ISSN : 2455-9679
SJIF Impact Factor : 6.008

IJRTSM
INTERNATIONAL JOURNAL OF RECENT TECHNOLOGY SCIENCE & MANAGEMENT

"A REVERSIBLE AND NON-SEPARABLE ENCRYPTION SCHEME BASED OPTIMAL DATA HIDING TO IMPROVE THE SECURITY OF MEDICAL IMAGES: A LITERATURE REVIEW"

Shivani Sharma [1], Ankur Khare [2]

[1] Research Scholar, Department of Computer Science and Application, Rabindranath Tagore University, Raisen, Madhya Pradesh, India

[2] Assistant Professor, Department of Computer Science and Application, Rabindranath Tagore University, Raisen, Madhya Pradesh, India

god.chosen1@gmail.com
khareankur94@gmail.com

Corresponding Author: khareankur94@gmail.com

ABSTRACT

With the increasing reliance on digital medical imaging for diagnosis and treatment, ensuring the security and integrity of sensitive medical data has become a critical concern. Traditional encryption methods provide confidentiality but often compromise the usability of images for medical analysis. To address this issue, Reversible Data Hiding (RDH) and Non-Separable Encryption (NSE) have emerged as promising solutions, allowing secure image transmission while maintaining the capability for lossless recovery. This review paper explores the latest advancements in reversible and non-separable encryption-based optimal data hiding techniques, focusing on their role in enhancing medical image security. This study provides a comprehensive analysis of various encryption and data hiding methodologies, including histogram shifting, difference expansion, and deep learning-assisted techniques. It evaluates their effectiveness in terms of security, imperceptibility, embedding capacity, and computational complexity. The paper also discusses current challenges such as trade-offs between robustness and reversibility, real-time processing limitations, and the impact of encryption on medical image quality. By synthesizing recent research, this review aims to bridge the gap between encryption and data hiding techniques, offering insights into designing optimal security frameworks for medical imaging. Future research directions are suggested, including AI-driven encryption models, blockchain-integrated medical data protection, and lightweight RDH techniques for real-world healthcare applications.

Keywords: *Reversible Data Hiding, Non-Separable Encryption, Blockchain, Confidentiality, Lossless Recovery, Complexity.*

I. INTRODUCTION

Medical imaging has become an integral part of modern healthcare, facilitating diagnosis, treatment planning, and telemedicine applications. However, with the increasing digitization of medical records and images, the threat of cyberattacks, unauthorized access, and data breaches has also grown. Conventional encryption techniques such as AES, RSA, and DES ensure data confidentiality but fail to support medical image usability, which is crucial for accurate diagnosis and analysis [4, 8].

To address this limitation, Reversible Data Hiding (RDH) and Non-Separable Encryption (NSE) have been proposed as

ISSN : 2455-9679
SJIF Impact Factor : 6.008

advanced techniques to provide both security and lossless recovery of encrypted medical images. RDH allows data to be embedded into images while ensuring exact reconstruction after decryption, making it highly suitable for applications where image fidelity is paramount. NSE further enhances security by preventing the separation of the original image and the hidden data, ensuring end-to-end integrity [12, 24].

Medical images such as X-rays, MRIs, CT scans, and ultrasound images contain highly sensitive patient information that, if compromised, could lead to privacy violations, identity theft, and fraud. Existing security measures focus primarily on encryption, but they often introduce distortions that hinder image processing and analysis. An ideal solution should:

- Ensure robust encryption without affecting the diagnostic quality of images [5].
- Enable reversible data hiding for embedding metadata, authentication signatures, or additional security information [7].
- Resist cyber threats such as brute-force attacks, watermarking removal, and unauthorized decryption.
- Support real-time transmission and processing in telemedicine and cloud-based healthcare systems [11].

This paper aims to provide a detailed review of state-of-the-art encryption and optimal data hiding techniques for medical image security. The key areas of focus include:

- Reversible Data Hiding (RDH) Methods – Techniques such as histogram shifting, difference expansion, prediction-error expansion, and deep learning-based approaches.
- Non-Separable Encryption (NSE) Techniques – Secure encryption schemes that prevent the separation of hidden data and encrypted medical images.
- Performance Metrics & Evaluation – Analysis of security strength, imperceptibility, embedding capacity, computational efficiency, and robustness.
- Current Challenges & Open Issues – Limitations in existing techniques, including trade-offs between embedding rate and reversibility, real-time processing constraints, and encryption vulnerabilities.
- Future Research Directions – Exploration of AI-driven security models, blockchain-integrated medical data protection, and lightweight encryption techniques for resource-constrained healthcare environments.

This review aims to provide valuable insights for researchers and practitioners looking to enhance medical image security while maintaining diagnostic integrity. By bridging the gap between encryption and data hiding, it paves the way for more secure, efficient, and privacy-preserving medical image transmission systems.

II. Literature Review

Y. C. Lin [1] proposes a reversible data hiding technique optimized for progressive image transmission. The method enables the embedding and retrieval of hidden information while allowing partial image reconstruction during transmission. The approach enhances data security and image quality in communication systems. Experimental evaluations confirm its effectiveness in preserving image integrity and minimizing transmission overhead, making it suitable for bandwidth-constrained applications. X. Zhang [2] introduces a separable reversible data hiding scheme for encrypted images. The proposed method enables data extraction and image restoration without requiring decryption. It supports multiple access levels, allowing data recovery by different parties without compromising security. The technique is particularly useful for cloud storage and privacy-preserving applications. Experimental results demonstrate its efficiency in maintaining high embedding capacity and low distortion.

V. Suresh et al. [3] proposes a separable reversible data hiding scheme using the RC4 algorithm. The method enhances security by encrypting the embedded data while ensuring lossless recovery of the original image. The approach is tested for robustness against various attacks, including noise addition and compression. Experimental results validate its effectiveness in maintaining high security and imperceptibility, making it suitable for secure communication applications. R. Jose et al. [4] introduces an improved separable reversible data hiding scheme for encrypted images.

ISSN : 2455-9679
SJIF Impact Factor : 6.008

The proposed approach enhances embedding capacity and retrieval accuracy while maintaining high security. The method ensures that data extraction and image restoration can be performed independently. Experimental analysis confirms its superiority over existing schemes in terms of robustness and efficiency.

A. M. Abdirashid et al. [5] proposes a frequency domain-based image steganography method for secure data hiding. The approach utilizes transform domain techniques to achieve imperceptible embedding while ensuring robustness against various attacks. The paper evaluates the method's performance in terms of security, capacity, and imperceptibility, making it a promising solution for covert communication. F. Cao et al. [6] introduces a separable reversible data hiding method for encrypted VQ-encoded images. The proposed scheme allows independent extraction of hidden data and image recovery, enhancing security and flexibility. The technique is tested against various compression scenarios, demonstrating its efficiency in secure image transmission applications.

D. Xu et al. [7] proposes a reversible data hiding method based on two-dimensional histogram modification. The technique enhances embedding capacity while preserving image quality. It is evaluated for robustness against attacks and distortions, proving effective in secure data communication and image processing applications. P. Rashmi et al. [8] introduces an enhanced Lorenz-chaotic encryption method for partial medical image encryption and data hiding in big data healthcare. The technique ensures high security and robustness while enabling reversible data extraction. The proposed approach is evaluated for its effectiveness in protecting medical records, demonstrating superior security and imperceptibility.

K. Y. Ng et al. [9] explores a scrambling embedding technique for partially encrypted images. The method enhances security by applying scrambling operations before embedding data. It ensures that the original image remains protected while maintaining a balance between embedding capacity and perceptual quality. Experimental results validate its robustness against attacks. R. Motomura et al. [11] introduces a reversible data hiding technique using prediction error expansion in compressible encrypted images. The approach balances high embedding capacity with minimal visual distortion, making it suitable for secure image storage and transmission. The method is tested under various compression rates, proving its efficiency in maintaining data integrity.

H. Ye et al. [12] explores an image steganography method using interpolation and difference histogram shifting. The proposed approach enhances embedding efficiency and security while preserving image quality. The study evaluates its performance against state-of-the-art techniques, demonstrating its suitability for secure multimedia applications. G. Wibisono et al. [13] presents a hybrid reversible data hiding method for encrypted satellite images using fluctuation modification extraction and Reed-Solomon code embedding. The technique enhances robustness against noise and compression artifacts while ensuring accurate data recovery. The method is validated through extensive experimental analysis, proving its effectiveness in remote sensing applications.

Z. Hua et al. [14] introduces a reversible data hiding scheme using cipher feedback secret sharing. The approach enhances data security by integrating encryption with reversible embedding techniques. The method is evaluated for its resilience against attacks and its ability to support secure multimedia transmission. C. Yu et al. [15] proposes a hierarchical embedding scheme for reversible data hiding in encrypted images. The technique supports multi-level access control while preserving the original image quality. The study demonstrates its efficiency in secure cloud storage and multimedia protection applications.

F. Ren et al. [16] introduces an interpolation and histogram shift-based reversible information hiding scheme for medical images. The approach ensures lossless image recovery while enabling secure data embedding. Experimental evaluations confirm its effectiveness in medical image security and telemedicine applications. J. S. Pan et al. [17] presents an information hiding method based on a two-level mechanism and lookup table approach. The technique enhances security and embedding efficiency, making it suitable for digital watermarking and data authentication applications. The method is tested under various conditions, proving its robustness and flexibility.

F. Ren et al. [18] (2025) propose a reversible data hiding and authentication scheme for encrypted images that leverages prediction error compression (PEC). The method enables secure embedding of secret information while preserving the reversibility of the image. By integrating image authentication and PEC, the scheme not only hides data efficiently but also ensures integrity verification, making it suitable for secure multimedia communication and cloud storage systems. X. Zhang et al. [19] (2024) present an advanced reversible data hiding technique for encrypted images

ISSN : 2455-9679
SJIF Impact Factor : 6.008

using asymmetric coding and bit-plane block compression. This novel approach focuses on increasing data hiding capacity while minimizing distortion. The technique leverages the redundancy in encrypted bit-planes and uses a layered compression framework, ensuring a balance between high payload and lossless recovery, which is essential in privacy-preserving image sharing.

R. Martyniak and M. Dzwonkowski [20] (2025) introduce a reversible data hiding method that combines pixel prediction with ERLE (Extended Run-Length Encoding) compression. Designed for encrypted images, the method enhances embedding capacity by accurately predicting pixel values and compressing the prediction errors. This hybrid technique ensures full image recovery post decryption and embedding extraction, making it suitable for secure and reversible multimedia processing. F. Ren et al. [21] (2024) develop a dual-purpose data hiding and authentication scheme specifically for medical images, utilizing a double POB (Position and Offset Block) mechanism. The scheme supports both authentication and lossless data embedding within encrypted medical images, preserving diagnostic quality. It demonstrates strong applicability in telemedicine and cloud-based medical imaging systems, where security and data integrity are critical.

C. Y. Weng et al. [22] (2024) propose a high payload data hiding scheme based on image interpolation and histogram shifting. This method enables embedding of large quantities of data while maintaining image quality and reversibility. The algorithm adapts well to both low and high-resolution images and is particularly effective in scenarios requiring covert communication or digital watermarking. R. Sihwali and D. Ibrahim [23] (2025) present a new image encryption method using an optimized smart codebook that dynamically encodes image blocks. The approach increases encryption efficiency and reduces redundancy by adapting to image content patterns. This method enhances image protection against cryptanalytic attacks, making it suitable for secure transmission in emerging tech environments like IoT and smart surveillance.

J. Kolangiappan [24] (2024) introduces a secure reversible image data hiding approach operating directly in the encrypted domain using key modulation. This technique modifies encrypted pixels based on key patterns, allowing reversible embedding without prior decryption. It ensures both data confidentiality and recoverability, which is crucial for privacy-preserving applications such as cloud storage or secure photo sharing. F. Yan et al. [25] (2024) provide a comprehensive review of quantum-enabled algorithms in medical image processing. The paper surveys quantum techniques for tasks like image segmentation, enhancement, and classification. The authors highlight the significant computational advantages and security potentials offered by quantum computing in handling large-scale, sensitive medical datasets, and discuss future directions and open challenges in the intersection of quantum AI and healthcare imaging.

Here's a structured table 1 with the requested details:

Table 1 Comparative Analysis

Paper	Proposed Methodology	Performance Parameters	Advantages	Limitations
Y. C. Lin (2011) [1]	Progressive image transmission with reversible data hiding	Embedding rate, quality, computational complexity	Enables stepwise transmission with security	Increased complexity in progressive extraction
X. Zhang (2012) [2]	Separable reversible data hiding in encrypted images	Reversibility, capacity, security	Ensures separability, high embedding rate	Increased computational complexity
V. Suresh et al. (2013) [3]	RC4-based separable reversible data hiding	Security, capacity, key sensitivity	Strong encryption with lossless recovery	Key dependency, encryption overhead
R. Jose et al. (2013) [4]	Improved separable reversible data hiding	Capacity, PSNR, security	Higher security & embedding rate	Trade-off between security & efficiency

ISSN : 2455-9679
SJIF Impact Factor : 6.008

Paper	Proposed Methodology	Performance Parameters	Advantages	Limitations
A.M. Abdirashid et al. (2022) [5]	Frequency domain image steganography	Capacity, robustness	Strong security for frequency-based hiding	Susceptible to frequency domain attacks
F. Cao et al. (2022) [6]	VQ-encoded image data hiding	PSNR, security, reversibility	Effective for vector quantized images	Computationally expensive
D. Xu et al. (2018) [7]	2D histogram modification for separable data hiding	Capacity, imperceptibility	High capacity & minimal distortion	Increased processing time
P. Rashmi et al. (2022) [8]	Lorenz-chaotic encryption for medical images	Encryption strength, PSNR	Secure against brute force attacks	Computational complexity
K. Y. Ng et al. (2022) [9]	Scrambling embedding in partially encrypted images	Robustness, security	Improved security for partially encrypted images	Decryption complexity
H. Y. Chen et al. (2022) [10]	2D histogram shifting for JPEG images	PSNR, capacity	Higher embedding rate for JPEG images	Sensitive to lossy compression
R. Motomura et al. (2022) [11]	Prediction error expansion for compressible encrypted images	Embedding capacity, PSNR	Lossless data recovery	Limited to compressible images
H. Ye et al. (2021) [12]	Image interpolation & difference histogram shift	Image quality, security	High security with interpolation techniques	Increased computational load
G. Wibisono et al. (2020) [13]	Hybrid RDH in satellite images	Capacity, robustness	Effective for satellite imagery protection	Processing-intensive
Z. Hua et al. (2022) [14]	Cipher feedback secret sharing for encrypted images	Security, reversibility	Enhanced protection for encrypted images	Key management challenges
C. Yu et al. (2022) [15]	Hierarchical embedding for encrypted images	Capacity, robustness	Multi-level embedding with high security	Complexity in implementation
F. Ren et al. (2023) [16]	Interpolation & histogram shift for medical images	PSNR, imperceptibility	High fidelity and secure embedding	Processing overhead
J S. Pan et al. (2022) [17]	Two-level hiding & lookup table approach	Capacity, robustness	Enhanced security and storage efficiency	Requires large lookup tables
F. Ren et al., (2025) [18]	Reversible data hiding using Prediction Error Compression (PEC) with image authentication	Embedding capacity, PSNR, authentication accuracy	High reversibility, combined security & integrity, suitable for encrypted images	Compression-dependent, complexity may rise with high-resolution images
X. Zhang et al., (2024) [19]	Reversible data hiding using Asymmetric Coding +	Payload (bits), PSNR, Bit Error	High hiding capacity, bit-level efficiency,	Complex implementation,

ISSN : 2455-9679
SJIF Impact Factor : 6.008

Paper	Proposed Methodology	Performance Parameters	Advantages	Limitations
	Bit-Plane Block Compression	Rate	good visual quality	encryption format sensitive
R. Martyniak et al. (2025) [20]	Pixel Prediction and ERLE Compression in encrypted images	PSNR, Embedding Rate, Recovery Accuracy	Lossless recovery, lightweight compression, simple prediction model	Limited capacity in textured regions, prediction errors may reduce performance
F. Ren et al., (2024) [21]	Dual-purpose scheme for medical images using Double Position-Offset Block (POB)	PSNR, authentication accuracy, embedding capacity	Preserves medical image quality, dual functionality (authentication + hiding)	Medical format-specific, may require tuning for different modalities
C. Y. Weng et al., (2024) [22]	High-capacity hiding using Interpolation and Histogram Shifting	Payload, PSNR, histogram distortion	High payload, flexible for different image types, easy to implement	Sensitive to histogram changes, may reduce robustness under compression
R. Sihwali et al., (2025) [23]	Image encryption using Optimized Smart Codebook for block-based dynamic encoding	Encryption time, entropy, key space, robustness	Enhanced encryption strength, adaptive to image features	Codebook generation may be computationally expensive
J. Kolangiappan, (2024) [24]	Secure reversible data hiding using Key Modulation in Encrypted Domain	Embedding capacity, reversibility rate, PSNR	No decryption needed, suitable for cloud-based use, high security	Modulation scheme complexity, encryption scheme dependent
F. Yan et al., (2024) [25]	Review of quantum-enabled medical image processing methods (segmentation, classification)	Coverage breadth, algorithm complexity, computation cost	Highlights quantum speed-up and security, comprehensive	Theoretical focus, lacks practical validation in real-world medical systems

This table 1 provides a comprehensive comparative analysis of various research papers focusing on reversible data hiding and encryption techniques for image security.

Here are some research gaps identified from the above research papers related to reversible data hiding (RDH) and encryption techniques for image security:

1. Limited Embedding Capacity

Many existing techniques, such as histogram shifting and difference expansion, suffer from low data embedding capacity. There is a need for optimized algorithms that can embed more data while maintaining imperceptibility.

2. Trade-off Between Security and Reversibility

Approaches like RC4-based separable RDH [3] and Lorenz-chaotic encryption [8] focus on security but introduce challenges in maintaining fully reversible data recovery. Developing hybrid techniques that balance encryption strength and reversibility is necessary.

3. Computational Complexity and Processing Overhead

ISSN : 2455-9679
SJIF Impact Factor : 6.008

Methods like 2D histogram modification [7] and prediction error expansion [11] require high computational resources, making them inefficient for real-time applications. Optimization is needed to improve processing speed and energy efficiency.

4. Vulnerability to Image Compression and Transmission Distortions

   Approaches such as lossless LSB embedding and transcoding robust data hiding lack robustness when dealing with lossy compression (JPEG) and noise during transmission. More resilient techniques should be developed to ensure data integrity in real-world networks.

5. Lack of Standardized Datasets for Evaluation

   Many studies [5, 6] use limited, custom datasets, making it difficult to compare performance across different methods. A benchmark dataset and evaluation framework for RDH in encrypted images would enhance reproducibility.

6. Inadequate Adaptation for Medical Images

   While many researchers [8, 16] propose solutions for medical image encryption and data hiding, many existing methods are not optimized for DICOM images, CT scans, and MRI data. More research is needed to adapt RDH techniques for medical applications while preserving diagnostic quality.

7. Security Risks in Key Management and Encryption

   Techniques such as cipher feedback secret sharing [14] and hierarchical embedding [15] rely on encryption keys, but key management and secure key exchange mechanisms remain underexplored. More robust cryptographic protocols should be integrated.

8. Limited Real-World Deployment and Practical Implementations

   Most studies focus on theoretical models with little real-world validation. Approaches like scrambling embedding [9] and hybrid RDH for satellite images [13] need to be tested in real-world scenarios, such as telemedicine and secure cloud storage.

9. Lack of AI and Deep Learning Integration

   Few works explore machine learning and AI-based optimization for RDH. Leveraging deep learning (CNNs, GANs) for adaptive data hiding and extraction could significantly enhance performance in complex images and dynamic environments.

10. Inefficient Reversibility in High-Resolution and Colour Images

    Many existing RDH schemes [1, 2] perform well on grayscale images but struggle with high-resolution and colour images due to increased complexity. Further research is needed to extend RDH techniques for high-resolution multimedia applications.

V. CONCLUSIONS

The rapid evolution of reversible and non-separable encryption schemes for optimal data hiding has significantly contributed to enhancing medical image security. This review has highlighted the strengths and limitations of existing methodologies, emphasizing the need for improved embedding capacity, computational efficiency, robustness, and real-world applicability. While traditional histogram shifting, difference expansion, and separable reversible data hiding techniques have laid a strong foundation, the integration of AI-driven optimization, blockchain-based key management, and quantum cryptography presents promising directions for future advancements.

By addressing critical challenges such as dataset standardization, real-time processing, and high-resolution image security, researchers can develop more scalable, secure, and efficient encryption-based data hiding techniques. Furthermore, the fusion of cloud computing, IoT, and deep learning-driven RDH mechanisms will ensure secure transmission and storage of sensitive medical data. This study provides a structured roadmap for advancing the field,

ISSN : 2455-9679
SJIF Impact Factor : 6.008

with a strong focus on enhancing security, improving imperceptibility, and ensuring full reversibility—ultimately contributing to better healthcare data protection and privacy.

REFERENCES

1. Y. C. Lin, "Reversible data hiding for progressive image transmission", Signal Processing: Image Communication, vol. 26(10), pp. 628–645, 2011.
2. X. Zhang, "Separable reversible data hiding in encrypted image", IEEE Transactions Information Forensics and Security, Vol. 7(2), pp. 826–832, 2012.
3. V. Suresh, C. Saraswathy," Separable Reversible Data Hiding Using Rc4 Algorithm" IEEE International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME) pp. 164-168, 2013.
4. R. Jose, Gincy Abraham, "Separable Reversible Data Hiding in Encrypted Image with Improved Performance", IEEE International Conference on Microelectronics, Communication and Renewable Energy, pp. 01-05, 2013.
5. A. M. Abdirashid, S. Solak and Aditya Kumar Sahu, "Data Hiding based on Frequency Domain Image Steganography", European Journal of Science and Technology, pp. 71-76, 2022.
6. F. Cao, Y. Fu, H. Y. M. Bot Mian Zou, Jian Li and Chuan Qin, "Separable Reversible Data Hiding in Encrypted VQ-Encoded Images", Security and Communication Network, Wiley Hindawi, Volume 2022, pp. 1-16, 2022.
7. D. Xu, K. Chen, R. Wang and S. Su, "Separable Reversible Data Hiding in Encrypted Images based on Two-Dimensional Histogram Modification", Security and Communication Networks, Wiley Hindawi, Volume 2018, pp. 1-14, 2018.
8. P. Rashmi, M. C. Supriya and Qiaozhi Hua, "Enhanced Lorenz-Chaotic Encryption Method for Partial Medical Image Encryption and Data Hiding in Big Data Healthcare", Security and Communication Networks, Wiley Hindawi, Vol. 2022, pp. 1-9, 2022.
9. K. Y. Ng and S. Ong, "Scrambling Embedding in Partially Encrypted Images", Proceedings of APSIPA Annual Summit and Conference, Chiang Mai, Thailand, pp. 1-6, 2022.
10. H. Y. Chen, Y. Zhou, Y. Wang and Y. Chen, "A Novel Two Dimensional Reversible Data Hiding Scheme based on High Efficiency Histogram Shifting for JPEG Images", International Journal of Distributed Sensor Networks, Vol. 18(3), pp. 1-14, 2022.
11. R. Motomura, S. Imaizumi and H. Kiya, "A Reversible Data Hiding Method with Prediction Error Expansion in Compressible Encrypted Images", Applied Sciences, MDPI, Vol. 12(9418), pp. 1-18, 2022.
12. H. Ye, K. Su, X. Cheng and S. Huang, "Research on Reversible Image Steganography of Encrypted Image based on Image Interpolation and Difference Histogram Shift", IET Image Processing, Wiley, pp. 1-14, 2021.
13. G. Wibisono, A. Syahputra Nasution, Firmansyah and Anton Satria Prabuwono, "Hybrid Reversible Data Hiding in Encrypted Satellite Images using Fluctuation Modification Extraction and Reed Solomon Code Embedding", IEEE Access, pp. 1-18, 2020.
14. Z. Hua, Y. Wang, S. Yi, Yicong Zhou and Xiaohua Jia, "Reversible Data Hiding in Encrypted Images using Cipher Feedback Secret Sharing", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 32 (8), pp. 4968-4982, 2022.
15. C. Yu, X. Zhang, X. Zhang, G. Li and Z. Tang, "Reversible Data Hiding with Hierarchical Embedding for Encrypted Images", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 32 (2), pp. 451-466, 2022.
16. F. Ren, Y. Liu, X. Zhang and Qiang Li, "Reversible Information Hiding Scheme based on Interpolation and Histogram Shift for Medical Images", Multimedia Tools and Applications, pp. 1-27, 2023.
17. J. S. Pan, X. X. Sun, H. Yang, Vaclav Snasel and Shu Chuan Chu, "Information Hiding based on Two Level Mechanism and Look Up Table Approach", Symmetry, MDPI, Vol. 14 (315), pp. 1-17, 2022.
18. F. Ren, Z. Zhang, K. Jiang, P. Zhang and T. Yang, "Reversible Data Hiding and Authentication Scheme for Encrypted Image based on Prediction Error Compression", Scientific Reports, Vol. 15 (11636), pp. 1-14, 2025.

ISSN : 2455-9679
SJIF Impact Factor : 6.008

19. X. Zhang, F. He, C. Yu, C. N. Yang and Z. Tang, "Reversible Data Hiding in Encrypted Images with Asymmetric Coding and Bit-Plane Block Compression", IEEE Transactions on Multimedia, Vol. 26, pp. 10174-10188, 2024.
20. R. Martyniak, and M. Dzwonkowski, "Reversible Data Hiding in Encrypted Images with Pixel Prediction and ERLE Compression", Computational Science, ICCS, Lecture Notes in Computer Science, Vol. 15906, Springer, Cham, pp. 1-8, 2025.
21. F. Ren, X. Shi, E. Tang and M. Zeng, "Data Hiding and Authentication Scheme for Medical Images using Double POB", Applied Sciences, MDPI, Vol. 14 (2664), pp. 1-21, 2024.
22. C. Y. Weng, H. Y. Weng, N. S. Shongwe and C. T. Huang, "High Payload Data Hiding Scheme based on Interpolation and Histogram Shifting", Electronics, MDPI, Vol. 13 (738), pp. 1-17, 2024.
23. R. Sihwali and D. Ibrahim, "A New Image Encryption Method using an Optimized Smart Codebook", Wiley Human Behavior and Emerging Technologies, Vol. 2025, pp. 1-15, 2025.
24. J. Kolangiappan,"Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation", International Journal of Trend in Research and Development, pp. 1-4, 2024.
25. F. Yan, H. Huang, W. Pedrycz and K. Hirota, "Review of Medical Image Processing using Quantum enabled Algorithms", Artificial Intelligence Review, Vol. 57 (300), pp.1-52, 2024.