Journal of Computers Vol. 32 No. 2, 2021, pp. 108-123
doi:10.3966/199115992021043202010

A Remote Sensing Image Encryption Method Combining Chaotic Neuron and Tent Map

Xitong Xu, Shengbo Chen*

College of Geo-exploration Science and Technology, Jilin University, Changchun 130026, China
xuxitong.2007@163.com

Received 28 April 2020; Revised 11 August 2020; Accepted 15 September 2020

Abstract. Aiming at the characteristics of remote sensing images with large amount of data, and the shortcomings of low-dimensional chaotic systems such as small key space and poor randomness of generated chaotic sequences, chaotic neurons are introduced. Considering that the chaotic sequence generated by flat tent map is more uniform than other chaotic systems and conforms to the two-dimensional characteristics of images, a remote sensing image encryption method combining chaotic neuron and tent map is proposed. The initial key to this method is generated from the plaintext image hash value. This study takes GF-2 multi-spectral image as an example, and the research area selects the area around Songyuan city, covering a variety of ground object types. In the simulation results and comparative analysis, information entropy, gray histogram, correlation coefficient and other indicators are used for comparison and analysis. These operations have fully verified that the method which has good key sensitivity can fully resist differential attacks and other means of cracking, and effectively protect all kinds of information inside the remote sensing images.

Keywords: remote sensing image, encryption, chaotic neuron, flat tent map

1 Introduction

In recent decades, remote sensing technology has experienced rapid development, and remote sensing images have been widely used in various fields. Remote sensing image encryption has become an important research direction. Pixels of digital images have the inherent characteristics of high correlation and data redundancy [1]. On the basis of digital image features, remote sensing images are characterized by large data volume, rich texture details and diversified information. Traditional encryption methods are difficult to meet the needs of remote sensing image encryption. Image encryption is different from text or binary data encryption [2]. Chaotic systems are sensitive to initial conditions and unpredictable. Small changes of initial values make the random sequences generated by chaotic systems completely different [3-5].

A classical encryption scheme used by many researchers consists of two parts: permutation and diffusion [6]. Permutation means to change the relevance of pixels by changing the position of pixels. Diffusion is to use pseudorandom sequence to process the pixel value. Most image encryption methods are based on this encryption method. These encryption methods improve the encryption effect by improving existing chaotic maps or introducing new chaotic maps [7-11].

In the process of encryption, the choice of chaotic map has an important impact on the encryption effect. The randomness of low-dimensional chaotic sequences is relatively poor, so the encryption effect is limited [12-14]. The complexity of high-dimensional chaotic maps computation is very large [15]. In addition, the chaotic sequence used by most encryption methods is not uniform during permutation. Therefore, some pixels are ignored in the process of exchange. Another factor that affects the security of encryption methods is that the encryption methods are not combined with the plaintext images [16].

At present, there are still few encryption methods using different bands of the whole remote sensing

* Corresponding Author

image to verify the encryption effect. Besides, the widely used low-dimensional chaotic sequences with non-uniform distribution and high-dimensional chaotic sequences with large amount of computation are not suitable for remote sensing image encryption. Therefore, this paper proposes an effective remote sensing image encryption method. This method combines flat tent map with chaotic neuron, and uses plaintext images to generate the key to enhance the key sensitivity of the encryption method.

In view of the above, this paper makes the following contributions:

(1) The plaintext images are combined with the key. This method generates a set of keys through the SHA-256 function for initial key selection.

(2) The problem of using non-uniform chaotic sequences is solved. In this paper, the flat tent map is introduced. It is compared with other chaotic maps.

(3) Chaotic neuron is introduced to solve the limitation of high-dimensional chaotic maps. Chaotic sequences generated by chaotic neuron have good randomness and avoid large computation.

(4) The different bands of remote sensing image are used for practical verification. The results fully verify the security and reliability of the encryption method

2 Related Work

Research on remote sensing image encryption is increasing gradually. In recent years, Ye et al. [17] proposed a remote sensing image encryption method using block cipher, but only gray images of size 512×512 are used in the validation. Also, Liu et al. [18] proposed a remote sensing image encryption scheme in DNA rules, but only gray images of size 256×256 and 512×512 are used in the validation. The encryption methods for remote sensing images were not verified in different bands of the whole remote sensing images. A function that can be used to widen the initial value range of one-dimensional chaotic maps was proposed by [12], and a new two-dimensional logistic chaotic map was proposed by [13]. These methods effectively improve the key space and Lyapunov exponent, but the non-uniform distribution of chaotic sequences was not solved. Tong et al. [19] proposed an image encryption scheme using a new high-dimensional chaotic map. This scheme has good encryption effect, but it also generates a lot of computation.

Based on the advantages and disadvantages mentioned above, this paper proposes a remote sensing image encryption method combining chaotic neuron and tent map.

3 Data and Encryption Methods

3.1 Research Data

GF-2 is equipped with two PMS (panchromatic/multi-spectral), including a panchromatic image with spectral range of 0.45-0.90 μm and resolution of 1m, and a multi-spectral image with resolution of 4m consisting of 4 bands: blue (0.45-0.52 μm), green (0.52-0.59 μm), red (0.45-0.69 μm), and near infrared (0.77-0.89 μm) [20].

In this study, the multi-spectral image in GF-2 PMS data on April 14, 2019 was selected as the research data. The image after true color synthesis is shown in Fig. 1, covering the study area around Changling county, Songyuan city, Jilin province. The selected research data covers a variety of ground object types (e.g. residential land, forest land, and water) and can fully verify the security of the encryption method proposed in this paper.

3.2 Chaotic Neuronal Dynamical System

Chaotic neurons are the basic unit of chaotic neural network and the basis of chaotic neural network research [21]. However, chaos neural network has been put forward with a variety of architectural methods, which are widely used in associative memory, combinatorial optimization and other problems [22]. Chen proposed a chaotic neural network model in 1996, which has abundant chaotic dynamics and can overcome the local minimum. Chaotic neural network architecture composed of single chaotic neuron has the same characteristic. When it is always in chaotic state, the generated chaotic sequences can be well used in image encryption [23].

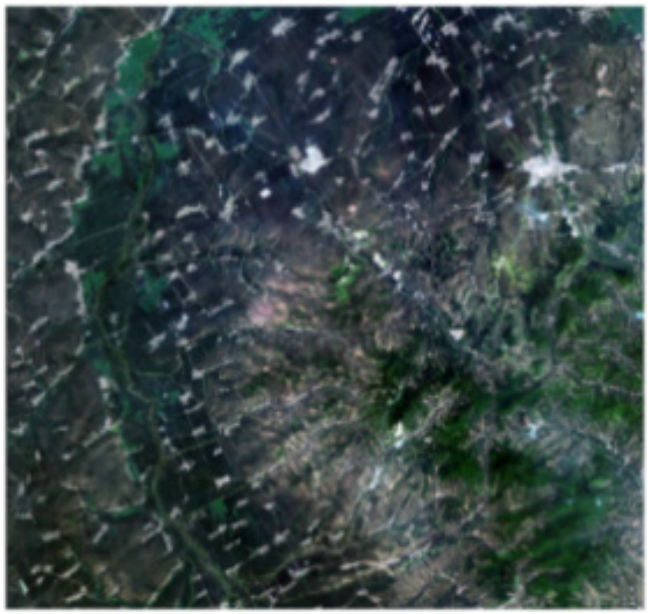


Fig. 1. True color synthesis of GF-2 multi-spectral image

In this paper, the chaotic neuron dynamic system that always remains chaotic state is obtained by improving the chaotic neural network proposed by Chen. The chaotic neuron in Chen chaotic neural network is as follows:

$$\begin{cases} y_i(t+1) = ky_i(t) - z_i(t)(x_i(t) - I_0) \\ x_i(t) = f(y_i(t) = 1/(1+\exp - y_i(t)/\varepsilon) \\ z_i(t+1) = (1-\beta)z_i(t) \end{cases}. \quad \textbf{(1)}$$

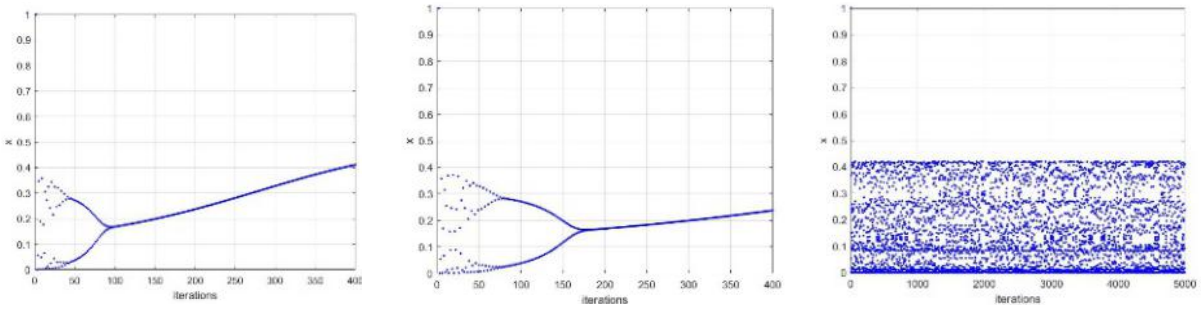
In the formula, x_i and y_i are the input and output of neuron *i* respectively. I_0 is constant, $I_0 > 0$. ε is the steepness parameter of the excitation function, and k is the damping factor, $0 \le k \le 1$. β is the simulated annealing parameter, $0 < \beta < 1$. $z_i(t)$ is a self-feedback term.

With the increase of simulated annealing speed, the former coefficient of self-feedback term decreases, and the time of chaotic neuron in chaotic search state is shorter. Therefore, when the simulated annealing speed is zero, chaotic neuron can be kept in a chaotic state all the time. A chaotic neuron dynamic system that keeps in a chaotic state all the time can be obtained [23]. The chaotic neuron in Chen chaotic neural network is analyzed below.

$\varepsilon = 0.004$, $k = 0.6$, $\beta = 0.01$, $I_0 = 0.1$, $y(0) = 0.3$, $z(0) = 0.1$, respectively. After 400 iterations, the evolution diagram of chaotic neuron is shown in Fig. 2(a). $\varepsilon = 0.004$, $k = 0.6$, $\beta = 0.005$, $I_0 = 0.1$, $y(0) = 0.3$, $z(0) = 0.1$, respectively. After 400 iterations, the chaotic neuron evolution diagram is shown in Fig. 2(b). Both of them enter the inverted bifurcation after several iterations from the chaotic state, and the chaotic phenomenon disappears. With the decrease of β, the annealing speed decreases and the transient chaotic region increases.

If the parameter β is equal to 0, $\varepsilon = 0.004$, $k = 0.6$, $I_0 = 0.1$, $y(0) = 0.3$, $z(0) = 0.1$, respectively. After 400 iterations, the evolution diagram of chaotic neuron is shown in Fig. 2(c). Under this parameter condition, the evolution diagram of Lyapunov exponent is shown in Fig. 3.

It can be concluded from Fig. 2(c) and Fig. 3 that when the simulated annealing speed is zero, Lyapunov is always greater than zero, and chaotic neuron always remains chaotic. The chaotic time series generated by the chaotic neuronal dynamic system have infinite period and good pseudo-randomness. Therefore, the chaotic time series fully meet the requirements of remote sensing image encryption.



(a) $\beta = 0.01$ (b) $\beta = 0.005$ (c) $\beta = 0$

Fig. 2. Chaotic neuron evolution diagram

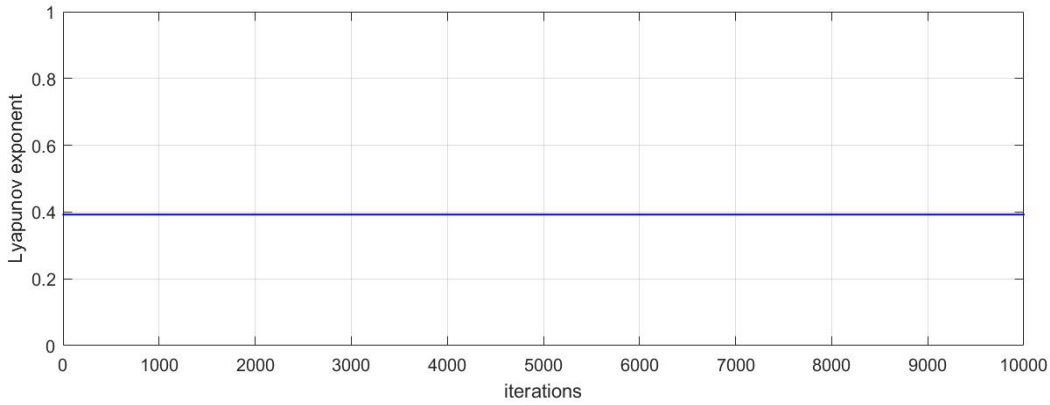


Fig. 3. Lyapunov exponent evolution diagram

3.3 Flat Tent Map

The definition of flat tent map is shown in formula (2).

$$x_{i+1} = \begin{cases} \dfrac{x_i}{\alpha} & x_i \in [0, \alpha] \\ \dfrac{1-x_i}{1-\alpha} & x_i \in [\alpha, 1] \end{cases} \quad y_{j+1} = \begin{cases} \dfrac{y_j}{\beta} & y_j \in [0, \beta] \\ \dfrac{1-y_j}{1-\beta} & y_j \in [\beta, 1] \end{cases} . \tag{2}$$

Formula (2) iteratively produces two chaotic sequences x and y. By combining sequence x with sequence y, a two-dimensional chaotic system can be obtained. The system has the characteristic of uniform distribution [24]. It can achieve a better permutation effect for all pixels of the image during the encryption process.

In order to prove the advantages of flat tent map, the following comparative analysis is made on the distribution uniformity of flat tent map. $\alpha = 0.2$, $\beta = 0.6$, $x_1 = 0.35$, $x_2 = 0.65$. The range of the map is (0,1), and the plane of 1×1 is divided into 100×100 parts. Flat tent map was iterated for 10^6 times, and the number of times falling into each square is shown in Fig. 4.

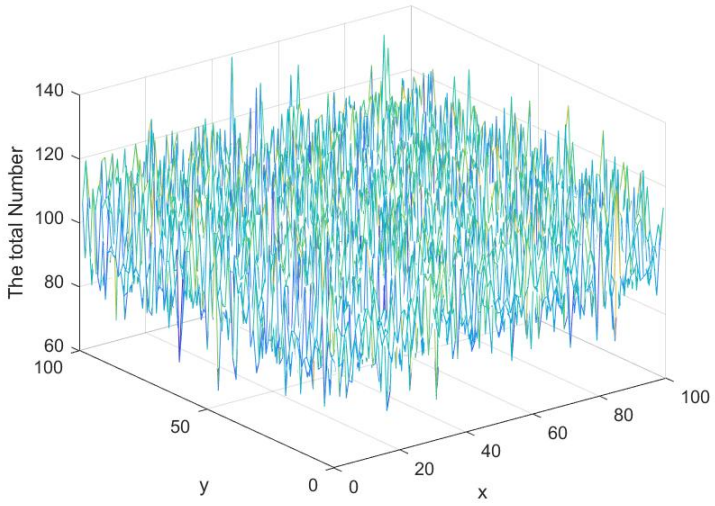


Fig. 4. Flat tent map

Fig. 4 shows that the maximum value is 139 and the minimum value is 66. In addition, the original two-dimensional logistic map and the two-dimensional logistic map for image permutation proposed by [13] are introduced. The original two-dimensional logistic map is defined by

$$\begin{cases} x_{i+1} = \alpha x_i (1 - x_i), x \in (0,1) \\ y_{i+1} = \beta y_i (1 - y_i), y \in (0,1) \end{cases}. \quad \textbf{(3)}$$

Set parameters as follows, $\alpha = 4$, $\beta = 4$, $x_1 = 0.15$, $x_2 = 0.35$. The distribution figure is shown as Fig. 5.

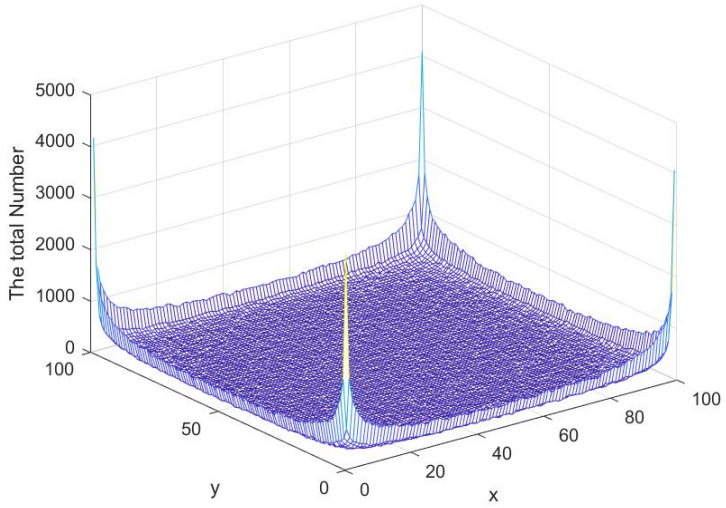


Fig. 5. Original two-dimensional logistic map

Fig. 5 shows that the maximum value is 4154 and the minimum value is 24. The two-dimensional logistic map proposed by [13] is defined by

$$\begin{cases} x_{i+1} = r(3y_i + 1)x_i (1 - x_i), x \in (0,1) \\ y_{i+1} = r(3x_{i+1} + 1)y_i (1 - y_i), y \in (0,1) \end{cases}. \quad \textbf{(4)}$$

Set parameters as follows, $r = 1.19$, $x_1 = 0.8909$, $x_2 = 0.3342$. The distribution figure is shown as Fig. 6.

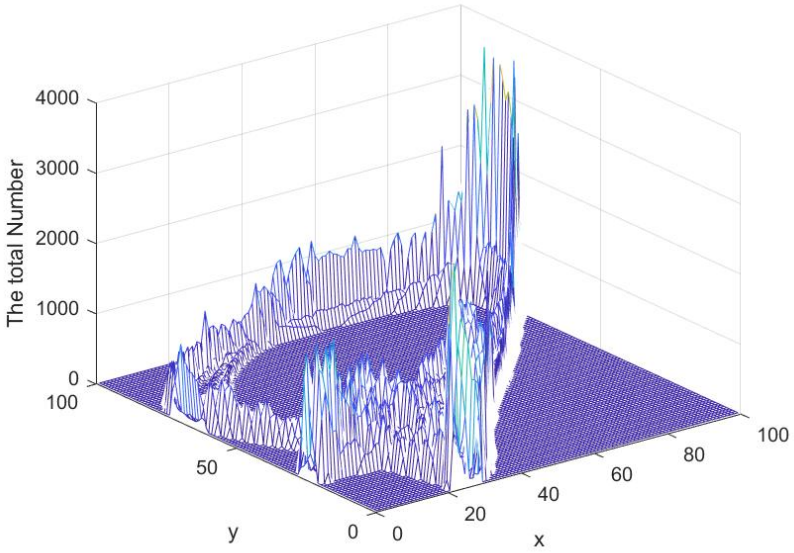


Fig. 6. Two-dimensional logistic map proposed by [13]

Fig. 6 shows that the maximum value is 3931 and the minimum value is 0.

Compared with other chaotic maps, the distribution of flat tent map is more uniform. This ensures that the points in the image are fully transformed during permutation.

3.4 Encryption Process

Step 1: Generate key set

(1) The SHA-256 function is used to calculate the 256-bit hash value of the plaintext image. Denote the hash value as *K*, and divide K into 16 sub-sequences k_i.

$$K = [k_1, k_2, ..., k_{16}]. \tag{5}$$

(2) Convert the subsequence k_i to decimal.

$$k_i = hex2dec(k_i). \tag{6}$$

(3) First, remove the secondary maximum value and the secondary minimum value in the sequence, and then the maximum value $k_{\max}$ and the minimum value $k_{\min}$ in K are selected to normalize other elements in *K*.

$$k_i' = \frac{(k_i - k_{\min})}{(k_{\max} - k_{\min})}. \tag{7}$$

(4) $k_{\max}$ and $k_{\min}$ are not involved in the operation. The sequence K' is composed of the normalized elements. Take K' as the initial key set.

$$K' = [k_1', k_2', ..., k_{12}']. \tag{8}$$

Step 2: The first round of image permutation

(1) The original image size is $M \times N$. Initial parameters α and β of the flat tent map are k_1' and k_1' in the initial key set. k_3' and k_4' are selected from the initial key set as the initial keys.

(2) Take the larger value of *M* and *N*, and set the value as *U*. Iterate the flat tent map $Q_0 + U$ times. *a* and *b* respectively take the last *M* elements and the last *N* elements of two sequences.

(3) The following modifications were made to sequence *a*

$$a' = floor(aM) + 1. \tag{9}$$

(4) permutate image columns, the permutation process is shown in Fig. 7.

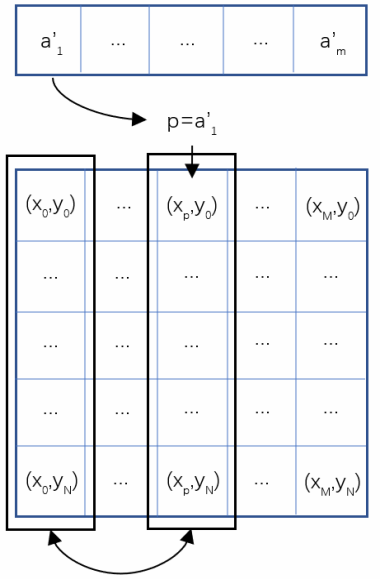


Fig. 7. The permutation process

(5) The following modifications were made to sequence b :

$$b' = floor(bN) + 1. \tag{10}$$

(6) permutate image rows, the permutation process is shown in Fig. 8.

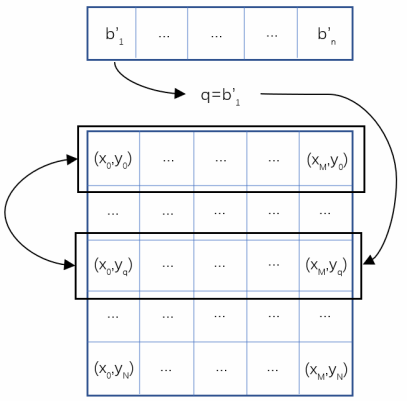


Fig. 8. The permutation process

(7) After the permutation is completed, the permutated image H is obtained.

Step 3: Image diffusion

(1) Parameters ε and β of chaotic neuron are set as the given key: $\varepsilon = 0.04$, $\beta = 0$. Parameters k, I_0, $z(0)$ and $y(0)$ are respectively k_5', k_6', k_7', and k_8' in the initial key set.

(2) The chaotic sequence is generated iteratively by chaotic neuron. The number of iterations is $Q_1 + M \times N$. Q_1 is used to eliminate the transient effect of chaos. And the sequence p takes the last $M \times N$ elements. In order to employ p efficiently, the sequence p is modified as follows:

$$p' = (floor(p) \times 10^8) \bmod 256. \tag{11}$$

(3) After generating sequence p', we employ the formula(11) to diffuse the permutated image H.

$$H' = p' \oplus H. \tag{12}$$

Step 4: The second round of image permutation

(1) Initial parameters α and β of the flat tent map are k_9' and k_{10}' in the initial key set. k_{11}' and k_{12}'

are selected from the initial key set as the initial keys.

(2) Iterate the flat tent map $Q_0 + U$ times. a and b respectively take the last M elements and the last N elements of two sequences. The elements in the two sequences are combined into pairs respectively to generate the corresponding relation with the pixels in the H'.

$$\begin{cases} i = floor(a_m M) + 1 \\ j = floor(b_n M) + 1 \end{cases}. \tag{13}$$

(3) The permutation process is shown in Fig. 9. After the permutation is completed, the cipher image is obtained.

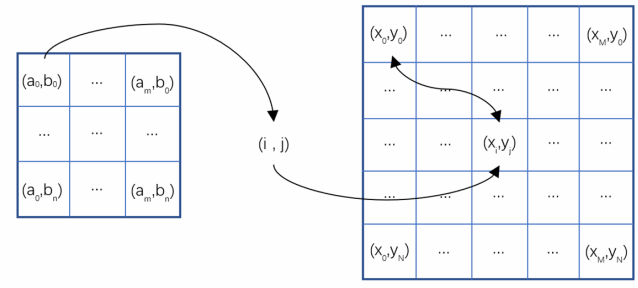


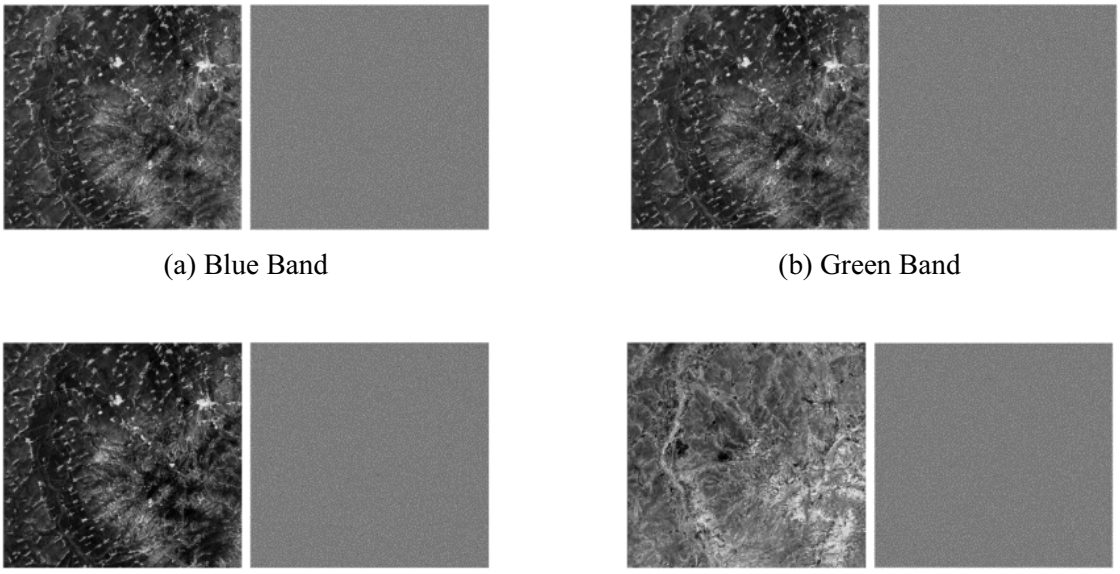
Fig. 9. The permutation process

The decryption process is the reverse process of the encryption process.

4 Simulation Results and Comparative Analysis

4.1 The Simulation Results

In the experiment, the GF-2 multi-spectral remote sensing image of size 6908×7300 was used for simulation under the environment of Matlab2017a. The blue band, green band, red band, and near-infrared band were used as plaintext images, and the encryption effect of the encryption method on the whole remote sensing image was verified, the encrypted images are shown in Fig. 10.



(a) Blue Band (b) Green Band

(c) Red Band (d) Near-infrared Band

Fig. 10. GF-2 remote sensing image of each band plaintext and ciphertext image

4.2 Information Entropy

Information entropy is a measurement standard for the information purity contained in digital images [25]. As the uncertainty of digital image information increases, information entropy will also increase. The calculation formula of information entropy is shown in formula (14):

$$H(x) = -\sum_{i=0}^{n} p(X_i) \log_2 p(X_i). \tag{14}$$

In the formula, n represents the grayscale level of an image, and $p(X_i)$ represents the probability of the grayscale value (X_i). For a completely random image with a grayscale level of 256, the theoretical value of $H(x)$ is 8 [26]. Table 1 records the information entropy of plaintext images and ciphertext images.

Table 1. Information entropy

	Band			
	Blue	Green	Red	Near-infrared
Plaintext image	5.8615	6.1778	6.4496	7.5758
Ciphertext image	7.9994	7.9986	7.9996	7.9999

According to the observation of the data in Table 1, the information entropy of the ciphertext images of different bands encrypted by our method is the maximum value, which is close to the ideal value, and is much better than the encryption results of other chaotic maps.

4.3 Correlation Analysis

As a kind of digital image, remote sensing images show high correlation between adjacent pixels. This is directly related to spectral information, texture information, and other remote sensing information. When adjacent pixels of remote sensing images have strong correlation, remote sensing information can be obtained quickly. Therefore, the correlation coefficient can be used as an important evaluation index to evaluate the degree of hiding remote sensing information [27]. The correlation calculation formula is shown in formula (15):

$$\begin{cases} \bar{x} = \dfrac{1}{N}\sum_{i=1}^{N} x_i \\ D(x) = \dfrac{1}{N}\sum_{i=1}^{N} x_i - \bar{x} \\ \operatorname{cov}(x, y) = \dfrac{1}{N}\sum_{i=1}^{N} (x_i - \bar{x})(y_i - \bar{y}) \\ \rho_{xy} = \dfrac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \end{cases}. \tag{15}$$

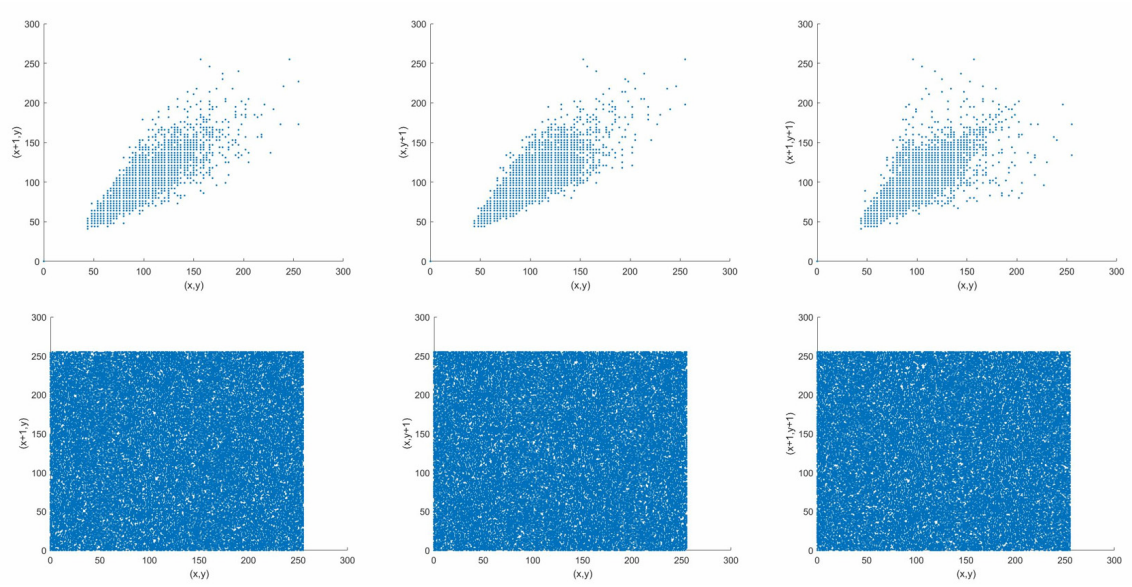
In the formula, x and y are the gray values of adjacent pixels, and ρ_{xy} represents the correlation coefficient between two adjacent pixels. Table 2 lists the correlation coefficients of different methods. In addition, in order to observe the correlation more intuitively, the remote sensing images of the size 256×256 were randomly cropped. The correlation distribution map was made based on them.

Table 2. Comparing the correlation coefficients of different methods

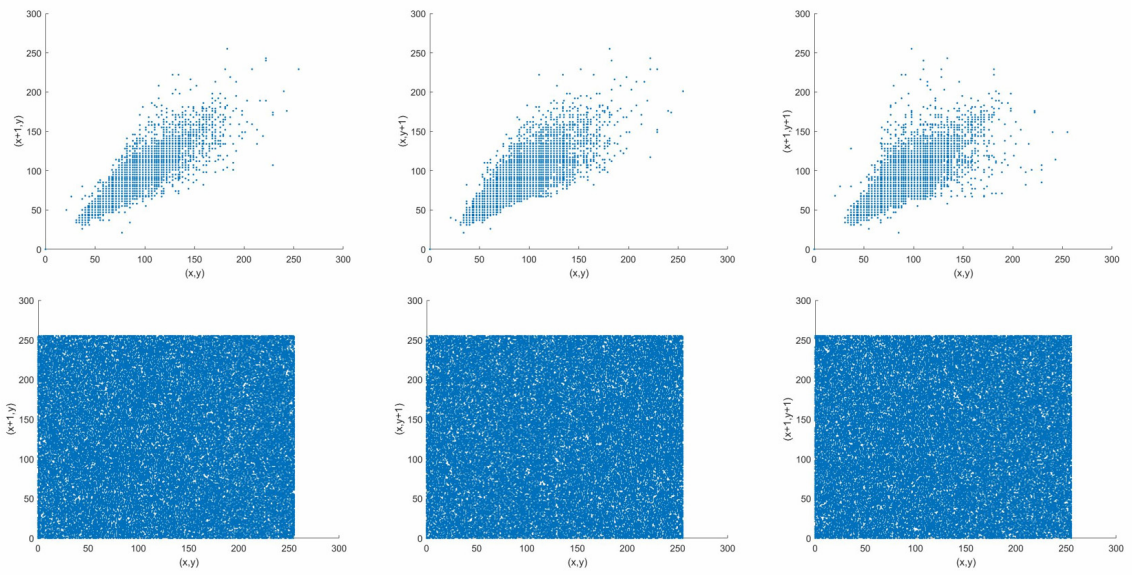
The encryption algorithm		Band			
		Blue	Green	Red	Near-infrared
Plaintext image	Horizontal	0.9569	0.9414	0.9548	0.9232
	Vertical	0.9566	0.9430	0.9543	0.9286
	Diagonal	0.9221	0.8983	0.9173	0.8625

Table 2. Comparing the correlation coefficients of different methods (continue)

The encryption algorithm		Band			
		Blue	Green	Red	Near-infrared
[12]	Horizontal	0.0061	0.0062	0.0059	0.0109
	Vertical	0.0125	0.0133	0.0140	0.0173
	Diagonal	0.0028	0.0030	0.0030	0.0044
[13]	Horizontal	0.0218	0.0210	0.0248	0.0150
	Vertical	0.0053	0.0052	0.0063	0.0032
	Diagonal	0.0124	0.0120	0.0141	0.0085
[14]	Horizontal	0.0064	0.0063	0.0066	0.0072
	Vertical	-0.0417	-0.0426	-0.0556	-0.0201
	Diagonal	0.0031	0.0032	0.0033	0.0029
ours	Horizontal	0.0023	0.0025	-0.0024	0.0020
	Vertical	0.0001	0.0002	0.0002	0.0003
	Diagonal	0.0001	0.0001	0.0001	0.0001

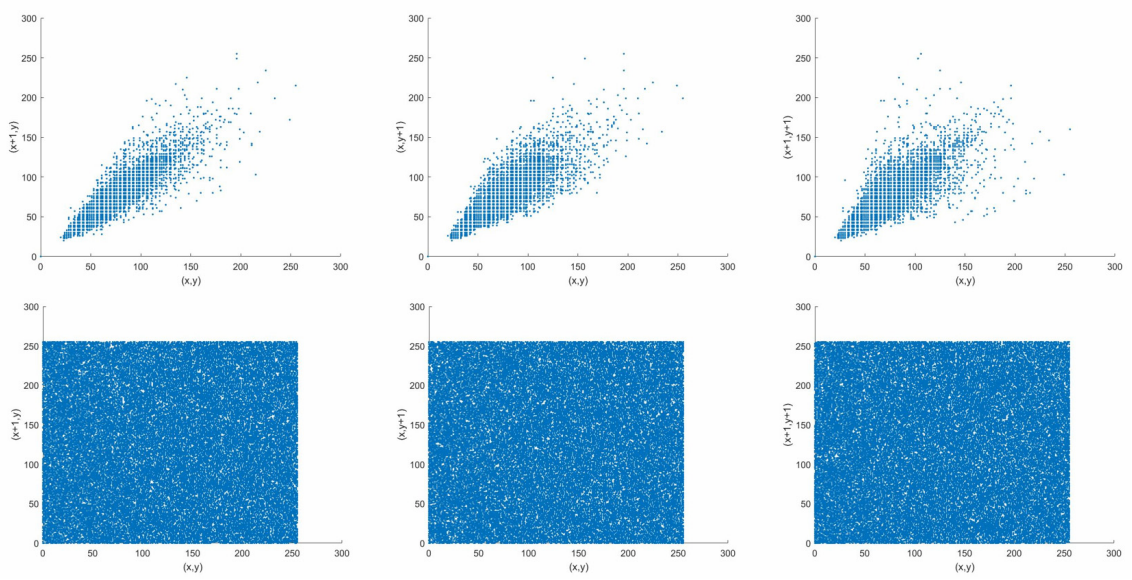


(a) Blue band

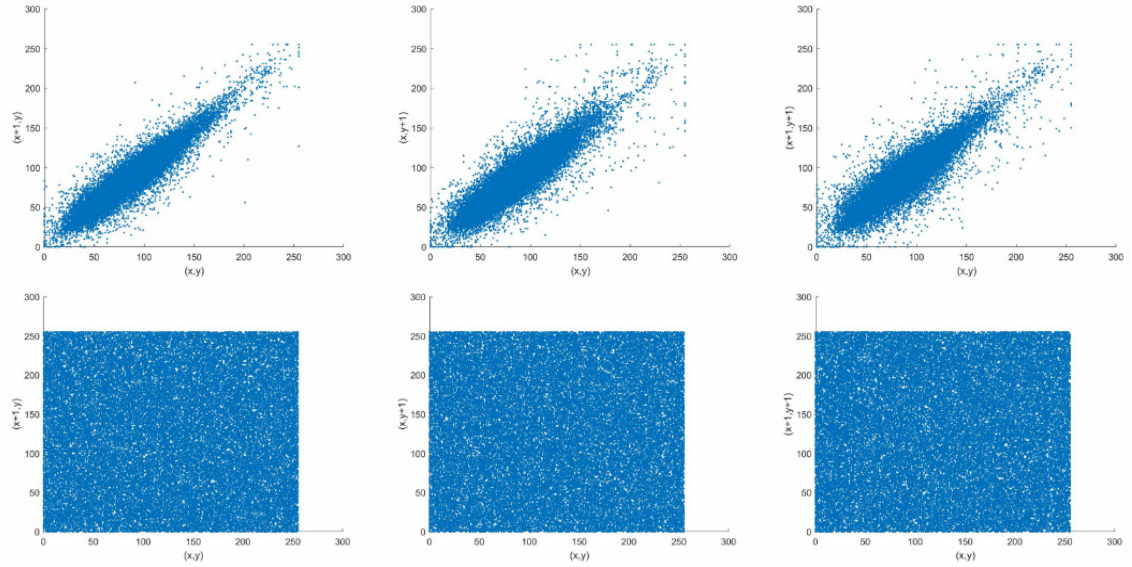


(b) Green band

Fig. 11. Correlation distribution of plaintext image and ciphertext image in horizontal, vertical and diagonal directions



(c) Red band



(d) Near-infared band

Fig. 11. Correlation distribution of plaintext image and ciphertext image in horizontal, vertical and diagonal directions (continue)

According to Table 2 and Fig. 11, it can be concluded that our method achieves the best encryption effect.

4.4 Histogram Analysis

Grayscale histogram refers to the number of times each gray value appears in the grayscale image, so as to reflect the occurrence frequency of different grayscale levels in the grayscale image. The gray histograms calculated from different images is shown in Fig. 12.

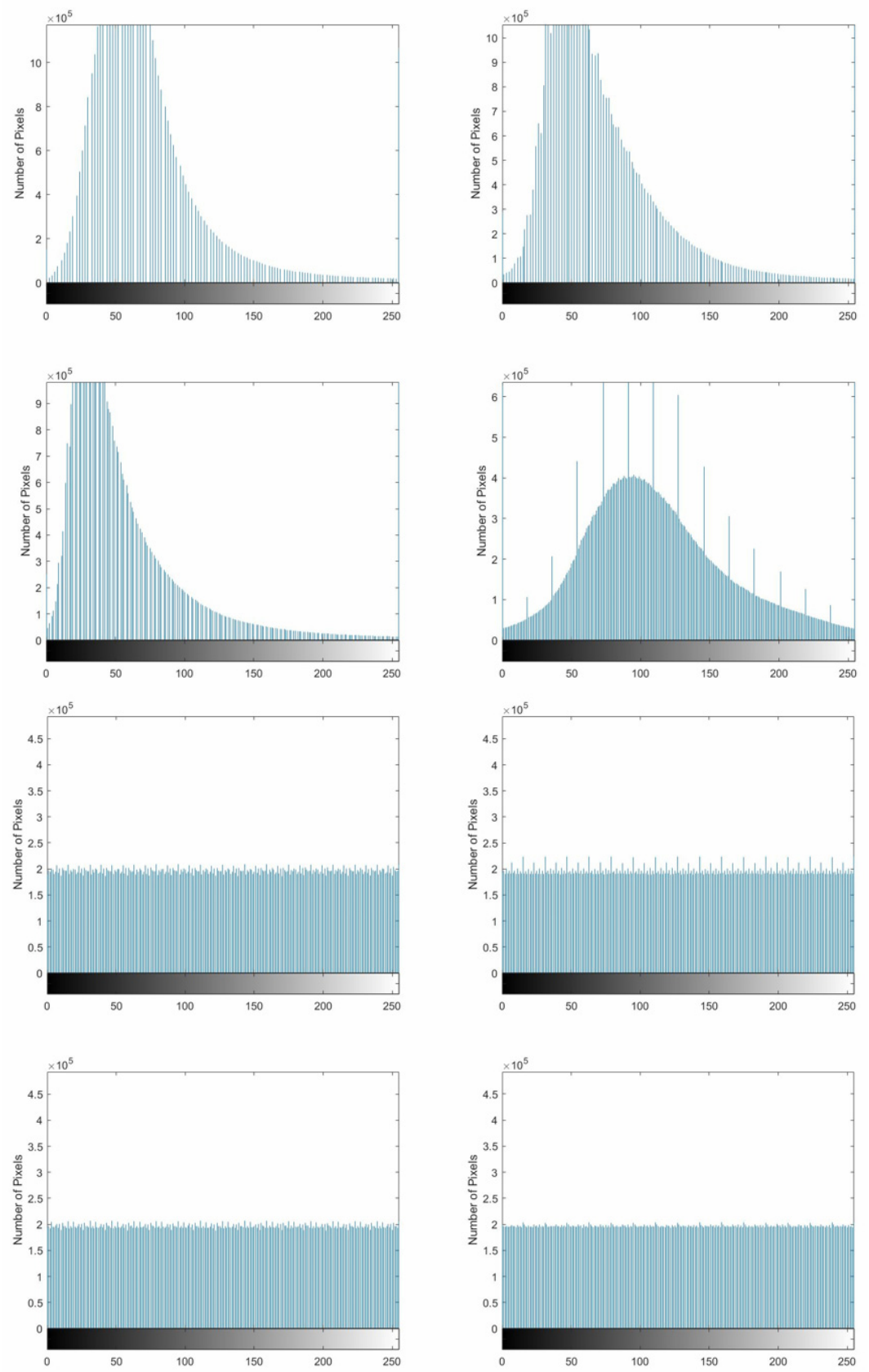


Fig. 12. Gray histogram of plaintext and ciphertext in blue band, green band, red band and near-infrared band

According to Fig. 12, it can be concluded that the gray distribution of the ciphertext image has reached good equilibrium state. The encryption method effectively hid the information distribution characteristic of different bands of the remote sensing image.

4.5 Resistance to Differential Attack Analysis

Differential attack is a method to decipher codes by comparing the differences and similarities between the modified ciphertext and the original ciphertext. Therefore, the ability to resist differential attack is an important criterion to measure the effectiveness of encryption. In this experiment, the number of pixel change rate (NPCR) and unified average changing intensity (UACI) were used to quantitatively analyze the ability to resist differential attack [28].

Under ideal conditions, the NPCR value is 0.9961 and the UACI value is 0.3346. The closer the calculated result is to the ideal value, the better the encryption method can resist differential attack. The calculated values of NPCR and UACI are shown in Table 3.

Table 3 shows that NPCR and UACI are close to ideal values This indicates that the encryption method can resist differential attack.

Table 3. The NPCR and UACI of different bands after individual pixel was modified

Band	NPCR (%)	UACI (%)
Blue	99.5125	33.4716
Green	99.5127	33.4654
Red	99.5113	33.4622
Near-infrared	99.5121	33.4636

4.6 Key Sensitivity Test

Key sensitivity is to make small changes to the keys and then decrypt the image. In addition, in order to quantitatively judge the difference between correctly decrypted image and incorrectly decrypted image, mean square error is introduced to measure the grayscale change between images [29]. $D(i, j)$ is defined as the changed image, and $B(i, j)$ is the original image. Mean square error E_{MS} is calculated as formula (16).

$$E_{MS} = \frac{1}{M \times N} \sum_{i=1}^{m} \sum_{j=1}^{N} [D(i, j) - B(i, j)]^2 .. \quad \textbf{(16)}$$

In the formula, M and N are the number of rows and columns of the matrix respectively.

In the experiment, the mean square error of the original images, the encrypted images, the correctly decrypted images and the incorrectly decrypted images in different bands of the remote sensing image were calculated, and the results are listed in Table 4.

Table 4. Gray mean square deviation

$P(i, j)$	$D(i, j)$	E_{MS}
Plain image of blue band	Cipher image	10471.69
	Decrypted image	0
	Error decryption image	10472.11
Plain image of green band	Cipher image	10724.45
	Decrypted image	0
	Error decryption image	10722.18
Plain image of red band	Cipher image	12711.26
	Decrypted image	0
	Error decryption image	12710.90
Plain image of near-infrared band	Cipher image	87784.67
	Decrypted image	0
	Error decryption image	87839.65

According to Table 4, Correct decryption is only possible with the correct key. The mean square error of the error decrypted images is almost the same as the mean square of the encrypted images, so it is impossible to obtain effective information from the error decrypted images.

4.7 Key Space Analysis

The key space is an intuitive embodiment of the effectiveness and security of the encryption method. The chaotic system is very sensitive to parameters. When the initial condition changes slightly, the chaotic system will change greatly. Therefore, the key space is closely related to the security of encryption. The initial key of the method in this paper is generated by the plaintext hash value, and the key also includes the initial control parameters of chaotic neuron. In this case, even if the individual pixel values change very little, the initial conditions change a lot. In general, the encryption method can resist brute-force attack.

5 Discussion

This paper proposed a novel remote sensing image encryption method combining chaotic neuron and tent map. We analysis the security of the method from several aspects, including information entropy, correlation analysis, histogram analysis, differential attack analysis and key sensitive analysis. The experimental results prove the method can resist various existing attack schemes against remote sensing images.

In order to verify the true effect of the encryption method, the proposed method was used to encrypt different bands of GF-2 remote sensing image. This is a part that has not been verified with many remote sensing image encryption methods. Table 1 shows the information entropy of different bands after encryption, and Fig. 12 shows the gray histogram of plaintext images and ciphertext images. These prove that the encryption method can ensure the information of remote sensing image can not be leaked. Table 2 compares the proposed encryption method with other methods in terms of correlation coefficient. The correlation coefficient reflects the degree of correlation between adjacent pixels in different directions. Therefore, the correlation coefficient is the key index to test the encryption effect. The proposed method achieves the minimum in all directions of different bands. In both horizontal and vertical directions, the encryption effect of our method is greatly improved compared with other methods. This proves that our method is suitable for remote sensing images with a large amount of information. Table 3 gives the average NPCR and UACI for differential attack, the results of different bands all approach the ideal value. The results show that the proposed method has acceptable ability against differential attack. Table 4 shows that minor changes in the keys will lead to incorrect decryption, while correct decryption can completely restore the information in the remote sensing images.

6 Conclusion

In this paper, a remote sensing image encryption method combining chaotic neurons and flat tent map is proposed. This method is used to encrypt multiple bands of GF-2 remote sensing image multi-spectral data. Due to the large amount of remote sensing image data and the rich information of remote sensing image, the encryption performance of chaotic system can be more accurately reflected. This study proves the security and effectiveness of the proposed method. In addition, compared with the complex image encryption process, the method is more suitable for the remote sensing image encryption. Besides, in the experimental verification process, the encryption method is compared with other low-dimensional chaotic map encryption methods which are often used for image encryption. This further verifies the security and feasibility of the remote sensing image encryption method proposed by our study. It also provides some reference for the research of remote sensing image encryption.

Remote sensing images contain high-frequency information and low-frequency information. Low-frequency information refers to the subject feature, and high-frequency information refers to texture information. For remote sensing images, encrypting two types of information separately may get better effect. However, the proposed method does not consider the two types of information. In future, we plan to decompose the information of remote sensing images and encrypt different information separately.

Acknowledgments

This work is supported by Jilin province and Jilin university co-building project (SXGJXX2017-2) and the program for JLU science and technology innovative research team (JLUSTIRT, 2017TD-26).

References

[1] Y. Zhang, The unified image encryption algorithm based on chaos and cubic S-Box, Information Sciences, 50(6)(2018) 361-377.

[2] Y.-G. Yang, J. Tian, H. Lei, Y.-H. Zhou, W.-M. Shi, Novel quantum image encryption using one-dimensional quantum cellular automata, Information Sciences, 345(2016) 257-270.

[3] Y. Liu, X.-J. Tong, J. Ma, Image encryption algorithm based on hyperchaotic system and dynamic S-box, Multimedia Tools and Applications 75(13)(2015) 7739-7759.

[4] H.-J. Liu, X.-Y. Wang, Triple-image encryption scheme based on one-time key stream generated by chaosand plain images, Journal of Systems and Software 86(3)(2013) 826-834.

[5] A. Kumar, M.K. Ghose, Extended substitution-diffusion based image cipher using chaotic standard map, Communications in Nonlinear Science and Numerical Simulation 16(1)(2011) 372-382.

[6] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, International Journal of Bifurcation and Chaos 8(1998) 1259-1284.

[7] J.-X. Chen, Z.-L. Zhu, C. Fu, H. Yu, L.-B. Zhang, A fast chaos-based image encryption scheme with adynamic state variables selection mechanism, Communications in Nonlinear Science and Numerical Simulation 20(2015) 846-860.

[8] X.-J. Tong, The novel bilateral-diffusion image encryption algorithm with dynamical compound chaos, Journal of Systems and Software 85(2012) 850-858.

[9] X.-L. Chai, An image encryption algorithm based on bit level Brownian motion and new chaotic systems, Multimedia Tools and Applications 76(1)(2015) 1-17.

[10] H. Hsiao, J. Lee, Color image encryption using chaotic nonlinear adaptive filter, Signal Processing 117(2015) 281-309.

[11] J.S. Armand Eyebe Fouda, J.Yves Effa, M. Ali, Highly secured chaotic block cipher for fast image encryption. Applied Soft Computing 25(2014) 435-444.

[12] C. Pak, L.-L. Huang, A new color image encryption using combination of the 1D chaotic map, Signal Processing 138(9) (2017) 129-137.

[13] Y. Wu, G.-L. Yang, H.-X. Jin, P.N. Joseph, Image encryption using the two-dimensional logistic chaotic map, Journal of Electronic Imaging 21(1)(2012) 013-014.

[14] Y.-G. Su, C. Tang, X. Chen, B.-Y. Li, W.-J. Xu, Z.-K. Lei, Cascaded Fresnel holographic image encryption scheme based on a constrained optimization algorithm and Henon map, Optics and Lasers in Engineering 88(1)(2017) 20-27.

[15] Q.-Y. Xu, K.-H. Sun, C. Cao, C.-X. Zhu, A fast image encryption algorithm based on compressive sensing and hyperchaotic map, Optics and Lasers in Engineering 121(10)(2019) 203-214.

[16] S.-J. Li, C.-Q. Li, G.-R. Chen, N.G. Bourbakis, K.T. Lo, A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks, Signal Processing: Image Communication 23(2008) 212-223.

[17] G.-D. Ye, X.-L. Huang, A novel block chaotic encryption scheme for remote sensing image, Multimedia Tools and Applications 75(2016) 11433-11446.

[18] H. Liu, B. Zhao, L.-Q. Huang, A remote-sensing image encryption scheme using DNA bases probability and two-dimensional logistic map, IEEE Access 7(2019) 65450-65459.

[19] X.-J. Tong, Z. Wang, M. Zhang, Y. Liu, H. Xu, J. Ma, An image encryption algorithm based on the perturbed high-dimensional chaotic map, Nonlinear Dynamics 80(2015) 1493-1508.

[20] China resources satellite application center, Gaofen-2 [EB/OL], <http://www.cresda.com/CN/Satellite/3128.shtml>, 2014 (accessed 20.03.30)

[21] M. Inoue, S. Fukushima, A neural network of chaotic oscillators, Progress of Theoretical Physics 87(3)(1992) 771-774.

[22] Z.-Q. Hu, W.-J. Li, J.-F. Qiao, Variable frequency sinusoidal chaotic neural network and application, Journal of Physics 66(09)(2017) 17-27.

[23] Y.-S. Wang, Research on chaos algorithm in digital image encryption, [dissertation] University of Electronic Science and Technology, 2011.

[24] H.-L. Qin, X.-B. Li, A chaotic global optimal search method based on tent map, Journal of Electrical Machinery and Control 008(001)(2004) 67-70.

[25] H. Shi, Wang Lidan, Multi-process image encryption scheme based on compressed sensing and multi-dimensional chaotic system. Journal of Physics 68(20)(2019) 39-52.

[26] J. Wang, G.-P. Jiang, Security analysis and improvement of a hyperchaotic image encryption algorithm, Journal of Physics 60(06)(2011) 83-93.

[27] M.K. Mandal, M. Kar, S.K. Singh, V.K. Barnwal, Symmetric key image encryption using chaotic Rossler system, Security and Communication Networks 7(2014) 2145-2152.

[28] S. Behnia, A. Akhshani, H. Mahmodi, A. Akhavan, A novel algorithm for image encryption based on mixture of chaotic maps, Chaos, Solitons and Fractals 35(2)(2008) 408-419.

[29] G.-Y. Jiang, D.-J. Huang, X. Wang, M. Yu, Research Progress of Image Quality Evaluation Method. Journal of Electronics and Information 032(001)(2010) 219-226.