Journal of Computer Science and Artificial Intelligence
ISSN: 3078-8242 (Print), ISSN: 3078-2309 (Online) | Vol. 4, No. 3, 2025

Key Technology Breakthrough and Application Expansion of Image Encryption Authentication Based on SA-QE Collaboration

Qing Gan *, Zihao Zhao, Yi Du, Mengyuan Sun, Haoran Zhang

Anhui University of Finance and Economics, Bengbu, China

* **Corresponding author**: 3022954802@qq.com

Abstract: With the rapid development of digital multimedia technology, images, as an important carrier of information dissemination, have been widely applied in fields such as healthcare, security, commerce, and social networking. However, images are highly susceptible to tampering, duplication, and illegal use during transmission and storage, posing severe challenges to their authenticity and integrity. Traditional image authentication techniques exhibit significant deficiencies in terms of security, robustness, and invisibility, making them difficult to meet the increasing security demands. This paper proposes a novel image authentication method that integrates Sparse Approximation (SA) and Quantum Encryption (QE), aiming to enhance the security and anti-attack capabilities of digital images. The method first performs subsampling and sparsification on the watermark image, extracts multi-scale features of the image using Discrete Wavelet Transform (DWT), and generates a highly random measurement matrix through quantum logic mapping to achieve encryption and exchange of sparse coefficients. Subsequently, Singular Value Decomposition (SVD) is employed to embed the encrypted watermark information into the low-frequency components of the host image, ensuring the invisibility and robustness of the watermark. Experimental results demonstrate that the proposed method exhibits excellent performance in resisting noise, geometric transformations, and enhancement attacks. When the correct key is used, the watermark can be accurately recovered, while the use of an incorrect key results in complete distortion of the watermark, effectively preventing illegal extraction. The research presented in this paper provides an efficient and secure technical path for digital image copyright protection and content authentication.

Keywords: Image authentication, sparse approximation, quantum encryption, digital watermarking, discrete wavelet transform, singular value decomposition.

1. Introduction

In today's digital age, image has become one of the core media of information expression and dissemination. From medical image diagnosis to satellite remote sensing monitoring, from e-commerce product display to social media content sharing, images are used everywhere. However, with the increasingly powerful function of image editing software, the phenomenon of malicious tampering, forgery or unauthorized use of image content is common. This not only seriously infringes the intellectual property rights of the creators, but also may cause serious misleading in key areas such as judicial evidence collection and news reporting, threatening the social trust system. Therefore, how to effectively ensure the authenticity, integrity and source credibility of digital images has become an important issue to be solved in the field of information security.

Domestic scholars have carried out many explorations in the field of sparse processing and quantum encryption, laying the foundation for image authentication technology: lvyanlin et al. (2020) proposed sparse approximation coding (SAC) method to solve the problem that the traditional matrix factorization algorithm is difficult to capture the inherent geometric structure of data, combined with matrix factorization and L1 regularization to build an optimization model. Experiments on the coil20 dataset show that its clustering accuracy is 8-17% higher than that of Laplace sparse representation and other methods, which can more effectively represent and encode images [1]; Shicuiping et al. (2014) proposed an image sparse representation method based on hybrid transform to solve the problems of insufficient approximation performance of tetrolet transform for smooth images and limited advantages of wavelet transform for detail images. First, the low-frequency part of the image is processed by wavelet transform and principal component transform, and then the high-frequency part is processed by tetrolet transform. Experiments show that this method is superior to the single transform in both subjective and objective quality [2]; Lu Aiping (2020) describes quantum images based on the neqr model, uses three chaotic sequences to generate random rotation angles, and uses a controlled rotating gate to randomly rotate each color bit by $\pm \pi/4$ radians to complete encryption. When decrypting, reverse rotation is sufficient. This scheme has strong key sensitivity (the key space is up to 10^{13}~10^{15}), and the adjacent pixels of the encrypted image have low correlation and uniform histogram [3]; Lu Aiping (2021) proposed a color image quantum encryption scheme based on chaotic sequences. After the classical image is converted to frqi quantum image, the pixel position and gray value are scrambled through three kinds of chaotic sequences and controlled revolving gates. After encryption, the image histogram is evenly distributed and the key space is large. The security of the scheme is verified by classical computer simulation [4]; Xieyuhui (2024) proposed a parallel chaotic encryption algorithm based on blocking operation (improved blocking scheme and key recombination) and a fast encryption algorithm based on bitwise operation (high-low bit separation and combined scrambling) to overcome the shortcomings of traditional image encryption technology in terms of security and

efficiency, which are respectively suitable for multi-core parallel and single core operating environments. Experiments show that the two algorithms have high security and practicability when processing large-scale image data [5]. Foreign research shows a diversified development trend in the field of image security, and the technology exploration is more extensive: Chen Tong and others took the lead in combining sparse approximation with image processing, and proposed a matrix sparse low rank approximation and local preserving model for unsupervised image feature selection. The l2,1-norm sparse regularization of the Kronecker product of two transformation matrices in glram avoids trivial solutions and improves the accuracy of feature selection [6]; Emerson tegan h et al. Studied two path construction methods (Euclidean geodesic based on the linear combination of two atoms and 2-walters geodesic based on the optimal transmission mapping between atoms), and proposed a path based dictionary enhancement strategy to optimize the sparse coding and denoising effect of the standard data set through learning dictionary and structured dictionary, while reducing the amount of image data while retaining key information [7]; Saswatitrivedy et al. Developed an effective fragile watermarking scheme, which can accurately locate the tampered area in the digital image. Compared with other related schemes, this scheme provides better watermark image perception quality and lower false tamper detection rate [8]; Gao Yuhui et al. Used the image processing method of parallel compressed sensing to significantly improve the efficiency of image encryption. At the same time, they used the combination of discrete data sequence subsets generated by the two-dimensional discrete hyperchaotic system for index scrambling and forward-backward diffusion, combined with the sum of the original image initial key and partial pixel values, and generated the initial value and control parameters of the 2d-sls chaotic sequence through sha-512 hash, making the algorithm highly robust to known plaintext and selected plaintext attacks [9]; Xiuli Chai et al. Proposed a new color image encryption scheme to generate a visually meaningful ciphertext image and significantly enhance the connection between the plaintext image and the encryption process. Although foreign research involves multi technology integration, there is still a gap in the collaborative optimization of sparse approximation and quantum encryption, which is difficult to meet the comprehensive requirements of image authentication for security, robustness and processing efficiency at the same time [10].

This paper proposes a new image authentication framework combining sparse approximation (SA) and quantum cryptography (QE). According to the sparse approximation theory, natural signals (such as images) have sparse representation under appropriate bases or dictionaries, that is, only a few non-zero coefficients are needed to accurately reconstruct the original signal. This feature is not only conducive to data compression, but also provides a natural "cover" for information hiding. By encrypting and embedding the watermark information in the sparse domain, the risk of detection and destruction can be effectively reduced. On the other hand, quantum encryption uses the principles of quantum mechanics (such as superposition state, entanglement and measurement collapse) to generate a key sequence with high randomness and unpredictability, which injects a stronger security gene into the traditional encryption algorithm. The combination of quantum encryption and sparse approximation is expected to significantly improve the anti cracking ability of the system while ensuring the robustness of the watermark.

2. Relevant Theoretical and Technical Background

2.1. Sparse Approximation

Sparse approximation is a signal processing technology. Its core idea is to use an over complete base (or "dictionary") to represent the signal, so that the representation of the signal under the base is as "sparse" as possible, that is, most of the coefficients are zero or close to zero, and only a few coefficients have large values. For digital images, although the pixel matrix itself usually does not have sparsity, after appropriate transformation (such as DWT, DCT), its transformation coefficients often show significant sparsity characteristics - energy is concentrated on a few low-frequency coefficients, while most high-frequency coefficients are close to zero.

In this study, sparse approximation is mainly used for watermark image preprocessing. The watermark image is decomposed into low frequency (LL) and high frequency (LH, HL, Hh) subbands by discrete wavelet transform (DWT). Because the low-frequency subband contains the main contour and structure information of the image and has high energy concentration, it is more suitable for sparse processing. Then, each subband is divided into several small blocks, and each block is sparse represented to obtain a set of sparse coefficients. These sparse coefficients not only have a small amount of data, but also embody the key characteristics of watermark, and provide an ideal data basis for subsequent encryption and embedding.

2.2. Quantum Encryption and Quantum Logic Mapping

Quantum Encryption Is Not An Encryption Algorithm That Runs directly on a quantum computer, but a classical encryption scheme that uses the principles of quantum mechanics (such as randomness and non cloning) for reference. Among them, quantum logic map is a pseudo-random sequence generator based on quantum chaos theory. Compared with the traditional chaotic map, quantum logic map has stronger initial sensitivity, longer period and higher randomness, and can generate almost unpredictable key stream.

In this study, quantum logic mapping is used to generate measurement matrix. Measurement matrix plays a key role in compressed sensing and sparse representation. Its role is to project the original signal into a low dimensional space while retaining its main information. A high-quality measurement matrix should have good incoherence and randomness to ensure the reconfigurability and safety of the signal. The element sequence of the measurement matrix generated by quantum logic mapping is extremely random, which makes it difficult for the attacker to infer the original watermark or key through statistical analysis or reverse engineering even if he obtains part of the ciphertext.

The above technical framework of the fusion of sparse approximation and quantum encryption can be clearly presented through the core process diagram, and the logical relationship and operation steps of each link are shown in the figure1.

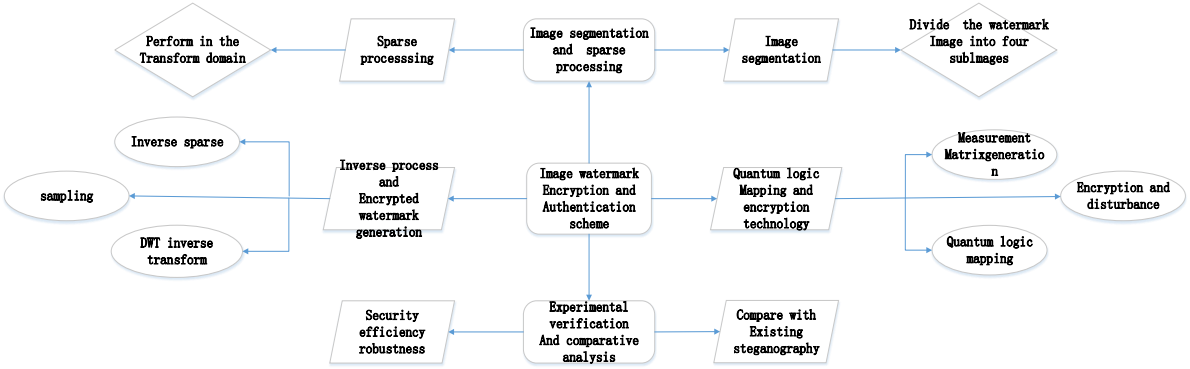


Figure 1. Schematic Diagram of the Projects's Main Content

2.3. Discrete Wavelet Transform (DWT)

Discrete Wavelet Transform (DWT) is a multi-resolution signal analysis tool that can decompose an image into sub bands of different scales and directions. A single DWT can decompose an image into four sub bands: LL (low frequency), LH (horizontal detail), HL (vertical detail), and HH (diagonal detail). The LL subband represents a rough approximation of the image, while the other three subbands contain the edges and texture details of the image. The multi-scale characteristics of DWT make it widely used in image compression, denoising, and watermark embedding.

In this study, DWT was used for two key steps: first, to decompose the watermark image for processing in sparse domains; The second is to decompose the host image and provide appropriate frequency components for watermark embedding. Due to the sensitivity of the human eye to low-frequency information, embedding watermarks in LL sub bands can improve the robustness of watermarks while ensuring invisibility, as low-frequency components are relatively stable in most image processing operations.

2.4. Singular Value Decomposition (SVD)

Singular Value Decomposition (SVD) is a matrix decomposition technique that can decompose any matrix into the product of three matrices: U, ∑, and V ^ T. ∑ is the diagonal matrix, and its diagonal elements are called singular values, representing the energy distribution of the matrix. Singular values have good stability and robustness, and even if the image is slightly disturbed, the variation of their singular values is relatively small. This feature makes SVD an ideal tool for embedding digital watermarks.

In this study, SVD was used in the watermark embedding stage. Specifically, first perform SVD decomposition on the DWT low-frequency sub-band of the host image to obtain its singular value matrix. Then, embed the encrypted watermark information into these singular values. Due to the fact that singular values reflect the overall structural features of an image, modifying them has a minimal impact on visual quality, thereby ensuring the invisibility of the watermark. Meanwhile, due to the stability of singular values, even if the host image is subjected to a certain degree of attack, watermark information can still be effectively extracted.

2.5. Watermark Performance Evaluation Indicators

In order to objectively evaluate the performance of the proposed method, this article adopts the following five commonly used indicators:

Peak Signal to Noise Ratio (PSNR): measures the degree of distortion between the host image and the original image after embedding a watermark, with higher values indicating better image quality.

Normalized cross-correlation (NCC): measures the similarity between the extracted watermark and the original watermark, with values closer to 1 indicating higher fidelity of the watermark.

Mean Structural Similarity (MSSIM): Evaluating image quality from three dimensions: brightness, contrast, and structure, which is more in line with human visual characteristics.

Entropy: measures the randomness and information content of an image, commonly used to evaluate encryption performance. The entropy value of the encrypted image should be close to the theoretical maximum value (such as 8 for 8-bit images).

Normalized Absolute Error (NAE): measures the absolute difference between the extracted watermark and the original watermark, with smaller values indicating higher extraction accuracy.

3. Image Authentication Algorithm Based on Sparse Approximation and Quantum Encryption

This algorithm is mainly divided into three stages: watermark encryption, watermark embedding, and watermark extraction and verification.

3.1. Watermark Encryption

Watermark encryption is the core component of this algorithm, aimed at converting the original watermark image into a highly secure and difficult to crack encrypted watermark. This process includes the following five sub steps:

(1) Watermark preprocessing and subsampling. Firstly, divide the original watermark image (such as 256 × 256 pixels) into four equal sub images (each with 128 × 128 pixels). This block processing not only facilitates parallel computing and improves efficiency, but also enables fault-tolerant recovery when some data is damaged. Subsequently, each sub image is subjected to a first-order discrete wavelet transform (DWT) to obtain its respective LL, LH, HL, and HH sub bands. Due to the fact that DWT subbands are not sparse, further processing is required.

(2) Sparse processing. Sparse the DWT sub bands (especially LL sub bands) of each sub image block by block. The specific approach is to divide each subband into b × b small blocks (such as 8 × 8), and then perform sparse representation under a preset sparse basis (such as DCT basis) to obtain a set of sparse coefficients. Most of these

coefficients are zero or close to zero, with only a few having larger values, thus achieving data compression and feature extraction.

(3) Sparse coefficient exchange and quantum encryption. This is the key innovation of this algorithm. Unlike traditional pixel level encryption, this method operates at the sparse coefficient level. Firstly, generate a highly random sequence using quantum logic mapping and construct a measurement matrix based on it. This matrix is used for nonlinear transformation of sparse coefficients, disrupting their original distribution. Subsequently, the 'Sparse Coefficient Exchange Procedure' is executed, which involves exchanging coefficient positions between sparse blocks of different sub images according to specific rules (controlled by a key). For example, swap the maximum coefficient in a sparse block of sub image 1 with the minimum coefficient in the corresponding block of sub image 3. This operation not only increases the chaos of the data, but also achieves information fusion across sub images, significantly improving the encryption strength.

(4) Measurement Matrix Design. The design of the measurement matrix is directly related to the security of encryption. In this study, the rows and columns of the measurement matrix were filled with chaotic sequences generated by quantum logic mapping. Due to the extreme sensitivity of quantum chaotic sequences to initial conditions, even small changes in the key will result in completely different matrices, ensuring the vastness of the key space and resistance to brute force cracking.

(5) Encryption watermark generation. After completing encryption, it is necessary to restore the encryption coefficients of the sparse domain to image form. This process is called 'inverse sparsification', which involves performing inverse discrete cosine transform (DCT) on each encrypted sparse block to restore it to a dense block of pixels. Subsequently, all blocks are reorganized into complete sub bands and subjected to inverse DWT (IDWT) to obtain encrypted sub images. Finally, the four encrypted sub images are merged into a complete encrypted watermark image through the "anti sampling" operation. The image appears as noise visually and cannot recognize the original content, but it contains complete watermark information.

3.2. Watermark embedding

The goal of the watermark embedding stage is to seamlessly integrate the encrypted watermark information into the host image while ensuring that the visual quality of the host image is not affected. In this stage, a strategy combining DWT and SVD is adopted, and the specific embedding process is shown in the figure2:

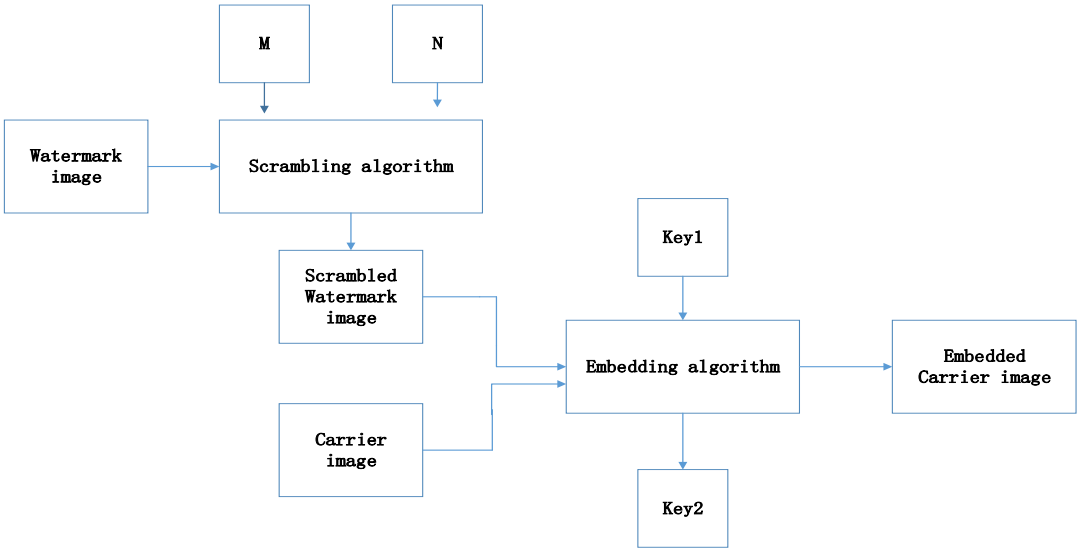


Figure 2. Schematic diagram of image watermark embedding process

(1) Host image decomposition. Firstly, perform a first level DWT on the host image (such as 512 × 512 pixels) to obtain its LL, LH, HL, and HH sub bands. Due to the fact that the LL subband contains the main energy of the image and is relatively stable, it is chosen to embed a watermark in this subband.

(2) SVD decomposition and watermark embedding. Perform singular value decomposition (SVD) on the LL subband to obtain three matrices: U, ∑, and V ^ T. Among them, ∑ is the diagonal matrix of singular values. Scale or block the encrypted watermark image (256 × 256) appropriately to match its size with ∑. Then, using the additive embedding rule, the watermark information is superimposed onto the singular value of ∑. For example, watermark pixel values can be modulated proportionally into small variations of singular values. Due to the minimal impact of singular value perturbations on the overall structure of the image, it can effectively ensure the quality of the embedded image.

(3) Reconstructing watermarked images. After embedding, use the modified singular value matrix ∑ 'and the original U and V ^ T matrices to reconstruct the matrix and obtain new LL sub bands. Finally, perform inverse DWT (IDWT) on this new LL subband along with the unmodified LH, HL, and HH subbands to generate the final watermarked host image.

3.3. Watermark Extraction and Verification

Watermark extraction is the inverse operation of the embedding process, which needs to be performed with the correct key.

The image extraction process is shown in the figure3:

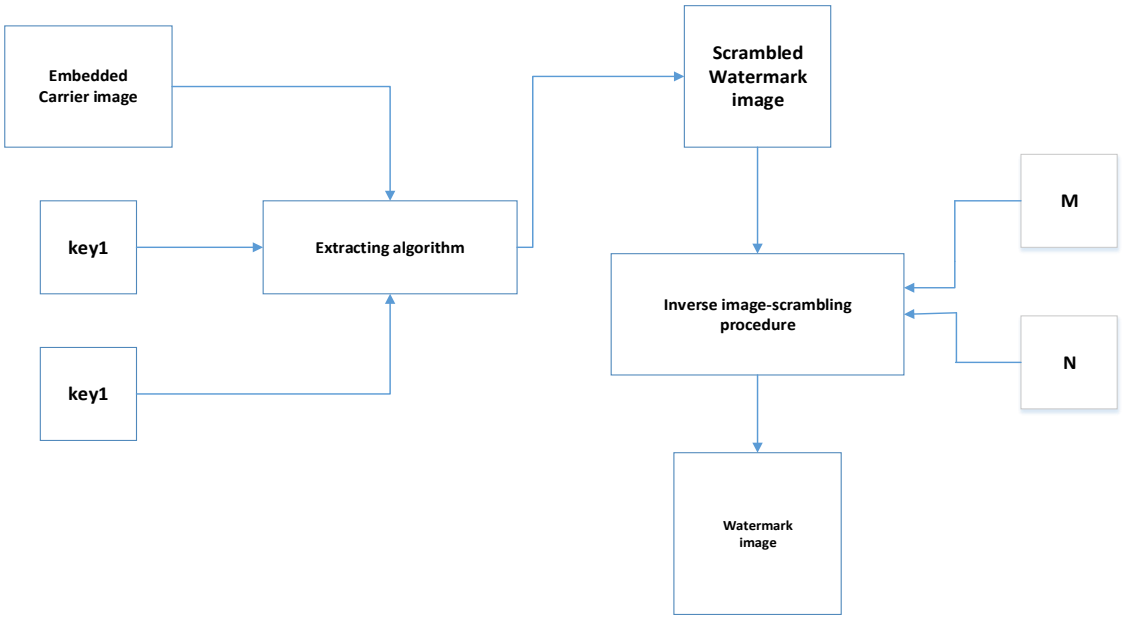


Figure 3. Schematic diagram of image extraction process

(1) Encryption watermark recovery. Firstly, perform the same DWT decomposition on the watermarked host image as during embedding to obtain its LL sub bands. Perform SVD decomposition on the subband to extract singular values containing watermark information. Then, based on the embedding rules, reverse calculation is performed to recover the singular values of the encrypted watermark and reconstruct it into the encrypted watermark image.

(2) Watermark decryption. The decryption process is completely opposite to the encryption process. Firstly, the recovered encrypted watermark is subsampled and DWT is performed to obtain the sub bands of four sub images. Then, using the same quantum key, generate a measurement matrix and perform inverse coefficient swapping operation to restore the original order of sparse coefficients. Next, perform inverse sparsification (IDC) and inverse DWT to obtain four decrypted sub watermarks. By reverse sampling and merging, the original watermark image can be obtained.

(3) Certification and Verification. Compare the extracted watermark with the original watermark and calculate metrics such as NCC and MSSIM. If the indicator value is higher than the preset threshold, it is considered that the image has not been tampered with and the authentication has been passed; Otherwise, it is determined that the image integrity is compromised.

4. Experimental Results and Performance Analysis

4.1. Verification of Imperceptibility of Watermark (Visual Indistinguishability Test)

The core requirement for imperceptibility of watermarks is that the watermarked image has no significant visual difference from the original host image. This experiment verifies this from both subjective visual and objective indicators:

(1) Subjective visual comparison: Using Peppers image as the host image, embedding Mandril and Cameraman watermarks, observing the color transition and texture details of the watermarked image, it was found that it was completely consistent with the original image; Further extracting the edge contour maps of both, the comparison results show that the edge distribution is not missing or distorted, proving that the watermark embedding does not damage the structural integrity of the host image.

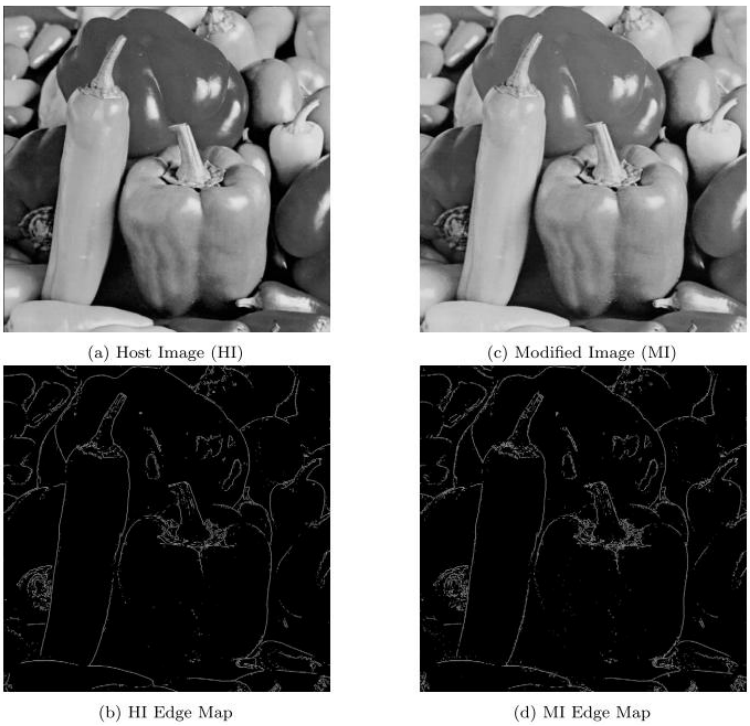


Figure 4. Visual quality analysis between 'pepper' host image (HI) and its corresponding modified Image

(2) Objective metric (PSNR) testing. PSNR is a key indicator for measuring the degree of image distortion, and usually PSNR $\geq$ 30dB is sufficient to meet the requirement of visual distortion free. The experimental data statistics of 10 test images show that the PSN values of watermarked images are distributed in the range of 33-43dB, with an average PSNR of 42.7dB. Among them, the PSNR of Peppers image is 42.78dB, and the PSNR of Lena image is 42.65dB, both far exceeding industry standards, which quantitatively confirms the excellent invisibility of watermarks.

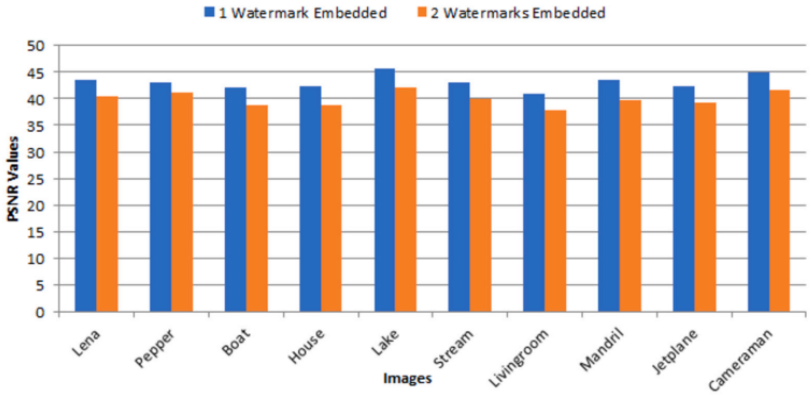
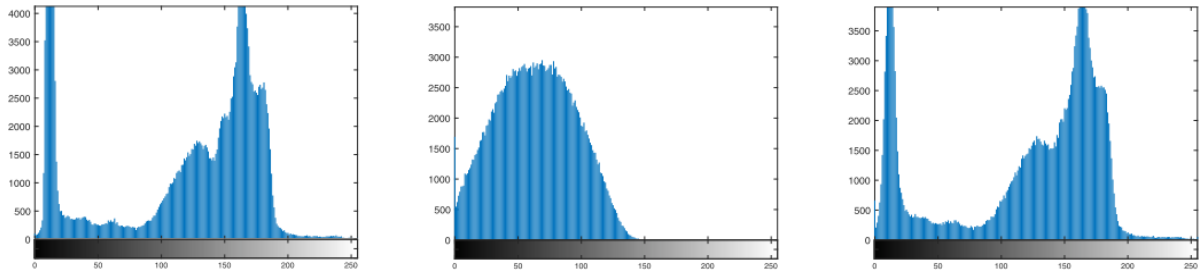


Figure 5. PSER values of the modified images with respect to their corresponding host images

4.2. Robustness and Security Assessment (Anti Attack+Anti Cracking Testing)

Robustness refers to the ability to accurately restore watermarks even after a modified image is attacked; Security refers to the difficulty of cracking or tampering with encrypted watermarks, which is verified through four aspects: histogram, correlation, anti attack testing, and key verification

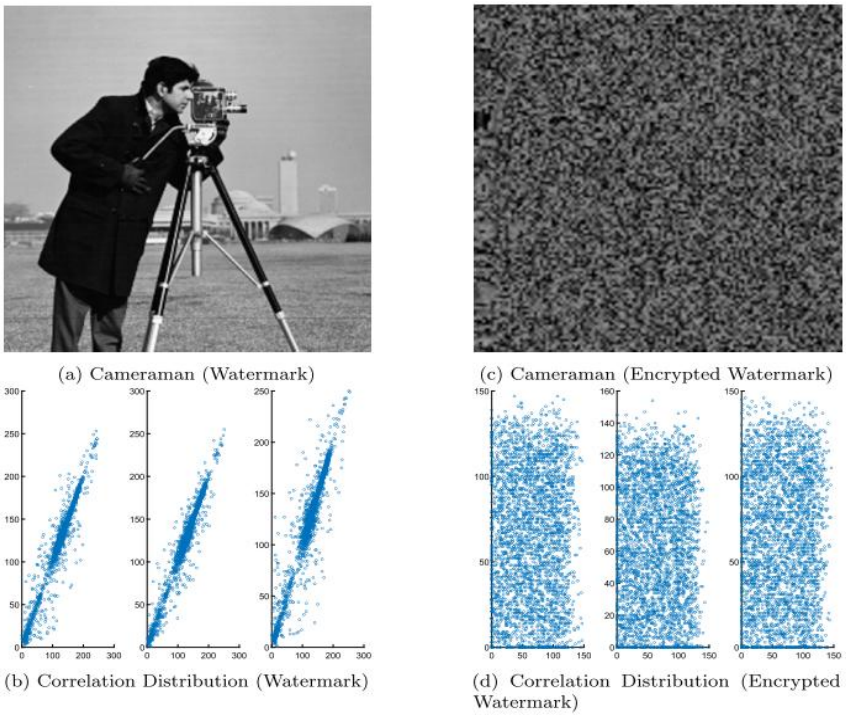
(1) Histogram analysis. The histogram of the original watermark (such as Cameraman) shows a "centralized" distribution, while the histogram of the encrypted watermark shows a "uniform" distribution (with randomly arranged pixels). The histogram of the decrypted watermark highly overlaps with the original watermark, indicating that encryption effectively shuffles the watermark data and decryption can fully recover it.



(a) Watermark Image Histogram (b) Encrypted Watermark Histogram (c) Decrypted Watermark Histogram

Figure 6. Histogram analysis of the watermark Image (WI, Cameraman) iamge, encrypterd image, and decrypted image

(2) Correlation analysis. The pixels of the original watermark have strong correlation (such as horizontal correlation=0.9865 and vertical correlation=0.9367 in the Mandril image), and after encryption, the pixel correlation drops to -0.03~0.03 (close to random), making it difficult for attackers to crack the watermark through "statistical pixel patterns", greatly improving security.



(a) Cameraman (Watermark) (c) Cameraman (Encrypted Watermark)

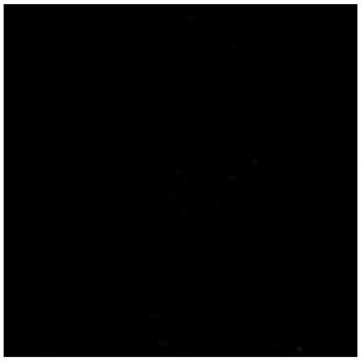
(b) Correlation Distribution (Watermark) (d) Correlation Distribution (Encrypted Watermark)

Figure 7. Correlation distribution along horizontal, vertical, and diagonal for the watermark and encrypted watermark

(3) Anti attack test. Apply enhanced attacks (Gaussian low-pass filtering, median filtering), noise attacks (Gaussian noise, salt and pepper noise, intensity 0.01~0.08), and geometric attacks (10 ° rotation, 0.8 times scaling) to the modified image. The results show that after the attack, PSNR is still ≥ 33 dB, NCC (water print similarity, closer to 1, better) ≥ 0.95, MSSIM (structural similarity) ≥ 0.98, and the watermark can be clearly restored.

(4) Key uniqueness verification. Test the impact of different keys on watermark recovery. When using the 'correct quantum measurement matrix (key)', a clear original watermark can be extracted; If replaced with an incorrect key (such as a randomly generated measurement matrix), the extracted result will be a nearly black meaningless image with no valid watermark information. This result confirms that the key is the only key to decryption, and the system can resist brute force attacks.

(a) 'Cameraman' extracted secret image (using correct secret-keys)



(b) 'Cameraman' extracted secret image (using wrong secret-keys)

Figure 8. Visual quality analysis between the 'Camereman' recover secure watermark image using correct and wrong secret-keys (from the 'Pepper' modified image)

4.3. Embedding Capacity Test (Evaluation of Multi watermark Carrying Capacity)

Embedding capacity refers to the amount of watermark data that can be carried by a unit of host image, and is an important indicator for measuring the practicality of the method. The experimental results show that in a host image of 512 × 512 pixels, this method can simultaneously embed two encrypted watermarks of 256 × 256 pixels, with an embedding capacity of 4 bpp (i.e. each pixel can carry 4 bits of watermark data); If only one watermark is embedded, the capacity is 2bpp. This data far exceeds traditional DWT/SVD methods (usually with an embedding capacity of<1bpp), and can meet the storage requirements of multi-dimensional authentication data such as "copyright identification+traceability information" in practical scenarios.

5. Conclusion

The image authentication technology based on sparse approximation and quantum encryption proposed in this article demonstrates significant advantages in terms of security, robustness, and invisibility. By performing coefficient exchange and quantum encryption in the sparse domain, the confidentiality of the watermark is effectively improved; By combining the embedding strategies of DWT and SVD, the stability of the watermark is enhanced while ensuring visual quality.

However, this method also has some limitations. Firstly, sparse approximation assumes that the data has sparsity, which may require additional sparsity processing for non sparse images, increasing computational complexity. Secondly, algorithms are sensitive to parameters such as block size and embedding strength, and require careful tuning to achieve optimal performance. In addition, the implementation of quantum logic mapping relies on precise numerical calculations, which have certain requirements for computational accuracy.

Acknowledgments

This work is supported by funded by the Undergraduate Research and Innovation Fund Project of Anhui University of Finance and Economics (Project Number: XSKY25152).

References

[1] LvYanlin, Tao Yuting, Zhang Yan Analysis and Improvement of Image Encoding Algorithm Based on Sparse Approximation [J]. Journal of Jinling University of Science and Technology, 2020, 36 (04): 18-21.

[2] Shi Cuiping, Zhang Junping, Zhang Ye A new image sparse representation based on mixed transformation [J]. Journal of Harbin Institute of Technology, 2014, 46 (09): 36-42.

[3] Lu Aiping, Li Panchi Quantum Image Encryption Scheme Based on Chaotic Sequence [J]. Computer and Modernization, 2020, (03):86-92.

[4] Lu Aiping, Li Panchi Quantum encryption scheme for color images based on chaotic sequences [J]. Computer and Digital Engineering, 2021, 49 (04): 692-697+730.

[5] XieYuhui Research and Application of Chaos based Image Encryption Technology [D]. Lanzhou Jiaotong University, 2024.

[6] Chen Tong and Chen Xiuhong. Sparse low-rank approximation of matrix and local preservation for unsupervised image feature selection [J]. Applied Intelligence, 2023, 53(21): 25715-25730.

[7] Emerson Tegan H and Olson Colin and Doster Timothy. Path-Based Dictionary Augmentation: A Framework for Improving k-Sparse Image Processing. [J]. IEEE transactions on image processing: a publication of the IEEE Signal Processing Society, 2019, 29: 1259-1270.

[8] SaswatiTrivedy and Arup Kumar Pal. A Logistic Map-Based Fragile Watermarking Scheme of Digital Images with Tamper Detection [J]. Iranian Journal of Science and Technology, Transactions of Electrical Engineering, 2017, 41(2): 103-113.

[9] Gao Yuhui and Liu Jingyi and Chen Shiqiang. Image encryption algorithms based on two-dimensional discrete hyperchaotic systems and parallel compressive sensing [J]. Multimedia Tools and Applications, 2023, 83(19): 57139-57161.

[10] Xiuli Chai et al. Hiding cipher-images generated by 2-D compressive sensing with a multi-embedding strategy [J]. Signal Processing, 2020, 171: 107525-107525.