Research Article

On the Security Analysis of a Hopfield Chaotic Neural Network-Based Image Encryption Algorithm

Yingchun Hu , Simin Yu , and Zeqing Zhang

School of Automation, Guangdong University of Technology, Guangzhou 510006, China

Correspondence should be addressed to Yingchun Hu; 1111704006@mail2.gdut.edu.cn

Received 8 May 2020; Accepted 29 June 2020; Published 30 July 2020

Guest Editor: Shao-Bo He

Copyright © 2020 Yingchun Hu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In this paper, the security analysis of a color image encryption algorithm based on Hopfield chaotic neural network is given. The original chaotic image encryption algorithm includes permutation encryption and diffusion encryption. The result of cryptanalysis shows that the chaotic sequences generated by this algorithm are independent of plaintext image, and there exist equivalent permutation key and equivalent diffusion key. Therefore, according to chosen-plaintext attack, the equivalent diffusion key and the equivalent permutation key can be obtained by choosing two special plaintext images and the corresponding ciphertext images, respectively, and the plaintext image is further recovered from the ciphertext image. Theoretical analysis and numerical simulation experiment results verify the effectiveness of the analytical method. Finally, some improved suggestions for the original encryption algorithm are proposed to promote the security.

1. Introduction

With the rapid development of network technology, the security and privacy protection problems of multimedia information have become a hot subject. In order to promote the security of information transmission, scholars have proposed a large amount of image encryption algorithms based on different mechanisms and theories, such as chaotic map [1–13], neural network [14], DNA [15–18], and so on. The security performance of the image encryption algorithms mainly depends on statistical test indicators, such as key space, histogram, key sensitivity analysis, information entropy, differential attack, and so on. However, statistical test indicator is an essential condition and not a sufficient condition for measuring security presented in [19]; moreover, some of them are proven to be insecure due to their inherent pitfalls [20–30]. Therefore, it is necessary to perform cryptanalysis in order to improve the security of the image encryption algorithms.

In recent years, many image encryption algorithms have been cryptanalyzed by the researchers. For example, in [20], the cryptanalysis of an image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps

(IEC-BPMC) proposed in [1] is given; it is pointed out that IEC-BPMC is insecure against chosen-plaintext attack. In [21], the security analysis of an image chaotic encryption algorithm based on Latin cubes and bit cubes presented in [2] is proposed; it is reported that the generation of Latin cubes is independent of plain image, while in the diffusion stage, when any one bit in the plain image changes, the corresponding number of bits in the cipher image follows the change with obvious regularity. According to chosen-plaintext attack, only a maximum of $2.5 \times \sqrt[3]{w \times h} + 6$ plaintext images are needed to crack the ciphertext images of size $w \times h$ resolution. In [22], according to chosen-ciphertext attack, the security analysis for a self-synchronization and closed-loop feedback-based chaotic stream cipher proposed in [3] is given; it has shown that, under the condition that only one unknown key needs to be deciphered while the remaining keys are all known, most secret keys can be deciphered accurately. In addition, the attack complexity of the proposed method is lower than that of the exhaustive attack. In [23], the security performance for an 8D self-synchronous and feedback-based chaotic stream cipher with low 8 bits of state variables for encryption proposed in [4] is analysed, according to known-plaintext

attack and divide-and-conquer attack, 49 secret keys can be obtained, and an improved chaotic stream cipher is proposed for improving the ability to resist divide-and-conquer attack and chosen-ciphertext attack. According to chosen-plaintext attack, in [24], the security analysis of an image encryption algorithm based on 3D bit matrix permutation presented in [5] is given and proposes some improved suggestions in order to enhance security performance. The cryptanalysis of the image encryption algorithm proposed in [7] is presented in [25]; it is reported that the equivalent secret keys can be obtained by utilizing chosen-plaintext attack and further recover the original plaintext image from the ciphertext image. In [26], the security analysis of an image encryption algorithm based on improved hyper-chaotic sequence presented in [8] is given; it is shown that only 1-pair known plaintext-ciphertext image can crack the original encryption algorithm by using known-plaintext attack. In [27], the cryptanalysis of an image encryption algorithm with one round diffusion structure proposed in [9] is reported to find that the original encryption algorithm has equivalent secret keys, so that it can be deciphered by known-plaintext and chosen-plaintext attack. In [28], it is pointed out that permutation-only encryption structure presented in [10] is insecure against known-plaintext attack and chosen-plaintext attack, respectively; for given image of size MN , the original encryption algorithm is cracked by only using $\lceil \log_L(MN) \rceil$ plaintext-ciphertext images. The image encryption algorithm based on DNA encoding and spatiotemporal chaos is proposed in [15]; nevertheless, it is broken in [29] by using chosen-plaintext attack and chosen-ciphertext attack with lower computation complexity and data complexity, respectively. In [30], the security analysis of an image encryption algorithm based on 2D Henon-Sine map and DNA proposed in [17] is given; it is found that cipher image can be cracked by utilizing chosen-plaintext attack without known keys, and its attack complexity is $O(18)$.

In 2019, a color image encryption algorithm based on Hopfield chaotic neural network (CIEA-HCNN) is given in [14]. CIEA-HCNN adopts permutation encryption-diffusion encryption structure; in the permutation encryption phase, firstly, the parameters of Arnold cat map are generated by chaotic sequence and then Arnold cat map is used to scramble the pixel positions of plaintext image. In the diffusion encryption stage, diffusion matrix is generated by utilizing Hopfield chaotic neural network, and then bitwise XOR operation is performed by using diffusion matrix on the scrambled image to obtain the ciphertext image. Some statistical test results are proposed in CIEA-HCNN, and it is claimed that the encryption algorithm has a higher security performance against various attacks. However, CIEA-HCNN has the following inherent defects from the view of cryptanalysis:

- (1) The chaotic sequences generated by key-streams are independent of plaintext image; for given secret key parameters and the size of the plaintext image, the chaotic sequences remain unchanged regardless of the plaintext image.

- (2) The diffusion encryption structure is too simple, there is no ciphertext feedback mechanism, and there exists equivalent diffusion key. According to chosen-plaintext attack, the equivalent diffusion key is broken by choosing one special plaintext image and its corresponding ciphertext image without known keys.
- (3) The permutation encryption structure is a permutation-only encryption process. After deciphering the diffusion encryption structure, the original encryption algorithm becomes a permutation-only encryption structure; in [28], it is pointed out that permutation-only is insecure and cannot resist chosen-plaintext attack and known-plaintext attack. Moreover, parameters of Arnold cat map generated by chaotic sequence depend solely on the secret keys, and the position $(0, 0)$ is always mapped into itself in Arnold cat map.

According to the above shortcomings, one obtains that CIEA-HCNN is insecure, and it is vulnerable to chosen-plaintext attack or known-plaintext attack. An attacker can successfully crack the original encryption algorithm by using the equivalent diffusion key and the equivalent permutation key without knowing the secret keys.

The rest of the paper is organized as follows. Section 2 briefly introduces CIEA-HCNN under study. Section 3 analyses the security performance of CIEA-HCNN by using chosen-plaintext attack. Section 4 gives the numerical simulation experiments and the suggestions for improvement. Section 5 concludes the paper.

2. Chaotic Encryption Algorithm under Study

In this section, Hopfield chaotic neural network and Staged composite chaotic map proposed in [14] are first given, and then CIEA-HCNN is introduced in detail.

2.1. Hopfield Chaotic Neural Network. In 1982, American physicist Hopfield first proposed Hopfield chaotic neural network given in [31]. It is a fully connected neural network, mainly used providing model of simulation human memory. Simultaneously, Hopfield chaotic neural network is also a feedback neural network, and the output signal of each neuron in the network is usually fed back to itself by using other neurons. The iterative equation of Hopfield chaotic neural network is given by

$$x = -x_i + \sum_{i=1}^3 w_{ij}v_i, \quad (1)$$

$$v_i = \tan h(x_i) = \frac{e^{x_i} - e^{-x_i}}{e^{x_i} + e^{-x_i}}, \quad (2)$$

$$w = \begin{bmatrix} 2 & -1 & 0 \\ 1.7 & 1.71 & 1.1 \\ -2.5 & -2.9 & 0.56 \end{bmatrix}, \quad (3)$$

where state variable $x_i \in [0, 1]$, $i = 1, 2, 3$, $j = 1, 2, 3$, v denotes a hyperbolic tangent function, and w represents a weight matrix.

2.2. Staged Composite Chaotic Map. Staged composite chaotic map is a novel phased chaotic map which combines Logistic map with Tent map, given by

$$x_{n+1} = \begin{cases} 16\mu x_n(0.5 - \mu x_n), & (0 \leq x_n < 0.25), \\ 16\mu(0.5 - x_n)(0.5 - \mu(0.5 - x_n)), & (0.25 \leq x_n < 0.5), \\ 16\mu(x_n - 0.5)(0.5 - \mu(x_n - 0.5)), & (0.5 \leq x_n < 0.75), \\ 16\mu(1 - x_n)(0.5 - \mu(1 - x_n)), & (0.75 \leq x_n < 1), \end{cases} \quad (4)$$

where control parameter $\mu \in [0, 2]$, state variable $x_n \in [0, 1]$, $n = 0, 1, 2, \dots$. The system is chaotic defined by equation (4) when $\mu \in (0.33, 2]$.

2.3. Description of CIEA-HCNN. In [14], CIEA-HCNN consists of secret keys selection, chaotic sequences generation, permutation encryption, and diffusion encryption, as shown in Figure 1, where $x'_1, x'_2, \mu_1, \mu_2, m_0, m_r, m_g, m_b$ are secret key parameters, X, Y, Z, W are chaotic sequences generated by Staged composite chaotic map, α and β are parameters of Arnold cat map, T is a permutation matrix, H_1, H_2, H_3 are sequences generated by Hopfield chaotic neural network, D is a diffusion matrix, P is a color plaintext image, S is a temporary permutation encryption image of P , S' is a permutation encryption image of P , C' is a diffusion encryption image of S' , and C is a ciphertext image corresponding to the plaintext image P ; the detailed encryption principles of CIEA-HCNN are presented as follows:

- (1) Choose secret key parameters. CIEA-HCNN includes eight secret key parameters $x'_1, x'_2, \mu_1, \mu_2, m_0, m_r, m_g, m_b$, where x'_1, x'_2, μ_1, μ_2 are initial values and control parameters of Staged composite chaotic map and m_0, m_r, m_g, m_b are iterative numbers of Staged composite chaotic map.
- (2) Generate chaotic sequences X, Y, Z, W . From equation (4), iterate Staged composite chaotic map m_0 times; one gets the chaotic sequence $X = \{x_1, x_2, \dots, x_{m_0}\}$. Simultaneously, one obtains three chaotic sequences $Y = \{y_1, y_2, \dots, y_{m_r}\}$, $Z = \{z_1, z_2, \dots, z_{m_g}\}$, and $W = \{w_1, w_2, \dots, w_{m_b}\}$. Actually, only four state variables $x_{m_0}, y_{m_r}, z_{m_g}, w_{m_b}$ are used in the following encryption process.
- (3) Encrypt image by the chaotic encryption algorithm. The encryption object of CIEA-HCNN is a color plaintext image of size $M \times N \times 3$ denoted by $P = \{P(i, j, k)\}_{i=1, j=1, k=1}^{M, N, 3}$, where $P \in \{0, 1, \dots, 255\}$ [14], and hereinafter referred to as the plaintext image. The ciphertext image of P is represented by $C = \{C(i, j, k)\}_{i=1, j=1, k=1}^{M, N, 3}$, where $C \in \{0, 1, \dots, 255\}$. Besides, the plaintext image P has Red, Green, and Blue channels; for the sake of convenience of

expression, one simplifies the three channels to R, G, and B channels. The steps for CIEA-HCNN are shown as follows:

Step 1: Permutation Encryption. First, F transform x_{m_0} of the chaotic sequence X ; one obtains control parameters α and β of Arnold cat map, given by

$$\begin{cases} \alpha = \text{floor}(\text{mod}(x_{m_0} \times 2^{24}, N)), \\ \beta = \text{floor}(\text{mod}(\text{mod}(x_{m_0} \times 2^{48}, 2^{24}), N)), \end{cases} \quad (5)$$

where N is the width of the plaintext image P , mod represents a modular operation, and floor rounds a real number to the nearest integer.

In Figure 1, scramble R, G, B channels of P by utilizing Arnold cat map, respectively, and get the corresponding temporary permutation encryption image denoted by $S = \{S(i, j, k)\}_{i=1, j=1, k=1}^{M, N, 3}$; the iterative equation of Arnold cat map is defined as

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{bmatrix} 1 & \alpha \\ \beta & \alpha\beta + 1 \end{bmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \text{mod } N, \quad (6)$$

where (x_n, y_n) and (x_{n+1}, y_{n+1}) represent the before and after coordinate of permutation encryption through using Arnold cat map; moreover, the default number of Arnold cat map iterations is set as 1 [14]. According to Figure 1 and equation (6), one gets

$$T = \begin{bmatrix} 1 & \alpha \\ \beta & \alpha\beta + 1 \end{bmatrix} = \begin{bmatrix} a & b \\ \delta & \varepsilon \end{bmatrix}. \quad (7)$$

Finally, scan R, G, B three channels of S in a raster order from left to right and up to down; one obtains the permutation encryption image $S' = \{S'(k, l)\}_{k=1, l=1}^{3, MN}$ with the size of $3 \times MN$, given by

$$S'(k, l) = \begin{bmatrix} S'(1, 1) & S'(1, 2) & \dots & S'(1, MN) \\ S'(2, 1) & S'(2, 2) & \dots & S'(2, MN) \\ S'(3, 1) & S'(3, 2) & \dots & S'(3, MN) \end{bmatrix}. \quad (8)$$

Step 2: Diffusion Encryption. First, set the chaotic sequences y_{m_r}, z_{m_g} , and w_{m_b} as the initial values of Hopfield chaotic neural network, substitute them into equations (1)-(2), iterate MN times, and get three sequences defined by $H_1(l)_{l=1}^{MN}, H_2(l)_{l=1}^{MN}, H_3(l)_{l=1}^{MN}$. Let $H = \{H(k, l)\}_{k=1, l=1}^{3, MN}$ be equal to $\{H_1(l)_{l=1}^{MN}, H_2(l)_{l=1}^{MN}, H_3(l)_{l=1}^{MN}\}$, such that

$$H(k, l) = \begin{bmatrix} H(1, 1) & H(1, 2) & \dots & H(1, MN) \\ H(2, 1) & H(2, 2) & \dots & H(2, MN) \\ H(3, 1) & H(3, 2) & \dots & H(3, MN) \end{bmatrix}. \quad (9)$$

FIGURE 1: Block diagram of CIEA-HCNN.

Then, $H(k, l)$ is quantified to obtain the diffusion matrix $D = \{D(k, l)\}_{k=1, l=1}^{3, MN}$ given by

$$D(k, l) = \text{mod}(\text{round}((\text{abs}(H(k, l)) - \text{floor}(H(k, l)) \times 10^{14}), 256), \quad (10)$$

where round denotes a round-off function and abs is an absolute value function.

In Figure 1, perform bitwise XOR operation on the permutation encryption image S' by utilizing diffusion matrix D , and then get the temporary ciphertext image $C' = \{C'(k, l)\}_{k=1, l=1}^{3, MN}$ defined as

$$C'(k, l) = D(k, l) \oplus S'(k, l), \quad (11)$$

where notation $\oplus$ denotes a bitwise XOR operation. Finally, convert the temporary ciphertext image C' into the ciphertext image C .

- (4) Decrypt image by using chaotic decryption algorithm. Decryption is the inverse process of encryption. First, convert the ciphertext image C into the temporary ciphertext image C' , then perform bitwise XOR operation by using C' and the diffusion matrix D , and get the permutation encryption image S' . Second, transform S' into the temporary permutation encryption image S . Finally, implement anti-scramble encryption for S by means of Arnold cat map, and further recover the plaintext image P from the encrypted image C .

3. Cryptanalysis

3.1. Preliminary Analysis of CIEA-HCNN. According to Kerckhoff's assumptions [32], one gets that the cryptosystem is open and its security depends solely on the secret keys rather than the cryptosystem itself; that is, the attacker knows everything about the cryptosystem except for the

secret keys. If the cryptosystem cannot resist various attacks, it is insecure. There are generally four common attack types for cryptanalysis given in Table 1 from the hardest to the easiest types. In Table 1, ciphertext-only attack is the hardest type, and chosen-ciphertext attack is the easiest type. The adversary reveals secret keys or the equivalent keys to break the cryptosystem by using the four common attack types listed in Table 1.

According to Figure 1, one obtains that CIEA-HCNN adopts permutation encryption-diffusion encryption structure. First, the diffusion encryption structure of CIEA-HCNN is too simple, and the diffusion matrix D is independent of plaintext image or ciphertext image. Therefore, one gets that CIEA-HCNN has the equivalent diffusion key. According to chosen-plaintext attack, the equivalent diffusion key can be broken by just selecting one pure plaintext image and the corresponding ciphertext image.

After cracking the equivalent diffusion key, CIEA-HCNN is simplified to a permutation-only encryption algorithm. In [28], it is pointed out that permutation-only encryption algorithm is insecure. For given secret key parameters and the size of the plaintext image, the generated chaotic sequences remain unchanged which are unrelated to the plaintext image and the corresponding ciphertext image; therefore, the values of α and β in Arnold cat map are fixed, and further the permutation matrix T also remains unchanged. Indeed, the permutation matrix T is the equivalent permutation key of CIEA-HCNN. An attacker can break the permutation-only encryption algorithm by using the permutation matrix T . In addition, the position $(0, 0)$ is always mapped into itself in Arnold cat map.

According to the above analysis, one gets that the security performance of CIEA-HCNN depends only on the diffusion matrix D and the permutation matrix T ; indeed, it means that the equivalent diffusion key and the equivalent permutation key exist in CIEA-HCNN. The adversary can reveal the equivalent keys by using chosen-plaintext attack and further successfully break the original encryption algorithm. Therefore, the problem of cracking secret key parameters $x'_1, x'_2, \mu_1, \mu_2, m_0, m_r, m_g, m_b$ in the original encryption algorithm can be solved by chosen-plaintext attack

TABLE 1: Four common attack types for cryptanalysis.

Attack types	Available resource
Ciphertext-only attack	The attacker only knows the ciphertext
Known-plaintext attack	The attacker knows any given plaintext and also knows the corresponding ciphertext
Chosen-plaintext attack	The attacker can obtain access to the encryption machinery, choose the plaintext that would be useful for deciphering, and also know the corresponding ciphertext
Chosen-ciphertext attack	The attacker can obtain access to the decryption machinery, choose the ciphertext that would be useful for deciphering, and also know the corresponding plaintext

and transforming it into solving the equivalent diffusion key and the equivalent permutation key. Moreover, according to Figure 1, one obtains the simplified block diagram of CIEA-HCNN, as shown in Figure 2. In Figure 2, ET denotes the equivalent permutation key, and ED represents the equivalent diffusion key.

FIGURE 2: Simplified block diagram of CIEA-HCNN.

3.2. Cracking CIEA-HCNN by Using Chosen-Plaintext Attack. The basic method of cracking the permutation encryption and the diffusion encryption structure shown in Figure 2 is that, according to chosen-plaintext attack, one adopts divide-and-conquer strategy to separate the permutation encryption from the diffusion encryption through choosing the plaintext that would be useful for breaking, on this basis, and further deciphering the equivalent permutation key ET and the equivalent diffusion key ED , respectively. The detailed procedures of cracking the equivalent permutation key ET and the equivalent diffusion key ED are presented as follows.

3.2.1. Deciphering the Equivalent Diffusion Key ED . According to chosen-plaintext attack, choose a full zero image denoted by $P_1 = \{P_1(i, j, k)\}_{i=1, j=1, k=1}^{M, N, 3}$, and get the corresponding ciphertext image defined as $C_1 = \{C_1(i, j, k)\}_{i=1, j=1, k=1}^{M, N, 3}$. Next, using the obtained P_1 and C_1 as known conditions, one further gets the corresponding equivalent diffusion key ED .

The specific approaches for cracking the equivalent diffusion key ED are given as follows.

Step 1. Choose a full zero plaintext image as P_1 , according to chosen-plaintext attack, and get its corresponding ciphertext image as C_1 . From Figure 1, one obtains the temporary ciphertext image $C'_1 = \{C'_1(k, l)\}_{k=1, l=1}^{3, MN}$ corresponding to C_1 .

Step 2. According to equation (11) and Figure 2, one has

$$C'_1(k, l) = S'_1(k, l) \oplus ED(k, l). \quad (12)$$

Since all pixels of P_1 are zero, after performing the permutation encryption operation for P_1 , $\{S'_1(i, j, k)\}_{i=1, j=1, k=1}^{M, N, 3} = \{S'_1(k, l)\}_{k=1, l=1}^{3, MN} = 0$ holds.

Step 3. From equations (11)-(12) with $\{S'_1(k, l)\}_{k=1, l=1}^{3, MN} = 0$, one obtains the equivalent diffusion key ED defined as

$$ED(k, l) = C'_1(k, l). \quad (13)$$

3.2.2. Deciphering the Equivalent Permutation Key ET . After breaking the equivalent diffusion key ED , the original permutation encryption-diffusion encryption structure is simplified to permutation-only encryption structure. Besides, since the original image chaotic encryption algorithm adopts the same permutation matrix to the three channels of the plaintext image, the work of deciphering the equivalent permutation key ET sets the R channel of the plaintext image as an example as follows. First, choose a plaintext image defined as $P_2 = \{P_2(i, j, k)\}_{i=1, j=1, k=1}^{M, N, 3}$, and suppose the pixels of coordinates (i_1, j_1) and (i_2, j_2) in R channel are $P_2(i_1, j_1, 1) = \zeta \neq 0$ and $P_2(i_2, j_2, 1) = \lambda \neq 0$, respectively. Moreover, $(i_1, j_1) \neq (1, 1)$, $(i_2, j_2) \neq (1, 1)$ and $\zeta \neq \lambda$, others are full zero, and let all pixels of G channel and B channel be full zero. One obtains the corresponding ciphertext image described by $C_2 = \{C_2(i, j, k)\}_{i=1, j=1, k=1}^{M, N, 3}$. Then using the obtained P_2 and C_2 as known conditions, one further gets the corresponding equivalent permutation key ET . Note that the equivalent permutation key ET is not affected by the number of Arnold cat map iterations.

The specific steps for cracking the equivalent permutation key ET are presented as follows.

Step 1. According to chosen-plaintext attack, choose one plaintext image as P_2 , and get its ciphertext image defined as C_2 . Then, the temporary ciphertext image as $C'_2 = \{C'_2(k, l)\}_{k=1, l=1}^{3, MN}$ is obtained by using the ciphertext image C_2 .

Step 2. Substitute $\{C'_2(k, l)\}_{k=1, l=1}^{3, MN}$ and $\{ED(k, l)\}_{k=1, l=1}^{3, MN}$ with equation (11); the permutation encryption image denoted as $S'_2 = \{S'_2(k, l)\}_{k=1, l=1}^{3, MN}$ is described by

$$S'_2(k, l) = ED(k, l) \oplus C'_2(k, l). \quad (14)$$

Step 3. Convert the permutation encryption image S'_2 of size $3 \times MN$ into the temporary permutation encryption image $S_2 = \{S_2(i, j, k)\}_{i=1, j=1, k=1}^{M, N, 3}$ of size $M \times N \times 3$, and then compare $S_2(:, :, 1)$ with $P_2(:, :, 1)$ one by one; one gets

$$\begin{cases} P_2(i_1, j_1, 1) = S_2(m_1, n_1, 1) = \zeta, \\ P_2(i_2, j_2, 1) = S_2(m_2, n_2, 1) = \lambda. \end{cases} \quad (15)$$

According to equations (6)-(7), one obtains

$$\begin{bmatrix} m_1 - 1 \\ n_1 - 1 \end{bmatrix} = ET \begin{bmatrix} i_1 - 1 \\ j_1 - 1 \end{bmatrix} \bmod N = \begin{bmatrix} a & b \\ \delta & \varepsilon \end{bmatrix} \begin{bmatrix} i_1 - 1 \\ j_1 - 1 \end{bmatrix} \bmod N, \quad (16)$$

$$\begin{bmatrix} m_2 - 1 \\ n_2 - 1 \end{bmatrix} = ET \begin{bmatrix} i_2 - 1 \\ j_2 - 1 \end{bmatrix} \bmod N = \begin{bmatrix} a & b \\ \delta & \varepsilon \end{bmatrix} \begin{bmatrix} i_2 - 1 \\ j_2 - 1 \end{bmatrix} \bmod N. \quad (17)$$

From equations (16)-(17), one sees that (i_1, j_1) , (i_2, j_2) , (m_1, n_1) , and (m_2, n_2) are given, and only the equivalent permutation key ET is unknown; therefore, one can solve the equation by combining equations (16)-(17), defined as

$$\begin{cases} a = \left[\frac{(m_1 - 1) - b \times (j_1 - 1)}{(i_1 - 1)} \right] \bmod N, \\ b = \left[\frac{(m_2 - 1) \times (i_1 - 1) - (m_1 - 1) \times (i_2 - 1)}{(j_2 - 1) \times (i_1 - 1) - (j_1 - 1) \times (i_2 - 1)} \right] \bmod N, \\ \delta = \left[\frac{(n_1 - 1) - \varepsilon \times (j_1 - 1)}{(i_1 - 1)} \right] \bmod N, \\ \varepsilon = \left[\frac{(n_2 - 1) \times (i_1 - 1) - (n_1 - 1) \times (i_2 - 1)}{(j_2 - 1) \times (i_1 - 1) - (j_1 - 1) \times (i_2 - 1)} \right] \bmod N. \end{cases} \quad (18)$$

According to equation (18), one obtains the equivalent permutation key ET by adopting one special plaintext image and the corresponding ciphertext image.

For the sake of understanding the above analysis, take the plaintext image $P_3 = \{P_3(i, j, k)\}_{i=1, j=1, k=1}^{4, 4, 3}$ of size $4 \times 4 \times 3$ as an example, given by

$$\begin{aligned} P_3(:, :, 1) &= \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \\ P_3(:, :, 2) &= \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \\ P_3(:, :, 3) &= \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \end{aligned} \quad (19)$$

After performing the permutation-only encryption on P_3 , one gets the temporary permutation encryption image denoted by $S_3 = \{S_3(i, j, k)\}_{i=1, j=1, k=1}^{4, 4, 3}$, such that

$$\begin{aligned} S_3(:, :, 1) &= \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \\ S_3(:, :, 2) &= \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \\ S_3(:, :, 3) &= \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \end{aligned} \quad (20)$$

According to equations (19)-(20), one has

$$\begin{cases} (i_1, j_1) = (2, 2), \\ (i_2, j_2) = (2, 3), \\ (m_1, n_1) = (4, 3), \\ (m_2, n_2) = (2, 2). \end{cases} \quad (21)$$

Then substituting equation (21) into equation (18), according to $N = 4$, one obtains $a = 1, b = 2, \delta = 3, \varepsilon = 3$ and further gets the equivalent permutation key ET , defined as

$$ET = \begin{bmatrix} 1 & 2 \\ 3 & 3 \end{bmatrix} \bmod 4. \quad (22)$$

3.2.3. Recover the Plaintext Image by Using the Equivalent Diffusion Key ED and the Equivalent Permutation Key ET . First, convert the ciphertext image C into the temporary ciphertext image C' . According to equation (11) and the equivalent diffusion key ED , the permutation encryption image denoted by S' can be obtained from the temporary ciphertext image C' . Second, convert the permutation encryption image S' into the temporary permutation encryption image denoted by S . Finally, recover the plaintext image defined by P from the ciphertext image C by utilizing the equivalent permutation key ET .

According to the above security analysis, the process of cracking CIEA-HCNN by adopting chosen-plaintext attack is described in Algorithm 1.

4. The Numerical Simulation Experiments for Breaking CIEA-HCNN

In the numerical simulation experiments, color images Lena, Baboon, and Pepper are taken as three examples, where the size of the image is 512×512 . The secret keys are set as $x'_1 = 0.6$, $x'_2 = 0.7$, $\mu_1 = 1.46$, $\mu_2 = 1.5$, $m_0 = 1740$, $m_r = 150$, $m_g = 160$, and $m_b = 180$. The numerical simulation experiments are operated under MATLAB R2017a running on desktop computer with Intel (R) Core (TM) i7-7700 CPU 3.6 GHz, 16 G memory RAM, and 1 TB hard drive; the operation system is Microsoft Windows 7.

4.1. The Experiments for Breaking CIEA-HCNN by Using Chosen-Plaintext Attack. First, according to the analysis in Section 3.2.1, choose a full zero plaintext image of size 512×512 denoted by P_1 and get the corresponding ciphertext image C_1 , as shown in Figures 3(a) and 3(b). Based on equation (12), P_1 and C_1 , one obtains the equivalent diffusion key ED given by

$$ED = \begin{bmatrix} 14 & 22 & 235 & 32 & 251 & \dots & 8 & 204 & 43 & 90 & 27 \\ 113 & 92 & 79 & 61 & 173 & \dots & 179 & 198 & 197 & 13 & 26 \\ 221 & 55 & 122 & 95 & 18 & \dots & 41 & 72 & 103 & 88 & 166 \end{bmatrix}_{3 \times 262144}. \quad (23)$$

Second, according to Section 3.2.1, construct a color image of size 512×512 defined by P_2 , let the pixels of the coordinates (2, 2) and (2, 3) be 1 and 2 in the R channel of the plaintext image P_2 , other pixels are set as 0, and all pixels of the G and B channels are defined as 0, as shown in Figure 4(a). According to chosen-plaintext attack, one can get the corresponding ciphertext image of P_2 denoted by C_2 , as shown in Figure 4(b). Recover the permutation encryption image represented by S'_2 from the ciphertext image C_2 by using the equivalent diffusion key ED , and then convert the permutation encryption image into the temporary permutation encryption image S_2 , as shown in Figure 4(c). Based on equation (15), and comparing P_2 with S_2 , one gets

$$\begin{cases} P_2(2, 2, 1) = S_2(m_1, n_1, 1) = 1, \\ P_2(2, 3, 1) = S_2(m_2, n_2, 1) = 2. \end{cases} \quad (24)$$

According to equations (16)-(18), one obtains the equivalent permutation key ET defined as

$$ET = \begin{bmatrix} 1 & 162 \\ 275 & 7 \end{bmatrix} \bmod(512). \quad (25)$$

Finally, according to Section 3.2.3, the plaintext images of Lena, Baboon, and Pepper with the size of 512×512 are recovered by using the equivalent diffusion key ED and the equivalent permutation key ET ; moreover, in order to verify that the recovered plaintext image is equal to the original plaintext image, performing the bitwise XOR operation on them, one gets a full zero image. The breaking results on CIEA-HCNN with RGB color Lena, Baboon, and Pepper are shown in Figure 5.

4.2. Attack Complexity Analysis. The attack complexity consists of time complexity and data complexity. On the aspect of time complexity, according to chosen-plaintext attack, the cracking time of CIEA-HCNN is 11.164 seconds for the color image with the size of 512×512 , and the encryption time is 5.813 seconds. Moreover, on the aspect of data complexity, given the same size of color image, the data complexity of breaking CIEA-HCNN is $O(1)$. Therefore, the experimental results verify that the attack method is both effective and efficient, meanwhile having lower attack complexity.

4.3. Suggestions for Improvement. According to the security defects of CIEA-HCNN, the suggestions for improvement are given as follows:

- (1) In the permutation encryption structure, one can construct the combination of parameters of Arnold cat map and the characters of plaintext image such as all pixels sum and average and hash value of the plaintext information. One adopts multiple-round permutation encryption based on the encryption efficiency. Simultaneously, one suggests that using different permutation matrix performs the scrambling operation on the three R, G, B channels of the color image, respectively. Moreover, after the permutation encryption, exchange the pixel of coordinate (0, 0) to the other random pixel to improve the security of the original permutation encryption.
- (2) In the diffusion encryption structure, one could add some nonlinear diffusion encryption structure and ciphertext feedback mechanism to enhance the combination of plaintext, keys, and ciphertext and further promote the security of the original encryption algorithm.
- (3) One suggests that multiple-round encryption algorithm is proposed to improve the security based on the higher efficiency.

Input: P_1, P_2, C
Output: Recover the plaintext image P from the given ciphertext image C

- (1) $C_1 = \text{Encryption}(P_1)$
- (2) According to equation (11), $ED = C_1$
- (3) $C_2 = \text{Encryption}(P_2)$
- (4) According to equation (11) and ED , $S'_2 = \text{bitxor}(C_2, ED)$
- (5) $S_2 \leftarrow S'_2$
- (6) for $i = 1$ to M do
- (7) for $j = 1$ to N do
- (8) for $k = 1$ to 1 do
- (9) $[m_1, n_1] = \text{find}(S_2(:, :, 1) == 1)$
- (10) $[m_2, n_2] = \text{find}(S_2(:, :, 1) == 2)$
- (11) end for
- (12) end for
- (13) end for
- (14) $b = \text{mod}((m_2 - m_1), N)$; $a = \text{mod}((m_1 - 1 - b), N)$
- (15) $\varepsilon = \text{mod}((n_2 - n_1), N)$; $\delta = \text{mod}((n_1 - 1 - \varepsilon), N)$
- (16) $ET = [a \ b; \ \delta \ \varepsilon]$
- (17) $S' = \text{bitxor}(C', ED)$; $S \leftarrow S'$
- (18) $P = (ET)^{-1}(S)$
- (19) return P

ALGORITHM 1: Cracking CIEA-HCNN by using chosen-plaintext attack.

FIGURE 3: Zero plaintext image P_1 and its corresponding ciphertext image C_1 . (a) Zero plaintext image P_1 . (b) Its corresponding ciphertext image C_1 .

FIGURE 4: Plaintext image P_2 , the corresponding ciphertext image C_2 , and the temporary permutation encryption image S_2 . (a) Plaintext image P_2 . (b) The corresponding ciphertext image C_2 . (c) The temporary permutation encryption image S_2 .

FIGURE 5: The breaking results on CIEA-HCNN with RGB color Lena, Baboon, and Pepper. (a) Lena ciphertext image. (b) Recovered permutation image of Lena. (c) Recovered plaintext image of Lena. (d) Difference image of Lena. (e) Baboon ciphertext image. (f) Recovered permutation image of Baboon. (g) Recovered plaintext image of Baboon. (h) Difference image of Baboon. (i) Pepper ciphertext image. (j) Recovered permutation image of Pepper. (k) Recovered plaintext image of Pepper. (l) Difference image of Pepper.

5. Conclusions

In this paper, the security analysis of a color image encryption algorithm based on Hopfield chaotic neural network called CIEA-HCNN is given. CIEA-HCNN adopts permutation encryption-diffusion encryption structure; from the view of cryptanalysis, it has the equivalent keys due to the inherent defects. Therefore, one can obtain the equivalent permutation key and the equivalent diffusion key by utilizing the chosen-plaintext attack and further crack CIEA-HCNN. Theoretical analysis and numerical simulation experiment results verify the effectiveness of the deciphering method; as for the color image of size $M \times N$, the data complexity is $O(1)$. Finally, some suggestions are proposed to improve the security of chaotic encryption algorithm. The reported results may help the designers of chaotic cryptography realize the importance of the essential

structure of a color image encryption algorithm based on Hopfield chaotic neural network.

Data Availability

The data and code used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Key Research and Development Program of China (No. 2016YFB0800401) and

the National Natural Science Foundation of China (No. 61532020, 61671161).

References

- [1] A. Shafique and J. Shahid, "Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps," *The European Physical Journal Plus*, vol. 133, no. 8, pp. 1–16, 2018.
- [2] M. Xu and Z. Tian, "A novel image cipher based on 3D bit matrix and Latin cubes," *Information Sciences*, vol. 478, no. 4, pp. 1–14, 2019.
- [3] Q. Gan, S. Yu, C. Li, J. Lü, Z. Lin, and P. Chen, "Design and ARM-embedded implementation of a chaotic map-based multicast scheme for multiuser speech wireless communication," *International Journal of Circuit Theory and Applications*, vol. 45, no. 11, pp. 1849–1872, 2017.
- [4] Z. Lin, S. Yu, J. Lu, S. Cai, and G. Chen, "Design and ARM-embedded implementation of a chaotic map-based real-time secure video communication system," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 25, no. 7, pp. 1203–1216, 2015.
- [5] W. Zhang, H. Yu, Y.-l. Zhao, and Z.-l. Zhu, "Image encryption based on three-dimensional bit matrix permutation," *Signal Processing*, vol. 118, no. 1, pp. 36–50, 2016.
- [6] X. Li, Z. Xie, J. Wu, and T. Li, "Image encryption based on dynamic filtering and bit cuboid operations," *Complexity*, vol. 2019, Article ID 7485621, 16 pages, 2019.
- [7] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D sine logistic modulation map for image encryption," *Information Sciences*, vol. 297, pp. 80–94, 2015.
- [8] C. Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences," *Optics Communications*, vol. 285, no. 1, pp. 29–37, 2012.
- [9] B. Norouzi, S. Mirzakhaki, S. M. Seyedzadeh, and M. R. Mosavi, "A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process," *Multimedia Tools and Applications*, vol. 71, no. 3, pp. 1469–1497, 2014.
- [10] C. Fu, B.-b. Lin, Y.-s. Miao, X. Liu, and J.-j. Chen, "A novel chaos-based bit-level permutation scheme for digital image encryption," *Optics Communications*, vol. 284, no. 23, pp. 5415–5423, 2011.
- [11] M. Zhou and C. Wang, "A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks," *Signal Processing*, vol. 171, p. 107484, 2020.
- [12] G. Cheng, C. Wang, and H. Chen, "A novel color image encryption algorithm based on hyperchaotic system and permutation-diffusion architecture," *International Journal of Bifurcation and Chaos*, vol. 29, no. 9, p. 1950115, 2019.
- [13] C. Xu, J. Sun, and C. Wang, "An image encryption algorithm based on random walk and hyperchaotic systems," *International Journal of Bifurcation and Chaos*, vol. 30, no. 4, p. 2050060, 2020.
- [14] X.-Y. Wang and Z.-M. Li, "A color image encryption algorithm based on Hopfield chaotic neural network," *Optics and Lasers in Engineering*, vol. 115, no. 4, pp. 107–118, 2019.
- [15] C. Song and Y. Qiao, "A novel image encryption algorithm based on DNA encoding and spatiotemporal chaos," *Entropy*, vol. 17, no. 10, pp. 6954–6968, 2015.
- [16] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A novel chaotic image encryption scheme using DNA sequence operations," *Optics and Lasers in Engineering*, vol. 73, no. 5, pp. 53–61, 2015.
- [17] J. Wu, X. Liao, and B. Yang, "Image encryption using 2D Hénon-Sine map and DNA approach," *Signal Processing*, vol. 153, no. 12, pp. 11–23, 2018.
- [18] S. Wang, C. Wang, and C. Xu, "An image encryption algorithm based on a hidden attractor chaos system and the Knuth-Durstenfeld algorithm," *Optics and Lasers in Engineering*, vol. 128, p. 105995, 2020.
- [19] F. Özkaynak, "Brief review on application of nonlinear dynamics in image encryption," *Nonlinear Dynamics*, vol. 92, no. 2, pp. 305–313, 2018.
- [20] H. Wen and S. Yu, "Cryptanalysis of an image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps," *The European Physical Journal Plus*, vol. 134, no. 7, pp. 1–16, 2019.
- [21] Z. Zhang and S. Yu, "On the security of a Latin-bit cube-based image chaotic encryption algorithm," *Entropy*, vol. 21, no. 9, p. 888, 2019.
- [22] Z. Lin, G. Wang, X. Wang, S. Yu, and J. Lü, "Security performance analysis of a chaotic stream cipher," *Nonlinear Dynamics*, vol. 94, no. 2, pp. 1003–1017, 2018.
- [23] Z. Lin, S. Yu, and X. Feng, "Cryptanalysis of a chaotic stream cipher and its improved scheme," *International Journal of Bifurcation and Chaos*, vol. 28, no. 7, Article ID 1850086, 2018.
- [24] J. Wu, X. Liao, and B. Yang, "Cryptanalysis and enhancements of image encryption based on three-dimensional bit matrix permutation," *Signal Processing*, vol. 142, no. 1, pp. 292–300, 2018.
- [25] W. Feng, Y. He, H. Li, and C. Li, "Cryptanalysis and improvement of the image encryption scheme based on 2D logistic-adjusted-sine map," *IEEE Access*, vol. 7, no. 1, pp. 12584–12597, 2019.
- [26] C. Li, Y. Liu, T. Xie, and M. Z. Q. Chen, "Breaking a novel image encryption scheme based on improved hyperchaotic sequences," *Nonlinear Dynamics*, vol. 73, no. 3, pp. 2083–2089, 2013.
- [27] L. Y. Zhang, Y. Liu, F. Pareschi et al., "On the security of a class of diffusion mechanisms for image encryption," *IEEE Transactions on Cybernetics*, vol. 48, no. 4, pp. 1163–1175, 2018.
- [28] C. Li and K.-T. Lo, "Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," *Signal Processing*, vol. 91, no. 4, pp. 949–954, 2011.
- [29] H. Wen, S. Yu, and J. Lü, "Breaking an image encryption algorithm based on DNA encoding and spatiotemporal chaos," *Entropy*, vol. 21, no. 3, pp. 1–18, 2019.
- [30] M. Li, M. Xu, J. Luo, and H. Fan, "Cryptanalysis of an image encryption using 2D henon-sine map and DNA approach," *IEEE Access*, vol. 7, no. 5, pp. 63336–63345, 2019.
- [31] J. J. Hopfield, "Neural networks and physical systems with emergent collective computational abilities," *Proceedings of the National Academy of Sciences*, vol. 79, no. 8, pp. 2554–2558, 1982.
- [32] D. R. Stinson, "Cryptography theory and practice," *Computers & Mathematics with Applications*, CRC Press, Boca Raton, FL, USA, 1995.