

Research on reversible information hiding algorithm of remote sensing image based on generative countermeasure network

Yang Haitao, Changgong Zhang, Jinyu Wang*

School of Aerospace Information, University of Aerospace Engineering, 101416, Beijing, China
812548088@qq.com

Abstract: The reversible information of the remote sensing image of the generative countermeasure network is encrypted and hidden, so as to improve the security performance of the remote sensing image transmission of the generative countermeasure network. A reversible information hiding method for remote sensing images based on block cascade chaotic fitness control is proposed. In a chaotic system, reversible information random coding transmission control protocol construction and random decryption protocol calculation are carried out on reversible information of the remote sensing image of the generative countermeasure network, chaotic mapping decomposition is carried out on the remote sensing image of the generative countermeasure network to be hidden to obtain three gray-scale images, block key matching and random coding are respectively carried out on the three images by using multidimensional Logistics chaotic mapping to generate an image Gaussian random pixel sequence, The features of the coded output generative countermeasure network remote sensing image are recombined by pixel edge scrambling method, and the hidden key is generated under the reversible information random coding transmission control protocol, thus realizing reversible information hiding of the generative countermeasure network remote sensing image. Simulation results show that this method has strong pixel decorrelation, large key space, improved reversible information hiding degree, strong anti-attack ability and good encryption and hiding performance.

Keywords: generative countermeasure network; Remote sensing image; Reversible information; hide

1. Introduction

With the maturity of remote sensing imaging technology, 3D remote sensing radar image plotting method is used to obtain 3D geographic and object information, which is widely used in resource exploration, urban planning, agricultural development and other fields. Three-dimensional remote sensing detection imaging uses radar remote sensing pulses working in infrared and visible light bands to scan three-dimensional images. Remote sensing image detectors turn electrical pulses into light pulses and send the scanned radar imaging results to a display, thus realizing digital surface imaging with low cost, high density, high speed and high precision, which constitutes a generative countermeasure network. The reversible information of remote sensing images is transmitted in cyberspace and shared and used by users. However, for some reversible information of generative countermeasure network remote sensing images with strong security and confidentiality, it is necessary to encrypt and hide them in storage and dissemination, otherwise, military secrets and national geographic information secrets will be leaked, etc. With the expansion of the application direction of reversible information of generative countermeasure network remote sensing images, people pay great attention to the security problems in storage and dissemination [2], and the research on encryption and hiding of reversible information of generative countermeasure network remote sensing images has become a hot spot in information security research.

At present, most of the encryption and cognition methods for reversible information of remote sensing images of generative countermeasure network adopt the image encryption method based on a single chaotic system or a simple chaotic system [3]. Through the nonlinear feature decomposition and chaotic feature mapping reconstruction of image pixels, the vector quantization method is used for image pixel correlation coding [4], and the sensitive key of image encryption is constructed to realize the encryption and decryption algorithm design. However, because a single chaotic system is adopted, It is easy to have the problems of insufficient key space and low complexity of encryption key sequence, which leads to poor encryption. For this reason, the related literature has improved the design

of image encryption algorithm. Among them, a hologram encryption algorithm based on Gyrator transform is proposed in literature [5], which constructs a binary random phase template in image encryption, uses spatial hiding algorithm to quantify the gray value of the host image, and uses reference beam incident angle multiplexing method to realize sensitive key encryption of hologram, which has good encryption performance, but the algorithm calculates Literature [6] proposes a Fourier transform holographic multi-image encryption method under spherical wave illumination, which has good encryption performance for the original image to be encrypted on the input surface illuminated by spherical wave emitted by point light source, and reduces the number of templates used in the encryption system, but the real-time encryption of the interference image in the output field is not good. Literature [7] proposes an image compression and encryption algorithm based on the combination of DCT transform and DNA operation. Firstly, discrete cosine transform compression and Chen chaotic system are used to scramble the image, and hyperchaotic mapping is used to encode and fuse the image pixel features, which improves the insensitivity of the encrypted hidden image to the original image and solves the problems of large amount of data and slow transmission rate after image encryption, but it cannot solve the problems of small key space and low security of the image encryption and hiding algorithm. To solve the above problems, this paper proposes a reversible information hiding method for remote sensing images based on block cascade chaotic fitness control^[8]. In a chaotic system, reversible information random coding transmission control protocol construction and random decryption protocol calculation are carried out on reversible information of the remote sensing image of the generative countermeasure network, chaotic mapping decomposition is carried out on the remote sensing image of the generative countermeasure network to be hidden to obtain three gray-scale images, block key matching and random coding are respectively carried out on the three images by using multidimensional Logistics chaotic mapping to generate an image Gaussian random pixel sequence, The features of the generated network remote sensing image are recombined by pixel edge scrambling method, and the hidden key is generated under the reversible information random coding transmission control protocol, so as to realize the reversible information hiding of the generated network remote sensing image. Finally, the experimental test and analysis are carried out, and the validity conclusion is obtained.

2. Construction of reversible information random coding transmission control protocol based on chaotic system and decomposition of chaotic map

2.1 Construction of reversible information random coding transmission control protocol based on chaotic system

In the chaotic system, the reversible information random coding transmission control protocol of the reversible information of the generative countermeasure network remote sensing image is constructed. Logistic chaotic system^[9], Hyperhenon chaotic system, Lorenz chaotic system and piecewise linear chaotic mapping system are respectively used to construct the reversible information random coding transmission control protocol model of the reversible information of the generative countermeasure network remote sensing image. Chaotic motion is a seemingly random dynamic model which obeys the deterministic law, which was discovered by American meteorologist E. Lorenz in 1963. It can be effectively used in image encryption. Logistic chaotic time series under continuous self-mapping on closed interval I is described as follows:

$$x_{n+1} = \mu x_n (1 - x_n) \quad (0 < x_n < 1) \quad (1)$$

Logistic chaos is used as continuous self-mapping for pixel value feature decomposition of reversible information of network remote sensing image, and the image is divided into 8pixel × 8pixel sub-blocks. In the matrix coordinate position of the image, Hyperhenon chaotic map is used to scramble the two-dimensional plaintext image of reversible information of network remote sensing image. Hyperhenon chaotic map is defined as:

$$\begin{cases} X_{k+1} = c - Y_{k+1}^2 - d \cdot Z_{k+1} \\ Y_{k+1} = X_k \\ Z_{k+1} = Y_k \end{cases} \quad k = 0, 1, 2, \dots \quad (2)$$

When $c = 1.76$, $d = 0.1$, the system is in hyperchaotic state, and the hyperchaotic sequence is constructed by the key stream sensitive domain characterization method. The row-column permutation mapping of reversible information of the generated network remote sensing image is obtained by using

the sum of two sets of random numbers generated by Logistic chaotic mapping and additional key rotation as follows:

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = \rho x - y - xz \\ \dot{z} = xy - \beta z \end{cases} \quad (3)$$

The Lorenz high-dimensional system is used to calculate the hash of the image reversible information random coding transmission control protocol, and the image reversible information random coding transmission control protocol is constructed by processing a packet with a length of 512bit each time. In the hash calculation of the image reversible information random coding transmission control protocol, the hash value $H_0^{(0)}$, $H_1^{(0)}$, $H_2^{(0)}$, $H_3^{(0)}$, $H_4^{(0)}$ and the 512-bit packet message are used as input messages in each cycle, and the Logistic chaotic map is used for pixel scrambling processing^[10]. Based on four stages and 20 rounds of operation, the hexadecimal expression of the reversible information random coding transmission control protocol based on chaotic system is obtained as follows:

$$H_0^{(0)} = 0x67452301 ; H_1^{(0)} = 0xEFCDA89 ; H_2^{(0)} = 0x98BADCFE ; H_3^{(0)} = 0x10325476 ; H_4^{(0)} = 0xC3D2E1F0$$

To sum up, the calculation process of random decryption protocol constructed by reversible information random coding transmission control protocol based on chaotic system is shown in Figure 1.

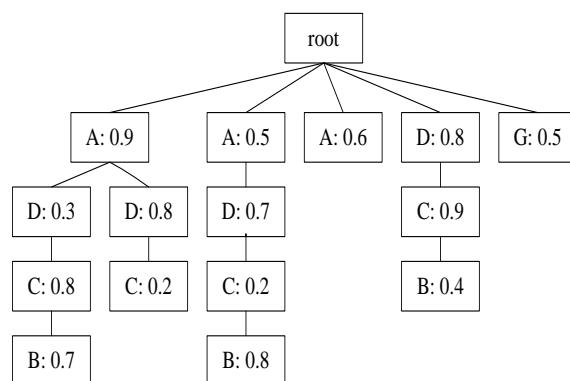


Fig. 1 Calculation process of random decryption protocol constructed by reversible information random coding transmission control protocol

2.2 Image chaotic map decomposition

On the basis of constructing reversible information random coding transmission control protocol and calculating random decryption protocol for reversible information of remote sensing image of generative countermeasure network in chaotic system, in order to reduce the pixel correlation in image encryption and hiding^[11], it is necessary to decompose the remote sensing image of generative countermeasure network to obtain three gray-scale images by chaotic mapping. The chaotic mapping decomposition uses piecewise linear chaotic mapping (KWLCM) to circularly move each pixel by bit, and the piecewise linear chaotic mapping is defined as follows:

$$x_{i+1} = F_{p_i}(x_i) = \begin{cases} x_i / p_i & 0 \leq x_i < p_i \\ (x_i - p_i) / (0.5 - p_i) & p_i \leq x_i < 0.5 \\ F_p(1 - x_i) & x_i \geq 0.5 \end{cases} \quad (4)$$

Randomly select an integer, and traverse the reversible information of the remote sensing image of the generative countermeasure network in segments. First, move each pixel circularly by bit for a limited number of times. The corresponding relationship between the elements in the vector quantization matrix and the elements in the matrix is as follows:

$$Q^r(i, j) = Q(r_i, j) \quad (5)$$

The moment of gray image is substituted into Hyperhenon chaotic map, and the elements in the matrix represent RGB components of reversible information of remote sensing image of generative countermeasure network, which are:

$$Q^{rc}(i, j) = Q^r(i, c_j) \quad (6)$$

By iteratively calculating the reversible information of the gray-scale generation confrontation network remote sensing image generated in each round, the corresponding relationship between the elements in the matrix and the elements in the matrix can be obtained:

$$Q^{rc}(i, j) = Q(r_i, c_j) \quad (7)$$

Assuming that the reversible information of each generative countermeasure network remote sensing image has the same size, and taking the position of x_1, y_1, z_1 in D, E, F , as the permutation matrix, the chaotic mapping decomposition result of reversible information of generative countermeasure network remote sensing image is obtained as follows:

$$f_t(H_1, H_2, H_3) = \begin{cases} (H_1 \wedge H_2) \vee ((H_1 \setminus) \wedge H_3) & 0 \leq t \leq 19 \\ H_1 \oplus H_2 \oplus H_3 & 20 \leq t \leq 39 \\ (H_1 \wedge H_2) \vee (H_1 \wedge H_3) \vee (H_2 \wedge H_3) & 40 \leq t \leq 59 \\ H_1 \oplus H_2 \oplus H_3 & 60 \leq t \leq 79 \end{cases} \quad (8)$$

Wherein, \oplus represents the exclusive or of R component and \wedge component of reversible information of generative countermeasure network remote sensing image, the bitwise sum of R component and \vee component, the bitwise OR of G component and B component, and the bitwise inversion, which can be expressed as follows

$$W_t = \begin{cases} M_t & 0 \leq t \leq 15 \\ S_1(W_t - 3 \oplus W_t - 8 \oplus W_t - 14 \oplus W_t - 16) & 16 \leq t \leq 79 \end{cases} \quad (9)$$

Through the above processing, the chaotic mapping decomposition of reversible information of the generative countermeasure network remote sensing image to be encrypted is realized, and the block key block matching and random coding of high-dimensional chaotic sequences are carried out on three RGB component gray images, so as to generate a Gaussian random pixel sequence of reversible information of the generative countermeasure network remote sensing image, and the image hiding algorithm is designed^[12].

3. Optimization design of image hiding method

3.1 Pixel edge scrambling

In order to improve the encryption security of reversible information hiding of network remote sensing images, this paper proposes a reversible information hiding method of network remote sensing images based on block cascade chaos fitness control. Block key matching and random coding are carried out on the gray image decomposed by chaotic map of the generative countermeasure network remote sensing image to be hidden, and the Gaussian random pixel sequence of the image is generated.

After randomly rearranging the reversible information sequence $Y = \{y_1, y_2, \dots, y_{WN}\}$ of the encrypted one-dimensional generative countermeasure network remote sensing image, the sequence C:

$$\begin{cases} C_i = B'_i \oplus B'_{i+1} \oplus B'_{i+2} \oplus Y'_i & \text{if } i \bmod 2 = 0 \\ C_i = B'_i \oplus B'_{i+1} \oplus B'_{i+2} \oplus -Y'_i & \text{if } i \bmod 2 = 1 \end{cases} \quad (10)$$

Then, the Gaussian random pixel sequence of the image is converted into the reversible information pixel edge scrambling of the network remote sensing image in a generating way, and the steps are as follows:

Step1: Obtaining the initial value sum of the r component of the gray image under the reversible information random coding transmission control protocol through the Hash value of the reversible information of the generative countermeasure network remote sensing image;

Step2: Change the statistical distribution of reversible information of plaintext generation against network remote sensing image, substitute the initial value into Hyperhenon piecewise chaotic linear map, generate ciphertext image sequence after iteration, substitute it into two random Lorenz chaotic systems, and generate G component pixel scrambling sequence of reversible information of network remote sensing image through iteration:

$$Z = \{z_1, z_2, \dots, z_{W*N}\} \quad (11)$$

$$Z' = \{z'_1, z'_2, \dots, z'_{W*N}\} \quad (12)$$

Step3: Carry out high-dimensional vector quantization decomposition of Hyperhenon chaotic map on Z_1 and G , and carry out exclusive OR with Z and Z' to obtain pixel shift times of gray image and image Gaussian random pixel sequence of gray image;

$$Z_1 = \{z_{11}, z_{12}, \dots, z_{1,W*N}\} \quad (13)$$

$$Z'_1 = \{z'_{11}, z'_{12}, \dots, z'_{1,W*N}\} \quad (14)$$

$$\begin{cases} z_{li} = (z_i \times 10^{14}) \bmod 3 + 2, & \text{if } i \bmod 3 = 0 \\ z_{li} = (z_i \times 10^{14}) \bmod 3 + 10, & \text{if } i \bmod 3 = 1 \\ z_{li} = (z_i \times 10^{14}) \bmod 3 + 18, & \text{if } i \bmod 3 = 2 \end{cases} \quad (15)$$

$$\begin{cases} z'_{li} = (z'_i \times 10^{14}) \bmod 3 + 2, & \text{if } i \bmod 3 = 0 \\ z'_{li} = (z'_i \times 10^{14}) \bmod 3 + 10, & \text{if } i \bmod 3 = 1 \\ z'_{li} = (z'_i \times 10^{14}) \bmod 3 + 18, & \text{if } i \bmod 3 = 2 \end{cases} \quad (16)$$

Step4: Using two sets of Lorenz equations, the pixels in the gray image are converted into a one-dimensional sequence with the size of 0, and the whole image is divided into blocks with 16*16 basic units to obtain a sequence $G_i^S = \{g_{i1}^S, g_{i2}^S, \dots, g_{i,W*N}^S\}$, $g_{li}^S = \text{circshift}(g_i, z_{li})$.

Step5: Set the initial value to 0, and scramble the pixel edges of the gray images of three RGB components to obtain:

$$g_{li}^C = (g_{li}^S + g_{1,i-1}^C) \bmod 256 \oplus z'_{li} \quad (17)$$

Step6: Transform the Gaussian random pixel sequence of the image into an image matrix, and scramble the pixels with row random numbers and column random numbers to build a hidden key.

3.2 Generation of reversible information hiding key for remote sensing image based on generative countermeasure network

The features of the coded output generative countermeasure network remote sensing image are recombined by pixel edge scrambling method, and the hidden key is generated under the reversible information random coding transmission control protocol to realize reversible information hiding of the generative countermeasure network remote sensing image. The steps are as follows:

Step1: Take the positions of x , y , z as encrypted chaotic maps with initial values and generated by permutation matrix, and generate sequences according to random rearrangement;

Step2: Decrypting the gray image, and performing reversible information random coding transmission control protocol reconstruction on the gray sequence to obtain an encrypted column of the ciphertext image;

Step3: Convert the reversible information of the ciphertext-generated countermeasure network remote sensing image to be decrypted into a one-dimensional sequence;

Step4: Take the decrypted, RGB, and three images as the sub-keys of the second round, and generate the reversible information of the network remote sensing image:

$$\begin{cases} B'_i = C_i \oplus C_{i+1} \oplus C_{i+2} \oplus Y'_i & \text{if } i \bmod 2 = 0 \\ B'_i = C_i \oplus C_{i+1} \oplus C_{i+2} \oplus -Y'_i & \text{if } i \bmod 2 = 1 \end{cases} \quad (18)$$

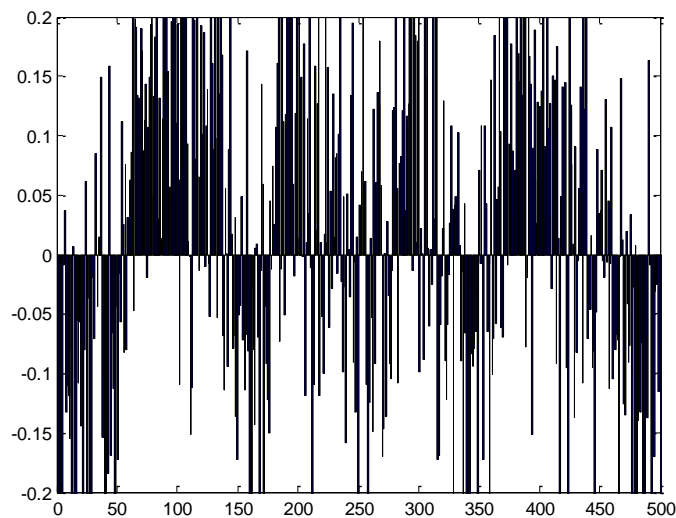
Step5: Convert the reversible information sequence of the hidden generative countermeasure network remote sensing image into a hidden key, and convert the additional key in the gray image into a gray pixel sequence with the size of, thereby recovering the reversible information of the original generative countermeasure network remote sensing image.

4. Experimental test analysis

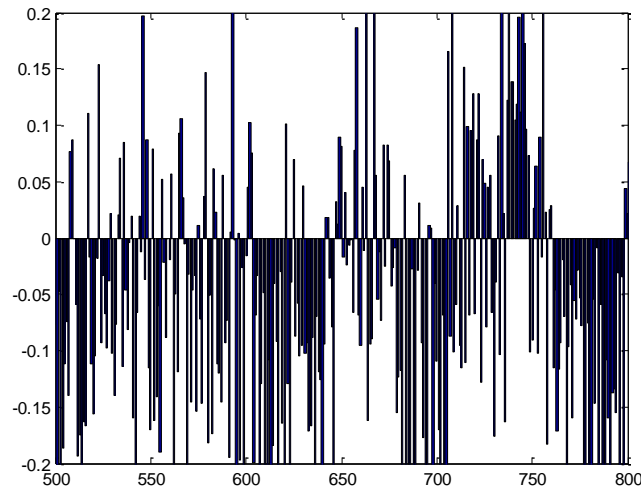
In order to test the performance of the image hiding method designed in this paper in realizing reversible information encryption and hiding of network remote sensing images, a comparative simulation experiment is conducted. Matlab simulation is adopted in the experiment. The hardware environment of the experiment is a computer with Intel(R) Pentium(R) Dual as the main processor, 1.8GHz, 0.98G the main frequency and 0.98 G memory. The sample image in the experiment is a house image scanned by 3D remote sensing radar, as shown in Figure 2. The image has 256 gray levels, and the initial values of the key space are generated by the Hash values of reversible information of the original plaintext generated anti-network remote sensing image, which are respectively,,,,, and, and the size are $u = 3.9754$, $c_0 = 0.8161$, $p = 0.1208$, $x_{first} = 0.4063$, $(r_1 = 12, r_2 = 2, r_3 = 9)$, and. The initial keys are $u = 3.9754$, $c_0 = 0.8161$, $p = 0.1208$, $x_{first} = 0.4063$, $(r_1 = 12, r_2 = 2, r_3 = 9)$, and (r_4, r_5, r_6) . (r_1, r_2, r_3) . And are floating-point numbers. According to the above simulation environment and parameter settings, the image is encrypted and hidden. The method in this paper is used to decompose the reversible information of the generated anti-network remote sensing image by chaotic mapping, and encrypt the three gray-scale image distributions decomposed by chaotic mapping. Because histogram is an effective measure of the encryption effect of image hiding method on the original plaintext image, in simulation analysis, histogram is used for statistical analysis of encryption effect. Figure 3 shows the encryption result of reversible information of anti-network remote sensing image.



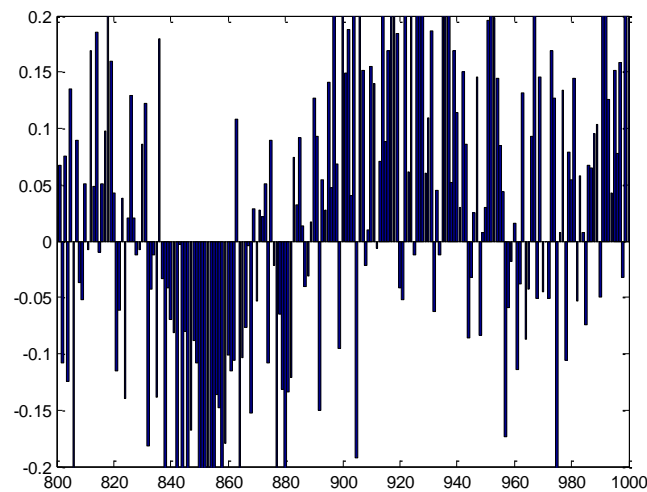
Fig.2 Sample pictures.



(a) R weight



(b)G weight



(c)B weight

Fig. 3 Reversible information encryption and histogram of remote sensing image against network

According to the above simulation results of anti-network remote sensing image reversible information encryption and hiding, the histogram of RGB components of the original image is approximately evenly distributed, and its statistical characteristics are obvious, so it is easy to be attacked by plaintext. Using this method to encrypt and hide the remote sensing radar image, the histogram of anti-network remote sensing image reversible information has changed greatly compared with the histogram of the original image, and the effective information of the image cannot be read from the histogram, which shows that this algorithm has higher anti-attack ability. In order to quantitatively describe the performance against reversible information encryption and hiding of network remote sensing images, three indexes, such as pixel correlation, pixel number change rate of RGB component NPCR normalized pixel value and average change intensity UACI, are used to analyze the encryption performance. The distribution of NPCR and UACI values describes the performance of large key space against reversible information hiding degree of network remote sensing images, and the statistical results are shown in Table 1 and Table 2.

Comparing the results in Table 1 and Table 2, it is known that the algorithm in this paper has a small correlation with pixels when it is used to encrypt and hide reversible information of network remote sensing images. The correlation of horizontal, vertical and diagonal pixels is almost zero by averaging 50 experiments, which shows that the method in this paper has good decorrelation performance and good stability against reversible information encryption of network remote sensing images. The performance of NPCR index and UACI index is superior, which shows that this method has a large key

space and good key sensitivity against reversible information hiding of network remote sensing images.

Table 1 Pixel Correlation Test

Test times	Pixel correlation	Visual fusion degree	Spatial resolution
10	0.4180	42.2727	2.4355
20	0.4409	44.5909	2.2204
30	0.4126	41.7273	2.2473
40	0.4490	45.4091	2.2957
50	0.4018	40.6364	2.3280
60	0.4072	41.1818	2.2043
70	0.3870	39.1364	2.3871
80	0.3978	40.2273	2.3226
90	0.4112	41.5909	2.0699
100	0.3856	39.0000	2.2473
110	0.3748	37.9091	2.3065
120	0.3667	37.0909	2.2473

Table 2 Statistical average of NPCR index and UACI index

Test times	NPCR	UACI	Hidden depth
10	109.4118	27.7612	266.4706
20	115.4118	29.2836	242.9412
30	108.0000	27.4030	245.8824
40	117.5294	29.8209	251.1765
50	105.1765	26.6866	254.7059
60	106.5882	27.0448	241.1765
70	101.2941	25.7015	261.1765
80	104.1176	26.4179	254.1176
90	107.6471	27.3134	226.4706
100	100.9412	25.6119	245.8824
110	98.1176	24.8955	252.3529
120	96.0000	24.3582	245.8824

5. Conclusions

In this paper, the encryption and hiding optimization method of reversible information of remote sensing images of generative countermeasure network is studied, and a reversible information hiding method of remote sensing images of generative countermeasure network based on block cascade chaotic fitness control is proposed. In a chaotic system, reversible information random coding transmission control protocol construction and random decryption protocol calculation are carried out on reversible information of the remote sensing image of the generative countermeasure network, chaotic mapping decomposition is carried out on the remote sensing image of the generative countermeasure network to be hidden to obtain three gray-scale images, block key matching and random coding are respectively carried out on the three images by using multidimensional Logistics chaotic mapping to generate an image Gaussian random pixel sequence, The features of the coded output generative countermeasure network remote sensing image are recombined by pixel edge scrambling method, and the hidden key is generated under the reversible information random coding transmission control protocol, thus realizing reversible information hiding of the generative countermeasure network remote sensing image. The research shows that this method is used to generate the reversible information encryption and hiding of network remote sensing images, which has low pixel correlation and strong pixel de-correlation. Both NPCR and UACI are very close to their ideal values, which shows that the key space is large, the reversible information hiding degree is

improved, and it can resist a large degree of attack.

References

- [1] WANG T, YANG J, JI Z, et al. Probabilistic diffusion for interactive image segmentation[J]. *IEEE Transactions on Image Processing*, 2019, 28(1):330-342.
- [2] BAMPIS C G, MARAGOS P, BOVIK A C. Graph-driven diffusion and random walk schemes for image segmentation [J]. *IEEE Transactions on Image Processing*, 2017:26(1):35-50.
- [3] DUAN Youxiang, ZHANG Hanxiao, SUN Qifeng, SUN Youkai. Image super-resolution reconstruction algorithm based on Laplacian pyramid generative adversarial network. *Journal of Computer Applications*, 2021, 41(4): 1020-1026.
- [4] XU Guangxian, XU Shanqiang, GUO Xiaojuan, HUA Yiyang. Image compression-encryption algorithm combined DCT transform with DNA operation[J]. *LASER TECHNOLOGY*, 2015, 39(6): 806-810.
- [5] LIU Hao, SHI Jia-ming, YUAN Zhong-cai, et al. Numerical Simulation and Experimental Study of Multi-band Trace TNT Detection by Imaging. *Acta Photonica Sinica*, 2016, 45(5): 0514004.
- [6] YANG Z M, WANG L Q, WANG Y. Application research of deep learning algorithm in question intention classification[J]. *Computer Engineering and Applications*, 2019, 55(10):154-160.
- [7] HUANG Y, PAISLEY J, LIN Q, et al. Bayesian nonparametric dictionary learning for compressed sensing MRI[J]. *IEEE Transactions on Image Processing*, 2014, 23(12): 5007-5019.
- [8] SHEN L, SUN G, HUANG Q, et al. Multi-level discriminative dictionary learning with application to large scale image classification[J]. *IEEE Transactions on Image Processing*, 2015, 24(10): 3109-3123.
- [9] SONG M F, JIA D Z, GUO J W, et al. A point cloud compression algorithm based on K-neighborhood cuboid [J]. *Science of Surveying and Mapping*, 2019, 44(10):93-100.
- [10] HU Xueying, GUO Hairu, ZHU Rong. Image super-resolution reconstruction based on hybrid deep convolutional network. *Journal of Computer Applications*, 2020, 40(7): 2069-2076.
- [11] NAN F Z, QIAN Y R, XING Y N, et al. Survey of single image super resolution based on deep learning[J]. *Application Research of Computers*, 2020, 37(2):321-326.
- [12] BIAN Y A, LI X, LIU Y, et al. Parallel coordinate descent newton method for efficient L1-regularized loss minimization[J]. *IEEE Transactions on Neural Networks and Learning Systems*, 2019, 30(11):3233-3245.