DOI: 10.21917/ijivp.2025.0528

# ELECTRONIC HEALTHCARE RECORDS FOR SECURE AND ROBUST MULTIPLE IMAGE WATERMARKING USING BLOCKCHAIN TECHNOLOGY

**N. Mohananthini[1], C. Ananth[2] and S. Kasinathan[3]**
[1]*Department of Electrical and Electronics Engineering, Muthayammal Engineering College, India*
[2,3]*Department of Computer and Information Science, Annamalai University, India*

***Abstract***

***An addition of Electronic Healthcare Records (EHRs) along with watermarking and blockchain technology has opened new avenues for assured and efficient data managing in healthcare systems. The present paper explores an innovative framework for leveraging EHRs in secure and robust multiple image watermarking using blockchain technology. The proposed approach embeds imperceptible watermarks into medical images to enhance authentication, copyright protection, and traceability, addressing critical concerns of data integrity and unauthorized access into healthcare. Blockchain technology exists employed for store watermarking and metadata securely, ensuring tamper-proof verification and decentralized control. The system uses advanced cryptographic techniques and adaptive watermarking algorithms to achieve high robustness against attacks such as compression, noise, and geometric transformations. Comprehensive experiments validate the efficiency of the presented method, demonstrating its developing towards protect sensitive medical data, foster trust among stakeholders, and support the scalability of modern healthcare ecosystems. This research highlights a transformative pathway for integrating watermarking with blockchain technologies to strengthen the security and reliability of EHR systems.***

***Keywords:***

***Blockchain Technology, Composite Technique, Electronic Healthcare Records, Multiple Image Watermarking, Segmented Technique, Successive Technique***

## 1. INTRODUCTION

Electronic Healthcare Records (EHRs) have transformed modern healthcare by enabling efficient storage, sharing, and retrieval of patient information. These records include sensitive records like, medical backgrounds, analytic imaging, and healing plans, which are crucial for clinical decision-making and research. However, as the healthcare sector becomes increasingly digitalized, ensuring the security, privacy, and authenticity of EHRs has become a significant concern. Protecting this data from unauthorized access, tampering, and misuse is essential for maintaining patient trust and compliance with regulatory standards.

Image watermarking offers a viable solution for safeguarding medical images within EHR systems. By embedding imperceptible data directly into images, watermarking enhances the traceability and integrity of medical records. It ensures that images can be authenticated and tracked without compromising their quality. Despite its potential, traditional watermarking methods often struggle with challenges such as resilience to attacks, scalability, and effective integration into large-scale healthcare systems.

Blockchain technology provides an innovative approach to overcoming these challenges: with decentralized as well as immutable records, blockchain ensures data honesty furthermore offers a transparent mechanism for verifying modifications and access. By integrating blockchain with image watermarking techniques, a secure and robust framework can be developed for managing medical images in EHR systems. This integration not only fortifies watermark reliability but also creates a verifiable and tamper-resistant audit trail.

This paper presents a novel methodology that integrates blockchain technology besides multiple image watermarking to address the critical challenges faced in managing EHRs. The proposed approach is designed to enhance security, maintain data authenticity, and support scalability within healthcare systems. The following sections outline the theoretical basis, system architecture, and empirical evaluation of this framework, demonstrating its potential to set new standards for secure healthcare data management.

### 1.1 PROBLEM DEFINITION

- Maintaining the integrity of medical images is critical to avoid any alterations that could compromise clinical diagnoses or research outcomes. Verifying the authenticity of these images in distributed systems remains a challenge.
- As the volume of medical images grows exponentially, traditional image watermarking techniques face difficulties in scaling efficiently while maintaining performance and reliability.
- Traditional watermarking methods are vulnerable to attacks, such as cropping, compression, or tampering, which can compromise the embedded data's robustness and reliability.
- EHR systems often involve multiple stakeholders and platforms, necessitating a solution that works seamlessly across heterogeneous environments without loss of data fidelity.
- EHRs often contain highly sensitive and personal medical information, which makes them attractive targets for unauthorized access, data breaches, and misuse. Ensuring robust protection of this data is essential.

Existing systems lack a decentralized and immutable mechanism to record all interactions with medical images, leading to gaps in auditability and accountability.

## 2. RELATED WORKS

The watermarked images are encrypted when stored in a block to preserve the integrity. The multi-layered secured framework for protects the confidentiality and integrity of the data, though further promote transparent and secured sharing between stake-holders as discussed in [1]. The new integration of blockchain enabled encryption and image watermarking presented in [2]. The medical related image uses the microwave transform to provide multiple resolution coefficients. For the HH waveband, the

surface detection method is used to generate the surface coefficients. Borish Kshetrimayum et al. [3] proposed using blockchain technology to improve medical data management through encryption and fingerprint watermarking. An encryption is used for hefty medical image safeguard and fingerprint watermarking to ensure records integrity within blockchain platforms. Their proposed method has been tested in the environment and proved to be effective in assuring the safety of watermarked images and protecting the network from cruel attacks. A new cryptographic system that is fully adapted to the assets constraints in IoMT environments is presented in [4]. Their crypto system is analyzed for watermarking productivity; strong and Peak Signal-to-Noise Ratio (PSNR) measurement has been utilized to evaluate the robustness of the watermarking against several attacks.

The protected watermarking technique used advancements of multi resolution singular value decomposition (SVD), discrete wavelet transform (DWT), and adaptive neuro-fuzzy inference model is presented in [5]. Their proposed method illustrates the robustness and imperceptibility. Fatma khallaf et al. [6] presented cryptosystem brawn was tested various attacks with numerous complete measures. The development of protected and personal arrangements of medical related image embedded used on blockchain technology, possibly relieving threats connected among cyber attacks on smart medical equipments. A holistic approach to secure and safeguard medical image records by addressing two problems [7], the first is image tamper detection using medical image deep fake detection to decipher whether the image has been modified or not, and the second is to employ various cryptographic methods like, digital signatures, hashing and watermarking to secure the images from getting tampered itself. A hashing based process with the Integer Wavelet Transform provides secured watermarking for private medical data in [8]. Experiment results demonstrated that perceptual assets of the images were whole in provisions of PSNR and Structural Similarity Index (SSI). Kedar Nath Singh et al. [9] proposed a secured watermarking used on multimodal medical image fusion (WatMIF). They cipher the cover medium with a key placed encryption algorithm. The Non Subsampled Contourlet Transform (NSCT) used combination method is engaged to blend the Magnetic Resonance Imaging (MRI), Computed Tomography (CT) scanned pictures to create the multiple images. The encrypted medium covered the merged watermark with redundant DWT and Randomized Singular Value Decomposition (RSVD). Their results calculated their algorithm concerned robustness, security as well as invisibility.

Secure watermarking algorithms designed to ensure the transmission and storage of DHR in blockchain-based healthcare applications [10]. Their method used Non Sub-sampled Shear-let Transform (NSST) along with Multi Resolution Singular Value Decomposition (MRSVD) to add watermark to the medical original image. Their experimental results of the watermarking technology demonstrated substantial resilience to various attacks while preserving the high quality of the marked image with regular PSNR as well as NC values. Chetna Sharma et al. [11] proposed a novel reversible watermarking supported on adaptive prediction error expansion, it recovered cover image behind extracted unseen information. Digital Image watermarking with image thrashing method is discussed in [12] headed for provides verification of colour images. The method has ability to tamper localization as well as tamper detection. Their method is blind watermarking that does not required original data at intention. The strength of multi-level DWT along with influence of Convolution Neural Network's (CNN) combined and proposed a robust blind image watermarking method in [13]. Their presented model grants highest value watermark extracted in symmetrical, image processing and antagonistic attacks included second watermarking with attacker. A novel Deep Mark Net approach for robust image and video watermarking is introduced in [14]. Experimental results demonstrated that Deep Mark Net effectiveness, achieving a accuracy and maintaining watermark integrity under compression and noise attacks.

User identification and transactions in the proposal are applied blockchain sustaining the possession of the method and metadata in immutable, translucent as well as decentralized mode [15]. Meng Zhaoxiong et al. [16] examined a machine learning approach to improve perceptual hashing. Images are first transformed using different techniques to generate a set of images. The set of images is fed into a CNN to calculate feature features, and the data in the middle layer of the CNN is output as machine learning data. Li Ming et al. [17] proposed a block watermark to protect the privacy, integrity and availability of the selected additional images, which successfully combines multimedia watermarking, compression and interstellar file system and blockchain technology. The simplicity of watermarking schemes furthermore benefits of blockchain technology in shielding digital copyright information from tampering have created and implemented an environmentally friendly copyright protection scheme discussed in [18, 19]. Tao Chen et al. [20] proposed the part of zero image watermarking method in copyright, storage and authentication scheme. It studied a zero image watermarking used scheduled blockchain and constructs a structure based on the framework. Zhaoxiong Meng et al. [21] proposed blockchain technology, digital watermarking, hashing function, QR code, Inter Planetary File System (IPFS). The blockchain technology is employed to accumulate secured watermark data and present timestamp certification for multiple image watermarks to prove the formation orders. Their work also improved copyright protection of multiple creations. Image watermarking techniques has been used authentication field in [22]. The blockchain technology is a comparatively fresh technology and associated to image authentication. They utilized blockchain technology to elude any authentication.

# 3. METHODOLOGY

## 3.1 MULTIPLE WATERMARKING

Multiple image watermarking is a technique where unique data is embedded into multiple images to ensure security, authenticity, and traceability. This approach is particularly beneficial in scenarios involving large datasets, such as medical imaging in healthcare systems. By embedding information into several images, it becomes possible to maintain data integrity and create a robust mechanism for verifying image authenticity. This method also aids in deterring unauthorized usage and ensuring accountability in data handling. Furthermore, the use of advanced algorithms enhances the resilience of watermarks against tampering, compression, or other attacks.

### 3.2 SECURED HASH ALGORITHM (SHA)

The Secured Hash Algorithm (SHA) is a cryptographic hashing function widely used for ensuring data integrity and security. It operates by generating a fixed length hash value from input record, regardless of the record's volume. SHA is designed to be a one-way function, meaning the hash value cannot be reversed to retrieve the original input. It is commonly utilized in digital signatures, authentication protocols, and blockchain systems to verify data authenticity. Various versions of SHA, like, SHA-1, SHA-256, and SHA-512, present different levels of security and performance. Among these, SHA-256 is particularly popular for its balance between computational efficiency and robustness against cryptographic attacks. By ensuring that a slight modify in the input record produces a significantly dissimilar hash, SHA provides a reliable mechanism to detect data tampering. Its integration into modern security frameworks highlights its critical role in protecting digital information.

### 3.3 BLOCKCHAIN TECHNOLOGY

Blockchain technology is a de-centralized along with distributed ledger that records transactions across many nodes in a protected and tamper-resistant method. By eliminating require for a central authority, blockchain ensures transparency and trust among participants. Each block in the chain includes a cryptographic hashing value of the previous block, a time-stamp and transaction record, building it almost not possible to modify past records. Blockchain is generally utilized in many industries, including healthcare, supply chain and finance, for its facility to present a verifiable with immutable record of every transactions. Smart contracts, an integral feature of blockchain, automate processes by executing predefined conditions, further enhancing efficiency and security. Its applications extend to data integrity, secure sharing, and decentralized identity management, making it a transformative technology for safeguarding sensitive information. When integrated with technologies like blockchain, multiple image watermarking can offer an additional layer of transparency and security. This combination ensures a reliable and scalable framework for managing sensitive digital assets across distributed systems.

## 4. PROPOSED WORK

The proposed work has integrating of multiple watermarking with Blockchain Technology, firstly, more than one watermarks are embedded to medical images. Then the embedded watermarked images store to a block of de-centralized distributed ledger in the blockchain technology. The medical images like CT scan images, MRI scan images and other medical related images, treated as original images. The symbols or icons or unique number of the hospital or doctor's identifications are treated as watermark images. The watermarked image stored into a block using blockchain technology is shown in Fig.1. The proposed models are shown below:

### 4.1 ARRANGEMENTS OF THE BLOCK

The arrangements of the block have 3 separations as shown in Fig.2. It has top, middle and bottom of the blocks.

- The top of the block has three parts: Block number, Nonce, Hash number of the present block
- The middle of the block a part: Watermarked Medical Image
- The bottom of the block has two parts: Time stamp and Hash number of the prior block

The functions of every parts is discussed as follows, The Block number is the serial number of the block, Nonce is the system generated automatic number like a random number, for the purpose of avoid duplication, the hash number of the present block is the value for entire block using the Secured Hash Algorithm (SHA-256). Time stamp is the creation of the block's date and time.

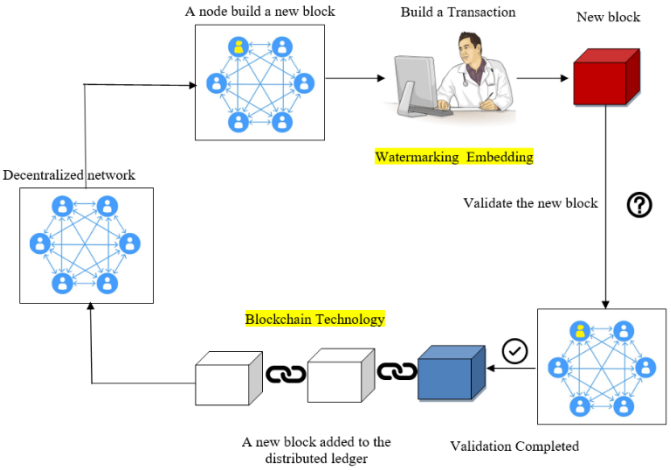


Fig.1. Overview of functioning principle

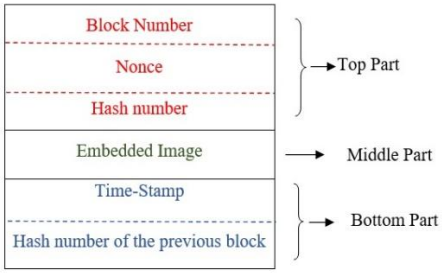


Fig.2. Arrangements of the block parts

### 4.2 SUCCESSIVE EMBEDDING MODEL

Successive watermarking is a technique in digital watermarking where multiple watermarks are embedded sequentially into a digital image. The patient's scanned images analyze more than one doctor in the same or different hospitals, every time they are inserted his watermark. The embedding method is shown in Fig.3.

**Algorithm -** Successive embedding model

Input: Medical images and Hospital/Doctor's information

Output: Embedded Image block

Allocation: Id number of this block and Hash of the prior block

1. **if** the node validate the block **then**
2. $I_{(x,y)}$ ← Medical Image (Original Image)
3. $J_{1(x,y)}$ ← Hospital/Doctor's authentication image (Watermark 1)

4. $J_{2(x,y)}$ ← Hospital/Doctor's authentication image (Watermark 2)
5. $K_{1(x,y)}$ ← $I_{(x,y)} + (\alpha \times J_{1(x,y)})$
6. $K_{2(x,y)}$ ← $K_{1(x,y)} + (\alpha \times J_{2(x,y)})$
7. *Embedded Image* ← $K_{2(x,y)}$
8. Stored the Embedded image to the block
9. **else**
10. unauthorized data
11. **end if**
12. Stored the date and time
13. Stored the hash number of this block

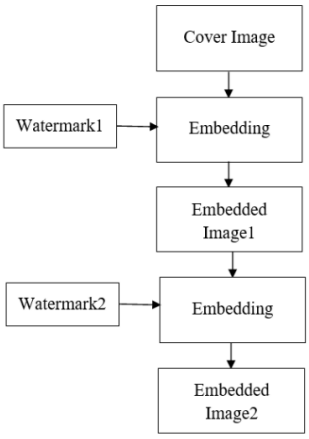


Fig.3. Successive embedding model

## 4.3 SEGMENTED EMBEDDING MODEL

Segmented watermarking is a technique used in digital watermarking where the content is divided into smaller segments, and each segment is individually watermarked. The patient's scanned images analyze more than one doctor in the same or different hospitals, they are inserted his watermark in analysed smaller segments. The embedding method is shown in Fig.4.

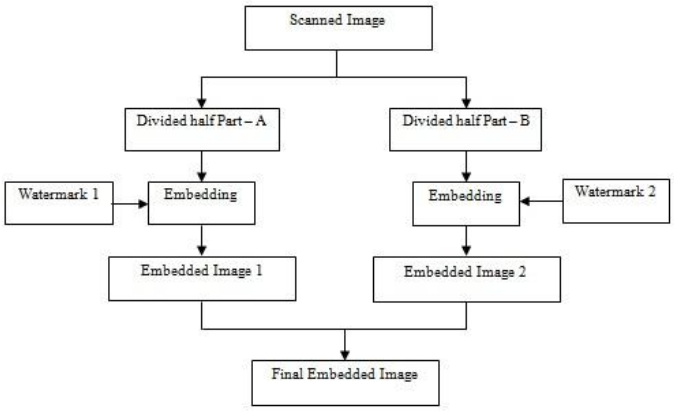


Fig.4. Segmented embedding model

**Algorithm -** Segmented embedding model

Input: Medical images and Hospital/Doctor's information

Output: Embedded Image block

Allocation: Id number of this block and Hash of the prior block

1. **if** the node validate the block **then**
2. $I_{(x,y)}$ ← Medical Image (Original Image)
3. $J_{1(x,y)}$ ← Hospital/Doctor's authentication image (Watermark 1)
4. $J_{2(x,y)}$ ← Hospital/Doctor's authentication image (Watermark 2)
5. $I_{1(x,y)} + I_{2(x,y)} \leftarrow I_{(x,y)}$
6. $K_{1(x,y)}$ ← $I_{1(x,y)} + (\alpha \times J_{1(x,y)})$
7. $K_{2(x,y)}$ ← $I_{2(x,y)} + (\alpha \times J_{2(x,y)})$
8. $K_{(x,y)} \leftarrow K_{2(x,y)} + K_{1(x,y)}$
9. *Embedded Image* ← $K_{(x,y)}$
10. Stored the Embedded image to the block
11. **else**
12. unauthorized data
13. **end if**
14. Stored the date and time
15. Stored the hash number of this block

## 4.4 COMPOSITE EMBEDDING MODEL

Composite watermarking is a technique where multiple watermarks are embedded simultaneously into a single piece of digital image. The patient's scanned images analyze more than one doctor in the same or different hospitals, they are inserted the watermark, all the watermarks are combined in a watermark and analysed. The embedding method is shown in Fig.5.

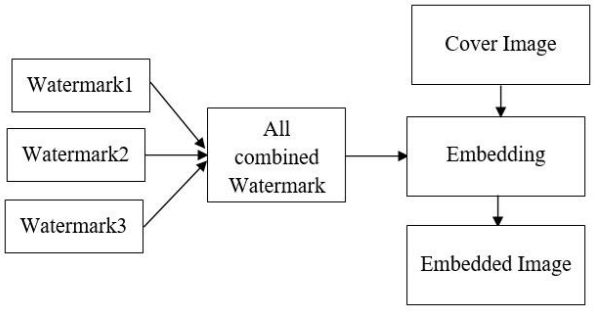


Fig.5. Composite embedding model

**Algorithm -** Composite embedding model

Input: Medical images and Hospital/Doctor's information

Output: Embedded Image block

Allocation: Id number of this block and Hash of the prior block

1. **if** the node validate the block **then**
2. $I_{(x,y)}$ ← Medical Image (Original Image)
3. $J_{1(x,y)}$ ← Hospital/Doctor's authentication image (Watermark 1)
4. $J_{2(x,y)}$ ← Hospital/Doctor's authentication image (Watermark 2)
5. $J_{3(x,y)}$ ← Hospital/Doctor's authentication image (Watermark 3)
6. $J_{(x,y)} \leftarrow J_{1(x,y)} + J_{2(x,y)} + J_{3(x,y)}$
7. $K_{(x,y)}$ ← $I_{(x,y)} + (\alpha \times J_{(x,y)})$
8. *Embedded Image* ← $K_{(x,y)}$

9. Stored the Embedded image to the block
10. **else**
11. unauthorized data
12. **end if**
13. Stored the date and time
14. Stored the hash number of this block

## 4.5 EHR USING BLOCKCHAIN TECHNOLOGY

Blockchain technology is a de-centralized, distributed ledger model that each data transaction in the entire network of nodes. It guarantees security, transparency and unalterable of transaction, creating it a foundational technology for different applications beyond cryptocurrencies. The proposed work utilized the advantages of blockchain technology in the field of health care management. The three types of multiple watermarking techniques created embedding blocks. Each individual embedding block is connected to the previous block of the entire blockchain. The first block's previous hash value is zero. The first block is also called genesis block.

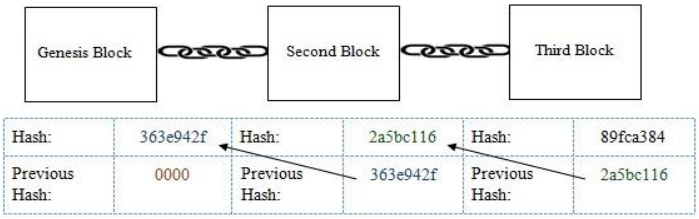


Fig.6. EHR with Blockchain technology

## 5. RESULTS AND DISCUSSION

The analysis of three models in electronic healthcare records, are tested with scanned images as original images with dimension of 512×512 and the watermarks dimension of 48×48 are shown in Fig.7.

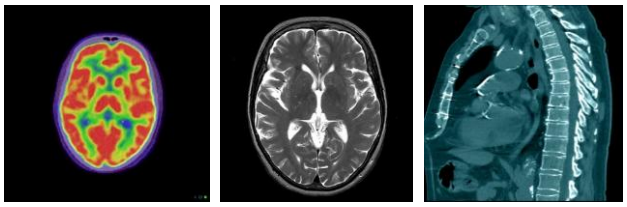

Image – 1 Image – 2 Image – 3

Original Images

Logo – 1 Logo - 2

Watermark Images

Fig.7. Testing Images

## 5.1 PERFORMANCE ANALYSIS

Watermarking Techniques Analysis: The embedded image quality of each watermarked image compared with the original image by calculating Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) values. The recovered watermark image quality of each watermark compared with the host watermark by calculating values of Normalized Correlation (NC).

$$MSE = \frac{1}{N}\sum_{j=0}^{N}(I_w - I\ )^2 \tag{1}$$

where, $I_w$ is watermarked image and $I$ is original image

$$PSNR(dB) = 10\log_{10}\frac{255^2}{MSE} \tag{2}$$

$$NC = \frac{\sum_{i=1}^{H}\sum_{j=1}^{L}W(i,j)\times W'(i,j)}{\sum_{i=1}^{H}\sum_{j=1}^{L}[W(i,j)]^2} \tag{3}$$

The Table.1 shows the PSNR values of the proposed models

Table.1. PSNR values on proposed models

| Models | **Image 1** | **Image 2** | **Image 3** |
|---|---|---|---|
| | **PSNR (dB)** | **PSNR (dB)** | **PSNR (dB)** |
| Successive Technique | 44.0062 | 43.9432 | 43.9752 |
| Segmented Technique | 42.1351 | 42.0303 | 41.9743 |
| Composite Technique | 40.1742 | 39.9692 | 39.9512 |

The Table.2 shows the NC values of the proposed models

Table.2. NC values on proposed models

| Models | **Image 1** | | **Image 2** | | **Image 3** | |
|---|---|---|---|---|---|---|
| | **Logo 1 NC** | **Logo 2 NC** | **Logo 1 NC** | **Logo 2 NC** | **Logo 1 NC** | **Logo 2 NC** |
| Successive Technique | 0.9973 | 0.9982 | 0.9892 | 0.9895 | 0.9854 | 0.9862 |
| Segmented Technique | 0.9953 | 0.9964 | 0.9923 | 0.9929 | 0.9943 | 0.9952 |
| Composite Technique | 0.9965 | 0.9974 | 0.9972 | 0.9974 | 0.9964 | 0.9968 |

The proposed watermarking techniques tested with various attacks. The Table,3 shows the values with attacks. The attacks levels are speckle noise variance - 0.005, the median filtering intensity - 0.03, the rotation – 60-degree, compression quality factor 20.

Table.3. PSNR (dB) values on proposed models with attacks

| **Models** | **Attacks** | **Image1** | **Image2** | **Image3** |
|---|---|---|---|---|
| Successive Technique | Speckle Noise | 28.6543 | 27.3076 | 27.7384 |
| | Median Filtering | 33.5651 | 33.6386 | 33.3265 |
| | Cropping | 18.7176 | 18.7386 | 17.8254 |
| | Rotation | 9.8665 | 9.8647 | 9.8636 |
| | JPEG Compression | 35.5341 | 35.6453 | 34.9892 |
| Segmented Technique | Speckle Noise | 27.1543 | 27.2007 | 27.1522 |
| | Median Filtering | 33.5801 | 33.4893 | 33.4902 |
| | Cropping | 18.3754 | 18.2142 | 17.9998 |

| | | | | |
|---|---|---|---|---|
| | Rotation | 8.6982 | 8.6917 | 8.7211 |
| | JPEG Compression | 35.3414 | 35.2009 | 35.0073 |
| Composite Technique | Speckle Noise | 34.6793 | 34.6721 | 33.6875 |
| | Median Filtering | 20.4923 | 20.5021 | 20.2174 |
| | Cropping | 19.0254 | 19.0115 | 18.9951 |
| | Rotation | 9.7991 | 9.8021 | 9.8132 |
| | JPEG Compression | 36.3585 | 36.4003 | 36.4141 |

Table.4. NC values on proposed models with attacks

| Models | Attacks | Image1 | | Image2 | | Image3 | |
|---|---|---|---|---|---|---|---|
| | | NC1 | NC2 | NC1 | NC2 | NC1 | NC2 |
| Succ. | Speckle Noise | 0.9900 | 1.0000 | 0.9800 | 1.0000 | 0.9900 | 1.0000 |
| | Median Filtering | 0.9900 | 1.0000 | 0.9900 | 1.0000 | 0.9900 | 1.0000 |
| | Cropping | 0.5300 | 0.9800 | 0.5300 | 0.9900 | 0.5300 | 0.9800 |
| | Rotation | 0.3600 | 0.9600 | 0.3400 | 0.9600 | 0.3600 | 0.9500 |
| | JPEG Comp. | 1.0000 | 0.9700 | 1.0000 | 0.9800 | 1.0000 | 0.9800 |
| Segm. | Speckle Noise | 0.9900 | 0.9900 | 0.9900 | 0.9900 | 0.9900 | 0.9900 |
| | Median Filtering | 0.9900 | 1.0000 | 0.9900 | 1.0000 | 0.9900 | 1.0000 |
| | Cropping | 0.5800 | 0.5300 | 0.5800 | 0.5400 | 0.5800 | 0.5400 |
| | Rotation | 0.3200 | 0.3100 | 0.3200 | 0.3100 | 0.3100 | 0.3600 |
| | JPEG Comp. | 1.0000 | 1.0000 | 1.0000 | 1.0000 | 1.0000 | 1.0000 |
| Comp. | Speckle Noise | 0.9971 | 0.9997 | 1.0000 | 1.0000 | 0.9948 | 0.9953 |
| | Median Filtering | 0.9973 | 1.0000 | 0.9991 | 1.0000 | 0.9983 | 1.0000 |
| | Cropping | 0.5621 | 0.5256 | 0.5652 | 0.5254 | 0.5616 | 0.5246 |
| | Rotation | 0.3242 | 0.3892 | 0.3243 | 0.3876 | 0.3352 | 0.3974 |
| | JPEG Comp. | 1.0000 | 1.0000 | 1.0000 | 1.0000 | 1.0000 | 1.0000 |

The proposed model is creating a block and adding the blockchain. The blockchain is immutable, tamper proof.

## 5.2 COMPARISON WITH RELATED MODELS

The proposed work compared by the existing system. Table 5 shows the models of the current technique among the Blockchain using models Brahim [1], Divyanshu [5], and Ahmed [18], and without Blockchain using models Kahla [4] and Chetna [11]. The table proved that the present model to achieved and faced the entire properties in electronic healthcare records.

Table.5. Comparison by existing models

| Properties | Brahim [1] | Kahla [4] | Divyanshu [5] | Chetna [11] | Ahmed [18] | Proposed system |
|---|---|---|---|---|---|---|
| Unforgeablity | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Privacy protection | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Partial models | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Admission control | ✓ | × | × | ✓ | ✓ | ✓ |
| Blockchain support | ✓ | × | ✓ | × | ✓ | ✓ |
| Complete models | × | × | × | × | × | ✓ |

## 6. CONCLUSION

The integration of EHRs with secure and robust multiple image watermarking, powered by blockchain technology, presents a transformative advance to addressing image security and integrity challenges in the healthcare sector. By embedding imperceptible watermarks in medical images, this framework enhances authentication, copyright protection, and traceability while safeguarding sensitive patient information. Blockchain technology ensures a de-centralized and secured environment for managing watermarking keys and metadata, presenting an added layer of safety and transparency. The proposed system demonstrates resilience against common attacks, such as compression and noise, and ensures robust watermark recovery, creating it a viable solution for realistic applications. Moreover, the decentralized nature of blockchain fosters trust among stakeholders, minimizes the threat of data breaks, and supports the scalability required for modern healthcare ecosystems. The convergence of EHRs, watermarking, and blockchain technology represents a significant advancement in medical data management, offering a secure, reliable, and future-proof solution for protecting healthcare information. Future research could further refine the algorithms and explore additional use cases, such as integrating artificial intelligence for automated watermarking and validation processes.

## REFERENCES

[1] Brahim Ferik, Lakhdar Laimeche, Abdallah Meraoumia, Omar Aldabbas, Muath Alshaikh, Abdelkader Laouid and Mohammad Hammoudeh, "A Multi-Layered Security Framework for Medical Imaging: Integrating Compressed Digital Watermarking and Blockchain", *IEEE Access Multidisciplinary*, Vol. 12, pp.187604-187622, 2024.

[2] Praveen Kumar Mannepalli, Vineet Richhariya, Susheel Kumar Gupta, Piyush Kumar Shukla, Pushan Kumar Dutta, Subrata Chowdhury and Yu-Chen Hu, "A Robust Blockchain-Based Watermarking using Edge Detection and Wavelet Transform", *Multimedia Tools and Applications*, Vol. 83, pp. 11112-111127, 2024.

[3] Borish Kshetrimayum, Kausthav Pratim Kalita, Chelsea Dambe R. Sangma and Heman Budathoki, "A Secure Storage of Watermarked Images and Encrypted Data in a Blockchain-Based Healthcare Platform", *Proceedings of International Conference on Innovations in Computational Intelligence and Computer Vision*, pp 533-543, 2024.

[4] Mohammed El Habib Kahla, Mounir Beggas, Abdelkader Laouid, Muath AlShaikh and Mohammad Hammoudeh, "An IoMT Image Crypto-System based on Spatial Watermarking and Asymmetric Encryption", *Multimedia Tools and Applications*, Vol. 83, pp. 86681-86706, 2024.

[5] Divyanshu Awasthi, Priyank Khare, Vinay Kumar Srivastava and Amit Kumar Singh, "ANFIS Optimization-Based Watermarking for Securing Integrity of Medical Images with Blockchain Authentication", *Computers and Electrical Engineering*, Vol. 118, pp. 1-7, 2024.

[6] Fatma Khallaf, Walid El-Shafai, El-Sayed M. El-Rabaie and Fathi E. Abd El-Samie, "Blockchain-Based Color Medical Image Cryptosystem for Industrial Internet of Healthcare Things (IoHT)", *Multimedia Tools and Applications*, Vol. 83, pp. 30014-30025, 2024.

[7] U Kumaran, Gurupriya M, Harshitha Reddy Thodathara, Aryagopal, Aditya Vijjapu, Gattamaneni Harish, "Enhancing Healthcare Image Record Security via CNN-based Tamper Detection, Watermarking, and Digital Signatures", *Proceedings of International Conference on Self Sustainable Artificial Intelligence Systems*, pp. 1-6, 2024.

[8] C.H. Rupa, S.K. Arshiya Sultana, R. Pavana Malleswari, C.H. Dedeepya, Thippa Reddy Gadekallu, Hyoung-Kyu Song and Md Jalil Piran, "IoMT Privacy Preservation: A Hash-Based DCIWT Approach for Detecting Tampering in Medical Data", *IEEE Access Multidisciplinary,* Vol. 12, pp. 97298-97308, 2024.

[9] Kedar Nath Singh, Om Prakash Singh, Amit Kumar Singh and Amrit Kumar Agrawal, "WatMIF: Multimodal Medical Image Fusion-Based Watermarking for Telehealth Applications", *Cognitive Computation*, Vol. 16, pp. 1947-1976, 2024.

[10] Gurleen Kaur, Bakul Gupta and Ashima Anand, "Semi-Blind Watermarking and Blockchain-Based Approach for Copyright Protection of Medical Images", *Proceedings of International Conference on Security and Privacy*, pp. 21-29, 2024.

[11] Chetna Sharma and Neeraj Jain, "Performance Evaluation and Comparative Analysis of Watermarking Algorithm based on Adaptive Prediction Method", *ICTACT Journal on Image and Video Processing*, Vol.9, No. 2, pp. 18761881, 2018.

[12] Hiral A Patel and Dipti B Shah, "Semi-Fragile Blind Watermarking Mechanism for Color Image Authentication and Tampering," *ICTACT Journal on Image and Video Processing*, Vol. 11, No. 3, pp. 2355-2359, 2021.

[13] Sai Shyam Sharma and Venkatachalam Chandrasekaran, "A Novel 3-level DWT and CNN-based Blind Grayscale Image Watermarking for Copyright Protection against Adversarial Attacks", *ICTACT Journal on Image and Video Processing*, Vol. 11, No. 4, pp. 2460-2469, 2021.

[14] Chhavi Bajpai, Manish Gaur and Gajendrasinh N. Mori, "Deepmarknet for Robust Image and Video Watermarking Embedding and Detection", *ICTACT Journal on Image and Video Processing,* Vol. 15, No. 1, pp. 3375-3378, 2024.

[15] Venkata Raghava Kurada, Pallav Kumar Baruah, "Blockchain Enabled, Collaborative Platform Blockchain for AI as a service," *ICTACT Journal on Image and Video Processing*, Vol. 13, No. 3, pp. 2909-2916, 2023.

[16] Meng Zhaoxiong, Morizumi Tetsuya, Miyata Sumiko and Kinoshita Hirotsugu, "Perceptual Hashing based on Machine Learning for Blockchain and Digital Watermarking", *Proceedings of International Conference on Smart Trends in Systems Security and Sustainablity*, pp. 1-7, 2019.

[17] Ming Li, Leilei Zen, Le Zhao, Renlin Yang, Dezhi An and Haiju Fan, "Blockchain-Watermarking for Compressive Sensed Images", *IEEE Transactions and Journals*, Vol. 4, pp. 1-19, 2016.

[18] Ahmed S. Alghamdi, Surayya Naz, Ammar Saeed, Eesa Al Solami, Muhammad Kamran and Mohammed Saeed Alkatheiri, "A Novel Database Watermarking Technique using Blockchain as Trusted Third Party", *Computers, Materials and Continua*, Vol. 70, No. 1, pp. 1585-1601, 2022.

[19] Baowei Wang, Shi Jiawei, Weishen Wang and Peng Zhao, "A Blockchain-based System for Secure Image Protection using Zero-watermark", *Proceedings of International Conference on Mobile Ad Hoc and Sensor Systems*, pp. 78-85, 2020.

[20] Tao Chen, Zhao Qiu, Gengquan Xie, Lin Yuan, Shaohua Duan, Hao Guo, Dahao Fu and Hancheng Huang, "A Image Copyright Protection Method using Zero-Watermark by Blockchain and IPFS", *Journal of Information Hiding and Privacy Protection*, Vol. 3, No. 3, pp. 131-142, 2021.

[21] Zhaoxiong Meng, Tetsuya Morizumi, Sumiko Miyata and Hirotsugu Kinoshita, "Design Scheme of Copyright Management System Based on Digital Watermarking and Blockchain", *Proceedings of International Conference on Computer Software and Applications*, pp. 1-4, 2018.

[22] Alsehli Abrar, Wadood Abdul and Sanaa Ghouzali, "Secure Image Authentication using Watermarking and Blockchain", *Intelligent Automation and Soft Computing*, Vol. 28, No. 2, pp. 577-591, 2021.