Hindawi
Security and Communication Networks
Volume 2021, Article ID 9698371, 27 pages
https://doi.org/10.1155/2021/9698371

Research Article

A Novel Multiband Remote-Sensing Image Encryption Algorithm Based on Dual-Channel Key Transmission Model

Zefei Liu[1,2] **Jinqing Li**[1,2] **Xiaoqiang Di**[1,2,3] **Zhenlong Man**[1,2] **and Yaohui Sheng**[1,2]

[1] *School of Computer Science and Technology, Changchun University of Science and Technology, Changchun 130022, China*
[2] *Jilin Key Laboratory of Network and Information Security, Changchun 130033, China*
[3] *Information Center, Changchun University of Science and Technology, Changchun 130022, China*

Correspondence should be addressed to Jinqing Li; lijinqing@cust.edu.cn

Received 13 July 2021; Revised 10 August 2021; Accepted 28 October 2021; Published 18 November 2021

Academic Editor: Zhenhua Tan

With the rapid development of remote sensing technology, satellite remote sensing images have been involved in many areas of people's lives. Remote sensing images contain military secrets, land profiles, and other sensitive data, so it is urgent to encrypt remote sensing images. This paper proposes a dual-channel key transmission model. The plaintext related key is embedded into the ciphertext image through bit-level key hiding transmission strategy, which enhanced the ability of ciphertext image to resist known-plaintext attack and chosen plaintext attack. In addition, a multiband remote sensing image encryption algorithm based on Boolean cross-scrambling and semi-tensor product diffusion is designed. Firstly, the pixel positions of each band of the remote sensing image are disturbed. Then, the random sequence generated by the four-dimensional chaotic system is processed and deformed to obtain a Boolean matrix. Based on the generated Boolean matrix and certain rules, the cross-confusion between the bands is carried out. Finally, the semi-tensor product operation is used in the diffusion process. Simulation results and experimental analysis show that the proposed algorithm obtains a larger key space and has stronger antiattack ability than other remote sensing image encryption algorithms. It can meet the security transmission of multiband remote sensing image in open space.

1. Introduction

Under the background of globalization, Internet technology has never stopped its development pace. The emergence of various kinds of social media has enabled a large amount of private information to be transmitted on the open network [1]. In recent years, with the rapid development of space science and information technology [2–4], massive amounts of remote sensing image information need to be transmitted in an open network and shared service environment [5]. Remote sensing images play an important role in agriculture, land, water resources, minerals, weather, and air pollution monitoring, disaster prevention and mitigation, national defense, and many other fields, providing a solid technical guarantee of the sustainable development of the national economy [6]. They are also the key source of information acquisition, data analysis, and processing. In addition, sensor systems for acquiring remote sensing images are usually installed on satellites, spacecraft, space stations, etc. As a result, remote sensing images are exposed to space radiation environment, and the information contained in the images will inevitably face severe interference attacks and risks of being stolen during transmission [7, 8]. Therefore, protecting the security of remote sensing images gradually highlights its importance.

Image encryption is a key and effective mean to protect the security of image information. In recent years, scholars have put forward a large number of excellent algorithms for image encryption [9]. Due to its complexity and extreme sensitivity to initial values and parameters [10], chaotic systems have become a typical encryption method as a pseudorandom number generator for image encryption. The existing advanced encryption technologies based on chaotic system include DNA encoding [11–16], S-box replacement

[17–19], Zigzag scrambling [20, 21], lifting scheme [22, 23], mathematical model [24], and compressive sensing [25].

In earlier years, Professor Xingyuan Wang and his team designed an encryption algorithm based on one-time key. The algorithm improves the dynamic degradation phenomenon but fails to solve the cyclic state of the chaotic system after a certain number of iterations [26]. In the same year, a chaotic image encryption algorithm based on simple perceptron was proposed by them to expand the periodicity of chaotic system [24]. In 2015, Zhang et al. designed a color image encryption scheme based on the 2DNLCML system and performed cross-mutation genetic operations on the pixel matrix of each color channel. Thus, the complexity of calculation is effectively reduced [27]. Subsequently, Chen et al. innovatively projected the three-color components of the color image into the three-dimensional space and performed the scrambling and diffusion operations based on the three-dimensional projection scrambling method and DNA coding technology, respectively [15]. This provides a new idea for color image encryption. Reference [28] proposes a bit-level arrangement and high-dimensional chaotic mapping to encrypt color images, which obtains a large enough key space and can resist common attacks. Recently, Wang et al. have adopted a bit-based scrambling method, combined with a dynamic superposition diffusion algorithm [29], and achieved good encryption results.

However, these encryption algorithms all use the same operation to encrypt each band (color channel) of the image. This faces that when an attacker cracks a grayscale image, the entire image is easily intercepted. To solve this problem, this paper introduces a new method based on Boolean cross-selection scrambling. The pixel values of all bands are shuffled as a whole to destroy the correlation between the bands, which greatly improve the security of multiband remote sensing. Beyond that, these algorithms transmit plaintext related keys and common keys together, which may not be able to truly achieve the plaintext related purpose of the key. To this end, this paper designs a dual-channel key transmission model, which embeds the key related to the plaintext into the ciphertext image. In this way, the algorithm's ability to resist known-plaintext and selected plaintext attacks is enhanced.

It is worth noting that, with the urgent need for privacy protection and in-depth research by scholars, many excellent encryption algorithms have recently emerged. Literature [30] improves the efficiency of the algorithm by means of parallel diffusion, so as to achieve the purpose of fast encryption. In literature [31], fractal sorting matrix (FSM) is designed by utilizing the idea of fractal features, which effectively improves the security of encryption algorithm. The team also designed a triple image encryption and hiding algorithm based on compressed sensing subsequently. The three-pixel matrix after compression and encryption is embedded into the color carrier image, which meets the requirements of visual significance and the era of big data [25]. For personal image data, Wang and Yang proposed a new TMDPCML chaotic system, which extracts the private information of the image and performs block encryption [1]. This algorithm fully guarantees the security of personal image information. The core points of these papers have provided us with many new ideas for designing algorithms.

Image encryption actually achieves the purpose of confusing pixel values by performing a series of operations on the pixel matrix. It is worth mentioning that there is a new type of matrix operation, semi-tensor product, which was first proposed by Cheng [32]. It expands the traditional matrix multiplication and no longer requires that the number of columns in the front matrix be equal to the number of rows in the back matrix. This new type of operation method is widely used in mathematics, nonlinear control systems, and physics [33–37]. In recent research, this kind of calculation method has begun to emerge in the field of image encryption. The semi-tensor product can be used to generate the reaction matrix of the diffusion stage of the encryption algorithm [38], so that the algorithm can not only be used for ordinary images, but also meet the needs of Boolean network encryption [39, 40]. Besides, it has also contributed to reducing the data volume and storage space of the measurement matrix of the compressed sensing algorithm [41], effectively improving the efficiency of the encryption algorithm. It is thus clear that the semi-tensor product operation can exert its unique advantages in the field of image encryption.

The above algorithms are mostly aimed at ordinary digital images, and their security has reached a very high level so far. Yet, compared with ordinary digital images, remote sensing images have the characteristics of multiple bands, large pixel resolution, and large data volume [42]. Conventional digital image encryption methods are not suitable for application on remote sensing images [43].

In order to design the algorithm suitable for remote sensing image encryption, which takes into account high efficiency, low energy consumption, and security, scholars have carried out a large number of analyses and researches. In 2012, Zhang et al. proposed a hybrid domain remote sensing image encryption algorithm [44]. In this scheme, the PWLCM system is used in the transform domain to sort the low-pass subband coefficients decomposed by the discrete wavelet transform of the image, and the reconstructed image is diffused in the spatial domain through the exclusive OR operation. This algorithm combines the advantages of the transform domain and the spatial domain, and it is effective. However, the effect may be unsatisfactory for remote sensing images with large amount of data. In 2016, Ye and Huang adopted block encryption for big size remote sensing images, which significantly improved the encryption efficiency [45]. In the following year, based on the consideration of reducing satellite energy costs, Huang et al. used compressed sensing to encrypt remote sensing images [46]. But it may cause the problem that the remote sensing image cannot be completely restored. Recently, Bentoutou et al. designed an efficient image encryption method based on chaotic mapping and advanced encryption standards [47]. The algorithm has high security, which makes the research of remote sensing image encryption advance a big step forward.

But in general, these remote sensing image encryption algorithms still have some problems, such as insufficient key space and the ability of antiattack to be improved. In addition, since the remote sensing images themselves contain some confidential information, the loss of image data may bring immeasurable consequences. In order to save space, ordinary images are usually compressed in the encryption process. Lossy compression will cause the loss of image information, and it is likely to cause the loss of important information in remote sensing images. Therefore, this compression method is not suitable for encryption of remote sensing images.

Based on the above discussion and some unsolved problems in existing image encryption algorithms, the main contributions of the algorithm proposed in this paper are as follows:

(1) A dual-channel key transmission model is proposed. Plaintext related key is transmitted through a special bit-level key hiding transmission strategy, which can resist known-plaintext attack and chosen plaintext attack.

(2) A new method of cross-Boolean selective scrambling (CBSS) is proposed. The Boolean matrix is generated by the Chaotic flow with plane of equilibria (CFPE) system and used for the cross-mixing process of multiple bands. This cross-band disorganized method of pixel positions greatly improves the security of the scrambling stage. It avoids the risk of the whole image being stolen from the traditional color image encryption single-channel cracking.

(3) A diffusion method is designed by combining the semi-tensor product with the CFPE system. Compared with conventional diffusion methods such as exclusive OR operation, it can obtain stronger antiattack ability and meet the high security requirements of remote sensing image transmission in open space.

The remainder of this paper is structured as follows. In Section 2, we introduce the preparation work of the simple four-dimensional chaotic system and semi-tensor product operation. Section 3 describes the proposed key transmission frame. The proposed encryption algorithm is described in Section 4. In Section 5, the simulation and security analysis of the experimental results are carried out. Finally, the paper is summarized in the last Section 6.

2. Preliminaries and Related Work

2.1. Chaotic Flow System. The chaotic system should be sensitive to the initial value and parameters. The algorithm uses a simple four-dimensional chaotic system, Chaotic flow with plane of equilibria (CFPE) [48], which is defined as

$$\begin{cases} \dot{x} = y, \\ \dot{y} = z, \\ \dot{z} = z + ayw - zw, \\ \dot{w} = xy + byz, \end{cases} \tag{1}$$

where x, y, z, w are the state variables, and a, b are the parameters of the system. When $a = -1$ and $b \in [0.87, 1]$, the system is chaotic. Figure 1 illustrates the random behavior of the sequences x, y, z and w generated by CFPE system when $a = -1$, $b = 1$, with 2×10^4 iterations. The attractor of CFPE system in three-dimensional space is depicted in Figure 2. Lyapunov exponent (LE) is an important parameter to measure chaotic system. When LE > 0, the system will enter into chaotic state; when LE ≤ 0, the system is stable. Thus, a system, which is chaotic, must show at least one positive LE. Figure 3 is the LEs of the CFPE system. It can be seen that when $a = -1$ and $0.87 \le b \le 1$, the CFPE system has two positive LEs. Therefore, it is a hyperchaotic system (when the chaotic system has two or more positive LEs, the system is hyperchaotic). Based on the above analysis, the CFPE system has remarkable dynamic behavior and meets the needs of image encryption. Therefore, apply it to image encryption for the first time in this paper.

2.2. Semi-tensor Product. Semi-tensor product of matrix is a new type of matrix multiplication operation, which breaks the limitation of traditional matrix operation that the number of columns of the former matrix must be as the same as the number of rows of the latter matrix. Semi-tensor product is not only applied in differential geometry, mathematical logic, system nonlinearity, and control theory, but also its application field is expanding in recent years and shows its great advantages in image processing. Semi-tensor product was first proposed by Cheng in reference [32], and then its definition is briefly described as follows.

Definition 1. Let $X \in M_{1\times np}$ be a row vector and let $Y \in M_{p\times 1}$ be a column vector. Divide the row vector X equally into p blocks $X^1, X^2, \ldots, X^p$, where $X^i \in M_{1\times n}$, $i = 1, 2, \ldots, p$. $Y = [y_1, y_2, \ldots, y_p]^T$. The left semi-tensor product can be defined as

$$\begin{cases} X \propto Y = \sum_{i=1}^{p} X^i y_i \in R^n, \\ Y^T \propto X^T = \sum_{i=1}^{p} y_i (X_i)^T \in R^n, \end{cases} \tag{2}$$

where $\propto$ represents the left semi-tensor product operator.

Definition 2. Let $U \in M_{m\times n}$ and $V \in M_{p\times q}$. Suppose that n and p satisfy $\bmod(n, p) = 0$ or $\bmod(p, n) = 0$, and the left semi-tensor product W of U and V is calculated by

$$\begin{aligned} W &= U \propto V \\ &= \left(W^{ij}\right) = \begin{bmatrix} W^{11} & W^{12} & \cdots & W^{1q} \\ W^{21} & W^{22} & \cdots & W^{2q} \\ \vdots & \vdots & \ddots & \vdots \\ W^{m1} & W^{m2} & \cdots & W^{mq} \end{bmatrix} \\ &= \begin{bmatrix} U^1 \propto V_1 & U^1 \propto V_2 & \cdots & U^1 \propto V_q \\ U^2 \propto V_1 & U^2 \propto V_2 & \cdots & U^2 \propto V_q \\ \vdots & \vdots & \ddots & \vdots \\ U^m \propto V_1 & U^m \propto V_2 & \cdots & U^m \propto V_q \end{bmatrix}, \end{aligned} \tag{3}$$

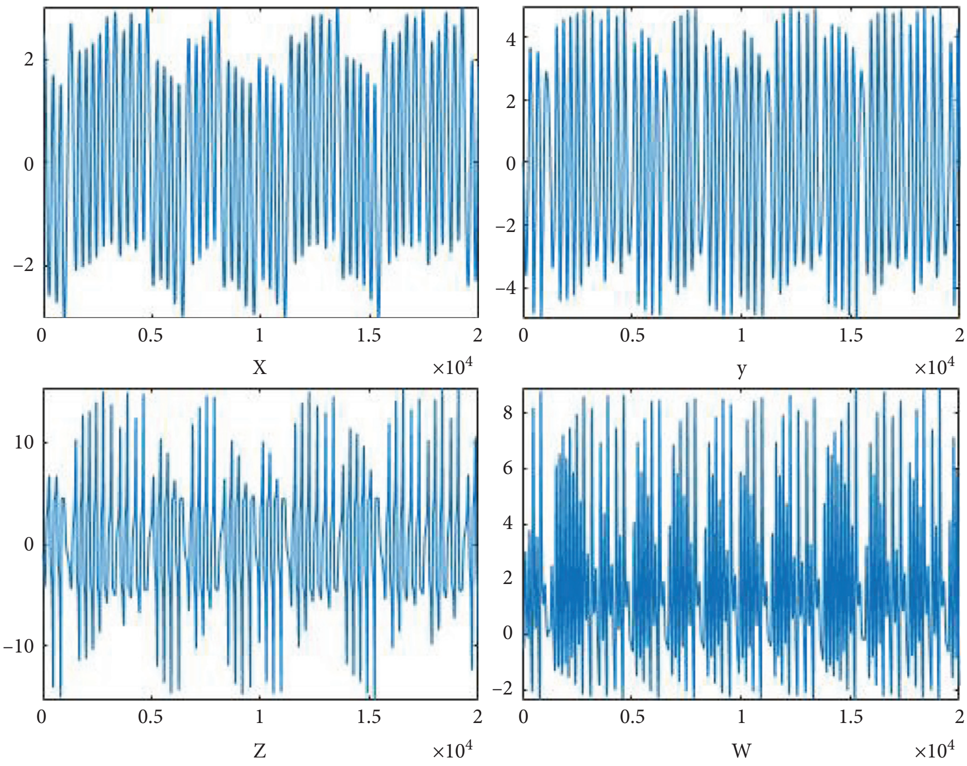


Figure 1: Random behavior of CFPE.

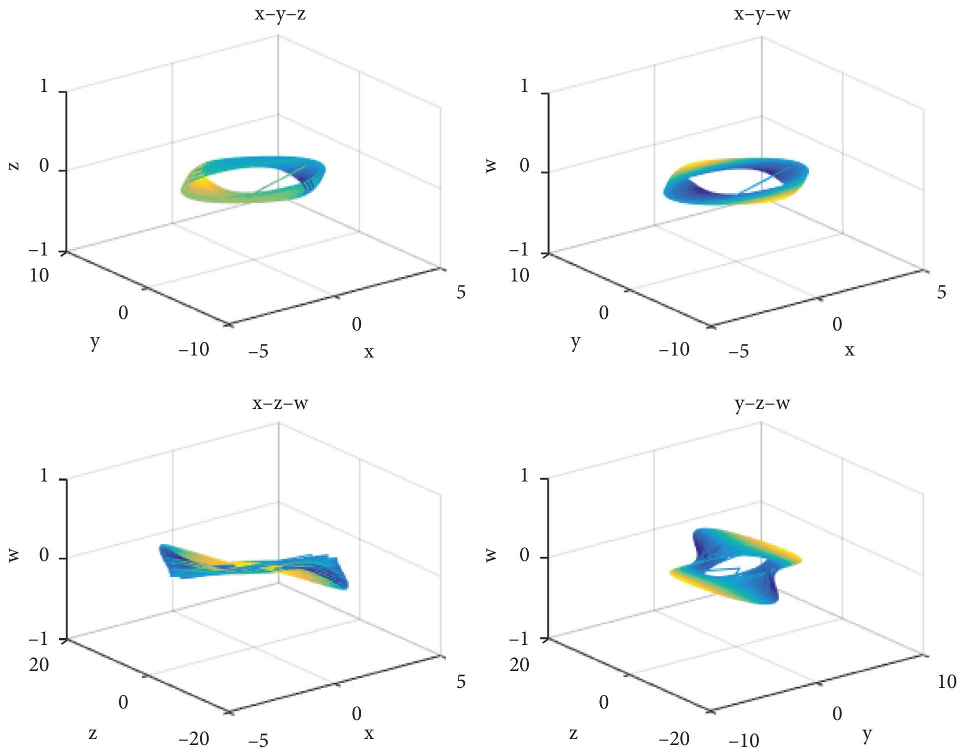


Figure 2: The attractors of CFPE system.

where U^i is the i-th row of U and V_j is the j-th column of $V, i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, q$. The sign mod () represents the remainder operation.

Proposition 1. *Let $A \in M_{p\times q}, B \in M_{s\times t}$.*

If $q/s = n$, then the left semi-tensor product of A and B is defined as

$$A \propto B = A\left(B \otimes I_n\right). \quad (4)$$

If $s/q = n$, then the left semi-tensor product of A and B is defined as

$$A \propto B = \left(A \otimes I_n\right)B, \quad (5)$$

where I_n is the identity matrix of order n. The symbol $'' \otimes$ stands for Kronecker product. When $q = s$, the semi-tensor product is equivalent to the traditional matrix multiplication. For two matrixes $M = (m_{ij}) \in M_{a\times b}, N = (n_{ij}) \in M_{c\times d}$, the Kronecker product is described by the following:

$$M \otimes N = \begin{bmatrix} m_{11}N & \cdots & m_{1b}N \\ \vdots & \ddots & \vdots \\ m_{a1}N & \cdots & m_{\mathrm{ab}}N \end{bmatrix}. \quad (6)$$

Example 1. Next, give a simple example to perform a semi-tensor product operation.

Suppose $A = \begin{bmatrix} 1 & 0 & 2 & 1 \\ 3 & 1 & 2 & 4 \\ 1 & 5 & 3 & 2 \\ 2 & 4 & 7 & 3 \end{bmatrix}, B = \begin{bmatrix} 1 & -2 \\ 2 & -3 \end{bmatrix}$, then

$$\begin{aligned} A \propto B &= A\left(B \otimes I_2\right) \\ &= A\begin{bmatrix} 1\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & -2\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ 2\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & -3\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & 2 & 1 \\ 3 & 1 & 2 & 4 \\ 1 & 5 & 3 & 2 \\ 2 & 4 & 7 & 3 \end{bmatrix}\begin{bmatrix} 1 & 0 & -2 & 0 \\ 0 & 1 & 0 & -2 \\ 2 & 0 & -3 & 0 \\ 0 & 2 & 0 & -3 \end{bmatrix} \\ &= \begin{bmatrix} 5 & 2 & -8 & -3 \\ 7 & 9 & -12 & -14 \\ 7 & 9 & -11 & -16 \\ 16 & 10 & -25 & -17 \end{bmatrix}. \end{aligned} \quad (7)$$

3. Key Transmission Frame

3.1. Dual-Channel Key Transmission Model. In the design of image encryption algorithm, for making the ciphertext image sensitive enough to the plaintext image and the key, some inherent properties of the plaintext image are usually used to generate the key [49–51]. Thus, the key and ciphertext can be changed with the small change of plaintext image. Although this method is beneficial to resist differential attack, there are security problems of known-plaintext attack and chosen plaintext attack in key transmission.

To fill this significant gab, a dual-channel key transmission model is innovatively proposed, in which plaintext related key and ordinary symmetric key are transmitted in two different ways. Obviously, this transmission method must ensure that there exists a plaintext related key. The integral model is portrayed in Figure 4. For ordinary symmetric key, the traditional secure channel is still adopted. Yet the plaintext related key is transmitted by a special bit-level key hiding transmission strategy, which embeds the key into the ciphertext image and will be elaborated at Section 3.2. When the decryptor obtains the ciphertext image through the network, it first extracts the plaintext related key from the image and then decrypts it combined with the symmetric key from the secure channel. The two types of keys work on the chaotic system together as encryption keys, and the attacker cannot restore the original image correctly when intercepting any single key. This dual-channel key transmission model effectively enhances the security of images.

3.2. Bit-Level Key Hidden Transmission Strategy. Here, we will explain the bit-level key hidden transmission strategy mentioned above at length. This new type of transmission strategy effectively solves the security problems encountered in the transmission of plaintext related keys. As described in Figure 5, the specific steps are as follows:

step 1. Set the size of a remote sensing image I to $H \times W \times n$. $H \times W$ is the image size and n shows the number of bands. Convert plaintext related key s into a t-bit binary number s', where the generation method of s is shown in equation (8) in this paper. (Let $s = 272222294$ and $t = 32$ in the example diagram.)

$$s = \mathrm{sum}\left(I\left(:\right)\right), \quad (8)$$

where s calculates the sum of all pixel values of the original remote sensing image I. Readers can also set other algorithms to generate plaintext related key s.

step 2. Iterate the Logistic mapping $f(\tau) = \lambda\tau(1 - \tau)$ for $1000 + t \times 3$ times and discard the first 1000 values to obtain KEY. Process it by equation (9) to get KEY′ with size of $t \times 3$, and divide KEY′ into three equal sequences, which are denoted as q, u, v with size of t.

$$\mathrm{KEY}' = \mathrm{mod}\Big(\mathrm{floor}\Big(\mathrm{KEY} \times 10^{12}\Big), 256\Big) + 1. \quad (9)$$

step 3. Get the sequence q' in the range of $[1, n]$ by equation (10). q' is used to select the band, where the hidden position of random pixel is located, and u, v determine the particularized position of the hidden position in q'-th band pixel matrix. In this way, obtain t randomly selected pixel values, which are recorded as *RP*.

$$q' = \mathrm{mod}\left(q, n\right) + 1. \quad (10)$$

step 4. First convert *RP* into corresponding 8-bit binary numbers. The last bit value of each binary number is extracted and connected in turn to obtain a 32-bit binary number *LC*. Meanwhile, record the decimal number corresponding to *LC*, noted as *LD* and transmit it to the decryption party as a key.

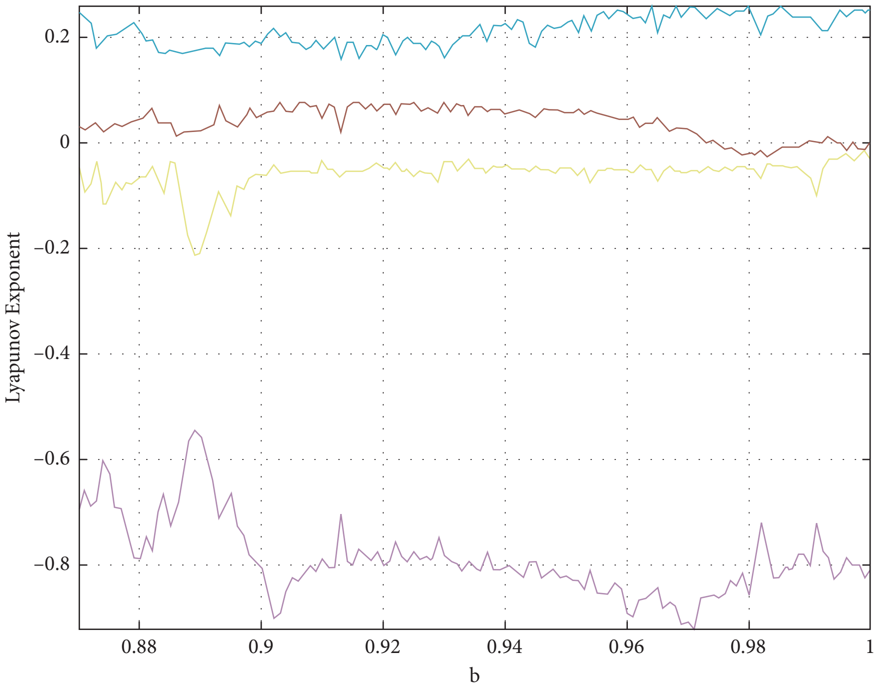


Figure 3: Lyapunov exponents diagram for the CFPE system.

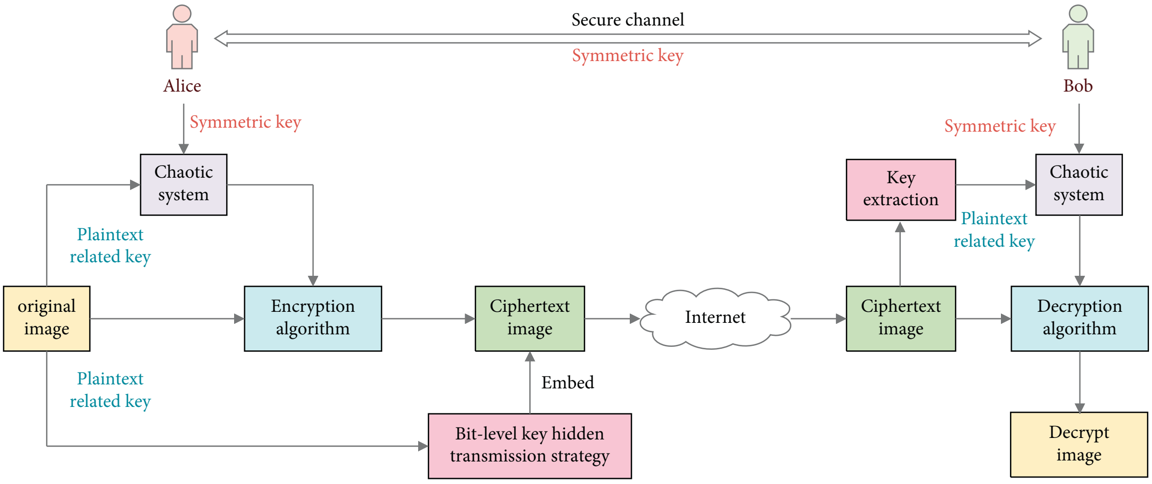


Figure 4: Dual-channel key transmission model.

step 5. Perform bitwise XOR on *LD* and *s* generated above to obtain a 32-bit last binary sequence *CP* containing plaintext related information.

step 6. The last bit of the selected pixel *RP* is updated with *CP* and then replaced in the ciphertext image. By this means, the relevant information of plaintext has been embedded in ciphertext image. And the final ciphertext image is obtained.

step 7. When the decryptor receives the ciphertext image, it first uses the chaotic key stream sequence to ascertain the hidden position of the plaintext related key. After that, converting the extracted pixel value into 8-bit binary numbers, the last bits are concatenated to obtain a 32-bit binary sequence. Perform bitwise XOR operation with the key *LD* to obtain the hidden plaintext related key *s*.

It is worth mentioning that although we embed a plaintext related key in the encrypted image, this key is only hidden in about 30 pixels (accounting for only 0.05% of the total number of image pixels). What is more, we only embedded it into the last-bit of the 8-bit binary form of the 0.05% pixel. Combined with the part of the security analysis results of the experiment, the bit-level key hidden transmission strategy proposed in this paper does not increase the risk of ciphertext images being attacked.

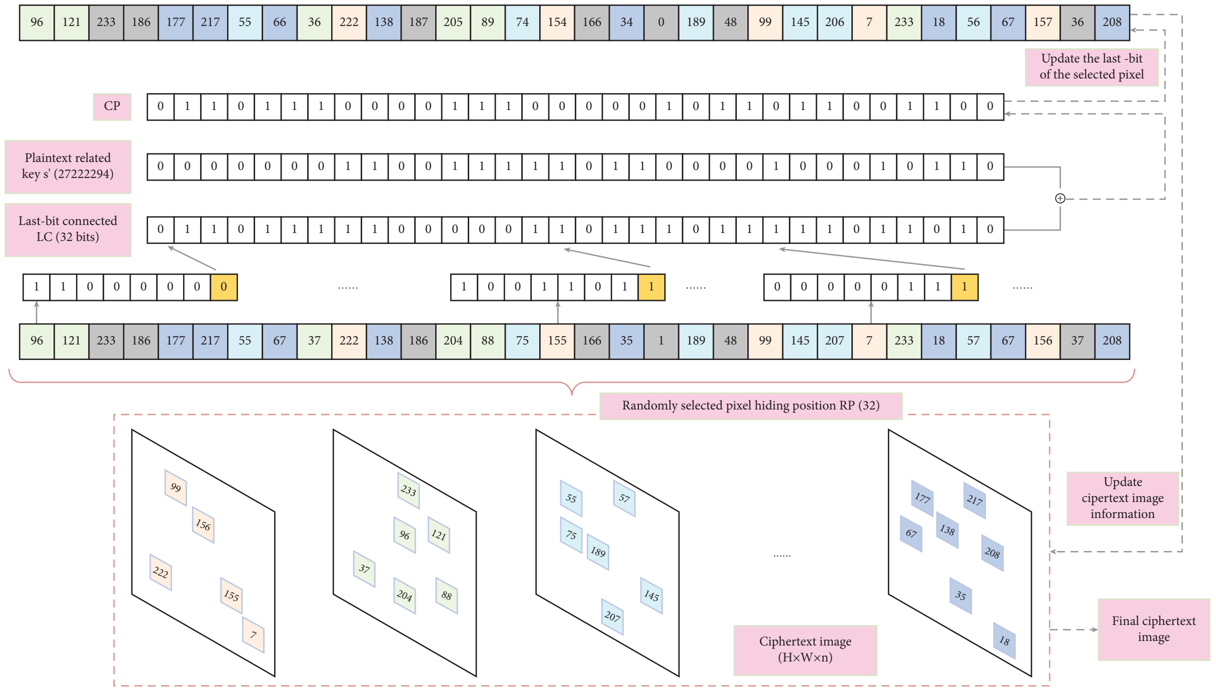


Figure 5: Bit-level key hidden transmission strategy.

4. Image Encryption and Decryption Algorithm

Choose a remote sensing image with size of $M \times N \times n$ as the original image P, where M is the height, N is the width, and n indicates the bands number of the remote sensing image. The encryption flow chart of b-band remote sensing image is illustrated in Figure 6.

For convenience, set $n = 4$ in the algorithm description below. The proposed encryption process will be divided into three stages: generation of chaotic sequences, scrambling stage, and diffusion stage.

4.1. Generation of Chaotic Sequences. The four-dimensional hyperchaotic system CFPE can not only avoid the long iteration time of high-dimensional chaotic systems, but also show excellent chaotic characteristics. Therefore, it is used for the encryption process, which is proposed by this paper. The generation of chaotic sequences is described as follows:

Iterate the four-dimensional chaotic system $p + M \times N$ times with initial value x_0, y_0, z_0, w_0 and parameters a, b. In order to eliminate the transient effect, the former p group values were discarded. p represents plaintext related chaotic key pointer, and its calculation method is given as follows:

$$p = \mathrm{mod}\left(\frac{s \times \log_2 10^6}{L}, K\right) + 10K, \tag{11}$$

where the calculation method of s is as equation (8); floor stands for rounding down function; mod represents the remainder function; K, L are parameters, which are set by the users; and $K, L \in N^+$ and $K \in [20, 256]$, $L \le 20$. It should be emphasized that the plaintext related information s in the chaotic key pointer p will be embedded into the final ciphertext information through the bit-level key hidden transmission strategy.

After that, four chaotic sequences X_1, X_2, X_3, X_4 with size of $M \times N$ are obtained, i.e., $X_1 = x_{11}, x_{12}, \ldots, x_{1,M\times N}$, $X_2 = x_{21}, x_{22}, \ldots, x_{2,M\times N}$, $X_3 = x_{31}, x_{32}, \ldots, x_{3,M\times N}$, $X_4 = x_{41}, x_{42}, \ldots, x_{4,M\times N}$.

As shown in equation (12), modify chaotic sequence X_1, X_2, X_3, X_4 to generate XD_1, XD_2, XD_3, XD_4, separately.

$$\begin{cases} XD_1 = \mathrm{mod}\left(\mathrm{floor}\left(\mathrm{mod}\left(X_1, 1\right) \times 10^6\right), 256\right), \\ XD_2 = \mathrm{mod}\left(\mathrm{floor}\left(\mathrm{mod}\left(X_2, 1\right) \times 10^6\right), 256\right), \\ XD_3 = \mathrm{mod}\left(\mathrm{floor}\left(\mathrm{mod}\left(X_3, 1\right) \times 10^6\right), 256\right), \\ XD_4 = \mathrm{mod}\left(\mathrm{floor}\left(\mathrm{mod}\left(X_4, 1\right) \times 10^6\right), 256\right), \end{cases} \tag{12}$$

where the operation 'mod1' will get the output value between 0 and 1. The specific calculation method is

$$x\mathrm{mod}1 = \begin{cases} x - \lfloor x \rfloor, & x \ge 0, \\ |\lfloor x \rfloor| + x, & x < 0. \end{cases} \tag{13}$$

The first $(M/8) \times (N/8)$ values of the generated chaotic sequence XD_i are intercepted as the first round of diffusion matrixes, which is noted as XF_1, XF_2, XF_3 and XF_4. The subsequent $(M/4) \times (N/4)$ elements, which are called XFD_1, XFD_2, XFD_3 and XFD_4, are used in the second round.

4.2. Scrambling Stage. Original remote sensing image P is divided into four bands: red, green, blue, and infrared. Figure 7 depicts the scrambling stage. It can be found that, after two rounds of scrambling, the pixel values of the four

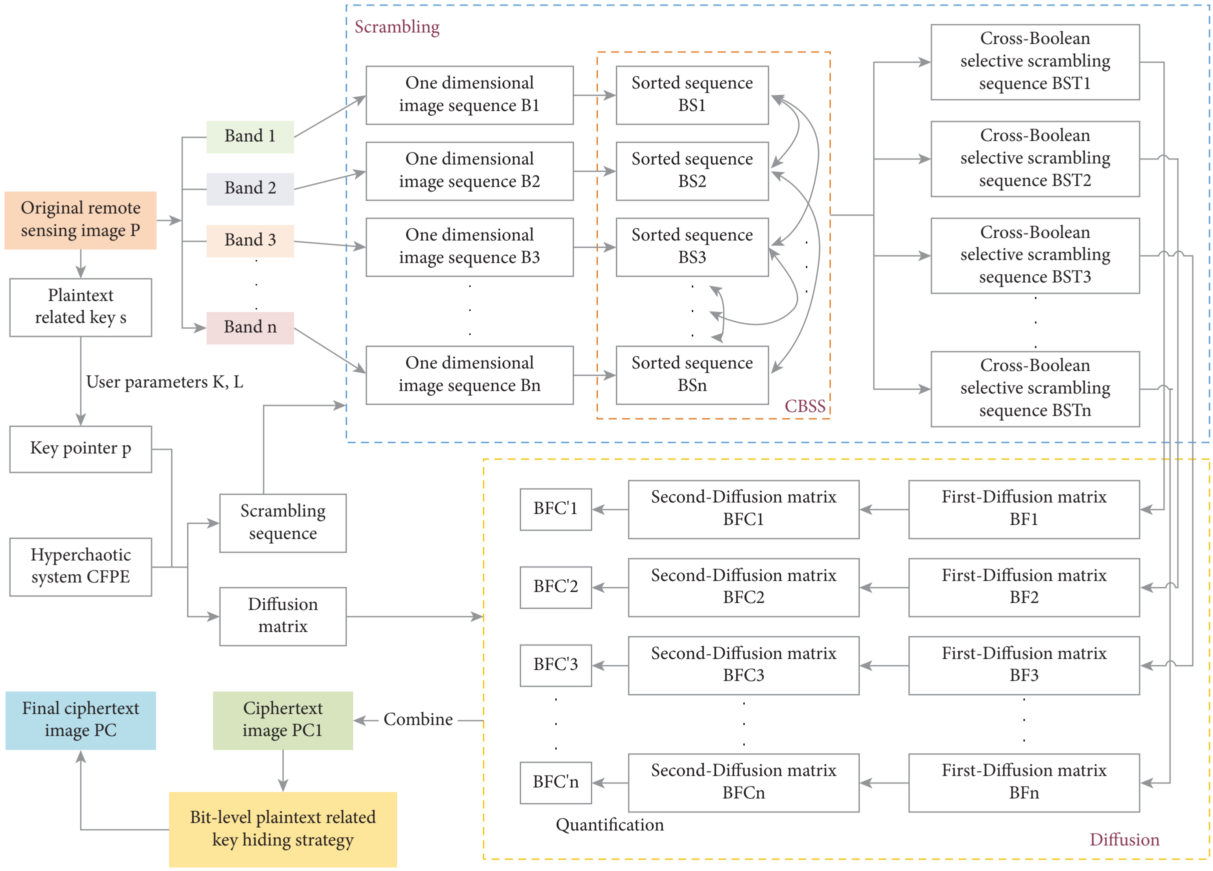

Scrambling
Original remote sensing image P
Plaintext related key s
User parameters K, L
Key pointer p
Hyperchaotic system CFPE
Band 1
Band 2
Band 3
Band n
One dimensional image sequence B1
One dimensional image sequence B2
One dimensional image sequence B3
One dimensional image sequence Bn
Sorted sequence BS1
Sorted sequence BS2
Sorted sequence BS3
Sorted sequence BSn
CBSS
Cross-Boolean selective scrambling sequence BST1
Cross-Boolean selective scrambling sequence BST2
Cross-Boolean selective scrambling sequence BST3
Cross-Boolean selective scrambling sequence BSTn
Scrambling sequence
Diffusion matrix
BFC'1
BFC'2
BFC'3
BFC'n
Second-Diffusion matrix BFC1
Second-Diffusion matrix BFC2
Second-Diffusion matrix BFC3
Second-Diffusion matrix BFCn
First-Diffusion matrix BF1
First-Diffusion matrix BF2
First-Diffusion matrix BF3
First-Diffusion matrix BFn
Quantification
Diffusion
Combine
Final ciphertext image PC
Ciphertext image PC1
Bit-level plaintext related key hiding strategy

Figure 6: Encryption flow chart.

bands are well fused. Therefore, it is impossible for attackers to crack the whole remote sensing image by cracking a single band. The security of encryption has been greatly improved. Scrambling stage is implemented by the following steps:

step 1. Convert the four bands of P into one-dimensional pixel sequences B_1, B_2, B_3 and B_4.

step 2. The chaotic sequences X_1, X_2, X_3, X_4 are arranged from small to large to receive location index sequence XS_1, XS_2, XS_3, XS_4. Find the position of the elements XS in the original sequence X, and record the position information into the corresponding location index matrix location M_1, location M_2, location M_3, location M_4.

$$\begin{cases} (XS_1, \text{location } M_1) = \text{sort}(X_1), \\ (XS_2, \text{location } M_2) = \text{sort}(X_2), \\ (XS_3, \text{location } M_3) = \text{sort}(X_3), \\ (XS_4, \text{location } M_4) = \text{sort}(X_4). \end{cases} \tag{14}$$

step 3. Image sequences B_1, B_2, B_3 and B_4 are sorted according to the position information in the index matrixes to obtain the matrix BS_1, BS_2, BS_3 and BS_4 after the first scrambling. The implementation is represented by Eq. (15).

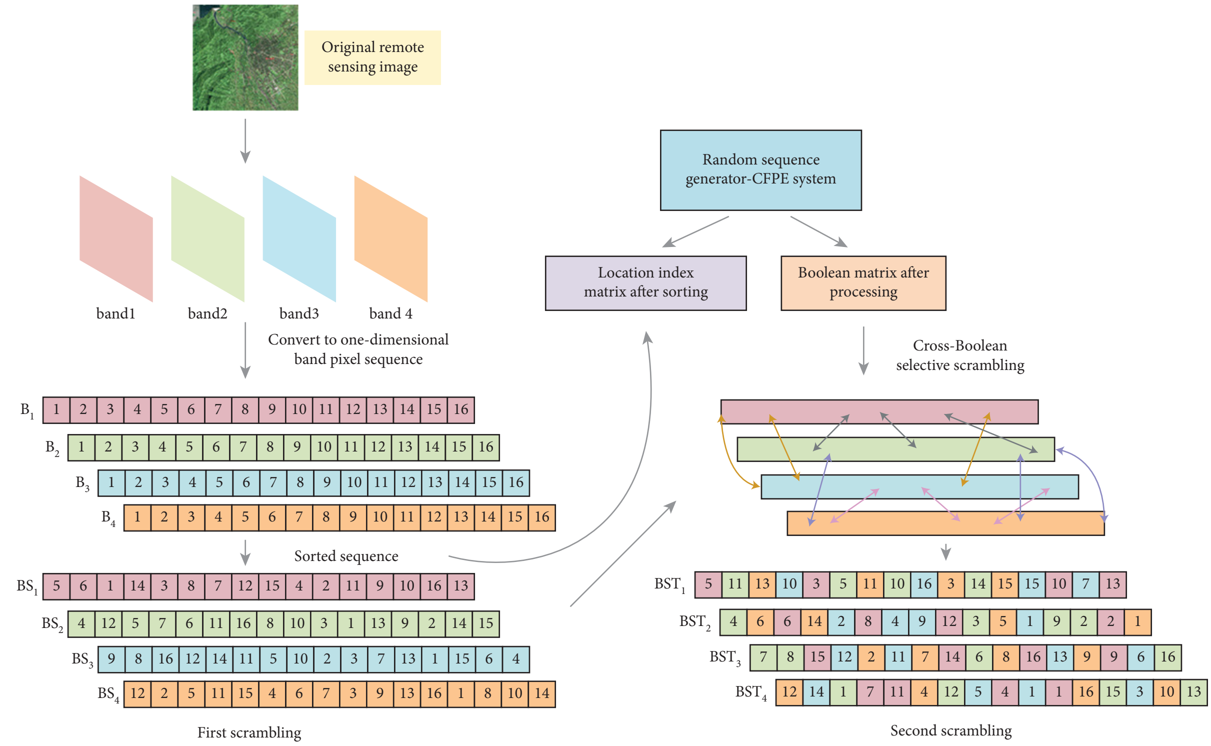
$$\begin{cases} BS_1(j) = B_1(\text{location } M_1(j)), \\ BS_2(j) = B_2(\text{location } M_2(j)), \\ BS_3(j) = B_3(\text{location } M_3(j)), \\ BS_4(j) = B_4(\text{location } M_4(j)), \end{cases} \tag{15}$$

where $j = 1, 2, \ldots, M \times N$.

step 4. Map the chaotic sequences X_1, X_2, X_3, X_4 into Boolean matrixes $X_{1\_\text{exchange}}, X_{2\_\text{exchange}}, X_{3\_\text{exchange}}, X_{4\_\text{exchange}}$. All elements in the matrixes are composed of 0 or 1. The transformation method is as follows:

$$\begin{cases} X_{1\_\text{exchange}} = \text{mod}(\text{floor}(X_1 \times 10^{12}), 2), \\ X_{2\_\text{exchange}} = \text{mod}(\text{floor}(X_2 \times 10^{12}), 2), \\ X_{3\_\text{exchange}} = \text{mod}(\text{floor}(X_3 \times 10^{12}), 2), \\ X_{4\_\text{exchange}} = \text{mod}(\text{floor}(X_4 \times 10^{12}), 2). \end{cases} \tag{16}$$

step 5. The generated Boolean matrix is used to cross-scrambling the pixel matrix after the first scrambling. Here, a new scrambling method cross-Boolean selective scrambling (CBSS) is proposed. According to the values of the elements in the Boolean matrix, perform cross-scrambling operations to the pixel values of four bands


Original remote sensing image
band1
band2
band3
band 4
Convert to one-dimensional band pixel sequence
Sorted sequence
First scrambling
Random sequence generator-CFPE system
Location index matrix after sorting
Boolean matrix after processing
Cross-Boolean selective scrambling
Second scrambling

B_1: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
B_2: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
B_3: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
B_4: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

BS_1: 5 6 1 14 3 8 7 12 15 4 2 11 9 10 16 13
BS_2: 4 12 5 7 6 11 16 8 10 3 1 13 9 2 14 15
BS_3: 9 8 16 12 14 11 5 10 2 3 7 13 1 15 6 4
BS_4: 12 2 5 11 15 4 6 7 3 9 13 16 1 8 10 14

BST_1: 5 11 13 10 3 5 11 10 16 3 14 15 15 10 7 13
BST_2: 4 6 6 14 2 8 4 9 12 3 5 1 9 2 2 1
BST_3: 7 8 15 12 2 11 7 14 6 8 16 13 9 9 6 16
BST_4: 12 14 1 7 11 4 12 5 4 1 1 16 15 3 10 13

FIGURE 7: Scrambling stage.

```
Input: Boolean matrix $X_{1\_\text{exchange}}, X_{2\_\text{exchange}}, X_{3\_\text{exchange}}, X_{4\_\text{exchange}}$ and $BS_1, BS_2, BS_3, BS_4$.
  for $j = 1$ to $M \times N$ do
      if $X_{1\_\text{exchange}} = 1$ then
          exchange $(BS_1(j), BS_2(j))$
      else if $X_{2\_\text{exchange}} = 1$ then
          exchange $(BS_3(j), BS_4(j))$
      else if $X_{3\_\text{exchange}} = 1$ then
          exchange $(BS_1(j), BS_3(j))$
      else if $X_{4\_\text{exchange}} = 1$ then
          exchange $(BS_2(j), BS_4(j))$
      end if
  end for
Output: CBSS matrixes $BST_1, BST_2, BST_3$ and $BST_4$
```

ALGORITHM 1: CBSS process.

like shuffling. The specific way is described in Algorithm 1. Loop the crossover operation until the last pixel; afterwards, the pixel matrixes $BST_1, BST_2, BST_3, BST_4$ after CBSS are obtained. It is also called the second scrambling.

4.3. Diffusion Stage. The diffusion process is designed by combining the semi-tensor product with the CFPE system. The simulation of single band diffusion operation is given in Figure 8.

First round: The diffusion matrix XF_1, XF_2, XF_3 and XF_4 is reshaped into square matrixes XF_1', XF_2', XF_3' and XF_4', with sizes $(M/8) \times (N/8)$. Then, the pixel matrix and diffusion matrix of each band after scrambling perform matrix semi-tensor product operation, respectively. As shown in equation (17), the pixel matrix after the first diffusion, which are called BF_1, BF_2, BF_3 and BF_4 with size of $M \times N$, is obtained.

$$\begin{cases} BF_1 = BST_1 \propto XF_1', \\ BF_2 = BST_2 \propto XF_2', \\ BF_3 = BST_3 \propto XF_3', \\ BF_4 = BST_4 \propto XF_4'. \end{cases} \tag{17}$$

Second round: In order to obtain better pixel obfuscation effect and enhance the security of the algorithm, the second diffusion operation is performed on matrix BF_1, BF_2, BF_3 and BF_4 by semi-tensor product operation. Similarly, the matrix

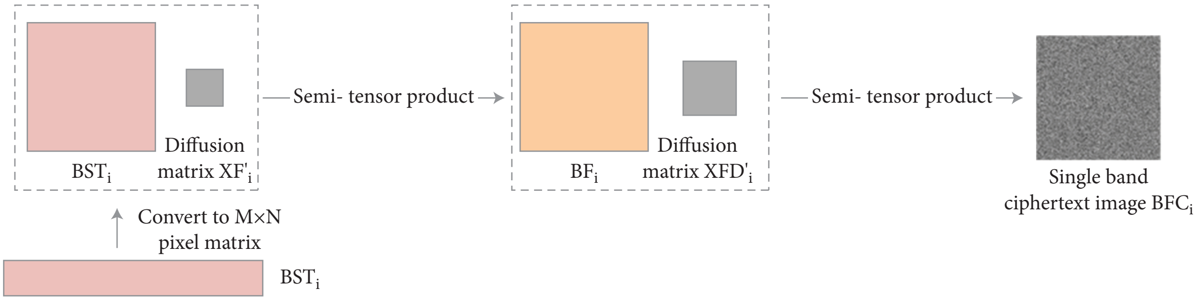

Semi- tensor product
Diffusion matrix XF'$_i$
BST$_i$
Semi- tensor product
Diffusion matrix XFD'$_i$
BF$_i$
Single band ciphertext image BFC$_i$
Convert to M×N pixel matrix
BST$_i$

Figure 8: Single band diffusion simulation.

XFD_1, XFD_2, XFD_3 and XFD_4 is reshaped into square matrix XFD_1', XFD_2', XFD_3' and XFD_4' with size of $(M/4) \times (N/4)$, in which the size of the matrix is different from that of the first diffusion. Through the operation of equation (18), we will get the ciphertext matrix of each band BFC_1, BFC_2, BFC_3 and BFC_4. In order to quantify the elements within the pixel value range 0 ~ 255, perform equation (19). The ciphertext image $PC1$ is obtained by synthesizing the four bands BFC_1', BFC_2', BFC_3' and BFC_4' after encryption.

$$\begin{cases} BFC_1 = BF_1 \propto XFD_1', \\ BFC_2 = BF_2 \propto XFD_2', \\ BFC_3 = BF_3 \propto XFD_3', \\ BFC_4 = BF_4 \propto XFD_4', \end{cases} \tag{18}$$

$$\begin{cases} BFC_1' = BFC_1 - \text{integer}_M\left(BFC_1\right), \\ BFC_2' = BFC_2 - \&ImaginaryI;\,\text{nteger}_M\left(BFC_2\right), \\ BFC_3' = BFC_3 - \text{integer}_M\left(BFC_3\right), \\ BFC_4' = BFC_4 - \text{integer}_M\left(BFC_4\right), \end{cases} \tag{19}$$

where the function $\text{integer}_l H = \text{floor}\left(H/l\right) \times l$.

Then, the plaintext related key s is embedded into the ciphertext image PC1 through the bit-level key hiding transmission strategy in Section 3.2 to get the final ciphertext image PC.

Each step in the encryption process is reversible; i.e., this algorithm is symmetric encryption. Therefore, the detailed structure of decryption is given in Figure 9 directly without too much description.

5. Experimental Results and Security Analysis

5.1. Simulation Result. In order to test the encryption effect of this algorithm, the simulation experiment on MATLAB 2015b platform is completed. The computer environment is equipped with Intel (R) Core (TM) i7-6500U CPU @2.50 GHz, 8.00 GB RAM and Windows 10 operating system. The remote sensing image in the experiment is from Gaofen Image Dataset (GID) released by Wuhan University in 2020, which is extracted from Gaofen-2 (GF-2) satellite [52]. Multiband remote sensing image processing is based on a complete remote sensing image processing platform, the Environment for Visualizing Images (ENVI). In order to ensure that the experimental results do not lose generality, we capture 10 remote sensing images with the size of 256 × 256 from the GID database. They are composed of four bands: red, green, blue, and near infrared. The encryption and decryption effects of 10 remote sensing images and all-black and all-white images are shown in Figure 10.

For the sake of clarity to observe the encryption effect of the four bands, the encryption and decryption results of two remote sensing images "Land1" and "Land2" are further demonstrated in Figures 11 and 12. It can be found from the experimental renderings that the encrypted image is noise-like information without any visible information.

5.2. Statistical Analysis

5.2.1. Histogram Analysis. Histogram statistics are the frequency of each gray value in the image, which is one of the important observable indicators to investigate the robustness for encryption algorithms. Figures 13 and 14 illustrate the histograms of remote sensing images "Land 1" and "Land 2" individually. It can be seen from (i–l) of the two figures that the histogram of each band after encryption presents a smooth trend, and each pixel value appears to be well distributed. Consequently, it is impossible to obtain the relevant information of pixel values from the histogram of the ciphertext images.

In order to further analyze the mathematical quality of the histogram, the variance of the encrypted image histogram is used to measure the uniformity of the image encryption. When the key changes, the closer the two variance values are, the higher the uniformity of the encrypted image is. The calculation formula of variance is shown in

$$\text{var}\left(Z\right) = \frac{1}{n^2} \sum_{i=1}^{n} \frac{\left(z_i - z_j\right)^2}{2}, \tag{20}$$

where Z represents the histogram vector; $Z = z_1, z_2, z_3, \ldots, z_{256}$, z_i and z_j refer to the number of pixel values of i and j in the ciphertext image, respectively. In the test experiment of image uniformity, we utilized equation (20) to calculate the variance of the ciphertext image histogram of the four bands of two remote sensing images "Land 1" and "Land 2." The results are listed in Table 1. The variance in the first column of Table 1 is calculated from the original key key, and the subsequent columns are the variance obtained by only parameter of secret keys changed in a, b, x_0, y_0, z_0, w_0. It can be seen that the average value of the variance is about 5400, which indicates that the number of

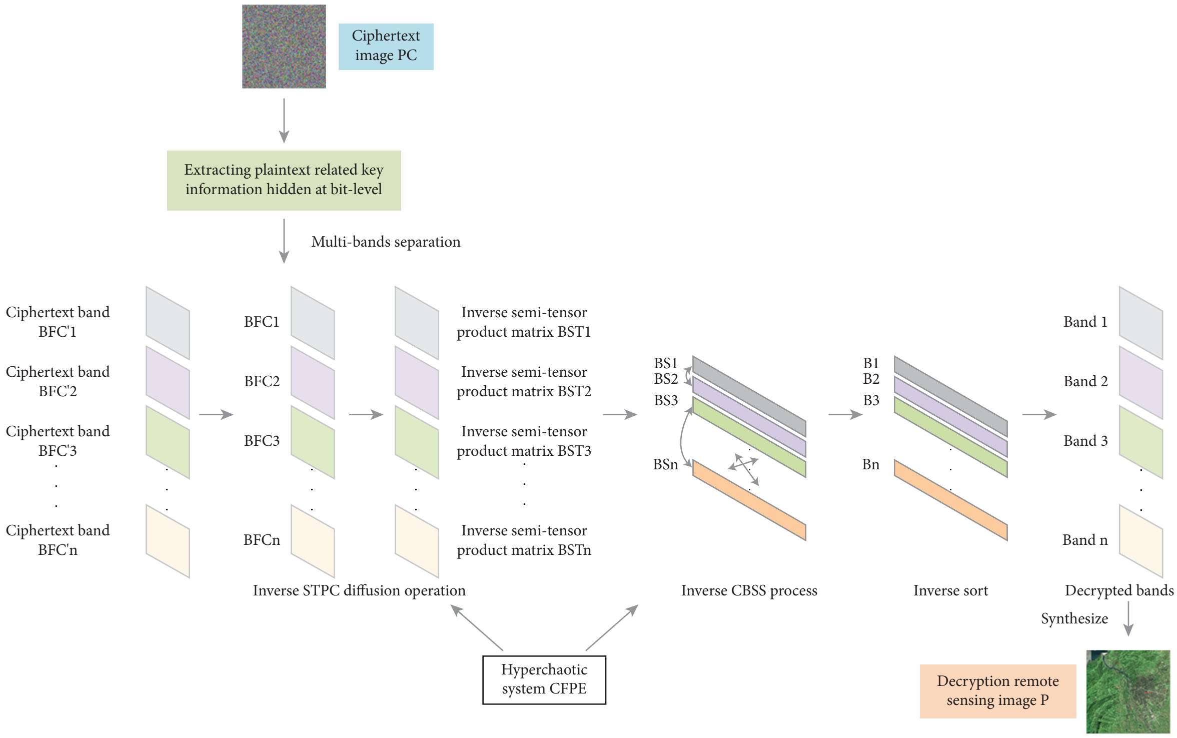

Ciphertext image PC
Extracting plaintext related key information hidden at bit-level
Multi-bands separation
Ciphertext band BFC'1
Ciphertext band BFC'2
Ciphertext band BFC'3
Ciphertext band BFC'n
BFC1
BFC2
BFC3
BFCn
Inverse semi-tensor product matrix BST1
Inverse semi-tensor product matrix BST2
Inverse semi-tensor product matrix BST3
Inverse semi-tensor product matrix BSTn
BS1
BS2
BS3
BSn
B1
B2
B3
Bn
Band 1
Band 2
Band 3
Band n
Inverse STPC diffusion operation
Inverse CBSS process
Inverse sort
Decrypted bands
Synthesize
Hyperchaotic system CFPE
Decryption remote sensing image P

Figure 9: Decryption structure.

fluctuations in the pixel value in the ciphertext image is about 70. At the same time, the effectiveness of the algorithm is proved.

For the purpose of measuring the stability of the variance of the histogram when different keys encrypt the same image, we calculated the percentage of variance difference between the original key and other different keys. As shown in Table 2, when only one parameter is changed, the variance percentage of the histogram is less than 1%, the key y_0 is the closest to stability, and the fluctuation of the key w_0 is relatively large. The difference in variance value indicates that the histogram depends on the original image in the proposed algorithm. It also proves that the scheme can resist arbitrary statistical attacks [53].

5.2.2. Correlation Coefficient Analysis. Correlation coefficient is a statistical index to reflect the close degree of correlation between variables. The closer the value of the correlation coefficient to 1, the higher the degree of correlation between the two variables. On the contrary, when the value tends to 0, two variables can be regarded as uncorrelated. In the analysis of image encryption security, the correlation coefficient is used to test the correlation of adjacent pixels. There is usually a strong correlation between the gray values of adjacent pixels in an image. Hence, a good encryption algorithm should reduce the correlation of adjacent pixels as much as possible to prevent attackers from obtaining information from adjacent pixels when intercepting ciphertext image. The correlation coefficient is calculated as follows [54]:

$$R_{pq} = \frac{\operatorname{cov}(p,q)}{\sqrt{D(p)}\sqrt{D(q)}},$$

$$\begin{cases} \operatorname{cov}(p,q) = \dfrac{1}{n}\displaystyle\sum_{i=1}^{n} p_i - E(p))(q_i - E(q)), \\ E(p) = \dfrac{1}{n}\displaystyle\sum_{i=1}^{n} p_i, D(p) = \dfrac{1}{n}\displaystyle\sum_{i=1}^{n} (p_i - E(p))^2, \\ E(q) = \dfrac{1}{n}\displaystyle\sum_{i=1}^{n} q_i, D(q) = \dfrac{1}{n}\displaystyle\sum_{i=1}^{n} (q_i - E(q))^2, \end{cases} \tag{21}$$

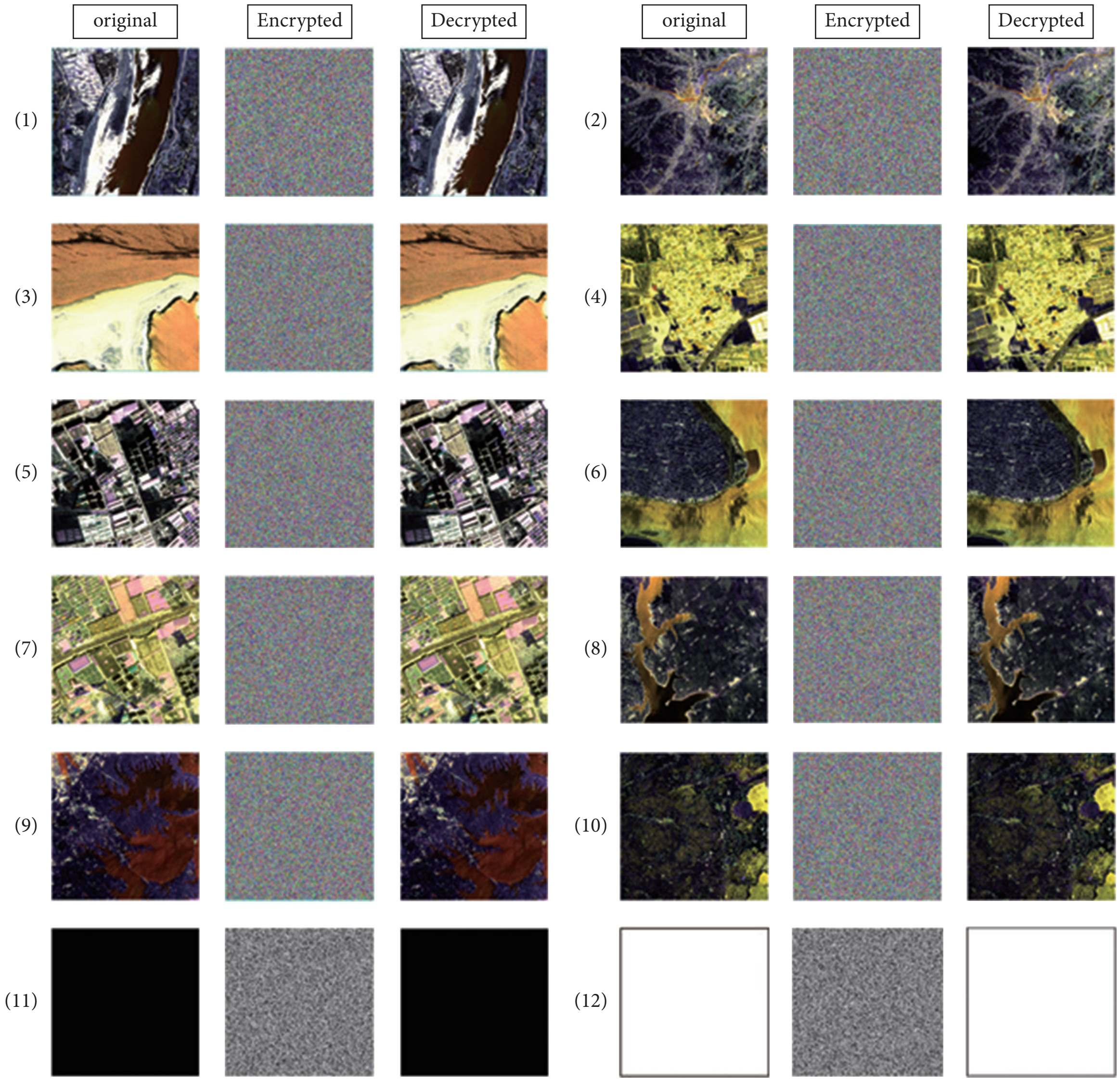


Figure 10: The encryption and decryption results. (1)–(10) show the experimental results of 10 remote sensing images; (11)–(12) are test results of all-black and all-white images, respectively.

where n is the number of pairs of adjacent pixels, p_i and q_i are a pair of adjacent pixel values, $E(p)$ is the mean of p, $E(q)$ is the mean of q, $D(p)$ is the variance of p, $D(q)$ is the variance of q, and $\operatorname{cov}(p, q)$ represents the covariance of p and q. Randomly select 5000 pairs of adjacent pixels from the original remote sensing image "Land1" and ciphertext remote sensing image, and calculate their correlation coefficients in horizontal, vertical, and diagonal directions, as shown in Table 3. In addition, compare the correlation coefficient analysis of remote sensing image encryption algorithm with other papers, which is also listed in Table 3. The correlation coefficient of the proposed algorithm is closer to 0, so the algorithm has higher security in the encryption of remote sensing images.

Figure 15 displays the distribution of adjacent pixels in the remote sensing image "Land 1," where (b–d) are the distribution of adjacent pixels in the horizontal, vertical, and diagonal of the original remote sensing image "Land 1," and (e–g) are the distribution of adjacent pixels in three directions of the ciphertext image; the distribution of adjacent pixels in the remote sensing image "Land 2" is depicted in Figure 16, where (b–d) are the distribution of adjacent pixels in the horizontal, vertical, and diagonal of the original remote sensing image "Land 2," and (e–g) are the distribution of adjacent pixels in three directions of the ciphertext image.

5.3. Information Entropy Analysis. Information entropy, proposed by Shannon [57], is used to quantify information. The more disordered the system is, the higher the information entropy is. The attackers need to cost more information to crack it. In image processing, the ciphertext image with larger information entropy can resist entropy attack. For a 256-level gray image, the maximum information entropy is 8; that is, the ideal value of information entropy is 8. Calculate the information entropy of ten remote sensing

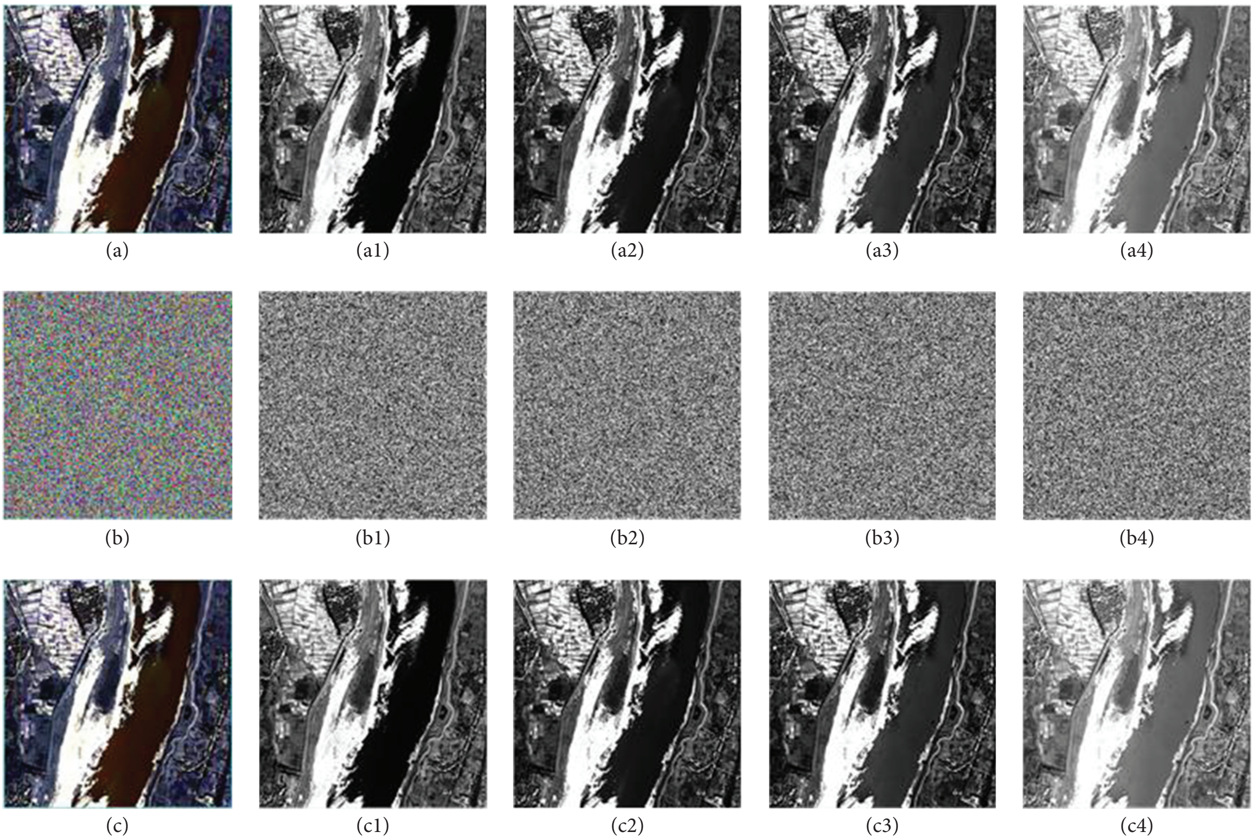


Figure 11: The encryption and decryption results of remote sensing image "Land1": (a) original remote sensing image "Land 1," (a1–a4) four bands of "Land 1," (b) the encrypted image of four bands synthesized by ENVI, (b1)–(b4) the encrypted images of four bands respectively, (c) decrypt image of "Land 1," and (c1)–(c4) decrypted images of four bands, respectively.

images captured from GID, and list the average values in Table 4. The calculation method is shown in equation (22). Among them, the highest information entropy is 7.9994. Besides, compared with other similar remote sensing image encryption algorithms [58, 59], the results show that the proposed algorithm has higher information entropy.

$$H = \sum_{i=1}^{255} p(x_i)\log_2 \frac{1}{p(x_i)}, \tag{22}$$

where x_i represents the i-th pixel value, and $p(x_i)$ represents the probability of x_i.

5.4. Plain Image Sensitivity Analysis. The plain image sensitivity indicates the impact of the small changes in the original image on the generated ciphertext image. In order to resist differential attacks, the ciphertext is required to be sufficiently sensitive to the original image. Pixel change rate (NPCR), uniform average change intensity (UACI), and blocked average changing intensity (BACI) are three major judgment indexes. The NPCR and UACI are calculated by equations (23) and (24). In Ref. [60], Zhang used some extreme examples to find that BACI can more accurately describe the visual difference between the two images compared to NPCR and UACI. Its calculation is as equation (25) [61].

$$\begin{cases} \mathrm{NPCR} = \dfrac{\sum_{i,j} D(i,j)}{MN} \times 100\%, \\ D(i,j) = \begin{cases} 0, & c(i,j) = c'(i,j), \\ 1, & c(i,j) \neq c'(i,j), \end{cases} \end{cases} \tag{23}$$

$$\mathrm{UACI} = \frac{\sum_{i,j} \left| c(i,j) - c'(i,j) \right|}{MN} \times 100, \tag{24}$$

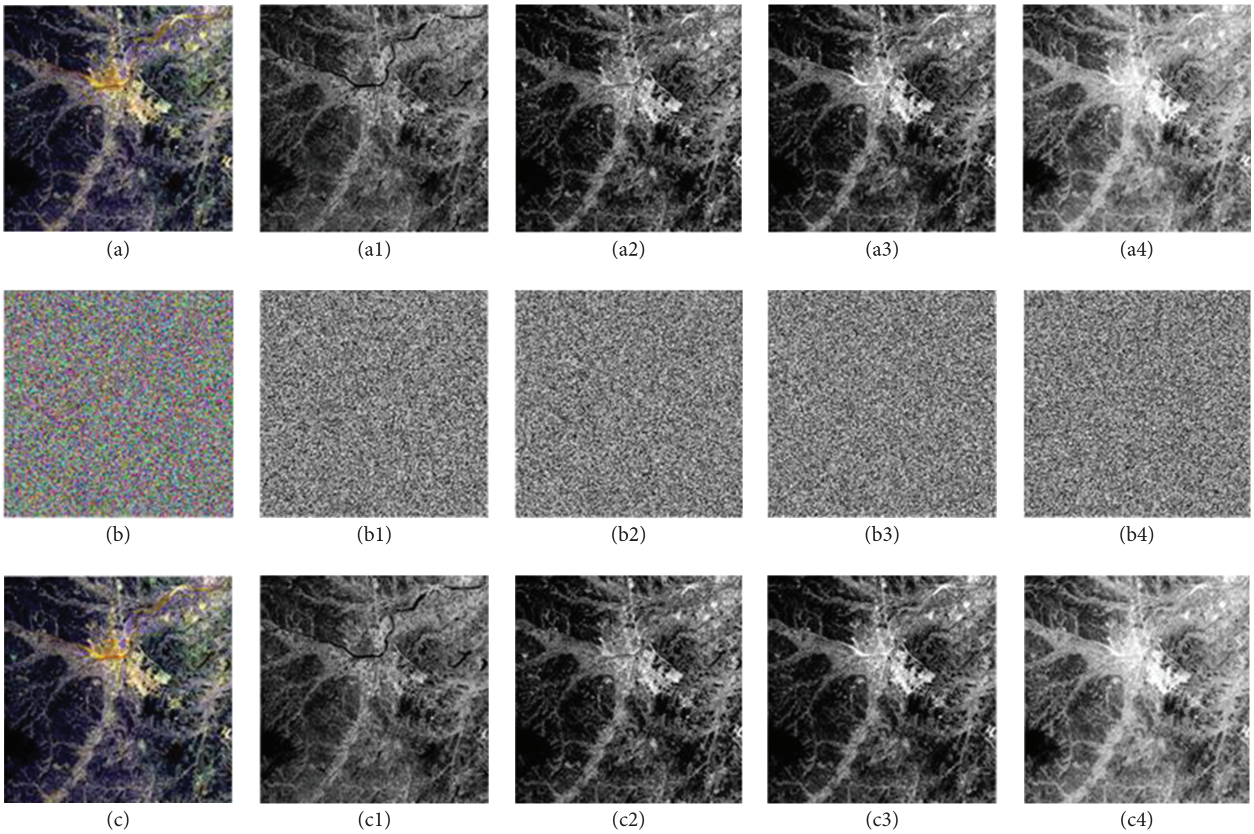


Figure 12: The encryption and decryption results of remote sensing image “Land2”: (a) original remote sensing image ”Land 2”, (a1–a4) four bands of “Land 2,” (b) the encrypted image of four bands synthesized by ENVI, (b1–b4) the encrypted images of four bands respectively, (c) decrypt image of “Land 2,” and (c1–c4) decrypted images of four bands, respectively.

$$\begin{cases} \text{BACI} = \dfrac{1}{(M-1)(N-1)} \displaystyle\sum_{i=1}^{(M-1)(N-1)} \dfrac{m_i}{255}, \\ B = \left|C - C'\right|, \\ B_i = \begin{bmatrix} b_{i1} & b_{i2} \\ b_{i3} & b_{i4} \end{bmatrix}, \\ m_i = \dfrac{1}{6}\left(\left|b_{i1} - b_{i2}\right| + \left|b_{i1} - b_{i3}\right| + \left|b_{i1} - b_{i4}\right| + \left|b_{i2} - b_{i3}\right| + \left|b_{i2} - b_{i4}\right| + \left|b_{i3} - b_{i4}\right|\right), \end{cases} \tag{25}$$

where M and N represent the size of the image. C and C' are the normal ciphertext image and the ciphertext image obtained by changing one pixel of the original image. $c(i, j)$ and $c'(i, j)$ are the pixel values of the i-th row and j-th column in the two images, respectively. Divide B into 2×2 small squares, namely, B_i, which can be divided into $(M - 1) \times (N - 1)$ blocks in total. m_i is the mean value of the i-th block B_i.

Test the ciphertext image in four bands of the original remote sensing image “Land 1” and the ciphertext image with only one pixel value changed, and get the values of NPCR, UACI, and BACI, which are listed in Table 5. The ideal values of these three indicators are 99.6094, 33.4635, and 26.7712, respectively, indicated in bold in the table.

Compared with other algorithms, it is obvious that the values of NPCR, UACI, and BACI are very close to the ideal value; what is more, the NPCR value has reached the ideal value of 99.6094% in band 1 and band 2.

In order to prove that the proposed algorithm has a strong antidifferential attack ability to any remote sensing image, without loss of generality, NPCR, UACI, and BACI of the above-mentioned ten remote sensing images are measured and plotted in line-charts. On account of that, it is an intuitive way to observe the effects. As shown in Figures 17–19, the test

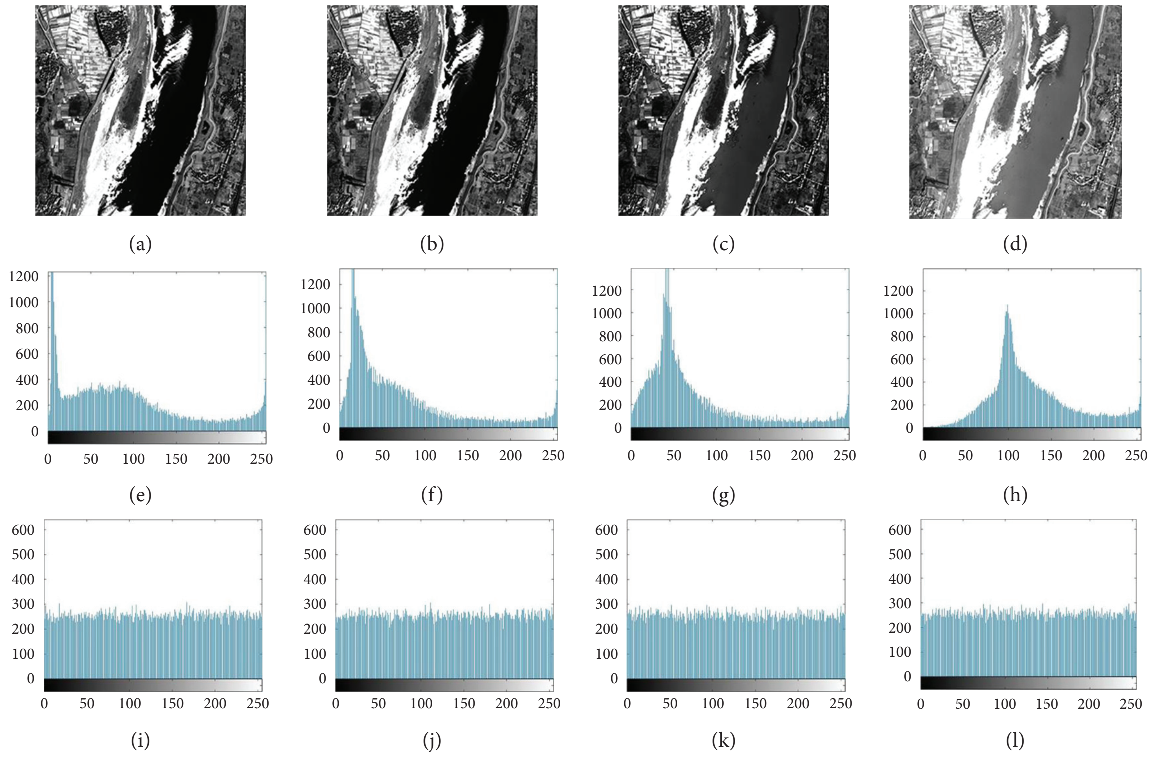


Figure 13: Histograms of remote sensing image “Land 1”: (a–d) four bands of original remote sensing image “Land 1”; (e–(h) histograms of original band 1, band 2, band 3, and band 4, respectively; (i–l) histograms of encrypted band 1, band 2, band 3, and band 4 correspondingly.

results of four bands of ten remote sensing images fluctuate around the ideal value. Therefore, the algorithm proposed in this paper has excellent resistance to differential attacks and sufficiently sensitive to the original images.

5.5. Key Analysis

5.5.1. Key Space Analysis. Key space is a crucial index to detect the ability of encryption algorithm to resist violent attacks. The larger the key space is, the more difficult it is for the attacker to crack the ciphertext image by violent attack. A key space greater than 2^{100} can resist general violent attacks [62]. Considering the initial conditions $(x_0, y_0, z_0, w_0, a, b)$, (τ_0, λ) of iterating hyperchaotic system CFPE and logistic map, there exist the user parameters K, L, and key LD during the Bit-level key hidden transmission strategy. The key space is $(10^{16})^{11} = 10^{176}$ (the precision of each initial key is 10^{16}), which is far greater than 2^{100}. Therefore, the proposed algorithm has enough key space and can easily resist the attacker’s violent attack.

5.5.2. Key Sensitivity Analysis. Key sensitivity reflects the impact of a small change in the test key on the decryption result. In algorithms with high key sensitivity, even if only one bit of the key is changed, the original image cannot be obtained. Figure 20 shows the decrypted images obtained by making minor changes to the key. It is clearly visible that although only 10^{-15} of the key is changed, the correct original image cannot be obtained. Apparently, the proposed algorithm is highly sensitive to the key.

On top of that, we also analyzed the impact of small changes in the key on the ciphertext. Make one of the keys change slightly, leaving the rest unchanged. In order to test the sensitivity of the key x_0, the remote sensing image “Land 1” is encrypted with x_0 and $x_0 + 10^{-15}$ separately. Figure 21 shows the ciphertext image generated by two security keys in the four bands of the remote sensing image, and the difference between the two images. By changing only one bit of x_0, the differences of the obtained ciphertext images of the four bands are 99.5986938%, 99.5803833%, 99.6520996 %, and 99.5712280%, respectively. When testing the sensitivity of the key y_0, use y_0 and $y_0 + 10^{-15}$ to encrypt the remote sensing image “Land 2.” The ciphertext image is generated by two security keys in the four bands of the remote sensing image, and the difference between the two images is depicted in Figure 22. By changing only one bit of y_0, the differences of the obtained ciphertext images of the four bands are 99.5727539%, 99.6200562%, 99.58648682%, and 99.61853027%, respectively. The above-mentioned analysis illustrates that the key of the proposed algorithm is highly sensitive [63].

5.6. Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity (SSIM).

PSNR is an objective indicator to measure the level of image distortion. In the field of image encryption, the PSNR value of the original image and the encrypted image can be calculated to reflect the degree of deterioration of the image after encryption. In addition, PSNR is defined by Mean Square Error (MSE). Generally, the larger MSE and the smaller PSNR indicate the greater degree of image

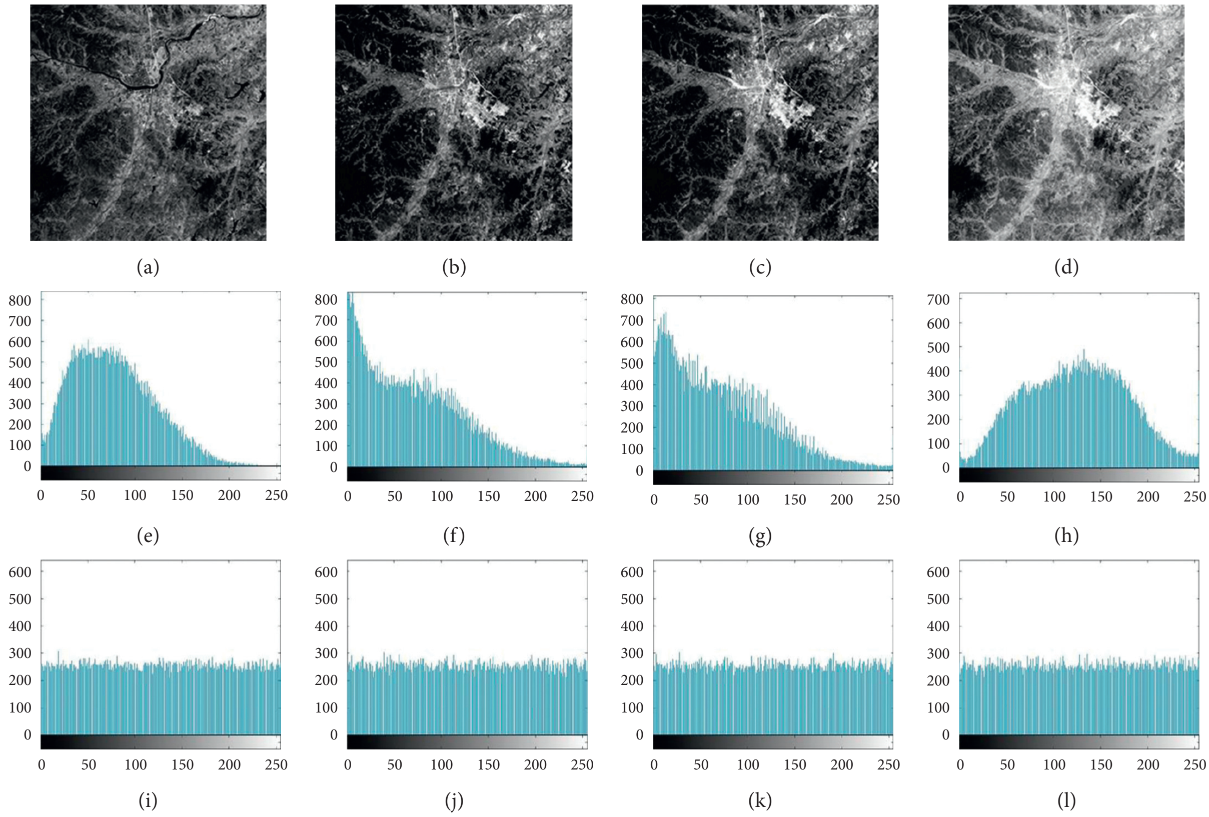


Figure 14: Histograms of remote sensing image “Land 2”: (a–d) four bands of original remote sensing image “Land 2”; (e–h) histograms of original band 1, band 2, band 3, and band 4, respectively; (i–l) histograms of encrypted band 1, band 2, band 3, and band 4 correspondingly.

distortion; that is, no trace of the original image can be seen from the encrypted image. They are defined as [64]

$$\mathrm{MSE} = \frac{1}{\mathrm{MN}} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [P(i,j) - C(i,j)]^2,$$
$$\mathrm{PSNR} = 10 \times \log_{10}\left(\frac{\mathrm{MAX}_I^2}{\mathrm{MSE}}\right), \quad (26)$$

where M and N represent the size of the image. $P(i,j)$, $C(i,j)$ represent the pixel of the original image and the ciphertext image. MAX_I is the maximum value of the pixel. Table 6 lists the PSNR and MSE results of the four bands of the remote sensing image “Land 1.”

SSIM is an index used to compare the structural similarity of two images. Give two images p and q, and the SSIM of the two images can be computed according to the following equation [65]:

$$\left\{ \mathrm{SSIM}(p,q) = \frac{\left(2\mu_p u_q + c_1\right)\left(2\sigma_{\mathrm{pq}} + c_2\right)}{\left(\mu_p^2 + \mu_q^2 + c_1\right)\left(\sigma_p^2 + \sigma_q^2 + c_2\right)}, \quad c_1 = (k_1 L)^2, c_2 = (k_2 L)^2, \right. \quad (27)$$

where μ_p is the average of p, μ_q is the average of q, σ_p is the variance of p, σ_q is the variance of q, and σ_{pq} is the covariance of p and q. Generally, L is the dynamic range of the pixel, the default is 255. $k_1 = 0.01, k_2 = 0.03$, and c_1, c_2 are constants used to maintain stability. The value range of SSIM is from 0 to 1. The larger the SSIM is, the more similar the two images are.

Test the SSIM of the four bands of the original remote sensing image “Land 1” with the encrypted image, and the SSIM of the four bands of the original remote sensing image with the decrypted image is correspondingly denoted as SSIM (P-E) and SSIM (P-D). The results are listed in Table 7. It can be found out that the proposed encryption and decryption algorithms have good security. The original pixels

Table 1: Variances of histograms compared among different secret keys in the proposed algorithm.

Ciphered image	Key	a	b	x_0	y_0	z_0	w_0
"Land 1"-band 1	5454.2782	5478.8581	5472.9992	5462.8407	5447.7279	5469.3017	5416.0631
"Land 1"-band 2	5472.8114	5477.6482	5428.1442	5493.6636	5461.4228	5459.2488	5471.6316
"Land 1"-band 3	5480.7724	5450.5600	5483.4220	5456.6077	5477.3988	5489.3375	5440.6728
"Land 1"-band 4	5455.1598	5436.5124	5438.7333	5477.4676	5462.1770	5448.0602	5502.1723
"Land 2"-band 1	5448.3267	5470.9090	5475.3840	5476.8830	5463.2324	5436.1533	5460.8489
"Land 2"-band 2	5467.5530	5462.5173	5439.5414	5476.7673	5442.1222	5436.8146	5.4543574
"Land 2"-band 3	5473.8409	5464.1859	5454.0860	5439.9397	5464.7477	5463.4851	5.4618519
"Land 2"-band 4	5469.2184	5487.1035	5474.6082	5447.6050	5462.4425	5460.6294	5.4355897
Average	5465.2451	5466.0368	5458.3648	5466.4718	5460.159	5457.8788	5455.3985

Table 2: Percentage of variances difference of histograms compared among different secret keys in the proposed algorithm.

Ciphered image	a (%)	b (%)	x_0 (%)	y_0 (%)	z_0 (%)	w_0 (%)
"Land 1"-band 1	0.45	0.34	0.16	0.12	0.28	0.70
"Land 1"-band 2	0.09	0.82	0.38	0.21	0.25	0.02
"Land 1"-band 3	0.55	0.05	0.44	0.06	0.16	0.73
"Land 1"-band 4	0.34	0.30	0.41	0.13	0.13	0.86
"Land 2"-band 1	0.41	0.50	0.52	0.27	0.22	0.23
"Land 2"-band 2	0.09	0.51	0.17	0.47	0.56	0.24
"Land 2"-band 3	0.18	0.36	0.62	0.17	0.19	0.22
"Land 2"-band 4	0.33	0.10	0.40	0.12	0.16	0.61
Average	0.31	0.37	0.39	0.19	0.24	0.45

Table 3: Correlation coefficient.

Algorithm		Horizontal	Vertical	Diagonal
Proposed	Original image	0.9070	0.8793	0.8098
	Ciphertext image	0.0007	0.0064	0.0004
Ref. [13]	Ciphertext image	0.0017	0.0153	0.0046
Ref. [44]	Ciphertext image	−0.0039	−0.0196	0.0027
Ref. [55]	Ciphertext image	−0.0047	0.0025	0.0014
Ref. [56]	Ciphertext image	0.0019	0.0038	−0.0019

will not be lost in the decryption process, which is lossless decryption.

5.7. NIST Randomness Test. The National Institute of Standard and Technology (NIST) provides a Special Publication 800 – 22 test package, called the NIST Randomness Test, which includes 16 test methods. For each test, there is a test result. If the P value is greater than 0.01, the test is successful. The main purpose of this test is to analyze the randomness of any binary sequence produced by the encryption system and determine the variety of randomness that may exist in the sequence. In this paper, we tested the four sets of chaotic sequences X, Y, Z, W generated by the CFPE chaotic system and ciphertext image. The test results are shown in Tables 8 and 9. It can be seen from Table 8 that the processed chaotic sequence has passed all NIST tests, so the generated chaotic key has randomness and meets the encryption requirements. In addition, Table 9 shows that the ciphertext image has also passed the NIST test, and the ciphertext image has good randomness.

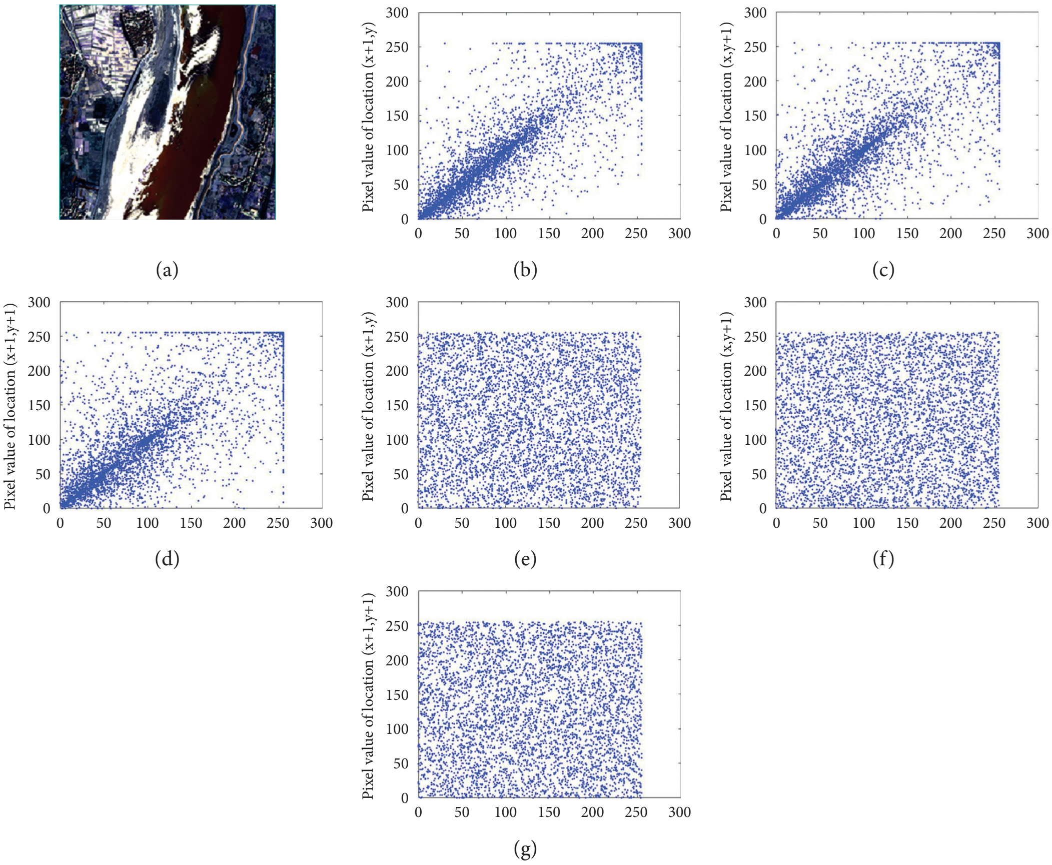
5.8. Classical Types of Attacks. Assuming that the cryptanalyst knows all the frameworks of the encryption system used, there are four classical types of attacks according to the cryptanalyst's mastery of plaintext and ciphertext information [66]:

(1) Ciphertext-only attack: the cryptanalyst has no other auxiliary information except the intercepted ciphertext

(2) Known-plaintext attack: in addition to ciphertext, the cryptanalyst has also mastered the corresponding relationship between some plaintext and ciphertext

(3) Chosen plaintext attack: the cryptanalyst has access to the encryptor and the ability to select or control the plaintext; he can choose any plaintext favorable to attack and get the corresponding ciphertext

(4) Chosen ciphertext attack: the cryptanalyst has access to the decryption machine and can select the ciphertext and get the corresponding plaintext



(a)

(b)

(c)

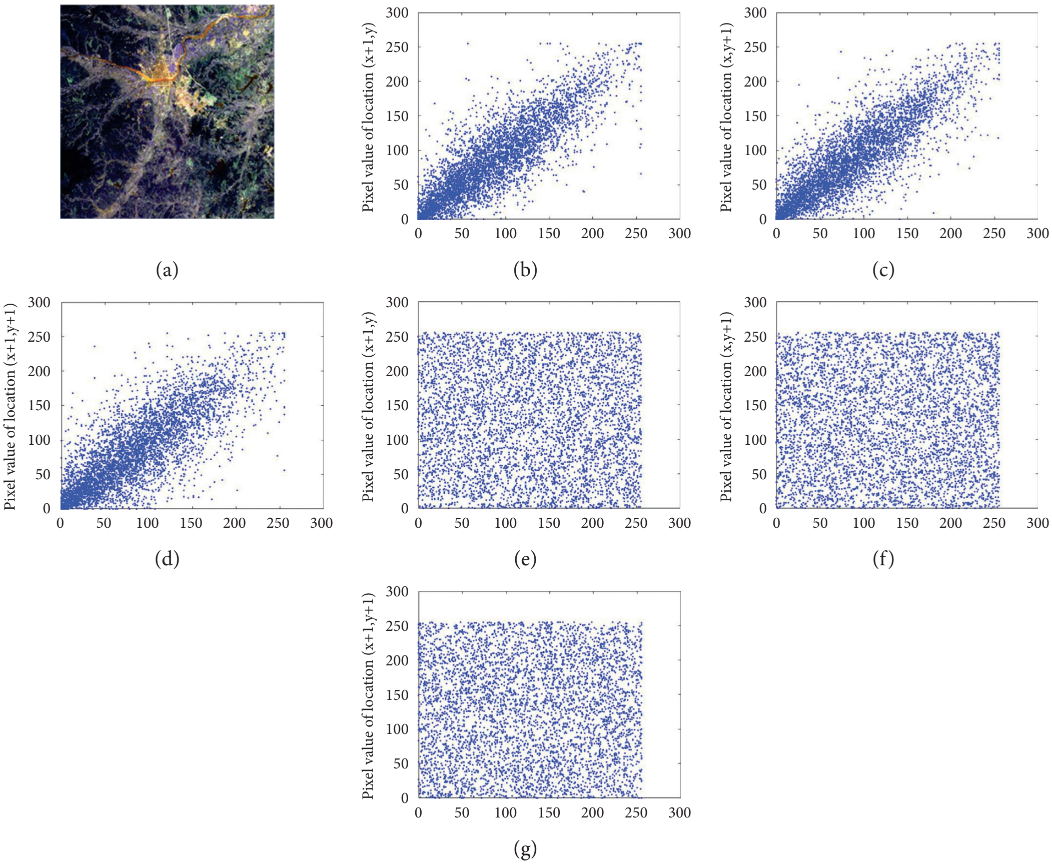
(d)

(e)

(f)

(g)

Figure 15: Remote sensing image "Land 1": horizontal, vertical, and diagonal correlation of adjacent pixels.



(a)

(b)

(c)

(d)

(e)

(f)

(g)

Figure 16: Remote sensing image "Land 2": horizontal, vertical, and diagonal correlation of adjacent pixels.

Table 4: Information entropy.

Algorithm	Information entropy
Proposed average	7.9993
Ref. [13]	7.9977
Ref. [31]	7.9972
Ref. [55]	7.9991
Ref. [58]	7.9992
Ref. [59]	7.9963
Ref. [56]	7.9974

Table 5: Plain image sensitivity.

Algorithm	Proposed		Ref. [35]	Ref. [1]	Ref. [13]	Ref. [55]	Ref. [58]	Ref. [56]	Ideal value
NPCR (%)	Band 1	99.6094	99.5700	99.6127	99.5987	99.6200	99.6100	99.5865	**99.6094**
	Band 2	99.6094	99.6200						
	Band 3	99.6048	99.6100						
	Band 4	99.5407	99.6100						
UACI (%)	Band 1	33.5062	33.4200	33.4472	33.3371	33.3800	33.5000	33.2533	**33.4635**
	Band 2	33.5841	33.4900						
	Band 3	33.4604	33.5100						
	Band 4	33.4199	33.4700						
BACI (%)	Band 1	26.7312	—	—	—	—	—	—	**26.7712**
	Band 2	26.7833	—						
	Band 3	26.7326	—						
	Band 4	26.7835	—						

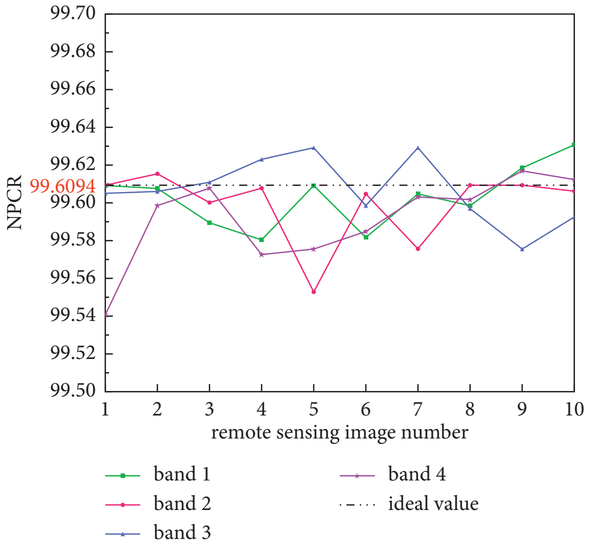


Figure 17: Line graph: NPCR values of four bands of ten remote sensing images.

It can be seen that the intensity of chosen plaintext attack is the highest. If a cryptosystem can resist chosen plaintext attack, it must be able to resist the other three classical attacks. And resistance to known-plaintext attack and chosen plaintext attack should make the key contain sequences related to the plaintext. Resistance to known-plaintext attack and chosen plaintext attack should make the key contain sequences related to the plaintext. When generating the chaotic sequence, this paper adds the chaotic key pointer p calculated from the pixel value information s of the plaintext image. And pass s through a special bit-level key hidden transmission strategy. Therefore, encrypted images rely heavily on original images in the proposed algorithm, which can effectively resist the known-plaintext attack and chosen plaintext attack.

5.9. Time Analysis. The running time can be used to measure the efficiency of encryption algorithms. Algorithms that run too long are often not suitable for practical applications. In order to test the efficiency of the proposed algorithm, the encryption time of the aforementioned 10 remote sensing

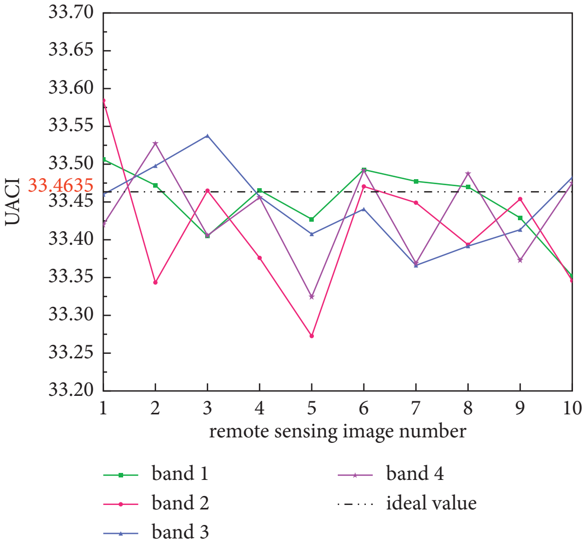


Figure 18: Line graph: UACI values of four bands of ten remote sensing images.

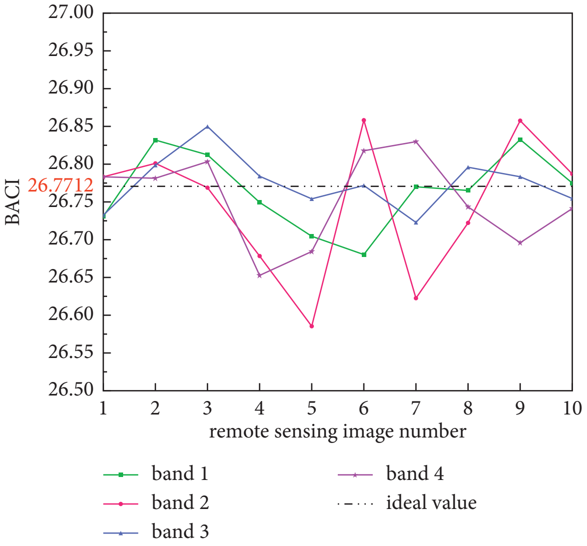


Figure 19: Line graph: BACI values of four bands of ten remote sensing images.

images was recorded, which is listed in Table 10. Calculate the average time of 10 encryptions and compare it with the current advanced encryption algorithms. It can be clearly seen from Table 11 that the encryption algorithm proposed in this paper has a great advantage in time. Since the algorithm is symmetric, the decryption time is theoretically consistent with the encryption time. Meet the needs of real-time encryption processing of remote sensing images.

5.10. Robustness Analysis. Remote sensing images may suffer from external noise pollution during transmission, and they may also face the danger of losing pixels. Remote sensing images may suffer from external noise pollution during transmission, and they may also face the danger of losing pixels. The designed algorithm should be robust enough to resist these inevitable threats.

5.10.1. Noise Attacks. Image transmission in open space is vulnerable to various noise attacks. A good encryption algorithm should be able to resist this type of attack. To this end, we add Salt and Pepper noise and Gaussian noise, respectively, to the ciphertext image and test the ability of the algorithm to resist noise attack by analyzing the recovery degree of decrypted image.

In the ciphertext image of remote sensing image "Land 1," Salt and Pepper noise of $0.1, 0.3, 0.4$ are added successively, and the image after adding noise is decrypted. The decryption results are shown in Figure 23. It is thus clear that although the decrypted image contains noise, the original image can be recovered well. In order to test the algorithm's ability to resist Gaussian attack, we add 0.2 and 0.3 Gaussian noise to the ciphertext image of "Land 1" in turn. The decryption results are depicted in Figure 24. In case of Gaussian noise attack, the proposed algorithm can also restore the original image.

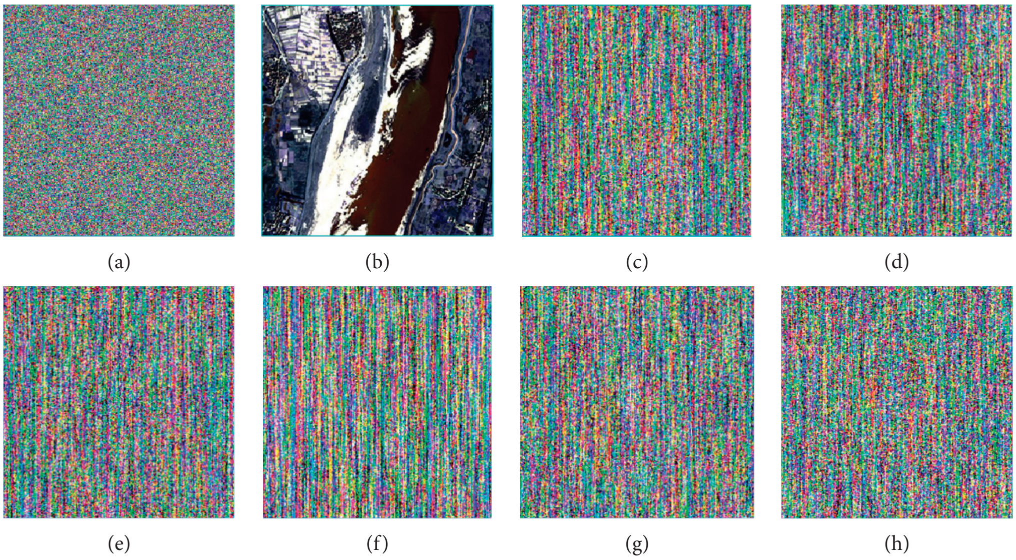


Figure 20: : (a) The ciphertext image of "Land 1." (b) The decrypted image with correct key. (c) The decrypted image with key $x_0 + 10^{-15}$. (d) The decrypted image with key $y_0 + 10^{-15}$. (e) The decrypted image with key $z_0 + 10^{-15}$. (f) The decrypted image with key $w_0 + 10^{-15}$. (g) The decrypted image with key $a + 10^{-15}$. (h) The decrypted image with key $b + 10^{-15}$.

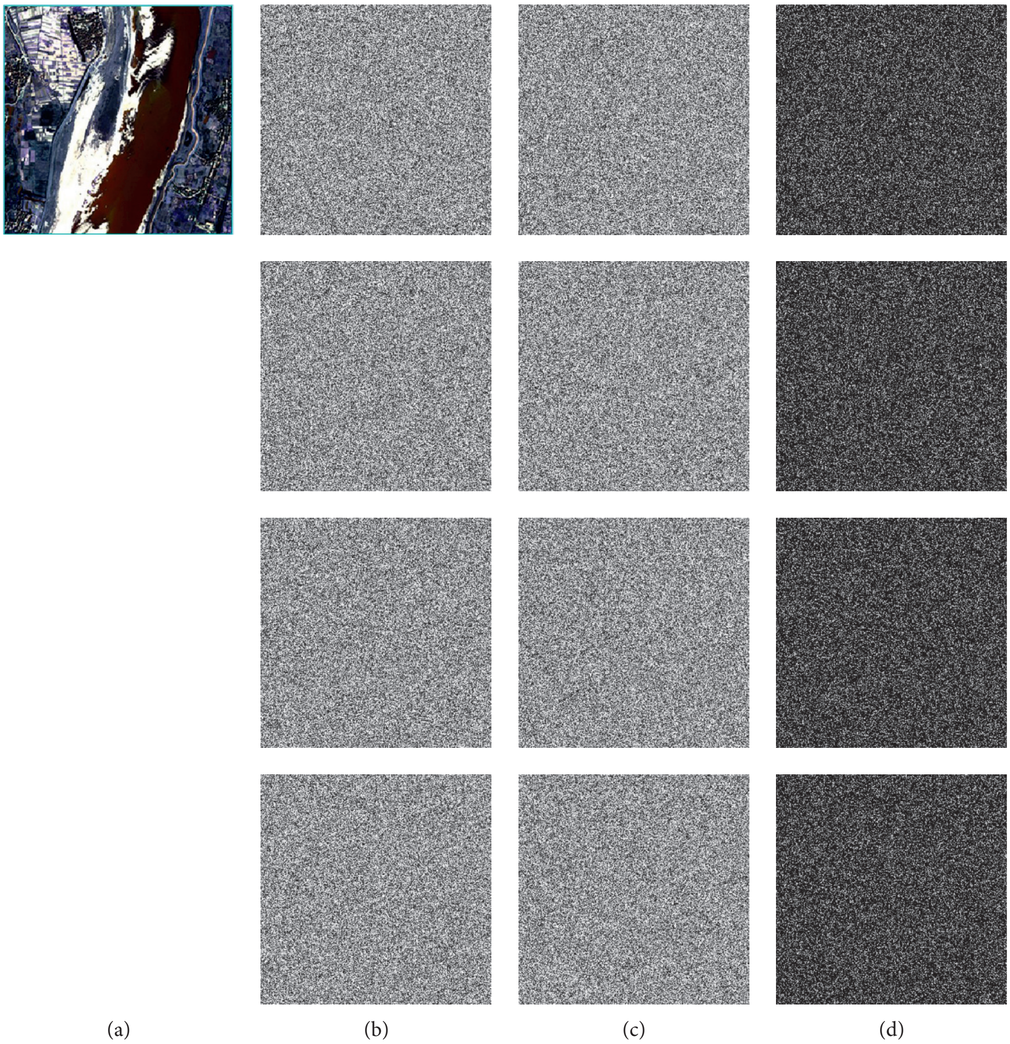


Figure 21: Key sensitivity of x_0: (a) the original remote sensing image "Land 1"; (b) ciphertext images in four bands with x_0; (c) ciphertext images in four bands with $x_0 + 10^{-15}$; (d) difference between (b) and (c).

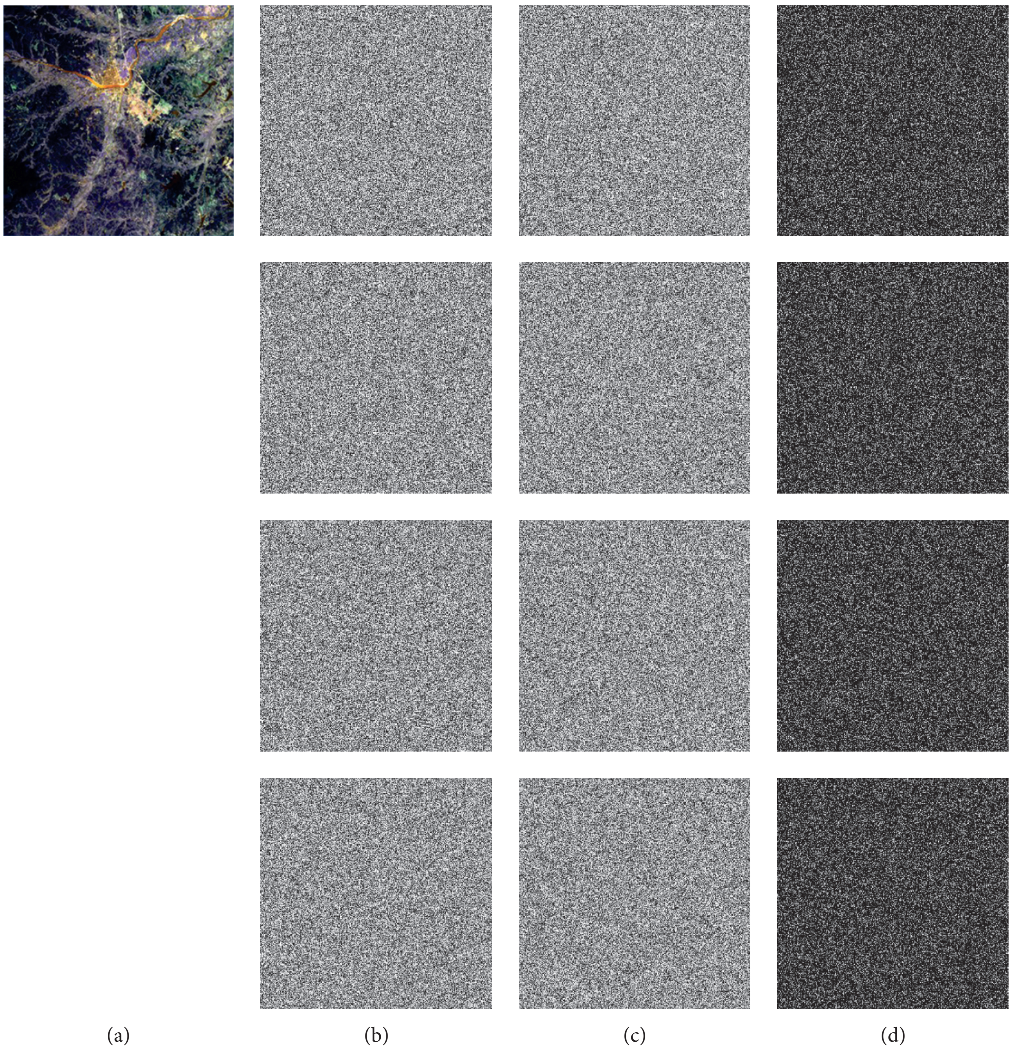


Figure 22: Key sensitivity of y_0: (a) the original remote sensing image "Land 2"; (b) ciphertext images in four bands with y_0; (c) ciphertext images in four bands with $y_0 + 10^{-15}$; (d) the difference between (b) and (c).

Table 6: PSNR and MSE results of four bands.

Index	MSE	PSNR (dB)
Band 1	13080.9182	6.9644
Band 2	13752.1862	6.7471
Band 3	13002.3486	6.9906
Band 4	9477.3510	8.3639

Table 7: SSIM results of four bands.

Index	SSIM (P-E)	SSIM (P-D)
Band 1	0.0075	1.0000
Band 2	0.0049	1.0000
Band 3	0.0079	1.0000
Band 4	0.0077	1.0000

In addition, the PSNR values of the original remote sensing image and decrypted image after the Salt and Pepper noise attack of 0.3, 0.4 and Gaussian noise of 0.3

Table 8: NIST test of the processed chaotic sequence.

Test name	P value	Result
Approximate entropy	0.378093	Success
Block-frequency	0.384873	Success
Cumulative sums forward	0.893580	Success
Cumulative sums reverse	0.905208	Success
FFT	0.604215	Success
Frequency test	0.666546	Success
Linear complexity	0.890721	Success
Long runs of ones	0.882498	Success
No overlapping templates	0.110798	Success
Overlapping templates	0.508376	Success
Rank	0.330551	Success
Runs	0.175513	Success
Serial	0.652639	Success
Serial	0.235251	Success
Universal	0.529976	Success
Random excursions	0.017341	Success
Random excursions variant	0.720249	Success

Table 9: NIST test of ciphertext.

Test name	P value	Result
Approximate entropy	0.427387	Success
Block-frequency	0.029985	Success
Cumulative sums forward	0.487697	Success
Cumulative sums reverse	0.465932	Success
FFT	0.586651	Success
Frequency test	0.977964	Success
Linear complexity	0.359776	Success
Long runs of ones	0.636096	Success
No overlapping templates	0.649028	Success
Overlapping templates	0.420637	Success
Rank	0.212753	Success
Runs	0.596840	Success
Serial	0.864691	Success
Serial	0.886909	Success
Universal	0.423527	Success
Random excursions	0.990540	Success
Random excursions variant	0.948230	Success

Table 10: Encryption time of 10 remote sensing images.

Image number	1	2	3	4	5	6	7	8	9	10
Time (s)	0.1979	0.2111	0.2571	0.2310	0.2325	0.2210	0.2347	0.2424	0.2330	0.2333

Table 11: Comparison of encryption time.

Algorithms	Time (s)
Proposed average	0.2293
Ref. [14]	5.3671
Ref. [41]	2.1328
Ref. [59]	2.8180
Ref. [65]	0.3328

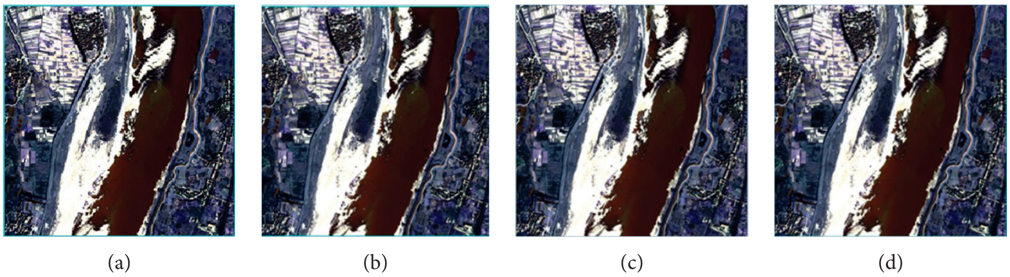


Figure 23: Salt and pepper noise attack: (a) the original remote sensing image "Land 1"; (b) decrypted image after 0.1-salt and pepper noise; (c) decrypted image after 0.3- salt and pepper noise; (d) decrypted image after 0.4- salt and pepper noise.

are individually as calculated. The data in Table 12 shows that the PSNR value is higher than 40 dB, indicating that the decrypted image is very close to the original image. The proposed algorithm is sufficient to resist noise attacks.

5.10.2. Clipping Attack. Cut the encrypted remote sensing image "Land 1" 1/8, 1/4, and 1/2, respectively. The decrypted result is as Figure 25. It is noticeable that, in the face of the cut ciphertext image, the proposed algorithm can still effectively restore the original image. Hence, the algorithm is robust.

Through the above-mentioned massive security analysis, the proposed remote sensing image encryption algorithm is safe and effective. It can ensure that remote sensing images resist various types of attacks and threats during transmission.

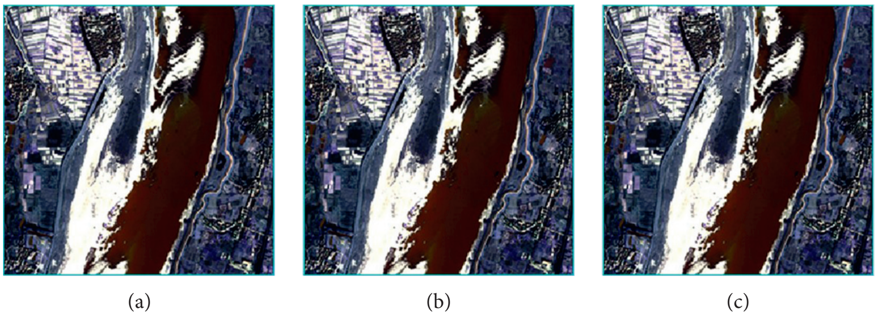


Figure 24: Gaussian noise attack: (a) original remote sensing image “Land 1”; (b) decrypted image after 0.2- Gaussian noise; (c) decrypted image after 0.3- Gaussian noise.

Table 12: The PSNR between the original images and the decrypted images in noise attacks.

Noise (“Land 1”)	Band	PSNR (dB)
0.3-salt and pepper noise	Band 1	66.8066
	Band 2	66.9355
	Band 3	66.8508
	Band 4	66.7532
0.4-salt and pepper noise	Band 1	65.1262
	Band 2	65.3300
	Band 3	65.3161
	Band 4	65.3126
0.3 Gaussian noise	Band 1	88.5141
	Band 2	91.5244
	Band 3	89.3059
	Band 4	93.2853

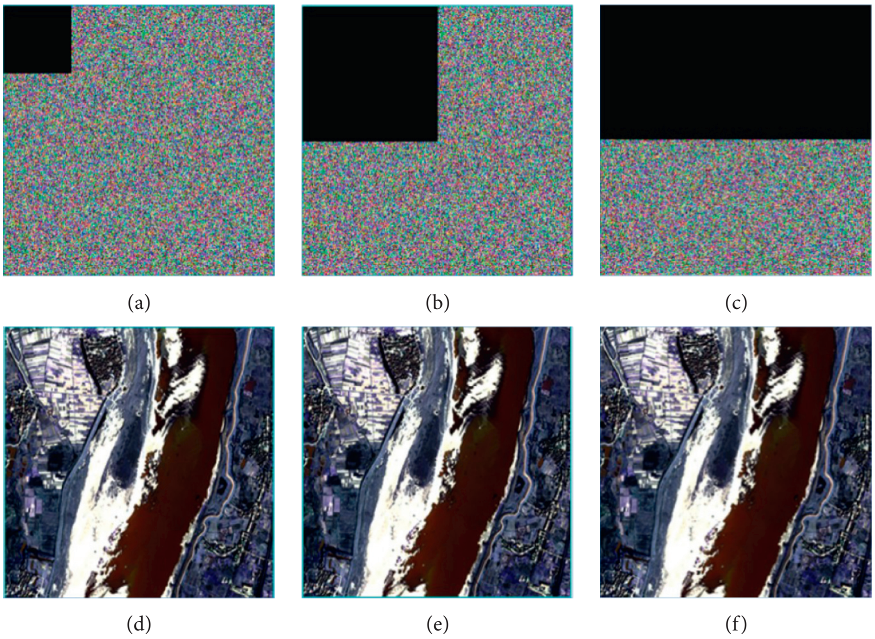


Figure 25: (a) Encrypted remote sensing image “Land 1” after 1/8 cutting and (d) the corresponding decrypted image. (b) Encrypted remote sensing image “Land 1” after 1/4 cutting and (e) the corresponding decrypted image. (c) Encrypted remote sensing image “Land 1” after 1/2 cutting and (f) the corresponding decrypted image.

6. Conclusion

We propose a new dual-channel key transmission model to deal with the plaintext related key. Furthermore, the encryption algorithm based on the combination of Boolean matrix cross-selection scrambling and semi-tensor product diffusion for the multiband characteristics of remote sensing images is designed. A simple four-dimensional chaotic system, CFPE, is used to generate Boolean matrices with cross-selection scrambling. Each band after the first scrambling of remote sensing image is cross-confused, so that each of which contains pixel information of other bands. It effectively enhances the dependence between bands and improves the security of scrambling stage. Then, the semi-tensor product is used to diffuse the pixel value of the image. Various security analysis experiments show that the proposed algorithm achieves higher information entropy and ideal index results compared with the recent encryption algorithms for remote sensing images. Although the encryption of 4-band remote sensing images is listed in this paper, the idea of this algorithm can be extended to remote sensing images of more bands. Similarly, it can also be applied to ordinary color and grayscale images encryption by reducing channels.

Data Availability

The used test images are all included in the paper.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This research was funded by the National Key Research and Development Projects (No. 2018YFB1800303); the Natural Science Foundation of Jilin Province (No. 20190201188JC); the Research on Teaching Reform of Higher Education in Jilin Province (No. JLLG685520190725093004); and the subject of Educational Science Planning in Jilin Province (No. GH180148).

References

[1] X. Wang and J. Yang, “A privacy image encryption algorithm based on piecewise coupled map lattice with multi dynamic coupling coefficient,” *Information Sciences*, vol. 569, pp. 217–240, 2021.

[2] A. S. Kumar, S. Camacho, N. D. Searby, J. Teuben, and W. Balogh, “Coordinated capacity development to maximize the contributions of space science, technology, and its applications in support of implementing global sustainable development agendas-a conceptual framework - sciencedirect,” *Space Policy*, vol. 51, 2020.

[3] P. T. Metzger and T. Philip, “Space development and space science together, an historic opportunity,” *Space Policy*, vol. 37, pp. 77–91, 2016.

[4] B. Fieque, P. Chorier, A. Lamoure, and O. Offranc, “Status of space activity and science detectors development at Sofradir,” in *Proceedings of the International Conference on Space Optics—ICSO 2018*, Chania, Greece, October 2018.

[5] J. Guo and L. Wang, “Learning to upgrade internet information security and protection strategy in big data era,” *Computer Communications*, vol. 160, pp. 150–157, 2020.

[6] G. M. Nair, “Role of communications satellites in national development,” *IETE Technical Review*, vol. 25, pp. 3–8, 2008.

[7] W. Chen, Y. Zhou, E. Zhou, Z. Xiang, W. Zhou, and J. Lu, “Wildfire risk assessment of transmission-line corridors based on naïve bayes network and remote sensing data,” *Sensors*, vol. 21, no. 2, p. 634, 2021.

[8] M. Jirousek, S. Anger, S. Dill, and M. Peichl, *Challenges in Very High Resolution Imaging of Satellites and Objects in Space*, SPIE Defense + Commercial Sensing, Baltimore, MA, USA, 2019.

[9] J. Zhou, J. Li, and X. Di, “A novel lossless medical image encryption scheme based on game theory with optimized ROI parameters and hidden ROI position,” *IEEE Access*, vol. 8, pp. 122210–122228, 2020.

[10] X. Huang and G. Ye, “An image encryption algorithm based on hyper-chaos and DNA sequence,” *Multimedia Tools and Applications*, vol. 72, no. 1, pp. 57–70, 2014.

[11] H. Liu, X. Wang, and A. kadir, “Image encryption using DNA complementary rule and chaotic maps,” *Applied Soft Computing*, vol. 12, no. 5, pp. 1457–1466, 2012.

[12] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, “A novel chaotic image encryption scheme using DNA sequence operations,” *Optics and Lasers in Engineering*, vol. 73, pp. 53–61, 2015.

[13] H. Liu, B. Zhao, and L. Huang, “A remote-sensing image encryption scheme using DNA bases probability and two-dimensional logistic map,” *IEEE Access*, vol. 7, pp. 65450–65459, 2019.

[14] I. Nadeem, H. Muhammad, A. Sagheer, K. M. Adnan, and U. R. Zia, “Dynamic 3D scrambled image based RGB image encryption scheme using hyperchaotic system and DNA encoding,” *Journal of Information Security and Applications*, vol. 58, 2021.

[15] L.-p. Chen, H. Yin, L.-g. Yuan, A. M. Lopes, J. A. T. Machado, and R.-c. Wu, “A novel color image encryption algorithm based on a fractional-order discrete chaotic neural network and DNA sequence operations,” *Frontiers of Information Technology & Electronic Engineering*, vol. 21, no. 6, pp. 866–879, 2020.

[16] A. Alghafis, F. Firdousi, M. Khan, S. I. Batool, and M. Amin, “An efficient image encryption scheme based on chaotic and Deoxyribonucleic acid sequencing,” *Mathematics and Computers in Simulation*, vol. 177, pp. 441–466, 2020.

[17] C. Adams and S. Tavares, “The structured design of cryptographically good s-boxes,” *Journal of Cryptology*, vol. 3, no. 1, pp. 27–41, 1990.

[18] S. Farwa, T. Shah, N. Muhammad, N. Bibi, A. Jahangir, and S. Arshad, “An image encryption technique based on chaotic s-box and Arnold transform,” *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 6, pp. 360–364, 2017.

[19] H. S. Alhadawi, M. A. Majid, D. Lambić, and M. Ahmad, “A novel method of s-box design based on discrete chaotic maps and cuckoo search algorithm,” *Multimedia Tools and Applications*, vol. 80, no. 5, pp. 7333–7350, 2020.

[20] W. Xingyuan, Z. Junjian, and C. Guanghui, “An image encryption algorithm based on zigzag transform and LL compound chaotic system,” *Optics & Laser Technology*, vol. 119, Article ID 105581, 2019.

[21] G. Hu and B. Li, “A uniform chaotic system with extended parameter range for image encryption,” *Nonlinear Dynamics*, vol. 103, no. 3, pp. 2819–2840, 2021.

[22] Y. Zhang, “The fast image encryption algorithm based on lifting scheme and chaos,” *Information Sciences*, vol. 520, pp. 177–194, 2020.

[23] Y. Zhang, “A new unified image encryption algorithm based on a lifting transformation and chaos,” *Information Sciences*, vol. 547, pp. 307–327, 2021.

[24] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, “A chaotic image encryption algorithm based on perceptron model,” *Nonlinear Dynamics*, vol. 62, no. 3, pp. 615–621, 2010.

[25] X. Wang, C. Liu, and D. Jiang, “A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT,” *Information Sciences*, vol. 574, pp. 505–527, 2021.

[26] H. Liu and X. Wang, “Color image encryption based on one-time keys and robust chaotic maps,” *Computers & Mathematics with Applications*, vol. 59, no. 10, pp. 3320–3327, 2010.

[27] Y.-Q. Zhang, Y. He, P. Li, and X.-Y. Wang, “A new color image encryption scheme based on 2DNLCML system and genetic operations,” *Optics and Lasers in Engineering*, vol. 128, Article ID 106040, 2020.

[28] H. Liu and X. Wang, “Color image encryption using spatial bit-level permutation and high-dimension chaotic system,” *Optics Communications*, vol. 284, no. 16-17, pp. 3895–3903, 2011.

[29] J. Wang, J. Li, X. Di, J. Zhou, and Z. Man, “Image encryption algorithm based on bit-level permutation and dynamic overlap diffusion,” *Ieee Access*, vol. 8, pp. 160004–160024, 2020.

[30] X. Wang, L. Feng, and H. Zhao, “Fast image encryption algorithm based on parallel computing system,” *Information Sciences*, vol. 486, pp. 340–358, 2019.

[31] Y. Xian and X. Wang, “Fractal sorting matrix and its application on chaotic image encryption,” *Information Sciences*, vol. 547, pp. 1154–1169, 2021.

[32] D. Cheng, “Semi-tensor product of matrices and its application to Morgen’s problem,” *Science in China*, vol. 44, pp. 195–212, 2001.

[33] H. Fan, J.-e. Feng, M. Meng, and B. Wang, “General decomposition of fuzzy relations: semi-tensor product approach,” *Fuzzy Sets and Systems*, vol. 384, pp. 75–90, 2020.

[34] S. Wang, J. Feng, J. Zhao, and J. Xia, “Controllability decomposition of dynamic-algebraic Boolean control networks,” *International Journal of Control*, vol. 93, no. 7, pp. 1684–1695, 2020.

[35] D. Cheng and Y. Dong, “Semi-tensor product of matrices and its some applications to physics,” *Methods and Applications of Analysis*, vol. 10, pp. 565–588, 2013.

[36] D.-z. Cheng and L.-j. Zhang, “On semi-tensor product of matrices and its applications,” *Acta Mathematicae Applicatae Sinica, English Series*, vol. 19, no. 2, pp. 219–228, 2003.

[37] D. Cheng, H. Qi, and A. Xue, “A survey on semi-tensor product of matrices,” *Journal of Systems Science and Complexity*, vol. 20, no. 2, pp. 304–322, 2007.

[38] X. Wang and S. Gao, “Application of matrix semi-tensor product in chaotic image encryption,” *Journal of the Franklin Institute*, vol. 356, no. 18, pp. 11638–11667, 2019.

[39] X. Wang and S. Gao, “Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network,” *Information Sciences*, vol. 539, pp. 195–214, 2020.

[40] X. Wang and S. Gao, “Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory,” *Information Sciences*, vol. 507, pp. 16–36, 2020.

[41] W. Wen, Y. Hong, Y. Fang, M. Li, and M. Li, “A visually secure image encryption scheme based on semi-tensor product compressed sensing,” *Signal Processing*, vol. 173, Article ID 107580, 2020.

[42] Z. Yu and Z. Yang, “Method of remote sensing image detail encryption based on symmetry algorithm,” *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–9, 2021.

[43] E.-H. Bensikaddour, Y. Bentoutou, and N. Taleb, “Embedded implementation of multispectral satellite image encryption using a chaos-based block cipher,” *Journal of King Saud University - Computer and Information Sciences*, vol. 32, no. 1, pp. 50–56, 2020.

[44] X. Zhang, G. Zhu, and S. Ma, “Remote-sensing image encryption in hybrid domains,” *Optics Communications*, vol. 285, no. 7, pp. 1736–1743, 2012.

[45] G. Ye and X. Huang, “A novel block chaotic encryption scheme for remote sensing image,” *Multimedia Tools and Applications*, vol. 75, no. 18, pp. 11433–11446, 2016.

[46] X. Huang, G. Ye, H. Chai, and O. Xie, “Compression and encryption for remote sensing image using chaotic system,” *Security and Communication Networks*, vol. 8, no. 18, pp. 3659–3666, 2015.

[47] Y. Bentoutou, E.-H. Bensikaddour, N. Taleb, and N. Bounoua, “An improved image encryption algorithm for satellite applications,” *Advances in Space Research*, vol. 66, no. 1, pp. 176–192, 2020.

[48] A. Bayani, K. Rajagopal, A. J. M. Khalaf, S. Jafari, G. D. Leutcho, and J. Kengne, “Dynamical analysis of a new multistable chaotic system with hidden attractor: antimonotonicity, coexisting multiple attractors, and offset boosting,” *Physics Letters A*, vol. 383, 2019.

[49] Z. J. Huang, S. Cheng, L. H. Gong, and N. R. Zhou, “Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform,” *Optics and Lasers in Engineering*, vol. 124, Article ID 105821, 2020.

[50] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, “A color image cryptosystem based on dynamic DNA encryption and chaos,” *Signal Processing*, vol. 155, pp. 44–62, 2019.

[51] X. Chai, J. Fu, J. Zhang, D. Han, and Z. Gan, “Exploiting preprocessing-permutation–diffusion strategy for secure image cipher based on 3D latin cube and memristive hyperchaotic system,” *Neural Computing & Applications*, vol. 33, pp. 1–32, 2021.

[52] X.-Y. Tong, G.-S. Xia, Q. Lu et al., “Land-cover classification with high-resolution remote sensing images using transferable deep models,” *Remote Sensing of Environment*, vol. 237, Article ID 111322, 2020.

[53] Y.-Q. Zhang and X.-Y. Wang, “A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice,” *Information Sciences*, vol. 273, pp. 329–351, 2014.

[54] G. Ye, K. Jiao, X. Huang, B.-M. Goi, and W.-S. Yap, “An image encryption scheme based on public key cryptosystem and quantum logistic map,” *Scientific Reports*, vol. 10, no. 1, 2020.

[55] X. Zhang and X. Wang, “Remote-sensing image encryption algorithm using the advanced encryption standard,” *Applied Sciences*, vol. 8, no. 9, p. 1540, 2018.

[56] X. Wang, L. Liu, and Y. Zhang, “A novel chaotic block image encryption algorithm based on dynamic random growth technique,” *Optics and Lasers in Engineering*, vol. 66, pp. 10–18, 2015.

[57] C. E. Shannon, “A mathematical theory of communication,” *Bell System Technical Journal*, vol. 27, no. 4, pp. 623–656, 1948.

[58] M. Sedighi, S. K. Mahmoudi, and A. S. Amini, “Proposing a new method for encrypting satellite images based ON hash function and chaos parameters,” in *Proceedings of the 2019 GeoSpatial Conference 2019 – Joint Conferences of SMPR and GI Research*, pp. 949–953, University of Tehran, Tehran, Iran, 12-14 October 2019.

[59] M. Madani, Y. Bentoutou, and N. Taleb, “An improved image encryption algorithm based on cyclic rotations and multiple chaotic sequences: application to satellite images,” *Journal of Electrical and Electronics Engineering*, vol. 10, pp. 29–34, 2017.

[60] Y. Zhang, “The unified image encryption algorithm based on chaos and cubic s-box,” *Information Sciences*, vol. 450, pp. 361–377, 2018.

[61] Y. Wu, J. P. Noonan, and S. Agaian, “NPCR and UACI randomness tests for image encryption. cyber journals: multidisciplinary journals in science and technology,” *Journal of Selected Areas in Telecommunications (JSAT)*, vol. 1, pp. 31–38, 2011.

[62] G. Alvarez and S. Li, “Some basic cryptographic requirements for chaos-based cryptosystems,” *International Journal of Bifurcation and Chaos*, vol. 16, no. 08, pp. 2129–2151, 2006.

[63] Y.-Q. Zhang and X.-Y. Wang, “A new image encryption algorithm based on non-adjacent coupled map lattices,” *Applied Soft Computing*, vol. 26, pp. 10–20, 2015.

[64] M. Zhou and C. Wang, “A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks,” *Signal Processing*, vol. 171, Article ID 107484, 2020.

[65] Z. Hua, K. Zhang, Y. Li, and Y. Zhou, “Visually secure image encryption using adaptive-thresholding sparsification and parallel compressive sensing,” *Signal Processing*, vol. 183, Article ID 107998, 2021.

[66] X. Wang, L. Teng, and X. Qin, “A novel colour image encryption algorithm based on chaos,” *Signal Processing*, vol. 92, no. 4, pp. 1101–1108, 2012.