Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2015, Article ID 501054, 10 pages
http://dx.doi.org/10.1155/2015/501054

Research Article

Color Image Encryption Algorithm Based on TD-ERCS System and Wavelet Neural Network

Kun Zhang and Jian-bo Fang

School of Mathematics and Statistics, Chuxiong Normal University, Chuxiong, Yunnan 675000, China

Correspondence should be addressed to Kun Zhang; zhangkunpost@qq.com

Received 9 August 2014; Revised 14 November 2014; Accepted 26 November 2014

Academic Editor: Vishal Bhatnaga

In order to solve the security problem of transmission image across public networks, a new image encryption algorithm based on TD-ERCS system and wavelet neural network is proposed in this paper. According to the permutation process and the binary XOR operation from the chaotic series by producing TD-ERCS system and wavelet neural network, it can achieve image encryption. This encryption algorithm is a reversible algorithm, and it can achieve original image in the rule inverse process of encryption algorithm. Finally, through computer simulation, the experiment results show that the new chaotic encryption algorithm based on TD-ERCS system and wavelet neural network is valid and has higher security.

1. Introduction

With the rapid growth and application of multimedia based on the Internet system, image security becomes an important issue. Since the size of digital image is always much greater than text file and the digital images contents are strongly correlated, the traditional encryption algorithms such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), and Advanced Encryption Standard (AES) have the weakness of low-level efficiency [1, 2].

Chaos is a ubiquitous phenomenon in nature and chaotic system is also a complex nonlinear, nonequilibrium dynamic process. Chaos theory is established since 1970s from many different research areas, such as physics, mathematics, biology, and chemistry [3]. The chaotic systems are characterized by sensitive dependence on initial conditions and system parameters, similarity to random behavior, no periodicity, and continuous broadband power spectrum [4]. Most properties can meet some requirements of encryption. Therefore, image encryption technique based on chaotic system has more useful and practical applications in the recent years [5, 6]. However, many of the proposed schemes show some deficiencies, such as small key space and weak security [7]. TD-ERCS system is a new class of discrete chaotic map systems based on the physical model of ellipse reflecting activity. Many researchers have proposed that TD-ERCS system is a discrete chaotic system with the steady complexity, and the pseudorandom sequences generated by TD-ERCS are suitable for use in information encryption [8, 9].

In computer science field, an artificial neural network (ANN) is massively parallel distributed processor made up of simple processing units that has a natural propensity for storing experiential knowledge and making it available for use. As ANNs have many important properties, such as massively parallel, highly connected structures consisting of a number of simple and nonlinear processing elements [10], artificial neural networks (ANNs) have already been applied to solve the image encryption. Many encryption methods based on ANNs have been suggested in research literature and can deal with the intractable problem of fast and highly secure encryption [11, 12].

A new color image encryption algorithm is designed in the paper. In Section 2, the mapping equation of TD-ERCS system is given. In Section 3, wavelet neural networks algorithm is presented in detail. In Section 4, the image encryption algorithm based on TD-ERCS system and wavelet neural network is proposed. Finally, experimental results and some conclusions are given in Section 5.

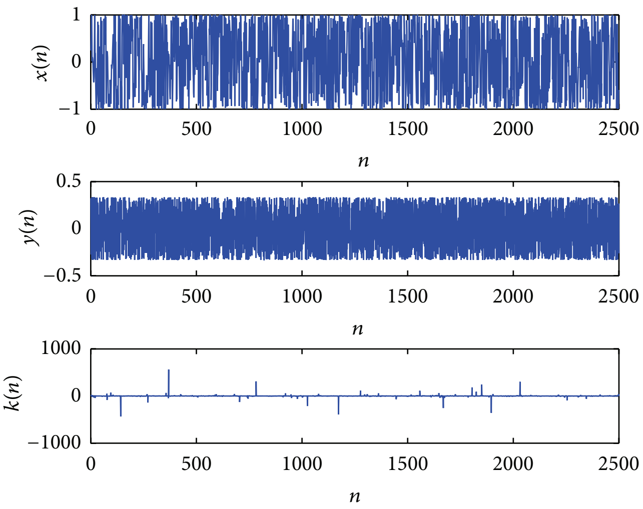


Figure 1: Time responses of TD-ERCS for seed parameters ($\mu = 0.3324$, $x_0 = 0.2456$, $\alpha = 2.143$, and $m = 2$).

2. Tangent-Delay Ellipse Reflecting Cavity-Map System

In 2004, Li-Yuan et al. found a new chaotic system bearing the name of Tangent-Delay Ellipse Reflecting Cavity-Map System (TD-ERCS) [13]. TD-ERCS system is a discrete chaotic system and has many properties such as the maximum Lyapunov exponent which is over zero, unchangeable equiprobability distribution, and zero correlation in total field [14]. TD-ERCS is described by

$$\begin{gathered}
x_n = \frac{-\left[2k_{n-1}y_{n-1} + x_{n-1}\left(u^2 - k_{n-1}^2\right)\right]}{u^2 + k_{n-1}^2}, \\
k_n = \frac{2k'_{n-m} - k_{n-1} + k_{n-1}\left(k'_{n-m}\right)^2}{1 + 2k_{n-1}k'_{n-m} - \left(k'_{n-m}\right)^2}, \\
k'_{n-m} = \begin{cases} -\dfrac{x_{n-1}}{y_{n-1}}\mu^2 & n < m \\ -\dfrac{x_{n-m}}{y_{n-m}}\mu^2 & n \geq m, \end{cases} \\
y_n = k_{n-1}\left(x_n - x_{n-1}\right) + y_{n-1}, \\
k'_0 = -\frac{x_0}{y_0}\mu^2, \\
k_0 = -\frac{\tan\alpha + k'_0}{1 - k'_0\tan\alpha},
\end{gathered} \tag{1}$$

where (μ, x_0, α, m) are called TD-ERCS seed parameters. In TD-ERCS seed parameters, $\mu \in (0, 1]$, initial $x_0 \in [-1, 1]$, $\alpha \in [0, \pi]$, and tangent-delay parameters $m = 2, 3, 4, 5, \ldots$. Figure 1 shows the time responses of TD-ERCS chaotic systems, for TD-ERCS seed parameters ($\mu = 0.3324$, $x_0 = 0.2456$, $\alpha = 2.143$, $m = 2$), iterations $n = 2500$ in (1).

3. Wavelet Neural Networks

3.1. The Wavelet Base Function. A cluster of functions which are got by time shift and scale stretch-out and drawback of mother wavelet function $u(t)$ are called the wavelet base functions. The wavelet base function is shown as follows [15]:

$$u_{a,b}(t) = \frac{1}{\sqrt{a}}u\left(\frac{t-b}{a}\right), \tag{2}$$

where a, b are the scale and translation parameters, respectively. The mother wavelet function $u(t)$ is satisfied using the following equation:

$$C_u = \int_{-\infty}^{+\infty} \frac{|U(f)|}{|f|} df < \infty, \tag{3}$$

where $U(f)$ is Fourier transform of $u(t)$.

3.2. The Model of Wavelet Neural Networks. Wavelet neural networks (WNNs) have emerged as new feed forward neural network based on wavelet transform, in which discrete wavelet function is used as the node activation function [16]. Since wavelet neural networks combine self-studying of neural network and the function of time-frequency localization of wavelet transform, they have strong ability to approximate and robust [17].

The architecture of the WNNs is presented in Figure 2. Wavelet neural networks commonly consist of three layers: input layer, hidden layer, and output layer. All the neurons in the layer are connected to the neurons in the next layer [18].

The output of three-layer WNNs is calculated in the form

$$y_k \approx \sum_{j=1}^{n} \omega_{jk}\psi\left(\frac{\sum_{i=1}^{r} u_{ij}x_i - b_j}{a_j}\right), \quad k = 1, 2, \ldots, m, \tag{4}$$

where r is the neurons number in the input layer, m is the neurons number in the output layer, n is the neurons number in the hidden layer, and ω_{jk} is the connection weight between the jth neuron of hidden layer and the kth neuron of output layer. u_{ij} is the connection weight between the ith neuron of input layer and the jth neuron of hidden layer. b_j is the translation factor of the jth neuron in hidden layer. a_j is the expansion and contraction factor of the jth neuron in hidden layer. x_i is the ith neuron of input layer; y_k is the kth neuron of output layer. In the hidden layer, the activation function of neuron is Morlet wavelet function in [19]

$$\psi(t) = \cos(1.75t)\, e^{-t^2/2}. \tag{5}$$

Let us define error function $e(t)$ as

$$e(t) = y_e(t) - y(t), \tag{6}$$

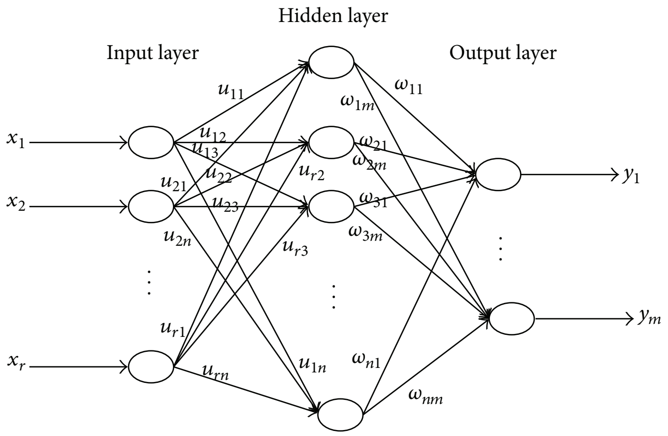


Figure 2: The architecture of wavelet neural networks.

where $y_e(t)$ is the model actual output and $y(t)$ is the desired output at time t. Then the cost function E can be defined as

$$E = \frac{1}{2}\sum_{i=1}^{N}\left(y_e(t) - y(t)\right)^2 = \frac{1}{2}\sum_{i=1}^{N}\left(e(t)\right)^2. \tag{7}$$

Using the gradient descent algorithms, the weight vector for every neuron in wavelet neural networks is updated as follows [20]:

$$\begin{aligned}
\Delta\omega_{jk}(l+1) &= -\eta\frac{\partial E}{\partial\omega_{jk}(l)} + \alpha\Delta\omega_{jk}(l),\\
\Delta u_{ij}(l+1) &= -\eta\frac{\partial E}{\partial u_{ij}(l)} + \alpha\Delta u_{ij}(l),\\
\Delta a_j(l+1) &= -\eta\frac{\partial E}{\partial a_j(l)} + \alpha\Delta a_j(l),\\
\Delta b_j(l+1) &= -\eta\frac{\partial E}{\partial b_j(l)} + \alpha\Delta b_j(l),\\
\omega_{jk}(l+1) &= \omega_{jk}(l) + \Delta\omega_{jk}(l+1),\\
u_{ij}(l+1) &= u_{ij}(l) + \Delta u_{ij}(l+1),\\
a_j(l+1) &= a_j(l) + \Delta a_j(l+1),\\
b_j(l+1) &= b_j(l) + \Delta b_j(l+1),
\end{aligned} \tag{8}$$

where l represents the backward step number and η and α are the learning and the momentum constants, differing in the ranges 0.01 to 0.1 and 0.1 to 0.9, respectively.

4. Image Encryption Based on TD-ERCS and Wavelet Neural Networks

4.1. Process of Permutation Cryptography. Let S be a real set: $S = \{s_1, s_2, \ldots, s_n\}$. A permutation process of order n refers to the operation of replacing an arrangement $\{p_i \mid p_i = i, i = 1, 2, \ldots, n\}$ by a second arrangement $\{q_i \mid q_i = \pi(s_i)\}, \pi(s_i)$ denoted by the s_i numerical order in the S set in ascending or descending order, and $\pi(s_i) \in N$. Permutations group is represented as

$$\phi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(s_1) & \pi(s_2) & \cdots & \pi(s_n) \end{pmatrix}. \tag{9}$$

The reverse of this permutation process is specified as

$$\phi^{-1} = \begin{pmatrix} \pi(s_1) & \pi(s_2) & \cdots & \pi(s_n) \\ 1 & 2 & \cdots & n \end{pmatrix} \tag{10}$$

which retrieves the original arrangement.

Definition 1. A permutation π of X is a bijective function from X to X.

Based on Definition 1, the permutation cryptography process can be defined as follows.

Definition 2 (see [21]). If any data matrix X is transformed to a cipher-matrix $\varphi_z = \emptyset_z(X)$ where $\emptyset_z$ is any permutation operation, then the original matrix X can be obtained again from φ_z with the inverse operation of $\emptyset_z$ on it; that is, $\emptyset_Z^{-1}(\varphi_z) = \emptyset_Z^{-1}(\emptyset_z(X)) = X$, as $\emptyset_Z^{-1}\emptyset_z$ forms an identity operator.

For example, suppose that plaintext G is

$$G = \begin{bmatrix} 0.234 & 1.222 & 0.007 & 0.145 & 0.201 & 0.341 \end{bmatrix}. \tag{11}$$

The G permutations group in ascending order is

$$\phi_G = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 1 & 6 & 2 \end{bmatrix}. \tag{12}$$

Permutation cipher H is

$$H = \begin{bmatrix} 0.004 & 0.421 & 0.107 & 0.423 & 0.007 & 0.221 \end{bmatrix}. \quad (13)$$

The H permutations group in ascending order is

$$\phi_H = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 6 & 2 & 4 \end{bmatrix}. \quad (14)$$

Then

$$\begin{aligned} \phi_M = \phi_G \phi_H &= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 1 & 6 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 6 & 2 & 4 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 2 & 1 & 4 & 5 \end{bmatrix}. \end{aligned} \quad (15)$$

The ciphertext M is

$$M = \begin{bmatrix} 0.234 & 0.201 & 0.007 & 0.341 & 1.222 & 0.145 \end{bmatrix}. \quad (16)$$

The decryption process is

$$\begin{aligned} \phi_G = \phi_M \phi_H &= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 2 & 1 & 4 & 5 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 6 & 2 & 4 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 1 & 6 & 2 \end{bmatrix}. \end{aligned} \quad (17)$$

4.2. Encryption Process. In the paper, the image encryption based TD-ERCS and WNNs mainly consist of two stages. The first stage of whole encryption system is chaotic sequence generation. In the chaotic sequence generation, a new chaotic sequence is generated by wavelet neural networks and TD-ERCS. The second stage of whole encryption system is the confusion stage. Since images are digital, a map is defined to transform the chaotic sequence to another sequence which consists of integers. Then the image can be encrypted by use of permutation operation and XOR with the integer sequence [22].

4.3. The Chaotic Sequence Generator. In this paper, we used chaotic sequences generated by TD-ERCS system and wavelet neural networks. Since wavelet neural networks have good capacity to approach arbitrary nonlinear mapping, they can possess chaotic state through studying of TD-ERCS chaotic sequence and modeling. The model system structure of chaotic sequences generator based on wavelet neural networks is shown in Figure 3. The feedback from the WNNs output end to input end shaped closed-loop structure and makes the output chaotic sequence feedback to input end as the initial value for next output sequence, so as to output the chaotic sequences continuously. The training data of WNNs are given by the TD-ERCS sequence. After the weights of WNNs are determined by learning algorithm, chaotic sequence $x(n)$ has been produced.

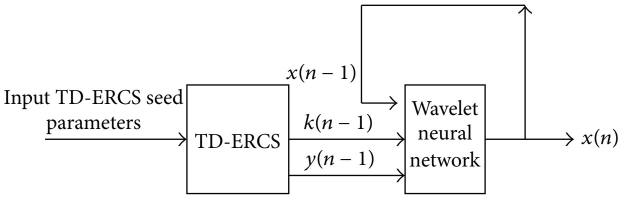


Figure 3: The model system structure of chaotic sequences generator based on WNNs.

4.4. Encryption Algorithm. Assume a square image H consists of $M \times N$ pixels as

$$H = \left\{ h_{ij} \mid 1 \le i \le M, 1 \le j \le N \right\}, \quad (18)$$

where h_{ij} denotes pixel (i, j) of H image. The steps involved in the implementation of our encryption algorithm based on TD-ERCS and WNNs can be summarized as shown below.

Step 1. Set TD-ERCS seed parameters (μ, x_0, α, m) and generate TD-ERCS chaotic sequences x_n, y_n, z_n.

Step 2. Utilize WNNs to practice the chaotic sequences x_n, y_n, z_n and determine the weights of WNNs. The weights of WNNs and TD-ERCS seed parameters (μ, x_0, α, m) are the key and are transmitted to the receiver by secure channel.

Step 3. Calculate the size of the image $m \times n$, and image is changed to one-dimensional vector in the order of rank h_k [23]:

$$k = (i - 1) \cdot n + j \quad 1 \le k \le m \cdot n. \quad (19)$$

Step 4. Use the chaotic sequence generator to produce chaotic sequence $x'(n)$.

Step 5. Select $x'(n)$ as permutation ciphers and calculate image vector C_n by the permutation cryptography process.

Step 6. Generate a new chaotic sequence β_n:

$$\beta_n = \frac{\arccos\left(x'_n\right)}{\pi}, \quad 0 \le \beta_n \le 1, \quad (20)$$

where β_n binary forms are $\beta_n = (0.b_{n1} b_{n2} \cdots b_{np})$, $b_{ij} = \{0, 1\}$, and use β_k sequence to produce B_k:

$$B_k = b_{k1} b_{k2} \cdots b_{kp}. \quad (21)$$

Step 7. Calculate encrypted image vector H_k:

$$H_k = C_k \oplus B_k, \quad (22)$$

where the $\oplus$ means XOR. The encryption process is finished.

The encryption algorithm is a reversible algorithm and the original image can be obtained by applying the inverse process of the encryption algorithm. The secret

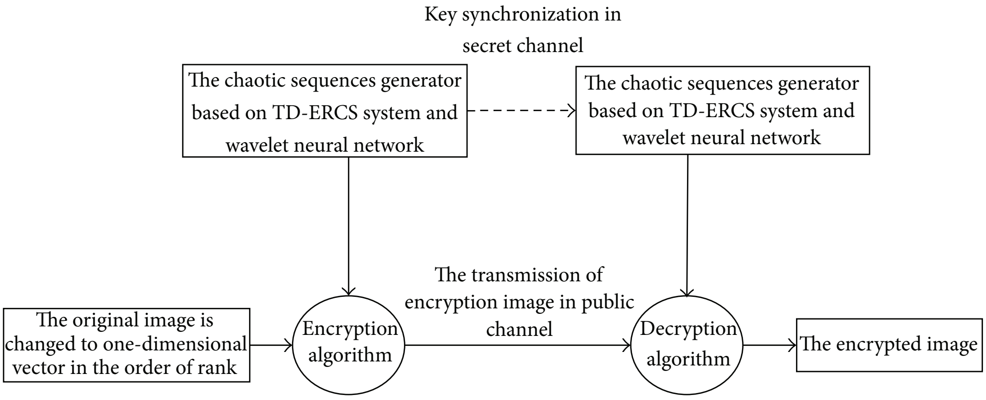
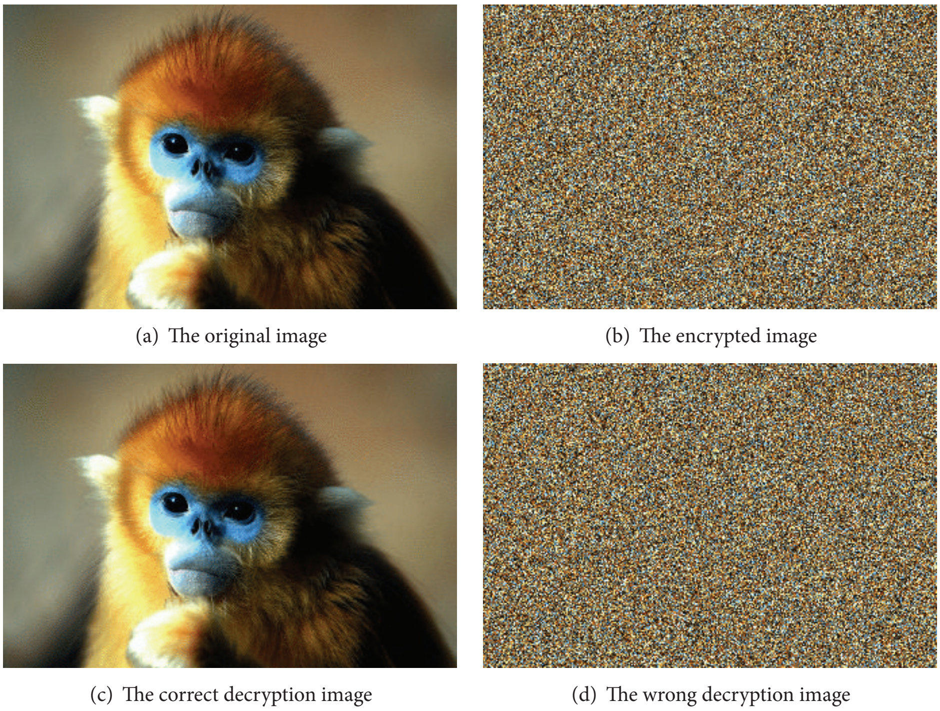

Key synchronization in secret channel
The chaotic sequences generator based on TD-ERCS system and wavelet neural network
The chaotic sequences generator based on TD-ERCS system and wavelet neural network
The transmission of encryption image in public channel
The original image is changed to one-dimensional vector in the order of rank
Encryption algorithm
Decryption algorithm
The encrypted image

Figure 4: The secret communication model of image based on TD-ERCS system and wavelet neural network.


(a) The original image

(b) The encrypted image

(c) The correct decryption image

(d) The wrong decryption image

Figure 5: The results of color image encryption algorithm.

communication model based on TD-ERCS system and wavelet neural network is shown in Figure 4.

5. Experimental Results and Analysis

In the paper, experimental analysis of the proposed image encryption algorithm has been done. The experiment has been implemented in the Matlab 2009a in Figure 5(a). The original image is 256 level grayscale and 225 × 336 size. The structure of WNNs was a three-layer wavelet neural network, in which the number of input layer neurons is three, the number of output layer neurons is one, and the number of hidden layer neurons is six. TD-ERCS system seed parameters are 0.1256, 0.8130, 0.5325, and 2. After 100 times iterations, the cost function E of wavelet neural network was 0.1696. The connection weights of wavelet neural network between input layer and hidden layer are given by

$$W_1 = \begin{bmatrix} 0.5768 & 0.8776 & -0.3325 & -1.0721 & 0.9519 & -0.7115 \\ -0.9919 & -0.5254 & 0.4382 & 0.7774 & -0.0699 & 0.6609 \\ 0.5320 & -1.3329 & 0.0147 & -0.0876 & 0.4870 & -1.106 \end{bmatrix}. \quad (23)$$

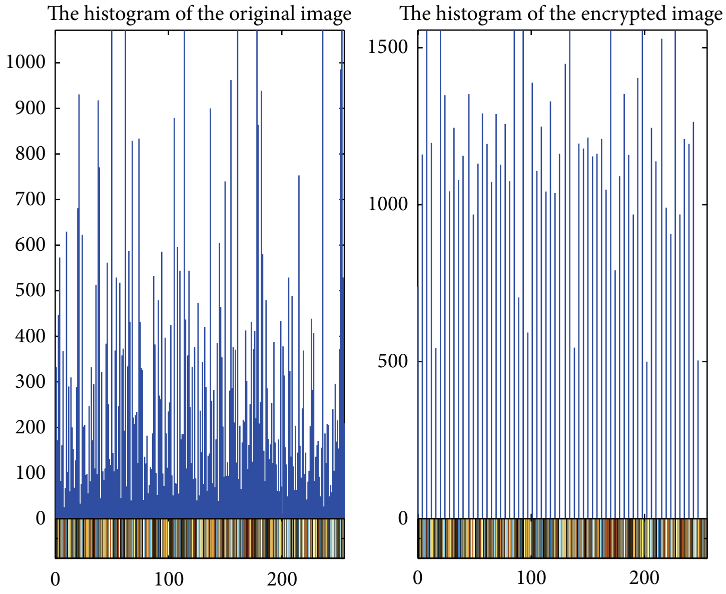


FIGURE 6: The histogram of the original and encrypted image.

The connection weights between hidden layer and output layer are given by

$$W_2 = \begin{bmatrix} -0.0813 \\ 0.7212 \\ 0.4381 \\ 0.2880 \\ 0.2938 \\ -0.2485 \end{bmatrix}. \tag{24}$$

The translation factors vector is given by

$$B = \begin{bmatrix} -0.0679 & 0.1035 & -0.4452 & -1.6843 & -0.0160 & -0.3100 \end{bmatrix}. \tag{25}$$

The expansion and contraction factors vector is given by

$$A = \begin{bmatrix} 0.8826 & -0.2703 & 0.4648 & 0.0897 & 1.5915 & -0.8423 \end{bmatrix}. \tag{26}$$

Lyapunov exponent is a useful way to characterize and quantify chaotic phenomena arising in dynamical systems, which describe the temporal evolution of small perturbations of the initial conditions [24]. The maximum Lyapunov exponent of chaotic sequence is 0.6312 by Wolf's algorithm, and the result shows that the system is chaotic system [25]. The encrypted image is shown in Figure 5(b), which is rough-and-tumble and unrecognizable. As Figure 5(c) shows the decrypted image using the same encryption key is an exact version of the original image. Figure 5(d) shows the error between the original image and decrypted image, which is zero.

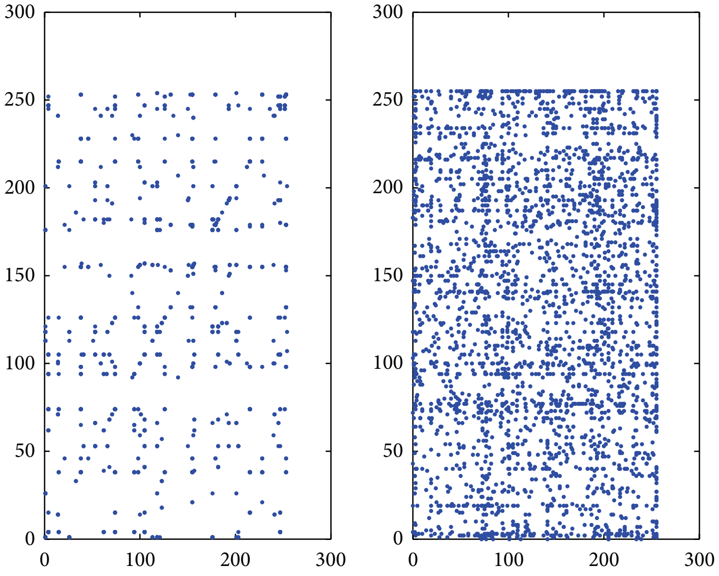
5.1. Key Space Analysis. For a secure image encryption algorithm, the key space should be large enough to make brute-force attacks infeasible [26]. In our algorithm, the TD-ERCS seed parameters and the connection weights of wavelet neural network can be used as keys. If the precision is 10^{-4} in the above test, the key space size is at least 10^{195}. The key space is large enough so that it can resist the exhaustive attack effectively.

5.2. Histograms Analysis. The image histogram is an important statistical characteristic of digital image and can illustrate how pixels in an image are distributed by graphing the number of pixels at each color intensity level [27]. The histograms of the original image and the encrypted image are shown in Figure 6. It is shown that the histogram of the encrypted image is fairly uniform and the encryption algorithm has covered up all the characters of the original image.

5.3. Correlation Coefficient Analysis. In the image data, each pixel is in neighborhood with eight adjacent pixels and is highly correlated with its adjacent pixels [28]. To test the correlation between two vertically adjacent pixels, two horizontally adjacent pixels, and two diagonally adjacent pixels in the encryption image, we randomly select 3015 pairs of two adjacent (in horizontal, vertical, and diagonal direction) pixels from the original and encryption image. Then, calculate their correlation coefficient using the following four formulas [29, 30]:

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

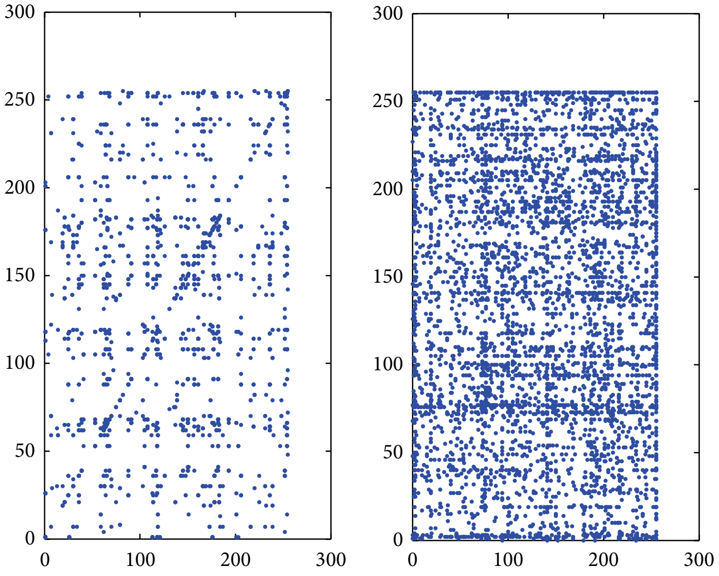
$$D(x) = \frac{1}{N}\sum_{i=1}^{N} [x - E(x)]^2,$$



(a) Original image

(b) Encryption image

Figure 7: The correlation analysis of original and encryption image in horizontal.



(a) Original image

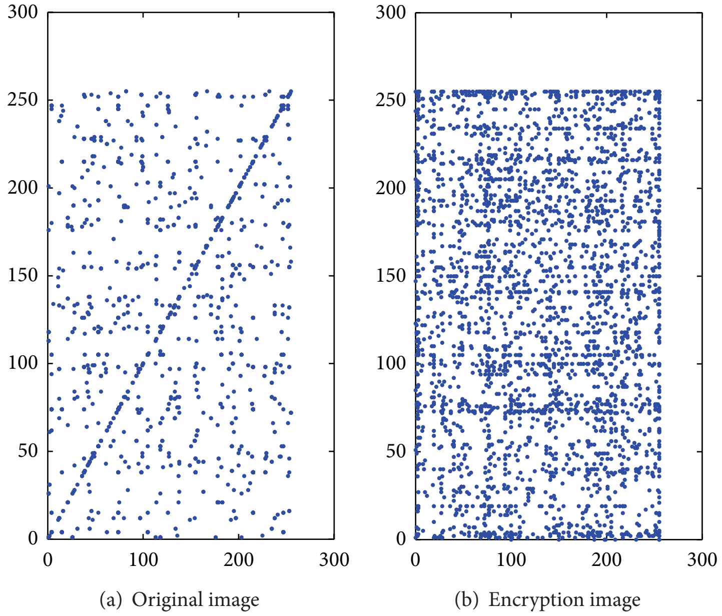
(b) Encryption image

Figure 8: The correlation analysis of original and encryption image in vertical.

$$\mathrm{COV}(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left[x_i - E(x)\right]\left[y_i - E(y)\right],$$
$$r_{xy} = \frac{\mathrm{COV}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \quad (27)$$

where $E(x)$ is the expected value and N is the number of pixels. $D(x)$ is the estimation of variance of x, and $\mathrm{COV}(x,y)$ is the estimation of covariance between x and y, where x and y are grayscale values of two adjacent pixels in the image. The correlation of two adjacent (in horizontal, vertical, and diagonal direction) pixels from the original and encryption image is shown in Figures 7, 8, and 9. Table 1 gives the correlation coefficients of the original image and the encrypted image. The experiment data show that there is a high correlation between the adjacent pixels of the original image. The correlation coefficients of the encrypted image are almost zero, and the adjacent pixels of the encrypted image are almost irrelevant.

5.4. Differential Analysis. In image encryption, the cipher resistance to differential attacks is commonly analyzed via



(a) Original image

(b) Encryption image

Figure 9: The correlation analysis of original and encryption image in diagonal.

Table 1: The correlation coefficients of the original image and the encrypted image.

	Horizontal	Vertical	Diagonal
Original image	0.9998	0.9506	0.9469
Encrypted image	0.0015	0.0096	−0.0140

the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) tests [31]. NPCR and UACI can be mathematically defined by

$$D(i,j)=\begin{cases}0, & \text{if } C^1(i,j)=C^2(i,j)\\ 1, & \text{if } C^1(i,j)\neq C^2(i,j)\end{cases}$$

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

$$\mathrm{UACI}=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(\left(C^1(i,j)-C^2(i,j)\right)/255\right)}{M\times N}\times 100\%, \tag{28}$$

where C^1, C^2 are ciphertext images before and after one pixel change in a plaintext image, respectively. $C^1(i,j)$ are the pixel value at grid (i,j) in C^1. $C^2(i,j)$ are the pixel value at grid (i,j) in C^2. It is clear that NPCR concentrates on the absolute number of pixels which changes value in differential attacks, while the UACI focuses on the averaged difference between two paired ciphertext images [32]. In this paper, the NPCR between the original image and the encryption image is 0.00132%, and the UACI is 0.0000005%. The results demonstrate that the proposed scheme can survive differential attack.

5.5. Key Sensitivity Test.

An ideal image encryption scheme has to be key-sensitive, meaning that a tiny change in the key will produce completely different encrypted image. For testing the key sensitivity of encryption algorithm, this paper has performed sensitivity analysis according to the following steps [33].

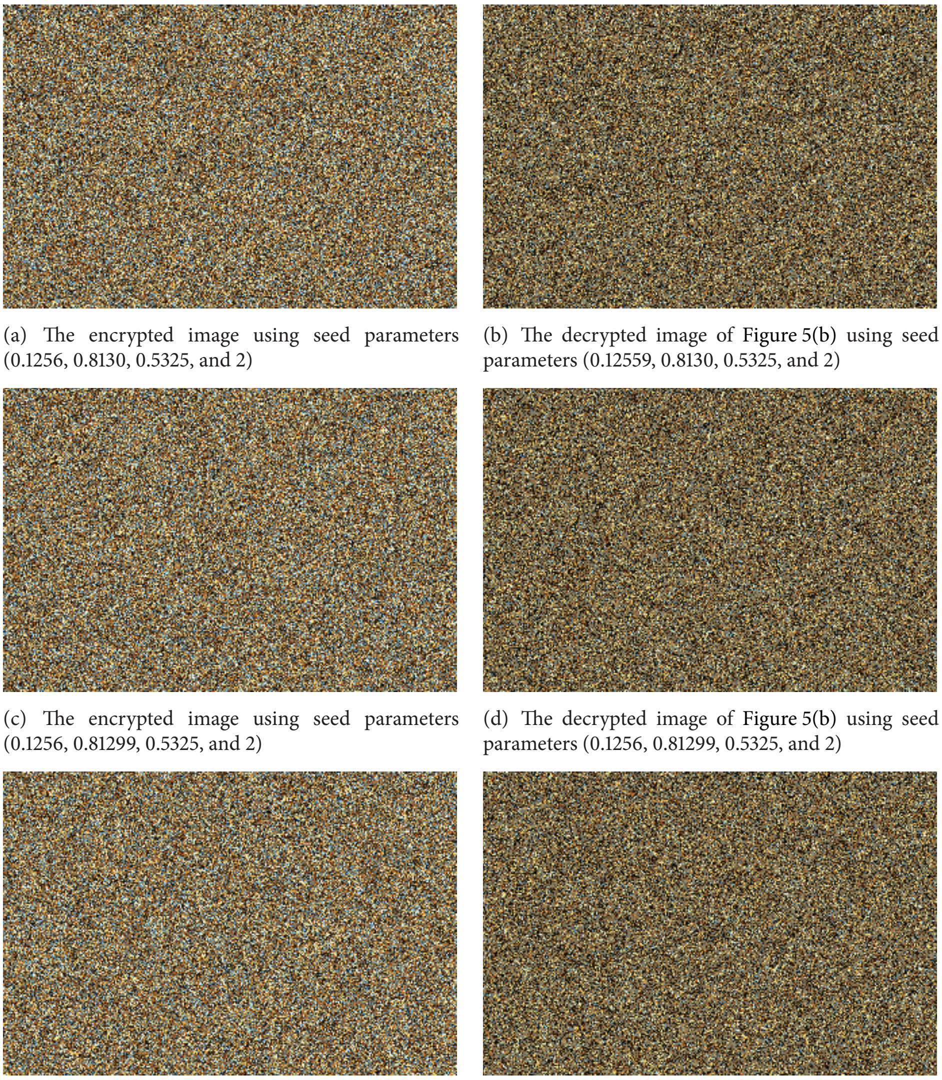
(1) An original image in Figure 5(a) is encrypted by using TD-ERCS system seed parameters (0.1256, 0.8130, 0.5325, and 2) and the resultant image is referred to as encrypted image A as shown in Figure 5(b).

(2) The same original image is encrypted by making the slight modification in the seed parameters (0.12559, 0.8130, 0.5325, and 2). The encrypted image is shown in Figure 10(a) and the decrypted image of image A using seed parameters (0.12559, 0.8130, 0.5325, and 2) is shown in Figure 9(b).

(3) The same original image is encrypted by making slight modification in the seed parameters (0.1256, 0.81299, 0.5325, and 2) and the encrypted image is shown in Figure 10(c). Figure 10(d) has shown the decrypted image of image A using seed parameters (0.1256, 0.81299, 0.5325, and 2).

(4) The same original image is encrypted by making the slight modification in the seed parameters (0.1256, 0.8130, 0.53249, and 2) and the encrypted image is shown in Figure 10(e). Figure 10(f) has shown the decrypted image of image A using seed parameters (0.1256, 0.8130, 0.53249, and 2).

Figure 10 clearly shows that the image A is not correctly decrypted by using TD-ERCS system seed parameters (0.12559, 0.8130, 0.5325, and 2), (0.1256, 0.81299, 0.5325, and 2), and (0.1256, 0.8130, 0.53249, and 2), which has also only one bit difference between the correct key and the wrong key.



(a) The encrypted image using seed parameters (0.1256, 0.8130, 0.5325, and 2)

(b) The decrypted image of Figure 5(b) using seed parameters (0.12559, 0.8130, 0.5325, and 2)

(c) The encrypted image using seed parameters (0.1256, 0.81299, 0.5325, and 2)

(d) The decrypted image of Figure 5(b) using seed parameters (0.1256, 0.81299, 0.5325, and 2)

(e) The encrypted image using seed parameters (0.1256, 0.8130, 0.53249, and 2)

(f) The decrypted image of Figure 5(b) using seed parameters (0.1256, 0.8130, 0.53249, and 2)

Figure 10: Key sensitive test.

6. Conclusion

The TD-ERCS system is a highly complex nonlinear dynamic system based on the physical model of ellipse reflecting cavity. In this paper, an image encryption scheme based on TD-ERCS system and wavelet neural networks is presented. All parts of the proposed encryption algorithm were simulated using computer code. Theoretical and experimental results indicate that the image encryption algorithm based on TD-ERCS system and wavelet neural networks has advantages of large key space and high-level security, while maintaining acceptable efficiency. Finally, the proposed image encryption is suitable for any size digital image and can be widely applied in other information security fields.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This research was partially supported by the National Natural Science Foundation of China (no. 11261001).

References

[1] F. Chiaraluce, L. Ciccarelli, E. Gambi, P. Pierleoni, and M. Reginelli, "A new chaotic algorithm for video encryption," *IEEE Transactions on Consumer Electronics*, vol. 48, no. 4, pp. 838–844, 2002.

[2] Y. Huang, R. Xu, and W. Lin, "An algorithm for JPEG compressing with chaotic encrypting," in *Proceedings of the International Conference on Computer Graphics, Imaging and Visualisation (CGIV '06)*, pp. 137–140, IEEE, July 2006.

[3] H. Bai-Lin, *Starting with Parabolas: An Introduction to Chaotic Dynamics*, Shanghai Scientific and Technological Education Publishing House, Shanghai, China, 1993, (Chinese).

[4] L. Kocarev, M. Sterjev, A. Fekete, and G. Vattay, "Public-key encryption with chaos," *Chaos*, vol. 14, no. 4, pp. 1078–1082, 2004.

[5] R. Matthews, "On the derivation of a "chaotic" encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989.

[6] F. Dachselt and W. Schwarz, "Chaos and cryptography," *IEEE Transactions on Circuits and Systems. I. Fundamental Theory and Applications*, vol. 48, no. 12, pp. 1498–1509, 2001.

[7] G. Alvarez and S. Li, "Breaking an encryption scheme based on chaotic baker map," *Physics Letters A*, vol. 352, no. 1-2, pp. 78–82, 2006.

[8] S. Ke-Hui, T. Guo-Qiang, and S. Li-Yua, "The complexity analysis of TD-ERCS discrete chaotic pseudo-random sequence," *Acta Physica Sinica*, vol. 57, pp. 3359–3366, 2008.

[9] L.-Y. Sheng, G.-Q. Li, and Z.-W. Li, "One-way Hash function construction based on tangent-delay ellipse reflecting cavity-map system," *Acta Physica Sinica*, vol. 55, no. 11, pp. 5700–5706, 2006.

[10] N. F. Güler, E. D. Übeyli, and I. Güler, "Recurrent neural networks employing Lyapunov exponents for EEG signals classification," *Expert Systems with Applications*, vol. 29, no. 3, pp. 506–514, 2005.

[11] L. Chen and K. Aihara, "Chaotic simulated annealing by a neural network model with transient chaos," *Neural Networks*, vol. 8, no. 6, pp. 915–930, 1995.

[12] L. Chen and K. Aihara, "Strange attractors in chaotic neural networks," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 47, no. 10, pp. 1455–1468, 2000.

[13] S. Li-Yuan, S. Ke-Hui, and L. Chuan-Bing, "Study of a discrete chaotic system based on tangent-delay for elliptic reflecting cavity and its properties," *Acta Physica Sinica*, vol. 53, no. 9, pp. 2871–2876, 2004.

[14] L.-Y. Sheng, L.-L. Cao, K.-H. Sun, and J. Wen, "Pseudo-random number generator based on TD-ERCS chaos and its statistic characteristics analysis," *Acta Physica Sinica*, vol. 54, no. 9, pp. 4031–4037, 2005.

[15] R. Q. Quiroga and H. Garcia, "Single-trial event-related potentials with wavelet denoising," *Clinical Neurophysiology*, vol. 114, no. 2, pp. 376–390, 2003.

[16] Y. C. Pati and P. S. Krishnaprasad, "Analysis and synthesis of feedforward neural networks using discrete affine wavelet transformations," *IEEE Transactions on Neural Networks*, vol. 4, no. 1, pp. 73–85, 1993.

[17] A. Subasi, M. Yilmaz, and H. R. Ozcalik, "Classification of EMG signals using wavelet neural network," *Journal of Neuroscience Methods*, vol. 156, no. 1-2, pp. 360–367, 2006.

[18] N. Chauhan, V. Ravi, and D. Karthik Chandra, "Differential evolution trained wavelet neural networks: application to bankruptcy prediction in banks," *Expert Systems with Applications*, vol. 36, no. 4, pp. 7659–7665, 2009.

[19] A. Grossmann and J. Morlet, "Decomposition of Hardy functions into square integrable wavelets of constant shape," *SIAM Journal on Mathematical Analysis*, vol. 15, no. 4, pp. 723–736, 1984.

[20] Q. Zhao, Z. Sun, F. Sun, and J. Zhu, "Appearance-based robot visual servo via a wavelet neural network," *International Journal of Control, Automation and Systems*, vol. 6, no. 4, pp. 607–612, 2008.

[21] A. Mitra, Y. V. S. Rao, and S. R. M. Prasanna, "A new image encryption approach using combinational permutation techniques," *World Academy of Science, Engineering and Technology*, vol. 2, pp. 831–835, 2008.

[22] H. Gao, Y. Zhang, S. Liang, and D. Li, "A new chaotic algorithm for image encryption," *Chaos, Solitons and Fractals*, vol. 29, no. 2, pp. 393–399, 2006.

[23] K. Zhang and X.-A. Fu, "Color image encryption algorithm based on tangent-delay ellipse reflecting cavity map system," in *Proceedings of the International Conference on Image Analysis and Signal Processing*, pp. 25–27, 2012.

[24] C. Dellago and H. A. Posch, "Lyapunov exponents of systems with elastic hard collisions," *Physical Review E*, vol. 52, no. 3, pp. 2402–2406, 1995.

[25] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, "Determining Lyapunov exponents from a time series," *Physica D: Nonlinear Phenomena*, vol. 16, no. 3, pp. 285–317, 1985.

[26] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos," *Physics Letters A*, vol. 372, no. 4, pp. 394–400, 2008.

[27] Y. Mao, G. Chen, and S. Lian, "A novel fast image encryption scheme based on 3D chaotic Baker maps," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 14, no. 10, pp. 3613–3624, 2004.

[28] A. N. Pisarchik and M. Zanin, "Image encryption with chaotically coupled chaotic maps," *Physica D: Nonlinear Phenomena*, vol. 237, no. 20, pp. 2638–2648, 2008.

[29] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[30] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, and A. Akhavan, "A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps," *Physics Letters iA*, vol. 366, no. 4-5, pp. 391–396, 2007.

[31] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos, Solitons & Fractals*, vol. 35, no. 2, pp. 408–419, 2008.

[32] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber Journals*, pp. 31–38, 2011.

[33] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.