Earth Science Informatics
https://doi.org/10.1007/s12145-024-01424-1

RESEARCH

A novel secure scheme for remote sensing image transmission: an integrated approach with compression and encoding

Haiyang Shen[1,2] · Jinqing Li[1,2] · Xiaoqiang Di[1,2,3] · Xusheng Li[1,2] · Zhenxun Liu[1,2] · Makram Ibrahim[4]

Received: 12 April 2024 / Accepted: 21 July 2024

Abstract

With the advancement of technology and the maturity of various aerial imaging techniques, data proprietors have awareness of the importance of secure protection for remote sensing images. In order to protect sensitive data of images, we propose a secure encoding scheme for compressing remote sensing images to decrease potential risks of data disclosure associated with such images. First, we designed the Sin chaos paradigm for constructing chaotic systems in various dimensions. As a result through relevant experiments, this chaos paradigm demonstrated effective scalability and stability. In addition, DNA transposition methods have been introduced to extend DNA encoding, expanding the range of DNA encoding from 1 to 4 and achieving dynamic selection of DNA transposition methods. This method reduces potential threats that conflict with fixed DNA encoding methods. In addition, in order to ensure the security of symmetric encryption and the efficiency of asymmetric encryption during key transmission, an elliptical curve "ring" key hiding strategy is adopted. Although the key embedding occupies 1.2% of the space in the ciphertext image, data redundancy realizes the implicit transmission of the key, improving the decryption efficiency of remote sensing images. In response to the above research, we propose a secure compression encoding scheme based on Sin chaotic paradigm and DNA transposition to ensure the security of remote sensing images. After cropping the original remote sensing image to a size of 1/16, the original image can still be decrypted. In addition, when the noise attack reaches 0.3, the ciphertext image can also be restored. Performance analysis and experimental data results show that our proposed secure compression encoding scheme has excellent robustness and security.

Keywords Sin Chaos paradigm · Image security · DNA transversion · "Ring" key concealment transmission

Introduction

With the development of technology and the progress of the times, satellite remote sensing has gradually entered people's field of vision (Rementeria 2022). The distribution of marine resources, changes in climate and the environment, geographical landscapes, and the monitoring of geological disasters are all closely related to the lives of all of humanity (Zhang and Wang 2022). In order to gain a deeper understanding of the land we inhabit, for the sustainable development of Earth's resources, and for the future habitat of our descendants, we need to explore our planet and apply technology to the maintenance of its sustainable development (Maiwald 2023). Because satellite remote sensing can accurately capture changes in the ocean, land, and climate (Zheng et al. 2023), and provide more reference value for protecting the Earth, many researchers have invested in the study of satellite remote sensing (Alsubaei et al. 2023). Due to the large volume of remote sensing data and the complexity of processing, many researchers have studied issues related to securely transmitting post-processed remote sensing data to authorized users and securely storing remote sensing data images (Yuan and Hao 2020). One of the most common methods is to convert remote sensing data images into visually unrecognizable noise images (ciphertext images) to ensure security

Communicated by: Hassan Babaie

✉ Jinqing Li
lijinqing@cust.edu.cn

1 School of Computer Science and Technology, Changchun University of Science and Technology, Changchun, China

2 Jilin Province Key Laboratory of Network and Information Security, Changchun, China

3 Information Center of Changchun University of Science and Technology, Changchun, China

4 National Research Institute of Astronomy and Geophysics, Helwan, Egypt

Published online: 06 August 2024

in ciphertext images. Common remote sensing data image processing techniques involve the following technical fields: chaotic systems (Li et al. 2022), DNA coding (Yildirim 2022; Chen et al. 2023; Zheng et al. 2021), key transmission (Wang et al. 2022; Liu et al. 2021), compressed sensing (Bao and Zhu 2022; Nan et al. 2022) and other related technologies.

Chaos systems exhibit characteristics such as high sensitivity to control parameters and initial conditions, a large key space, non-linearity, and pseudo-randomness (Zheng et al. 2021). They are often referred to as the "darlings of cryptography" and find wide applications in areas such as key generation and image encryption. Chaos arises within nonlinear systems within specific parameter ranges, resulting in complex chaotic behavior. The existence of chaotic behavior offers extensive prospects for the application of chaotic systems in the field of cryptography. In the realm of one-dimensional chaotic systems, Meng et al. (2022) proposed a DICOM region of interest encryption scheme based on a one-dimensional $e^{\lambda-\cos-cot}$ chaotic map. Wang et al. (2020) introduced an image protection encryption scheme based on one-dimensional sinusoidal chaos system (I1DS) using dynamic shift and synchronous shuffle diffusion. Feng et al. (2023) proposed a new fractional order three-dimensional Lorenz chaotic system and a two-dimensional sine constrained polynomial hyperchaotic map. Based on the new chaotic system, more key space is obtained to solve the problem of multi image encryption. The proposal of this scheme provides us with new ideas on how to design a scalable chaotic system to solve the security problem of remote sensing images. Liang and Zhu (2023) introduced a one-dimensional sinusoidal cosine chaotic map (SCCM) and utilized multiple chaotic sequences within SCCM to permute the rows and columns of an image for enhanced security. In order to improve the security of encryption algorithms, Feng et al. (2024) proposed an efficient IE algorithm based on 2D-SQPM and pixel fusion strategy (IEASP). This scheme uses a universal key stream to avoid the need for constantly changing keys, and pixel fusion reduces the computational cost of encryption operations. The use of two rounds of vector level image filtering, chaotic pixel stacking, and fast intra vector scrambling methods has improved the encryption speed and enhanced the security of the encryption algorithm. In high-dimensional chaotic systems, Gao et al. (2023) introduced a three-dimensional model encryption scheme based on cascaded chaotic systems, providing a key pool for encryption schemes. Wang et al. (2022) presented a high-dimensional chaotic system with conditional symmetry. While existing chaotic systems have shown almost perfect advantages in research, they face the challenge of handling large-scale remote sensing data images that require a massive data volume, a larger key space, and a broader range of parameter choices. Hence, an extensible Sin paradigm chaotic system has been proposed, allowing for the construction of chaotic systems with different dimensions to cater to diverse requirements and increasing the flexibility of chaotic systems. Chaotic systems constructed under this paradigm exhibit excellent chaotic properties and randomness, as demonstrated through various performance analyses.

Due to the large amount of data in remote sensing images, improving the encryption efficiency of remote sensing images by reducing the amount of data is a concern. However, how can we reduce the amount of data in remote sensing images? (Eldin et al. 2009) further improved the performance of the system by concatenating powerful channel codes such as Low Density Parity Check (LDPC) coding with space-time block coding OFDM scheme. With this approach, the storage proportion of remote sensing images was reduced by converting between different domains, thereby compressing remote sensing images, reducing the amount of data in remote sensing images, and improving the transmission efficiency of remote sensing images. Due to the difference between remote sensing images and ordinary digital images, remote sensing images have the characteristic of multiple bands. How to ensure the security of each band in remote sensing images is a key issue that we need to consider. Feng et al. (2022) converted planar images into three-dimensional images, and then performed three rounds of planar level permutation, planar level pixel filtering, and three-dimensional chaotic image superimposition, which is very suitable for multi band remote sensing images. Therefore, capturing the features of different bands of remote sensing images for band segmentation and cross plane encryption is another key point of our research.

DNA encoding is a term rooted in the biological domain. Due to its complex and versatile combination methods, as well as the close relationship between DNA encoding and digital data, many scholars have applied DNA encoding to the process of image encryption, increasing the complexity of encryption schemes. In the field of image security, DNA encoding plays a crucial role. For instance, Yildirim (2022) enhanced the security of optical images by applying DNA encoding to optical image encryption. Feng et al. (2021) proposed an image encryption scheme based on Feistel network and dynamic encoding of deoxyribonucleic acid (DNA). This scheme analyzes the vulnerabilities in the encryption scheme to avoid security risks during the encryption process and improve the stability and security of the encryption scheme. Bao and Zhu (2022) combined DNA encoding with compressed sensing, thereby improving the robustness and security of the encryption scheme. While DNA encoding enhances the security of encryption schemes, it can introduce security risks due to its fixed combination methods. In order to verify the security of DNA encoding, Wen and Lin (2024) proposed a cryptographic analysis scheme for image encryption using quantum chaotic mapping and DNA encoding. This scheme first obtains an equivalent permutation key

through differential cryptographic analysis, then uses only four special plaintext images and their corresponding cryptographic images to eliminate DNA domain substitution based on selective plaintext attacks, and finally restores the original plaintext image. Experimental results have shown that there are certain security risks associated with using DNA encoded encryption schemes; In addition, Wen and Lin (2023) proposed a cryptanalyzing an image cipher using multiple Chaos and DNA operations also confirmed the existence of certain security risks in DNA encoding, and proposed a method for selecting plaintext attacks on ICIC-DNA. Firstly, differential analysis is used to decipher the DNA base arrangement process, followed by the elimination of DNA domain encryption, and finally, a complete decryption is achieved using an equivalent key. Feng et al. (2021) demonstrated through analysis of image encryption schemes based on pixel level filtering and DNA level diffusion (PFDD) that their encryption schemes are insufficient to resist selected plaintext attacks (CPAs). The above analysis shows that in order to ensure the security of remote sensing images, it is necessary to break the original DNA combination method. As a result, we propose DNA transversion. Building upon the original DNA encoding, DNA transversion expands the selection range and combination methods of DNA encoding, thus addressing the security risks associated with the aforementioned issues. Finally, by combining plaintext images with chaotic systems, we can resist the chosen plaintext attack to ensure the security, stability, and robustness of our proposed encryption scheme.

In cryptography, there exist symmetric encryption algorithms and asymmetric encryption algorithms. To enhance image security, many researchers have conducted extensive research by combining symmetric encryption with image encryption. For example, Lone and Qureshi (2022) integrated symmetric keys with chaotic systems to enhance image security. Symmetric encryption is known for its speed and resource efficiency; however, it faces challenges when it comes to secure key transmission and distribution. Additionally, Chen and Ye (2022) proposed an asymmetric image encryption scheme by combining SHA-3 and RSA. As for asymmetric encryption, it ensures secure key transmission and distribution through public-private key pairs, but it involves significant resource overhead, making it challenging to improve performance in large-scale data encryption scenarios. In order to protect the security of encryption keys, Alshaer et al. (2021) improved system security and reduced quantum bit error rate through quantum key distribution technology. This scheme provides us with a new idea for protecting the keys of remote sensing images. How to prevent key leakage, ensure the security and robustness of the keys, is another important focus for us to protect the security of remote sensing images. Eldin et al. (2009) used two wavelet functions with adaptive frame size to embed encrypted watermarks in low-frequency components. Only the authorized party can detect the copyright information embedded in the host audio signal, which has good security. The method of verifying data integrity through key hiding is also applicable to images. Therefore, we propose an elliptic curve ring key hiding strategy to ensure the security of the key. In view of the aforementioned issues, we propose an elliptic curve and a "ring" key hiding and transmission strategy, which effectively circumvents the problems associated with secure key transmission in symmetric encryption and the resource overhead in asymmetric encryption schemes.

Sum of the relevant research mentioned above, this paper proposes a secure transmission, compression, and encoding scheme based on the Sin paradigm and DNA transversion. This scheme is designed to safeguard the security of remote sensing images. Through a series of performance analyses and tests, it has been verified that the encryption scheme proposed in this paper is eligible to be employed for protecting the security of remote sensing images. The contributions of this paper are as follows:

(1) Designed a Sin paradigm for constructing chaotic systems, which can be used to create chaotic systems of different dimensions, all of which exhibit outstanding chaotic behavior.
(2) A novel DNA transversion encoding rule is proposed, which combines DNA transversion with DNA encoding rules to achieve dynamic selection of transformation rules and ensure the stability and security of the encryption scheme.
(3) An elliptic curve "Ring" key concealment transmission strategy is designed based on elliptic curves, which is capable to solve effectively the leakage risk of key transmission in symmetric cryptography systems, also resist known plaintext attacks and chosen plaintext attacks.
(4) A secure compression encoding scheme for remote sensing images is proposed that the original image could be restored even the compression ratio reaches 25%.

The rest of the article is described as follows: Section "Definition of Sin paradigm" describes the process of designing chaotic systems using the Sin paradigm and performs experimental analysis of the chaotic system. Section "DNA transversion(DNA-TRV)" describes the DNA coding and decoding rules, the proposed DNA transversion rules, and the conversion process of the three rules. Section "The elliptic curve "Ring" hiding and transmission strategy" describes the elliptic curve "Ring" key transmission hiding strategy In Section "Secure compression encoding of remote sensing images", the specific process of the encryption scheme. Section "Experimental analysis" analyzes the experimental results, security performance, and future prospects of the encryption scheme.

Definition of Sin paradigm

In this section, we will provide a detailed introduction to the process of constructing chaotic systems using the Sin paradigm, and analyze the performance of different dimensions of chaotic systems constructed using the Sin paradigm to demonstrate the feasibility of our proposed Sin paradigm for constructing chaotic systems.

Basic one-dimensional chaotic system definition

The Sin paradigm is designed by coupling two underlying chaotic systems (Cubic mapping and Iterative mapping) with deformation tuning parameters. The mathematical representation of the Cubic mapping (Zhou et al. 2023) is as follows:

$$U_{i+1} = \varphi U_i \left(1 - U_i^2\right) \tag{1}$$

φ in the above equation is the control parameter, and here we set the initial value $U_i = 0.2$. The Iterative mapping is a one-dimensional iterative mapping (He et al. 2001) proposed by Alexander Mikhailov in 1993 with the following mathematical representation:

$$V_{j+1} = \sin\left(\frac{\sigma\pi}{V_j}\right) \tag{2}$$

σ in the above equation is the control parameter, and here we set the initial value $V_i = 0.3$. Like many one-dimensional chaotic systems, Cubic and Iterative mappings have chaotic behavior and are simple and fast, however, they have some limitations, such as small key space, unstable chaotic systems and insufficient nonlinearity. Therefore, we have to seek new algorithms to build excellent chaotic systems for generating keys.

$\mathbb{Z}D - \mathrm{Sin}^{\mathbb{Z}}$ chaotic systems

In order to address the shortcomings of one-dimensional chaotic systems, we propose a Sin paradigm that can not only construct chaotic systems of different dimensions, but also exhibit good nonlinear and chaotic performance.

Definition of $\mathbb{Z}D - \mathrm{Sin}^{\mathbb{Z}}$ chaotic systems

The definition of Sin paradigm is as follows:

$$\aleph_{n+1}^{\mathbb{Z}} = \sin\left(\pi\omega\left(1 - \beth_n^{2^{\mathbb{Z}}}\right) + \sin\left(\frac{\omega}{\aleph_n^{\mathbb{Z}}}\right)\right) \tag{3}$$

In the above Sin paradigm, $\aleph$ and $\beth$ represent the state variables of the paradigm, $\mathbb{Z}$ indicates the dimensionality of the paradigm, n denotes the number of iterations of the paradigm, and ω represents the control parameter of the paradigm. Next, we will describe the complete construction process of the Sin paradigm through Algorithm 1.

Algorithm 1 The construction process of the Sin paradigm.

Input: The Iterative map, the Cubic map.
Output: The hyperchaotic system $2D - Sin^2$.

1: Through the iteration of mappings and cubic mappings, we have devised a paradigm for generating chaotic sequences. $\omega \in R^+$ as the control parameter , $\aleph$,$\beth$ are the state variables of this system, $\mathbb{Z}$ represents the dimension of the paradigm.
$$\aleph_{n+1}^{\mathbb{Z}} = \omega\left(1 - \beth_n^{2^{\mathbb{Z}}}\right) + \sin\left(\frac{\omega}{\aleph_n^{\mathbb{Z}}}\right)$$
2: Employ π as the added coefficient to modulate the global map in step 1:
$$\aleph_{n+1}^{\mathbb{Z}} = \pi\omega\left(1 - \beth_n^{2^{\mathbb{Z}}}\right) + \sin\left(\frac{\omega}{\aleph_n^{\mathbb{Z}}}\right)$$
3: Control the output result range of the whole function in step 2 through Sine mapping to be $(-1, 1]$, the final paradigm is as follows:
$$\aleph_{n+1}^{\mathbb{Z}} = \sin\left(\pi\omega\left(1 - \beth_n^{2^{\mathbb{Z}}}\right) + \sin\left(\frac{\omega}{\aleph_n^{\mathbb{Z}}}\right)\right)$$
4: According to the comparison of time and memory consumption in different dimensions in Fig. 1, in order to save computational resources while generating a sufficient number of chaotic sequences, based on the above paradigm, a two-dimensional chaotic system was constructed and named $\mathbb{Z}D - Sin^{\mathbb{Z}}$.
$$\begin{cases} {x_{n+1}}^2 = \sin\left(\pi\omega\left(1 - {y_n}^{2^2}\right) + \sin\left(\frac{\omega}{{x_n}^{2^2}}\right)\right) \\ {y_{n+1}}^2 = \sin\left(\pi\omega\left(1 - {x_n}^{2^2}\right) + \sin\left(\frac{\omega}{{y_n}^{2^2}}\right)\right) \end{cases}$$

According to Algorithm 1, when $\mathbb{Z} = 1$, the constructed one-dimensional chaotic system ($1D - Sin^1$) is shown in Eq. 4:

$${x_{n+1}}^1 = \sin\left(\pi\omega\left(1 - {y_n}^{2^1}\right) + \sin\left(\frac{\omega}{{x_n}^1}\right)\right). \tag{4}$$

According to the above Algorithm 1, when $\mathbb{Z} = 2$, the constructed two-dimensional chaotic system ($2D - \mathrm{Sin}^2$) is shown in Eq. 5:

$$\begin{cases} {x_{n+1}}^2 = \sin\left(\pi\omega\left(1 - {\mathrm{y_n}}^{2^2}\right) + \sin\left(\frac{\omega}{{x_n}^2}\right)\right), \\ {y_{n+1}}^2 = \sin\left(\pi\omega\left(1 - {x_n}^{2^2}\right) + \sin\left(\frac{\omega}{{y_n}^2}\right)\right). \end{cases} \tag{5}$$

According to the above Algorithm 1, when $\mathbb{Z} = 2$, the constructed three-dimensional chaotic system ($3D - \mathrm{Sin}^3$) is shown in Eq. 6:

$$\begin{cases} {x_{n+1}}^3 = \sin\left(\pi\omega\left(1 - {\mathrm{y_n}}^{2^3}\right) + \sin\left(\frac{\omega}{{x_n}^3}\right)\right), \\ {y_{n+1}}^3 = \sin\left(\pi\omega\left(1 - {z_n}^{2^3}\right) + \sin\left(\frac{\omega}{{y_n}^3}\right)\right), \\ {z_{n+1}}^3 = \sin\left(\pi\omega\left(1 - {x_n}^{2^3}\right) + \sin\left(\frac{\omega}{{z_n}^3}\right)\right). \end{cases} \tag{6}$$

Next, we will conduct comprehensive performance tests on chaotic systems of different dimensions to verify the pseudo randomness and feasibility of the chaotic system constructed by the Sin paradigm.

Performance analysis

In this section, we verify the feasibility and effectiveness of generating different-dimensional chaotic systems using the proposed Sin paradigm through Run efficiency, Bifurcation diagrams, Lyapunov exponents, 0-1 tests, NIST tests, and Sample entropy.

Run efficiency

The running time and memory usage of chaotic systems for generating pseudo-random numbers are commonly used metrics to assess the performance of chaotic systems. Next, we will validate the feasibility of the $\mathbb{Z}D - \mathrm{Sin}^{\mathbb{Z}}$ by testing the following metrics: Run Time and Memory Usage.

Figure 1 presents the experimental results of time and memory consumption for different million iterations of $\mathbb{Z}D - \mathrm{Sin}^{\mathbb{Z}}$. It can be observed that the Run Time required for varying million iterations of $\mathbb{Z}D - \mathrm{Sin}^{\mathbb{Z}}$ is only at the microsecond level, indicating outstanding performance in generating chaotic sequences using the Sin paradigm. Memory Usage refers to the memory required for different million iterations of $\mathbb{Z}D - \mathrm{Sin}^{\mathbb{Z}}$, and even in the case of a 3D chaotic system with 4 million iterations generating 12 million random numbers, the memory usage is less than 1MB. This suggests that $\mathbb{Z}D - \mathrm{Sin}^{\mathbb{Z}}$ has extremely low memory usage. In conclusion, the Sin paradigm we propose is effective and feasible for constructing chaotic systems. (MS represents microseconds, KB means kilobytes, Mt indicates million iterations).

Bifurcation diagram

In the study of chaotic dynamic behavior, the chaotic behavior of chaotic systems is usually described by describing the bifurcation diagram or output distribution of chaotic sequences. Figure 2 shows the bifurcation diagrams (Jafari et al. 2021) of chaotic systems with different dimensions. As the parameters change, the output results of the chaotic map should be distributed as evenly as possible to ensure the randomness of the chaotic system.

As shown in Fig. 2(a), (b), (c), the small coverage range and uneven distribution of bifurcation graphs may cause instability in the performance of chaotic systems, which makes it difficult to predict and control the behavior of chaotic systems. On the contrary, as shown in Fig. 2(d), (e), (f), (g), (h), (i) the chaotic system constructed by the Sin paradigm exhibits stable pseudo-random characteristics and a more uniform distribution.

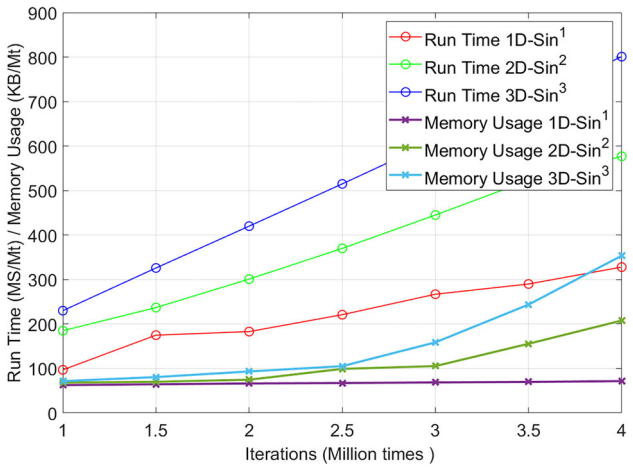

Fig. 1 Comparison of run time and memory usage of $\mathbb{Z}D - \mathrm{Sin}^{\mathbb{Z}}$

Lyapunov exponent analysis

The Lyapunov index often measures the degree of separation of a system over time due to fine-tuning of the initial value. If the chaotic system has pseudo-random behavior, it can be verified by the Lyapunov exponent (Sahoo and Roy 2022), and the Lyapunov exponent is particularly sensitive to the initial value transformation of the variables. The LE equation is as follows:

$$\gamma_{L(x)} = \lim_{i\to\infty} \frac{1}{i} \sum_{i=0}^{i-1} \ln \left| L'(x_i) \right| \tag{7}$$

A one-dimensional chaotic system with a positive Lyapunov exponent (LE) indicates that it is nonlinear, while having two or more positive Lyapunov exponents indicates that the chaotic system is hyperchaotic. Compared with Fig. 3 (a), (b), (c). Figure 3(d), (e), (f) has a more stable Lyapunov exponent output, indicating that our chaotic system has a more stable chaotic state compared to the basic chaotic system. From the Lyapunov exponents of chaotic sequences with different dimensions in Fig. 3(d), (e), (f), it can be seen that the chaotic sequence constructed by our scalable Sin paradigm is stable and feasible, and can serve as a pseudo random number generator to provide stable chaotic sequences.

0-1 test

Another common algorithm used to validate time series of chaotic systems is the 0-1 test (Gottwald and Melbourne 2016). Unlike the Lyapunov exponent, this test doesn't involve a phase space reconstruction module and solely focuses on the degree of deviation of the output result from 1. The closer the nonlinearity is to 1, the better the chaotic behavior.

In the 0-1 test results in Fig. 4, we can observe that, relative to Fig. 4(a), (b), (c), the chaotic system constructed using Sin paradigm on different dimensions, as shown in Fig. 4(d), (e), (f), has a 0-1 test result that is closer to 1 and exhibits a more

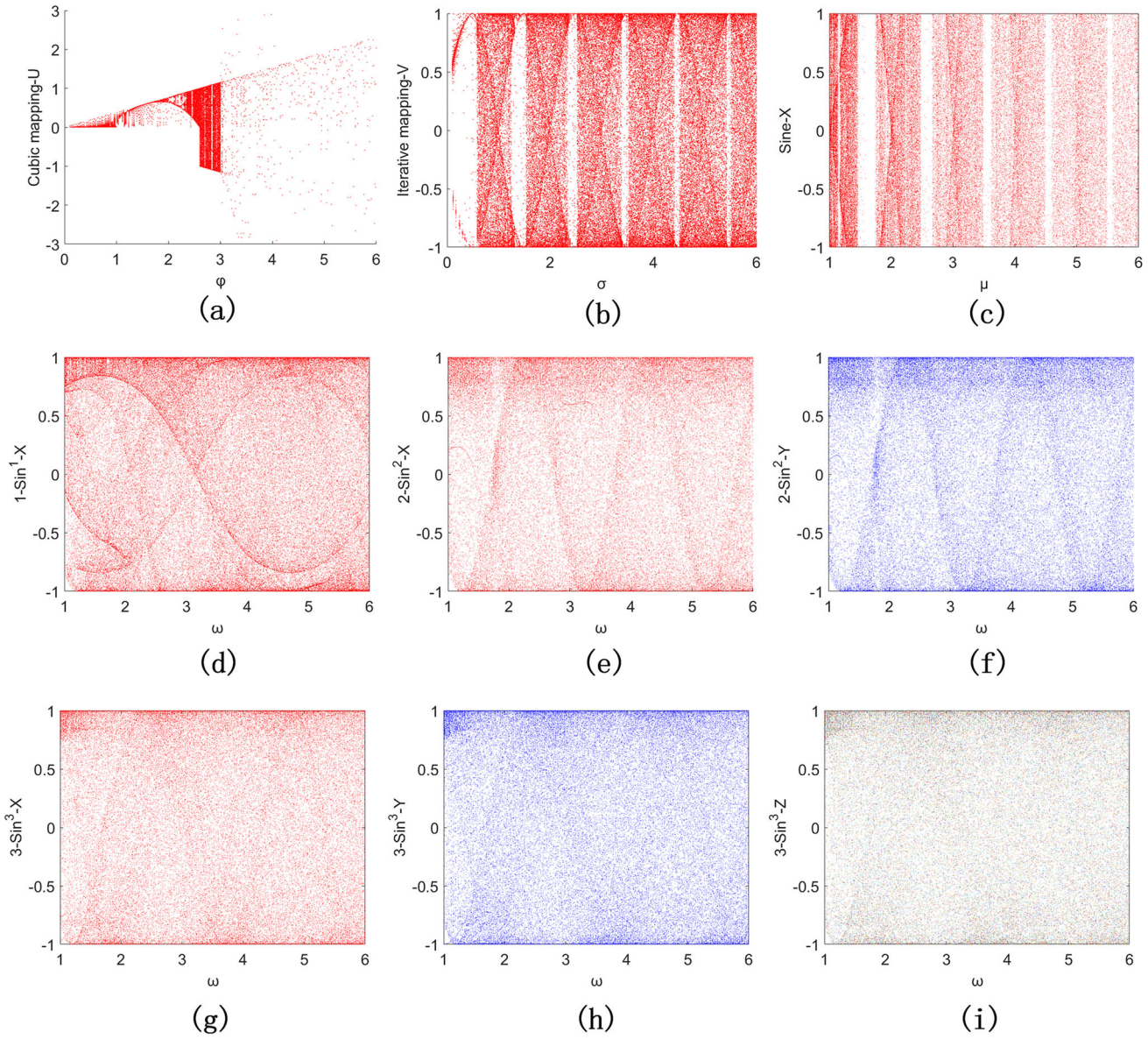

Fig. 2 Bifurcation diagram. (a) denotes the bifurcation diagram corresponding to Cubic mapping for parameter φ; (b) denotes the bifurcation diagram corresponding to Iterative mapping for parameter η; (c) denotes the bifurcation diagram corresponding to Sine mapping for parameter μ; (d) denotes the bifurcation diagram corresponding to $1D - \mathrm{Sin}^1$ for parameter ω; (e), (f) denotes the x-sequence and y-sequence bifurcation diagram corresponding to $2D - \mathrm{Sin}^2$ for parameter ω; (g), (h), (i) denotes the x-sequence , y-sequence and z-sequence bifurcation diagram corresponding to $3D - \mathrm{Sin}^3$ for parameter ω

stable output. This indicates that chaotic systems constructed using the Sin paradigm exhibit chaotic behavior and can be used for generating pseudo-random sequences.

NIST test

NIST SP 800-22 (Lv et al. 2022), the National Institute of Science and Technology, is a standard used to assess the quality of random number generators for cryptographic applications. It includes 15 types of tests, and NIST recommends using random number test sets with sizes greater than 10^6. Therefore, we should adhere to this rule when selecting random numbers. Only when the p-value is greater than 0.01 in the validation of sub-tests can we prove that the chaotic sequence generated by our chaotic system is random. Conversely, if the p-value is less than 0.01, it will not pass the NIST validation. From Table 1, We can easily observe that our proposed chaotic system $2D - \mathrm{Sin}^2$ has passed NIST testing, so this chaotic system has randomness and unpredictable.

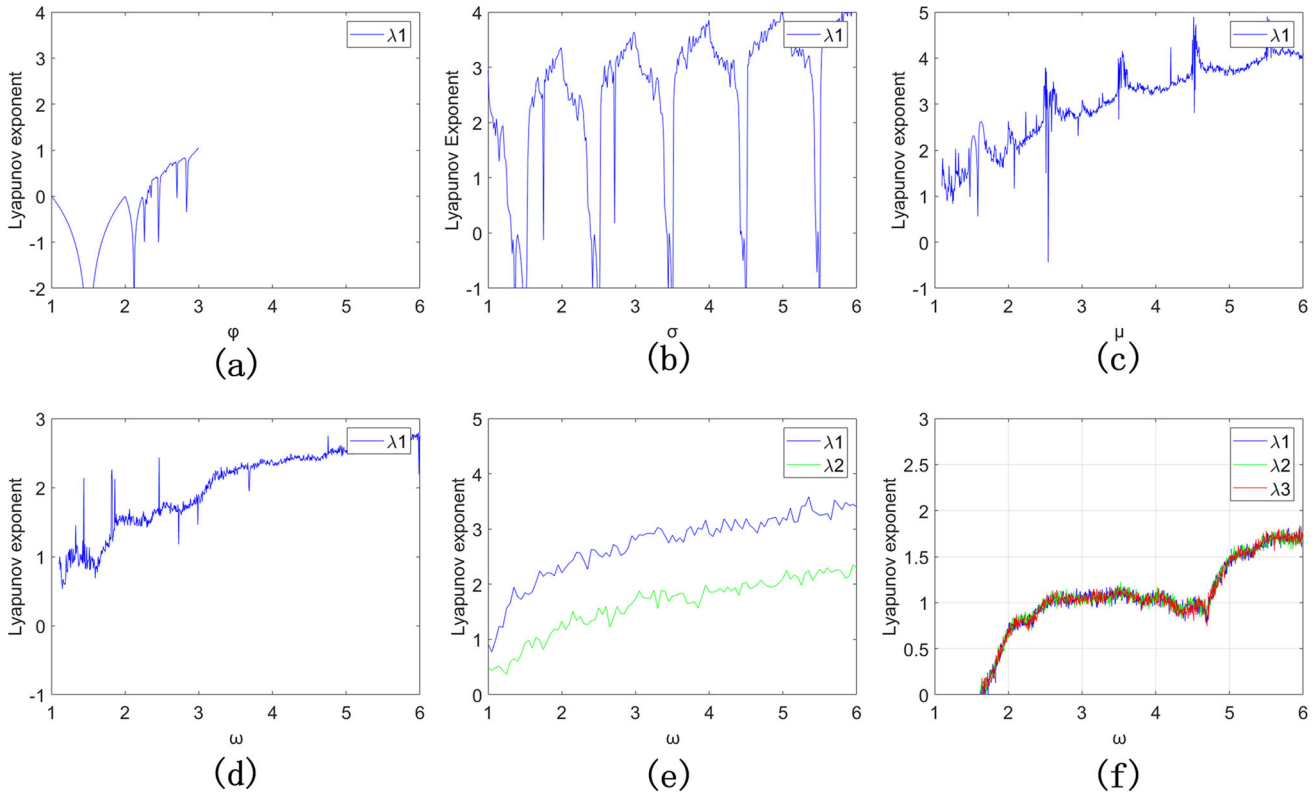

Fig. 3 Lyapunov exponent. (a) Cubic mapping Lyapunov exponent; (b) Iterative mapping Lyapunov exponent; (c) Sine mapping Lyapunov exponent; (d) $1D - \mathrm{Sin}^{1}$ Lyapunov exponent; (e) $2D - \mathrm{Sin}^{2}$ Lyapunov exponent; (f) $3D - \mathrm{Sin}^{3}$ Lyapunov exponent

Sample entropy

The pseudo-random characteristics of chaotic systems are one of the manifestations of nonlinear behavior. In the field of image encryption, chaotic systems play a key role in generating pseudo-random sequences for performing scrambling and diffusion operations on images. Therefore, the security of encrypted images is closely related to the complexity of pseudo-random sequences. The higher the complexity of the pseudo-random sequence, the closer the chaotic sequence is to a truly random sequence, leading to higher security in the corresponding application systems. Therefore, in this section, sample entropy (Richman et al. 2004) (SE) is used to evaluate the complexity of different dimensional chaotic systems generated by the Sin paradigm.

Figure 5 shows the sample entropy of chaotic sequences generated by different dimensional chaotic systems. The chaotic sequence generated by the chaotic system constructed in this article exhibits chaotic behavior, and each chaotic sequence exhibits excellent chaotic behavior throughout its lifecycle. By observing the distribution of sample entropy, it can also be proven that the chaotic sequence generated by our proposed Sin paradigm constructed chaotic system has pseudo randomness, complexity, and unpredictability, applying them to construct key sequences is also more suitable.

The performance of chaotic systems was comprehensively tested using the above methods, verifying the unpredictability, feasibility, and stability of constructing chaotic systems using the Sin paradigm. Therefore, the chaotic system $\mathbb{Z}D - \mathrm{Sin}^{\mathbb{Z}}$ constructed by the Sin paradigm is applicable for pseudo random generators which is capable to can provide different dimensions of chaotic systems for encryption schemes.

DNA transversion(DNA-TRV)

In biology, DNA is encoded according to the Watson-Crick base-pairing rule, which includes four different nucleic acids (Ravichandran et al. 2021), namely A (adenine), T (thymine), C (cytosine), and G (guanine). According to the base pairing rule, which allows A to be paired with T and C to be paired with G,DNA encoding (Jasra and Moon 2022) preserves the biological information carried by the organism itself through different arrangements and combinations of nucleic acid bases. The DNA coding rules are shown in

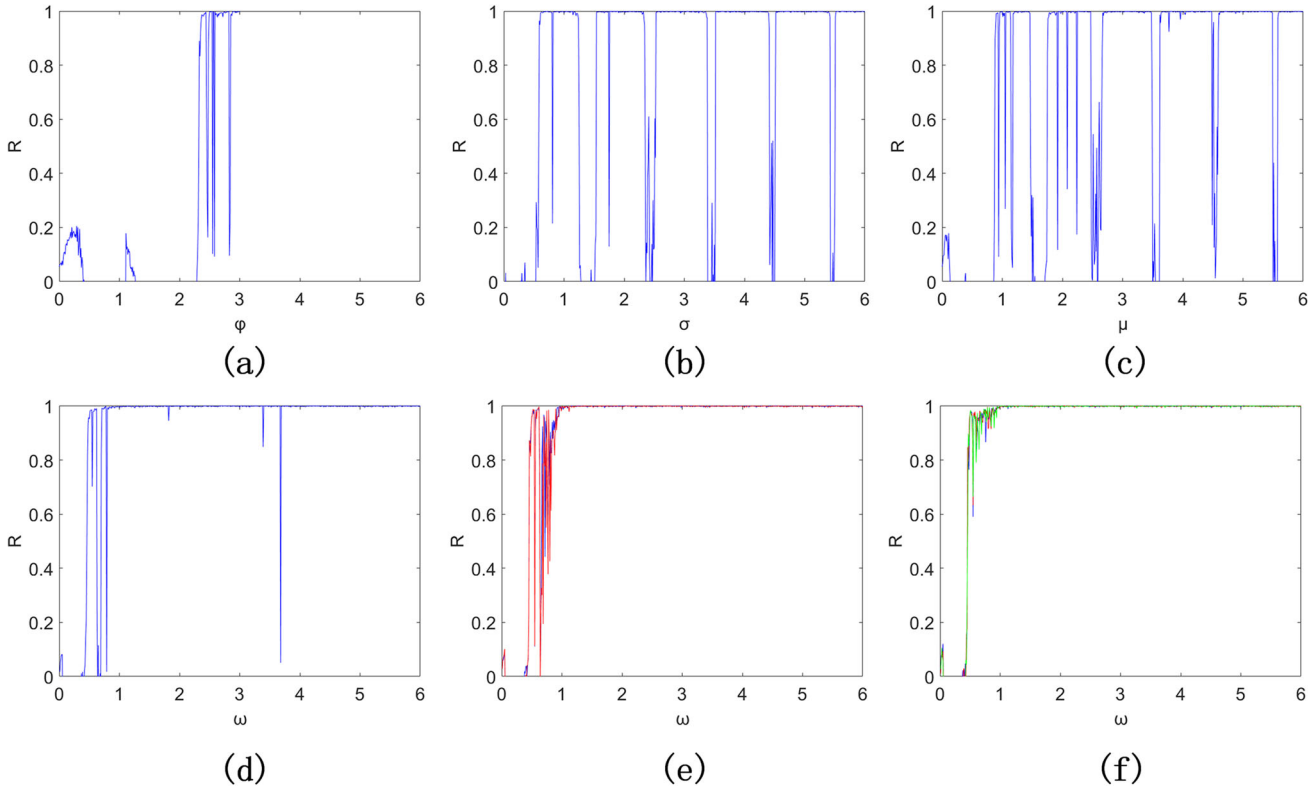

Fig. 4 0-1 test. (a) 0-1 test result graph of Cubic mapping; (b) 0-1 test result graph of Iterative mapping; (c) 0-1 test result graph of Sine mapping; (d) 0-1 test result graph of $1D-\mathrm{Sin}^1$; (e) 0-1 test result graph of $2D-\mathrm{Sin}^2$; (f) 0-1 test result graph of $3D-\mathrm{Sin}^3$

Table 2. Similarly, in the process of image encryption, the information of the original image is changed in the process of image encoding, addition, subtraction, Xor and decoding, making it impossible for attackers to obtain any valuable information from the modified image, thereby avoiding the leakage of the original image information.

DNA base transversion in molecular biology refers to the mutational phenomenon of interconversion between purines and pyrimidines on the DNA strand (Zheng et al. 2021). Base transversion can be spontaneous during DNA replication or repair, or can be induced by radiation or alkylating agents (Ray 2022). Figure 6 illustrates the normal state of the conversion between purines and pyrimidines, as well as the process of the transversion between purines and pyrimidines when DNA undergoes a reversal. Due to the presence of DNA transversion, more complex combinations between primitive purines and pyrimidines have emerged. If applied to image encryption, it not only breaks the fixed combination of primitive DNA encoding, but also expands the range of DNA encoding. It can be visually observed from the Fig. 7 that four different DNA transversion results are generated from one pixel point. This operation enhances the security of the data, because it not only breaks the original DNA coding method, but also expands the dynamic selection range of the DNA matrix, thus making the data more difficult to steal or tamper with.

The DNA transversion process is described in detail below. Based on the 4 DNA nucleic acid bases, the cor-

Table 1 The NIST test results of the improved $2D-\mathrm{Sin}^2$ chaotic system generated random sequence

Test lists	p-value	Result
Frequency tests	0.2331	√
Block frequency test	0.2636	√
Cumulative sums test	0.0437	√
Longest run test	0.2992	√
Rank test	0.8043	√
FFT test	0.0351	√
Non overlapping template	0.6024	√
Universal statistical	0.1223	√
Approximate entropy	0.2133	√
Random excursions	0.0821	√
Random excursions variant	0.1782	√
Serial test	0.0112	√
Linear complexity	0.6024	√
Runs test	0.5361	√
Overlapping template matching	0.2374	√

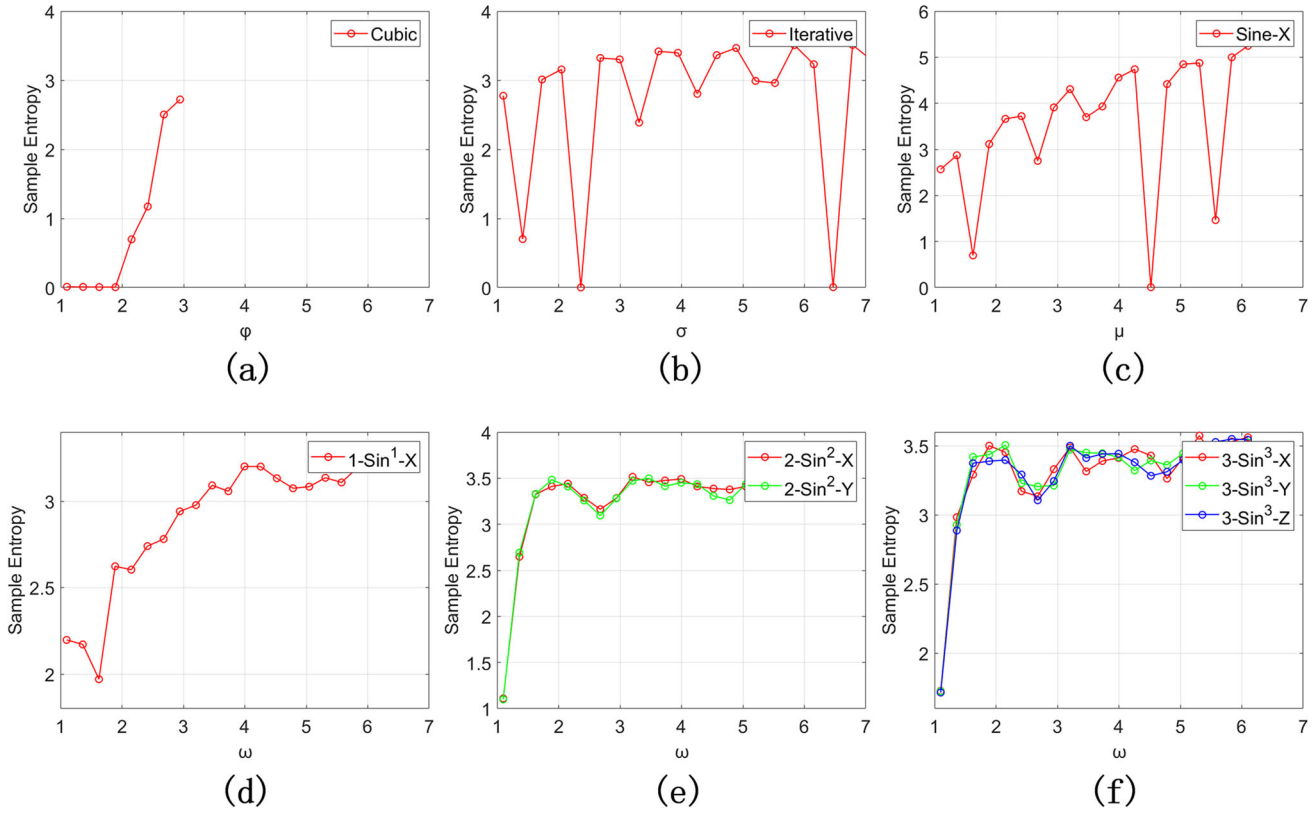

Fig. 5 Sample entropy. (a) presents the sample entropy of Cubic mapping; (b) presents the sample entropy of Iterative mapping; (c) presents the sample entropy of Sine mapping; (d) presents the sample entropy of $1D - \mathrm{Sin}^1$; (e) presents the sample entropy of $2D - \mathrm{Sin}^2$; (f) presents the sample entropy of $3D - \mathrm{Sin}^3$

responding 8 DNA-TRV rules are summarized, Table 3 summarizes the complete 8 DNA-TRV rules, each base A can be transversion to a T or G base, while T or G base can also be reversed to A. The process of implementing the DNA transversion rules is as follows: a pixel point is expressed in 8-bit binary, and the 8-bit binary is converted into 4-bit DNA code, and then the 4-bit DNA code is reversed and turned into 4 groups of DNA transversion codes, for example: a pixel point of 198 value, expressed in DNA coding Table 2 rule 1, its binary is 11000110, and the DNA code is TAGC, After the DNA coding of TAGC is processed by DNA transversion rule Table 3 , four sets of transversion combinations ATGC , ATAT, GCTA and GCGC are output. The DNA transversion process diagram is shown in Fig. 7, we can find that the DNA transversion rule changed the original DNA code, while generating a more complex DNA sequence. Since we can randomly select the DNA coding and decoding methods and DNA-TRV rules, the dynamic selection of the three rules can enhance the encryption effect to obtain better encryption performance.

The elliptic curve "Ring" hiding and transmission strategy

In the design scheme of encrypting remote sensing images, ensuring the secure transmission of keys and the degree of correlation between key stream elements and plaintext directly impact the encryption system's ability to withstand risks. Therefore, by constructing a plain- text-related strategy, the encryption system obtains a dynamic key pool while implementing the encryption system's one-time pad (OTP)

Table 2 DNA coding rules

	Rule 1	Rule 2	Rule 3	Rule 4	Rule 5	Rule 6	Rule 7	Rule 8
A	00	00	11	11	01	10	01	10
T	11	11	00	00	10	01	10	01
C	10	01	10	01	00	00	11	11
G	01	10	01	10	11	11	00	00

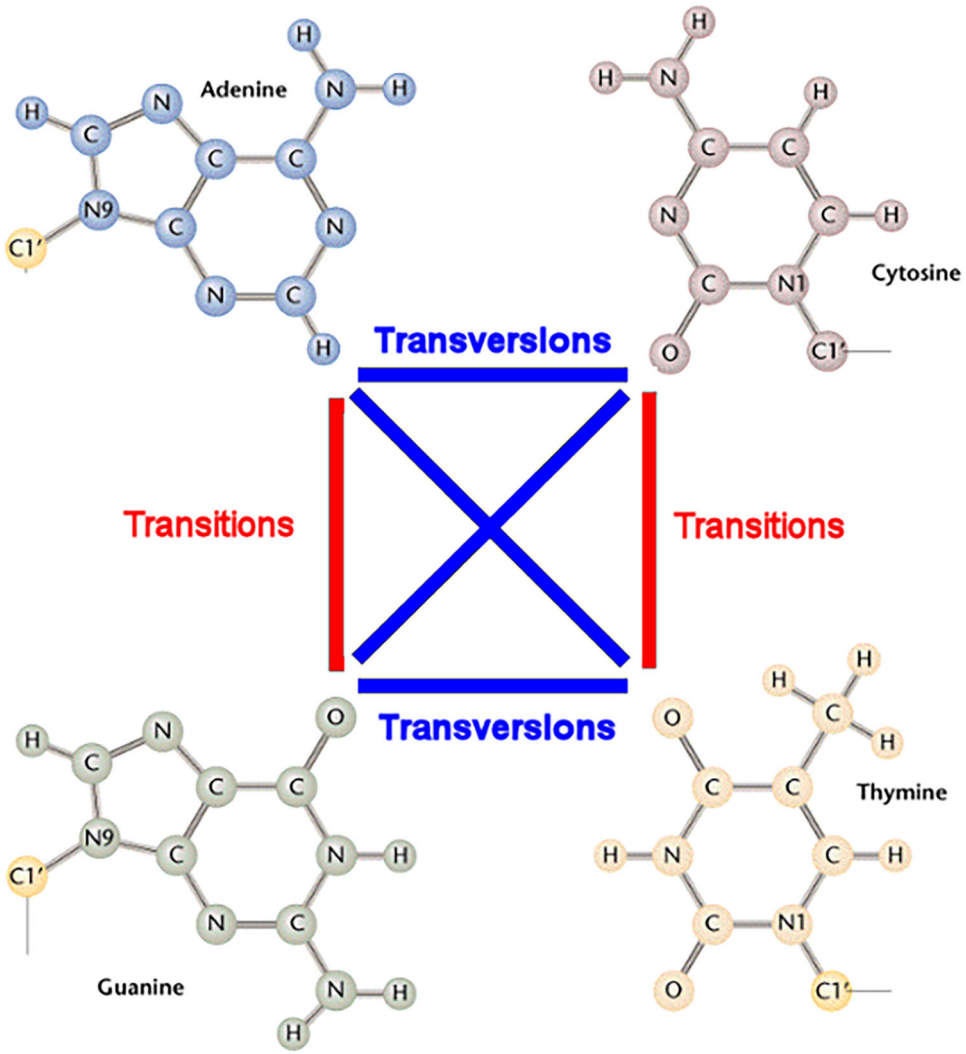

Fig. 6 Schematic diagram of normal DNA transitions and DNA transversions

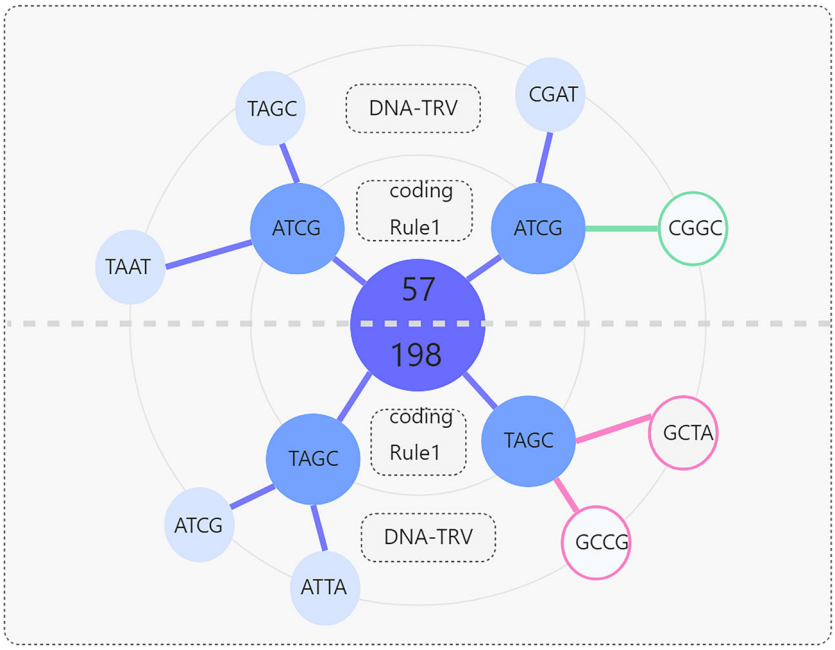

Fig. 7 Demonstration diagram of DNA-TRV

Table 3 DNA-TRV rules

	Rule 1	Rule 2	Rule 3	Rule 4	Rule 5	Rule 6	Rule 7	Rule 8
Primitive bases	AT	AT	GC	GC	TA	TA	CG	CG
Bases after transversion	CG	TA	CG	TA	AT	GC	AT	GC

mechanism, thereby enhancing the system's resistance to attacks and robustness. To address the issue of secure key transmission, Liu et al. (2021) employed a bit-level key hiding transmission strategy to embed the plaintext-related key into the ciphertext information. This strategy conceals the encryption key within the ciphertext image and transmits it to the intended receiver. During the decryption process, the receiver first extracts the plaintext-related key from the ciphertext and then uses it to decrypt the ciphertext. However, in the aforementioned approach, despite the fact that the key can be hidden in the ciphertext image and occupies only 0.05% of the pixel space, there remains a risk of key clipping attacks.

Elliptic curves are known for their unique mathematical properties, especially their unconventional group structures. In this structure, the sum of any two points on the curve is defined as the symmetric point about the X-axis of the third intersection of the line that passes through these two points and extends with the curve. This definition makes elliptic curves widely used in cryptography, especially in elliptic curve cryptography (ECC), where their advantages are significant. ECC is known for its efficient key generation algorithm and relatively small key size, which can provide superior performance while maintaining a high level of security. This makes it an indispensable part of modern cryptography, with applications covering multiple fields from encrypted communication to digital signatures. To further refine the key hiding strategy, We have proposed a new key hiding and transmission strategy called the elliptic curve (Li et al. 2023) "Ring" key hiding strategy, as shown in Fig. 8. For the initial value of $2D-\mathrm{Sin}^2$, a total of 96 binary bits are required to represent two sets of keys (16 * 6 bits each). By gradually embedding these 96 binary bits into the least significant bits of the ciphertext image, We constructed an elliptic curve "ring" key hiding and transmission strategy. This method enhances the robustness of the key hiding and transmission strategy of the entire encryption scheme. After various attack tests, the encryption scheme combined with the elliptic curve ring key hiding strategy has not only passed attack tests such as shear attacks and noise attacks, but also ensured the security of the initial key required for decryption. First, we transmit the initial value Msg of the $1D-\mathrm{Sin}^1$ chaotic system via an elliptic curve. The random sequence generated from this initial value is used to determine the location information for embedding the keys. Then, for the 96 binary bits of the key, they are sequentially embedded in the least significant bits of the ciphertext image according to the random numbers generated by the $1D-\mathrm{Sin}^1$ chaotic system. The embedding method is as shown in Fig. 8, This embedding part is in the form of a circular ring, comprising the outermost layer of the ciphertext image, with the ciphertext image's dimensions being 98x98 on the outer layer. Even if certain portions of the ciphertext are subject to truncation attacks, the recipient of the ciphertext image can still successfully extract the key and decrypt the message.

Step 1: We extract the plaintext-related keys $p_x^{(i)}$, $p_y^{(i)}$ and $p_\omega^{(i)}$ and name them as the set P i.e. $\mathrm{P}=\left\{p_x^{(i)},\quad p_y^{(i)},\quad p_\omega^{(i)}\right\}$,

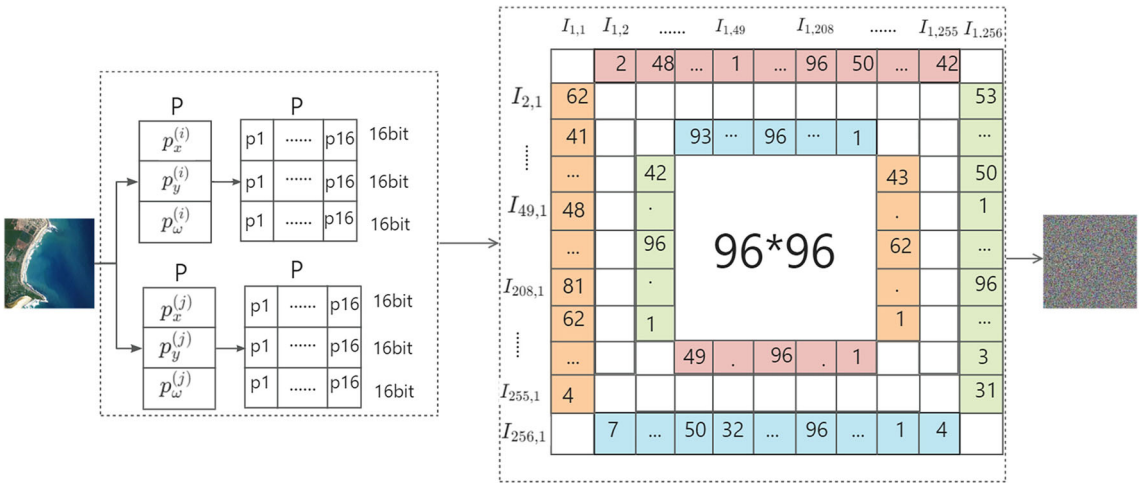

Fig. 8 The elliptic curve "Ring" hiding and transmission strategy

Since $p_x^{(i)}$, $p_y^{(i)}$ and $p_\omega^{(i)}$ are all floating-point numbers,we use an eight-bit binary representation for the integer part and the fractional part, which is equivalent to only one sixteen-bit binary for each key representation for each key. Since we need two sets of keys,we need a total of $P*2$ binary numbers, $P = 16*3$.

Step 2: The initial value of the $1D-\mathrm{Sin}^1$ chaotic system is denoted as Msg. An elliptic curve is defined as $E_o(a, b)$, and a point O on the elliptic curve is chosen as the base point. A large number K is selected as the private key, and the public key U is generated as $U = KO$. The elliptic curve $E_o(a, b)$, along with the points U and O, are provided to the user. Upon receiving the information, the user encodes the plaintext Msg into a point M on $E_o(a, b)$ and generates a random integer r.

$$\begin{cases} \text{Public Key Encryption: C} = \{\text{r}O, \text{M} + \text{rU}\} \\ \text{Private Key Decryption: M} + \text{rU} - \text{K(rO)} \\ = \text{M} + \text{r(KO)} - \text{K(rO)} \\ = \text{M} \end{cases} \tag{8}$$

Decoding point M yields the plaintext Msg.

Step 3: Based on the obtained plaintext Msg and the iterative $1D - \mathrm{Sin}^1$ chaotic system, the key P is inserted into the ciphertext image according to the chaotic sequence generated by the chaotic system. This allows the initial value of the encryption scheme's key to be concealed within the ciphertext image, as illustrated in Fig. 8.

Secure compression encoding of remote sensing images

Remote sensing images are distinct from digital images due to their large data volume and multiple spectral bands. Considering the uniqueness of remote sensing images, we propose a secure compression and encoding scheme based on DNA-TRV (DNA Transversion) and $2D - \mathrm{Sin}^2$, which we apply to enhance the security of remote sensing images. We employ compression sensing to reduce the data volume of remote sensing images and enhance their security through DNA-TRV and the $2D-Sin^2$ chaotic system. In this section, we will provide a detailed explanation of the secure compression and encoding process for remote sensing images. Figure 9 illustrates the workflow of the remote sensing image secure compression encoding process.

Key generation

An encryption scheme independent of both the ciphertext image and the encryption algorithm is more flexible but challenging to resist plaintext-related statistical attacks (Huang and Zhou 2022). Therefore, we extract the relevant information from the plaintext image's various bands as input to the $2D - \mathrm{Sin}^2$ chaotic system, generating plaintext-related keys to counteract plaintext-related attacks.

Step 1: Choose a color remote sensing image "RI" with dimensions M*N*k as the original plaintext image. (Here, M represents the width of the original image, N represents the height of the original image, and k represents the number of selected remote sensing image bands.)

Step 2: Split "RI" into different bands.

$$b_k^{(\iota)} = \text{shape}(RI(1:M), RI(1:N), k) \tag{9}$$

shape() function represents splitting the remote sensing image "RI" into k bands, where $b_k^{(\iota)}$ represents the ι-th band among the k bands.

Step 3: According to Eq. 10, randomly select the values of two bands from the remote sensing image "RI" to generate the initial values of the random number generator $(p_x^{(i)}, p_y^{(i)}, p_\omega^{(i)})$. Since the chosen initial values for the chaotic system are correlated with the plaintext, the encryption scheme is resistant to plaintext-related attacks.

$$\begin{cases} p_x^{(i)} = \mathrm{mod}\left(\frac{\mathrm{sum}(b_{\mathrm{mod}\,(i)} + b_{\mathrm{mod}\,(i+1)})}{M*N*2}, 1\right) \\ p_y^{(i)} = \mathrm{mod}\left(\frac{\mathrm{sum}(b_{\mathrm{mod}\,(i)} + b_{\mathrm{mod}\,(i+2)})}{M*N*2}, 1\right) \\ p_\omega^{(i)} = \mathrm{mod}\left(\frac{\mathrm{sum}(b_{\mathrm{mod}\,(i)} + b_{\mathrm{mod}\,(i+3)})}{M*N*2}, 1\right) + 1 \end{cases} \quad i \in N \tag{10}$$

The values obtained from Eq. 10, namely $p_x^{(i)}$, $p_y^{(i)}$ and $p_\omega^{(i)}$, serve as the initial values and control parameter (x_0, y_0, ω_0) for the iterations of the chaotic system. Here, mod() function represents the modulo operation, and "sum()" represents the summation function.

Step 4: Select two different values for i and j, to construct two sets of different initial key values. Name these sets as "userkey1" and "userkey2.", where $i \neq j, \quad i, j \in N$.

$$\begin{cases} \text{usekey 1} = \text{set}\left(p_x^{(i)}, p_y^{(i)}, p_\omega^{(i)}\right) \\ \text{usekey 2} = \text{set}\left(p_x^{(j)}, p_y^{(j)}, p_\omega^{(j)}\right) \end{cases} \tag{11}$$

set() function represents the collection of initial key values.

Generating chaotic sequences

Based on the performance analysis of the $2D - \mathrm{Sin}^2$ chaotic system in Section "Definition of Sin paradigm", it is known that it exhibits excellent randomness. Applying the chaotic system to an encryption scheme can enhance the stability and security of the encryption scheme.

Step 1: Use "userkey1" and "userkey2" as the initial values and control parameters (x_0, y_0, ω_0) for the $2D-\mathrm{Sin}^2$ chaotic

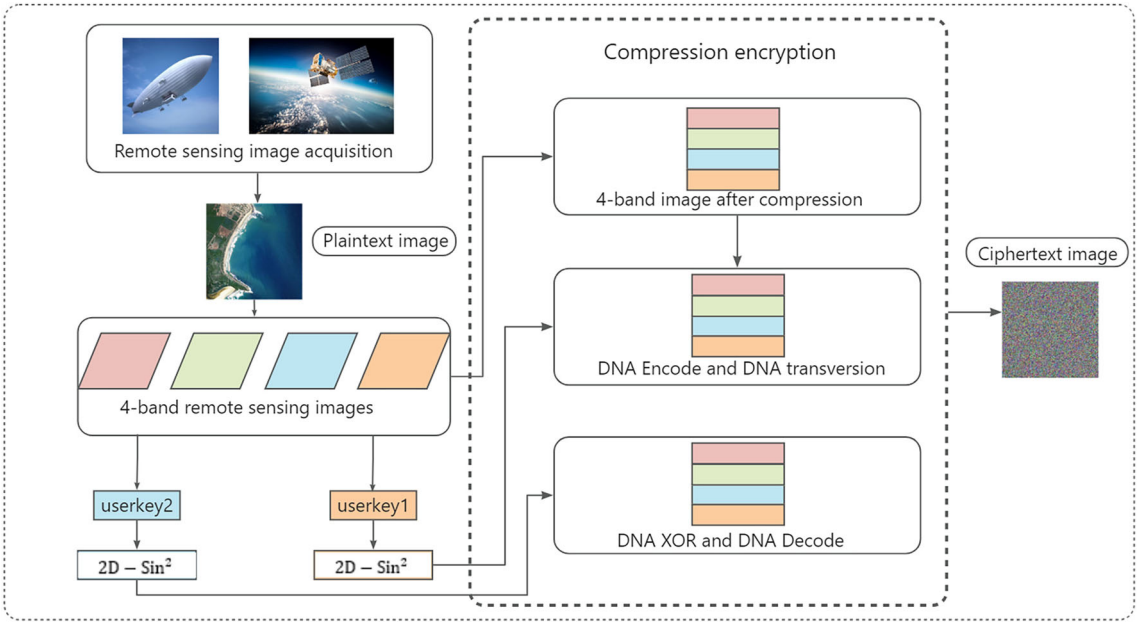

Fig. 9 Block diagram of remote sensing image secure compression coding

system. Input "userkey1" and "userkey2" into the chaotic system, respectively, and let the $2D - Sin^2$ chaotic system iterate M*N+S times for each set of parameters. To eliminate the initial disturbance of the chaotic system, discard the first S iterations of the chaotic sequence, resulting in two sets of two-dimensional chaotic sequences with a length of M*N, denoted as (X, Y) and (Z, W). These two sets of chaotic sequences will serve as the key pools for operations such as measurement matrix creation, DNA encoding, DNA-TRV, XOR operations, and DNA decoding.

Step 2: Sort the chaotic sequences X in ascending order to obtain index matrix X_{index}, as shown in (12):

$$X_{\text{index}} = \text{sort}(X) \tag{12}$$

sort() function represents a sorting operation in ascending order.

The process of secure compression coding

In this subsection, we achieve secure compression coding of remote sensing images through operations like Discrete Cosine Transformation and DNA-TRV.

Step 1: As described in Step 2 of Section "Key generation", split the remote sensing image "RI" into k bands. Since the red, green, blue, and infrared bands in remote sensing images contain sufficient information, we choose these four bands, i.e., k=4, as the focus of our research. The four bands are denoted as $b_k^{(\iota)}$, where ($\iota \in \{1, 2, 3, 4\}, k = 4$).

Step 2: Apply Discrete Cosine Transformation to $b_k^{(\iota)}$ to obtain $I_k^{(\iota)}$, thus transforming it in both domains, i.e., spatial and frequency domains.

$$I_k^{(\iota)} = \text{dct}\left(b_k^{(\iota)}\right), k = \{1, 2, 3, 4\} \tag{13}$$

In which, $b_k^{(\iota)}$ represents the ι-th band among the k bands; dct() denotes the Discrete Cosine Transformation; $I_k^{(\iota)}$ represents the transformation result of the ι-th band from the spatial domain to the frequency domain.

Step 3: Set up a threshold value T to the matrices obtained in Step 2, removing values whose absolute values are less than T. This results in a sparse matrix denoted as $I_{csk}^{(\iota)}$.

$$\begin{cases} c1 = \text{reshape}\left(I_k^{(\iota)}, [M, N]\right) \\ \text{thd} = \text{find}\left(abs(c1) < T\right) \\ c1_{thd} = 0 \\ I_{csk}^{(\iota)} = c1 - c1_{thd} \end{cases} \tag{14}$$

Algorithm 2 represents the pseudo-code for Eq. 14. T is a threshold value, and to preserve as much valid data as possible, we set the threshold value as $T \in (0.083, 0.087)$. reshape() function indicates that the data is reshaped to size M*N in the frequency domain, abs(c1) represents taking the absolute value of c1, find() function returns the indices that satisfy the condition, and in the context, it means returning the indices of all values whose absolute values are less than T. $c1_{thd}$ indicates setting the values whose absolute values

are less than T to 0, and $I_{csk}^{(\iota)}$ represents the final sparse matrix after threshold filtering.

Algorithm 2 The pseudocode representation of Eq. 14.

Input: $I_k^{(\iota)}$($I_k^{(\iota)}$ denotes the result of the transform from the spatial domain to the frequency domain.)

Output: $I_{csk}^{(\iota)}$(the sparse matrix)

1: Reshape the input data $I_k^{(\iota)}$ into a matrix c1 with dimensions $M * N$:
$c1 = \text{reshape}\left(I_k^{(\iota)}, [M, N]\right)$

2: Find indices of elements in c1 with absolute value less than T:
thd = find $(abs(c1) < T)$

3: Set the values in c1 at indices specified by thd to 0:
for index in thd:
$c1_{thd} = 0$
end

4: Calculate the final result $I_{csk}^{(\iota)}$ by subtracting $c1_{thd}$ from $c1$:
for i from 1 to M:
for j from 1 to N:
$I_{csk}^{(\iota)}$[i][j] = c1[i][i] − $c1_{thd}$
$I_{csk}^{(\iota)} = \text{reshape}\left(I_{csk}^{(\iota)}[\text{i}][\text{j}], [M, N]\right)$
end
end

Step 4: Take the first quarter of the X sequence, scramble it using the index sequence X_{index}, and then reconstruct the scrambled sequence into a measurement matrix of size M*N/4.

$$\begin{cases} \Phi_{sq} = X(1 : M * N * 1/4) \\ \Phi_{\text{scramble}} = \text{scramble}\left(X_{\text{index}}, \Phi_{\text{sq}}\right) \\ \Phi_{\text{matrix}} = \text{reshape}\left(\Phi_{\text{scramble}}, [\frac{M}{4}, N]\right) \end{cases} \tag{15}$$

Φ_{sq} represents the result of taking the first quarter of the X sequence, the scramble() function is used to scramble Φ_{sq} based on the index matrix, and the reshape() function is used to construct the scrambled matrix into a measurement matrix of size M*N/4.

Step 5: Perform compressive sensing operations on the sparse matrix $I_{csk}^{(\iota)}$ and the measurement matrix Φ_{matrix}, and then quantize to obtain a compressed matrix $CS^{(\iota)}$ of size M * N/4.

$$\begin{cases} S = \min \left\| Cs - \Phi_{\text{matrix}} \cdot I_{csk}^{(\iota)} \cdot S \right\|_2^2 + \lambda \|S\|_1 \\ CS^{(\iota)} = \Phi_{\text{matrix}} \cdot I_{csk}^{(\iota)} \cdot S \end{cases} \tag{16}$$

S represents the sparse coefficients, and LASSO (L1 norm minimization) is a widely used method to solve for sparse coefficients S by minimizing the objective function. In this context, $(\|\|_2)^2 2$ represents the square of the Euclidean distance, $\|\|_1$ represents the L1 norm, and λ is the regularization parameter controlling sparsity. By solving this optimization problem, one can obt ain the sparse representation coefficients S.

Step 6: Execute the operations from Step 2 to Step 5 sequentially for all four bands of images until all of them are compressed. Then, transform the compressed matrices of the four bands back to the spatial domain using inverse Discrete Cosine Transformation and combine them into a composite compressed matrix CE of size M * N.

$$CE^{(\iota)} = idct\left(CS^{(\iota)}\right) \tag{17}$$

The idct() function represents the inverse Discrete Cosine Transformation, and CE represents the composite compressed matrix $CE^{(\iota)}$ that combines all the individual compressed matrices into one.

Next, we will introduce the entire process of generating the ciphertext image by performing DNA encoding, DNA transversion, DNA XOR operations, and DNA decoding on the compressed image matrix, as shown in Fig. 10.

Step 7: To ensure the randomness in DNA encoding, use the chaotic sequence Y and the DNA encoding rules from Table 2 to perform DNA encoding on the composite compressed matrix CE, resulting in the DNA-encoded matrix Y_{DNA}.

$$Y_{DNA} = \text{DNAEncode}(\text{mod}(Y, 8) + 1, CE) \tag{18}$$

Where DNAEncode() function represents the DNA encoding operation.

Step 8: The introduction of DNA-TRV rules enhances the security of the encryption scheme. Here, perform DNA-TRV on the DNA encoded matrix Y_{DNA} based on the chaotic sequence Y and the DNA transversion rules from Table 3, resulting in the DNA-TRV matrix Y_{TRV}.

$$Y_{TRV} = \text{DNATrans}\left(\text{mod}(Y, 8) + 1, Y_{DNA}\right) \tag{19}$$

Where DNATrans() represents the DNA-TRV operation.

Step 9: Diffusion operations can enhance the encryption effectiveness of the scheme. Therefore, we use the chaotic sequence Z to construct the chaotic encoding matrix Z_{DNA} required for the diffusion operation.

$$Z_{DNA} = \text{DNAEncodeEncode}(\text{mod}(Z, 8) + 1) \tag{20}$$

Step 10: Perform XOR operations between the DNA transversion matrix Y_{TRV} and the chaotic encoding matrix Z_{DNA} according to Table 4 to obtain the final encrypted encoding matrix HyperDNA.

$$\text{HyperDNA} = Y_{TRV} \oplus Z_{DNA} \tag{21}$$

Step 11: Based on the chaotic sequence W, select the DNA decoding rules and transform the encoded DNA matrix into

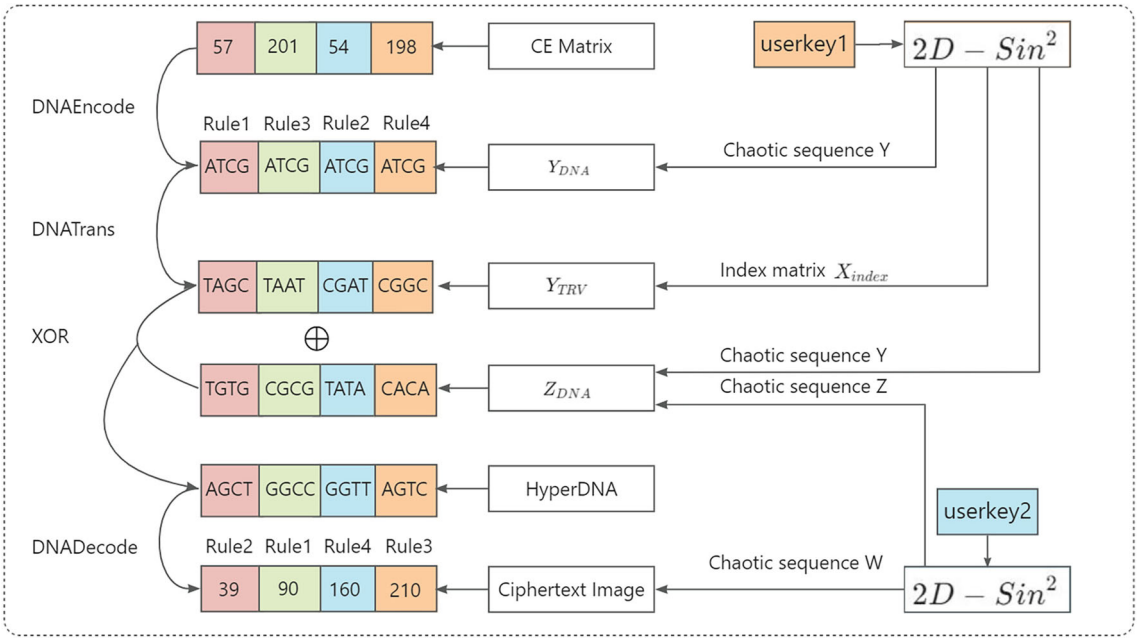

Fig. 10 Block diagram of secure compression coding based on DNA transversion

a numeric matrix, resulting in the final ciphertext image CI.

$$\mathrm{CI} = \mathrm{DNADecode}(\mathrm{mod}(W, 8) + 1,\ \mathrm{HyperDNA}) \tag{22}$$

Where DNADecode() function represents the DNA decoding operation.

The secure compression coding flowchart is shown in Fig. 11. Since the secure compression coding scheme uses symmetric encryption, the decryption of the ciphertext image is the inverse process of encryption, performing the reverse of the entire encryption step to reconstruct the original image. Therefore, it is not repeated here.

Experimental analysis

In this section, we simulated and evaluated the security performance of the algorithm, and the experimental simulation results showed that our proposed algorithm has a very perfect simulation effect. Source of test images: The remote sensing images in the experiment were obtained from the High Score Image Dataset (GID) released by Wuhan University in 2020, which was extracted from the Gaofen-2 (GF-2) satellite (Tong et al. 2020). Multi-band remote sensing image processing is based on a complete remote sensing image processing platform - Environmental Visualization Image (ENVI). The experimental equipment used a PC with Windows 10 , processor selected Intel(R) Core(TM) i5-7200U CPU @2.5GHz 2.70GHz, and data processing software used MATLAB R2021a for data simulation. The parameters of the chaotic system were selected from the explicit images obtained and labeled under the corresponding experimental results plots.

Table 4 DNA operations

⊕	A	G	C	T
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

Keyspace

A larger key space provides higher security and reduces the possibility of cracking the key. On the contrary, a smaller key space is vulnerable to attack methods such as brute force cracking, which reduces the security performance of the encryption scheme (Yan et al. 2021), therefore, a sufficiently large key well above 2^{100} $\left(10^{30} < 2^{100} < 10^{31}\right)$ indicates that the system is resistant to exhaustive attacks. The $2D - \mathrm{Sin}^2$ proposed in this paper has three initial values x_0, y_0, ω_0, and the pc precision we use can reach 10^{-15}, therefore, the key space of our proposed algorithm can reach $(10^{45})^3$, i.e., $10^{45} > 10^{31}$ is fully resistant to exhaustive attacks.

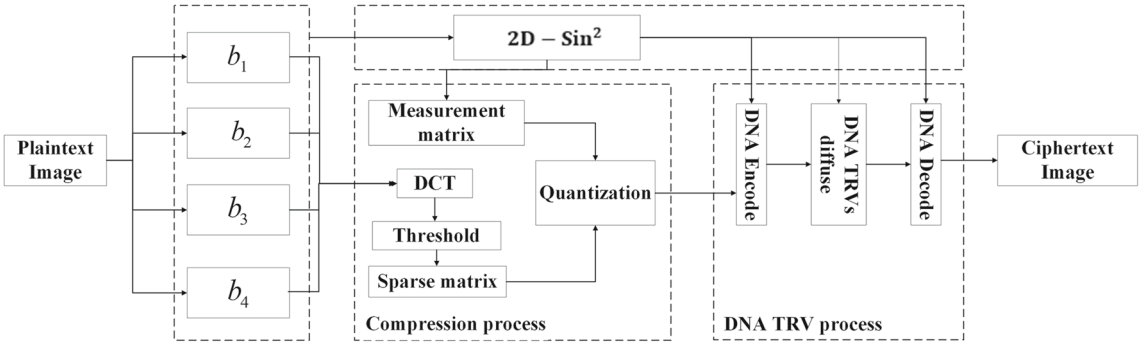

Fig. 11 Secure compression coding flow chart

Histogram analysis

Since histograms can clearly represent numerical relationships, they are applied to the frequency distribution of statistical image pixel values (Elkandoz and Alexan 2022), and it can visually reflect the basic pixel value distribution. Figure 12 shows the histogram of the plaintext image. The histogram distribution characteristics shown by remote sensing images are different due to different feature of the features, and after processing the remote sensing images by the proposed encryption solution, the distribution characteristics of remote sensing images tend to be the same, so it can resist the threat of attackers based on statistical characteristics. Figure 13 shows the histogram analysis of ciphertext image after secure compression coding.

Pixel correlation

Correlation measures the similarity or difference between adjacent image pixels vertically, horizontally and diagonally (Masood et al. 2022). In order to have a cryptographically secure image encryption scheme, the correlation

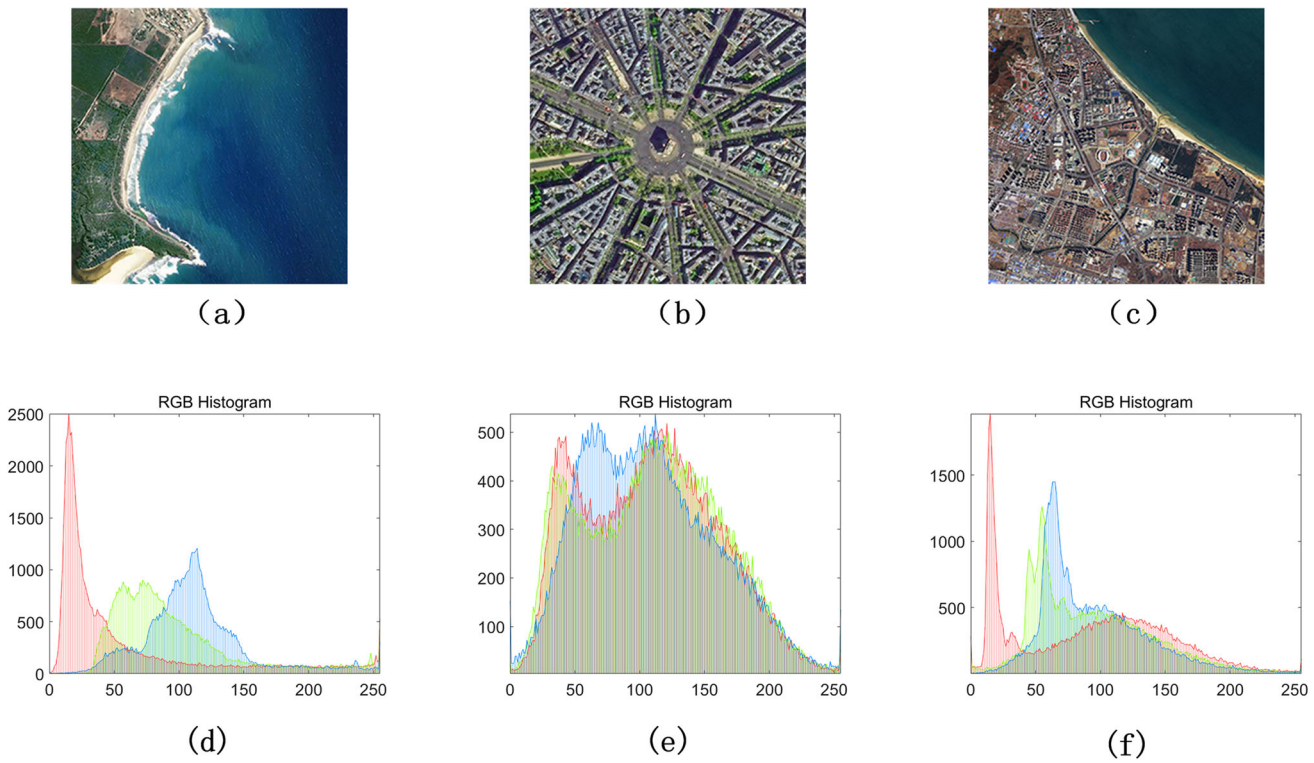

Fig. 12 Plaintext image histogram analysis. (a), (b), (c) represent different types of remote sensing images, (d), (e), (f) correspond to the RGB tricolor histograms of remote sensing images (a), (b), (c), respectively

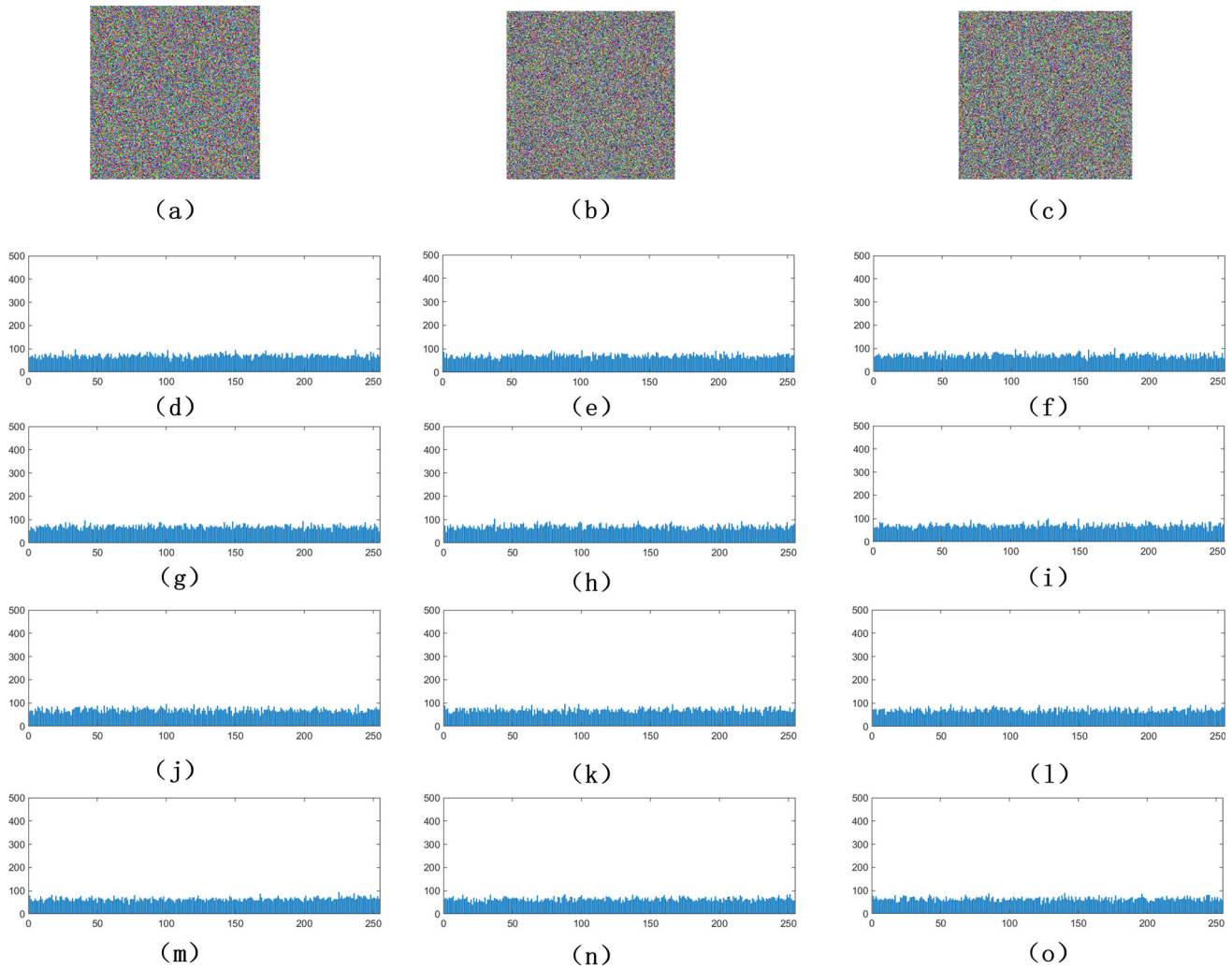

Fig. 13 Histogram analysis of ciphertext image after secure compression coding. (a),(b),(c) are the encrypted images corresponding to the plaintext images (a),(b),(c) in Fig. 12; (d),(g),(j),(m) correspond to the histograms of 4 parts after secure compression coding (CR=0.25) in Fig. 12(a); (e),(h),(k),(n) correspond to the histograms of 4 parts after secure compression coding (CR=0.25) in Fig. 12(b); (f), (i), (l), (o) correspond to the histogram of the 4 parts after secure compression coding (CR=0.25) in Fig. 12(c), respectively

between pixels should be eliminated and it is mathematically expressed as

$$r_{x,y} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{23}$$

where,

$$\mathrm{cov(x, y)} = \frac{1}{\mathrm{N}} \sum_{\mathrm{i}=1}^{\mathrm{N}} (\mathrm{x_i} - \mathrm{E(x)})\,(\mathrm{y_i} - \mathrm{E(y)}) \tag{24}$$

$$D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2 \tag{25}$$

$$\mathrm{E(x)} = \frac{1}{\mathrm{N}} \sum_{\mathrm{i}=1}^{\mathrm{N}} (\mathrm{x_i}) \tag{26}$$

In the above equation, $cov(x, y)$ denotes the covariance of adjacent pixels x, y, E denotes the expectation of x or y, D denotes the variance of x or y, and r represents the correlation of adjacent pixels. As shown in the figure, the horizontal, vertical, positive diagonal and negative diagonal correlation coefficients of adjacent pixel points are linear. This means that it is linearly correlated before encrypting the image. Figure 14 shows the pixel correlation of a plaintext image. In addition, the horizontal, vertical, diagonal and anti-diagonal correlation coefficient maps of the encrypted image

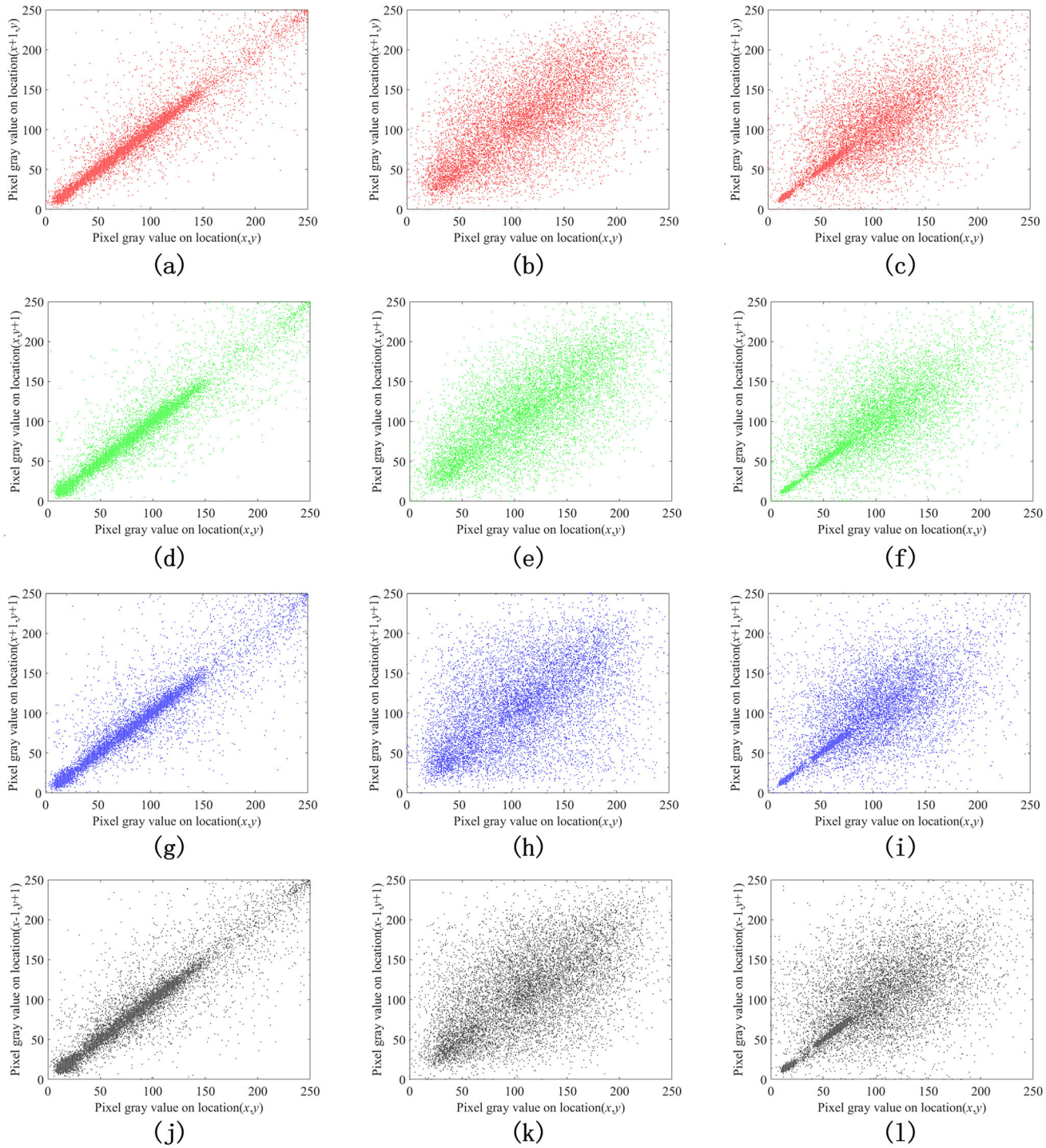

Fig. 14 Correlation of adjacent pixels of the original remote sensing image in horizontal, vertical, positive diagonal and negative diagonal. (a),(d),(g),(j) correspond to the correlations on the four directions of remote sensing image in Fig. 12(a); (b),(e),(h),(k) correspond to the correlations on the four directions of remote sensing image in Fig. 12(b); (c),(f),(i),(l) correspond to the correlations on the four directions of remote sensing image in Fig. 12(c)

are uniform with a scatter-like distribution. Figure 15 shows the pixel correlation of the ciphertext image. In this paper, a set of 10,000 adjacent pixels is selected along the horizontal, vertical, diagonal and anti-diagonal lines. The closely correlation of adjacent pixels was displayed obviously in diagonal.

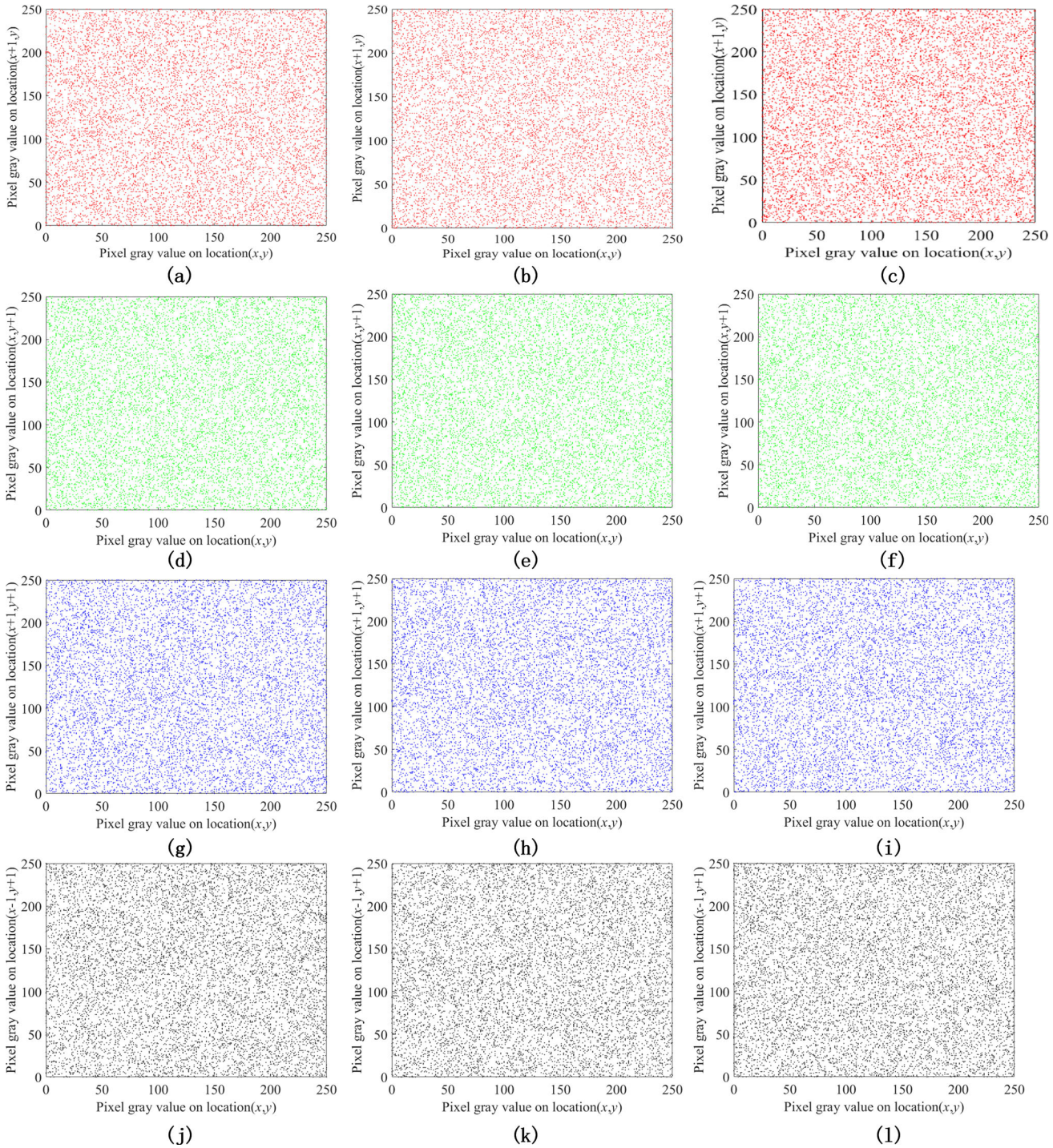

Fig. 15 Correlations of adjacent pixels in horizontal, vertical, positive diagonal and negative diagonal of ciphertext remote sensing images. (a),(d),(g),(j) correspond to the correlation of the four directions of the encrypted remote sensing image in Fig. 13(a); (b),(e),(h),(k) correspond to the correlation of the four directions of the encrypted remote sensing image in Fig. 13(b); (c),(f),(i),(l) correspond to the correlation of the four directions of the encrypted remote sensing image in Fig. 13(c)

Hypothetically, the pixel correlation need to be disordered if researchers aim to safeguard the security of remote sensing image data. Therefore, the randomness of adjacent pixels would be more effective after the encrypted image pixels be dispersed.

Information entropy

Uncertainty and randomness in the data contained in an image are related to the information entropy[14]. Higher entropy means less information is obtained from the image,

which is relatively more secure. The security of the encryption scheme gradually increases as the entropy value converges infinitely to 8, with the following equation:

$$H = -\sum_{0}^{255} P\left(L_i\right) \log_2 P\left(L_i\right) \tag{27}$$

In the above equation, $P(L_i)$ denotes the number of occurrences of pixel value L_i in each band, and if the image information entropy is 8, it means that the image is a completely random ciphertext image. In other words, the more infinitely close to 8 the information entropy is, the better the encryption algorithm proves to be and the more secure the encrypted image is. The information entropy of the original plain ciphertext images in different bands is given in Table 5. The results show that the encryption scheme is secure and feasible. By analyzing the information entropy of several different spectral bands before and after encryption and decryption, and comparing with similar research subjects, we can observe that the encryption algorithm we proposed is relatively effective, and the resulting ciphertext images exhibit a higher degree of randomness. Since only the information entropy of ciphertext images is given in reference (Zhang et al. 2020; Al-Khasawneh et al. 2022), only the information entropy of ciphertext images is shown in Table 5.

Sensitivity analysis

Since the statistical properties of plaintexts can be the target of differential attacks by attackers, the small differences among different images encrypted by the same encryption system may become vulnerabilities in the encryption system, so the sensitivity analysis of plaintexts is indispensable. We usually use the pixel change rate (NPCR) and the uniform change intensity (UACI) to measure whether the plaintext sensitivity can resist the differential attack (Wang et al. 2015). We encrypted three remote sensing images using the encryption scheme we proposed for testing purposes. By testing the NPCR and UACI values for different spectral bands, we found that the average NPCR value for different bands exceeded 99.60%, and the UACI value reached 33.30%. Comparing with references (Wang et al. 2015) and Lai et al. (2023), it can be observed from the data that our proposed encryption sch- eme has a significant advantage. The NPCR and UACI of different encryption schemes is shown in Table 6. The equations for the two methods mentioned above are as follows:

$$\mathrm{NPCR} = \frac{\sum_{\mathrm{m,n}} \mathrm{D(m,\,n)}}{\mathrm{M} \times \mathrm{N}} \tag{28}$$

$$\mathrm{UACR} = \frac{\sum_{\mathrm{s,t}} |\mathrm{C_1(\,m,\,n)} - \mathrm{C_2(m,\,n)}|}{\mathrm{M} \times \mathrm{N} \times \mathrm{L}} 100\% \tag{29}$$

where, $D(m,n) = \begin{cases} 0, & C_1(m,n) = C_2(m,n) \\ 1, & C_1(m,n) \neq C_2(m,n) \end{cases}$, C_1 is the encrypted image, C_2 is the scrambled encrypted image, M, N are the basic attributes of the test image i.e. width and height respectively.

Image autocorrelation test

Two dimensional autocorrelation function is a widely used tool in statistical research, signal processing (Li et al. 2023), and image processing. They play important roles in many applications, such as estimation filtering, image analysis, and detecting repetitive patterns and structures in images. In this article, we use the method of graph autocorrelation test

Table 5 Information entropy of different remote sensing images before and after encryption

Image	Item	Plain image	Cipher image
RI	b_1	0.0599	7.9970
	b_2	0.0483	7.9969
	b_3	0.0392	7.9973
	b_4	0.0213	7.9977
RI_1	b_1	0.0119	7.9971
	b_2	0.0168	7.9976
	b_3	0.0388	7.9973
	b_4	0.0014	7.9973
RI_2	b_1	0.0492	7.9975
	b_2	0.0280	7.9971
	b_3	0.0106	7.9972
	b_4	0.0042	7.9981
Ref (Al-Khasawneh et al. 2022)			7.9898
Ref (Wang et al. 2015)			7.9973

Table 6 NPCR and UACI of different remote sensing images

Image	item	NPCR(%)	UACI(%)
RI	b_1	99.69	33.31
	b_2	99.53	33.39
	b_3	99.61	33.32
	b_4	99.63	33.33
RI_1	b_1	99.60	33.43
	b_2	99.59	33.32
	b_3	99.62	33.38
	b_4	99.66	33.32
RI_2	b_1	99.58	33.42
	b_2	99.58	33.37
	b_3	99.63	33.36
	b_4	99.59	33.33
Ref (Wang et al. 2015)	b_1	99.58	33.25
	b_2	99.58	33.25
	b_3	99.58	33.25
	b_4	99.58	33.25
Ref (Lai et al. 2023)		99.59	33.28

to evaluate the probability that the pixel values of all pixel pairs in the image are equal. The core process of this method is to convert the image to the frequency domain and then calculate its autocorrelation image. Through this approach, we can obtain detailed information about the spatial correlation between pixels in the image, thereby revealing potential repetitive or periodic structures.

Figure 16 demonstrates the autocorrelation of the plaintext image, where we can observe that the plaintext image exhibits mountainous undulations, indicating a high degree of correlation. Figure 17 displays the autocorrelation of the ciphertext image, showing that the ciphertext image has no correlation except for a two-bit Dirac pulse signal at the center. By comparing Figs. 16 and 17, we can intuitively observe that our designed encryption scheme ensures the security of the remote sensing image, with the following equation:

$$S_x(a,b) = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} R_x(a,b)e^{-2\pi i(au+bv)}dudv = F\left[R_x(a,b)\right] \tag{30}$$

$$S_x = |F(X)|^2 = F(X)\cdot\bar{F}(X) \tag{31}$$

$$R(X) = F^{-1}[F(X)\cdot\bar{F}(X)] \tag{32}$$

In the above equation, $S_x(a,b)$ denotes the power spectral density, $R_x(a,b)$ denotes the autocorrelation function, $F(X)$ denotes the Fourier transform, $\bar{F}(X)$ denotes the conjugate transform, and $R(X)$ denotes the autocorrelation function of the signal X.

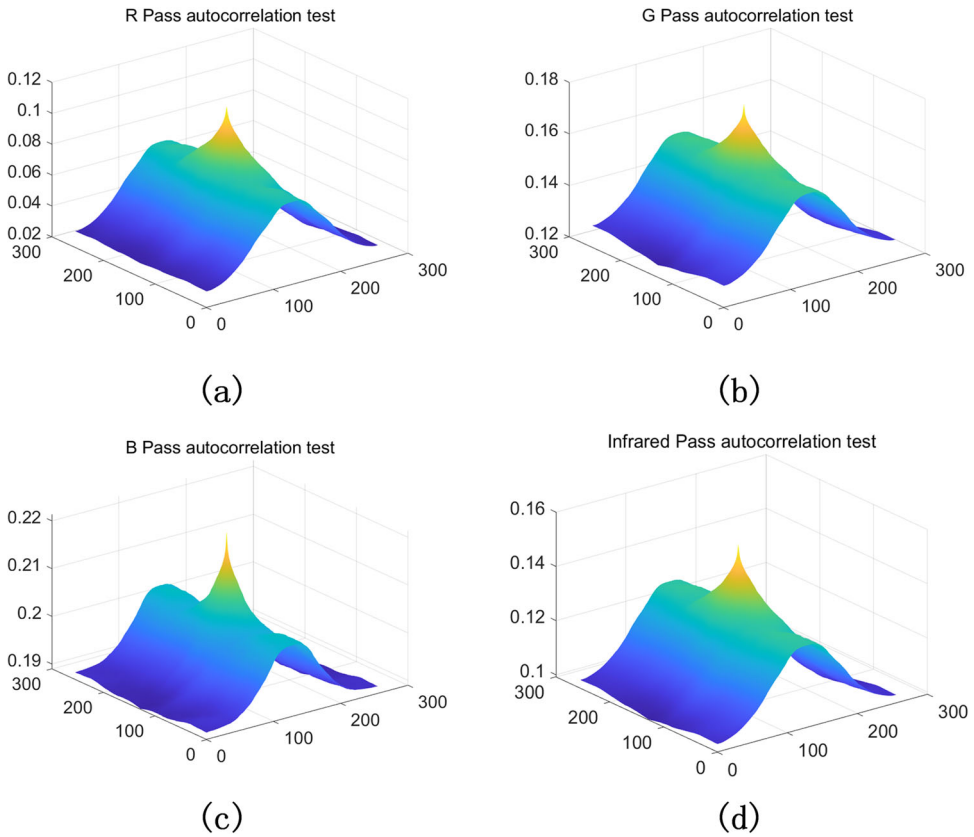

Fig. 16 Autocorrelation images of plaintext images. (a), (b), (c), (d) indicate the autocorrelation of the four bands of remote sensing images in Fig. 12(a), respectively

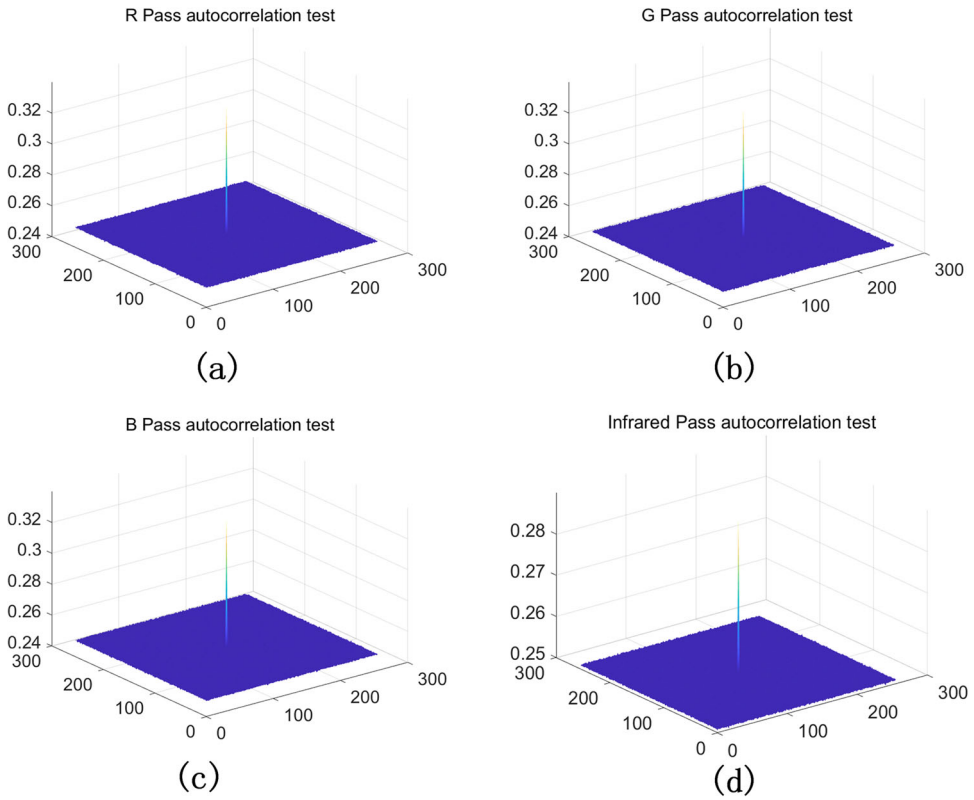

Fig. 17 Autocorrelation images of ciphertext images. (a), (b), (c), (d) correspond to the autocorrelation of the four bands of the ciphertext remote sensing image in Fig. 13(a), respectively

Peak signal-to-noise ratio (PSNR)

The performance and quality of encryption schemes are usually verified by calculating the peak signal-to-noise ratio (PSNR) of encrypted images (Lin et al. 2023). PSNR is a commonly used metric to measure image quality loss, which is calculated based on the mean square error (MSE) between the original image and the encrypted image. Specifically, PSNR is defined as the logarithmic reciprocal of the maximum possible peak signal and MSE of the original image. When calculating PSNR, it is usually assumed that the original image is an unencrypted clear image, while the encrypted image is a processed image using some encryption algorithm. The higher the value of PSNR, the smaller the distortion between the encrypted image and the original image, reflecting the effectiveness of the encryption algorithm in protecting image content. Its equation is expressed as:

$$PSNR = 10\log\left[\frac{I_{\max}^2}{MSE}\right] \tag{33}$$

Where $I_{\max}$ is the maximum pixel value, i.e. 255. MSE and PSNR are the basis of the image evaluation algorithm, PSNR is the peak signal-to-noise ratio and MSE is the mean square error. The typical peak signal-to-noise ratio value in image compression is usually at 30 to 40 dB, because it is inversely proportional to MSE, so the higher the MSE should be, the more serious the image distortion is. The PSNR value is inversely proportional to the quality of the encryption scheme; the lower the PSNR value, the higher the quality of the encryption scheme. The PSNR results for each band after encryption are given in Table 7. It can be observed that our proposed secure coding scheme has more stable and smaller

Table 7 PSNR values of different images

Image	Item	PSNR
RI	b_1	6.8564
	b_2	7.5537
	b_3	7.6048
	b_4	6.6763
RI_1	b_1	6.1527
	b_2	6.6435
	b_3	6.8932
	b_4	7.3251
RI_2	b_1	6.5759
	b_2	7.5218
	b_3	8.6231
	b_4	7.4537
Ref (Liu et al. 2021)	b_1	6.9644
	b_2	6.7471
	b_3	6.9906
	b_4	8.3639

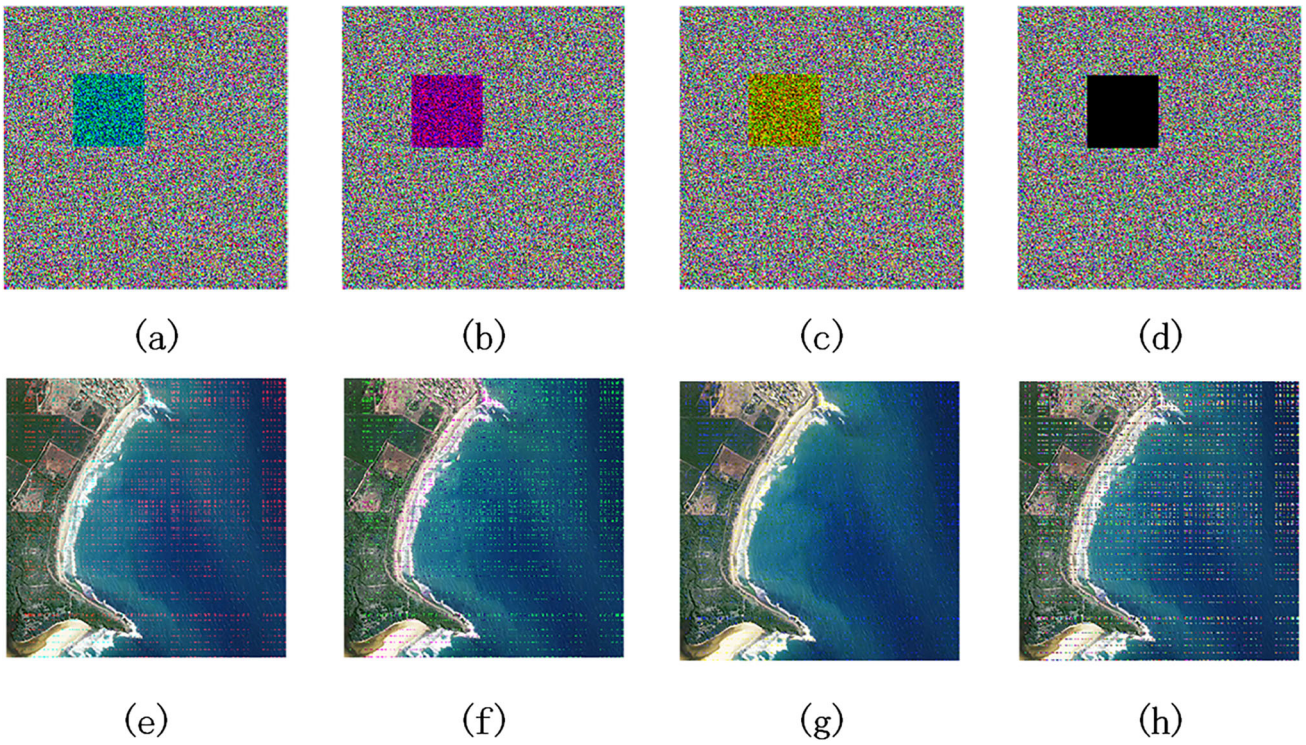

Fig. 18 Shearing attack. (a) indicates a 64*64 shearing attack on the encrypted image b_1 band; (b) indicates a 64*64 shearing attack on the encrypted image b_2 band; (c) indicates a 64*64 shearing attack on the encrypted image b_3 band; (d) indicates a 64*64 shearing attack on the whole encrypted image; (e), (f), (g), and (h) correspond to the recovered remote sensing images after the shearing attacks of (a), (b), (c), and (d), respectively

PSNR value, which further explains the security and stability of our proposed scheme.

Shearing attacks

During the process of encrypted image transmission, some data may be lost or attacked. Cut attack (Zhang and Xiao 2022) is a common method used for image attacks, in which the attacker simulates an attack on the encrypted ciphertext image by modifying certain segments of the ciphertext image. This makes it difficult for the data receiver to obtain complete transmission information. In this section, we performed cut attacks on different channels of the ciphertext image to test whether our proposed encryption scheme can resist cut attacks. The results, as shown in Fig. 18, demonstrate that the attacked data can still be decrypted and that the main

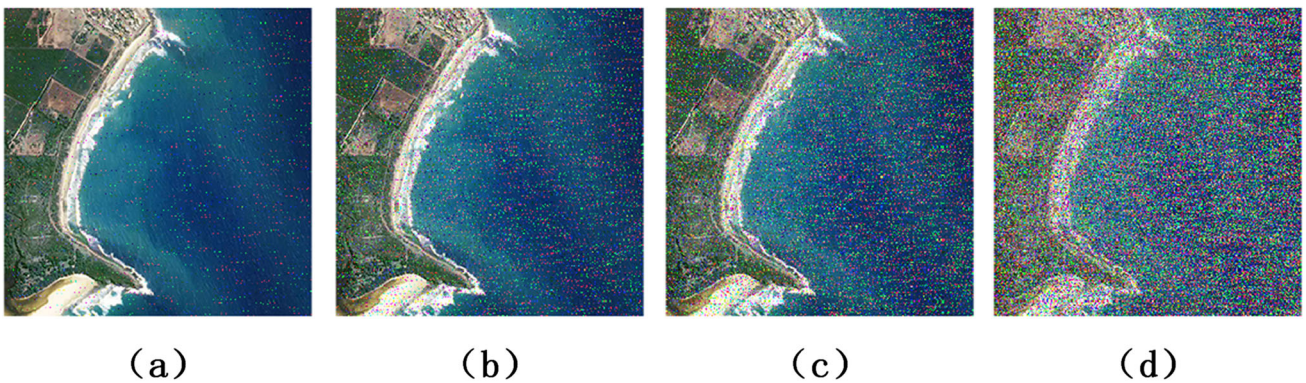

Fig. 19 Noise attack. (a) indicates the addition of 0.01 pretzel noise; (b) indicates the addition of 0.05 pretzel noise; (c) indicates the addition of 0.1 pretzel noise; (d) indicates the addition of 0.3 pretzel noise

information of the original image can be largely recovered. The test results indicate that our proposed encryption scheme possesses high robustness and security.

Noise attack

To test the security of the encryption scheme, typically two different levels of noise attacks are applied to the ciphertext image. Common noise attacks include Gaussian noise, salt-and-pepper noise, Poisson noise, and multiplicative noise. In this paper, salt-and-pepper noise attack is used to test the security of the encryption scheme. This type of attack introduces random pixel values in the image, simulating the noise and interference that may be encountered during the transmission process (Chen et al. 2022). By subjecting the encrypted image to salt-and-pepper noise attack, the quality and correctness of the decrypted image are observed to determine the image's resistance to various attacks during transmission. This method helps us gain a better understanding of the robustness of the image encryption algorithm, enabling optimization and improvement to enhance the image's security and reliability during transmission. The test results, as shown in Fig. 19, indicate that as the salt-and-pepper noise increases, the quality of the decrypted image gradually deteriorates. However, even when the salt-and-pepper noise reaches a relatively high level of 0.3, the outline of the original image can still be observed. The test results demonstrate that the encryption scheme proposed in this paper can resist salt-and-pepper noise attacks, thus proving its high robustness.

Conclusion

In the paper, firstly, a Sin chaos paradigm is designed, which enhances the fixed patterns of one-dimensional and high-dimensional chaos systems. By constructing chaotic systems of different dimensions, dynamic expansion of chaotic systems is achieved, thereby increasing the complexity and flexibility of chaotic systems. Experimental analysis demonstrates excellent chaotic behavior in the chaotic systems constructed using the Sin paradigm. Secondly, since remote sensing image data is extensive, DNA encoding is chosen for parallel processing of remote sensing images. To avoid potential threats arising from the fixed combinations of DNA encoding, DNA-TRV is proposed. The secondary expansion of DNA-TRV disrupts the fixed combinations of DNA encoding, allowing for dynamic selection of DNA encoding and further enhancing the security of the encryption scheme. Additionally, in conjunction with elliptic curves, an elliptic curve "Ring" key concealment and transmission strategy is introduced. This scheme combines the advantages of symmetric and asymmetric encryption, ensuring the security of key embedding locations while concealing the key within the ciphertext image. Finally, a secure compression coding scheme based on the Sin chaos paradigm and DNA permutation is designed and applied to the protection of remote sensing images. After analysis of experimental simulation, this scheme has been demonstrated to possess security, flexibility, scalability, and diversity. It effectively safeguards the security of remote sensing images and has successfully passed various performance tests.

Nevertheless, this scheme was supposed to be demonstrated better at this stage, however, shortcomings still exist such as only partial restoration of the irregular sensing region ROI type images, which will be conquered or searched relevant solutions in the following research. Furthermore, by combining remote sensing image compression and ciphertext retrieval technology, the encrypted remote sensing images will be uploaded to the cloud server within ciphertext form, which ensure data security of remote sensing images and save local storage resources.

Acknowledgements We would like to express our gratitude to Professor Makram Ibrahim for his assistance

Author Contributions Conceptualization, Methodology, Investigation, Writing - review & editing: [Haiyang Shen]; Software, Investigation, Writing- original draft: [Jinqing Li]; Visualization, Supervision, Funding acquisition: [Xiaoqiang Di]; review: [Xusheng Li]; Investigation: [Zhenxun Liu]; Investigation, Supervision: [Makram Ibrahim].

Funding This research was funded by the National Key Research and Development Program Science and Technology Development Plan Project of Jilin Province, China: Research on Key Technology of Optical Encryption for Remote Sensing Images (20220402013GH), Natural Science Foundation of Chongqing: Research on Privacy Protection Mechanism of Vehicle-to-everything Based on Blockchain (CSTB2022NS CQ-MSX1434), Natural Science Foundation of Chongqing (cstc2021jcyj-msxmX0500).

Data Availability Data will be made available on request.

Declarations

Competing Interests The authors declare no competing interests.

Informed Consent Not applicable for studies not involving humans.

Institutional Review Board Statement Not applicable for studies not involving humans or animals.

References

Al-Khasawneh MA, Uddin I, Shah SAA (2022) An improved chaotic image encryption algorithm using hadoop-based mapreduce framework for massive remote sensed images in parallel iot applications. Cluster Computing

Alshaer N, Nasr ME, Ismail T (2021) Hybrid mppm-bb84 quantum key distribution over fso channel considering atmospheric turbulence and pointing errors. IEEE Photonics J 13(6):1–9

Alsubaei FS, Alneil AA, Mohamed A, Hilal AM (2023) Block-scrambling-based encryption with deep-learning-driven remote sensing image classification. Remote Sensing 15(4):1022

Bao W, Zhu C (2022) A secure and robust image encryption algorithm based on compressive sensing and dna coding. Multimedia Tools and Applications 81(11):15977–15996

Chen Z, Ye G (2022) An asymmetric image encryption scheme based on hash sha-3, rsa and compressive sensing. Optik 267:169676

Chen Y, Xie S, Zhang J (2022) A novel double image encryption algorithm based on coupled chaotic system. Phys Scr 97(6):065207

Chen X, Mou J, Cao Y, Yan H, Jahanshahi H (2023) A chaotic color image encryption scheme based on improved arnold scrambling and dynamic dna encoding. Multimedia Tools and Applications, pages 1–22

Eldin SS, Nasr M, Khamees S, Sourour E, Elbanna M (2009) Ldpc coded mimo ofdm-based ieee 802.11 n wireless lan. In 2009 IFIP International Conference on Wireless and Optical Communications Networks, pages 1–5. IEEE

Eldin SS, Nasr M, Khamees S, Sourour E, Elbanna M (2009) Ldpc coded mimo ofdm-based ieee 802.11 n wireless lan. In: 2009 IFIP International conference on wireless and optical communications networks, pages 1–5. IEEE

Elkandoz MT, Alexan W (2022) Image encryption based on a combination of multiple chaotic maps. Multimedia Tools and Applications 81(18):25497–518

Feng W, Qin Z, Zhang J, Ahmad M (2021) Cryptanalysis and improvement of the image encryption scheme based on feistel network and dynamic dna encoding. IEEE Access 9:145459–145470

Feng W, Zhao X, Zhang J, Qin Z, Zhang J, He Y (2022) Image encryption algorithm based on plane-level image filtering and discrete logarithmic transform. Mathematics 10(15):2751

Feng W, Wang Q, Liu H, Ren Y, Zhang J, Zhang S, Qian K, Wen H (2023) Exploiting newly designed fractional-order 3d Lorenz chaotic system and 2d discrete polynomial hyper-chaotic map for high-performance multi-image encryption. Fractal and Fractional 7(12):887

Feng W, Zhang J, Chen Y, Qin Z, Zhang Y, Ahmad M, Woźniak M (2024) Exploiting robust quadratic polynomial hyperchaotic map and pixel fusion strategy for efficient image encryption. Expert Syst Appl 246:123190

Gao S, Wu R, Wang X, Wang J, Li Q, Wang C, Tang X (2023) A 3d model encryption scheme based on a cascaded chaotic system. Signal Process 202:108745

Gottwald GA, Melbourne I (2016) The 0-1 test for chaos: a review. Chaos detection and predictability, pages 221–47

He D, He C, Jiang LG et al (2001) Chaotic characteristics of a one-dimensional iterative map with infinite collapses. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 48(7):900–6

Huang ZW, Zhou NR (2022) Image encryption scheme based on discrete cosine stockwell transform and dna-level modulus diffusion. Optics & Laser Technology 149:107879

Jafari A, Hussain I, Nazarimehr F et al (2021) A simple guide for plotting a proper bifurcation diagram. International Journal of Bifurcation and Chaos 31(01):2150011

Jasra B, Moon AH (2022) Color image encryption and authentication using dynamic dna encoding and hyper chaotic system. Expert Syst Appl 206:117861

Lai Q, Hu G, Erkan U (2023) A novel pixel-split image encryption scheme based on 2d salomon map. Expert Syst Appl 213:118845

Li C, Sprott JC, Zhang X, Chai L, Liu Z (2022) Constructing conditional symmetry in symmetric chaotic systems. Chaos, Solitons & Fractals 155:111723

Li D, Li J, Di X, Li B (2023) Design of cross-plane colour image encryption based on a new 2d chaotic map and combination of ecies framework. Nonlinear Dyn 111(3):2917–2942

Li D, Li J, Di X (2023) Design of cross-plane colour image encryption based on a new 2d chaotic map and combination of ecies framework. Nonlinear Dyn 111(3):2917–42

Liang Q, Zhu C (2023) A new one-dimensional chaotic map for image encryption scheme based on random dna coding. Optics & Laser Technology 160:109033

Lin CH, Wen CH, Lai HY (2023) Multilayer convolutional processing network based cryptography mechanism for digital images infosecurity. Processes 11(5):1476

Liu Z, Li J, Di X, Man Z, Sheng Y (2021) A novel multiband remote-sensing image encryption algorithm based on dual-channel key transmission model. Security and Communication Networks 2021:1–27

Lone MA, Qureshi S (2022) Rgb image encryption based on symmetric keys using arnold transform, 3d chaotic map and affine hill cipher. Optik 260:168880

Lv Z, Sun F, Cai C (2022) A new spatiotemporal chaotic system based on two-dimensional discrete system. Nonlinear Dyn 109(4):3133–44

Maiwald V (2023) Frameworks of sustainability and sustainable development in a spaceflight context: a systematic review and critical analysis. Acta Astronautica

Masood F, Driss M, Boulila W (2022) A lightweight chaos-based medical image encryption scheme using random shuffling and xor operations. Wireless Pers Commun 127(2):1405–32

Meng X, Li J, Di X, Sheng Y, Jiang D (2022) An encryption algorithm for region of interest in medical dicom based on one-dimensional eλ-cos-cot map. Entropy 24(7):901

Nan SX, Feng XF, Wu YF, Zhang H (2022) Remote sensing image compression and encryption based on block compressive sensing and 2d-lcccm. Nonlinear Dyn 108(3):2705–2729

Ravichandran D, Banu SA, Murthy B et al (2021) An efficient medical image encryption using hybrid dna computing and chaos in transform domain. Medical & Biological Engineering & Computing 59:589–605

Ray A (2022) Dna mutation, repair, and recombination. Genetics Fundamentals Notes, pages 433–90

Rementeria S (2022) Power dynamics in the age of space commercialisation. Space Policy 60

Richman S, Douglas EL, Moorman JR (2004) Sample entropy. Methods Enzymol 384:172–184

Sahoo S, Roy BK (2022) Design of multi-wing chaotic systems with higher largest lyapunov exponent. Chaos, Solitons & Fractals 157:111926

Tong XY, Xia GS, Lu Q et al (2020) Land-cover classification with high-resolution remote sensing images using transferable deep models. Remote Sens Environ 237:111322

Wang X, Liu L, Zhang Y (2015) A novel chaotic block image encryption algorithm based on dynamic random growth technique. Opt Lasers Eng 66:10–8

Wang X, Li Y, Jin J (2020) A new one-dimensional chaotic system with applications in image encryption. Chaos, Solitons & Fractals 139:110102

Wang X, Liu C, Jiang D (2022) An efficient double-image encryption and hiding algorithm using a newly designed chaotic system and parallel compressive sensing. Inf Sci 610:300–325

Wang R, Li C, Kong S, Jiang Y, Lei T (2022) A 3d memristive chaotic system with conditional symmetry. Chaos, Solitons & Fractals 158:111992

Wen H, Lin Y (2023) Cryptanalyzing an image cipher using multiple chaos and dna operations. Journal of King Saud University-Computer and Information Sciences 35(7):101612

Wen H, Lin Y (2024) Cryptanalysis of an image encryption algorithm using quantum chaotic map and dna coding. Expert Syst Appl 237:121514

Yan X, Wang X, Xian Y (2021) Chaotic image encryption algorithm based on arithmetic sequence scrambling model and dna encoding operation. Multimedia Tools and Applications 80:10949–83

Yildirim M (2022) Optical color image encryption scheme with a novel dna encoding algorithm based on a chaotic circuit. Chaos, Solitons & Fractals 155:111631

Yuan G, Hao Q (2020) Digital watermarking secure scheme for remote sensing image protection. China communications 17(4):88–98

Zhang H, Wang Z (2022) Human activities and natural geographical environment and their interactive effects on sudden geologic hazard: A perspective of macro-scale and spatial statistical analysis. Appl Geogr 143:102711

Zhang R, Xiao D (2022) Double image encryption scheme based on compressive sensing and double random phase encoding. Mathematics 10(8):1242

Zhang S, Zheng J, Wang X (2020) Initial offset boosting coexisting attractors in memristive multi-double-scroll hopfield neural network. Nonlinear Dyn 102:2821–41

Zheng Y, Hong K, Wang B, Liu D, Chen T, Wang Z (2021) Genetic diversity for accelerating microbial adaptive laboratory evolution. ACS Synth Biol 10(7):1574–1586

Zheng Y, Hong K, Wang B et al (2021) Genetic diversity for accelerating microbial adaptive laboratory evolution. ACS Synth Biol 10(7):1574–86

Zheng Q, Huang W, Xia Q, Dong Y, Ye H, Jiang H, Chen S, Huang S (2023) Remote sensing monitoring of rice diseases and pests from different data sources: a review. Agronomy 13(7):1851

Zhou Z, Xu X, Yao Y, Jiang Z, Sun K (2023) Novel multiple-image encryption algorithm based on a two-dimensional hyperchaotic modular model. Chaos, Solitons & Fractals 173:113630