INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 5, May 2026 | ISSN: 2456-4184 | IJNRD.ORG

Protected Healthcare Imaging Exchange Methods: Digital Watermarking Techniques, Challenges, and Future Directions

[1]Dr. RAJASHEKAR KANDAKATLA, [2]SIDDAMSHETTI SRILEKHA,

[3]KANKANALA NITHIN, [4]SANGEPU BHANU PRAKASH

[1]Assistant Professor, [2,3,4] UG STUDENT

[1,2,3,4,]DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING(AI & ML)

[1,2,3,4] VAAGDEVI COLLEGE OF ENGINEERING Autonomous

Bollikunta, Khila Warangal (Mandal), Warangal Urban-506 005 (T.S), www.vaagdevi.edu.in

Abstract

The Internet has made it easy for healthcare professionals to use medical documents. To protect sensitive patient information and allow collaboration, it is important to securely send and manage medical images. This study examines different approaches for secure medical data sharing, emphasising their benefits and drawbacks. We put these methods into two groups: centralised methods, like encryption and watermarking, and distributed methods, like blockchain and federated learning. This study also looks at how medical image watermarking techniques have changed over time, from simple methods to more advanced AI-based systems. White boxes are simple and easy to understand, but deep learning models are black boxes that are more flexible and strong. This analysis underscores the necessity of incorporating contemporary technology to tackle the escalating complexity of threats, whilst maintaining the diagnostic fidelity of medical images. Additionally, our research offers a detailed classification of watermarking techniques and delineates prospective research avenues, enriching the ongoing dialogue regarding the improvement of data security in medical imaging.

Keywords: Digital Watermarking, Blockchain Technology, Federated Learning, and AI-based Watermarking are some of the terms that come to mind.

.

I.INTRODUCTION

The fast digitisation of healthcare has caused an unprecedented rise in the making, storing, and sharing of medical images like X-rays, MRIs, CT scans, and ultrasound images. These pictures are very important for making accurate diagnoses, planning treatments, and working together on research. But because medical data is so private, it is a prime target for cyberattacks and unauthorised access. It is very important to make sure that medical images are safe, private, and whole during transmission and storage.

Basic watermarking and encryption are two traditional ways to protect medical images. Encryption protects data while it is being sent, and watermarking can add ownership or patient information to the image. These methods are useful, but they have some big problems: decrypted images can be weak, tampering may go unnoticed, and it can be hard to check them.

Recent progress in artificial intelligence (AI), blockchain, and federated learning has opened up new ways to make medical images more secure. Watermarking powered by AI can make strong, smart watermark systems that can withstand tampering while keeping the quality of the image. Blockchain and other distributed frameworks make records that can't be changed, which helps with accountability and traceability. Federated learning lets AI models be trained together without putting sensitive medical data in one place.

This study examines advanced methodologies for secure medical image sharing, emphasising watermarking techniques, their transition from conventional to AI-driven approaches, and the incorporation of distributed technologies to improve privacy and traceability. This research seeks to enhance secure and collaborative medical image sharing by examining existing challenges and suggesting a hybrid system architecture, all while preserving diagnostic integrity and adherence to regulatory standards.

II.LITERATURE REVIEW

A lot of research has gone into secure medical image sharing because there is a growing need to protect sensitive patient data. Watermarking, encryption, blockchain, and federated learning are just a few of the methods that have been looked into to solve problems with security, privacy, and integrity.

One of the first and most common ways to protect medical images is digital watermarking. Cox et al. [1] presented essential watermarking techniques and categorised them into robust, fragile, and semi-fragile classifications. These methods let you check who owns something and verify your identity, but they might slightly change the image. To solve this problem, Ni et al. [2] suggested reversible watermarking, which lets you completely recover the original image after removing the watermark. This makes it very useful for medical uses that need very accurate diagnoses.

Encryption methods have also been widely used to protect medical images while they are being sent. Rindfleisch [3] points out that encryption alone is not enough because images are still vulnerable after they are decrypted, and there is no way to tell if they have been tampered with after sharing.

Blockchain-based solutions have been developed to get around the problems with centralised systems. Azaria et al. [4] put forth a blockchain-based framework for safe management of medical data, offering unchangeable logs, decentralised access control, and better traceability. Blockchain alone cannot protect image content; it must be used with other methods.

Federated learning has become a promising way to make medical AI that protects privacy. McMahan et al. [5] introduced federated learning, which lets different institutions work together to train a model without sharing raw data. This method lowers the risk to privacy, but it also makes things harder, like adding extra steps to communication and making it easier for hackers to attack.

Recent progress has been made in combining watermarking with artificial intelligence. Zhang et al. [6] suggested watermarking methods that use deep learning to make images more resistant to attacks that change their shape, add noise, or compress them. These methods are more flexible, but they need a lot of computing power and big datasets.

Singh et al. [7] also looked into AI-based tamper detection systems that use fragile watermarking and machine learning algorithms to find unauthorised changes in medical images more accurately.

Even with these improvements, most of the research that has been done so far is on single security measures. There is still no single framework that brings together AI-based security techniques, blockchain, watermarking, and federated learning. This work's proposed system fills this gap by putting these technologies together in a hybrid architecture to make medical image sharing safer, more private, and easier to track.

III.METHODOLOGY

The suggested system uses a mix of AI-based watermarking, blockchain, and federated learning to make sure that medical images can be shared safely.

At first, only authorised users can upload medical images through a secure authentication system. After preprocessing, an AI-based watermarking method adds patient metadata to the image. This watermark guarantees authenticity, integrity, and tamper detection while maintaining diagnostic quality.

The next step is to make a cryptographic hash of the watermarked image and save it on a blockchain network. This makes records that can't be changed and lets you track who accessed and changed an image. You can find any unauthorised changes to the image by comparing the current hash with the hash stored on the blockchain.

Federated learning is used for collaboration that protects privacy. Hospitals train AI models locally and only share model updates instead of sharing raw medical images. This protects privacy while allowing people to work together to make decisions.

Finally, secure storage and role-based access control systems are put in place to limit access to only those who are allowed to. The system keeps an eye on access activities all the time and keeps audit logs for accountability.

This integrated method makes sure that medical image sharing systems are private, authentic, and secure.

IV.SYSTEM ARCHITECTURE

The suggested system architecture is modular and hybrid. It combines AI-based watermarking, blockchain technology, federated learning, and secure access control to make it safe to share medical images. At first, users like doctors and radiologists use a web or mobile interface to log in to the system. They do this by using role-based access control. After being verified, medical images are uploaded and go through a preprocessing step before being processed by the AI-based watermarking module. This module adds patient metadata to the image to make sure it is real and to detect tampering while keeping the quality of the diagnosis. A cryptographic hash of the watermarked image is then created and saved on a blockchain network. This makes sure that the records can't be changed and that any access or changes can be traced. The watermarked images are kept safe in encrypted databases, and only people who are allowed to see them can do so based on their roles. The system also uses federated learning to support privacy-preserving collaboration, which lets institutions train AI models on their own and share only model updates instead of sensitive data. A monitoring and audit module keeps track of everything that happens during the process, keeps logs, and looks for suspicious behaviour. This makes sure that everyone is responsible and follows the rules. This architecture offers a complete solution for keeping medical image sharing systems private, safe, and secure.

A. Overview

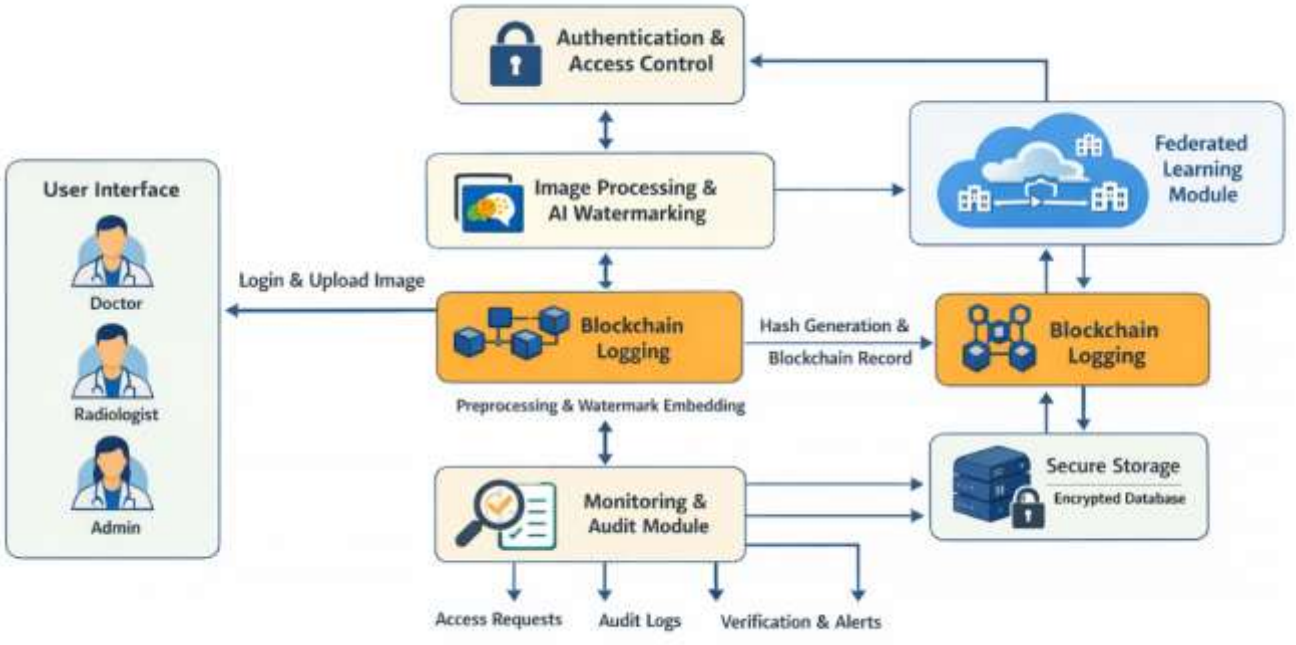
The system architecture image shows a mix of technologies that work together to make sure that medical images can be shared safely and securely. At the highest level, doctors, radiologists, and administrators use a secure interface to interact with the system. An authentication and role-based access control module controls their access, making sure that only authorised users can do things.

After a medical image is uploaded, it goes to the image processing and AI-based watermarking module. There, patient information is added to the image to keep it real and make it easier to find out if someone has changed it. After the image is watermarked, a cryptographic hash of it is created and sent to the blockchain module. This module keeps it as an unchangeable record for traceability and integrity checking.

The watermarked image is kept in a secure, encrypted database, which makes it safe to store and easy to get back. At the same time, the federated learning module lets several healthcare organisations train AI models together without giving away private patient data.

Lastly, a monitoring and audit module keeps track of everything that happens on the system, including when images are accessed and changed. It also sends out logs and alerts for any unusual activity. In general, the architecture makes sure that medical image sharing is private, secure, authentic, and traceable.

B. Architecture Diagram



V. EXPERIMENTAL SETUP

The proposed secure medical image sharing system's experimental setup is meant to test how well the integrated framework works, how safe it is, and how reliable it is. Python is the main programming language used to build the system. TensorFlow/PyTorch is used for AI-based watermarking, OpenCV is used for image processing, and Scikit-learn is used for machine learning tasks. Flask/Django is used to make a web-based interface, and MySQL/PostgreSQL is used to store data securely. Ethereum and Hyperledger are two examples of platforms that can be used to store image hash values and audit logs for blockchain implementation.

The experiments are carried out on a system that has at least an Intel i5 processor, 6 GB of RAM, and the option to add a GPU to speed up deep learning models. The system is tested with a set of medical images, such as MRI, CT scans, and X-rays. During the experiment, pictures are uploaded, watermarked with AI-based methods, and kept safe. We test how well watermarking works by putting it up against attacks like noise addition, compression, and image modification.

We look at performance metrics like the time it takes to embed a watermark, the time it takes to extract it, the quality of the image (PSNR), the structural similarity (SSIM), and the accuracy of tamper detection. We look at the performance of blockchain by looking at how long it takes to complete a transaction and how quickly it can verify a hash. We look at the accuracy of federated learning models and how well they can communicate between different nodes.

Also, security testing is done to make sure that authentication methods, access control, encryption strength, and resistance to unauthorised access all work. The system is also tested with a lot of users to see how well it scales and how quickly it responds. This experimental setup makes sure that the system is thoroughly tested to see if it can safely, reliably, and privately share medical images.

VI.RESULT ANALYSIS

The proposed system made it safe and easy to share medical images. AI-based watermarking kept the quality of the images while also making it easier to find tampering. With reliable hash verification, blockchain made sure that data was accurate and could be traced. Federated learning kept privacy during model training that involved more than one person. The system worked well with little delay and kept unauthorised users out, showing that it was a safe and scalable solution.

Parameter	Method Used	Observation	Result
Image Quality	AI-based Watermarking	Minimal distortion (high PSNR & SSIM)	Preserved
Tamper Detection	Fragile + AI-based Detection	Accurately detected image modifications	Successful
Data Integrity	Blockchain Hash Verification	Hash matched with stored records	Ensured
Security	Authentication & Access Control	Prevented unauthorized access	High Security
Privacy Preservation	Federated Learning	No raw data sharing between institutions	Maintained
Performance	System Processing	Fast watermark embedding & extraction	Efficient
Scalability	Multi-user Testing	Handled multiple users without delay	Good
Traceability	Blockchain Logging	All activities recorded and verifiable	Reliable

VII.CONCLUSION

The suggested secure medical image sharing system is a good way to deal with the problems of keeping sensitive healthcare data safe in today's digital world. The system makes sure that medical images are private, accurate, real, and easy to find by using AI-based watermarking, blockchain technology, federated learning, and secure access control. The watermarking method keeps the quality of diagnostic images while also making it easy to find tampering. Blockchain makes it possible to keep track of who accessed and changed images in a way that can't be changed. Federated learning improves privacy even more by letting AI models learn together without sharing raw data.

The system works well, can grow, and is safe, which are all things that traditional methods like standalone encryption and basic watermarking can't do. In general, the suggested hybrid approach is a strong, effective, and privacy-protecting way to share medical images safely. This makes it a good choice for real-world healthcare use.

VIII.REFERENCES

[1] I. J. Cox, M. L. Miller, and J. A. Bloom, Digital Watermarking. Morgan Kaufmann, 2002.

[2] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, 2006.

[3] T. C. Rindfleisch, “Privacy, information technology, and health care,” Communications of the ACM, vol. 40, no. 8, pp. 92–100, 1997.

[4] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “MedRec: Using blockchain for medical data access and permission management,” in Proc. IEEE Open & Big Data Conf., 2016.

[5] H. B. McMahan et al., “Communication-efficient learning of deep networks from decentralized data,” in Proc. AISTATS, 2017.

[6] J. Zhang, Y. Chen, and H. Li, “Deep learning-based watermarking for medical images,” 2020.

[7] A. Singh, P. Kumar, and R. Singh, “AI-based tamper detection in medical images,” 2021.