entropy

MDPI

Article

An Optical Image Encryption Method Using Hopfield Neural Network

Xitong Xu and Shengbo Chen *

College of Geo-Exploration Science and Technology, Jilin University, Changchun 130026, China; xitong19@mails.jlu.edu.cn
* Correspondence: chensb@jlu.edu.cn

Abstract: In this paper, aiming to solve the problem of vital information security as well as neural network application in optical encryption system, we propose an optical image encryption method by using the Hopfield neural network. The algorithm uses a fuzzy single neuronal dynamic system and a chaotic Hopfield neural network for chaotic sequence generation and then obtains chaotic random phase masks. Initially, the original images are decomposed into sub-signals through wavelet packet transform, and the sub-signals are divided into two layers by adaptive classification after scrambling. The double random-phase encoding in 4*f* system and Fresnel domain is implemented on two layers, respectively. The sub-signals are performed with different conversions according to their standard deviation to assure that the local information's security is guaranteed. Meanwhile, the parameters such as wavelength and diffraction distance are considered as additional keys, which can enhance the overall security. Then, inverse wavelet packet transform is applied to reconstruct the image, and a second scrambling is implemented. In order to handle and manage the parameters used in the scheme, the public key cryptosystem is applied. Finally, experiments and security analysis are presented to demonstrate the feasibility and robustness of the proposed scheme.

Keywords: optical image encryption; wavelet packet transform; double random phase encoding; 4*f* system; Fresnel domain; Hopfield neural network; single neuronal dynamic system

Citation: Xu, X.; Chen, S. An Optical Image Encryption Method Using Hopfield Neural Network. *Entropy* **2022**, *24*, 521. https://doi.org/10.3390/e24040521

Academic Editors: Xiaowei Li, Jian-Zhong Li and Yu Zhao

Received: 26 February 2022
Accepted: 5 April 2022
Published: 7 April 2022

1. Introduction

In the development of digital technology and computer industry, the requirements for information confidentiality has attracted increasing attention. In order to provide protection to multimedia applications, many algorithms have been developed during the past several decades. The application of optical methods in information security has become a hot trend due to its inherent capabilities of parallel processing [1–5]. The classic double random-phase encoding was proposed based on an optical Fourier transform system. Subsequently, a large number of approaches have been developed to searching for other types of optical encryption methods in different domains, such as fractional Fourier domain [6–8], Fresnel domain [9,10] and gyrator domain [11]. However, due to inherent symmetry and linearity, the security of such cryptosystems is greatly affected [12,13]. During the process of optical image encryption, it is necessary not only to conceal the information of whole image, but also to selectively encrypt the important information, so as to improve local security. In addition, considering the characteristics of chaotic systems (i.e., sensitivity to initial values, deterministic dynamics, nonlinear transformation and pseudo-randomness) [14,15], applying chaotic systems to optical image encryption may have a positive impact on the overall security.

Hopfield neural network, proposed for the first time by Hopfield in 1982 [16], is a typical dynamic neural network which has been applied in information processing and engineering, such as associative memory [17] and optimization problems [18]. It is worth noting that the Hopfield neural network plays a crucial role in neuro-computing due to its

similarity to brain dynamics [19], and the complex behaviors and properties of the Hopfield neural network have been investigated [20–23]. As more and more research is done to combine chaos theory and information security, neural networks have become a vital method to be considered in image encryption. Particularly, a Hopfield neural network with chaos can greatly improve the space–time complexity of an encryption scheme through outstanding nonlinear and associative memory effects [24–27]. However, few studies have integrated the Hopfield neural network and optical methods to enhance the security of information.

In recent years, chaotic systems have been combined with different cryptosystems and technologies for image encryption, such as compression sensing [28,29] and DNA [30,31]. The combination has been proved to effectively improve the key space and the stability of encryption algorithms [32,33], and plenty of simple chaotic systems (e.g., logistic map and sine map) have been applied due to uncomplicated structure [34–36]. Nevertheless, the security of optical image encryption cannot be improved by using simple chaotic systems on account of their structure and insufficient parameters. Moreover, the sensitivity to computer precision may cause the systems to degenerate into non-chaotic systems immediately [37]. The single neuronal dynamic system was derived from the Hopfield neural network by Xu et al. in 2021 [38]. The system has sufficient parameters and complex chaotic dynamical behavior, whereas chaos cannot always be maintained in the interval of some parameters. Fuzzy numbers have a large field of study with applications in dynamical systems, which promote the systems to present many chaos-related phenomena [39–41]. The single neuronal dynamic system also has the applicability to combine with fuzzy numbers to further enhance the stability and chaotic phenomena.

In this paper, a chaotic Hopfield neural network and fuzzy single neuronal dynamic system are combined with a hybrid optical method to construct a new encryption method. In this scheme, the input image is decomposed into sub-signals through wavelet packet transform, and the sub-signals are divided into two layers by adaptive classification after scrambling. The chaotic random-phase masks are constructed by chaotic sequences. The first layer of sub-signals is encrypted by double random phase encoding (DRPE) in 4*f* system, and the second layer is encrypted by double random phase encoding in Fresnel domain. After inverse wavelet packet transform, the obtained image is secondarily scrambled. In addition, the keys used in the process of encryption are integrated and hidden by RSA cryptosystem. Finally, simulation experiments demonstrate the feasibility and security of the proposed method.

2. Related Chaotic System and Public Key Cryptosystem

2.1. Fuzzy Single Neuronal Dynamical System

The single neuronal dynamical system in Hopfield neural network was proposed by Xu et al. in 2021 [38]. The mathematical model of the system is described as follows:

$$\begin{cases} v_i(t) = \frac{1}{1+exp(-\gamma u_i(t))} \\ v_i'(t) = v_i(t) \times 2^n - floor(v_i(t) \times 2^n) \\ u_i(t+1) = ku_i(t) + zv_i'(t) + h \end{cases} \tag{1}$$

where γ, k, z, h and n are system parameters. The robustness and sensitivity of single neuronal dynamical system has been verified in [38]. However, the performance of single neuronal dynamical system can be further improved by using fuzzy numbers.

In this work, we consider the triangular form of fuzzy number as Equation (2), and the full presentation of fuzzy number can be found in [42–44].

$$f_s(x) = \begin{cases} \frac{x}{s} \; 0 \le x \le z \\ \frac{1-x}{1-s} \; z \le x \le 1 \end{cases} \tag{2}$$

where s is the peak of the triangular fuzzy number.

We propose partitioning single neuronal dynamical system by combining it with the triangular form of fuzzy number to generate fuzzy single neuronal dynamical system fuzzy single neuronal dynamic system, as shown in Equation (3).

$$\begin{cases} v_i(t) = f_s(\frac{1}{1+\exp(-\gamma u_i(t))}) \\ v_i'(t) = v_i(t) \times 2^n - floor(v_i(t) \times 2^n) \\ u_i(t+1) = ku_i(t) + zv_i'(t) + h \end{cases} \tag{3}$$

Considering $s = 0.1$, the Lyapunov exponent evolution comparison between the single neuronal dynamical system and the fuzzy single neuronal dynamic system is performed, as shown in Figures 1–5. It can be seen that the stability of the fuzzy single neuronal dynamic system and the interval in the chaotic state are significantly increased. For parameter γ, Figure 1 shows the instances of entering the chaotic state at $\gamma > 132.8$ and $\gamma < -25.3$, which indicates there are larger chaos intervals on the both sides of the zero point. A similar phenomenon is also observed in parameters k and z. For parameter n, as shown in Figure 4, its Lyapunov exponent fluctuates more smoothly, which is similar to parameters k and z.

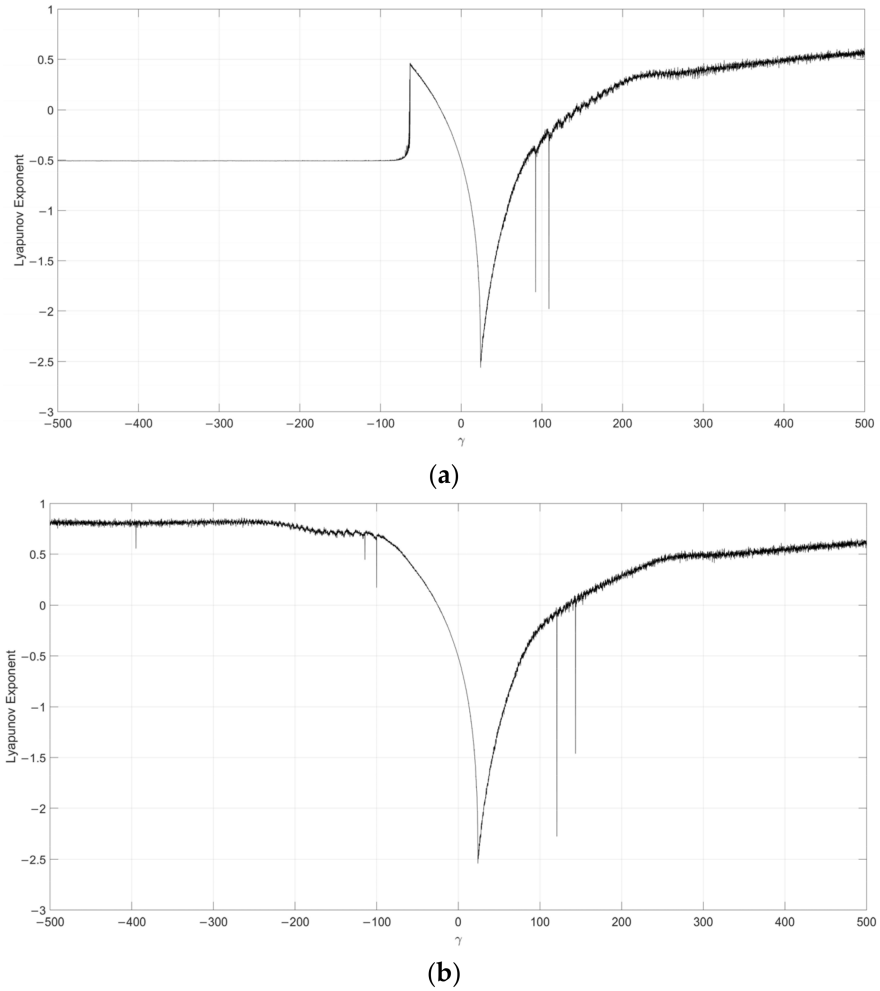
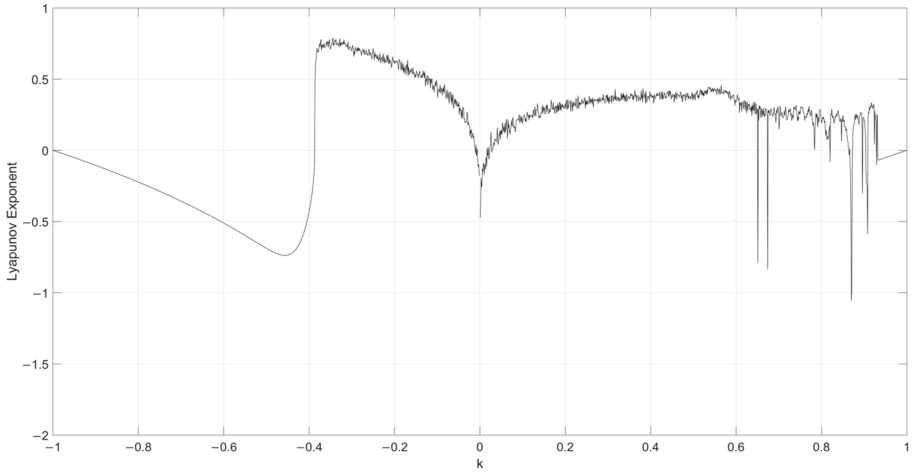
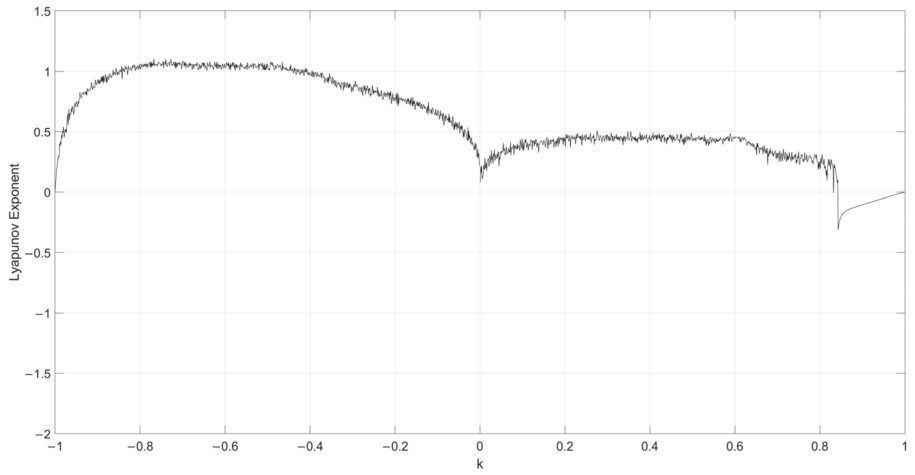


Figure 1. Lyapunov exponent diagram of parameter y when $s = 0.1$, $k = 0.5$, $z = -0.1$, $h = 0.01$ and $n = 14$ for (**a**) single neuronal dynamic system and (**b**) fuzzy single neuronal dynamic system.

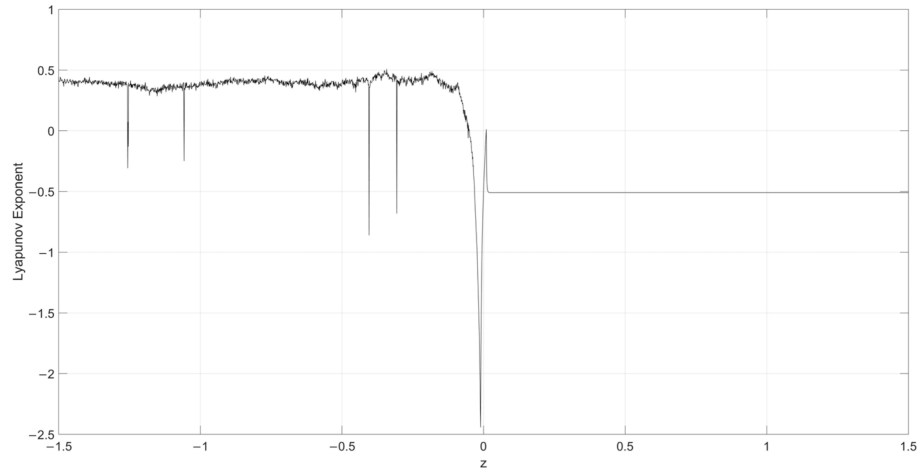


(**a**)



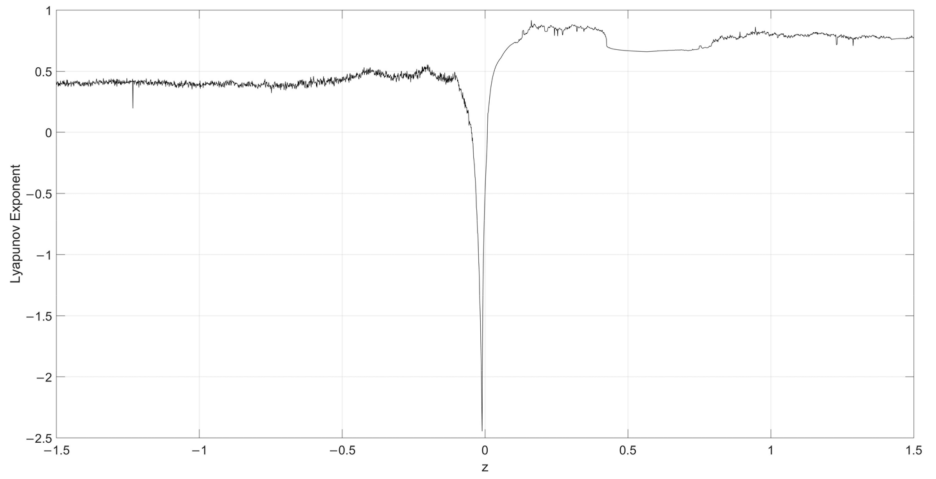
(**b**)

Figure 2. Lyapunov exponent diagram of parameter k when $s = 0.1$, $y = 250$, $z = -0.1$, $h = 0.01$ and $n = 14$ for (**a**) single neuronal dynamic system and (**b**) fuzzy single neuronal dynamic system.



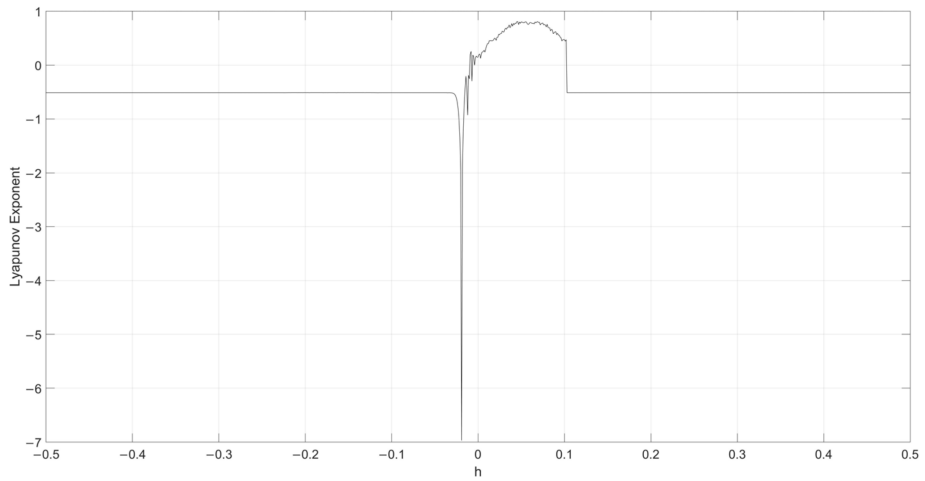
(**a**)

Figure 3. *Cont*.

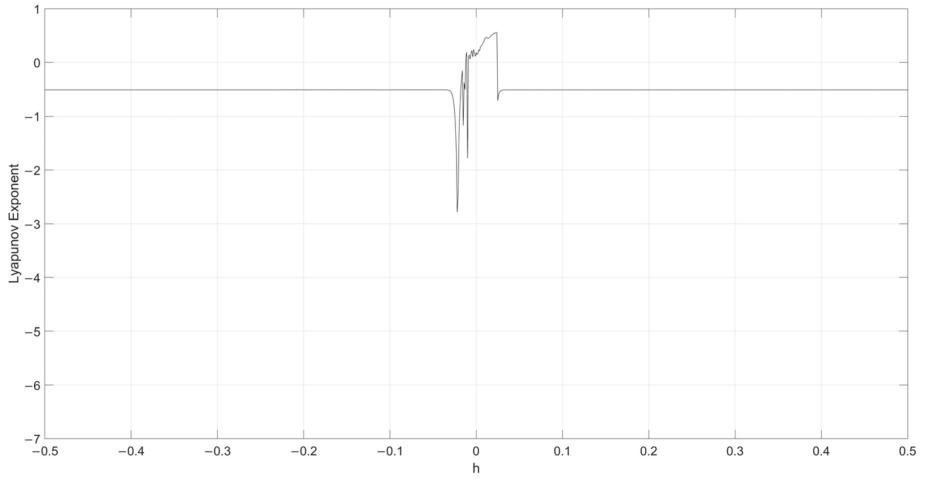


(**b**)

Figure 3. Lyapunov exponent diagram of parameter z when $s = 0.1$, $y = 250$, $k = 0.5$, $h = 0.01$ and $n = 14$ for (**a**) single neuronal dynamic system and (**b**) fuzzy single neuronal dynamic system.

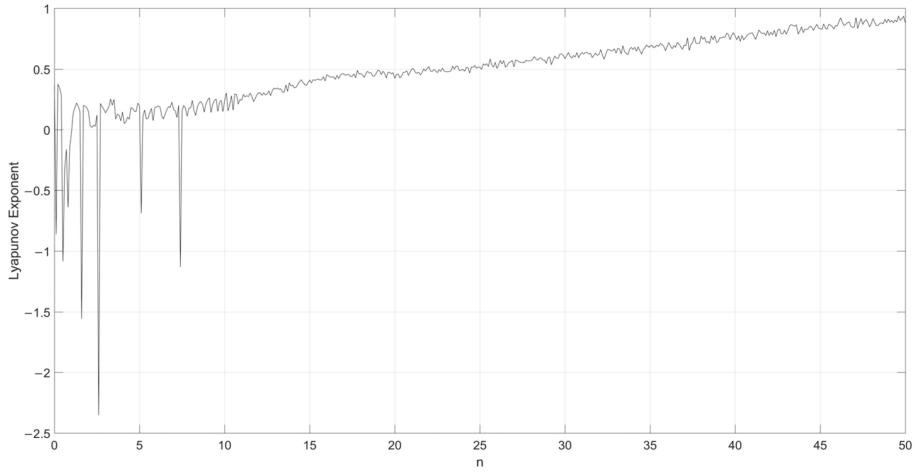


(**a**)

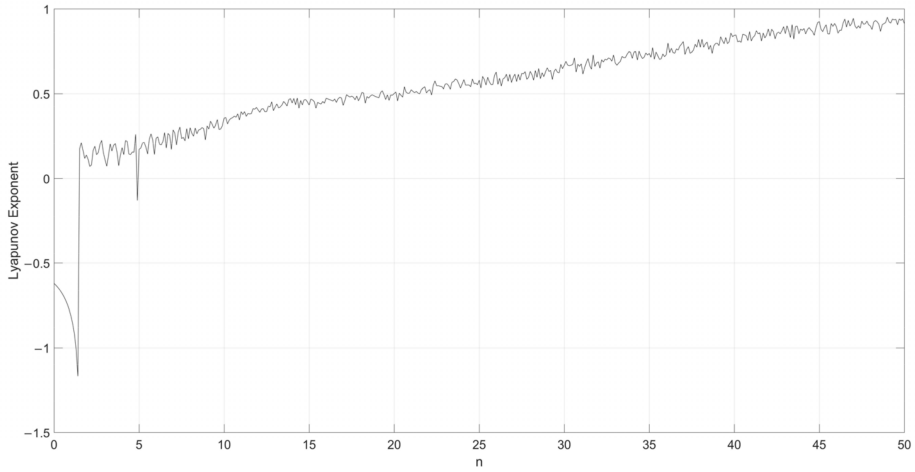


(**b**)

Figure 4. Lyapunov exponent diagram of parameter h when $s = 0.1$, $y = 250$, $k = 0.5$, $z = -0.1$ and $n = 14$ for (**a**) single neuronal dynamic system and (**b**) fuzzy single neuronal dynamic system.



(**a**)



(**b**)

Figure 5. Lyapunov exponent diagram of parameter n when $s = 0.1$, $y = 250$, $k = 0.5$, $z = -0.1$ and $h = 0.01$ for (**a**) single neuronal dynamic system and (**b**) fuzzy single neuronal dynamic system.

2.2. Hopfield Chaotic Neural Network

This paper considers a 3-neuron Hopfield network of the form:

$$\dot{x} = -x + W\varphi(x) \tag{4}$$

$$\varphi(x_i) = \tanh(x_i) = \frac{e^{x_i} - e^{-x_i}}{e^{x_i} + e^{-x_i}} \tag{5}$$

where $x = [x_1, x_2, x_3]^T$ is the neuron state vector, the neuron activation function $\varphi(x) = [\tanh(x_1), \tanh(x_2), \tanh(x_3)]^T$, and synaptic weight matrix is:

$$W = \begin{bmatrix} 2 & -1.58 & -0.27 \\ 1.87 & 1.71 & 1.04 \\ -6.92 & -0.58 & 1.1 \end{bmatrix} \tag{6}$$

When the 3-neuron Hopfield network applies the weight matrix, the system can display chaotic behavior. The dynamic behavior of the chaotic Hopfield network is complex and suitable for image encryption. Figure 6 demonstrates the phrase portrait of the network with the initial state $[0.1,\ 0.1,\ 0.1]$, which shows a double-scroll chaotic attractor.

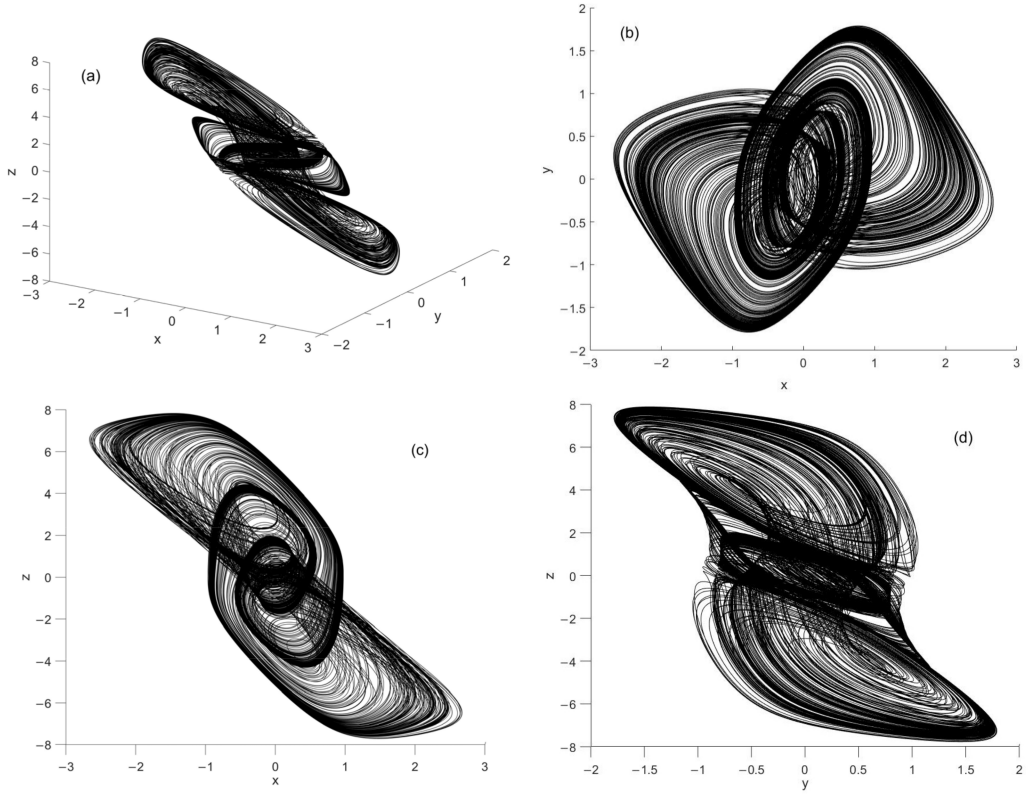


Figure 6. The double-scroll chaotic attractor of chaotic Hopfield neural network: (**a**) projection in x-y-z, (**b**) projection in x-y, (**c**) projection in x-z, (**d**) projection in y-z.

2.3. Public Key Cryptosystem

The RSA public key cryptosystem was proposed by Rivest et al. [45] in 1978, and its implementation depend on the difficulty of large integer decomposition. In RSA, users have their own public key (N, e) and private key d. The key generation process is described as follows:

- Two large prime numbers (i.e., p and q) are generated randomly, and $p \neq q$.
- The key N and Euler function $\varphi(N)$ are calculated as Equations (7) and (8):

$$N = p \cdot q \tag{7}$$

$$\varphi(N) = (p-1) \cdot (q-1) \tag{8}$$

- An integer number e is generated as one of public keys obeyed Equations (9) and (10):

$$1 < e < \varphi(N) \tag{9}$$

$$\gcd(e, \varphi(N)) = 1 \tag{10}$$

  where, gcd denotes the great common divisor.
- Then, d is calculated as Equation (11) as private key:

$$d = e^{-1} \; mod \; \varphi(N) \tag{11}$$

  where *mod* denotes the modulo operation.

After obtaining public key and private key, the plaintext is divided into multiple groups, each of which is a decimal number m of bit length less than N. The encryption operation can be described as Equation (12):

$$C = m^e \; mod \; N \tag{12}$$

where C represents the ciphertext. The decryption operation is performed as Equation (13):

$$m = C^d \ mod \ N \tag{13}$$

3. Algorithm Description

3.1. Encryption Steps

In this paper, an optical image encryption algorithm based on Hopfield neural network is proposed, as shown in Figure 7. To enhance the level of security, we use wavelet packet transform to decompose and filter the signal. Then, there are two layers in the subsequent encryption process. The DRPE method is applied to two layers through 4f system and Fresnel transform, respectively. Furthermore, RSA cryptosystem is performed for key-sequence management. It should be noted that there is no specific method and limitation for random matrix construction in the traditional DRPE. Thus, we construct random-phase masks to encrypt the decomposed signal by different chaotic sequences. The detail of the process is described in Figure 7.

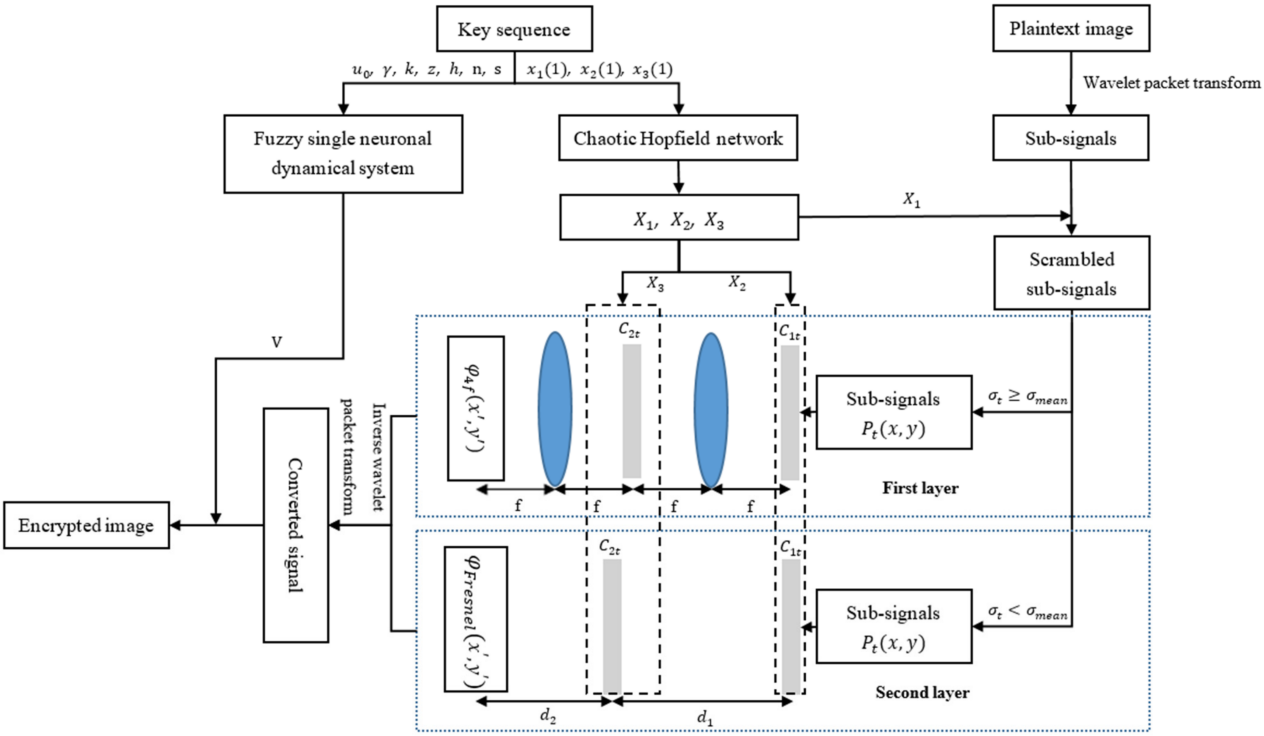


Figure 7. Diagram of the optical image encryption.

Suppose the size of plaintext image is $M \times N$, where M is the length of the row and N is the length of the column.

Step 1: The plaintext image is decomposed using m order wavelet packet transform, and sub-signals are obtained. Each sub-signal has a corresponding number, ranging from 1 to T. Set $x_1(1)$, $x_2(1)$, $x_3(1)$ as the initial values of the Hopfield chaotic neural network, and the $M \times N$ times iteration is performed to get three sequences.

Step 2: Calculate the state variable s by Equation (14). When $S = 0$, insert $\{x_1, x_2, x_3\}$ to new sequences. When $S = 1$, insert $\{x_2, x_3, x_1\}$ to new sequences. When $S = 2$, insert $\{x_3, x_1, x_2\}$ to new sequences. After $M \times N$ iterations, three new sequences X_1, X_2, X_3 are obtained.

$$S = mod(floor(\sqrt{x_1^2 + x_2^2 + x_3^2}, 3)) \tag{14}$$

Step 3: The sequence X_1 is divided into subsequences [$L1$, $L2$, . . . , LT], and each sub-signal is converted into a 1D matrix [$P1$, $P2$, . . . , PT]. Sort each sequence L in ascending

order, and matrix P' is obtained according to the sorting result. The process is shown in Figure 8. Then, P' is converted back to a 2D matrix.

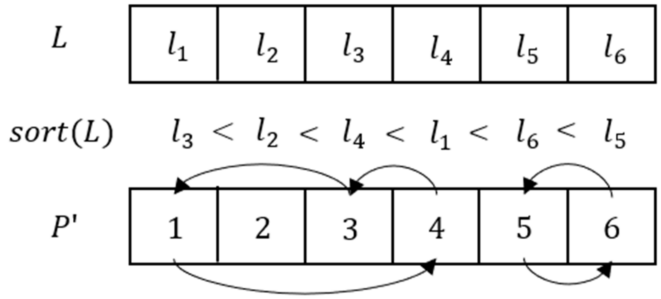


Figure 8. Scrambling process of matrix.

Step 4: The standard deviation σ_t of each scrambled sub-signal is calculated, and the mean of $[\sigma_1, \ldots, \sigma_t, \ldots, \sigma_T]$ is obtained. If $\sigma_t \geq \sigma_{mean}$, the sub-signal is assigned to the first layer. If $\sigma_t < \sigma_{mean}$, the sub-signal is assigned to the second layer.

Step 5: The sequence X_2 and X_3 is divided into subsequences numbered from 1 to T, respectively. Each subsequence is converted into matrix with the size of sub-signal. Then, perform Arnold scrambling on each chaotic matrix as in Equation (15):

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & \alpha \\ \beta & \alpha\beta + 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \ mod\ N \tag{15}$$

where (x, y) is the original coordinate, (x', y') is the scrambled coordinate.

Step 6: After Arnold scrambling, normalize each matrix from X_{2t} to obtain chaotic random matrix $g_t(x, y)$, and normalize each matrix from X_{3t} to obtain chaotic random matrix $r_t(x, y)$. Then construct chaotic random phase:

$$C_{1t}(x, y) = \exp[i2\pi g_t(x, y)] \tag{16}$$

$$C_{2t}(x, y) = \exp[i2\pi r_t(x, y)] \tag{17}$$

Step 7: Perform DRPE of 4f system on sub-signals of the first layer as in Equation (18). Then, DRPE of Fresnel transform is performed on sub signals of the second layer as in Equation (19):

$$\varphi_{4f}(x', y') = FT^{-1}\{FT[P_t(x, y) \cdot C_{1t}(x, y)] \cdot C_{2t}(x, y)\} \tag{18}$$

$$\varphi_{Fresnel}(x', y') = FrT_{\rho,d1}\left\{FrT_{\rho,d2}[P_t(x, y) \cdot C_{1t}(x, y)] \cdot C_{2t}(x, y)\right\} \tag{19}$$

where (x, y) is the original coordinate of sub-signal, (x', y') is the coordinate after DRPE in 4f system or Fresnel transform, ρ and is the incident light wavelength, d_1 and d_2 represent the diffraction distance. $FT[\cdot]$ and $FT^{-1}[\cdot]$ represent Fourier transform and inverse Fourier transform, respectively. $FrT[\cdot]$ represents Fresnel transform.

Step 8: Sub-signals are transformed into $M \times N$ matrix E by m order inverse wavelet packet transform. Then, the complex-value matrix E is normalized.

Step 9: u_0, γ, k, z, h, n and s are initial value and system parameters of fuzzy single neuronal dynamic system, therefore they are used as key sequence. Iterate fuzzy single neuronal dynamic system $M \times N$ times, and a chaotic sequence V is obtained. This sequence is used to scramble matrix E to obtain an encrypted image; the process is the same as Step 3.

The keys used in the process of encryption are divided into three sequences. The first sequence includes initial values of chaotic Hopfield neural network and parameters of Arnold scrambling (i.e., $x_1(1)$, $x_2(1)$, $x_3(1)$, α, β). The second sequence consists of initial value and system parameters of fuzzy single neuronal dynamic system (i.e., u_0, γ, k, z, h, n, s). The third sequence is composed of wavelet packet transform order, incident

light wavelength and diffraction distance (i.e., m, ρ, d_1, d_2). The ciphertext sequences are obtained by RSA cryptosystem using public keys N and e.

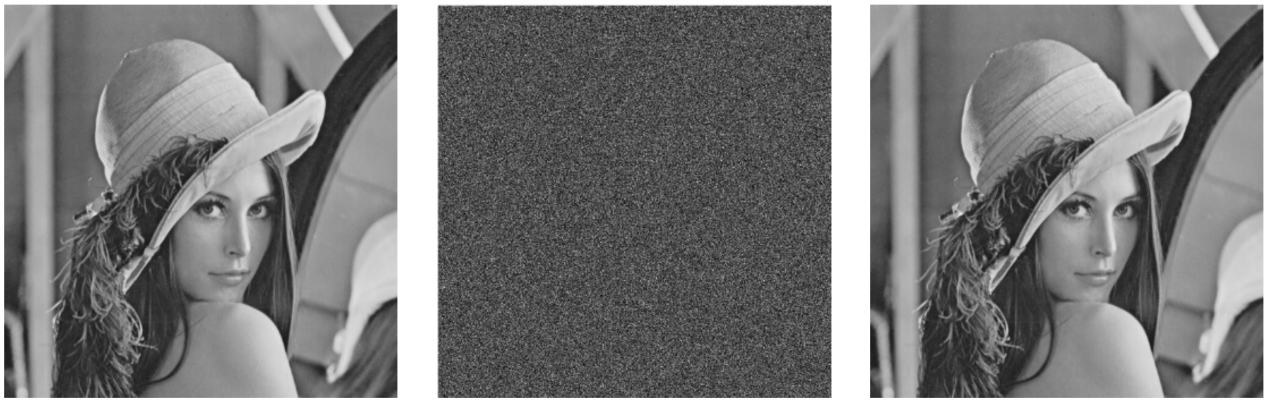
3.2. Image Decryption

In this work, keys used in the scheme are integrated and hidden by an RSA cryptosystem. Thus, the process of decryption can be performed for cases where three key sequences are retrieved. The users can restore the sequences to perform the decryption process according to private keys N and d.

4. Experimental Results and Security Analysis

4.1. Experimental Results

The numerical simulation and security verification of the algorithm are performed by Matlab R2017a. A standard grayscale image Lena of size 512×512 is shown in Figure 9a is the original image. The initial values and system parameters of the algorithm are $m = 2$, $x_1(1) = 0.1$, $x_2(1) = 0.1$, $x_3(1) = 0.1$, $u_0 = 0.1$, $\gamma = -250$, $k = -0.6$, $z = -0.1$, $h = 0.01$, $n = 14$, $s = 0.1$, $\rho = 632.8$ nm, $d_1 = 40$ mm, $d_2 = 50$ mm, $\alpha = 3$, $\beta = 5$, respectively. In addition, two prime numbers ($p = 257$ and $q = 311$) are applied in the RSA cryptosystem to obtain public key ($N = 79,927$, $e = 6937$) and private key ($d = 4393$). Figure 9b shows the encrypted grayscale image Lena, and the decrypted image with correct keys is shown as Figure 9c.



(**a**) (**b**) (**c**)

Figure 9. Encryption experiment results: (**a**) original image; (**b**) encrypted image; (**c**) decrypted image.

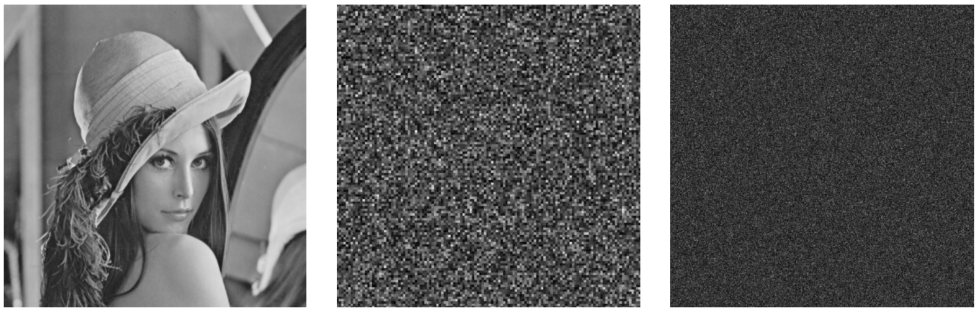
4.2. Security Analysis

4.2.1. Key Space Analysis

In this work, the precision of noninteger key is considered as 10^{-16}. This algorithm covers a chaotic Hopfield neural network with 3 noninteger initial values, fuzzy single neuronal dynamic system with 7 noninteger initial values and other system parameters. Thus, the key space is larger than 2^{128}, which is enough to resist brute force attacks [46,47].

4.2.2. Sensitivity Analysis

In order to test key sensitivity, the influence of varying initial values and system parameters on the decryption result is explored. When the initial deviation of the chaotic Hopfield neural network or fuzzy single neuronal dynamic system is 10^{-16}, the generated sequence and random phase masks cannot correctly decrypt the image, as shown in Figure 10.



(**a**) (**b**) (**c**)

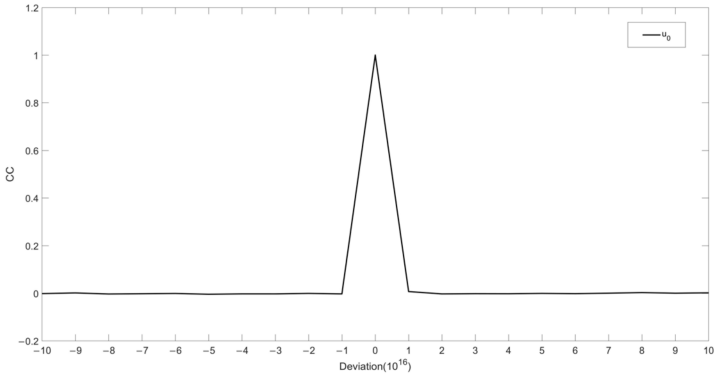
Figure 10. Encryption experiment results: (**a**) original image; (**b**) decrypted image with initial deviation 10^{-16} of $x_1(1)$; (**c**) decrypted image with initial deviation 10^{-16} of u_0.

In addition, the correlation coefficient (CC) is used as the criterion for quantitative analysis of the difference between the original image and decrypted image.

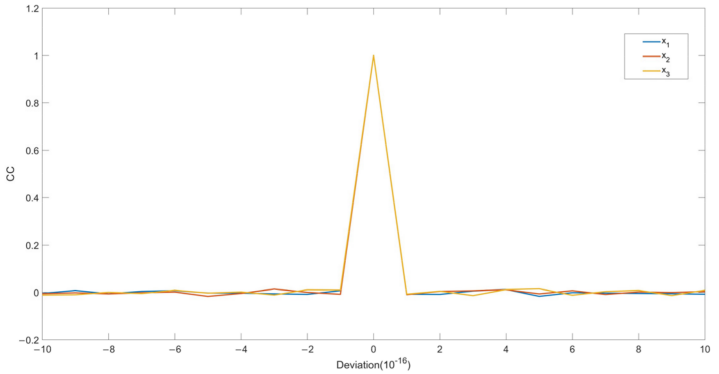
$$CC = \frac{\left|\sum_{i=1}^{m}\sum_{j=1}^{n}[f_1(i,j) - E(f_1(i,j))][f_2(i,j) - E(f_2(i,j))]\right|}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}[f_1(i,j) - E(f_1(i,j))]^2}\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}[f_2(i,j) - E(f_2(i,j))]^2}} \tag{20}$$

where $f_1(i,j)$ represents the plaintext image, $f_2(i,j)$ represents the recovered image, and $E(\cdot)$ represents the expected value operation.

The relationship between CC of the decrypted image and initial values is obtained, as shown in Figure 11. It can be seen that any information about the plaintext image cannot be retrieved when keys change slightly. Thus, the sensitivity of the algorithm is qualified.



(**a**)



(**b**)

Figure 11. Sensitivity analysis of the keys of chaotic systems: (**a**) decrypted CC curve of the key u_0; (**b**) decrypted CC curve of the keys $x_1(1)$, $x_2(1)$ and $x_3(1)$.

4.2.3. Correlation Analysis

Due to the discernibility of information in plaintext images, adjacent pixels are usually highly correlated. Therefore, the reduction of the correlation between adjacent pixels of the cipher images is necessary [48]. The calculation of pixel correlation is shown as Equation (21).

$$\begin{cases} \overline{x} = \frac{1}{N}\sum_{i=1}^{N} x_i \\ D(x) = \frac{1}{N}\sum_{i=1}^{N} x_i - \overline{x} \\ cov(x,y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - \overline{x}\,)(y_i - \overline{y}\,) \\ \rho_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \end{cases} \tag{21}$$

where x_i and y_i represent the values of adjacent pixels, and ρ_{xy} denotes the correlation between adjacent pixels. The results of correlation coefficients of plaintext images and cipher images in horizontal direction, vertical direction and diagonal direction are shown in Table 1.

Table 1. Correlation coefficients of plain images and cipher images in horizontal direction, vertical direction and diagonal direction.

Images		**Correlation Coefficient**		
		Horizontal	**Vertical**	**Diagonal**
Lena (512 × 512)	Plain image	0.9850	0.9719	0.9593
	Cipher image (our scheme)	−0.0005	−0.0033	−0.0009
	Cipher image [49]	0.9407	−0.0273	−0.0140
	Cipher image [50]	−0.0097	0.0032	−0.0051
	Cipher image [51]	−0.0084	−0.0017	−0.0019
	Cipher image [52]	−0.0023	0.0028	−0.0030
Cameraman (256 × 256)	Plain image	0.9592	0.9340	0.9089
	Cipher image (our scheme)	−0.0004	−0.0003	0.0030
	Cipher image [49]	0.9176	−0.0175	−0.0312
	Cipher image [50]	−0.0186	0.0053	0.0095
	Cipher image [51]	0.0208	0.0009	0.0021
	Cipher image [52]	0.0005	−0.0034	0.0008
Peppers (256 × 256)	Plain image	0.9651	0.9759	0.9457
	Cipher image (our scheme)	−0.0007	−0.0009	0.0041
	Cipher image [49]	0.9235	−0.0304	−0.0240
	Cipher image [50]	−0.0247	−0.0129	−0.0031
	Cipher image [51]	−0.0131	0.0024	0.0002
	Cipher image [52]	−0.0027	0.0010	−0.0069
Baboon (256 × 256)	Plain image	0.8003	0.8763	0.7627
	Cipher image (our scheme)	0.0015	−0.0030	0.0007
	Cipher image [49]	0.9323	−0.0482	−0.0306
	Cipher image [50]	−0.0155	−0.0251	0.0013
	Cipher image [51]	0.0026	−0.0015	0.0014
	Cipher image [52]	−0.0060	−0.0064	−0.0050

It should be noted that the scheme combines double random phase encoding in 4*f* system and Fresnel domain with Hopfield neural network to address inherent limitation of random matrix construction. The correlation coefficients of four encrypted images using various schemes are also demonstrated in Table 1. It can be seen that our method reaches relatively low correlation coefficients compared with other methods, which indicates that the integration of double random phase encoding and Hopfield neural network can achieve better performance.

4.2.4. Histogram Analysis

Histogram analysis is the statistic of the number of times each value appears, in order to demonstrate the distribution of pixel values [26]. The histogram of cipher image should not reflect any information about the original image. Figure 12 shows the histogram analysis of four images. It can be seen that the histograms of encrypted test images approximate Rayleigh distribution function, therefore the frequency distribution of plaintext images is hidden.

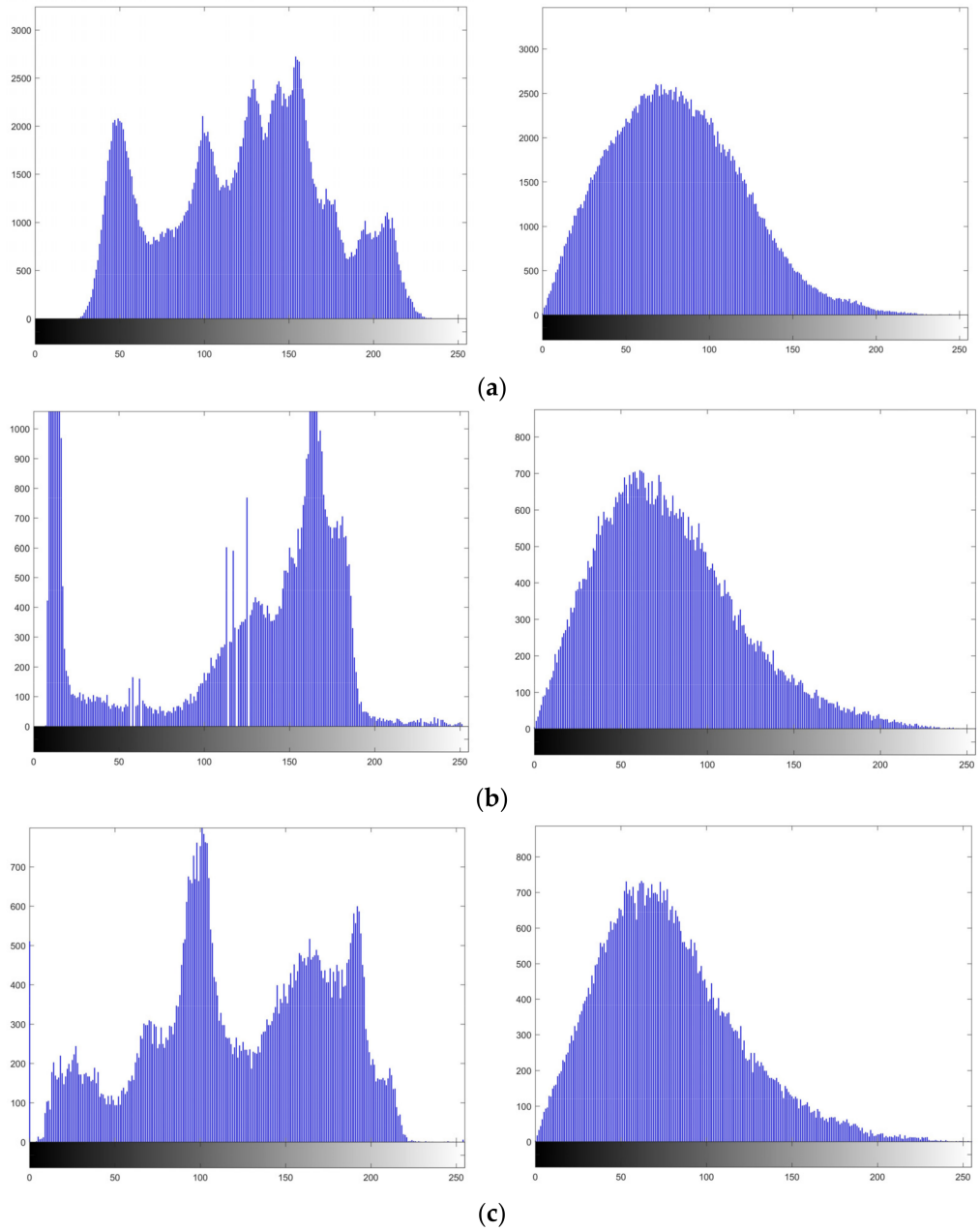


Figure 12. Histogram analysis of the plain images and cipher images: (**a**) Lena; (**b**) Cameraman; (**c**) Peppers.

4.2.5. Binary Image Test

Due to the simple content of binary images, the traditional methods are not applicable sometimes. To test the performance of the algorithm on binary images, the results of encryption are shown in Figure 13. It can be seen that our algorithm works well on binary images, and the correlation coefficients of cipher images are listed in Table 2.

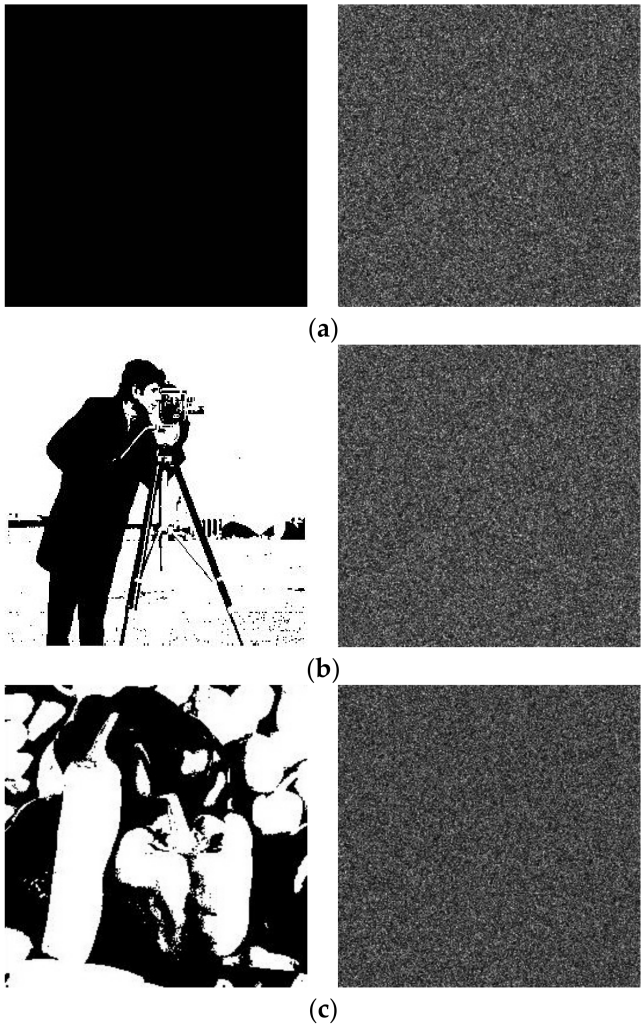


Figure 13. Binary images test: (**a**) black image and corresponding encrypted image; (**b**) cameraman and corresponding encrypted image; (**c**) peppers and corresponding encrypted image.

Table 2. Correlation coefficient of encrypted binary images.

Images		**Correlation Coefficient**		
		Horizontal	**Vertical**	**Diagonal**
Black (256 × 256)	Cipher image	0.0035	−0.0017	0.0022
Cameraman (256 × 256)	Cipher image	−0.0033	0.0007	0.0040
Peppers (256 × 256)	Cipher image	−0.0050	0.0010	−0.0030

4.2.6. Noise Attack

In practice, the cipher images may be affected by noise. We consider the robustness of our algorithm against noise by polluting the encrypted images of Lena with Gaussian random noise, which is expressed as:

$$M'(x,y) = \mathrm{M}(x,y) \times (1 + kG(x,y)) \tag{22}$$

where $M(x,y)$ denotes the original cipher image, $M'(x,y)$ denotes the noise-affected cipher image, k is the noise strength and $G(x,y)$ is the Gaussian random noise with zero-mean and variance 1. The decrypted images with the noise intensity k = 0.01, k = 0.05 and k = 0.1 are shown in Figure 14. The CC value changing with the noise strength is shown in

Figure 15. It can be seen that the contour of original image can be distinguished from the decrypted image.

(**a**) (**b**) (**c**)

Figure 14. Decrypted Lena obtained with (**a**) $k = 0.01$; (**b**) $k = 0.05$; (**c**) $k = 0.1$.

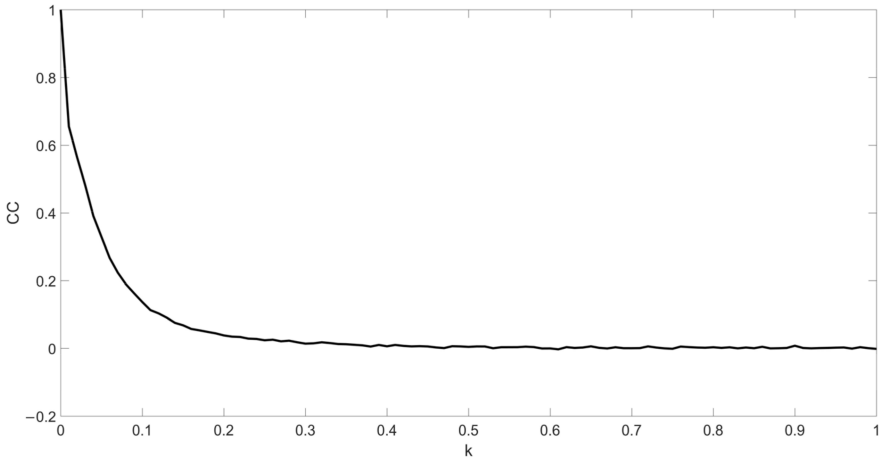


Figure 15. The CC curve of noise attack.

4.2.7. Comparative Analysis

The comparative analysis among different schemes is demonstrated in Table 3. The experimental environments are as follows: Matlab R2017a, AMD Ryzen 5 3600 6-Core Processor 3.60 GHz with 16 GB memory and Windows 10 Operation System, and grayscale Pepper is used as the plaintext image. Table 3 shows that our method reaches the lowest running time in the decryption process, and the running time is slightly higher than [50] in the encryption process. In addition, CC values between the original image and decrypted image are listed in Table 3. It can be seen that the scheme in this study achieves the highest CC value, which is related to the more accurate reconstruction of random phase mask by using the chaotic Hopfield neural network.

Table 3. Comparative analysis of different schemes.

Scheme	Encryption Time (s)	Decryption Time (s)	CC
[50]	0.1136	0.2031	0.9998
[51]	0.4111	0.4259	0.9996
[53]	0.2974	0.3708	0.9832
Our scheme	0.1249	0.1596	0.9999

5. Conclusions

This paper proposes an optical image encryption method using double random-phase encoding in 4*f* system and Fresnel domain based on chaotic system. The chaotic sequences

are constructed by applying a fuzzy single neuronal dynamic system and a Hopfield chaotic neural network. The plaintext image is decomposed into sub-signals by wavelet packet transform, and then the sub-signals are scrambled. By adaptive classification, the sub-signals are divided into two layers. The first layer and second layer are encrypted in 4*f* system and Fresnel domain, thus completing the hybrid encryption. After inverse wavelet packet transform, the encrypted image is obtained through another scrambling. The RSA cryptosystem is applied to the allocation and management of the keys used in the scheme. Numerical simulations have demonstrated the security and effectiveness of the proposed scheme. The suggested scheme implements selective encryption of the local image, which improves the protection efficiency of vital information. It should be noted that the fuzzy numbers effectively enhance the stability and key space of the single neuronal dynamic system, and different fuzzy numbers other than triangular may be applicable to more chaotic systems. In addition, the feasibility of combining the chaotic Hopfield neural network with optical methods to construct an image encryption scheme has been verified. In further work, the application of other neural networks or chaotic systems may have more positive effects on optical image encryption.

Author Contributions: Conceptualization, X.X.; methodology, X.X.; software, X.X.; validation, S.C.; investigation, X.X.; writing—original draft preparation, X.X.; writing—review and editing, S.C.; visualization, X.X.; supervision, S.C.; project administration, S.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the national key research and development program of China (Grant No. 2020YFA0714103).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: We thank the editors and the reviewers for their constructive suggestions and insightful comments, which helped us greatly to improve this manuscript.

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

References

1. Alfalou, A.; Brosseau, C. Optical image compression and encryption methods. *Adv. Opt. Photonics* **2009**, *1*, 589–636. [CrossRef]
2. Shi, Y.; Li, T.; Wang, Y.; Gao, Q.; Zhang, S.; Li, H. Optical image encryption via ptychography. *Opt. Lett.* **2013**, *38*, 1425–1427. [CrossRef] [PubMed]
3. Gong, L.; Deng, C.; Pan, S.; Zhou, N. Image compression-encryption algorithms by combining hyper-chaotic system with discrete fractional random transform. *Opt. Laser Technol.* **2018**, *103*, 48–58. [CrossRef]
4. Yao, L.; Yuan, C.; Qiang, J.; Feng, S.; Nie, S. An asymmetric color image encryption method by using deduced gyrator transform. *Opt. Lasers Eng.* **2017**, *89*, 72–79. [CrossRef]
5. Liansheng, S.; Xiao, Z.; Chongtian, H.; Ailing, T.; Asundi, A.K. Silhouette-free interference-based multiple-image encryption using cascaded fractional Fourier transforms. *Opt. Lasers Eng.* **2019**, *113*, 29–37. [CrossRef]
6. Unnikrishnan, G.; Joseph, J.; Singh, K. Optical encryption by double-random phase encoding in the fractional Fourier domain. *Opt. Lett.* **2000**, *25*, 887–889. [CrossRef]
7. Lima, J.B.; Novaes, L. Image encryption based on the fractional Fourier transform over finite fields. *Signal Process.* **2014**, *94*, 521–530. [CrossRef]
8. Zhao, T.; Ran, Q.; Yuan, L.; Chi, Y.; Ma, J. Security of image encryption scheme based on multi-parameter fractional Fourier transform. *Opt. Commun.* **2016**, *376*, 47–51. [CrossRef]
9. Situ, G.; Zhang, J. Double random-phase encoding in the Fresnel domain. *Opt. Lett.* **2004**, *29*, 1584–1586. [CrossRef]
10. Xu, H.; Xu, W.; Wang, S.; Wu, S. Asymmetric optical cryptosystem based on modulus decomposition in Fresnel domain. *Opt. Commun.* **2017**, *402*, 302–310. [CrossRef]
11. Rodrigo, J.A.; Alieva, T.; Calvo, M.L. Applications of gyrator transform for image processing. *Opt. Commun.* **2007**, *278*, 279–284. [CrossRef]
12. Hengzheng, W.; Xiang, P.; Peng, Z. Chosen-plaintext attack on double phase encoding encryption technique. *Acta Opt. Sin.* **2007**, *27*, 824.

13. Mehra, I.; Nishchal, N.K. Optical asymmetric image encryption using gyrator wavelet transform. *Opt. Commun.* **2015**, *354*, 344–352. [CrossRef]
14. Wu, G.-C.; Baleanu, D. Discrete fractional logistic map and its chaos. *Nonlinear Dyn.* **2014**, *75*, 283–287. [CrossRef]
15. Wang, Y.; Liu, Z.; Ma, J.; He, H. A pseudorandom number generator based on piecewise logistic map. *Nonlinear Dyn.* **2016**, *83*, 2373–2391. [CrossRef]
16. Hopfield, J.J. Neural networks and physical systems with emergent collective computational abilities. *Proc. Natl. Acad. Sci. USA* **1982**, *79*, 2554–2558. [CrossRef] [PubMed]
17. Yang, J.; Wang, L.; Wang, Y.; Guo, T. A novel memristive Hopfield neural network with application in associative memory. *Neurocomputing* **2017**, *227*, 142–148. [CrossRef]
18. Lázaro, O.; Girma, D. A Hopfield neural-network-based dynamic channel allocation with handoff channel reservation control. *IEEE Trans. Veh. Technol.* **2000**, *49*, 1578–1587. [CrossRef]
19. Yang, X.-S.; Yuan, Q. Chaos and transient chaos in simple Hopfield neural networks. *Neurocomputing* **2005**, *69*, 232–241. [CrossRef]
20. Njitacke, Z.; Kengne, J. Complex dynamics of a 4D Hopfield neural networks (HNNs) with a nonlinear synaptic weight: Coexistence of multiple attractors and remerging Feigenbaum trees. *AEU-Int. J. Electron. Commun.* **2018**, *93*, 242–252. [CrossRef]
21. Rech, P.C. Chaos and hyperchaos in a Hopfield neural network. *Neurocomputing* **2011**, *74*, 3361–3364. [CrossRef]
22. Li, J.; Liu, F.; Guan, Z.-H.; Li, T. A new chaotic Hopfield neural network and its synthesis via parameter switchings. *Neurocomputing* **2013**, *117*, 33–39. [CrossRef]
23. Zheng, P.; Tang, W.; Zhang, J. Some novel double-scroll chaotic attractors in Hopfield networks. *Neurocomputing* **2010**, *73*, 2280–2285. [CrossRef]
24. Bigdeli, N.; Farid, Y.; Afshar, K. A robust hybrid method for image encryption based on Hopfield neural network. *Comput. Electr. Eng.* **2012**, *38*, 356–369. [CrossRef]
25. Liu, Z.-H.; Zeng, G.-R.; Xie, F.-S. Chaotic image encryption algorithm based on discrete Hopfield network. *Comput. Eng.* **2012**, *38*, 112–115.
26. Wang, X.-Y.; Li, Z.-M. A color image encryption algorithm based on Hopfield chaotic neural network. *Opt. Lasers Eng.* **2019**, *115*, 107–118. [CrossRef]
27. Liu, L.; Zhang, L.; Jiang, D.; Guan, Y.; Zhang, Z. A simultaneous scrambling and diffusion color image encryption algorithm based on Hopfield chaotic neural network. *IEEE Access* **2019**, *7*, 185796–185810. [CrossRef]
28. Chai, X.; Zheng, X.; Gan, Z.; Han, D.; Chen, Y. An image encryption algorithm based on chaotic system and compressive sensing. *Signal Process.* **2018**, *148*, 124–144. [CrossRef]
29. Zhou, N.; Zhang, A.; Wu, J.; Pei, D.; Yang, Y. Novel hybrid image compression–encryption algorithm based on compressive sensing. *Optik* **2014**, *125*, 5075–5080. [CrossRef]
30. 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]
31. Wang, X.; Liu, C. A novel and effective image encryption algorithm based on chaos and DNA encoding. *Multimed. Tools Appl.* **2017**, *76*, 6229–6245. [CrossRef]
32. Zhou, N.; Pan, S.; Cheng, S.; Zhou, Z. Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing. *Opt. Laser Technol.* **2016**, *82*, 121–133. [CrossRef]
33. Ravichandran, D.; Praveenkumar, P.; Rayappan, J.B.B.; Amirtharajan, R. DNA chaos blend to secure medical privacy. *IEEE Trans. Nanobiosci.* **2017**, *16*, 850–858. [CrossRef] [PubMed]
34. Belazi, A.; Abd El-Latif, A.A. A simple yet efficient S-box method based on chaotic sine map. *Optik* **2017**, *130*, 1438–1444. [CrossRef]
35. Ye, G.; Huang, X. An efficient symmetric image encryption algorithm based on an intertwining logistic map. *Neurocomputing* **2017**, *251*, 45–53. [CrossRef]
36. Li, C.; Xie, T.; Liu, Q.; Cheng, G. Cryptanalyzing image encryption using chaotic logistic map. *Nonlinear Dyn.* **2014**, *78*, 1545–1551. [CrossRef]
37. Li, C.; Feng, B.; Li, S.; Kurths, J.; Chen, G. Dynamic analysis of digital chaotic maps via state-mapping networks. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2019**, *66*, 2322–2335. [CrossRef]
38. Xu, X.; Chen, S. Single neuronal dynamical system in self-feedbacked Hopfield networks and its application in image encryption. *Entropy* **2021**, *23*, 456. [CrossRef]
39. Valandar, M.Y.; Ayubi, P.; Barani, M.J. A new transform domain steganography based on modified logistic chaotic map for color images. *J. Inf. Secur. Appl.* **2017**, *34*, 142–151. [CrossRef]
40. Nieto, J.J.; Otero-Espinar, M.V.; Rodríguez-López, R. Dynamics of the fuzzy logistic family. *Discret. Contin. Dyn. Syst.-B* **2010**, *14*, 699.
41. Molaeezadeh, S.F.; Moradi, M.H. Bifurcating fuzzy sets: Theory and application. *Neurocomputing* **2013**, *118*, 268–278. [CrossRef]
42. Moysis, L.; Volos, C.; Jafari, S.; Munoz-Pacheco, J.M.; Kengne, J.; Rajagopal, K.; Stouboulos, I. Modification of the logistic map using fuzzy numbers with application to pseudorandom number generation and image encryption. *Entropy* **2020**, *22*, 474. [CrossRef] [PubMed]
43. Zimmermann, H.J. *Fuzzy Set Theory—And Its Applications*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2011.

44. Chakraverty, S.; Sahoo, D.M.; Mahato, N.R. *Concepts of Soft Computing: Fuzzy and ANN with Programming*; Springer: Berlin/Heidelberg, Germany, 2019.
45. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
46. François, M.; Grosges, T.; Barchiesi, D.; Erra, R. Pseudo-random number generator based on mixing of three chaotic maps. *Commun. Nonlinear Sci. Numer. Simul.* **2014**, *19*, 887–895. [CrossRef]
47. François, M.; Grosges, T.; Barchiesi, D.; Erra, R. A new image encryption scheme based on a chaotic function. *Signal Process. Image Commun.* **2012**, *27*, 249–259. [CrossRef]
48. Behnia, S.; Akhshani, A.; Mahmodi, H.; Akhavan, A. A novel algorithm for image encryption based on mixture of chaotic maps. *Chaos Solitons Fractals* **2008**, *35*, 408–419. [CrossRef]
49. Ahmad, J.; Khan, M.A.; Hwang, S.O.; Khan, J.S. A compression sensing and noise-tolerant image encryption scheme based on chaotic maps and orthogonal matrices. *Neural Comput. Appl.* **2017**, *28*, 953–967. [CrossRef]
50. Liu, Y.; Jiang, Z.; Xu, X.; Zhang, F.; Xu, J. Optical image encryption algorithm based on hyper-chaos and public-key cryptography. *Opt. Laser Technol.* **2020**, *127*, 106171. [CrossRef]
51. Alawida, M.; Samsudin, A.; Teh, J.S.; Alkhawaldeh, R.S. A new hybrid digital chaotic system with applications in image encryption. *Signal Process.* **2019**, *160*, 45–58. [CrossRef]
52. Lakshmi, C.; Thenmozhi, K.; Rayappan, J.B.B.; Amirtharajan, R. Hopfield attractor-trusted neural network: An attack-resistant image encryption. *Neural Comput. Appl.* **2020**, *32*, 11477–11489. [CrossRef]
53. Shahriyar, T.; Fathi, M.H.; Sekhavat, Y.A. An image encryption scheme based on elliptic curve pseudo random and advanced encryption system. *Signal Process.* **2017**, *141*, 217–227.