Mathematical Modeling and Algorithm Application
ISSN: 3006-0842 | Vol. 6, No. 1, 2025

Research on Image Authentication Technology Based on Sparse Approximation and Quantum Encryption

Qing Gan[1,*], Jiale Jiang[1], Ping Yu[1], Min Liu[1], Zihao Zhao[2]

[1]School of Management Science and Engineering, Anhui University of Finance and Economics, Bengbu, China

[2]School of Finance, Anhui University of Finance and Economics, Bengbu, China

[*] **Corresponding author**: Qing Gan (Email: 3022954802@qq.com)

Abstract: This paper aims to explore and apply a novel image authentication technology that integrates Sparse Approximation (SA), Quantum Encryption (QE), and Measurement Matrix (MM) to address the issues of integrity verification, copyright protection, and tamper resistance in the transmission and storage of digital images. With the widespread adoption of digital technology, images are susceptible to unauthorized modifications, and traditional authentication techniques struggle to balance robustness, security, and processing efficiency. This paper designs a preprocessing process involving watermark quad-segmentation, transform domain DCT sparsification, and sparse coefficient exchange, employs quantum logic mapping (λ=3.9, δ=0.01) to generate the measurement matrix, and constructs a full-chain technology solution encompassing "preprocessing-encryption-dual watermark embedding-recovery-verification". Experiments are conducted based on standard test images from the USC-SIPI image database. By comparing metrics such as Peak Signal-to-Noise Ratio (PSNR), Normalized Cross-Correlation (NCC), Mean Structural Similarity Index (MSSIM), and Normalized Absolute Error (NAE), the experiments verify the superiority of this technology in resisting noise (Gaussian noise, salt-and-pepper noise), geometric attacks (rotation, scaling), and enhancement attacks (Gaussian low-pass filtering, median filtering): PSNR reaches 42.78dB and NCC is nearly 0.9999 in the absence of attacks, and NCC still maintains 0.9989 under Gaussian noise (0.01 variance). This technology provides a solution for digital image authentication that combines high security with high efficiency, and can be applied in forensic investigation, copyright protection, secure communication, and other fields. It has positive significance for the in-depth research and wide application of image authentication technology.

Keywords: Sparse Approximation; Quantum Encryption; Image Authentication; Measurement Matrix; Discrete Wavelet Transform (DWT); Dual Watermark Embedding; Robustness

1. Introduction

In the digital era of rapid development of the Internet and multimedia technology, images, as the core carrier of information dissemination, are widely used in key areas such as medical diagnosis, government documents, and e-commerce. However, the widespread use of image processing tools has significantly reduced the cost of image tampering and forgery. Unauthorized content modification, copyright piracy, and other issues occur frequently, posing serious threats to the authenticity and integrity of digital images. Therefore, there is an urgent need to develop image authentication technology that combines high security, strong robustness, and efficiency. The following image illustrates the trade-off relationship between watermark visibility (i.e., imperceptibility), robustness, and the chosen embedding strength.

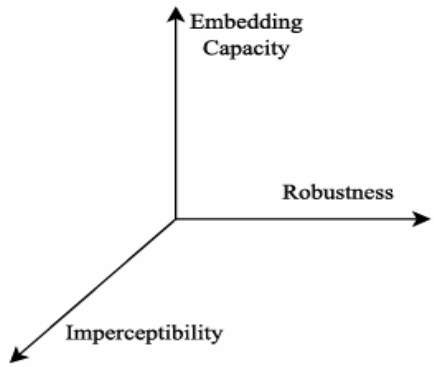

Figure 1. Trade-off between watermark visibility (i.e., imperceptibility), robustness, and chosen embedding strength

Domestic scholars have conducted numerous explorations in the fields of sparse processing and quantum encryption, laying the foundation for image authentication technology. Huang Yan [1] proposed integrating multiple linear classifiers in the model and constructing a discriminant term through data downsampling and encoding subspace mapping. This approach not only achieves sparse encoding and classifiers with strong discriminant ability but also combines decision trees to improve the encoding performance of nonlinear data, effectively reducing the model's dependence on data.

LvYanlin et al. [2] designed a new matrix decomposition method called Sparse Approximate Coding (SAC), which utilizes the LASSO solver to learn graphical basis vectors to obtain sparse vector values. Its recognition ability is significantly better than traditional matrix decomposition techniques. Chen Jie [3] focused on the fundamentals of quantum encryption technology and proposed the implementation of secure quantum key sharing between communicating parties through the transmission measurement of quantum superposition states. Combined with a symmetric encryption system with one-time pad, it can achieve unconditionally absolutely secure confidential communication. He Kaixing et al. [4] developed a fast anomaly detection algorithm based on orthogonal projection, which not only guarantees extremely high detection accuracy but also significantly improves computational efficiency, with an average running time that is over 90% shorter than the second-best algorithm across various datasets. SuJinfeng et al. [5] addressed the issues of reduced contrast, clarity, and loss of detail texture in existing infrared and visible light image fusion algorithms. They combined Robust Principal Component Analysis (RPCA), Compressive Sensing (CS), and Non-Subsampled Contourlet Transform (NSCT) to effectively optimize the image fusion effect. However, domestic research has primarily focused on the optimization and improvement of individual technologies, and has not yet achieved deep collaboration between sparse approximation and quantum encryption in image authentication scenarios.

Research abroad in the field of image security exhibits a diversified development trend, with broader technological exploration. Chen Tong et al. [6] pioneered the integration of sparse approximation and image processing, proposing a matrix sparse low-rank approximation and locality preserving model for unsupervised image feature selection. This model avoids trivial solutions by using the L2,1 norm sparse regularization of the Kronecker product of two transformation matrices in GLRAM, enhancing the accuracy of feature selection. Xiaopeng Yan et al. [7] further enriched the application of quantum encryption in the image domain. Through simulation experiments and numerical analysis verification, they found that encrypting scrambled images by first performing quantum encoding and then executing the Arnold transform, combined with the iteratively obtained M4 key matrix to complete the permutation diffusion of quantum images, can significantly improve the security of encryption methods. Xiao Dong Liu et al. [8] designed a four-dimensional chaotic quantum image encryption algorithm, fully utilizing the permutation, ergodicity, and randomness characteristics of the four-dimensional chaotic system's Arnold transform, as well as the larger key space provided by the four-dimensional Lorentz system. This algorithm addresses issues such as periodicity, small key space, and susceptibility to statistical analysis present in traditional encryption algorithms, while effectively reducing the correlation between pixels in images. Emerson Tegan H et al. [9] studied two path construction methods (based on the Euclidean geodesic of two atomic linear combinations and the 2-Waltz geodesic based on optimal transmission mapping between atoms), and proposed a path-based dictionary enhancement strategy. By learning the dictionary and structural dictionary optimization, they optimized the sparse encoding and denoising effects of the normalized dataset, reducing the amount of image data while retaining key information. Xinjia Li et al. [10] adopted binary sparse speckles instead of random speckles to implement CGI encryption, simplifying the key management process in the CGI encryption process. Zhou Nan-Run et al. [11] proposed a new multi-image encryption scheme based on the Quaternion Discrete Fractional-order Chebyshev Moment Transform (QDFrTMT) and cross-coupled chaotic systems. They cross-coupled the Logistic-sin exponential chaotic map with the piecewise linear chaotic map, obtaining the final ciphertext image through dual-layer encryption in both horizontal and vertical directions. Numerical simulation and security analysis verification showed that this algorithm has strong resistance to common attacks. Gong Li-Hua et al. [12] combined QFrOOFMMs with least squares support vector regression to design a dual-color image watermarking scheme based on geometric correction. They also proposed an image authentication method that integrates redundant discrete wavelet transform (RDWT), singular value decomposition (SVD), and Arnold scrambling techniques. SaswatiTrivedy et al. [13] developed an effective fragile watermarking scheme that can accurately locate tampered areas in digital images. Compared to other related schemes, this scheme provides better perceptual quality of the watermarked image and a lower false tamper detection rate. Gao Yuhui et al. [14] adopted parallel compressive sensing image processing methods to significantly improve image encryption efficiency. They used a subset combination of discrete data sequences generated by a two-dimensional discrete hyperchaotic system for index scrambling and forward-backward diffusion, and combined the initial key of the original image with some pixel values to generate the initial value and control parameters of the 2D-SLS chaotic sequence through SHA-512 hashing, making the algorithm robust against known plaintext and chosen plaintext attacks. Xiuli Chai et al. [15] proposed a new color image encryption scheme that generates visually meaningful ciphertext images, significantly enhancing 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, making it difficult to simultaneously meet the comprehensive requirements of image authentication for security, robustness, and processing efficiency.

In view of this, this paper aims to explore a novel image authentication technology that integrates sparse approximation (SA), quantum encryption (QE), and measurement matrix (MM), and constructs a full-chain solution of "preprocessing-encryption-dual watermark embedding –recovery -verification", to compensate for the deficiencies of existing research and provide a solution for digital image authentication that combines high security and efficiency.

2. Introduction to Image Authentication Technology

2.1. Principle and content of scarcity approximation

Sparse approximation is a powerful mathematical tool that allows us to represent complex signals, such as images, using a sparse set of coefficients derived from carefully selected bases. Quantum mechanisms, inspired by the principles of quantum physics, provide inherent properties of randomness, superposition, and entanglement, which can be utilized to

enhance encryption and verification processes. These will also be the focus of this project's research, aiming to apply the studied techniques to real-world scenarios, making them a promising solution for ensuring the authenticity, integrity, and credibility of digital images in various applications, including forensic investigations, copyright protection, and secure communication.

The main content of this technology is as follows:

Part 1: Divide the watermark image into four sub-images, and then perform sparsification processing in the transform domain. To further enhance security, transform the sparse data in the Discrete Wavelet Transform (DWT) domain and adopt a sparse coefficient exchange process.

Part 2: We generate a measurement matrix, fill its row vectors and column vectors with sequences generated by quantum logic mapping, and then perform encryption and data scrambling processing. During the encryption process, updated pixel positions are calculated based on the sparse subband coefficient exchange process. On this basis, sparse coefficient exchange between sub-images is realized.

Part 3: We generate encrypted watermarks through a series of steps including inverse sparsification, DWT, and sampling. These steps collectively enhance the algorithm's ability to resist various attacks, making it robust.

Part 4: Through experiments, we compared our scheme with a series of steganography methods, conducted a comparative analysis of various parameters of image encryption, and provided a comprehensive evaluation of the effectiveness of our proposed image authentication technology.

The technical framework integrating sparse approximation and quantum encryption mentioned above can be clearly presented through the schematic diagram of the core process, with the logical relationships and operational steps of each link shown in Figure 2.

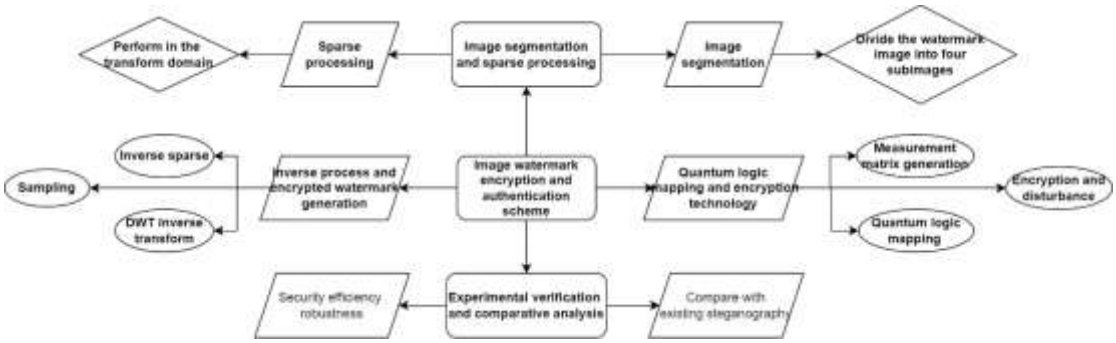

Figure 2. Schematic Diagram of the Projects's Main Content

2.2. Innovation points of image authentication technology

The image authentication technology proposed in this study has achieved multi-dimensional innovations in sub-image processing, encryption mechanisms, and watermark embedding. The specific innovations are as follows:

(1) Sub-image segmentation and sparsification. The watermark image undergoes a unique process, where it is divided into four distinct sub-images. These sub-images undergo sparsification in the transform domain, introducing an innovative strategy to enhance security.

(2) Sparse coefficient exchange process. A novel process involving sparse coefficient exchange is implemented within the discrete wavelet transform domain. This exchange mechanism introduces an innovative approach to handling watermark data, which contributes to enhancing overall security.

(3) Quantum logic mapping generated by measurement matrix. The process of generating the measurement matrix employs quantum logic mapping, which is a unique method of injecting quantum mechanical principles into watermarking. This quantum-inspired matrix construction represents a new technology for enhanced encryption.

(4) Encrypted watermark generation process. The generation of encrypted watermarks involves a series of steps such as inverse thinning, inverse DWT, and inverse sampling. This multifaceted process represents a new strategy for creating encrypted watermarks that can resist various attacks.

(5) Dual watermark embedding mechanism: Two encrypted watermarks are embedded into the host image LL2 sub-band. The singular values are modified through SVD, following the rule: "Modified LL2 sub-band singular value matrix = Host image LL2 sub-band singular value matrix + Scaling factor K (value 0.1) × Encrypted watermark LL2 sub-band singular value matrix." This provides dual security guarantees for authentication.

It is worth noting that the two-dimensional discrete wavelet transform (2D-DWT) involved in the dual watermark embedding process is a key technology for achieving frequency domain processing. Its decomposition process for images is shown in Figure 3.

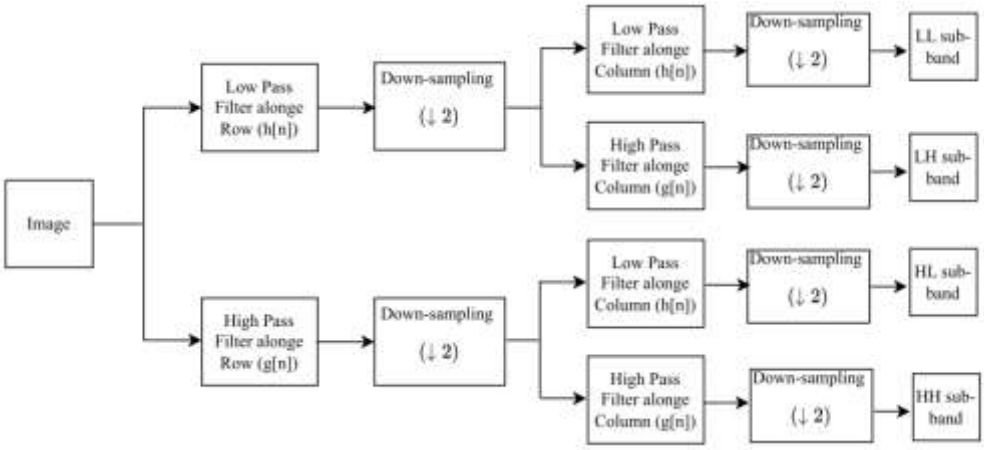

Figure 3. 2D-Discrete Wavelet Transformation on an image.

2.3. Technical route of image authentication

2.3.1. Watermark encryption

Watermark encryption is the primary step to ensure authentication security. It requires multi-step processing to achieve sparsification and quantum encryption of watermark data. The specific process is as follows:

(1) Watermark preprocessing: First, the watermark image is subsampled, and then each sub-image undergoes a Discrete Wavelet Transform (DWT). By applying wavelet transform to the four sub-sampled watermark images, their respective frequency representations can be obtained. However, the sub-bands obtained from the DWT of the watermark image are not sparse. Therefore, each sub-band involved in the next step will be thinned out block by block, and sparse coefficients will be obtained.

(2) Sparse coefficient exchange program: Different from the traditional approach of directly performing pixel exchange on images, this project performs pixel exchange on the sparse coefficients obtained in the previous step (referred to as coefficient exchange).

(3) Quantum logic mapping: By utilizing appropriate numerical values, quantum logic mapping can effectively compromise chaotic sequences and randomness.

(4) Measurement matrix design: Design the measurement matrix with the help of quantum logic mapping through a series of algorithm designs.

(5) Encrypted watermark generation: Generate an encrypted watermark to be embedded into the cover media by performing the steps of inverse sparsification, inverse DWT, and inverse sampling.

2.3.2. Watermark embedding

After completing watermark encryption, it is necessary to efficiently integrate the encrypted watermark with the host image. The watermark embedding process relies on the synergistic effect of discrete wavelet transform and singular value decomposition. The specific operational steps are as follows:

(1) Seamlessly integrate two different encrypted watermarks into the discrete frequency components of the host image or the original image. The effectiveness of this stage comes from the clever interaction of the conversion functions of the Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD).

(2) Perform two-dimensional inverse DWT on the sub-band image to obtain the modified host image with the embedded watermark.

The entire process of embedding the aforementioned watermark can be visually demonstrated through a schematic diagram, with the connection and data flow of each operational step shown in Figure 4.

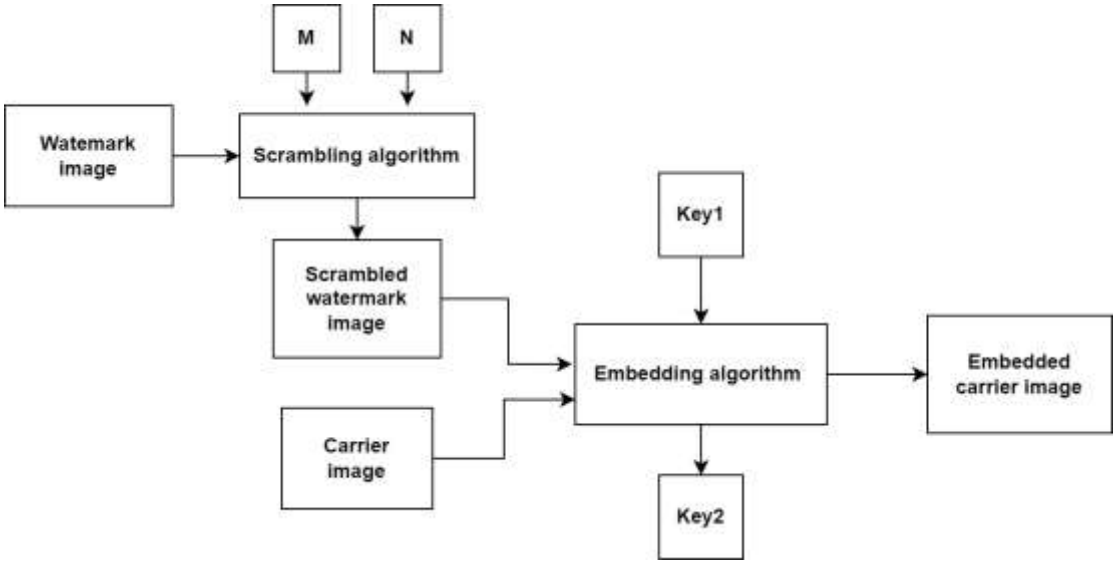

Figure 4. Schematic diagram of image watermark embedding process

2.3.3. Recovery of watermark

When verifying the integrity of an image, it is necessary to extract and recover the original watermark from the host image embedded with the watermark. This recovery process is the inverse operation of encryption and embedding. The specific steps are as follows:

(1) Encrypted Watermark Recovery: First, perform a two-dimensional DWT on the watermark image to obtain its four sub-bands. Next, obtain the matrix by performing SVD. Then, derive the singular values embedded in the watermark from the singular values of the watermark image. Finally, perform a two-dimensional inverse DWT to obtain the recovered encrypted watermark.

(2) Watermark decryption: After obtaining the encrypted recovery watermark, the decryption process is performed to obtain the original watermark data. This is the reverse of watermark encryption.

The key steps and data processing logic for watermark restoration and extraction can be clearly illustrated through a schematic diagram, with the specific process shown in Figure 5.

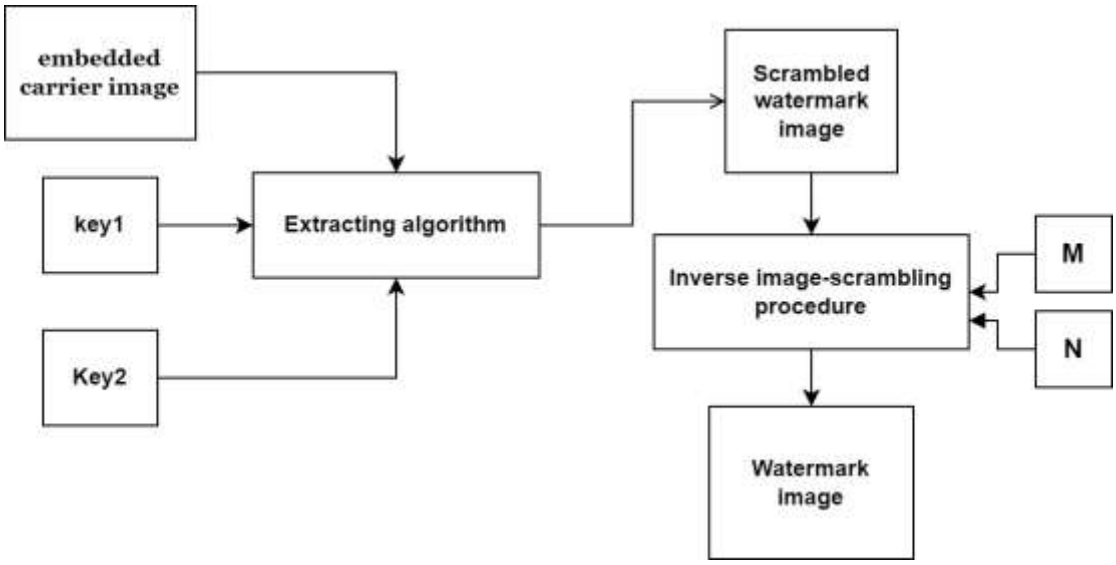

Figure 5. Schematic diagram of image extraction process

2.3.4. Verification experiment

Experiments were conducted using MATLAB on a machine, and a comprehensive evaluation index for this experiment was formed through visual assessment and comparison of numerical peak signal-to-noise ratio (PSNR), entropy, normalized cross-correlation (NCC) coefficient, mean structural similarity (MSSIM) index, and normalized absolute error (NAE). To comprehensively evaluate technical performance, a multi-dimensional evaluation index system needs to be established. The definitions and reference standards for each evaluation index are shown in Figure 6.

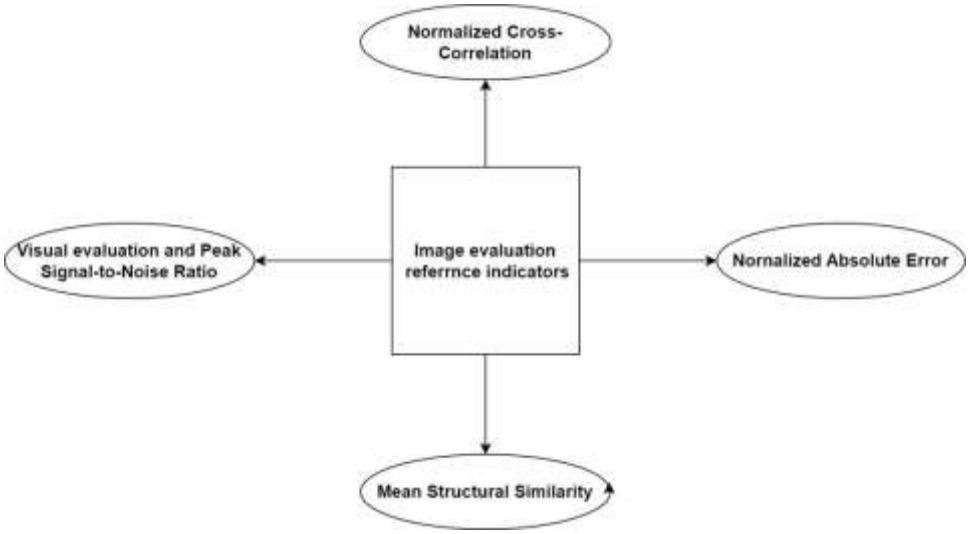

Figure 6. Schematic diagram of image evaluation reference indicators

2.4. Challenges faced by image authentication

Despite the advantages of this technology in terms of theory and scheme design, there are still numerous technical bottlenecks and unresolved challenges in the current field of image authentication, mainly including the following aspects:

(1) Large amount of data to be processed In image authentication, the amount of data to be processed is often substantial. How to reduce computational complexity and improve processing speed while ensuring sparse

approximation effect is a problem that needs to be addressed in image authentication technology.

(2) The high cost of quantum encryption machines limits their promotion in large-scale image authentication applications. How to reduce costs while maintaining the high security of quantum encryption is a challenge that image authentication technology needs to face.

(3) High computational complexity and difficulty in solving: Due to the non-convexity of the l0 norm in the mathematical model of sparse decomposition, obtaining sparse decomposition of image signals is an NP-hard problem when the dictionary is redundant. This means that in image authentication, if sparse approximation algorithms are to be used, they will face the challenges of high computational complexity and difficulty in solving.

(4) Technical maturity needs to be improved. Quantum encryption technology is currently still in the research and experimental stage, and its maturity needs to be further enhanced. How to effectively combine quantum encryption technology with existing image authentication technology to form a reliable quantum image authentication technology is a problem that image authentication technology needs to address.

(5) Establishment of an effective security evaluation system: The security evaluation of quantum image encryption requires consideration of multiple aspects, including the security at the quantum state level of quantum expression of images and the security of encryption algorithms in the quantum domain. How to establish an effective security evaluation system to ensure the security of quantum image authentication technology is a key focus for image authentication technology.

(6) Incomplete knowledge reserves and significant experimental investigation difficulties. Both domestically and internationally, there is a scarcity of applications that combine sparse approximation and quantum encryption in image authentication technology. This leads to inadequate basic knowledge reserves and hinders the conduct of experimental investigations.

3. Analysis of Problems Encountered During the Experiment

3.1. How to address the issue that spatial domain is not suitable for watermarking in scenarios where robustness, security, and capacity are highly required?

After subsampling the watermarked image, we perform a Discrete Wavelet Transform (DWT) on each sub-image. Once the preprocessing is complete, we proceed with encryption. During the image preprocessing and DWT processes, there are high requirements for our sampling process and algorithmic techniques. This issue is also one of the key points and innovations that we need to break through in this project.

3.2. In the sparse exchange procedure, how can we reduce data, better embed capacity, and enhance robustness?

Coefficient exchange is a reversible watermarking technique used to embed information into digital images while ensuring that the original image can be fully restored after watermark extraction. It carries watermark information by exchanging coefficient values in the data. In the technique proposed in this paper, we do not perform pixel exchange directly on image blocks, but on sparse coefficients (referred to as coefficient exchange) obtained in the previous step. In reversible watermarking, performing coefficient exchange on sparse coefficients rather than directly on image blocks is an interesting approach and also a major difficulty in this project's research.

3.3. In the process of watermark embedding, how can we make the watermark integrate and embed better?

This is a fundamental process that seamlessly integrates two distinct encrypted watermarks into the discrete frequency components of the host or original image. The efficacy of this stage stems from the ingenious interplay of the transformation capabilities of the Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). The initiation of this intricate procedure is marked by applying a two-dimensional Discrete Wavelet Transform to the host image. This transformative step decomposes the image into its distinct frequency components, which serves as a pivotal maneuver forming the basis for subsequent watermark integration.

3.4. How can we accurately calculate the measurement inverse matrix during the decryption process?

1) Requirements for nonsingular matrices: The effectiveness of the decryption process relies on the generated matrix being nonsingular. If the measurement matrix satisfies this criterion, it can be directly used for decryption, and its inverse can be calculated using traditional matrix inversion methods.

2) Pseudo-inverse calculation: However, if the measurement matrix happens to be singular, indicating the absence of an inverse, the pseudo-inverse calculation method is employed. This can serve as an alternative approach for handling matrices that do not meet the non-singularity conditions required for decryption.

4. Experiment and Results

4.1. Experimental Design and Dataset Introduction

4.1.1. Experimental process

This experiment revolves around "Image authentication technology based on sparse approximation and quantum encryption". The core objective is to verify the effectiveness of this technology in ensuring image authenticity and resisting malicious attacks, while comparing it with traditional image authentication methods to clarify its advantages. The specific experimental steps are as follows:

(1) Determine the experimental objective: To verify whether the image authentication technology that integrates sparse approximation, quantum encryption, and measurement matrix can maintain the integrity and extractability of the watermark in the face of common attacks (such as adding noise, image filtering, rotation, and scaling), while ensuring that the visual quality of the watermarked image is not significantly affected, and addressing the issues of "weak anti-attack capability" and "insufficient security" in traditional technologies.

(2) Design Method: Adopting a full-process scheme of "watermark preprocessing –encryption -embedding-

recovery-verification": First, the watermark image is segmented into multiple sub-images and undergoes sparsification processing in the transform domain; then, a measurement matrix is generated through quantum logic mapping to encrypt the sparse data; subsequently, with the help of Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD), the encrypted watermark is embedded into the host image; finally, the watermark is extracted through inverse operations, and by comparing with the original watermark, it is determined whether the image has been tampered with. Meanwhile, a control group (using only DWT watermark technology or only traditional encryption technology) is set up to highlight the innovativeness of this technology.

(3) Determine experimental settings and parameters: The commonly used MATLAB software is selected as the experimental tool, relying on cloud servers to ensure computational efficiency and avoid the impact of insufficient local device configuration on experimental progress. Key parameters are reasonably set according to technical requirements, such as selecting an appropriate wavelet basis function for DWT transformation, setting suitable quantum logic mapping parameters to generate chaotic sequences, using common solving tools to process sparse coefficients, and adjusting the watermark embedding strength based on the principle of "not affecting the visual effect of the host image".

(4) Conduct experimental operations and data collection: Complete the embedding and extraction training of watermarks on experimental data, adjust parameters to optimize technical effects; then simulate common attack scenarios (such as adding noise to images, processing images with filters, rotating or scaling images), collect key evaluation metric data, including metrics for measuring image quality, metrics for measuring watermark robustness, etc.

(5) Analyze and summarize the experimental results: Compare the performance of this technology with that of the control group under different attack scenarios, and analyze the enhancement effects of sparse approximation and quantum encryption on technology performance. Address the deficiencies found in the experiment (such as a slight decrease in watermark extraction effectiveness under extreme attacks), propose directions for subsequent optimization, and ultimately verify the feasibility of this technology in practical image authentication scenarios.

4.1.2. Dataset

The data for this experiment are all sourced from authoritative image databases such as UCID. Ten representative images were selected for detailed experimentation, namely Lena, Peppers, Boat, House, Lake, Stream, Living room, Mandril, Jetplane, and Cameraman. All images were resized to a uniform size: the host image (for embedding the watermark) was 512×512 pixels, and the watermark image (for authentication) was 256×256 pixels. The watermark image was further divided into 8×8 pixel blocks to accommodate the sparsification process.

Experimental key parameter settings: The scaling factor for SVD embedding is 0.1 (balancing watermark visibility and robustness), the control parameter for quantum logic mapping is 3.9, and the quantum correction term is 0.01 (considering both chaotic characteristics and randomness).

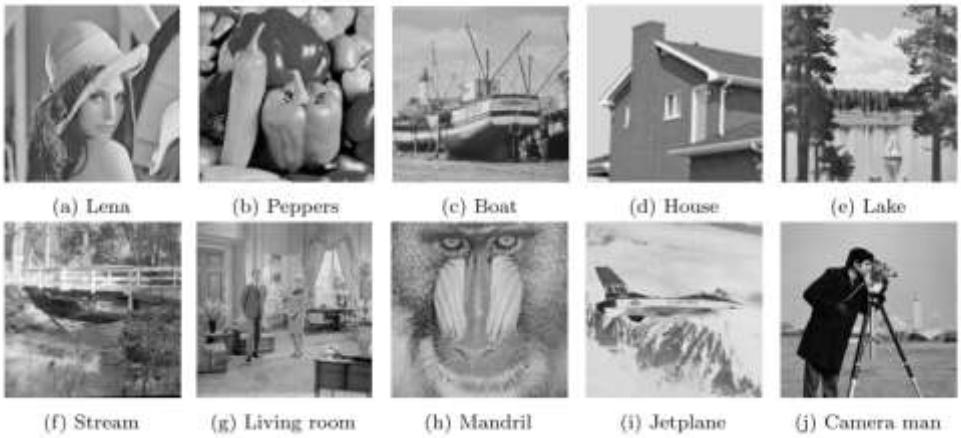

Figure 7. Test images used in our experiments

4.1.3. Core experimental process

To ensure the reproducibility and logicality of the experiment, it is necessary to clarify the core experimental process of "watermark encryption-embedding-recovery". The specific operations and data processing steps for each stage are as follows:

(1) The experiment is divided into three stages: "watermark encryption → watermark embedding → watermark recovery", with the specific process as follows:

Watermark encryption: Divide the 256×256 watermark image into four equally sized sub-images → Perform DWT decomposition on each sub-image (extracting the low-frequency LL sub-band) → Sparsify the LL sub-band block by block → Exchange sparse coefficients between sub-images through a random matrix → Generate a measurement matrix using quantum logic mapping to encrypt the sparse coefficients → Generate the final encrypted watermark through inverse sparsification, inverse DWT, and inverse sampling.

(2) Watermark embedding: Perform a 2-level DWT decomposition on the 512×512 host image (extract the low-frequency LL2 subband) → Perform an SVD decomposition on the LL2 subband → Embed the encrypted watermark into the singular value matrix of SVD → Obtain the "watermarked host image" (referred to as the "modified image") through inverse SVD and inverse DWT.;

(3) Watermark recovery: Repeat level 2 DWT and SVD decomposition on the modified image → Extract encrypted watermark → Decrypt using the measurement matrix (or pseudo-inverse if the matrix is singular) → Restore the

original watermark through inverse sparsification and inverse DWT.

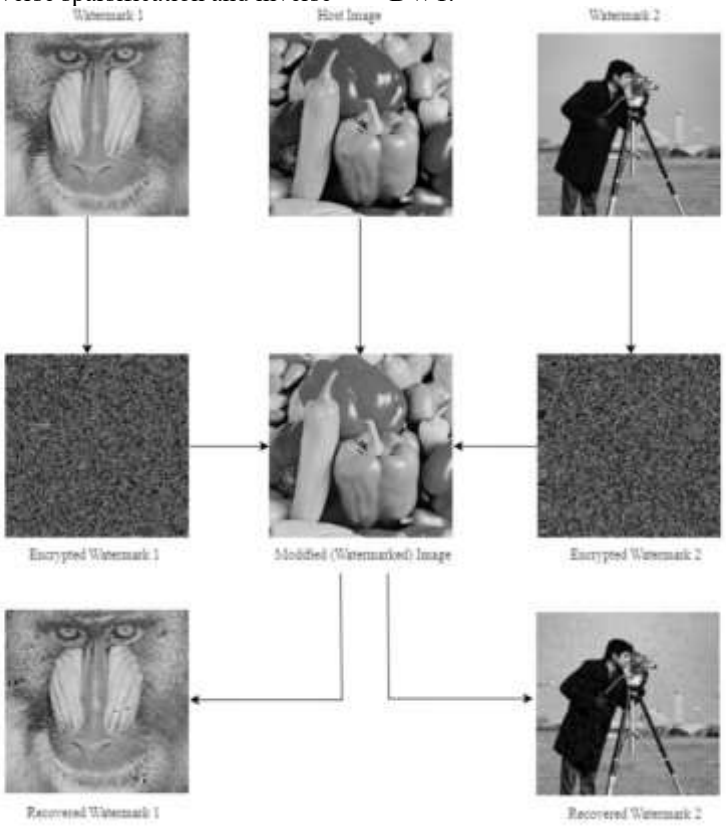

Figure 8. Example of Watermarks encryption, embedding, and recovery

4.1.4. Analysis of experimental results

(1) Imperceptibility of watermark (no visual distortion)

The imperceptibility of watermarking refers to the fact that "the visual difference between the modified image with embedded watermark and the original host image is so small that it cannot be distinguished by the naked eye". This is verified through visual assessment and PSNR metrics:

1) Visual assessment: Taking the Peppers host image as an example, after embedding both Mandril and Cameraman watermarks, the modified image's color and texture are completely consistent with the original image. Comparing the edge maps of the two (extracting image contours), there is no significant loss or distortion in edge distribution, indicating that the watermark embedding did not damage the structure of the host image.

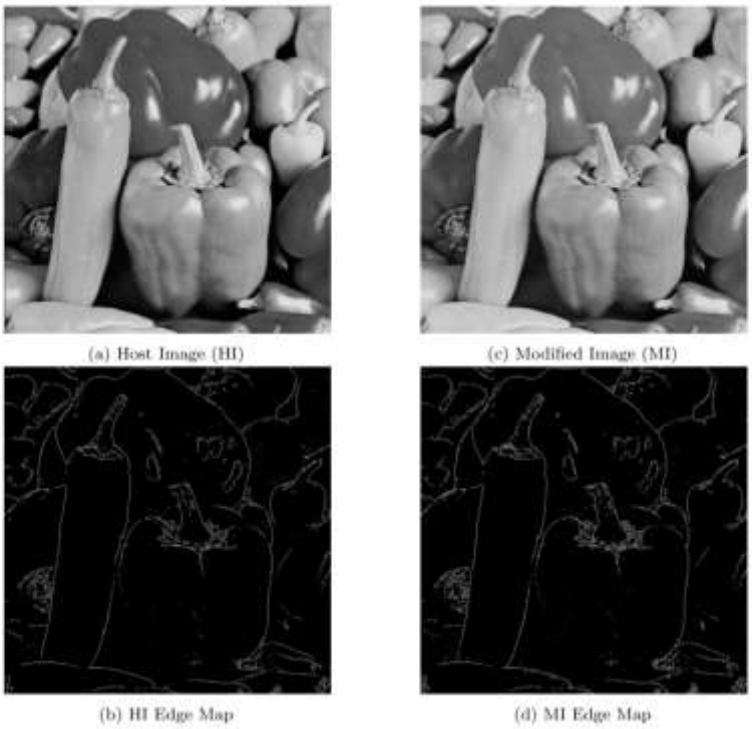

Figure 9. Visual quality analysis between 'pepper' host image (HI) and its corresponding modified Image

2) PSNR metric: The higher the PSNR, the smaller the difference between the modified image and the host image (usually PSNR≥30 dB meets the visual distortion-free requirement). In the experiment, the PSNR of 10 test images ranged from 33 to 43 dB, and the average PSNR without attack reached 42.7 dB (such as Peppers image with PSNR=42.78 dB and Lena image with PSNR=42.65 dB), far exceeding the industry standard, proving excellent watermark invisibility.

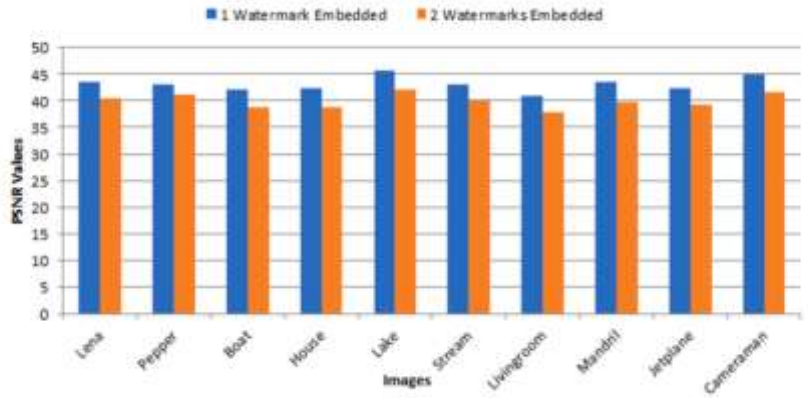

Figure 10. PSER values of the modified images with respect to their corresponding host images

(2) Robustness and security (anti-attack + anti-cracking)

Robustness refers to "accurately recovering the watermark even after the modified image is attacked"; security refers to "making it difficult for the encrypted watermark to be cracked or tampered with", 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) exhibits a "centralized" distribution, while the histogram of the encrypted watermark shows a "uniform" distribution (with pixels arranged randomly). The histogram of the decrypted watermark closely overlaps with the original watermark, indicating that encryption effectively disrupts the watermark data and decryption can fully recover it.

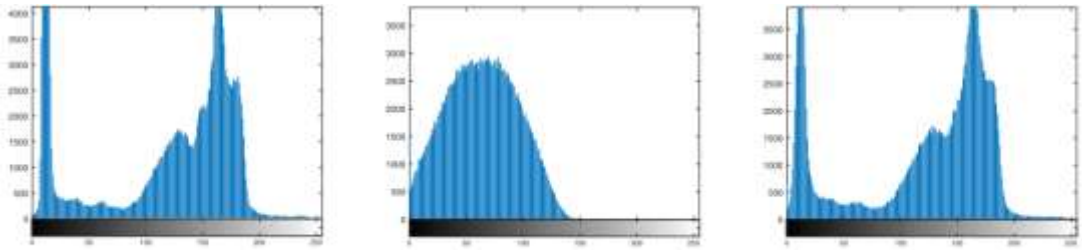

Figure 11. Histogram analysis of the watermark Image (WI, Cameraman) iamge, encrypterd image, and decrypted image

2) Correlation analysis: The pixels of the original watermark exhibit strong correlation (e.g., Mandril chart shows horizontal correlation = 0.9865, vertical correlation = 0.9367). After encryption, the pixel correlation drops to between -0.03 and 0.03 (approaching randomness), making it difficult for attackers to crack the watermark by "statistical pixel patterns", thus significantly enhancing security.

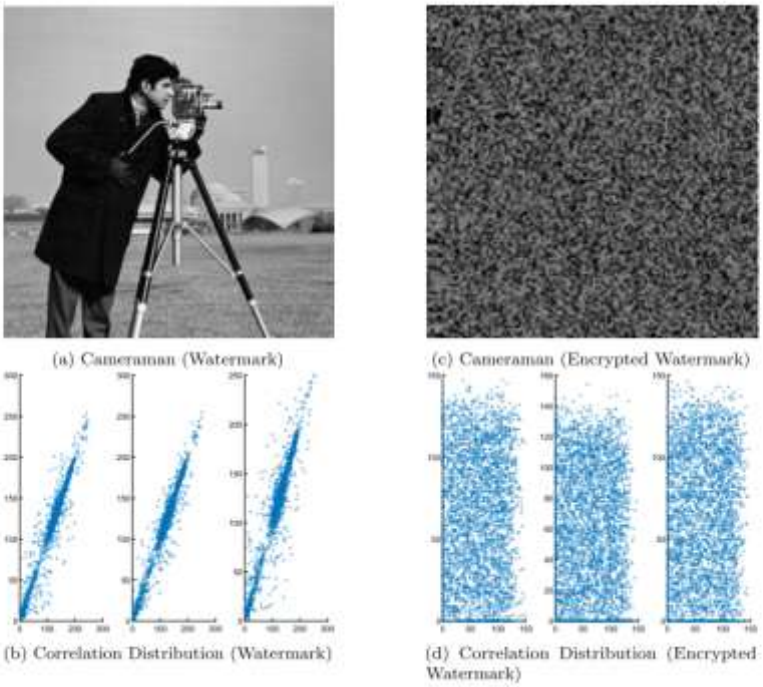

Figure 12. Correlation distribution along horizontal, vertical, and diagonal for the watermark and encrypted watermark

3) Anti-attack test: Enhancement attacks (Gaussian low-pass filtering, median filtering), noise attacks (Gaussian noise, salt-and-pepper noise, with intensity ranging from 0.01 to 0.08), and geometric attacks (10° rotation, 0.8 scaling) were applied to the modified image. The results showed that after the attacks, the PSNR remained ≥33 dB, the NCC (watermark similarity, the closer to 1 the better) was ≥0.95, the MSSIM (structural similarity) was ≥0.98, and the watermark could be clearly recovered.

4) Key Security: Only when using the "correct quantum measurement matrix" (key) can the clear watermark be recovered; if an incorrect key (such as a randomly generated measurement matrix) is used, the extracted watermark is almost a black image (with no valid information), indicating that the key is the sole key to decryption, and attackers cannot obtain the watermark through "brute force cracking".

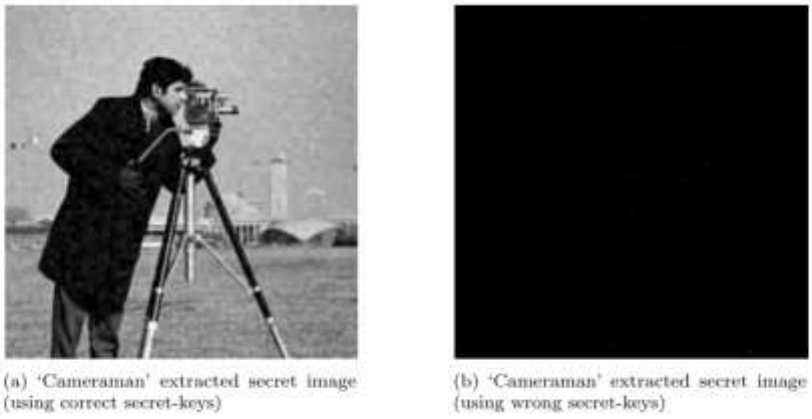

Figure 13. Visual quality analysis between the 'Camereman' recover secure watermark image using correct and wrong secret-keys (from the 'Pepper' modified image)

(3) Embedding capacity (multi-watermark storage capability)

The embedding capacity refers to the "amount of watermark data that can be carried by the host image". This method supports embedding two 256×256 encrypted watermarks in a 512×512 host image, achieving an embedding capacity of 4 bpp (4 bits of watermark data per pixel). If only one watermark is embedded, the capacity is 2 bpp, significantly surpassing traditional DWT/SVD methods (typically < 1 bpp), and can meet multi-dimensional authentication requirements such as "copyright information + traceability information".

(4) Comparison with existing technologies

Compared with four classic image authentication techniques (DCT watermarking, dual watermarking framework, sparse domain watermarking, and chaotic mapping encryption), this method has the following advantages:

1) Higher PSNR: Without attack, the PSNR of this method is higher than that of traditional DCT watermarking;

2) Stronger robustness: Under Gaussian noise (with a strength of 0.01), the NCC of this method is 0.9989, while that of the traditional dual watermarking framework is only 0.99;

3) Better security: The entropy value of the encrypted watermark (7.8~7.9 bit) is closer to 8 bit (completely random) than that of chaotic mapping encryption (7.5~7.6 bit), providing stronger resistance to statistical attacks.

5. Conclusions and Prospects

5.1. Conclusions

Through research, researchers can utilize a technology that integrates sparse approximation (SA), quantum encryption (QE), and measurement matrix (MM) to address issues related to digital image integrity assurance and copyright protection. This technology segments and sparsifies the watermark image, generates MM encryption through quantum logic mapping, and embeds the watermark by combining discrete wavelet transform (DWT) and singular value decomposition (SVD). Subsequently, the watermark can be extracted for comparison to determine whether the image has been tampered with.

This article designs an experimental process of "watermark encryption - embedding - recovery - verification": first, preprocess and sparsify the watermark image, then generate an encrypted watermark through quantum logic mapping and MM design, embed it into the host image, recover the watermark through inverse transformation, and finally evaluate the performance using MATLAB with metrics such as PSNR and NCC.

In summary, the research on this image authentication technology has formed a complete solution, which has advantages in anti-attack and security, and can support forensic investigation, copyright protection, and other scenarios. However, it still faces challenges such as large data processing volume, high cost of quantum encryption, and high computational complexity, which require further optimization.

5.2. Prospects

Image authentication technology based on sparse approximation and quantum encryption holds promising application prospects. Building upon existing solutions, further advancements can be made in terms of technical optimization, scenario adaptation, and multi-domain integration. For instance, to address the issue of high computational complexity, deep learning models can be integrated to enhance the efficiency of sparse coefficient solving. To reduce the cost of quantum encryption, a hybrid model combining quantum and classical encryption can be explored. For different scenarios, such as medical imaging and remote sensing images, a hierarchical encryption mechanism tailored for high-resolution images can be designed. Additionally, by integrating cryptography and big data technology, a multi-modal data authentication system can be researched, opening up new application scenarios such as supply chain image traceability and medical image privacy protection, thereby enhancing the practicality and applicability of the technology.

Acknowledgments

This work is supported by Anhui University of Finance and Economics National Innovation and Entrepreneurship Training Program Project (Project Number: 202410378132).

References

[1] Huang Yan. Research on Key Technologies of Structured Sparse Coding in Image Processing and Recognition [D]. South China University of Technology, 2018.

[2] Lv Yanlin, Tao Yuting, Zhang Yan. Analysis and Improvement of Image Coding Algorithm Based on Sparse Approximation [J]. Journal of Nanjing University of Science and Technology, 2020, 36(04): 18-21.

[3] Chen Jie. Applying Quantum Encryption to Ensure Information Security [J]. Information Construction, 2023(09): 63-64.

[4] He Kaixing, Jiang Zheng, Liu Bin, et al. Fast hyperspectral image anomaly detection based on orthogonal projection [J/OL]. Advances in Laser and Optoelectronics: 1-15 [2024-06-07]

[5] Su Jinfeng, Zhang Guicang, Wang Kai. Compression fusion of infrared and visible light images based on robust principal component analysis and non-subsampled contourlet transform [J]. Progress in Laser and Optoelectronics, 2020, 57(04): 84-93.

[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] Xiaopeng Yan and Lin Teng and Yining Su. A novel chaotic image encryption is based on fractional wavelet decomposition and quantum transform model[J]. Physica Scripta, 2024, 99(5):505-507.

[8] Xiao Dong Liu et al. Quantum image encryption algorithm based on four-dimensional chaos[J]. Frontiers in Physics, 2024, 12:389-412.

[9] 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.

[10] Xinjia Li et al. Computational ghost image encryption method based on sparse speckles[J]. Physica Scripta, 2024, 99(2):55-64.

[11] Zhou Nan-Run and Tong Liang-Jia and Zou Wei-Ping. Multi-image encryption scheme with quaternion discrete fractional Tchebyshev moment transform and cross-coupling operation[J]. Signal Processing, 2023, 211:91-97.

[12] Gong Li-Hua and Luo Hui-Xin. Dual color images watermarking scheme with geometric correction based on quaternion FrOOFMMs and LS-SVR[J]. Optics and Laser Technology, 2023, 167:123-124.

[13] Saswati Trivedy 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.

[14] 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.

[15] 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.