Meanwhile, enter the switching key d which is used to select a sequence by controlling the switch K_1 – K_6 on or off. Then, one sequence is selected from the generated 6-dimensional chaotic sequences. Discard the first 1000 elements of the selected sequence to conceal the transient effect and then extract the remaining $M \times N$ elements. These elements are quantified according to Equation (5) and denoted as the sequence S .

$$SQ = \text{mod}(\text{mod}(\text{abs}(S) \times 1000, 1000), 256). \quad (5)$$

Equation (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 2-D matrix, and elements in the 2-D matrix are traversed according to columns. After incremental sorting, the elements are put into a new empty matrix by columns, namely, the sorted chaotic matrix SCS . Additionally, 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 and the scrambling transformation is completed. To better understand the proposed scrambling algorithm, an example of the scrambling process is demonstrated in Figure 7, where $M = 3, N = 4$. Figure 7a,b represents 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 Figure 7c. The matrix ICS is used to scramble the plaintext matrix in Figure 7d. Ultimately, the resulting scrambled matrix is displayed in Figure 7e.

Figure 7. An example of a scrambling algorithm: (a) The 2D chaotic matrix. (b) The sorted chaotic matrix. (c) The position matrix. (d) The plaintext matrix. (e) The scrambled plaintext matrix.

3.2.2. Diffusion

The 501st to 503rd values of the sequence selected in the scrambling process are taken as the initial values denoted as x_1, x_2, x_3 of Chen's chaotic system. They are inputted into Chen's system, and the 4-order Runge–Kutta method was utilized to solve Chen's system

iteratively for $M \times N$ times. Then, the generated chaotic sequences C_1, C_2, C_3 are converted according to Equation (6).

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

where $n = 1, 2, \dots, M \times N$.

That is, the mean of three sequences is calculated and defined as the new sequence C . Then, the sequence C is quantified according to Equation (5). The quantized data is constructed as a diffusion matrix DM , whose size is $M \times N$. The XOR operations are performed on it and the three components of the scrambled image SI , respectively. Moreover, the ciphertext image CI in the form of RGB will be obtained after integration.

3.3. Decryption Scheme Design

3.3.1. First Decryption

Input the initial key, control parameters, and switching key d into the CNN hyperchaotic system. Following that, extract $M \times N$ 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 chaotic system. The initial values x_1, x_2 , and 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 respectively XOR the diffusion matrix DM with the three channels of the ciphertext image CI . The first stage of the decryption process is completed after integration, and the scrambled image SI is obtained.

3.3.2. Second Decryption (Reverse Scrambling)

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

3.4. Step to Encrypt and Decrypt Color Images

3.4.1. Steps to Encrypt

- Step 1: Initial keys $k_1, k_2, \dots, k_6$, 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: Input the initial values x_1, x_2, x_3 into Chen's chaotic 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.

Figure 6 shows the whole encryption process. Furthermore, as part of our validation, Figure 8a is the original plaintext image, the scrambled image is shown in Figure 8b, and Figure 8c shows the encryption effect. 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 can cover up the original image successfully.

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.

3.4.2. Steps to Decrypt

- Step 1: Initial keys $k_1, k_2, \dots, k_6$; 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.
- Step 3: The position matrix **ICS** in step1 is carried out the inverse scrambling on the RGB component of the scrambled image **SI**. Integrate it into the RGB form, the second stage of decryption process is completed.

The decryption effect is shown in Figure 8d. As seen throughout that figure, there is almost no visual difference between the decrypted image and the original plaintext image, indicating that the proposed scheme can successfully decrypt color images.

4. Experimental Results and Security Analysis

In this part, we conduct simulation tests to evaluate the quality of the proposed scheme. All simulation tests are carried out in the experimental environment of Matlab R2015b with a 2.90GHz CPU and 8GB memory.

4.1. Histogram Analysis

The histogram is one of the indexes to measure the quality 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 Figure 9. It can be intuitively observed that the distributions of original images are uneven before encryption, that is,

there is a significant difference in the probability of grayscale. Whereas, the histogram of the cipher image provides a uniform distribution, which enhances the difficulty of decryption. The outcome is evidence of our proposed scheme's strong resistance against statistical attacks.

Figure 9. Histogram tests: (a) The plaintext image. (b) Histogram for RGB components of the plaintext image. (c) The ciphertext image. (d) Histogram for RGB components of ciphertext image.

4.2. Correlation of Adjacent Pixels

The distinct correlation between adjacent pixels is the important features of images. Generally, attackers use it to decipher the ciphertext image. Therefore, making adjacent pixels uncorrelated is important in curtailing such efforts. The correlation should be extremely low (close to 0) in the encrypted image, a property that helps to make it unpredictable and disparate from the corresponding original image. In other words, the encryption scheme is considered to be effective if the information of cipher images cannot be obtained through adjoining pixels. Mathematically, the correlation calculation formula of adjoining pixels is as follows [34].

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i, \quad (7)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2, \quad (8)$$

$$\text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)), \quad (9)$$

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)D(y)}}, \quad (10)$$

where x and y are the gray values of two adjoining pixels in an image, $\text{cov}(x, y)$ represents the covariance, $D(x)$ represents the variance of the variable x , and $E(x)$ represents the expectation of variable x . The pixel distribution of plaintext image and cipher image in R, G, and B components of the scheme presented in this paper is shown in Figure 10. As can be observed from the figure, the adjoining pixels of the plaintext image are concentrated in the diagonal region, which is closely related, whereas the encrypted image pixels are distributed in the full region irregularly, which explains why the correlation of the cipher image has been effectively reduced. Table 1 describes the correlation between the three components of the plaintext image and the ciphertext image in the horizontal, vertical, and diagonal directions. These outcomes show that the two adjacent pixels in the plaintext image are highly correlated, whereas the correlation tends to zero in the encrypted image. Table 2 shows the correlation comparison between the scheme proposed in this paper and the scheme proposed in other references. It can be observed 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. As a result, it can be concluded that our scheme is security and free from statistical attacks.

Figure 10. Distribution of pixels: (a) Original image distribution of horizontal. (b) Cipher image distribution of horizontal. (c) Original image distribution of vertical. (d) Cipher image distribution of vertical. (e) Original image distribution of diagonal. (f) Cipher image distribution of diagonal.

Table 1. Correlation of adjoining pixels of the original plaintext image and the encrypted ciphertext image.

Image	Horizontal			R	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	

Table 2. Comparison of the correlation of the encrypted Lena image with other referenced schemes.

Scheme	Horizontal	Vertical	Diagonal
Ours	0.0076	−0.0125	0.0101
Reference [35]	0.0076	0.0130	0.0138
Reference [26]	0.0445	−0.0168	−0.0022
Reference [27]	0.0195	0.0086	−0.0260
Reference [10]	0.0113	0.0173	0.0099
Reference [36]	0.1410	0.1967	0.1116
Reference [12]	0.0172	0.0039	0.0277
Reference [37]	−0.0909	0.2389	0.0126

4.3. Information Entropy

Information entropy is utilized to quantitatively evaluate the randomness of random variables, which is defined in Equation (11).

$$H(s) = - \sum_{i=0}^L P(m_i) \log_2 p(m_i), \quad (11)$$

where m_i is the i -th grayscale value of the L -level grayscale image. Information entropy measures the distribution of grayscale values in an image. When the entropy values tend to 8, the pixel values are evenly distributed, and the password is not vulnerable to statistical attacks [26]. Therefore, an effective encryption scheme should introduce enough randomness in the image so that its entropy tends to the theoretical value of 8. The entropy values of original plaintext images and the encrypted ciphertext images in the three components are, respectively, calculated as shown in Table 3, which are very close to the optimum value. Consequently, it can be safely concluded that the information leakage from the proposed algorithm is insignificant.

Table 3. Information entropy tests of plaintext images and ciphertext images.

Images	Plaintext Image			Ciphertext Image		
	R	G	B	R	G	B
Lena (512 × 512)	7.2710	7.5310	6.9603	7.9997	7.9937	7.9976
Peppers (512 × 512)	7.3255	7.3912	6.9469	7.9932	7.9824	7.9969
Baboon (512 × 512)	7.6833	7.4466	7.6874	7.9941	7.9701	7.9838
Airplane (512 × 512)	6.9113	6.9853	6.5128	7.9933	7.9742	7.9994
Barbara (787 × 576)	7.7581	7.6078	7.5774	7.9915	7.9730	7.9806

4.4. Sensitivity Analysis

4.4.1. Key Sensitivity

Key sensitivity ensures that even a tiny change in the secret key would completely alter the encrypted and the decrypted images. Figure 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 suggests that the key sensitivity of the proposed scheme is satisfactory.

Figure 11. The test results of the key sensitivity: (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.

4.4.2. Plaintext Sensitivity

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 decode the key. Consequently, a satisfactory encryption scheme should be highly sensitive to alterations in the original images, so as to be resistant to differential attacks effectively [38]. The capability of resisting differential attacks is usually measured by the number of pixel of 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 Equation (12):

$$\text{NPCR} = \frac{\sum_{i=1}^M \sum_{j=1}^N \mathbf{D}(i, j)}{M \times N} \times 100\%, \quad (12)$$

where M and N represent the height and width of a image, and $\mathbf{D}(i, j)$ is the difference value of the pixels corresponding to the two encrypted images $\mathbf{C}_1$ and $\mathbf{C}_2$, which is defined in Equation (13):

$$\mathbf{D}(i, j) = \begin{cases} 1, & \mathbf{c}_1(i, j) \neq \mathbf{c}_2(i, j) \\ 0, & \mathbf{c}_1(i, j) = \mathbf{c}_2(i, j) \end{cases}. \quad (13)$$

The UACI measures the average intensity difference between two different images, which is defined in Equation (14):

$$UACI = \left[\sum_{i=1}^M \sum_{j=1}^N \frac{|c_1(i,j) - c_2(i,j)|}{255} \right] \times \frac{1}{M \times N}. \quad (14)$$

When NPCR reaches approximately 99.6% and UACI reaches approximately 33.4%, the algorithm meets the security criteria [8]. Table 4 presents the NPCR and UACI scores for the proposed scheme and its comparison alongside results reported in other references. Outcomes show that NPCR and UACI scores for the proposed scheme are close to the ideal scores. This performance matches those reported in the competing techniques. Consequently, it can be deduced that the proposed scheme is sensitive to plaintext and has sufficient resistance to differential attacks.

Table 4. The number of pixel of change rate (NPCR) and unified average changing intensity (UACI) of RGB component.

Images	NPCR(%)			UACI(%)		
	R	G	B	R	G	B
Peppers (512×512)	99.6059	99.6124	99.6197	33.4151	33.4492	33.3812
Baboon (512×512)	99.6128	99.5903	99.5781	33.3810	33.4133	33.3467
Airplane (512×512)	99.6166	99.5796	99.6128	33.4021	33.4243	33.3585
Barbara (787×576)	99.6098	99.6042	99.5877	33.4288	33.4573	33.3858
Reference [13]	99.6338	99.6094	99.5795	33.2918	33.6839	33.3533
Reference [14]	99.6000	99.6100	99.6100	33.5600	33.4500	33.4900
Reference [11]	99.6300	99.5900	99.6700	33.4300	33.3900	33.5100
Reference [37]	99.335	-	-	33.600	-	-

4.5. Key Space

Enough key space is an essential condition for resisting brute force attacks. In the scheme of this paper, the key includes the switching key d ranging from 1 to 6 and the initial values $k_1, k_2, \dots, k_6$ generated by the plaintext image; it is declared as double-precision type, and the key space of the encryption scheme is 6×2^{192} . Compared with other references, as shown in Table 5, the key space of the proposed scheme is huge, which is much larger than the theoretical requirement value 2^{128} . Therefore, the proposed scheme has sufficient ability to resist brute force attacks.

Table 5. Comparison of the key space with other referenced schemes.

Scheme	Key Space
Ours	6×2^{192}
Reference [35]	2^{159}
Reference [26]	10^{58}
Reference [27]	10^{56}
Reference [39]	10^{45}
Reference [12]	10^{56}
Reference [40]	2^{128}
Reference [24]	2^{128}
Reference [37]	10^{37}

4.6. Robustness Analysis

Robustness refers to the ability to decrypt the original image when the encrypted image is polluted or attacked by noise during transmission [41]. We added Pepper & Salt

noise and Gaussian noise with different noise densities to the cipher image respectively. The noise-contaminated ciphered images are then decrypted using the same key. The experimental results are shown in Figure 12; it can be seen that the encrypted image with noise can still be decrypted well. Therefore, the scheme is robust to Pepper & Salt noise and Gaussian noise added in ciphertext images.

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 variance value 0.01. (h) Cipher House image with Gaussian white noise with variance value 0.1. (i) Cipher House image with Gaussian white noise with variance value 0.15. (j) Decrypted image from cipher with Gaussian white noise with variance value 0.01. (k) Decrypted image from cipher with Gaussian white noise with variance value 0.1. (l) Decrypted image from cipher with Gaussian white noise with variance value 0.15.

Moreover, 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. The experimental results are shown in Figure 13. It can be

observed that the quality of the reconstructed images is still recognizable and acceptable by cropping a reasonable area, such as 6.25% or 25% of the cipher. Despite a loss rate of 50% in the content of the encrypted image, sufficient visual information is retained in the corresponding decrypted image. Therefore, these outcomes support the conclusion that the scheme proposed has satisfactory robustness.

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.

4.7. Known and Chosen-Plaintext Attacks

Known-plaintext attacks (KPA) are performed when both the original and encrypted images are known to the cryptanalyst. Such foreknowledge equips the attacker to predict some secret information and violate the cipher. In contrast, in the case of a chosen-plaintext attack (CPA), the cryptanalyst encrypts some particular images and examines their encrypted counterparts. Therefore, the attacker tries to recover the secret keys or estimate a process to decrypt the images without access to the keys. In our proposed scheme, the cryptanalyst is unable to acquire any sensitive information regarding the secret key by encrypting some known or particular images because the secret key depends on the input image, i.e., a one-time secret key for each input image. Therefore, the proposed algorithm is capable of withstanding any known and chosen-plaintext attack.

4.8. Randomness Tests Analysis

SP800-22 is a software package containing 16 randomness tests, which is released by the national institute of standards and technology (NIST) [42,43]. The randomness of the data stream is verified by these tests. Therefore, we use SP800-22 to make a qualitative judgment on the randomness of cipher images. The results are shown in Table 6. It can be concluded that the cipher images pass the test successfully through analyzing the data in Table 6. In other words, the cipher images generated by the proposed scheme in this paper have good randomness.

Table 6. Results of randomness tests.

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

5. Conclusions

In this paper, a novel plaintext-related color image encryption scheme based on the combination of the 6-dimensional CNN hyperchaotic system and Chen's system was proposed. Structurally, the proposed scheme is made up of three encryption phases: First, the key generation step that precedes the cryptographic phases is used to provide safeguards needed for the encryption phase. The plaintext image is utilized to extract the initial key. Following that, the initial key is utilized to generate the chaotic sequences. Finally, the selected chaotic sequence is used in the two stages of scrambling and diffusion to complete the image encryption. Here, 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 shortcoming of traditional stream ciphers that are not sensitive to changes in the plaintext. Additionally, the use of the 6-dimensional CNN hyperchaotic system expands the key space greatly and makes the scheme sufficient to resist various brute force attacks. Further, compared with the traditional encryption scheme based on a single chaotic system, combining CNN with a high-dimensional chaotic system can achieve higher security. Extensive experimental analysis including histogram, correlation of adjacent pixels, entropy, sensitivity, key space, robustness, randomness, and known and chosen-plaintext attacks establish the efficacy of the proposed scheme and support the conclusion that the proposed scheme is capable of withstanding targeted attacks aimed at violating its confidentiality and integrity.

Author Contributions: Conceptualization, Q.D.; Data curation, W.D.; Methodology, R.Z. and Q.D.; Software, R.Z. and L.Y.; Validation, L.Y. and D.J.; Writing—original draft, R.Z.; Writing—review and editing, D.J., J.S., and K.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China under Grant 61471158.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

CNN	Cellular Neural Network
UAV	Unmanned Aerial Vehicle
VLSI	Very Large Scale Integration
NPCR	Number of Pixel of Change Rate
PRNG	Pseudorandom Number Generator
UACI	Unified Average Changing Intensity
NIST	National Institute of Standards and Technology
KPA	Known-Plaintext Attack
CPA	Chosen-Plaintext Attack

References

- Jiang, Z. A note on chaotic secure communication systems. *IEEE Trans. Circuits Syst. I Fundam. Theory Appl.* **2002**, *49*, 92–96. [\[CrossRef\]](#)
- Fan, C.; Ding, Q. Analysing the dynamics of digital chaotic maps via a new period search algorithm. *Nonlinear Dyn.* **2019**, *97*, 831–841. [\[CrossRef\]](#)
- 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* **2019**, *29*, 1950206. [\[CrossRef\]](#)
- Kocarev, L. Chaos-based cryptography: A brief overview. *IEEE Circ. Syst. Mag.* **2001**, *1*, 6–21. [\[CrossRef\]](#)
- 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* **2020**, *8*, 110351–110361. [\[CrossRef\]](#)
- Özkaynak, F. Brief review on application of nonlinear dynamics in image encryption. *Nonlinear Dyn.* **2018**, *92*, 305–313. [\[CrossRef\]](#)
- 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.* **2020**, *19*, 1–31. [\[CrossRef\]](#)
- Xingyuan, W.; Le, F.; Hongyu, Z. Fast Image Encryption Algorithm Based on Parallel Computing System. *Inf. Sci.* **2019**, *486*, 340–358.
- Pak, C.; Huang, L. A new color image encryption using combination of the 1D chaotic map. *Signal Process.* **2017**, *138*, 129–137. [\[CrossRef\]](#)
- Belazi, A.; El-Latif, A.A.A.; Belghith, S. A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Process.* **2016**, *128*, 155–170. [\[CrossRef\]](#)
- Wang, X.; Zhao, Y.; Zhang, H.; Guo, K. A novel color image encryption scheme using alternate chaotic mapping structure. *Opt. Lasers Eng.* **2016**, *82*, 79–86. [\[CrossRef\]](#)
- Huang, X.; Ye, G. An image encryption algorithm based on irregular wave representation. *Multimed. Tools Appl.* **2018**, *77*, 2611–2628. [\[CrossRef\]](#)
- Broumandnia, A. The 3D modular chaotic map to digital color image encryption. *Future Gener. Comput. Syst.* **2019**, *99*, 489–499. [\[CrossRef\]](#)
- Chai, X.; Fu, X.; Gan, Z.; Lu, Y.; Chen, Y. A color image cryptosystem based on dynamic DNA encryption and chaos. *Signal Process.* **2019**, *155*, 44–62. [\[CrossRef\]](#)
- Sundari, T.J.V.; Karthika, K. Colour Image Encryption Using Chaotic System. *Res. J. Eng. Technol.* **2017**, *8*, 301–305. [\[CrossRef\]](#)
- 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. Light Electron Opt.* **2014**, *125*, 1671–1675. [\[CrossRef\]](#)
- Chua, L.O.; Yang, L. Cellular neural networks: Theory. *IEEE Trans. Circuits Syst.* **1988**, *35*, 1257–1272. [\[CrossRef\]](#)
- Döhler, F.; Mormann, F.; Weber, B.; Elger, C.E.; Lehnertz, K. A cellular neural network based method for classification of magnetic resonance images: Towards an automated detection of hippocampal sclerosis. *J. Neurosci. Methods* **2008**, *170*, 324–331. [\[CrossRef\]](#)
- Jamshidi, V. A VLSI Majority-Logic Device Based on Spin Transfer Torque Mechanism for Brain-Inspired Computing Architecture. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2020**, *28*, 1858–1866. [\[CrossRef\]](#)
- Ratnavelu, K.; Kalpana, M.; Balasubramaniam, P.; Wong, K.; Raveendran, P. Image Encryption Method based on Chaotic Fuzzy Cellular Neural Networks. *Signal Process.* **2017**, *140*, 87–96. [\[CrossRef\]](#)
- Jiao, S.; Zhou, C.; Shi, Y.; Zou, W.; Li, X. Review on Optical Image Hiding and Watermarking Techniques. *Opt. Laser Technol.* **2018**, *109*, 370–380. [\[CrossRef\]](#)
- Huang, Q.; Zhao, X.; Li, G. Research on the Application of Video Encryption Technology Based on 7 Dimensional CNN Hyper Chaos. In Proceedings of the 2018 10th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), Changsha, China, 10–11 February 2018; pp. 448–451.
- Wang, J.; Long, F.; Ou, W. CNN-based color image encryption algorithm using DNA sequence operations. In Proceedings of the 2017 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC), Shenzhen, China, 15–17 December 2017; pp. 730–736.

24. Wang, Y.; Zhao, Y.; Zhou, Q.; Lin, Z. Image encryption using partitioned cellular automata. *Neurocomputing* **2018**, *275*, 1318–1332. [\[CrossRef\]](#)
25. Qing, D.; Xiao, S.; Fang, Y. Hyperchaos in a simple CNN. *Int. J. Bifurc. Chaos* **2006**, *16*, 2453–2457.
26. Peng, J.; Zhang, D.; Liao, X. A Digital Image Encryption Algorithm Based on Hyper-chaotic Cellular Neural Network. *Fundam. Inform.* **2009**, *90*, 269–282. [\[CrossRef\]](#)
27. Li, J.; Bai, F.; Di, X. New color image encryption algorithm based on compound chaos mapping and hyperchaotic cellular neural network. *J. Electron. Imaging* **2013**, *22*, 3036. [\[CrossRef\]](#)
28. Suykens, J.A.K.; Chua, L.O. n-Double Scroll Hypercubes in 1-D CNNs. *Int. J. Bifurc. Chaos* **1997**, *7*, 1873–1885. [\[CrossRef\]](#)
29. Yen, J.C.; Guo, J.I. A new image encryption algorithm and its VLSI architecture. In Proceedings of the IEEE Workshop on Signal Processing Systems, Taipei, Taiwan, 22 October 1999; pp. 430–437.
30. 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.* **2010**, *15*, 124–133.
31. Koçak, H.; Palmer, K. Lyapunov exponents and stability in interval maps. *Sema J.* **2010**, *51*, 79–82. [\[CrossRef\]](#)
32. Chen, G.; Ueta, T. Yet Another Chaotic Attractor. *Int. J. Bifurc. Chaos* **1999**, *9*, 1465–1466. [\[CrossRef\]](#)
33. Zhou, T.; Yun, T.; Chen, G. Complex Dynamical Behaviors of the Chaotic Chen's System. *Int. J. Bifurc. Chaos* **2003**, *13*, 2561–2574. [\[CrossRef\]](#)
34. Liu, L.; Jiang, D.; An, T.; Guan, Y. A Plaintext-Related Dynamical Image Encryption Algorithm Based on Permutation-Combination-Diffusion Architecture. *IEEE Access* **2020**, *8*, 62785–62799. [\[CrossRef\]](#)
35. Fu, C.; Chen, Z.; Zhao, W.; Jiang, H. A new fast color image encryption scheme using Chen chaotic system. In Proceedings of the 2017 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Kanazawa, Japan, 26–28 June 2017; pp. 121–126.
36. Zhou, R.G.; Sun, Y.J.; Fan, P. Quantum image Gray-code and bit-plane scrambling. *Quantum Inf. Process.* **2015**, *14*, 1717–1734. [\[CrossRef\]](#)
37. Deng, J.; Zhao, S.; Wang, Y.; Wang, L.; Wang, H.; Sha, H. Image compression-encryption scheme combining 2D compressive sensing with discrete fractional random transform. *Multimed. Tools Appl.* **2017**, *76*, 1–21. [\[CrossRef\]](#)
38. 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.* **2014**, *85*, 290–299. [\[CrossRef\]](#)
39. 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. Off. Publ. Eur. Assoc. Signal Process. (EURASIP)* **2018**, *148*, 272–287. [\[CrossRef\]](#)
40. Liu, L.; Miao, S. An image encryption algorithm based on Baker map with varying parameter. *Multimed. Tools Appl.* **2017**, *76*, 16511–16527. [\[CrossRef\]](#)
41. Tong, X.; Zhang, M.; Wang, Z.; Liu, Y.; Xu, H.; Ma, J. A fast encryption algorithm of color image based on four-dimensional chaotic system. *J. Vis. Commun. Image Represent.* **2015**, *33*, 219–234. [\[CrossRef\]](#)
42. 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* **2019**, *20*, 83. [\[CrossRef\]](#) [\[PubMed\]](#)
43. 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. *Inf. Sci.* **2020**, *515*, 191–217.