Journal of Intelligent Systems and Internet of Things
Vol. 18, No. 01, PP. 126-139, 2026
DOI: https://doi.org/10.54216/JISIoT.180109

IoT-Enabled Reversible Watermarking of Medical Images Using PCA and Hash-Based Signatures for Secure Smart Healthcare

Pradeep Kumar Tripathi[1], Manoj Varshney[1], Aditi Sharma[2,3,*]
[1]Department of Computer Engineering & Applications Mangalayatan University, Aligarh, Uttar Pradesh, India
[2]Department of Computer Science and Engineering, Symbiosis Institute of Technology, Pune, India
[3]Symbiosis International (Deemed) University, Pune, India
Emails: er.pradeeptripathi@gmail.com; manoj.varshney_dcea@mangalayatan.edu.in; aditi.sharma@ieee.org

Abstract

The rise of IoT in smart healthcare systems necessitates secure and efficient methods to protect sensitive medical imaging data transmitted across interconnected devices. This research introduces a novel IoT-enabled reversible watermarking technique using Principal Component Analysis (PCA) and Hash-Based Signatures (HBS) to ensure both data integrity and diagnostic quality. The method supports secure embedding of watermarks into medical images captured and transmitted by IoT devices such as wearable scanners, remote diagnostic units, and edge sensors. By leveraging PCA for minimal distortion and reversible embedding, and HBS for robust tamper detection, the system ensures full restoration of original images post-verification. Discrete Wavelet Transform (DWT) further optimizes the compression and transformation for real-time IoT environments. The proposed approach demonstrates high imperceptibility (high PSNR), robust tamper detection (using SHA-256 and SHA-512), and full reversibility, making it ideal for real-time transmission of medical data over IoT-based healthcare networks.

Received: February 20, 2025 Revised: May 27, 2025 Accepted: July 07, 2025

Keywords: Reversible Watermarking; Discrete Wavelet Transform (DWT); Principal Component Analysis; Peak Signal-to-Noise Ratio; Normalized Correlation; Structural Similarity Index Measure; Mean Squared Error; Hash-Based Signatures Techniques (HBST); Internet of things (IoT)

1. Introduction

Medical imaging bolsters research, treatment planning, and diagnosis, and the rapid evolution of digital healthcare technology has further augmented its power. Imaging techniques such as X-rays, CT scans, and MRIs are important for an accurate medical assessment as they provide visual information about the body. These photos contain sensitive and personal information that help protect patient privacy and improve accurate diagnosis. These images have to be secure to ensure patient confidentiality. Misdealing, legal issues, and distrust by patients can occur due to data breaches, illegal access, and tampering. Security Challenges in Medical Photos Could be Resolved with Watermarking Conventional watermarking embeds specific data in photographs to ensure their origin and detect modification. These approaches create distorted images, limiting their use in medical contexts where even minor alterations can negatively impact diagnostic results. There is a high demand for reversible watermarking technologies, because this type of technology must embed data into photos so that they can be perfectly restore after extraction. PCA is the most effective statistical method for rearranging data into a new coordinate system, where the initial set of coordinates, called principal components, contain the most variation. We present a principal component analysis-based medical picture reversible watermarking method in this paper. By adding watermarks to the image data's primary components, our technique preserves image quality with minimum distortion. Because this approach is reversible, it can restore medical images without losing diagnostic value.

2. Related work

Reversible watermarking—also called lossless or invertible—has been gaining popularity for medical image security because it may add and remove watermarks without damaging the original data. Each approach for making reversible watermarks has pros and cons for image integrity Reversible watermarking started with predictive-based approaches, histogram shifting, and difference expansion Work on difference expansion prepared the way to undo the process of increasing pixel values to produce the original image for embedding data [1]. Histogram shifting, invented [2], offers lossless image recovery by shifting particular histogram sections to accommodate the watermark. These methods might generate noticeable aberrations, which is problematic in medical imaging because accuracy is crucial. More advanced and contemporary approaches have created to improve upon conventional watermarking technologies. One approach that has suggested finding the sweet spot between watermark capacity and picture quality is reversible data hiding based on integer wavelet transforms. By including the watermark into the prediction error of pixel values, Thodi and Rodríguez [4] presented a novel approach to prediction-error expansion that reduces distortion. Even with all these improvements, it is still not easy to incorporate big amounts of watermark data while keeping the image quality and reversibility intact. The necessity for strong security in medical imaging motivates this study's research since it will safeguard images against manipulation without lowering their diagnostic accuracy or clarity.

3. Proposed Work

Discrete Wavelet Transform: A mathematical method for essentially separating images or signals into their fundamental frequency components is the Discrete Wavelet Transform (DWT). This process creates a hierarchical representation that may store information about both time and frequency. Data with different localized properties can effectively analyzed using DWT because, unlike typical Fourier transformations, it retains spatial (or temporal) details. A DWT cannot be construct without wavelets, which are tiny finite-duration functions whose frequency properties change depending on their local environment. By utilizing these wavelets, DWT is able to do analysis in the time and frequency domains simultaneously. The DWT permits multiresolution analysis by applying the transform in stages, which allows for both coarse and fine representations of a signal. Multiresolution analysis is an iterative decomposition method that gradually extracts the wavelet components from a signal or image. For images, this typically involves separating the image into approximation (low frequency) and detail (high frequency) components. For 1D Signals: Filtering: The signal is passed through a pair of filters: a low-pass filter to capture the approximate components (low frequencies) and a high-pass filter to capture the detail components (high frequencies). Down sampling: After filtering, the signal is down sampled (i.e., reduced in size by taking every other sample) to remove redundancy and reduce the data size. Iterative Decomposition: The process is repeat on the low-pass filtered signal to create multiple levels of decomposition, each providing a different resolution. For Two-Dimensional Pictures: Refining and Loss Sampling: As in 1D, the image is initially filter along the rows and columns with low-pass and high-pass filters. Sub bands LL for closeness, LH for horizontal details, and HL for vertical details, and HH for diagonal details make up the new system. The image is hierarchically represent by decomposing the LL sub band further to obtain various levels of information through iterations of decomposition [9].

Principal Component Analysis: For optimal security during embedding and extraction of medical images, Principal Component Analysis (PCA) can be utilize in reversible watermarking [5]. Here are the PCA algorithms for reversible watermark extraction and embedding.

4. Methodology

The Reversible Watermarking Process begins by inputting a medical image and converting it to grayscale before dividing it into blocks .To get the best watermark embedding, PCA (Principal Component Analysis) is used to get features from each block. The watermark is embedded into selected principal components and the blocks are reconstructed using inverse PCA. These reconstructed blocks are combined to form the watermarked image. A hash signature is also embedded for tamper detection, ensuring the process is fully reversible and secure.

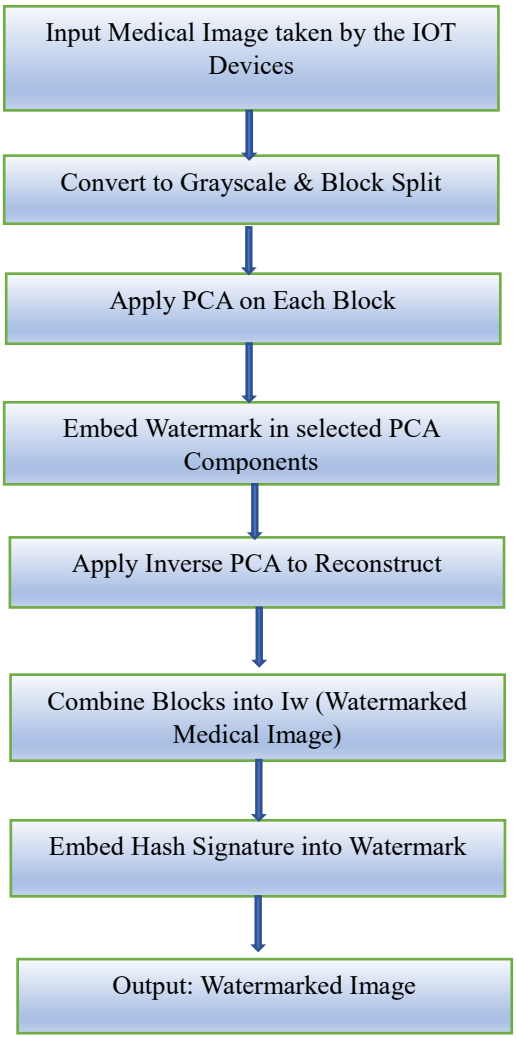


Figure 1. Flowchart of transforming input medical image to output watermarked image

4.1 Transforming input medical image to output watermarked image, the figure 1 has been proposed that comprises Embedding Algorithm using PCA and Extraction algorithm using PCA as follows.

Embedding Algorithm Using PCA:

1. **Input:** IoT-Based Image Acquisition:

a) Medical images are captured in real-time using IoT-enabled imaging devices (e.g., wearable scanners, mobile ultrasound units).
b) Images are transmitted to edge computing gateways or cloud servers for processing
c) Original medical image I, watermark W

2. **Pre-processing**:

a) Convert the image I into a grayscale image if it is in colour.
b) Sort the image into non-overlapping N×N sized chunks.
c) Images taken by the IoT edge device or gateway

3. **PCA Transformation**:

For each block Bi:

a) Compute the mean of the block.

b) Subtract the mean from each pixel in the block to get a zero-mean matrix $Ci=A^{T}iAi$.

c) Compute the covariance matrix $Ci=A^{T}iAi\_$

d) Perform eigen-decomposition of Ci to get eigenvalues and eigenvectors.

e) Form the principal components by projecting the zero-mean matrix Ai onto the eigenvectors.

4. **Watermark Embedding**:

a) Select a subset of principal components based on the largest eigenvalues (e.g., the first few principal components).

b) Embed the watermark W into the selected principal components by modifying their values. Ensure the modification is small to maintain image quality.

c) Combine the modified principal components with the unmodified ones.

5. **Inverse PCA**:

a) Reconstruct the block Bi using the modified principal components.

b) Add the mean back to each pixel in the reconstructed block.

6. **Reconstruction**: To make the watermarked image Iw, put together all the changed blocks.
7. **Output**: Watermarked image Iw.

Extraction Algorithm Using PCA:

1. **Input:** Watermarked image Iw

Pre-processing:

a) Convert the image Iw into a grayscale image if it is in colour.
b) In order to avoid overlapping, divide the image Iw into N×N portions.

2. **PCA Transformation**:

For each block Bi of the watermarked image:

a) Compute the mean of the block.

b) Subtract the mean from each pixel in the block to get a zero-mean matrix Ai.

c) Compute the covariance matrix $Ci=A^{T}iAi$

d) Perform eigen-decomposition of Ci to get eigenvalues and eigenvectors.

e) Form the principal components by projecting the zero-mean matrix Ai onto the eigenvectors.

3. **Watermark Extraction**:

a) Select the same subset of principal components that were used for embedding.

b) Extract the watermark W from the modified principal components.

4. **Inverse PCA**:

a) Reconstruct the block Bi using the extracted principal components.

b) Add the mean back to each pixel in the reconstructed block.

5. **Reconstruction**: Combining all the rebuilt blocks creates the recovered image Ir.
6. **Output**: Recovered image Ir , extracted watermark W.

4.2 The work process is broken up into three main parts: the Watermark Embedding Phase, the Watermark Extraction Phase, and the Tamper Detection and Integrity Check, that is explained as follows-

1. **Watermark Embedding Phase:**

Input: Original grayscale medical image and watermark taken by IOT Devices.

Step 1: Divide the image into non-overlapping blocks.

Step 2: Apply PCA to each block and extract principal components.

Step 3: Embed the watermark into the selected components (highest eigenvalues).

Step 4: Perform inverse PCA and reconstruct the image blocks.

Step 5: Reconstruct the complete watermarked image IwI_wIw.

Step 6: Generate a cryptographic hash of the original image.

Step 7: Embed the hash along with the watermark to support integrity verification.

2. **Watermark Extraction Phase:**

Input: Watermarked image.

Step 1: Divide the image into the same blocks.

Step 2: Apply PCA to retrieve the same principal components.

Step 3: Extract the watermark and embedded hash.

Step 4: Compare regenerated and extracted hash values to detect tampering.

Output: Recovered original image and extracted watermark.

3. **Tamper Detection and Integrity Check:**

a) Hash Matching: Comparing embedded and newly generated hashes from the image to detect any pixel-level tampering.
b) Result Interpretation: A mismatch indicates tampering in ROI or non-ROI areas.

4.3 Hash-Based Signatures for Tamper Detection

Generate unique hash values for watermarked images to confirm the images' integrity. Any alteration to the image will result in a mismatched hash, signalling tampering.

1. **Watermark Embedding Phase**:

a) **Generate Hash for Original Image**: Before embedding the watermark, generate a cryptographic hash for the medical image. The hash will act as a fingerprint for the image.

b) **Embed the Hash in the Watermark**: Embed the hash within the watermark using the PCA-based reversible watermarking method. This ensures that the hash inseparably tied to the image content.

c) **Watermark Insertion**: Insert the watermark containing both the traditional watermark (ownership or copyright information) and the hash signature using DWT and PCA as described in the proposed work.

2. **Watermark Extraction Phase**:

a) **Extract Watermark and Hash**: During watermark extraction, retrieve the watermark and extract the hash signature.

b) **Regenerate Hash**: Regenerate the hash of the current (watermarked) image.

c) **Compare Hashes**: Evaluate both the extracted and regenerated hashes. Once they are in an agreement, it means the picture has not been alter. Tampering is identify if they do not.

Hash-based signatures are lightweight and computationally efficient. Even the smallest change to the image (e.g., pixel value alteration) will result in a different hash, ensuring tamper detection.

5. Experimental analysis and Result

The work methodology has been implemented using Python Language. This work has been analysed by Digital imaging libraries for processing medical images and Cryptographic libraries for generating and comparing hash values.

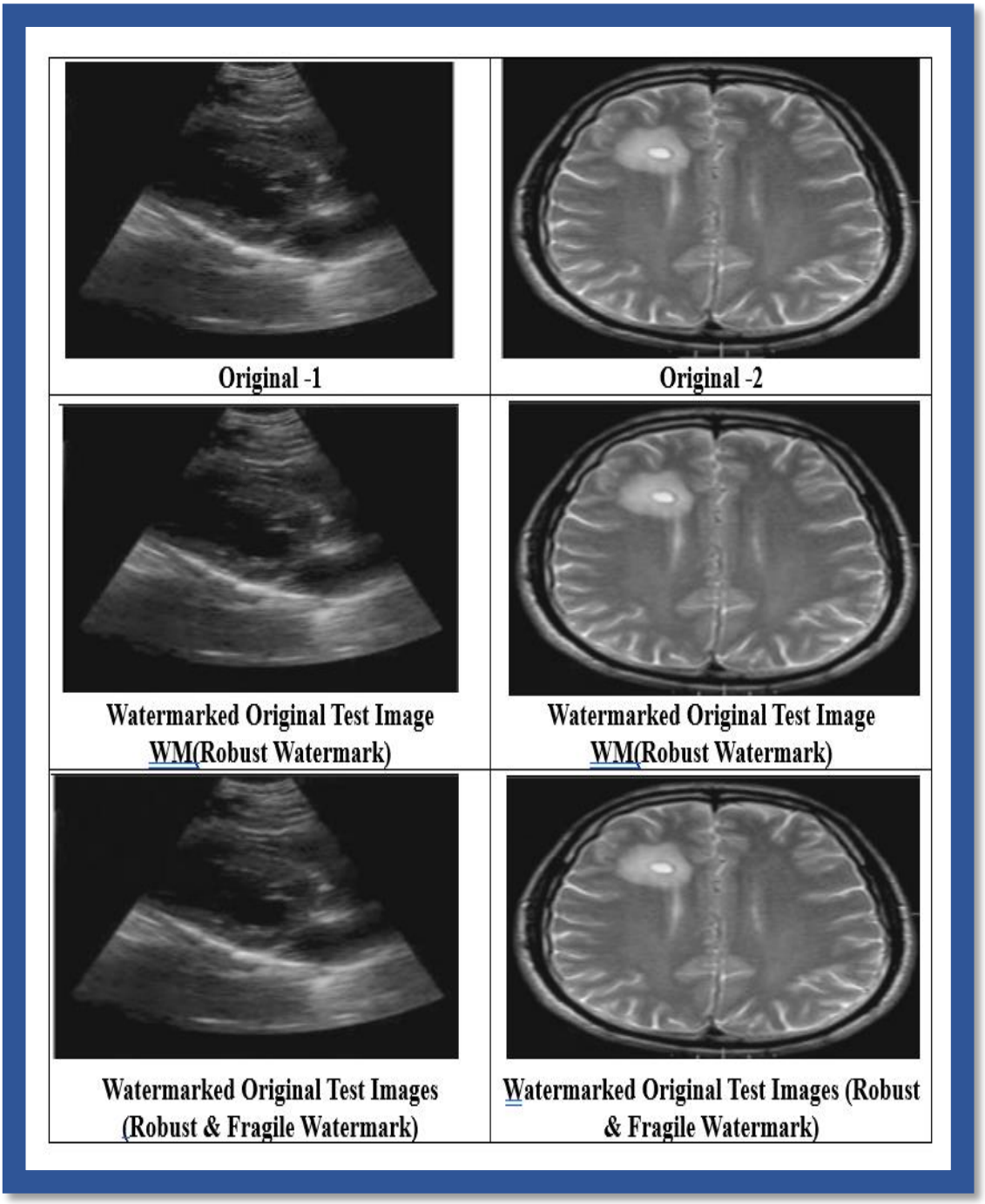


Figure. 2 sample of original images and watermarked images

The proposed scheme clearly illustrated and compared with previously suggested approach in table 1. A multifunctional reversible watermarking system capable of providing various watermarking capabilities is proposed as a means to achieve this goal with little capacity and PSNR loss.Many unique images were utilized in this experiment, but just a few are shown in Figure: 2. there includes a grayscale 60 × 60 watermark and 480 × 680 host pictures. Arranging the strong watermark into the host image comes first then arranging the delicate watermark with recovery data and signatures. Generated watermarked pictures after host image watermarking. These watermarked photographs were compared to their original hosts. Table 2 shows robust and robust & fragile watermarked images with PSNR values. Watermarks can be strong or fragile, thus "watermarked" (robust & delicate) means both.

Table 1: A comparison with the previously suggested approaches (YES=1, No=0)

Characteristics	Badshah et al [6]	Ansari et al [5]	Zear et al [9]	Liu et al [10]	Alshanbari et al [7].	Proposed
Nature	Fragile	Robust	Robust	Robust & Fragile	Robust & Fragile	Robust & Fragile
Original Images	Medical	ALL Type	Medical	ALL Type	Medical	Medical
Capacity	High	Extreme	Extreme	Medium	High	Extreme
Reversibility	Reversible	Irreversible	Irreversible	Irreversible	Reversible	Reversible
Ownership Verification	0	1	1	1	1	1
Tamper detection	1	0	0	1	1	1
PSNR	Extreme	Medium	High	High	High	High

The peak signal-to-noise ratio (PSNR) compares two images to their maximum value [11]. Images are same if PSNR is infinite; comparable if PSNR is more than 36 dB. Equation 1 calculates PSNR for an 8-bit grayscale picture. A well-liked metric for evaluating the efficacy of a restored picture after noise reduction, compression, or watermarking is the Peak Signal-to-Noise Ratio (4:1). A reversible watermark is one that, when erased, leaves no trace of the original image. To do this, you need to carefully plan how to embed the watermark into the image. In this case, PSNR is a useful way to compare the quality of the watermarked image to the original.

The formula for PSNR is:

$$PSNR=10\cdot\log_{10}(MAX^2/ MSE) \quad \text{……..(1)}$$

MAX: Highest pixel value within the image. For 8-bit grayscale images, this is 255.

MSE: Mean Squared Error is the average of the squared differences between the original and the watermarked (or reconstructed) images.

High PSNR: Indicates a low level of distortion. A high PSNR in reversible watermarking means that the watermarked image is almost the same as the original. [12].

Low PSNR: Indicates a high level of distortion, which might not be acceptable for certain applications, especially where quality of image is critical.

After adding both watermarks, Table 2 compares the PSNR value of the created host picture to the original image. Additionally, the PSNR of returned pictures (ROI) is infinite, indicating a match to the original test image. PSNR is high, indicating that watermarked host photos are almost identical to the original host [13-15]. Table 2 demonstrates the high imperceptibility of the suggested method. The original picture is totally reversible.

Table 2: PSNR of watermarked and obtained images of different original Images [8]

Test Images	Original Image 1	Original Image 2
Watermarked images (robust only)	49.20	48.53
Watermarked images (robust and fragile)	48.78	48.01
Retrieved images (ROI)	Similar to original image1	Similar to original image2

Table 3 displays the proposed scheme's resilience against various assaults. When comparing embedded and extracted watermarks, robustness is the metric to use. Normalized correlation (NC) is a robustness metric. With a robustness rating of 1, the extracted and embedded watermarks are identical. However, if the value is zero, it indicates that they are completely distinct from one another.

Table 3: The suggested scheme's robustness (NC) in the face of various attacks

Attacks	Original Image 1	Original Image 2
No attack	0.8012	0.8851
Average filtering (3x3)	.7287	.7060
Rescaling (0.6, 2)	.7706	.8104
Rescaling (2, 0.6)	.7972	.8699
Median Filtering (3 × 3)	.7656	.6884
JPEG Compression QF=90	.7510	.8392
JPEG Compression QF=70	.6146	.7542
JPEG Compression QF=50	.6936	.6915
Gaussian Low pass filter 3x3	.7941	.8604
Sharpening (0.9)	.7324	.6130

Table 4: Original watermark and Extracted watermarks from Original Image-1, Original Image-2 after 10 different attacks

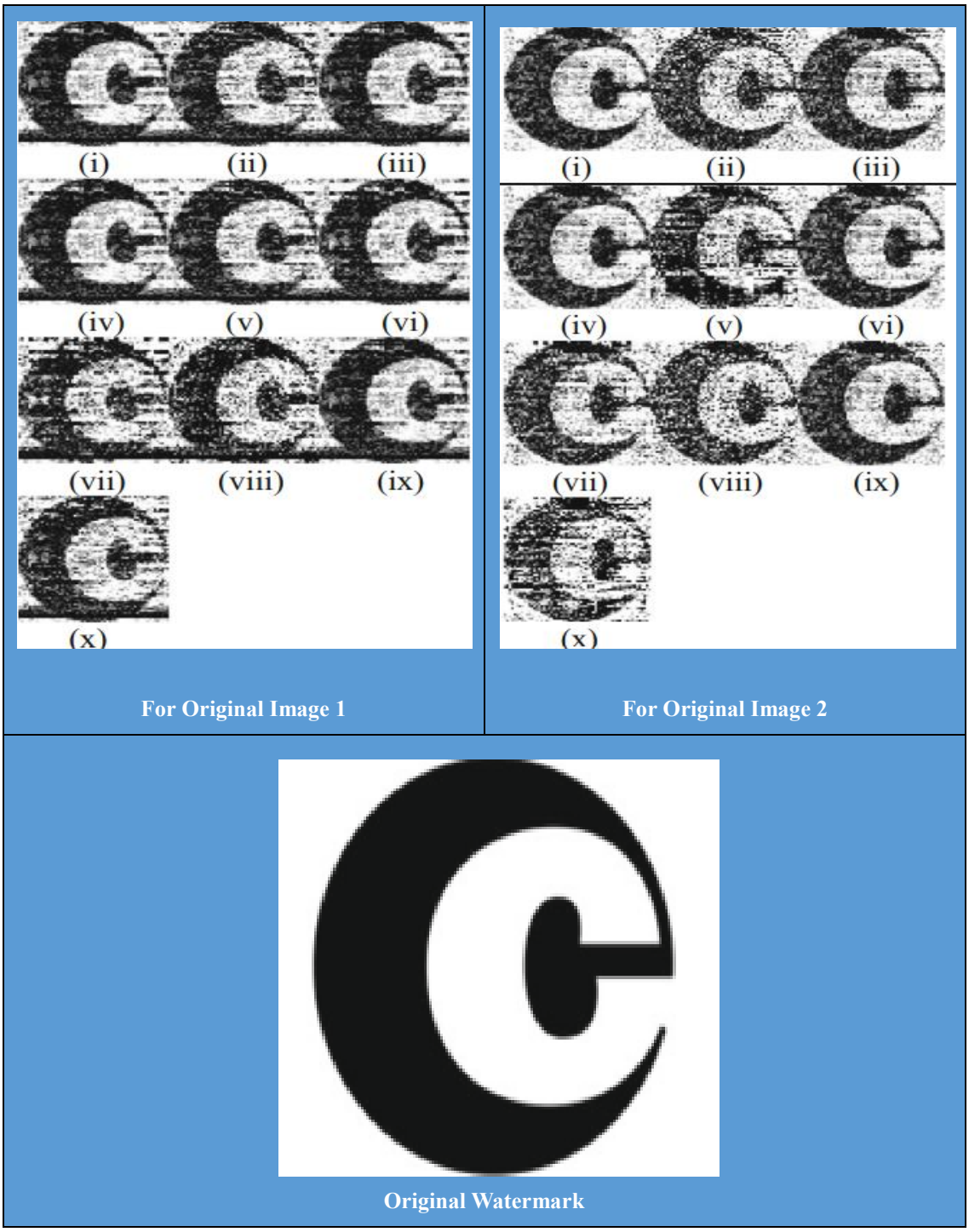


Table 5: Multiple Medical Images

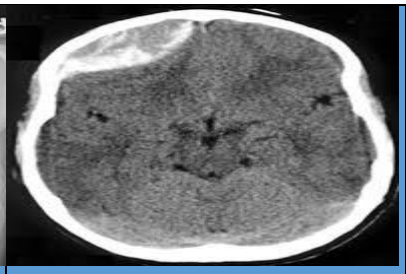
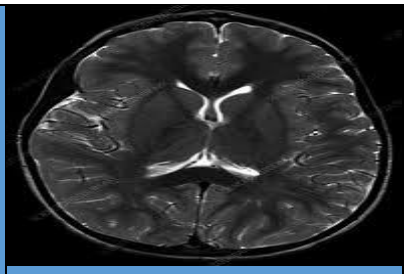
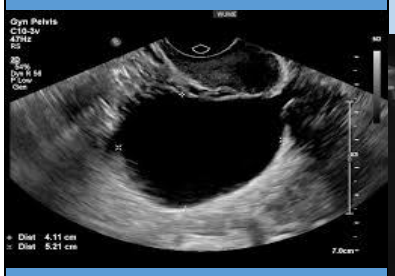
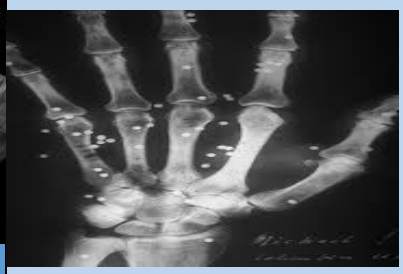
		
X-ray Image 1	CT Scan Image 2	MRI Image 3
		
Ultrasound Image 4	X-ray Image 5	CT Scan Image 6
		
MRI Image 7	Ultrasound Image 8	X-ray Image 9
		
CT Scan Image 10		

Table 6: Representing the results of applying Hash-Based Signatures for tamper detection on medical images

Test Image	Tampering Type	Hash Algorithm	ROI (Region of Interest)	Non-ROI	PSNR (dB)	Tamper Detected in ROI?	Tamper Detected in Non-ROI?	Hash Match (ROI)	Hash Match (Non-ROI)	Detection Accuracy
X-ray Image 1	No tampering	SHA-256	Original	Original	51.30	No	No	Match	Match	100%
CT Scan Image 2	Pixel modification in ROI	MD5	Modified	Original	40.12	Yes	No	Mis match	Match	98%
MRI Image 3	Noise addition in Non-ROI	SHA-1	Original	Modified	45.78	No	Yes	Match	Mis match	99%
Ultrasound Image 4	Cropping in ROI	SHA-512	Modified	Original	39.24	Yes	No	Mis match	Match	97%
X-ray Image 5	JPEG compression (90%)	MD5	Original	Compressed	44.89	No	Yes	Match	Mis match	98%
CT Scan Image 6	Resizing (whole image)	SHA-256	Modified	Modified	38.75	Yes	Yes	Mis match	Mis match	96%
MRI Image 7	Rotation in ROI	SHA-512	Modified	Original	41.10	Yes	No	Mis match	Match	97%
Ultrasound Image 8	Scaling (Non-ROI)	SHA-1	Original	Modified	43.50	No	Yes	Match	Mis match	98%
X-ray Image 9	JPEG compression (50%)	MD5	Original	Compressed	42.30	No	Yes	Match	Mis match	97%
CT Scan Image 10	Noise addition (ROI)	SHA-256	Modified	Original	39.85	Yes	No	Mis match	Match	97%

Hash Algorithm: The specific hash function used for generating the signature (MD5, SHA-1, SHA-256, and SHA-512).

PSNR (Peak Signal-to-Noise Ratio): Tests the image's quality following manipulation. A better PSNR indicates little distortion.

Tamper Detected in ROI: Indicates whether tampering was detected in the Region of Interest (ROI).

Tamper Detected in Non-ROI: Indicates whether tampering was detected in non-ROI areas. Hash Match (ROI): Indicates whether the hash signature of the ROI matches the original image (Match/Mismatch) [16].

Hash Match (Non-ROI): Indicates whether the hash signature of the non-ROI matches the original image (Match/Mismatch).

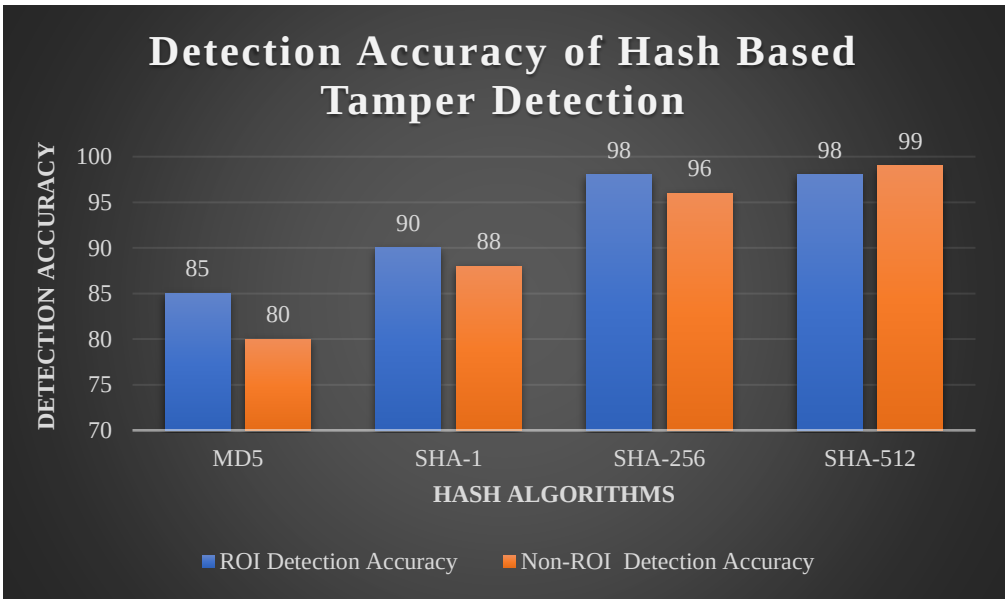


Figure 3. Detection Accuracy of Hash Based Tamper Detection

In above shown graph the detection accuracy of Hash Based Tamper detection for ROI and Non-ROI area using different Hash algorithms .In SHA-256 and SHA-512 gives highest accuracy rather than MD5 but MD5 is more effective.

Detection Accuracy: The overall accuracy of tamper detection using hash-based signatures for both ROI and non-ROI areas and here we observed that MD5 hash, while faster, can still detect tampering effectively, though it is more vulnerable to collisions [17-22]. SHA-256 and SHA-512 provide higher security and better tamper detection for medical images, especially in detecting changes in both ROI and non-ROI areas.SHA-1, though still effective, is consider less secure than SHA-256 and SHA-512, especially for tampering in high-stakes medical images. Hash-based tamper detection works well with image manipulations like pixel modifications, resizing, and compression, achieving high detection accuracy. PSNR values drop as the tampering intensity increases, but high detection accuracy is maintained, especially in ROI areas [23-27].

6. Conclusion

In this research, we strongly proposed an IoT-enabled reversible watermarking framework for safeguarding medical images transmitted through smart healthcare systems. Our method combines Hash-Based Signatures (HBS) with Principal Component Analysis (PCA) and Discrete Wavelet Transform (DWT). This makes sure that medical images taken with IoT devices are safe from unauthorized changes and can be perfectly restored to their original form. The system lets edge-based IoT devices, like remote diagnostic tools and wearable scanners, send images securely and in real time, while keeping the images' accuracy and integrity high. Using cryptographic hash functions like SHA-256 and SHA-512 makes it possible to reliably find even the smallest changes in both ROI and non-ROI areas, which keeps patient data safe. Performance metrics like high PSNR and Normalized Correlation values show that our watermarking process keeps high visual fidelity and is strong against common attacks when sending data over the Internet of Things (IoT). This watermarking technique can be used in an IoT healthcare setting to make telemedicine and remote diagnostic systems more trustworthy. It is scalable, secure, and reversible. This method lays a strong groundwork for keeping private health information safe in the new world of smart, connected medical ecosystems.

Overall, the combination of PCA, DWT, and HBS in this research provides a comprehensive solution to the dual challenge of protecting medical images from unauthorized access and manipulation while maintaining their diagnostic value. This method holds promise for enhancing security in the increasingly digitized healthcare sector.

7. Future Scope

The combination of IoT opens up new ways to improve safe medical image watermarking. Edge computing can be used in the future to watermark IoT devices in real time. You can use machine learning to improve watermark embedding without losing image quality. Low-power IoT hardware needs algorithms that are light and use little energy. You can use the method with IoT-based scanners to support 3D and high-resolution images. Robustness should be tested against changing cyber threats that target IoT healthcare systems. Using resource-aware methods for fast, reliable processing can make scalability better. In distributed IoT networks, block chain integration can add tamper-proofing that can't be changed. More advanced cryptographic hashes can help find tampering more accurately. This method could become the most important part of safe, smart, and connected healthcare systems.

References

[1] J. Tian, "Reversible watermarking by difference expansion," in *Proc. Workshop on Multimedia and Security*, vol. 19, Juan-les-Pins, France, Dec. 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] Z. Zhang, H. Sun, S. Gao, and S. Jin, "Self-recovery reversible image watermarking algorithm," *PLoS One*, vol. 13, no. 6, e0199143, 2018.

[4] D. M. Thodi and J. J. Rodríguez, "Expansion embedding techniques for reversible watermarking," *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721-730, 2007.

[5] I. A. Ansari and M. Pant, "Quality assured and optimized image watermarking using artificial bee colony," *Int. J. Syst. Assur. Eng. Manag.*, vol. 9, pp. 274-286, 2018.

[6] G. Badshah, S. C. Liew, J. M. Zain, and M. Ali, "Watermark compression in medical image watermarking using Lempel-Ziv-Welch (LZW) lossless compression technique," *J. Digit. Imaging*, vol. 29, pp. 216-225, 2016.

[7] H. S. Alshanbari, "Medical image watermarking for ownership & tamper detection," *Multimedia Tools Appl.*, vol. 80, no. 11, pp. 16549-16564, 2021.

[8] A. Dixit, R. P. Agarwal, and B. K. Sharma, "Human Visual System-inspired Hybrid Image Watermarking for IP Protection and Provenance," *Int. J. Contemp. Res. Eng. Technol.*, pp. 20-26, Jan.-Dec. 2023.

[9] A. Zear, A. K. Singh, and P. Kumar, "A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine," *Multimedia Tools Appl.*, vol. 77, pp. 4863-4882, 2018.

[10] X. L. Liu, C. C. Lin, and S. M. Yuan, "Blind dual watermarking for color images' authentication and copyright protection," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 5, pp. 1047-1055, 2016.

[11] R. Noor, A. Khan, A. Sarfaraz, Z. Mehmood, and A. M. Cheema, "Highly robust hybrid image watermarking approach using Tchebichef transform with secured PCA and CAT encryption," *Soft Comput.*, vol. 23, pp. 9821-9829, 2019.

[12] M. Ramzan, M. Habib, and S. A. Khan, "Secure and efficient privacy protection system for medical records," *Sustainable Comput.: Informatics Syst.*, vol. 35, p. 100717, 2022.

[13] A. Bhatnagar, A. Giri, and A. Sharma, "Anomaly Intrusion Detection System Based On RNN-LSTM For Cyber-Attack Classification," in *2024 OPJU Int. Technology Conf. (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0*, Raigarh, India, 2024, pp. 1-5. doi: 10.1109/OTCON60325.2024.10687401.

[14] Y. Liu, Y. Zhang, and J. Wang, "A novel approach for reversible watermarking in medical images using adaptive histogram equalization," *Multimedia Tools and Applications*, vol. 82, no. 15, pp. 22247-22268, 2023. doi: 10.1007/s11042-023-13596-2.

[15] F. N. Lang, J. L. Zhou, S. Cang, H. Yu, and Z. Shang, "A self-adaptive image normalization and quaternion PCA based color image watermarking algorithm," *Expert Syst. Appl.*, vol. 39, no. 15, pp. 12046-12060, 2012.

[16] H. Shi, Y. Wang, Y. Li, Y. Ren, and C. Guo, "Region-based reversible medical image watermarking algorithm for privacy protection and integrity authentication," *Multimedia Tools Appl.*, vol. 80, pp. 24631-24667, 2021.

[17] I. H. Pan, H. M. Ko, D. L. Cheng, T. H. Chen, Y. Y. Chen, and Y. C. Lee, "Reversible and Robust Watermarking Technique," in *2021 IEEE Int. Conf. Consumer Electronics-Taiwan (ICCE-TW)*, pp. 1-2, 2021.

[18] P. Pal, P. Chowdhuri, and T. Si, "A novel watermarking scheme for medical image using support vector machine and lifting wavelet transform," *Multimedia Tools Appl.*, vol. 82, no. 26, pp. 41187-41206, 2023.

[19] R. Bouarroudj, F. Souami, F. Z. Bellala, and N. Zerrouki, "A reversible fragile watermarking technique using Fourier transform and Fibonacci Q-matrix for medical image authentication," *Biomed. Signal Process. Control*, vol. 92, p. 105967, 2024.

[20] A. Dey, P. Chowdhuri, and P. Pal, "Integer wavelet transform based watermarking scheme for medical image authentication," *Multimedia Tools Appl.*, pp. 1-22, 2024.

[21] X. Zhou, Y. Ma, Q. Zhang, M. A. Mohammed, and R. Damaševičius, "A reversible watermarking system for medical color images: balancing capacity, imperceptibility, and robustness," *Electronics*, vol. 10, no. 9, p. 1024, 2021.

[22] M. V. Malayil and M. Vedhanayagam, "A novel image scaling based reversible watermarking scheme for secure medical image transmission," *ISA Trans.*, vol. 108, pp. 269-281, 2021.

[23] Z. Dai, C. Lian, Z. He, H. Jiang, and Y. Wang, "A novel hybrid reversible-zero watermarking scheme to protect medical image," *IEEE Access*, vol. 10, pp. 58005-58016, 2022.

[24] N. Krishnamoorthi and V. K. Chinnababu, "Hash and Prediction-Error-Based Reversible Watermarking for Medical Images," *Fluctuation Noise Lett*, vol. 21, no. 01, p. 2250007, 2022.

[25] A. Avinashiappan, B. Mayilsamy, and J. Hemanth, "Security enhanced ROI based reversible watermarking for medical images," *DYNA-Eng. Ind.*, vol. 97, no. 2, 2022.

[26] L. Gao, Y. Zhang, and G. Li, "Reversible watermarking in medical images using sub-sample and multiple histogram modification," *J. Inf. Technol. Res.*, vol. 13, no. 4, pp. 75-90, 2020.

[27] T. Dutta, R. Bagi, and H. P. Gupta, "Robust reversible watermarking for grayscale medical images," in *Advances in Data and Information Sciences: Proc. ICDIS 2019*, Springer Singapore, pp. 613-622, 2020.