Design and Optimization of Reversible Information Hiding Image Encryption Algorithms in the Context of Electronic Information Security

Li Zhang*, Keke Shan
School of Electrical and Electronic Engineering, Zhengzhou Railway Vocational & Technical College, Zhengzhou, 450052, China

***Abstract*—With the widespread application of electronic information, in order to meet the growing security needs in the field of electronic information security, a new encryption algorithm based on a novel chaotic map with traversal and chaos characteristics has been proposed. By introducing a hash algorithm and chaotic map, the randomness and nonlinear characteristics of the system are enhanced, and the confidentiality of data and the security of the system are improved. The encryption process includes generating chaotic sequences, constructing permutation boxes, and DNA encoding operations, ultimately generating cipher-text images with high randomness. Meanwhile, an information-hiding encryption algorithm with a four-dimensional conservative chaotic system is designed, which improves the randomness and initial value sensitivity of the algorithm by introducing a chaotic system, and optimized reversible information hiding and image encryption. The algorithm includes chaotic system encryption, additional data embedding, rearrangement strategy, and symmetric structure data extraction and image restoration. The algorithm was robust to images with 50% tampering degree, with an average peak signal-to-noise ratio of 31.26dB, demonstrating high key sensitivity. In the light home plot test, the peak signal-to-noise ratio reached 57.2dB. Under the same QF value but different embedding amounts, the signal-to-noise ratio of the algorithm was 46.9dB, which was superior to other algorithms, highlighting its outstanding performance in different challenges.**

***Keywords*—Information security; reversible information hiding; key sensitivity; chaos system optimization**

I. Introduction

In today's digital society, the transmission and storage of electronic information have become an indispensable part of daily life and commercial activities. However, currently, the security of electronic information has also received increasing attention [1]. Especially in image transmission and storage, protecting sensitive information from unauthorized access and malicious tampering has become an urgent task [2-3]. Although existing technologies have made progress in certain aspects, they still face challenges such as data loss and decreased image quality, which are particularly prominent in traditional information hiding and encryption methods. Field progress indicates that although various encryption and information hiding techniques have been proposed, most methods find it difficult to strike a balance between security and image quality [4-5]. The challenge lies in how to improve the security and ability to resist attacks of the system without sacrificing image quality. In addition, existing reversible information hiding techniques often have low efficiency in processing high-resolution images or complex scenes, and lack scalability when facing large-scale data. The unresolved issues include how to design an algorithm that can effectively resist various attacks while maintaining image integrity and visual quality, while also possessing high efficiency and good scalability. The importance of research lies in its aim to fill the gap in existing research by proposing an image encryption algorithm based on reversible information hiding, addressing the limitations of traditional methods, and improving the security of electronic information and data integrity. The innovation of the research is reflected in the following aspects: firstly, it introduces a new type of chaotic mapping and DNA encoding technology, enhancing the randomness and nonlinear characteristics of the algorithm, thereby improving the security of the system; Secondly, by optimizing the reversible information hiding and image encryption processes, it is possible to protect image privacy without losing key information of the image; Finally, this study also evaluated the performance of the algorithm, demonstrating its robustness and efficiency in different attack scenarios. I hope that research can promote the development of electronic information security technology and provide new ideas and methods for research in related fields.

The study is divided into five sections. Section II is a summary of previous privacy security and image encryption research. Section III is the design and optimization of reversible IEA enhanced by Chaotic Mapping and DNA encoding (CM-DNA). Section IV is the performance evaluation of reversible information Hiding Image Encryption Algorithm (HIEA) based on four-dimensional conservative chaotic systems. Section V is a conclusion of the entire paper.

II. Related Works

In the context of information digitization, many scholars have studied the privacy and security issues faced by image transmission. To address the privacy and security issues faced by medical institutions when using electronic medical records, Keshta and other scholars conducted a comprehensive review of relevant literature to understand the privacy and security issues faced by medical institutions when using EMR. The research content included academic articles, reports, and case studies [6]. To study the security vulnerabilities brought about by digital transformation, Akanksha et al. investigated and collected relevant data to analyze the potential risks and

vulnerabilities in digital transformation. This method took measures to evaluate and address identified risks to better control and manage risks [7]. To explain how the interaction between individual factors and organizational background affected information security behavior, scholars such as Lin proposed a theoretical framework, which was used to explain how information security behavior interacts with individual meaning construction and organizational culture [8]. Li et al. developed a data aggregation solution method, which can generate and use group session keys to protect sensitive patient information [9]. To summarize the correlation of individual cybersecurity awareness, knowledge, and behavior in information security, Zwilling and her team members analyzed survey data and explored the correlation of cybersecurity awareness, knowledge, behavior, and protection tools through statistical analysis and data comparison, as well as the impact of countries and gender on these relationships [10].

In today's digital information transmission and storage environment, the need to protect image privacy and confidential data is becoming increasingly prominent. Liu et al. developed a new method to protect the secret data. The study used Chunk Encryption (CE) to encrypt the original image, while using the Redundancy Matrix Representation (RMR) method to generate a space for accommodating secret data [11]. Hua designed a new solution using CFSS technology to solve the issue of accurately extracting embedded data while protecting the privacy of the original image. This scheme encrypted the original image into n smaller images using a key and sent them to the data hiding person [12]. Chen et al. developed a new RDH-EI model that utilized multiple data hiding agents and secret sharing techniques. This method divided the original image into multiple encrypted images of consistent size and hides them for data [13]. Ke and his team members proposed two data embedding methods. One was homomorphic differential extension (HDE-ED) in the encrypted domain, which supported extracting data from reconstructed images; Another approach was Differential Expansion (DE-IS) in image sharing, which supported extracting data from labeled shares before image reconstruction [14]. Liu et al. proposed a reversible data hiding algorithm with image camouflage encryption and bit plane compression, which converted secret images into another meaningful target image using camouflage encryption algorithm [15]. But there are still research limitations, as shown in Table I.

As shown in Table I, there are still issues in current research, such as a lack of specific technical solutions, unverified risk management practices, the security and applicability of blockchain solutions to be tested, limited universality of survey results, model complexity and practical application feasibility not evaluated, unproven deployment security and efficiency of data embedding methods, and the adaptability and robustness of algorithms to different image types to be confirmed. Overcoming these difficulties requires empirical research, cross sample testing, security evaluation, and algorithm optimization to enhance the practicality and universality of the research.

In summary, many experts have conducted in-depth research on privacy and security issues in the use of electronic medical records and digital image transmission in medical institutions, but there are still some shortcomings in current research. Therefore, research proposes the design and optimization of reversible information-hiding image encryption algorithms based on the background of electronic information security, improving the security and anti-attack capabilities of image encryption algorithms, etc., to promote the development of algorithms and their wider application in the field of electronic information security.

TABLE I. LIMITATIONS AND BLANKS OF CURRENT RESEARCH

Authors	Research Method	Research Findings	Limitations of the Study
Keshta et al.	Comprehensive literature review	Understanding privacy and security issues with EMR in medical institutions	Lack of specific solutions or technical measures proposed
Akanksha et al.	Data collection and analysis	Methods to evaluate and address potential risks and vulnerabilities in digital transformation	Lack of specific evaluation of risk control and management effectiveness
Lin et al.	Theoretical framework development	Explains the interaction between information security behavior and individual meaning construction and organizational culture	The theoretical framework may require further empirical research for validation
Li et al.	Blockchain-based data aggregation scheme	Generation of group session keys to protect sensitive patient information	The practicality and security of the scheme may need to be tested in broader scenarios
Zwilling et al.	Survey data analysis	Explores the correlation between cybersecurity awareness, knowledge, behavior, and protection tools	Restricted by the representativeness and breadth of survey samples
Liu et al.	Chunk Encryption and Redundancy Matrix Representation	A new method to protect secret data in the original image and embed secret data	The security and efficiency of the new method need further verification
Hua	CFSS technology	A new solution for accurately extracting embedded data while protecting the privacy of the original image	The practicality and adaptability of the scheme to different types of data await examination
Chen et al.	Multiple data hiders and secret sharing techniques	A new RDH-EI model using consistent size encrypted images for data hiding	The complexity of the model and its feasibility in practical applications await assessment
Ke et al.	Homomorphic differential extension (HDE-ED) and Differential Expansion (DE-IS)	Two data embedding methods supporting data extraction from reconstructed images or labeled shares	The security and efficiency of these methods in actual deployment await validation
Liu et al.	Reversible data hiding algorithm based on image camouflage and bit-plane compression	A method to transform secret images into meaningful target images	The robustness of the algorithm and its applicability to different types of images await examination

III. Design and Optimization of Reversible IEA Enhanced by CM-DNA

Section III mainly introduces two innovative reversible IEA. The first section designs an efficient reversible IEA based on CM-DNA. The second section optimizes the reversible information HIEA with a four-dimensional conservative chaotic system.

A. Design of an Efficient Reversible IEA with Novel CM-DNA

To ensure the confidentiality, integrity, and availability of data, a new chaotic mapping has been proposed. This mapping not only has ergodicity and chaos, but also generates random sequences with uniform, continuous, and divergent characteristics [16]. These prominent properties make this chaotic map particularly suitable for use in the field of encryption. By introducing this new type of chaotic mapping, the study aims to further enhance the randomness and nonlinear characteristics of encryption algorithms, to enhance the security of the system and its ability to resist crypt-analysis. Specifically, as shown in Eq. (1).

$$\begin{cases} x_{n+1} = a\sin(x_n) + by_n \\ y_{n+1} = -x_n \end{cases} \tag{1}$$

In Eq. (1), a and b belong to the control parameters; n represent natural numbers; x_n and y_n respectively represent the two states that will occur at step n. The stability properties of a system can usually be described by fixed points in discrete mappings, as shown in Eq. (2).

$$\begin{cases} a\sin(x^*) + by^* = 0 \\ -x^* = 0 \end{cases} \tag{2}$$

Eq. (2) is a two-dimensional chaotic map at point $x_{n+1} = y_{n+1} = 0$, which only contains one fixed point $P = (0,0)$. This study introduces the Jacobi matrix, as shown in Eq. (3)

$$J = \begin{bmatrix} a\cos(x) & b \\ -1 & 0 \end{bmatrix} \tag{3}$$

The steadiness of the fixed point $P = (x^*, y^*)$ is expressed by Eq. (3), which is substituted into equation $P = (0,0)$, as shown in Eq. (4)

$$J = \begin{bmatrix} a & b \\ -1 & 0 \end{bmatrix} \tag{4}$$

According to Eq. (4), the feature expression $P(\lambda) = \lambda^2 - a\lambda + b$ can be obtained, and the feature value can be calculated, as shown in Eq. (5).

$$\lambda_1 = \frac{a + \sqrt{a^2 - 4b}}{2}, \lambda_2 = \frac{a - \sqrt{a^2 - 4b}}{2} \tag{5}$$

A fixed point P is considered stable only if it satisfies the conditions $|\lambda_1| < 1$)and $|\lambda_2| < 1$, where λ_1 and λ_2 are the eigenvalues of the mapping. If the fixed point does not meet these conditions, it is considered unstable. However, the determination of global stability is influenced by parameters a and b, and therefore cannot be simply determined. To better understand global stability, Fig. 1 shows the local stability distribution of two eigenvalues $a \in [-5,5]$ and $b \in [-5,5]$ within the parameter range $|\lambda_1|$ and $|\lambda_2|$.

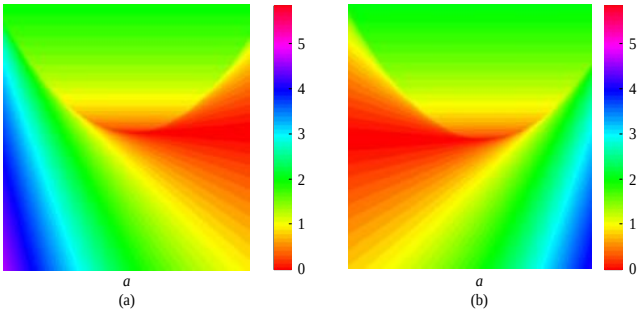


Fig. 1. Eigenvalue stability distribution chart.

In Fig. 1, the encoding color is closely related to the stability of fixed points. The yellow red area indicates that both feature values of the fixed point are less than 1, while the blue and red areas indicate that both feature values are greater than 1. The stability of fixed points can be determined by $|\lambda_1|, |\lambda_2|$. When both eigenvalues are less than 1, the P is stable. On the contrary, it is unstable. The stability of fixed points is influenced by the control parameters a and b, which can affect the calculation of eigenvalues and thus affect the stability of fixed points [17]. Therefore, the stability of Eq. (1) depends on the values of parameters a and b, and changes in these parameters can significantly affect the behavior and stability of fixed points.

Fig. 2 shows the encryption process of the algorithm. Firstly, use the $MD5$ hash algorithm to obtain the decimal sequence. This decimal sequence is converted into a key set $k1$, $k2$ using a specific equation, and is rounded down using the $floor$ function to assure the validity of the key. The setting of the system key involves selecting the initial value of the chaotic sequence. The key to this step is the introduction of hash algorithm and chaotic mapping to increase the randomness and security of the system. Finally, the generated chaotic sequence is transformed into a permutation matrix P in rows M and columns N, which serves as the key output of the encryption algorithm. Then, in the process of generating the permutation S box, the array is initialized first to prepare for subsequent operations. Subsequently, another key is used to iterate the chaotic mapping and obtain a set of random sequences. These random sequences are transformed and limited to a numerical range of 0 to 255 to ensure the validity of subsequent index values. Next, traverse the interval of the access sequence and record the index value of the sequence. Using the index values of these records again, replace the values in the matrix to be

permuted to form the S box. This S box not only contains random sequences generated through chaotic mapping, but also undergoes permutation to form a R matrix $M \times N$ after permutation in the S box. In the third step, a 4×4 image block size was selected to improve the processing efficiency of the algorithm. The number of blocks was determined by calculating the number of columns in the image. Subsequently, based on the calculated sub blocks of a certain row or column, the sub blocks were reorganized to form a partitioned matrix. To establish a connection with DNA encoding rules, the partitioned sub-matrix is transformed into a quaternary matrix to be encoded. Convert the sequence into the encoding, decoding, and operation codes for the image and sequence matrix through Eq. (6).

$$f_i = \mathrm{mod}\left(flood\left(A_i * 10^4 \right), x \right) \tag{6}$$

During the processing, operate in order, as shown in Eq. (7).

$$\begin{cases} U_p\left(u,[r_1,r_2,\ldots,r_n]\right)' = [r_n,r_{n-1},\ldots,r_1]' \\ Q_o\left(q,[s_n,s_{n-1},\ldots,s_1]\right)' = [s_1,s_2,\ldots,s_n]' \end{cases} \tag{7}$$

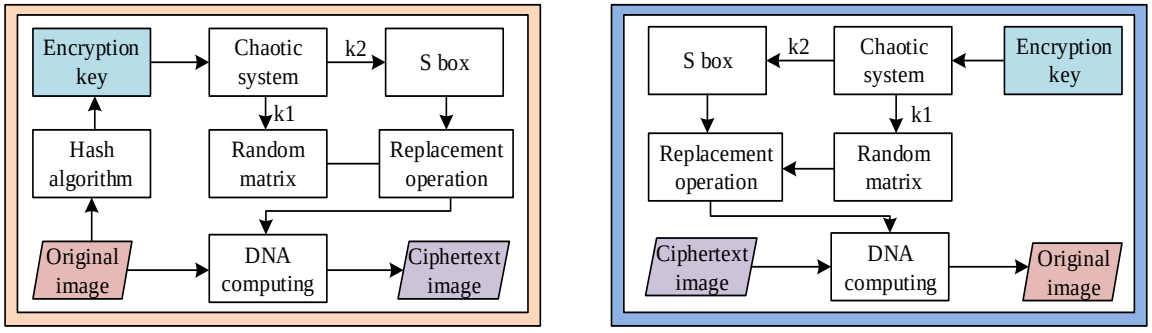
In Eq. (7), u represents an up shift, q represents a down shift, and $[s_1,s_2,\ldots,s_n]'$ represents a column matrix of n rows. Taking the four bases $[B,D,H,M]'$ in DNA encoding 1 as an example, perform up cycle shift as shown in Eq. (8).

$$f_{U_p} = \begin{bmatrix} U_p(B,[B,D,H,M])' \\ U_p(D,[B,D,H,M])' \\ U_p(H,[B,D,H,M])' \\ U_p(M,[B,D,H,M])' \end{bmatrix} = \begin{bmatrix} M & H & D & B\uparrow \\ B & M & H & D\uparrow \\ D & B & M & H\uparrow \\ H & D & B & M\uparrow \end{bmatrix} \tag{8}$$

In Eq. (8), the cyclic shift operation of the matrix starts from the rightmost column. The four types of bases move up one position in sequence, and the overflowing bases automatically fill the left column. To complete an up loop shift, there are four movement steps required. The downward shift is shown in Eq. (9).

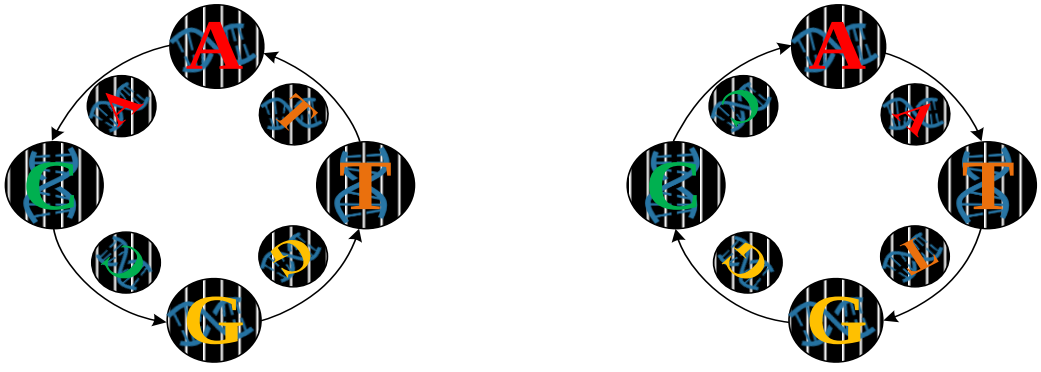
$$f_{D_o} = \begin{bmatrix} D_o(B,[B,D,H,M])' \\ D_o(D,[B,D,H,M])' \\ D_o(H,[B,D,H,M])' \\ D_o(M,[B,D,H,M])' \end{bmatrix} = \begin{bmatrix} M\downarrow & H & D & B \\ B\downarrow & M & H & D \\ D\downarrow & B & M & H \\ H\downarrow & D & B & M \end{bmatrix} \tag{9}$$

DNA cyclic shift begins in the leftmost column of the matrix, with four types of bases moving down one position. Overflowing bases are automatically filled to the right column similar to the upward cyclic shift. Completing a next loop shift requires four columns of movement steps. Fig. 3 vividly illustrates the DNA cyclic translocation, with clear steps of up and down cyclic translocation, forming a cyclic dynamic process. This process makes the generated shifted base structure more complex, while emphasizing the safety and complexity of DNA operations.



(a) Encryption process (b) Decryption process

Fig. 2. Algorithm encryption and decryption process.



(a) Upper circular shift (b) Lower cycle shift

Fig. 3. DNA base shift diagram.

Finally, it is necessary to select 8 DNA encoding methods. Subsequently, after determining the specific encoding rules, five operation methods were chosen. There are multiple combinations and choices of DNA encoding and operation methods here, which introduces the randomness of the calculation process. Finally, merge into the complete cipher-text image C.

B. Optimization of Reversible Information HIEA Based on Four-Dimensional Conservative Chaotic System

A four-dimensional conservative chaotic system was studied and designed, and its chaotic characteristics were analyzed in depth through the dynamics of the system [18]. On the basis of chaotic systems, further improve and optimize existing information hiding encryption algorithms. The four-dimensional conservative chaotic system is shown in Eq. (10).

$$\begin{cases} \dot{x} = (c-b)yz + (d-b)yw + (d-c)zw \\ \dot{y} = (a-c)xz + (a-d)xw - ndw \\ \dot{z} = (a-d)xw + (b-a)xy \\ \dot{w} = (b-a)xy + (c-a)xz + nby \end{cases} \tag{10}$$

In Eq. (10), set these parameters $a = 2.5$、$b = 1$、$c = 1$、$d = 3$、$n = 0.3$. The improved algorithm framework is shown in Fig. 4.

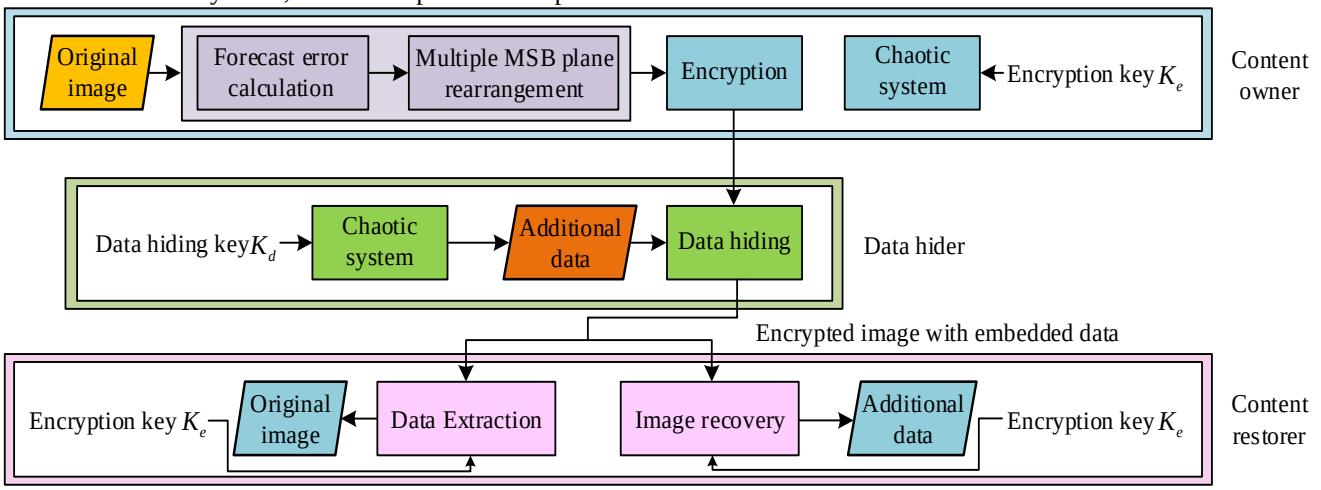


Fig. 4. Improved algorithm framework.

Current algorithms mainly achieve image encryption through simple pixel scrambling. However, this method has the problems of low algorithm complexity and insufficient security. The high randomness and initial sensitivity of chaotic systems are introduced to enhance the security of the algorithm and a comprehensive optimization of reversible information HIEA with pixel prediction and multi MSB plane rearrangement was carried out. The optimized algorithm mainly includes the following key steps. Firstly, a chaotic system is introduced for image encryption, which utilizes the high randomness of the chaotic system to add additional complexity to the encryption process. Secondly, additional data is generated through a chaotic system and embedded in the image to further enhance the randomness of encryption, making it more difficult for attackers to obtain information hidden in the image. Next, the extraction process of additional data is carried out at the decryption end to assure the integrity and correctness of the encrypted data. Finally, image restoration is carried out through optimized algorithms to ensure that the image does not lose information during encryption and decryption, while ensuring the reversibility of the entire system.

According to Fig. 5, detailed operations were conducted on the bit plane in accordance with academic standards for image processing. Firstly, by dividing the bit plane into sub-matrix blocks, a uniform block UB was defined as a block with the same numerical value, while blocks with different numerical values were defined as non-uniform blocks NUB. This division helps to gain a deeper understanding of the local structure of the image and provides a clear foundation for subsequent processing steps. After in-depth analysis of image characteristics, it was observed that a significant increase in the number of uniform blocks resulted in redundancy in the bit plane. To optimize the effectiveness of data embedding, a rearrangement strategy was adopted in the study, where non-uniform blocks were concentrated in the upper part of the plane, while uniform blocks were orderly arranged in the lower part. This strategy aims to reduce the complexity of the data embedding stage, thereby improving overall processing efficiency. After rearrangement, all non-uniform blocks were accurately marked. This labeling system clearly identifies non-uniform blocks that can be embedded in data (marked as 0) and non-uniform blocks that cannot be embedded in data (marked as 1). This labeling method provides an accurate and actionable basis for determining whether sub blocks can be embedded in data in the future.

According to the correlation between pixels, for each non-uniform block, according to the pattern in Fig. 6, the rule is shown in Eq. (11).

$$P = \begin{cases} 0, if\, M + N + B = 0 or 1 \\ 0, if\, M + N + B = 2 or 3 \end{cases} \tag{11}$$

In Eq. (11), in the bit plane, there are three elements M, N, and B, whose values can only be 0 or 1. Determine the value of

P based on the number of 0 and 1. If the current non-uniform block meets the above conditions, it can be defined as an embeddable data block; Otherwise, the block cannot embed additional data. This encryption algorithm is using a symmetric structure and includes two inverse processes. The receiver uses a data hiding key to perform an inverse process, extracts auxiliary data from the bottom right corner of the bit plane, and divides the encrypted image into 8 bit planes. For each embeddable bit plane, the receiver locates the embedded additional data through rules, and then extracts the data one by one in the opposite process. In the image restoration stage, the receiver uses the encryption key for lossless plain-text image restoration. The study first extracts auxiliary data from the lower right corner of the bit plane. Next, extract the auxiliary data of the remaining bit planes one by one, and perform lossless plain-text image restoration according to the prediction scheme. The encryption key is used to iterate chaotic systems, ensuring effective decryption operations. The key to algorithm design lies in the application of symmetric structures, enabling receivers to accurately extract data or restore images based on key types.

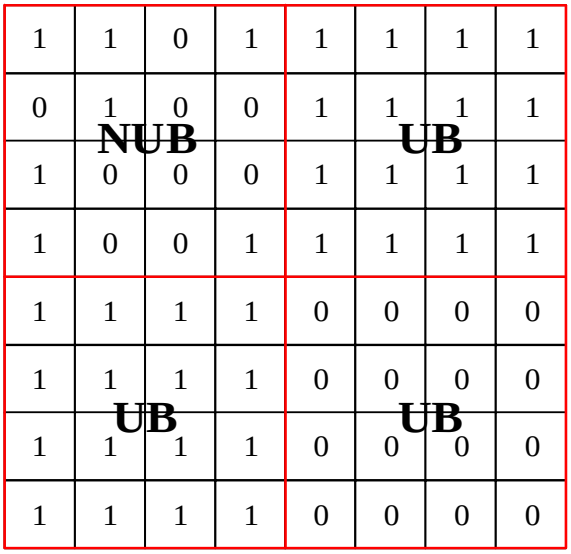


Fig. 5. Bit plane rearrangement.

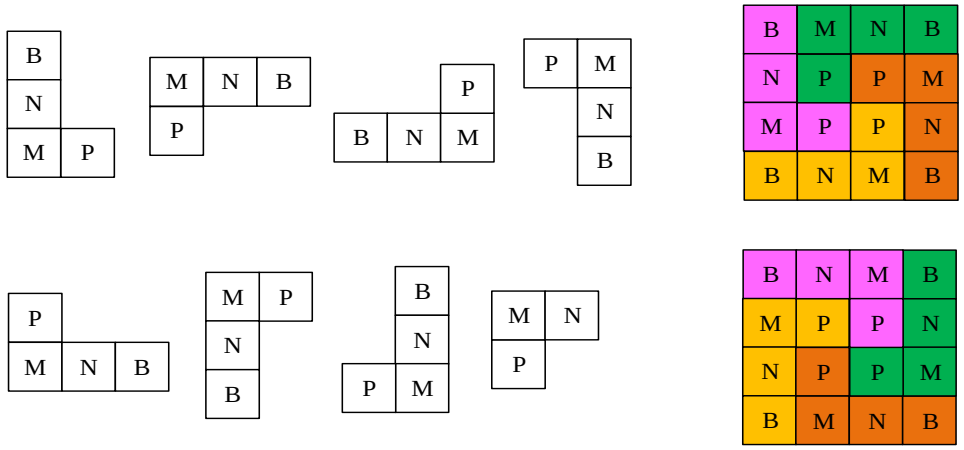


Fig. 6. Two "L" patterns for predicting P through M, N, and B.

IV. Performance Evaluation of Reversible Information HIEA Based on Four-Dimensional Conservative Chaotic System

In electronic information security, the design and optimization of reversible information HIEA are of great significance in ensuring the security and integrity of image data. In this field, secret sharing technology plays a crucial role in ensuring that encryption algorithms have high robustness in the face of various attacks. To evaluate the performance of these algorithms in different attack scenarios, the study selected four representative 256 x 256 test images, namely "Sailboats", "Motochross", "Light home", and "Six Shooter", as shown in Fig. 7. Correspondingly, a comprehensive tampering assessment is required for these images to verify the effectiveness of the algorithm in the context of electronic information security.

(a) Sailboats (b) Motocross (c) Light home (d) Six-Shooter

Fig. 7. Test image.

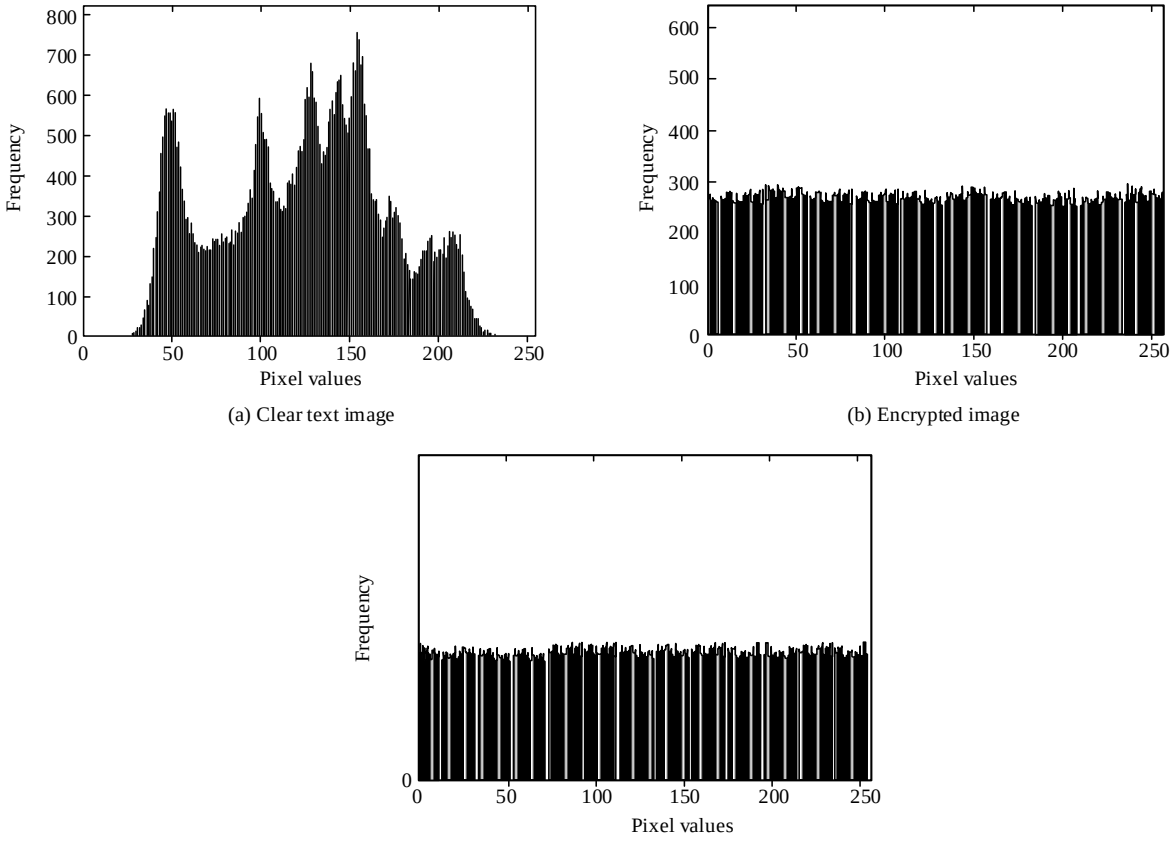
In Fig. 7, these images provide a diverse experimental basis for the design and optimization of reversible information HIEA in the context of electronic information security. These images represent samples of different scenes and complexities, providing rich testing scenarios for the experiment. The visual quality analysis of shadow image restoration secret images with different degrees of tampering was conducted on these images. This analysis covers different samples in various actual attack scenarios, including images of different scenes and complexities.

In Table II, the experimental design considers shadow images with different degrees of tampering to simulate various noise and tampering situations that may be encountered in actual situations. When the shadow image is subjected to up to 50% tampering, the average PSNR remains at the level of 31.26dB, indicating that the established model can still provide excellent visual effects in handling highly tampered situations, ensuring the visual quality of the image.

Fig. 8 shows the grayscale histograms of Sailboats plain-text images, encrypted images, and data embedded images. The grayscale histograms of the generated encrypted image and the embedded encrypted image show a uniform distribution, demonstrating the effectiveness of the algorithm in maintaining the statistical characteristics of the image. Fig. 8 shows the histogram of the original Sailboats image, used as a benchmark for comparison. The study considered two attack scenarios, presented in Fig. 8 (b) and 10 (c), respectively. In Fig. 8 (b), the simulated attacker intercepted two encrypted images and obtained the decryption key. Although the attacker possesses this information, they are still unable to obtain content related to the carrier image, successfully maintaining the security of the image. In Fig. 8 (c), the scenario extends to the attacker intercepting three encrypted cipher-text images, but unable to obtain the decryption key.

TABLE II. THE PROPORTION OF SHADOW IMAGES THAT HAVE BEEN TAMPERED WITH

Image	10%		12.5%		25%		30%		50%	
	PSNR	***SSIM***	***PSNR***	***SSIM***	***PSNR***	***SSIM***	***PSNR***	***SSIM***	***PSNR***	***SSIM***
Six-Shooter	38.65	0.982	38.07	0.979	35.28	0.959	34.33	0.952	31.26	0.926
Sailboats	31.18	0.966	30.34	0.958	27. 28	0.915	26.74	0.899	25.59	0.868
Light home	46.32	0.991	45.38	0.989	40.92	0.977	39.81	0.972	35.78	0.951
Motocross	42.57	0.989	42.35	0.988	40.45	0.982	39.35	0.979	33.12	0.964



(a) Clear text image

(b) Encrypted image

(c) Image with embedded data

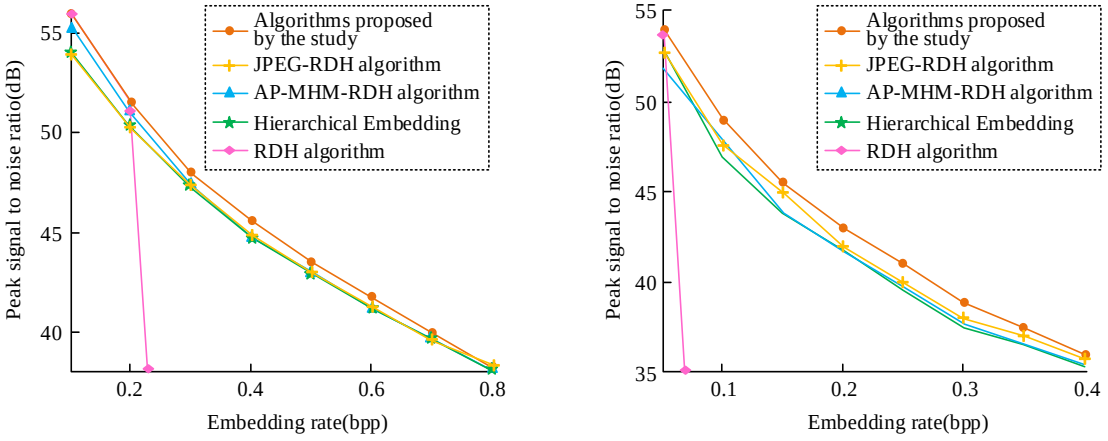
Fig. 8. Sailboats image histogram.

TABLE III. CORRELATION COEFFICIENT COMPARISON

Image		Original image			Cipher-text image		
		Vertical	*Diagonal*	*Level*	*Vertical*	*Diagonal*	*Level*
Motocross	Algorithms proposed by the study	0.9791	0.9539	0.9794	-0.0091	0.0024	-0.0050
	Hierarchical Embedding [19]	0.9756	0.9394	0.9758	0.0182	6.7947e-04	-0.0139
	RHD [20]	0.9371	0.9063	0.9371	0.0273	0.0208	0.0138
Cameraman	Algorithms proposed by the study	0.9587	0.9350	0.9596	-0.0024	-0.0020	0.0070
	Hierarchical Embedding	0.9567	0.9009	0.9568	0.0109	0.0114	-0.0011
	RHD	0.9272	0.9038	0.9261	-0.0363	-0.0356	0.0194

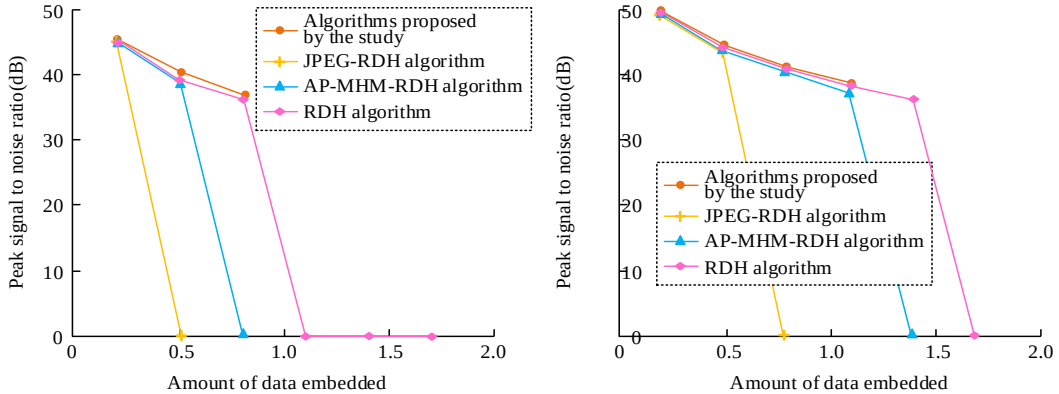
In Table III, encryption keys are set as $k1=[x01, y01]$ and $k2=[x02, y02]$. Motochross is selected as the test image. Firstly, by using the correct key for encryption, the corresponding encrypted image was obtained. Next, minor changes were made to the key, encryption is performed again, and the three indicators after minor changes were calculated. The measured values of the three indicators are close to the theoretical values, indicating that the algorithm exhibited high key sensitivity during the encryption process. The experimental results further verify the key sensitivity of the algorithm in processing Motochross images, and the differentially processed images shows significant changes even with minor changes in the key.

Fig. 9 shows the SNR under different embedding rates. In the test of the light home graph in Fig. 9, the algorithm significantly outperforms the JPEG-RDH method at the same capacity, with a PSNR of up to 57.2dB, surpassing the AP-MHM-RDH and RHD methods. In the Six Shooter image test in Fig. 9 (b), the PSNR of the algorithm reached 54.3dB, which is still outstanding compared to the AP-MHM-RDH method. However, compared with the Hierarchical Embedding method, the proposed algorithm showed stronger adaptive correction ability through improvement. Compared with the experimental results of JPEG-RDH, the multi-level correction model can achieve higher embedding capacity.



(a) Peak signal-to-noise ratio of light home image (b) Peak signal-to-noise ratio of Six-Shooter image

Fig. 9. SNR at different embedding rates.



(a) Light home image signal-to-noise ratio on QF-30 (b) Light home image signal-to-noise ratio on QF-50

Fig. 10. 4 Algorithms process the peak SNR of light home images with different values.

In Fig. 10, the SNR was obtained by testing the Light home image at different QF values. Fig. 10 shows the SNR with QF=30, while Fig. 10 (b) shows the SNR with QF=50. Further analysis was conducted on the peak SNR curves of Light home images with varying embedding amounts under different QF values. The algorithm proposed by the research institute performs better in SNR than other algorithms under the same QF value but different embedding amounts, reaching 46.9dB. As the embedding amount increases, the SNR of the algorithm gradually decreases, showing a trend of decreasing SNR as the embedding amount increases. Under different embedding amounts, this algorithm has a better SNR compared to other algorithms. As the embedding capacity increases, the decreasing trend of its SNR is clearly demonstrated.

V. Conclusion and Discussion

With the development of information hiding technology, the research background involves optimizing traditional image encryption algorithms to adapt to evolving security challenges. We have successfully designed and optimized a reversible information hiding image encryption algorithm (HIEA) based on a novel chaotic mapping and DNA encoding. By introducing hash algorithms and chaos theory, the algorithm significantly improves the randomness and nonlinearity of the image encryption process, thereby enhancing the confidentiality of data and the security of the system. The experimental results show that even at a level of up to 50% image tampering, this algorithm can still maintain an average peak signal-to-noise ratio of 31.26dB, demonstrating excellent robustness and high key sensitivity. In the Guangjiatu test, the algorithm achieved a peak signal-to-noise ratio of up to 57.2dB compared to existing JPEG-RDH methods, further verifying its superior performance in the field of image encryption.

In comparison with existing research, this algorithm demonstrates its innovation and effectiveness in multiple aspects. Firstly, compared with the research of Keshta I et al., this study not only identified privacy and security issues in electronic medical records, but also proposed specific technical solutions, filling the gap in the literature. Secondly, compared with the work of Akanksha K et al., the algorithm proposed in this study provides more specific evaluation and handling methods in risk management and control, enhancing the practicality and effectiveness of risk control. In addition, this study has made particularly outstanding contributions in the field of reversible information hiding. Compared with the Chunk Encryption and Redundancy Matrix Representation methods proposed by Liu Z L et al., this algorithm provides higher security and better data hiding performance while maintaining image quality. Although Hua Z's CFSS technology and Chen B et al.'s RDH-EI model have innovated in data hiding, this algorithm demonstrates better performance in terms of complexity and feasibility in practical applications by simplifying operational processes and optimizing chaotic systems. In terms of verification measures, this study used a comprehensive set of test images, including "Sailboats", "Motochross", "Light home", and "Six Shooter", which are not only representative in content, but also cover a wide range of application scenarios in resolution and complexity. Through testing on these images, this algorithm demonstrates stability and reliability in different attack scenarios.

Although this study has achieved significant results in the field of reversible information hiding image encryption, there is still room for further research and improvement. For example, the performance and efficiency of algorithms in processing higher dimensional data and larger scale images still need to be verified. In addition, the anti-attack ability of algorithms, especially their performance in the face of new network attack methods, is also a focus of future research. Finally, integrating this algorithm with technologies in other fields, such as blockchain and artificial intelligence, to further enhance its application potential in the field of electronic information security is also a direction worth exploring.

References

[1] Keshta I, Odeh A. Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal, 2021, 22(2): 177-183.

[2] Hua Z, Wang Y, Yi S, Zhou Y, Jia X. Reversible data hiding in encrypted images using cipher-feedback secret sharing. IEEE Transactions on Circuits and Systems for Video Technology, 2022, 32(8): 4968-4982.

[3] Ke Y, Zhang M, Zhang X, Liu J, Su T, Yang X. A reversible data hiding scheme in encrypted domain for secret image sharing based on Chinese remainder theorem. IEEE Transactions on Circuits and Systems for Video Technology, 2021, 32(4): 2469-2481.

[4] Culot G, Nassimbeni G, Podrecca M, Sartor M. The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. The TQM Journal, 2021, 33(7): 76-105.

[5] Yang C H, Weng C Y, Chen J Y. High-fidelity reversible data hiding in encrypted image based on difference-preserving encryption. Soft Computing, 2022, 26(4): 1727-1742.

[6] Keshta I, Odeh A. Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal, 2021, 22(2): 177-183.

[7] Akanksha K, Utkarsha Z, Sneha K, Andrade L. Email Security. Journal of Image Processing and Intelligent Remote Sensing (JIPIRS) ISSN 2815-0953, 2022, 2(06): 23-31.

[8] Lin C, Luo X. Toward a unified view of dynamic information security behaviors: insights from organizational culture and sensemaking. ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 2021, 52(1): 65-90.

[9] Li C T, Shih D H, Wang C C, Chen C, Chi C. A blockchain based data aggregation and group authentication scheme for electronic medical system. IEEE Access, 2020, 8(22): 173904-173917.

[10] Zwilling M, Klien G, Lesjak D, Wiechetek L, Cetin F, Basim H. Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 2022, 62(1): 82-97.

[11] Liu Z L, Pun C M. Reversible data hiding in encrypted images using chunk encryption and redundancy matrix representation. IEEE Transactions on Dependable and Secure Computing, 2020, 19(2): 1382-1394.

[12] Hua Z, Wang Y, Yi S, Zhou Y, Jia X. Reversible data hiding in encrypted images using cipher-feedback secret sharing. IEEE Transactions on Circuits and Systems for Video Technology, 2022, 32(8): 4968-4982.

[13] Chen B, Lu W, Huang J, Weng J, Zhou Y. Secret sharing based reversible data hiding in encrypted images with multiple data-hiders. IEEE Transactions on Dependable and Secure Computing, 2020, 19(2): 978-991.

[14] Ke Y, Zhang M, Zhang X, Liu J, Su T, Yang X. A reversible data hiding scheme in encrypted domain for secret image sharing based on Chinese remainder theorem. IEEE Transactions on Circuits and Systems for Video Technology, 2021, 32(4): 2469-2481.

[15] Liu J, Zhang R, Li J, Guan L, Jie C, Gui J. A reversible data hiding algorithm based on image camouflage and bit-plane compression. Computers, Materials & Continua, 2021, 68(2): 2633-2649.

[16] Yang X, Shu L, Chen J, Ferrag M A, Wu J, Nurellari E, Huang K. A survey on smart agriculture: Development modes, technologies, and

security and privacy challenges. IEEE/CAA Journal of Automatica Sinica, 2021, 8(2): 273-302.

[17] Dornelas R S, Lima D A. Correlation Filters in Machine Learning Algorithms to Select De-mographic and Individual Features for Autism Spectrum Disorder Diagnosis. Journal of Data Science and Intelligent Systems, 2023, 3(1): 7-9.

[18] Luo S, Choi T M. E - commerce supply chains with considerations of cyber - security: Should governments play a role?. Production and Operations Management, 2022, 31(5): 2107-2126.

[19] Yu C, Zhang X, Zhang X, Li G, Tang Z. Reversible data hiding with hierarchical embedding for encrypted images. IEEE Transactions on Circuits and Systems for Video Technology, 2021, 32(2): 451-466.

[20] Tang Z, Pang M, Yu C, Fan G, Zhang X. Reversible data hiding for encrypted image based on adaptive prediction error coding. IET Image Processing, 2021, 15(11): 2643-2655.