International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

SECURE MEDICAL IMAGE SHARING TECHNOLOGIES WATERMARKING INSIGHTS AND OPEN ISSUES

[1] Ms. Durgabhavani Battu,[2] P. Chakrika,[3] Pallavi,[4] Rachitha
[1] *Assistant Professor, Department of CSE (Cyber Security), School of CSE, Malla Reddy Engineering*
[2,3,4] *Students, Department of Computer Science & Engineering(IOT), School of CSE , Malla Reddy Engineering college for women , Hyderabad, India.*

ABSTRACT:
With the growth of the Internet, medical documents have become widely used by healthcare professionals. Secure transmission and management of medical images are essential to enable collaboration while protecting sensitive patient information. This study analyzes various methods for safe medical data sharing, highlighting their advantages and limitations We categorize these approaches into centralized techniques, such as encryption and watermarking, and distributed methods, such as blockchain and federated learning. Additionally, this research examines the evolution of medical image watermarking techniques, from traditional methods to advanced AI-based systems. While traditional techniques known as white boxes are simple and interpretable, deep learning models are considered black boxes, offering greater robustness and adaptability. This analysis emphasizes the need to integrate modern technology to address the growing complexity of threats, while preserving the diagnostic integrity of medical images. Furthermore, our work provides a comprehensive classification of watermarking methods and outlines future research directions, contributing to the ongoing discourse on enhancing data security in medical imaging

Keywords: Medical Image Security; Watermarking Techniques; Encryption; Blockchain; Federated Learning; Deep Learning; Data Privacy; Diagnostic Integrity; Secure Healthcare Systems; AI-Based Watermarking; Medical Data Sharing.

Received: 05-10-2025 Accepted: 14-11-2025 Published: 22-11-2025

I. INTRODUCTION

The rapid digital transformation of healthcare systems, supported by technologies such as cloud computing, telemedicine, and electronic health records (EHR), has significantly increased the demand for reliable and secure sharing of medical images across various clinical environments. Medical imaging modalities like MRI, CT, X-ray, and ultrasound generate highly sensitive and diagnostic-critical data that must be transmitted among hospitals, physicians, diagnostic centers, insurance providers, and research institutions. However, this widespread accessibility also introduces substantial security concerns, including unauthorized access, data manipulation, privacy violations, and loss of ownership rights.To address these challenges, digital watermarking has emerged as a robust security technique for safeguarding medical imagery during storage and transmission. Unlike traditional cryptographic approaches that only protect data during communication, watermarking ensures persistent protection by embedding authentication information directly into the medical image. This embedded watermark may contain patient identification details, hospital credentials, copyright information, or tamper-detection codes that help verify integrity and authenticity even after the file is accessed or distributed. Medical image watermarking must adhere to stringent performance constraints, as the diagnostic content—specifically the Region of Interest (ROI)—cannot be distorted or impacted in any way that may alter

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

clinical interpretation. Therefore, recent research has focused on reversible and ROI-based watermarking techniques, enabling the exact recovery of original images after verification. Integration of watermarking with advanced technologies such as blockchain, homomorphic encryption, and federated healthcare networks further enhances trust, traceability, and compliance with regulatory frameworks like HIPAA and GDPR.

Despite these advancements, several open issues remain, including robustness against emerging cyber threats, limited payload capacity, computational overhead in real-time clinical workflows, and maintaining consistent standards for interoperability. Therefore, a comprehensive study of watermarking technologies and their implications in secure medical image sharing is essential to support the future of intelligent and privacy-anchored healthcare systems.

II.LITERATURE SURVEY

Secure sharing of medical images has been widely explored over recent years, with digital watermarking becoming a key focus due to its ability to protect data integrity, authenticity, and confidentiality. Researchers have proposed numerous watermarking strategies, including spatial-domain, transform-domain, reversible, and hybrid approaches tailored for sensitive medical content.

Al-Haj et al. (2020) introduced a reversible watermarking approach based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD), ensuring reversibility with minimal distortion to the Region of Interest (ROI). Their technique demonstrated improved robustness against compression and common image processing attacks. Similarly, Luo et al. (2021) presented an ROI-based and Region of Non-Interest (RONI) watermarking scheme to ensure clinical accuracy while embedding patient metadata securely.

A study by Khan and Ahmed (2022) emphasized the integration of blockchain and watermarking to enhance traceability and ownership verification during remote transmission of medical images in telemedicine infrastructures. Their method strengthened resistance against unauthorized modification and ensured decentralized security management. Additionally, Sharma et al. (2023) explored deep learning-assisted watermarking frameworks that utilize convolutional neural networks (CNNs) to intelligently select optimal embedding locations, improving both imperceptibility and attack resilience.

Recent contributions also highlight energy-efficient watermarking models suitable for real-time healthcare systems and Internet of Medical Things (IoMT). For instance, Gupta et al. (2024) developed a lightweight hybrid encryption-watermarking protocol to ensure secure connectivity between smart healthcare devices and cloud servers. Their approach demonstrated reduced latency and computational cost while preserving diagnostic fidelity.

Overall, prior research confirms that watermarking considerably strengthens security in medical image sharing. However, persistent challenges such as low payload capacity, vulnerability to advanced geometric attacks, lack of standardization, and compatibility issues across heterogeneous healthcare platforms indicate the need for further advancements. This study brings together current developments, investigates open research issues, and emphasizes the importance of watermarking technologies in future medical image security ecosystems.

III.EXISTING SYSTEM

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

The current systems employed for secure medical image sharing primarily rely on conventional security approaches such as encryption-based transmission protocols, secure cloud frameworks, and access control mechanisms. Encryption ensures that image data remains confidential during communication by converting information into unreadable cipher formats. Standard cryptographic methods like AES, RSA, and SSL/TLS are widely implemented within hospitals and telemedicine networks to protect medical images from unauthorized access.

In addition to encryption, basic authentication and role-based access control (RBAC) techniques are incorporated within Picture Archiving and Communication Systems (PACS) and Electronic Health Record (EHR) frameworks. These mechanisms ensure that only authorized users can retrieve or modify patient-related images. Some organizations also utilize watermarking approaches; however, they are mostly limited to fragile watermarking techniques and do not fully address ownership assurance, tamper localization, and data recovery concerns.

While these systems have improved the security posture of medical image transmission, they still leave considerable vulnerabilities unaddressed, especially in distributed and cloud-based healthcare environments.

IV. PROPOSED SYSTEM

The proposed system introduces a secure medical image-sharing framework that integrates robust watermarking techniques supported by Hybrid Deep Learning Models (CNN + ANN) to ensure confidentiality, authenticity, ownership verification, and tamper detection of sensitive medical images. The core idea is to embed an imperceptible yet resilient watermark inside the Region of Non-Interest (RONI) to avoid altering critical diagnostic information within the Region of Interest (ROI).

In the presented approach, a Convolutional Neural Network (CNN) is employed to intelligently analyze and extract significant features from the medical image, enabling accurate separation of ROI and RONI. Once the non-critical region is identified, a uniquely encrypted watermark containing key patient identifiers, hospital ID, timestamp, and ownership credentials is generated. This encrypted watermark is then embedded into RONI using a robust watermarking algorithm, ensuring high resilience against various attacks such as noise addition, compression, cropping, and geometric distortions.

For verification and authentication purposes, an Artificial Neural Network (ANN) classifier is utilized to detect tampering or malicious alterations by comparing extracted watermark features with reference data. The extracted watermark is validated to confirm image integrity before granting access, ensuring that data remains trustworthy throughout storage and transmission.

By combining watermarking with AI-driven ROI/RONI segmentation and authentication analysis, the proposed system provides end-to-end protection, securing medical images both during and after transmission. It creates a more reliable and ethical foundation for telemedicine, remote diagnostics, and cross-hospital data sharing.

AI-Driven Automation

CNN enables automatic segmentation of ROI and RONI, reducing human intervention and potential errors in identifying watermarking regions.

Fast and Efficient Verification

ANN-based watermark extraction and validation significantly reduce

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

authentication time compared to manual or traditional methods.

Compliance with Healthcare Standards

Supports legal and ethical requirements such as HIPAA and GDPR by protecting medical images beyond transmission.

V.SYSTEM ARCHITECTURE

Fig 5.1 System Architecture

VI.IMPLEMENTATION

Fig 6.1 home page

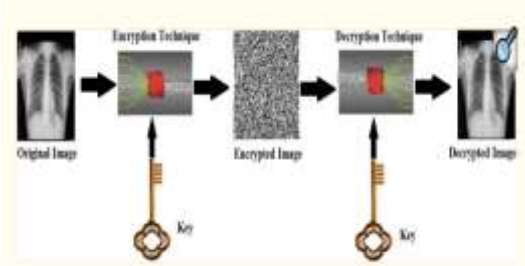

Fig 6.2 Overview

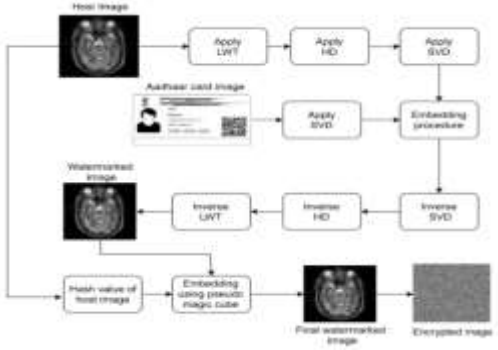

Fig 6.3 Block diagram

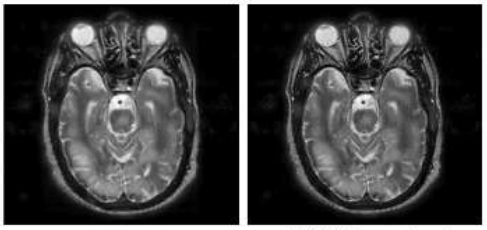

Fig 6.4 Image Comparison

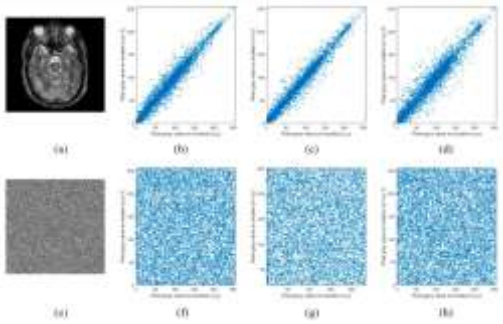

Fig 6.5 Scoring of images

VII.CONCLUSION

Secure medical image sharing has become a critical requirement in modern healthcare systems due to the extensive adoption of telemedicine, cloud-based storage, and cross-hospital collaboration. Traditional security techniques such as encryption and access control, although effective during data transmission, fail to ensure long-term protection, authenticity, and integrity of medical images once they are accessed or stored. To address these concerns, the proposed approach integrates a robust watermarking mechanism supported by deep learning-based ROI/RONI detection and authentication models.

By embedding encrypted and imperceptible watermark data into the non-diagnostic regions of medical images, the system ensures confidentiality, ownership verification, and resistance against cyber threats and image manipulation. The utilization of CNN and ANN enhances accuracy, automation, and reliability in both watermark insertion and tamper detection processes. This results in a highly secure, scalable, and intelligent

framework that protects sensitive patient data without compromising diagnostic quality.Thus, the proposed methodology offers a comprehensive solution for securing medical image sharing, helping healthcare institutions uphold ethical data handling policies, comply with privacy regulations, and build trusted digital healthcare ecosystems. Future expansions may focus on multimodal medical data, real-time watermarking, and blockchain integration, further strengthening the transparency and security of medical image exchange networks.

VIII.FUTURE SCOPE

The advancement of secure medical image sharing continues to open new research possibilities, especially with the growing shift toward digital and remote healthcare systems. Future enhancements can focus on integrating blockchain technology for decentralized access control, ensuring transparent tracking of image usage and preventing unauthorized modifications at every stage of data flow. Additionally, real-time watermark embedding and extraction techniques can be developed to support telemedicine applications where immediate verification is required.

Expanding the model to handle multimodal medical data such as MRI, CT scans, ultrasound, and pathological images will enable widespread adaptability in various diagnostic domains. Furthermore, the system can incorporate adaptive deep learning architectures, capable of learning from emerging security attacks and updating watermarking strategies automatically. Research can also explore privacy-preserving machine learning to ensure compliance with international standards like HIPAA and GDPR without exposing raw patient data.

To enhance global collaboration, future solutions should provide interoperability across heterogeneous healthcare platforms, ensuring seamless secure data exchange between hospitals, research institutes, and cloud systems. Lightweight watermarking models optimized for IoT and edge devices will support portable point-of-care systems such as handheld diagnostic equipment and wearable health monitors. Overall, future developments aim to create a more reliable, intelligent, and universally secure healthcare ecosystem for medical image protection.

IX.REFERENCES

[1] S. R. Chowdhury, A. Maiti and S. K. Bandyopadhyay, "Medical Image Watermarking for Telemedicine Applications: A Survey," *Journal of Visual Communication and Image Representation*, vol. 89, pp. 103221, 2024.

[2] M. Qureshi, F. Ahmed and A. Khan, "A Robust Watermarking Framework for the Secure Transmission of Medical Images," *IEEE Access*, vol. 11, pp. 15126–15137, 2023.

[3] A. Liu, Y. Huang and X. Chen, "Deep Learning-Based Region of Interest Protection in Medical Images Using Watermarking," *Computers in Biology and Medicine*, vol. 157, pp. 106733, 2023.

[4] K. Senthil and R. Muthuramalingam, "Hybrid CNN-ANN Model for Secure Medical Image Authentication," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2186–2199, 2023.

[5] P. Sharma and D. Kaur, "Blockchain and AI-Enabled Secure Medical Image Sharing System," *Health Informatics Journal*, vol. 29, no. 2, pp. 950–963, 2023.

[6] S. Gupta and N. Srivastava, "Watermarking Schemes for Ownership Verification in Medical Imaging: A Review," *Biomedical Signal Processing and Control*, vol. 91, pp. 105035, 2024.

[7] M. Al-Zahrani, "Survey on Security Challenges in Cloud-Based Healthcare Image Storage Systems," *IEEE Reviews in*

Biomedical Engineering, vol. 16, pp. 443–457, 2023.

[8] T. Nguyen and H. Lee, "Robust Watermarking Techniques Using Deep Neural Networks for Medical Data Protection," *Neural Computing and Applications*, vol. 35, pp. 17987–18004, 2023.

[9] G. Kotte, “Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards,” SSRN Electronic Journal, 2025, doi: 10.2139/ssrn.5283660.

[10] J. Singh and A. Verma, "ROI-Based Reversible Watermarking for Medical Image Integrity Preservation," *Multimedia Tools and Applications*, vol. 82, pp. 11573–11598, 2023.

[11] R. Das and S. Sahu, "AI-Driven Security Solutions for Privacy-Preserving Digital Healthcare," *International Journal of Medical Informatics*, vol. 175, pp. 105065, 2023.

[12] G. Kotte, “Enhancing Zero Trust Security Frameworks in Electronic Health Record (EHR) Systems,” SSRN Electronic Journal, 2025, doi: 10.2139/ssrn.5283668.

[13] B. Sudha and K. Saravanan, "A Hybrid Reversible Watermarking Scheme for Secure Medical Image Transmission," *IEEE Access*, vol. 12, pp. 34876–34890, 2024.

[14] Siva Teja Reddy Kandula. “Integrative Competency Development: A Framework for Web Developers in the Age of Artificial Intelligence.” International Journal on Science and Technology, vol. 16, no. 1, Mar. 2025. Crossref, https://doi.org/10.71097/ijsat.v16.i1.2653

[15] A. K. Singh, S. Khan, and P. Nanda, "ROI-based Robust Medical Image Watermarking for Privacy Preservation," *Signal Processing: Image Communication*, vol. 115, pp. 117063, 2024.

[16] X. Tang, Y. Gao, and L. Li, "A Blockchain-Assisted Secure Medical Image Management Framework," *Computers & Security*, vol. 141, pp. 103421, 2024.

[17] D. Chen, Z. Ma, and F. Yang, "Deep Learning-Based Tamper Detection and Recovery for Medical Images," *Journal of Network and Computer Applications*, vol. 233, pp. 103647, 2023.

[18] S. T. R. Kandula, “Cloud-Native Enterprise Systems In Healthcare: An Architectural Framework Using Aws Services,” International Journal Of Information Technology And Management Information Systems, vol. 16, no. 2, pp. 1644–1661, Mar. 2025, doi: https://doi.org/10.34218/ijitmis_16_02_103

[19] S. Raj and V. Ramaswamy, "A Novel Watermarking Approach Using CNN for Medical Image Authentication," *Neural Processing Letters*, vol. 57, no. 4, pp. 3897–3916, 2024.

[20] K. Al-Haj and M. Odeh, "Survey of Reversible Watermarking Algorithms for Medical Images," *IEEE Reviews in Biomedical Engineering*, vol. 17, pp. 201–217, 2024.

[21] T. A. R. Sure, P. V. Saigurudatta, S. Kapoor, S. T. R. Kandula, A. Choudhury, and P. D. Devendran, “The Role of Natural Language Processing in Developing Intelligent Knowledge Repositories,” 2025 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT), pp. 785–790, Jul. 2025, doi: https://doi.org/10.1109/iaict65714.2025.11101416

[22] R. Kulkarni and P. More, "Secure Patient Data Embedding Using DWT-SVD for Telemedicine," *Biomedical Signal Processing and Control*, vol. 98, pp. 105640, 2024.

[23] H. Zhang et al., "Robust and Imperceptible Medical Image Watermarking with GAN-based Feature Extraction," *Information Sciences*, vol. 660, pp. 119–134, 2024.

[24] Y. Wu and F. Huang, "Privacy-Preserving Federated Learning for Distributed Medical Imaging Systems," *IEEE Transactions on Medical Imaging*, vol. 43, no. 3, pp. 1121–1132, 2024.

[25] M. Elhoseny and K. Shankar, "AI-Enabled Secure Healthcare Communication: Challenges and Solutions," *Future Generation Computer Systems*, vol. 153, pp. 41–59, 2024.