MACHINE INTELLIGENCE RESEARCH
ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

SECURE SEMI-FRAGILE WATERMARKING: ENHANCING TAMPER DETECTION, LOCALIZATION, AND RECOVERY WITH CRYPTOGRAPHIC ALGORITHMS

Alina Dash
Department of Computer Science & Engineering, VSSUT, Burla, Odisha, India
*Email: alinadash_cse@vssut.ac.in
ORCID ID:0000-0002-2093-050X

Sanjib Kumar Nayak,
Department of Computer Science & Engineering, VSSUT, Burla, Odisha, India
Email: sknayak_ca@vssut.ac.in

Atul Vikas Lakra
Department of Computer Science & Engineering, VSSUT, Burla, Odisha, India
Email: atul.cs@gmail.com

Alina Mishra,
School of Computer Sciences, VSSUT, Burla, Odisha, India
Email: alinamishra88@gmail.com

Abstract
The use of digitized medical imagery, rich with patient health information, significantly aids in diagnostic procedures. However, the integrity of these images is paramount, as even slight variations can lead to misdiagnosis and adversely affect subsequent treatment by healthcare practitioners. Consequently, robust protection mechanisms are essential to guard against intentional manipulations such as compression, filtering, or forgery, as well as unintentional tampering and other forms of attack, thereby preserving the authenticity of these critical images. This study details a semi-fragile image watermarking methodology that employs a hash function-derived watermark for application to 512×512 grayscale host medical images. The method begins by dividing the host image into two separate regions: the Region of Interest (ROI) and the Region of Non-Interest (RONI). A fragile watermark is produced by performing the Lifting Wavelet Transform (LWT) on the RONI. This watermark is then embedded within the RONI of an image that has already been robustly watermarked, using the Least Significant Bit (LSB) replacement method.. Upon receipt, the authenticity of the watermarked image is validated, and any attacks are identified through a tamper detection process. Furthermore, a cryptosystem secret key is derived from specific coefficients using the Hybrid Chaotic Magic Transform (HCMT). The watermark itself is computed within blocks by permuting the six Most Significant Bits (MSBs) of each pixel. For every block, the Discrete Wavelet Transform (DWT) is applied to extract DC coefficients. Tampering or forgery is detected by comparing these extracted keys with the generated keys. For watermark localization, the arithmetic mean of a designated block and the Maximum Pixel Intensity (MPI) within that block are utilized. Additionally, the Lempel-Ziv-Welch (LZW) algorithm is implemented to compress the recovery data pertaining to the host image's ROI. The efficacy of this proposed method is systematically evaluated using Matlab

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

software. The findings demonstrate that the proposed work achieves high accuracy in tampering detection, maintains good imperceptibility of the watermark, and exhibits robustness against a variety of watermarking attacks. The scheme's robustness and fragility characteristics are quantified using Normalized Cross- Correlation (NC), Bit Error Rate (BER), and Peak Signal-to-Noise Ratio (PSNR). As a result, the developed system can accurately localize and detect tampering incidents and is also capable of recovering the tampered regions of the images.
Keywords: Semi-Fragile Robust Watermarking, Medical Image, ROI, RONI, Lifting Wavelet Transform, Hybrid Chaotic Magic Transform, Discrete Wavelet Coefficient, Lempel-Ziv-Welch, Tamper Detection and Localization.

Introduction

Due to the advancement of multimedia schemes and the internet, digital content has been concerned a lot of attention. In multimedia technologies, digital image manipulation, replacement, distribution and regeneration are simple, low-cost, and rapid [1]. With the extensive use of digital data and the Internet, infringements of intellectual property rights, such as illicit usage, copying, and digital content theft are becoming more common. Digital images are high-value-added content, which necessitates the protection of their intellectual property rights [2]. Consequently, to protect the digital content, embedded a watermark or secret image to the content of the owner's information which is then saved or distributed. The watermarking scheme is used for ownership assert by extracting the embedded watermark data extraction when needed. Various digital watermarking approaches have been developed based on the technologies in use, the application field, and other factors [3]. Copyright notice or another message can be added to digital media via digital watermarking technology. Based on the watermark embedding strategy, the watermarking approach is categorized into frequency and spatial domain techniques [4]. Researchers working in digital watermarking have met significant obstacles in designing new algorithms that may serve a variety of watermarking applications while also resisting a variety of multimedia attacks.

Digital Image Watermarking in Medical Images

A large number of pixels are combined to create a digital image and the spatial domain watermarking strategy is applied directly to the image pixels [5]. When the transform domain watermark approach is employed, the coefficient can be changed using various techniques such as DWT, discrete cosine transforms (DCT), discrete Fourier transform (DFT), etc. Recently, watermarking methods using Singular Value Decomposition (SVD) alter the image's single value and insert it into the carrier image directly. This approach is insufficiently secure, and watermarks have a significant negative influence on image quality [6]. Watermarking usually necessitates the employment of many techniques, depending on the application. Every technique has advantages and disadvantages. Because many colour spaces like YCbCr, YUV, and others are accessible, watermarking can be done in any of them. Instead of traditional watermarking methods have significant limits when it comes to medical images (MI) [7]. However, to enhance the performance, hybrid domain-based watermarking schemes were developed. The process for integration is based on a DWT-SVD, DWT-DCT, DWT-DCT-SVD and DWT-DFT [8-9]. Digital watermarks must meet the characteristics of imperceptibility, capacity and robustness. In

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

addition, any of the attacks should not remove the watermarking technology and should not have its quality impaired in the event of an attack. Furthermore, develop numerous digital watermarking strategies for improving the robustness of watermarking to resist geometric attacks [10]. The general study has been accompanied in recent years by the use of mathematical tools and the formulation of theoretical schemes for developing an efficient watermarking approach. Though, there is still a gap in practical implementations, as using complex image transformation schemes or complex encryption algorithms to improve security leads to needlessly high operation costs and computational complexities [11].

Semi-Fragile Watermarking Techniques

Semi-fragile Watermarking is the most commonly used technique for authenticating confidential data as it is tolerant of incidental changes to the data and in a noisy environment, it is sensitive to deliberate changes [12]. The original image features a watermark in the wavelet coefficients of the image hide by most of the present-day semi-fragile watermarking techniques. Yang and Sun by adding a human visual process to generate the watermark. Some techniques quantized the wavelet coefficients to hide the watermark. For example, the DWT coefficients from the second-level decomposition of the cover image were quantized for embedding the watermark [13]. One selected approximation coefficient of the non-overlapping low-frequency block of DWT is quantized, and with tamper localization, the image content is authenticated by a semi-fragile watermarking system proposed by several authors [14]. Although it doesn't deliberate the tampered RONI (region of non-interest) case, acceptable results in terms of multiple features and parametric values are presented in this scheme. Because the Region of Interest (ROI) recovery and the authentication depend on the reliability of the extracted information, in the tampered RONI case, the authenticity or reliability of the extracted data should have been investigated. However, the work concentrated on the JPEG attack and no deep analysis was provided to evaluate other types of attacks [15]. Further to enhance the semi-fragile watermarking strategy, this work proposed a new robust watermarking scheme. The remaining part of the work is structured as follows, section 2 illustrates the proposed literature survey of the work, section 3 portrays the problem statement and motivation of the work, and section 4 demonstrates the proposed research methodology. Section 5 reveals the experimentation and result discussion, and section 6 depicted the research conclusion.

Literature Review

Network security has steadily become a potentially major challenge in the information era, especially in this medical profession field, where image accuracy and safety are critical, and patient information must be included with nominal change. Henceforth, Li et al [16] had been proposed an integrated log-polar transform (LPT) and DCT for medical images. It was discovered that there was lossless integration of patient data into medical images. It overcomes the faults produced by the standard watermark embedding scheme, which modifies the original image data, and ensures the quality of medical images by using a zero-watermarking strategy. The algorithm's effectiveness was demonstrated by the positive experimental findings. However, different types of watermarking attacks are handled by proposing a hybrid DWT-SVD approach for watermarking embedding and extraction by Ali Alzahrani et al [17]. The host image was

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

embedded in four levels using the DWT technique and the fourth level was processed by the SVD approach. The proposed DWT-SVD obtained superior accuracy in finding the various attacks, according to the experimental results.

To protect the copyright protection of digital colour images requires a colour image watermarking method. Based on the decomposition of QR, an enhanced colour image watermarking approach for colour image matrix is introduced by Nha et al [18] to achieve this goal. Instead of using the Gram-Schmidt technique for QR factorization, the suggested method provides a novel strategy for finding elements of Q and R matrices. Moreover, the execution time has been greatly reduced, and the secret key has been made more resistant to some of the attacks that have been tested. The synchronisation signal is not currently included in the watermarking technique, resulting in very low performance for embedded images in terms of imperceptibility, robustness and anti-attack ability. Subsequently, SVD and scrambling-based watermarking were proposed by Lei Pei et al [19]. Encryption and dimension reduction are used to pre-process the digital watermark which is processed in portions and inserted in the synchronisation signal. The concept of sound channel low-frequency energy ratio was utilized for watermark image embedding into the host image after extraction is performed.

When embedding a watermark message in Asset Medical Images (AMI), extra caution is required since more information may impair the AMI quality, and changes in AMI grey levels may obstruct its interpretation. To address this issue, Tayel et al [20] proposed a hybrid encoded and adapted tuned neural network (TNN) for AMI watermarking. To eliminate visual portions in the low-frequency coefficient and noise and attacks in the high-frequency, embedding is conducted into the middle frequency coefficients of the AMI's DCT. This improves image robustness and capacity when compared to the spatial domain. Integrity and self-embedded image verification system were introduced by Alhumyani et al [21]. First, the images are split into separate segments with identical block sizes. Then, distinct ABW (Analytic Beta-Wavelet) orthogonal filters are used to implant a self-segment watermark for the image segment. Under various block sizes, predict the coefficients of ABW orthogonal filter to enhance image reconstruction. To get over the PC's mobility constraints, Hosny et al [22] utilized embedded devices like the Raspberry Pi. The images in the colour of the Quaternion Legendre-Fourier Moment in polar coordinates are used to construct a parallel robust watermarking algorithm on the Raspberry Pi (RPi) platform using parallel computing. In the host image, embedding the secret image which provides better results, and it is presented by utilizing the binary Arnold scrambling approach.

The grey wolf optimizer, which is used in DCT-based watermarking, could help in the quest for an optimum balance between robustness and imperceptibility. Moreover, Hu et al [23] investigated the feasibility of employing a Denoising Autoencoder (DAE) to improve the extracted watermark imperceptibility. The introduced DAE was found to be capable of reducing the bit error rate by 60%, resulting in a more visually recognisable recovered watermark. Based on chaotic sequence and Schur decomposition, Abdallah Soualmi et al [24] suggested a blind watermarking approach for medical photographs (CS). To produce encrypted images separated into sub-blocks, an efficient chaotic approach is used for the watermark and the cover image. The encrypted watermark bits are included in the cyphered cover image blocks via a Schur decomposition. The original watermark is extracted using the same CS. The testing findings show

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

that this technique delivers adequate image quality and robustness.

Sinhal et al [25] proposed a multipurpose MI watermarking technique that includes copyright protection, tamper localization and various segments of RONI, and ROI self-recovery with 100% reversibility. The ROI of the host image's recovery information is compressed using the Lempel-Ziv-Welch technique at first. After that, a transform domain-based embedding module is used to implant the watermark into the input image. The watermarking approach's effectiveness has been verified in terms of SSIM (Structural Similarity Index Measure) and PSNR (Peak Signal-to-Noise Ratio) was applied to compute the imperceptibility and Normalization Correlation (NC) employed to examine the watermarked images' robustness

.Zhao et al. [26] proposed a proactive framework for image manipulation detection using a deep semi-fragile watermarking technique. This integrates deep learning with semi-fragile watermarking to detect and localize manipulations with high precision, designing watermarks resistant to benign operations but sensitive to malicious edits.

Amrullah et al. [27] introduced TDSF, a two-phase tamper detection strategy within a semi-fragile watermarking framework using the two-level Integer Wavelet Transform (IWT). Their method aims to distinguish between legitimate modifications and malicious alterations, enhancing precision through combined watermark embedding and robust analysis, improving detection accuracy and localization granularity while preserving image fidelity.

Background Study

The swift evolution of information technology has spurred a growing need for telemedicine within the medical sector, resulting in a significant rise in the online transmission of medical images and associated data. These images frequently hold sensitive patient data requiring strict preservation against alteration, and meticulous attention is necessary to avoid unintentional breaches of patient confidentiality. As a result, developing effective information protection strategies for medical imagery has emerged as a crucial research focus. Against this backdrop, digital watermarking technologies have become a prominent method for ensuring information security and protecting copyright in the digital sphere. Specifically within the medical image domain, digital watermarking algorithms are increasingly utilized to bolster the safety and accuracy of medical visuals, reduce the risk of medical data manipulation, and safeguard patient privacy. Fragile watermarks, in particular, have gained traction for their utility in authenticating image data integrity and for copyright assertion.

Both fragile and semi-fragile watermarking techniques are frequently employed to guarantee the integrity and authenticity of image data. By fusing the advantages of robust and fragile watermarking techniques, semi-fragile watermarks provide a hybrid solution. They are especially good at spotting image manipulation and allowing for flexible (fuzzy) digital image identity authentication. Given that pictures and videos are frequently saved and sent in compressed formats, semi-fragile watermarking is particularly pertinent because it is made to resist compression without deteriorating. However, the watermark will probably be impacted if the image is altered without authorization, indicating tampering. Semi-fragile watermarking has been used in many earlier studies by embedding the watermark data in the spatial or transform (frequency) domains of images and videos, frequently using pipelines for processing that were manually created.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

However, key drawbacks of conventional methods include the prominance of embedded watermarks and increased distortions in result images, particularly when compression techniques are applied, leading to diminished robustness. Furthermore, many existing works have not been specifically engineered to address the fragility requirements pertinent to medical images. This gap serves as the primary motivation for the current study, which aims to introduce a robust semi-fragile watermarking algorithm specifically tailored for tamper detection, precise localization of alterations, and subsequent image recovery.

Proposed Research Methodology

In the current information age, network security presents a significant and growing challenge, particularly within the medical field. Here, the precision and integrity of images are paramount, and any inclusion of patient information must be done with minimal alteration to the diagnostic content. Medical images and associated reports constitute vital data that heavily influences subsequent clinical decisions and treatment outcomes. Unauthorized modifications to digital data, such as medical imagery, whether because of signal processing attacks or deliberate tampering by malicious actors, can severely compromise the diagnostic process, thereby endangering patient safety. The integration of watermarking with encryption techniques can enhance both the embedding capacity and overall security; however, this combination often disrupts the delicate equilibrium between execution speed, system robustness, and overall operational complexity. Therefore, this research introduces an efficient and robust image watermarking methodology specifically designed for medical images. To ensure content integrity, a semi-fragile watermark is employed within the digital images, enabling the localization of any tampered regions. The fundamental workflow of this research is depicted in Figure 1.

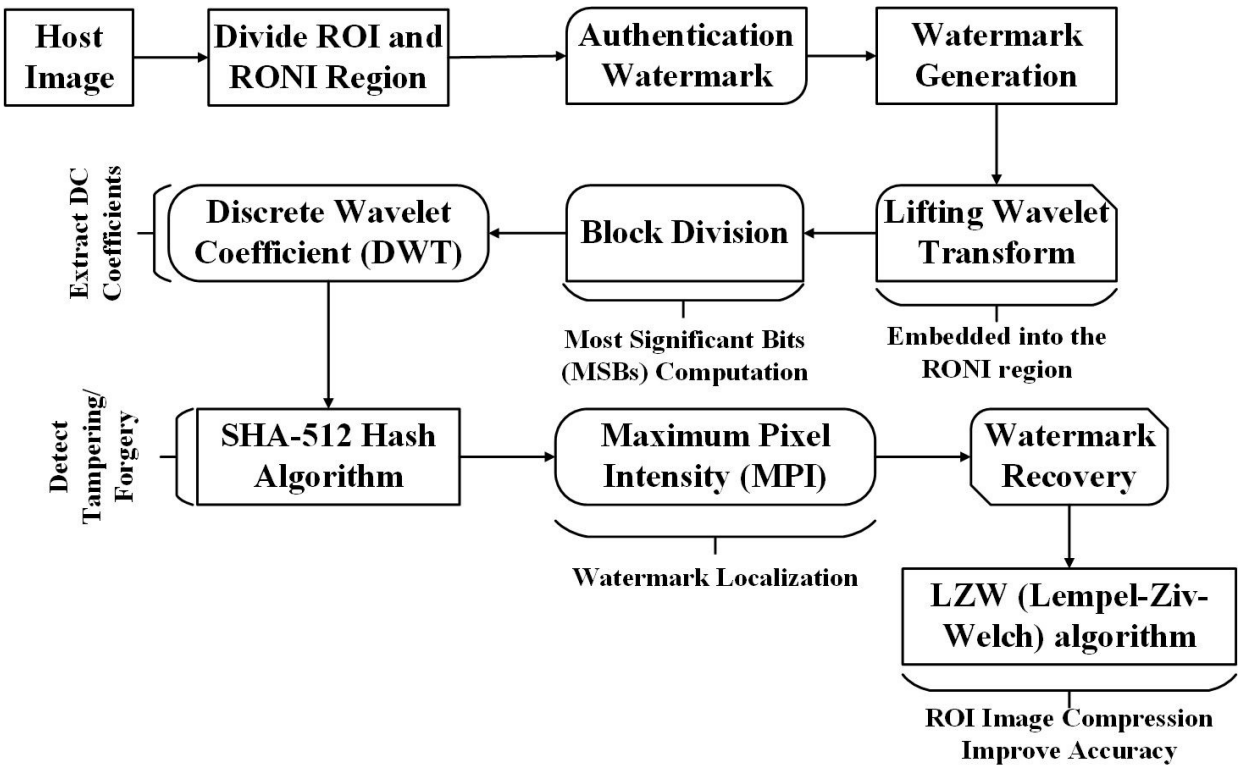


Figure 1: Process Flow Diagram of The Research Work

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

This study puts forth a novel watermarking technique designed for the detection and recovery of tampered medical images, leveraging a semi-fragile approach that incorporates Lifting Wavelet Transform (LWT) and hash functions. The proposed method aims for complete reversibility and encompasses functionalities for tamper detection across both Region of Interest (ROI) and Region of Non-Interest (RONI), alongside watermark embedding, extraction, and the recovery of ROI regions should tampering be identified. Tamper detection is managed using the Hybrid Chaotic Magic Transform (HCMT), while the localization of tampered areas is achieved through Maximum Pixel Intensity (MPI) analysis. A recovery tag, generated from the recovery watermark, is created using the Lempel-Ziv-Welch (LZW) algorithm. This tag is then transmitted to the receiver along with the watermarked image to facilitate restoration.

Watermark Generation

This study develops two primary types of watermarks: a recovery watermark and an authentication watermark. The process begins by segmenting the grayscale host medical image into distinct Region of Non-Interest (RONI) and Region of Interest (ROI) areas. Subsequently, the Lifting Wavelet Transform (LWT) domain is utilized to generate the authentication watermark, which is then embedded into the image destined to become the watermarked image. Following this, the watermarked image (or a precursor to it) is divided into 2×2 blocks. A 10-bit recovery watermark is generated for each block using a proposed DWT-based recovery watermark generation technique. This resulting fragile watermark is then embedded into the RONI portion of the robustly watermarked image through a Least Significant Bit (LSB) replacement methodology.

Lifting Wavelet Transform (LWT) Domain

LWT is a powerful tool for image analysis due to its more efficient and faster implementation compared to traditional wavelet transforms. The fundamental concept behind lifting wavelets is the design of new wavelets with improved features, starting from a basic wavelet. In this scheme, the watermark is dynamically embedded within LWT coefficients, and a secret key is utilized to enhance the system's security. The proposed method's security and robustness are further strengthened by factorization when combining LWT coefficients and significant variance.

LWT transforms an image into the frequency domain and is recognized as the fastest wavelet transform. At each level, LWT employs split and merge operations instead of the upsampling and downsampling used in conventional DWT. The parallel processing of poly-phase components by wavelet filters in LWT typically produces better results than the DWT approach.

The LWT algorithm simplifies reversibility as it operates directly in the integer domain. Signal decomposition in LWT is achieved through three steps: prediction, splitting, and updating.

Split: The given signal $S\ (n)$ is divided into non-overlapping odd $So(n)$ and even $Se(n)$ samples as:

$$S_e(n) = S\ (2n),\ S_O(n) = S\ (2n + 1) \quad (1)$$

(1) Predict: To predict each other if they are correlated by abstracting the difference, the samples obtained in the previous step can be used. The value of $G\ (n)$ can be calculated as:

$$G\ (n) = S_O(n) - P\ [S_e(n)] \quad (2)$$

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

Where, the predict operator is denoted as P $[Se(n)]$, and G (n) are the high-frequency component which is used for the description of error between the sample value originally taken and the value which is predicted.

Update: To reconstruct the abstract difference G (n), the update operator U $[G$ $(n)]$ is used to update the even samples $Se(n)$, it represents the low-frequency component L (n) which is a coarse approximation signal value S (n) taken originally as specified in the following equation:

$$\mathrm{L}\ (n) = S_e(n) + U\ [G\ (n)] \quad (3)$$

(b)Watermark Embedding Algorithm (using LWT)

The proposed digital image watermarking algorithm utilizes the significant differences calculated between LWT coefficients. Lifting wavelet coefficients are employed for embedding watermark bits. The selected image is initially transformed using three levels of LWT. The LH3 sub-band is identified as most suitable for binary watermark embedding compared to the LV3 sub-band.

Eight non-overlapping coefficients from the LH3 sub-band are grouped to form a single block. An initial secret seed value (Key2) is then used to shuffle these blocks. Within each block, the difference between the two maximum coefficients is estimated and considered a significant distinction. Watermark bits are subsequently shuffled randomly, similar to previous steps but using a different seed value (Key1). Security is implemented via a pseudo-random permutation technique based on block values. This technique is optimal for altering the order in which blocks are watermarked. Embedding watermark bits into the selected sub-band changes the block locations but does not require additional information beyond the digital watermark's size, which is preserved until extraction. The fragile watermark component is embedded into the RONI of the robustly watermarked image using an LSB replacement approach.

To obtain lower and higher frequency sub-bands, the host image undergoes a three-level LWT. Coefficients from the lower-frequency sub-band (LL-band) are grouped into 2x2 blocks. These blocks are randomly shuffled using an initial secret key. The variance value is then calculated for each selected block. An inverse-LWT (I-LWT) is performed to reconstruct the original image from the watermarked image.

The following steps are involved in the watermark embedding process:

Create a two-dimensional binary matrix of size N×N from the watermark image.

To jumble the binary watermark, use the two-dimensional Arnold Transform.

Create a one-dimensional watermark vector WW with a length of N×NN×N by flattening the jumbled matrix.

To further process the image data, apply a Lifting Wavelet Transform (LWT) with three levels.

Divide the LWT coefficients into non-overlapping blocks to create a coefficient matrix.

Incorporate the watermark bits, which are shown as a one-dimensional array, into the coefficient blocks' singular values (SVs).

Use the inverse Lifting Wavelet Transform to reconstruct the finished watermarked image.

Both hash keys and compressed recovery data are embedded using a delicate watermarking technique based on Least Significant Bit (LSB) replacement. After an image has been robustly watermarked, this combined data is placed into the segmented Region of Non-Interest (RONI).

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

The compressed watermark data can be directly embedded into the RONI thanks to the LSB technique.

The image serves as the host for delicate watermarking in this method. To create the delicate watermark, hash keys are created independently for the Region of Interest (ROI) and RONI. Furthermore, distinct hash keys are generated for every RONI segment. The RONI is separated into eight sub-regions, each of which is given a unique hash key to facilitate partial tamper localization, meaning each RONI sub-part will have a unique hash key. This helps confirm the authenticity of extracted recovery data and aids in identifying the tampered area. For detecting tampering within the RONI part with partial localization, this partitioning is beneficial, although a single hash key for the entire RONI would suffice for basic tamper detection without fine-grained localization. In the robust watermarked image $Wimg\_r$, $WatF$ is embedded using the following steps.

Step 1: Select n pixels of RONI to embed $WatF$. Here n is the fragile length sequence $WatF$.

Step 2: All the values of the pixel are converted to binary form.

Step 3: Replace the first LSB of all pixels using the fragile watermark's bit values $WatF$. Step 4: Convert all pixel values from binary to decimal form. Lastly, the final watermarked image $Wimg\_(r+f)$ is obtained.

Tamper Detection and Localization

In the watermarked image, the suggested tamper detection approach is employed on the receiver side for authenticity validation and attack identification. As a result,

cryptosystem and watermarking are used in the research to identify tampering and localise digital images. The block yields the watermark, permuting the six MSBs of each pixel. Consequently, the DWT is used for extracting the DC coefficients for each block. By applying the DWT followed by the block-based DCT technique, DC coefficients are obtained. Further, the grey level means can be extracted from the DC coefficient by dividing it by 8×8 blocks to form a new matrix. Finally, by using the singular value modification in the DWT domain, embed the watermark into the coefficient matrix.

Due to sensitive dependencies on system parameters, initial conditions, and random behaviour, chaotic research for image encryption has a vital significance. Consequently, a hybrid CMT based on the LA is used to shuffle the watermark image. A secure image chaotic cryptosystem is used to encrypt the watermark, from which excellent randomness is accomplished by shuffling the pixels. The extracted and generated keys are compared to identify tampering/forgery. For the localization watermark, the arithmetic mean of a preferred block and the MPI of that block is employed. Vector quantization (VQ), noise addition, cut-and-paste attacks and copy-move attacks, geometric attacks, continuous feature attacks, and collage attacks have all been tried with the suggested approach.

Discrete Cosine Transform

To create a single block, you can group the eight non-overlapping coefficients from the LH3 sub band. Following this step, an initial secret seed value (Key2) is employed to shuffle the remaining blocks. Within each block, the difference between the two maximum coefficients can be

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

estimated and treated as a significant distinction. Subsequently, bits for the watermark are shuffled randomly, much like in previous steps, but with different seed values (Key1) being utilized. Security is enforced through a pseudo-random permutation technique that is based on the block values. When it comes to altering the order in which blocks are watermarked, the pseudo-random permutations technique proves to be the most suitable choice. Once the watermark bits have been embedded in the selected subband, this process results in a change in the block locations. Importantly, it doesn't necessitate any additional information apart from the digital watermark size, which is kept intact until the watermark extraction phase. The fragile watermark is embedded in the RONI (Region of Non-Interest) of the robust watermarked image using an LSB replacement approach.

Both AC and DC coefficients are considered in the transformed matrix. On a block of size $N \times N$, applied the DCT technique is known as the block DCT. The perceptually significant coefficient is represented as the DC coefficient in a transformed block of DCT that is the left top corner elements and perceptually AC coefficients are represented as insignificant coefficients which are the remaining coefficients. For obtaining image frequency components in decreasing order, these coefficients are scanned zigzag. To embed the watermark, modify these AC and DC components. For taking transformation and inverse transformation of an image, equations (5) and (6) are used.

$$c\ (0,0) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{m-1} \sum_{y=0}^{n-1} f\ (x,y) \qquad (5)$$

$$c\ (u,v) = \frac{2}{\sqrt{MN}} \sum_{x=0}^{m-1} \sum_{y=0}^{n-1} c\ (u,v) \cos\left(\frac{(2x+1)\ un}{2M}\right) \cos\left(\frac{(2y+1)\ vn}{2N}\right)$$

Where $u = 1, \ldots, M-1$, V= $1, \ldots, N-1$. The inverse transform is

$$f\ (x,y) = \frac{1}{\sqrt{MN}}\ C(0,0) + \frac{2}{\sqrt{MN}} \sum_{x=0}^{m-1} \sum_{y=0}^{n-1} c\ (u,v) \cos\left(\frac{(2x+1)\ un}{2M}\right) \cos\left(\frac{(2y+1)\ vn}{2N}\right) \quad (6)$$

Discrete Wavelet Transform

It decomposes the input image into low-frequency, middle and high-frequency bands in new time and frequency scales, and this DWT is a transformation technique used for representing an image in a new. The low-frequency band value is the filter averaging value whereas the high-frequency coefficients are detail values or wavelet coefficients.

Decompose an image as a multistage transform by using the DWT. LL1, LH1, HL1, and HH1 are the four subbands of a decomposed image which is performed in the initial step while LL1 represents the coarse level coefficients, i.e., the approximation image, finest scale wavelet coefficients are represented as the HL1, LH1, and HH1.

Singular Value Decomposition

The matrices are analysed using the SVD which is a mathematical tool. In the form of three matrices, the given matrix A is decomposed in SVD such that, $A = USVT$ where,

$UTU = I$, $VTV = I$, I is an identity matrix, and U and V are orthogonal matrices. The columns of U are denoted as the left singular vectors of A, the right singular vectors of A are represented as

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

the columns of V, and the diagonal entries of S are called the SV of A. This decomposition is known as the SVD of matrix A. Usually, in the singular matrix, the watermark is embedded, and if embedded the watermark in the SVD orthogonal matrices then improved the host image's perceptibility, because of the very small matrix elements of orthogonal matrices it is not robust to many attacks. The applications of SVD's three main properties from the image processing viewpoints are given as follows:

When a small perturbation is added to an image, it has high stability for the SV of an image, that is not significantly changing the SV.

While the image geometry specifies the corresponding singular vectors pair, an image layer's luminance is specified by each singular value.

Intrinsic algebraic properties are represented in the singular values.

Watermark Extraction Algorithm

- Transform the watermarked image into RGB colour spaces.
- Apply DWT to decompose the respective colour space of a cover image in which the watermark is hidden.

$$[LL,\ LH,\ HL,\ HH] = 2dwt\ (\text{'colorspace'},\ \text{'filtername'}) \quad (7)$$

- Divide the mid-frequency band into smaller 4x4 blocks and apply DCT to each block, B^*_{ij} .
- Extract the DC coefficients σ_{ij} from every DCT transformed block and construct a new matrix C, which could be decomposed by the SVD technique,

$$C = U^* S^* V^{*T} \quad (8)$$

- Extract the SV from C matrix, then compare the variance between the watermarked SV and host image singular values, $S3 = (S^* - S)/\sigma$.
- Combine the obtained singular values with the watermark's orthogonal matrices,

$$W^* = U_W\ S3\ V_W^T \quad (9)$$

- Repeat same procedure for the watermark in order to extract from other bands.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

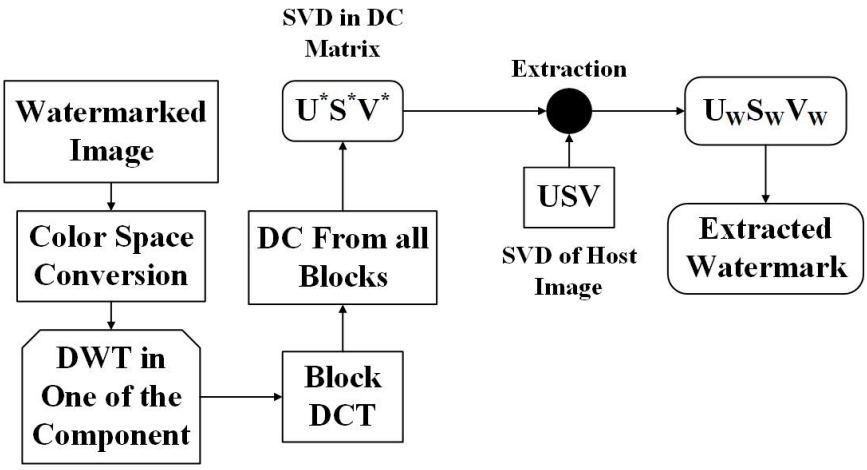


Figure 2: Extraction Process of Watermark

The original cover image is used for extracting the watermark from all frequency bands in the proposed method. Therefore, the algorithm can be classified as a non- blind watermarking technique. For all three color spaces of (RGB) an image, the above embedding and extraction algorithm can be tested.

Hybrid Chaotic Magic Transform

In this encryption scheme, the two-dimensional image feature is employed and with traditional encryption schemes, it is compared. Due to the combination of hybrid CMT with LA, HCMT-EE is a lightweight image encryption method. In this work,a fast improved secure image chaotic cryptosystem is built using the linear congruential generator (LCG), Lanczos algorithm (LA), and HCMT. In the HCMT, the input plain image P is given. There are four steps in HCMT: in ascending order, sorted the values of the image column pixel and row sorting are performed. By randomly shuffling all pixel positions, the confusion property is achieved by the pixel confusion phase and obtaining confused image M.

Based on the following steps, for every image block, the adapted encryption algorithm aims to confuse the pixel position:

Hybrid CMT algorithm shuffles matrix C: To obtain a sorted matrix C', in ascending order each column of C is sorted.

By connecting the pixels in C with locations (l(i,1),1),(l(i,2),2),(l(i,3),3),(l(i,4),4),…,(l(i,n),n) concerning CO, the shuffled index matrix I is generated.

In the clockwise directions, the pixel's P positions are shuffling to the right to do the pixel shuffling process.

Pixels are shifted to the right by the HCMT-EE algorithm's simultaneous clockwise pixel shuffling along the row and column directions. This method makes it possible to efficiently scramble image pixels while maintaining a high level of security and minimal computational complexity. Pixels are moved one position to the right in the first iteration of the encryption process, two positions in the second, three positions in the third, and four positions in the fourth. Experimental results and security analyses show that the clockwise pixel shifting employed in HCMT-EE offers faster encryption performance and introduces more image randomness than leftward or counter-clockwise shifting techniques.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

M is the result of shuffled matrix.

The hybrid CMT algorithm is used to do the shuffling process; here, the shuffled index matrix C' of size m×n is produced by using random chaotic matrix C with size m×n, where index matrix I is defined by I (i,j)=k for C^' (i,j)=C (k,j)

Let M be the resultant shuffled image and O be the original image with size m×n. The process of the original image's pixel shuffling is defined by

F (P,I)=M (10)

The chaotic matrix C generated the shuffled indexed matrix I, by sorting each column of chaotic matrix C in ascending order, sorted matrix C' is generated. The data position C' is shown in the index matrix, that is from the chaotic matrix C they are permuted. The pixel shuffling process where from HCMT, the resultant shuffled matrix M and matrix P for the original image are obtained.

The normalization of eigenvectors and large eigenvalues is performed by using the application of the Lanczos algorithm. It was invented by Cornelius Lanczos. The used q_1 as the random vector, matrix "k". α_m is the characteristic vectors and W_m is the characteristic roots, for loops being used to calculate eigenvalues and eigenvectors. Lanczos algorithm is as given in the following table 1.

Table 1: Tabulation for Lanczos Algorithm

Algorithm 1: Lanczos Algorithm
Start:
Initialization:
q_1= random vector with norm 1.
$q_0 = 0$
$\beta_{1=0}$
Step 1:
for $i = 1,2,3, \ldots m-1$
Step 1-1: $w'_i \leftarrow kq_i$
Steps 1-2: $\alpha_i \leftarrow w'_i . \ q_i$
Steps 1-3: $w_i \leftarrow w'_i - \alpha_i q_i - \beta_i q_{i-1}$
Steps 1-4: $\beta_{i+1} \leftarrow \|w_i\|$
Steps 1-5: $q_{i+1} \leftarrow w_i / \beta_{i+1}$
End for
Step 2: $q_m \leftarrow kq_m$
Step 3: $A_m \leftarrow w_m . q_m$
Return

Later, to identify the forgery or tampering images, the extracted and generated keys are compared.

(iv) Tamper Localization

The arithmetic mean of a selected block and the MPI in that block are utilized in the localization

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

watermark. In the image intensity, variation in them may cause huge variation, and the authentication at these levels gives better results. DNA encoding is used to generate 8 bits of authentication and localization watermark for each block. The mean of the block along with the MPI present in the same block is used to do the tamper localization.

The manipulated area is identified by one of the effective watermarking-based authentication system requirements or it is represented as localization where it verifies other areas as authentic and the manipulated area's locations are detected bythe authentication watermark. Store the information as the watermark used to recover the tampered area.

In the developed scheme, the average intensity of the block had been used. An image is dived into blocks by using this scheme and further divided each block into sub- blocks. In the authentication and recovery process, the sub-blocks and the block's average intensity will be used. Equation (11) is utilized to calculate the block's average intensity.

$$Block\ Average\ Intensity = \frac{(P_1+P_2+P_3\ldots+P_{15}+P_{16})}{} \tag{11}$$

Where, the intensity of the block pixels are $P1$ to $P16$. The sub-block average intensity is:

$$Sub-block\ Average\ Intensity = \frac{(P_1+P_2+P_5+P_6)}{4}$$

Where, $P1$, $P2$, $P5$ and $P6$ are the intensity of the pixel in a sub-block

(12)

For every block, the authentication information consists of one bit of authentication bit and in the following algorithm, one bit of parity check bit is generated:

For the block, the average intensity is denoted as $x1$ and its sub-blocks, compute $x1s$, denoted by avg_x1 and avg_x1s respectively. As an example, the value for avg_x1 is 85 and the values for avg_x1s are 99, 84, 81 and 77 respectively.

Generate the authentication bit, v, of each sub-block as:

Generate the parity check bit, p, of each sub-block as:

$$v = \begin{cases} 1 & if\ avg\_x1s \geq avg\_x1, \\ 0 & otherwise, \end{cases} \tag{13}$$

$$p = \begin{cases} 1 & if\ num\ is\ odd, \\ 0 & otherwise, \end{cases} \tag{14}$$

Where in the seven MSB of avg_ x1s, the 1s total number is represented as num. The authentication information generated is embedded as the watermark together with the block

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

average intensity that will be used for recovery purposes.

Watermark Recovery

The recovery tag is created using the recovered watermark utilizing the watermarked image it is delivered to the recipient. The Lempel-Ziv-Welch technique compresses the ROI's recovery information of the host image. Merge the hash keys and compressed recovery data by the LSB replacement-based fragile watermarking technique and in the robust watermarked image's segmented RONI area, inserted them. Without causing any damage, this method demonstrates that any manipulation with the ROI of the medical image can be detected and retrieved.

LZW (Lempel-Ziv-Welch) Algorithm

Lempel-Ziv-Welch (LZW) compression is especially useful for lossless watermark compression in medical image watermarking because it is used to remove repetitive data sequences. It is perfect for maintaining the integrity of medical data because it can reduce data size without causing any loss. LZW supports effective storage and quicker processing by ensuring that no data is lost during compression and decompression. The UNIX "compress" utility also uses this technique to increase performance while lowering storage needs. Furthermore, the LZW algorithm serves as the foundation for the popular GIF (Graphics Interchange Format) image file format. The method works by mapping input character strings to fixed-length codes using a string table. This table typically has 4096 entries, of which the first 256 are standard 8-bit characters. The remaining entries are used to encode recurring sequences. During encoding, repetitive patterns are assigned new entries, while during decoding, the compressed codes are translated back into the original data using the same table.

Check for Tampering

Similar to the embedding process, the hash keys are gathered for alteration in the image $Wimg\_(r+f)$ or detect tampering for RONI and ROI regions. Let $Hroi\_new$, $Hroni{-}1\_new$, $Hroni{-}2\_new$, $Hroni{-}3\_new$, $Hroni{-}4\_new$, $Hroni{-}5\_new$, $Hroni{-}6\_new$, $Hroni{-}7\_new$ and $Hroni{-}8\_new$ are the generated hash keys. Finally, to detect tampering, the corresponding hash keys are compared. If all analogous bits of $Hroi\_ext$ and $Hroi\_new$ are equal, then the ROI region that has not been tampered with is confirmed. On the other hand, the complete ROI region can be considered as tampered with, even if a single bit is not the same as the analogous bit. Likewise, for tampering check all eight RONI regions.

ROI Recovery

Process $ROIbin_ext$by converting each successive set of eight bits to a decimal value and reorganize the data according to the dimensions of the ROI region. This method guarantees complete reversibility when recovering the ROI region. Prior to initiating the ROI recovery, it is imperative to thoroughly inspect the embedded Region of Non-Interest (RONI) region, the storage site for recovery data, for any indications of tampering. Ensure the accuracy of hash keys and the accuracy of the extracted

recovery data by dividing the RONI region into eight components, facilitating tamper

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

localization. In the context of fragile embedding, the length (n) of the fragile sequence $WatF$ corresponds to the number of pixels say(N_pixels) required for the procedure. Typically, (N_pixels) is notably smaller than the entire RONI region of
the image. As a result, not all segmented RONI regions are indispensable for watermarking. The RONI-3 and RONI-1 regions are employed for embedding the fragile sequence $WatF$, ensuring that tampering in other RONI regions does not impact the extraction fragile sequence $WatF\_ext$. Consequently, complete reversibility in recovering the ROI region is attainable by leveraging the extracted recovery information.

Experimentation And Result Discussion

For experimental validation, the proposed algorithm utilized a standard 512x512 test image, into which a 64x64 watermark was embedded. An embedding intensity of 0.1 was consistently applied across all frequency bands. The selection of color channels and frequency bands can be adapted based on the specific application. If the watermark is relatively small, any individual color channel might be adequate. In this study, the algorithm's efficacy was assessed by embedding the watermark across all frequency bands.

The experimental evaluations revealed a high degree of robustness and imperceptibility against a wide range of digital threats. All simulations were performed using MATLAB software. The proposed methodology demonstrated strong resistance to various image processing manipulations, as well as copy-move and copy-paste attacks, efficiently detecting tampering in their presence.

Furthermore, the presented research reported superior average values for Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM) and Bit Error Rate (BER) when compared to existing schemes. The scheme's robustness was further validated against several image-processing attacks.

Table 2: Performance Values for Different Attacks

Attacks	PSNR	SSIM	NC
No Attack	54.3899	0.99571	0.99994
Speckle noise(0.1)	47.2644	0.97324	0.99994
Salt and pepper noise(0.1)	47.3333	0.98502	0.99994
Gaussian noise(0.02)	37.9959	0.83947	0.99993
Sharpening attack(0.02)	53.9973	0.99462	0.99994
Rotating attack(0.002)	44.5289	0.96456	0.99993
Motion blur(0.5)	52.3273	0.99415	0.99994
Average filter(0.8)	51.3416	0.99227	0.99994
JPEG compression(50)	49.5156	0.98811	0.99994

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

Histogram equalization(2)	49.9275	0.98812	0.99994
Gaussian low-pass filter(2x2)	51.3277	0.99224	0.99994
Winner filter(3x3)	54.3899	0.99571	0.99994

Table 2 summarizes the performance metrics (PSNR, SSIM, and Normalized Correlation- NC) under various attacks. These include: Speckle noise (at 0.1 variance), Salt and pepper noise (at 0.1 density), Gaussian noise (at 0.02 variance), Sharpening attack (factor 0.02), Rotating attack (0.002 degrees or radians - clarification needed from original context), Motion blur (strength 0.5), Average filter (strength 0.8), JPEG compression (quality factor 50), Histogram equalization (applied twice), Gaussian low-pass filter (2x2 kernel), and Winner filter (3x3 kernel), alongside a 'No Attack' baseline.

Table 3: Tabulation for Processing Time

Process	**Time**
Embedding	0.18463
Extraction	0.07311
Encryption	0.15920
Decryption	0.02576

The processing time for the research is detailed in Table 3, which itemizes the embedding, extraction, encryption, and decryption durations. Specifically, the embedding process took 0.18463 seconds, extraction required 0.07311 seconds, encryption was completed in 0.15920 seconds, and decryption took 0.02576 seconds.

Table 4: Extracted Watermarking Image

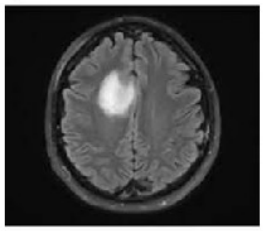
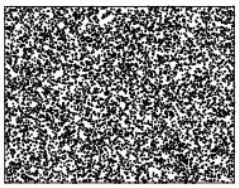
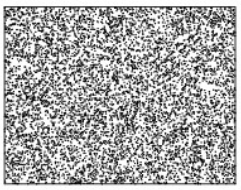
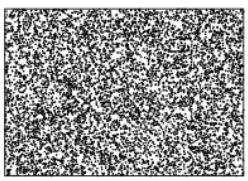
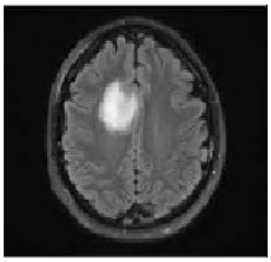
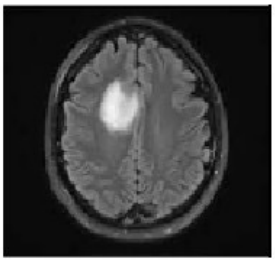
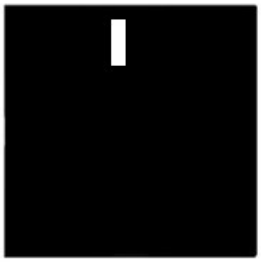
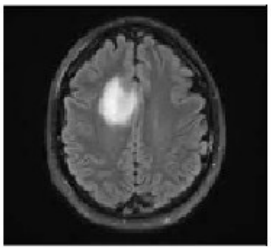
Embedding Factor	α=1.10	α=1.11	α=3.95	α=8
Extraction factor	α=1.10	α=1.12	α=3.96	α=8.01
Extracted Water Mark				

Table 4 illustrates the extracted watermarking images along with their respective embedding and extraction factors. This table also presents visual results of the extracted watermarks for a test image, confirming their visual quality. The embedding factors employed in this work were 1.10, 1.11, 3.95, and 8. Correspondingly, the extraction factors (α) were 1.10, 1.12, 3.96, and 8.01.

Table 5: Watermarked, Tampered and Recovery Image of Brain

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

Watermarked Image of Brain	Tampered Brain	Localization of Brain	Recovery Brain
			

Visual results are further presented in Table 5, which showcases a watermarked brain image, its tampered version, the resulting localization image, and the recovered brain image. Subsequently, figures detail detection and recovery for kidney, brain, and liver images.

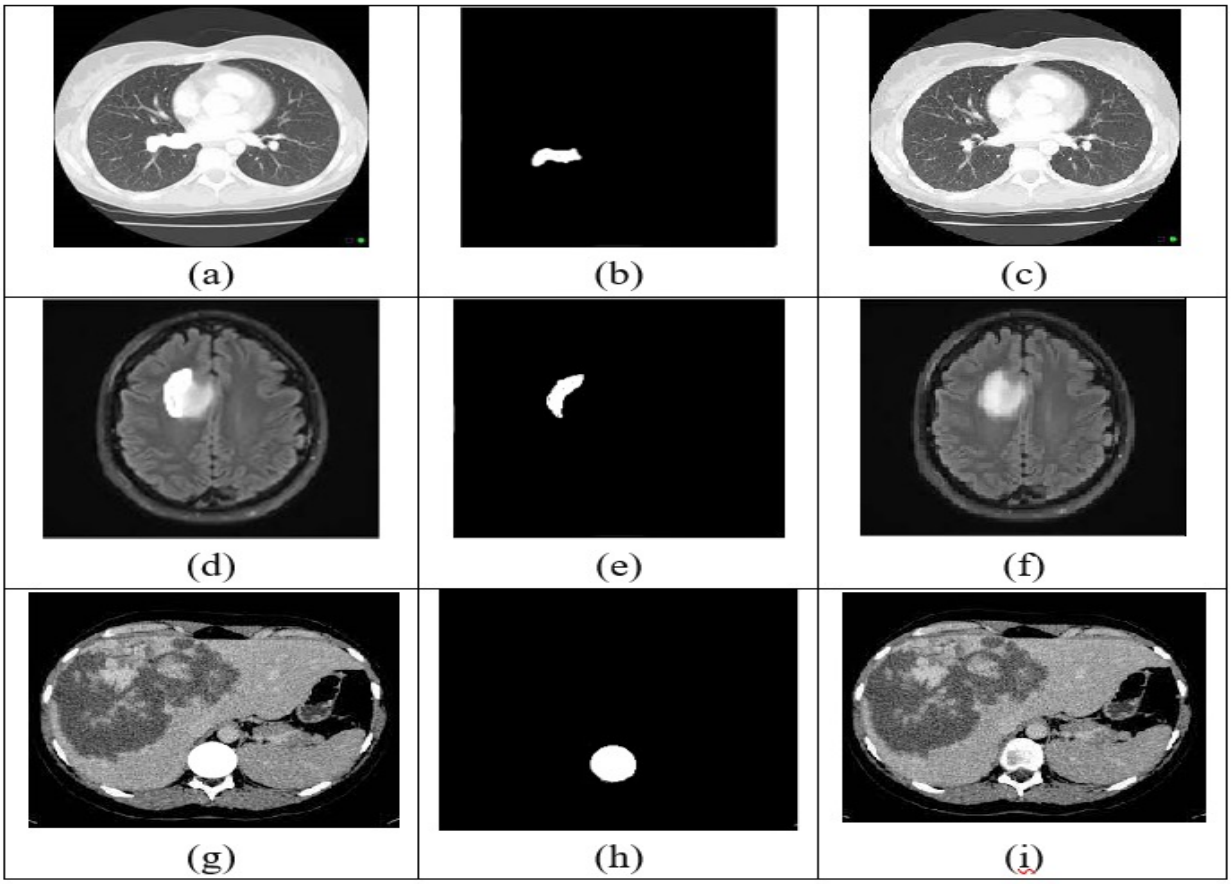


Figure 3 demonstrates the impact of a content removal attack on kidney, brain, and liver images. Specifically, Figures 3 (a), (b), and (c) display the tampered kidney image, its localized tamper image, and the recovered kidney image. Similarly, Figures 3 (d), (e), and(f) show the tampered, localized, and recovered brain images, while Figures 3 (g), (h), and (i) depict these stages for the liver image.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

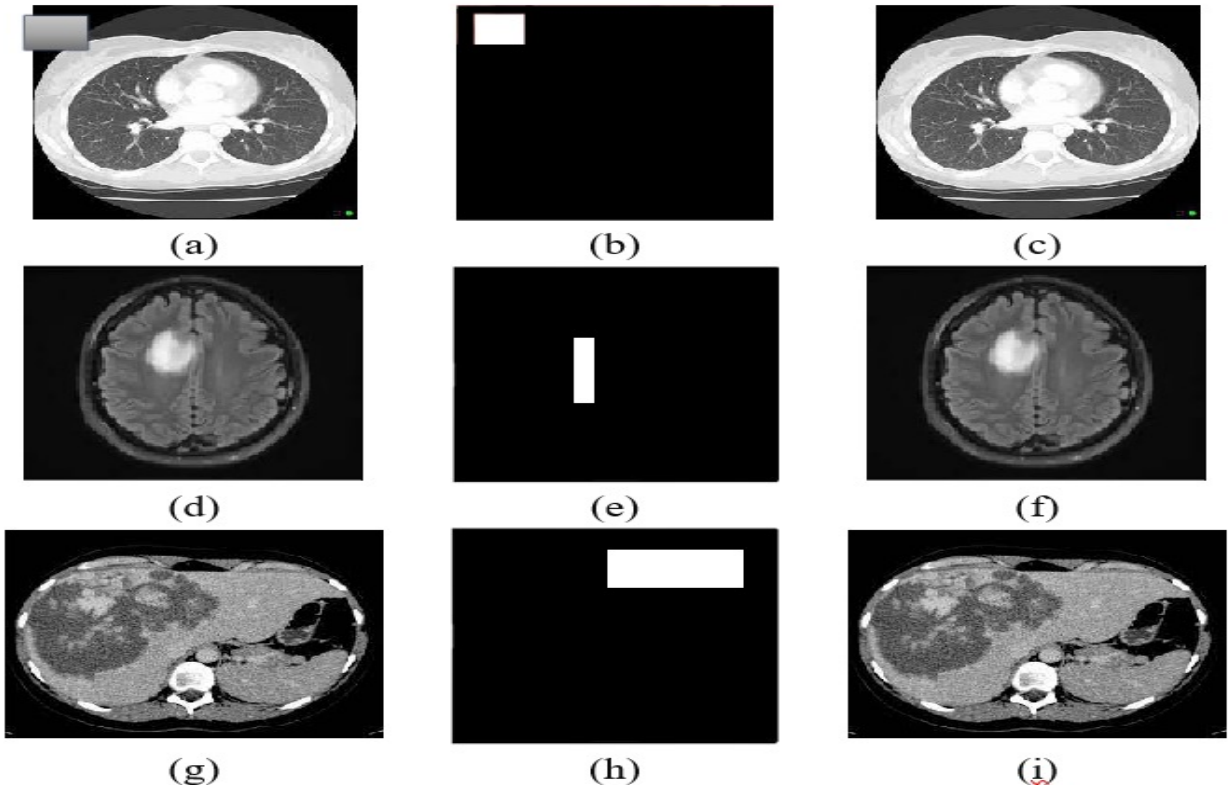


Figure 4: Tampered, Localized, and Recovered Image of Collage Attack

Figure 4 presents the outcomes of collage attacks on medical images (MI) of the kidney, brain, and liver. Figures 4 (a), (b), and (c) show the tampered, localized, and recovered kidney image. Figures 4 (d), (e), and (f) illustrate these stages for the brain image.
Likewise, Figures 4 (g), (h), and (i) display the tampered, localized, and recovered liver images subjected to a collage attack.

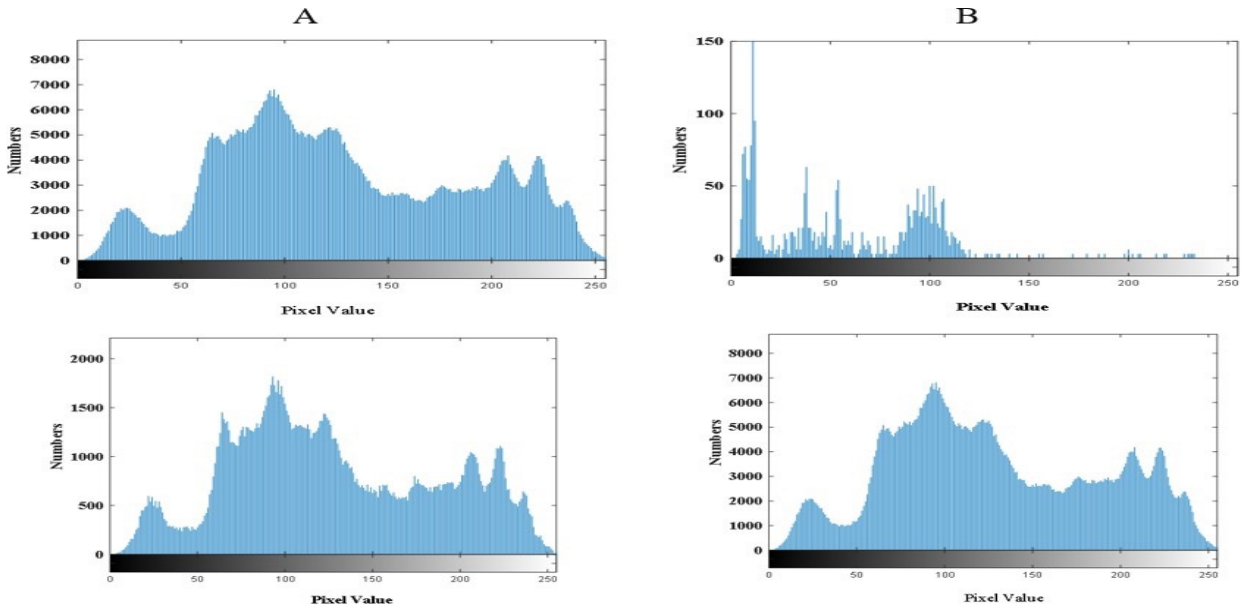


Figure 5: Pixel Image Values

Figure 5 displays simulation results for images composed entirely of zero-pixel values and all-one pixel values. To analyze the correlation of adjacent pixels in plain and cipher images, 8000

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

random pixel pairs were selected from each direction. For the initial graph (Figure A), pixel values were assessed based on ranges of 0 to 8000 and 0 to 2000, yielding high pixel values. In contrast, Figure B represents pixel value evaluations using ranges of 0 to 150 and 0 to 8000.

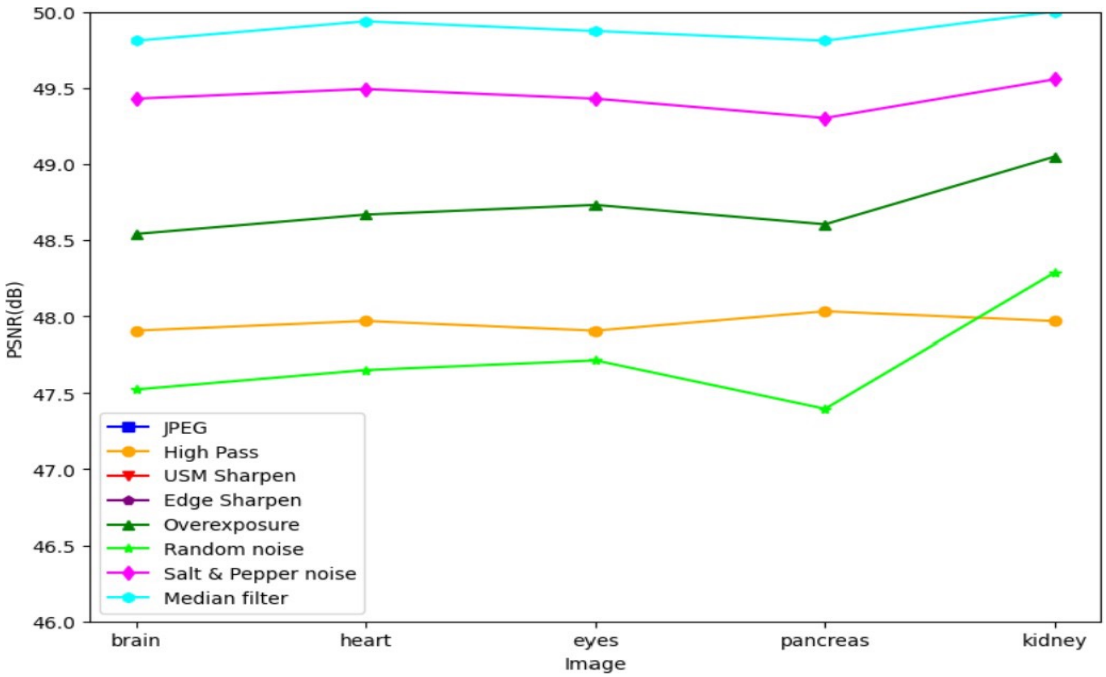


Figure 6: PSNR Graph for Different Images

The PSNR performance across different image types is depicted in Figure 6. This metric was measured for Brain, Heart, Eyes, Pancreas, and Kidney images subjected to various attacks: JPEG compression, High-pass filter, USM sharpening, Edge sharpening, Overexposure, Random noise, Salt and Pepper noise, and Median filter. The evaluation indicated that the median filter yielded higher PSNR values, while the High-pass filter resulted in lower PSNR values.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

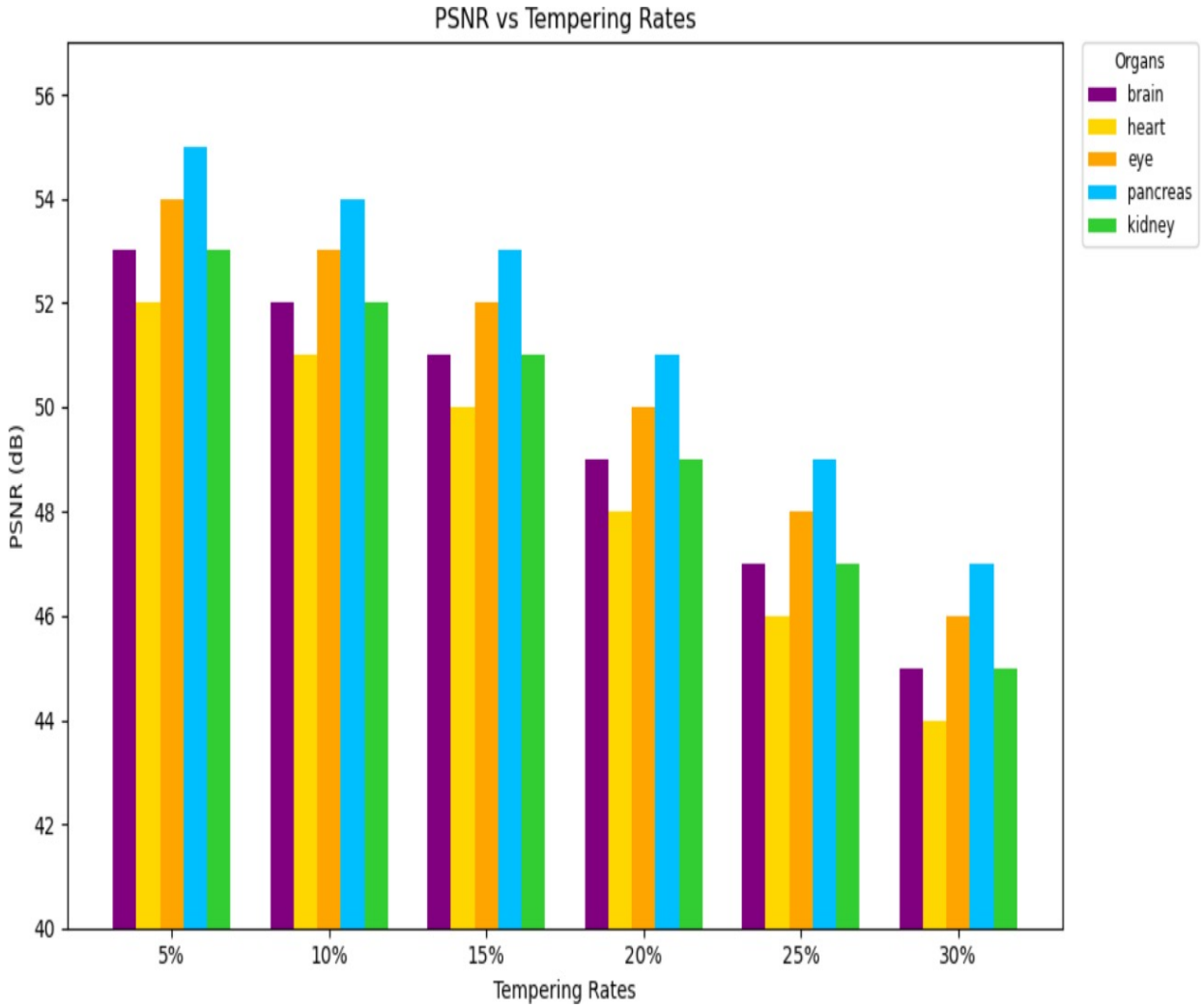


Figure 7: PSNR Graph to Tampering Rates

Figure 7 presents a PSNR graph illustrating performance based on varying tampering rates for Brain, Heart, Eyes, Pancreas, and Kidney images. The tampering rates considered were 5%, 10%, 15%, 20%, 25%, and 30%. Results showed that "medical data 2" (presumably one of the test images) achieved higher PSNR values, while standard test images like Lena and Man (referenced for comparison context) exhibited lower PSNR values under similar conditions.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

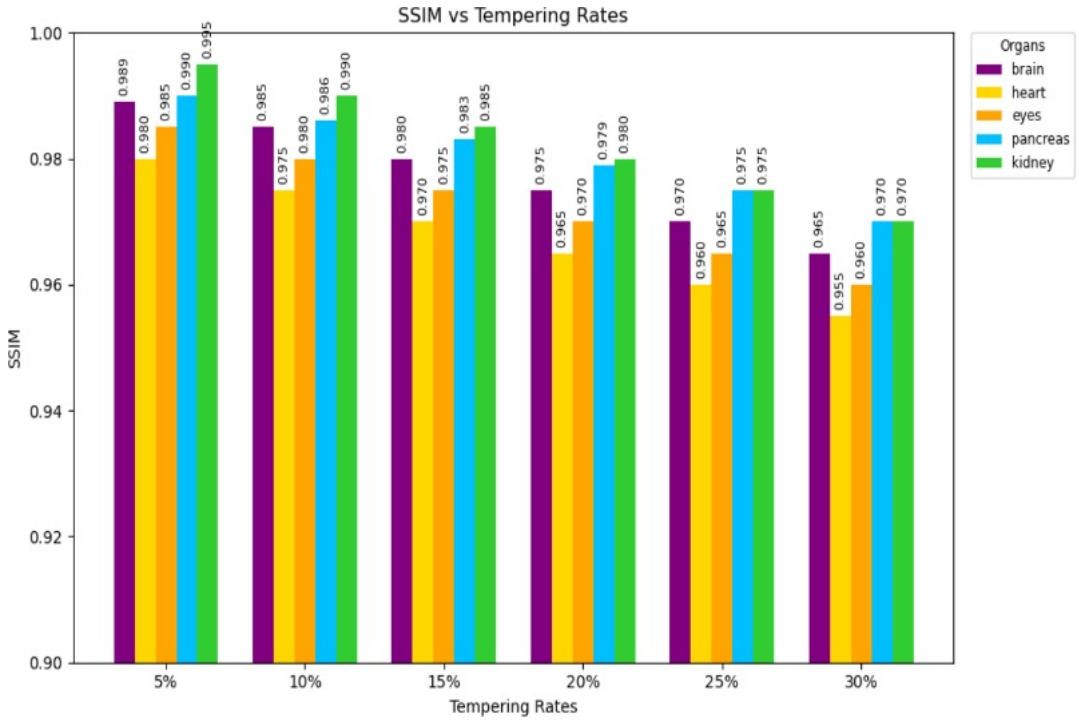


Figure 8: Structural Similarity Index

Figure 8 illustrates the Structural Similarity Index (SSIM) evaluation for the research. SSIM values were assessed for popular test images (Brain, Heart, Eyes, Pancreas, Kidney) across different tampering rates: 5%, 10%, 15%, 20%, 25%, and 30%. The proposed scheme demonstrated superior robustness against a range of signal-processing attacks. Despite its multipurpose design, the scheme consistently delivered strong performance and maintained high visual quality, as evidenced by an average SSIM value of 0.97. These findings indicate that the proposed scheme produces consistent and effective results across diverse image types, making it suitable for a broad spectrum of digital images.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

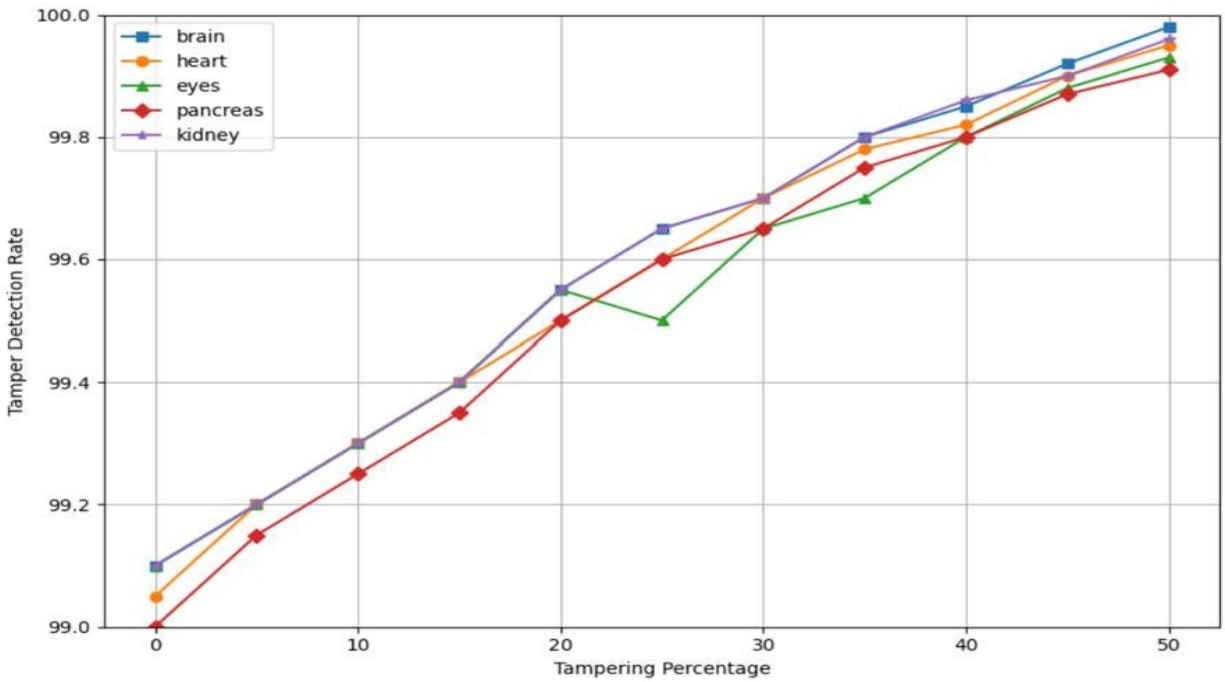


Figure 9: Performance Graph for Tamper Detection Rate

Figure 9 demonstrates the performance graph for the tamper detection rate. The detection capabilities of the proposed research were evaluated for Brain, Heart, Eyes, Pancreas, and Kidney images at tampering percentages of 10%, 20%, 30%, 40%, and 50%. The proposed method achieved tamper detection rates of 99.98% for Brain, 99.97% for Heart and Eyes, 99.965% for Kidney, and 99.91% for Pancreas.

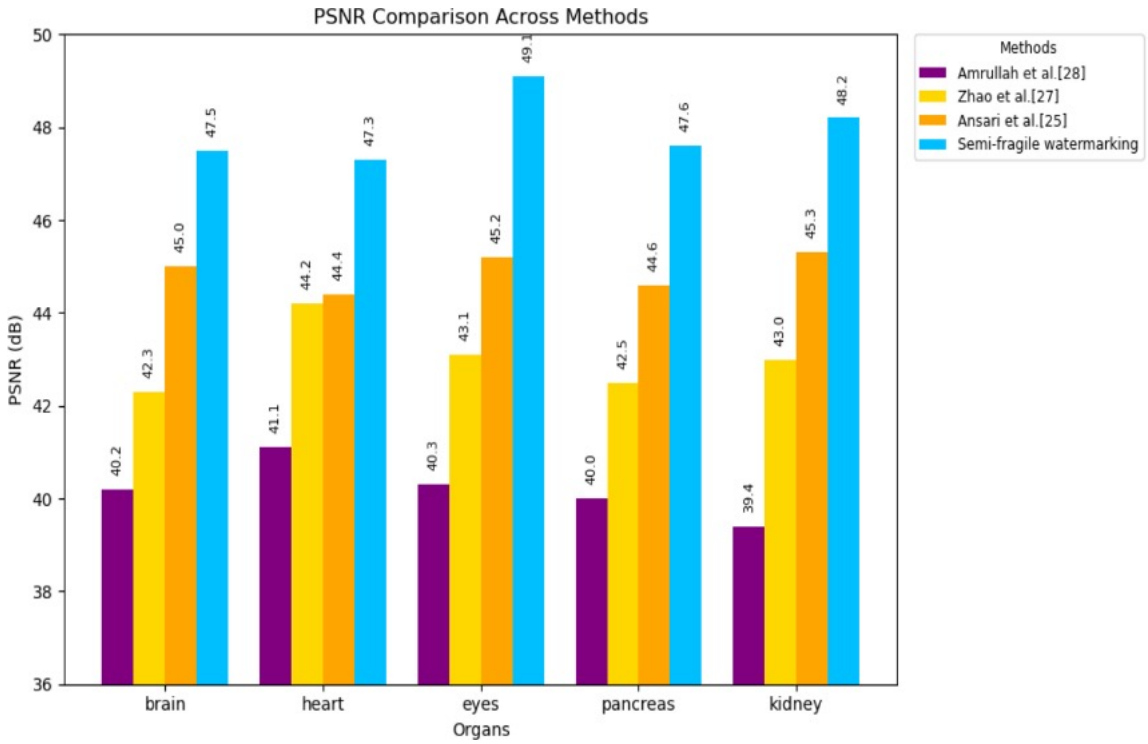


Figure 10: Comparison Graph for PSNR

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

A comparative PSNR graph is provided in Figure 10, where the proposed work is benchmarked against existing methods by Ansari, Zhao, Amrullah, and Qi using Brain, Heart, Eyes, Pancreas, and Kidney images. The proposed method exhibited higher PSNR values than these existing techniques. Specifically, its performance was 2.5% higher than Ansari's method, 4% higher than Zhao's, and 4.5% higher than Amrullah's.

Conclusion And Future scope

Digital image watermarking is a critical technique involving the embedding of covert data into digital images to safeguard against unauthorized alterations or content deletion. In the current landscape of digital advancements and the widespread adoption of teleradiological applications, this field remains a dynamic, intricate, and evolving area of research.This study introduces a novel algorithm to enhance tamper detection accuracy within semi- fragile watermarking schemes. The process commences with watermark embedding using the LWT (Lifting Wavelet Transform) algorithm. Subsequently, the research employs the HCMT (Hybrid Chaotic Magic Transform) for robust tamper detection. The precise location of the watermark is determined by analyzing the mean value of designated image blocks and the Most Prominent Intensity (MPI) within those blocks. The proposed methodology has been extensively evaluated against a variety of tampering attacks, demonstrating significantly improved robustness.To manage the recovery data, the Lempel-Ziv-Welch (LZW) algorithm is utilized for compressing information retrieved from the host image's Region of Interest (ROI). Ultimately, this paper assesses the efficiency, overall performance, and robustness of the proposed system, with a particular focus on tamper detection accuracy. Key performance indicators evaluated include the Tamper Detection Rate, Peak Signal-to-Noise Ratio (PSNR), False Positive Rate (FPR), False Negative Rate (FNR), and Structural Similarity Index (SSIM).The key findings highlight the superiority of the proposed work:The PSNR achieved by this research is notably higher, outperforming the Ansari, Zhao, and Amurllah methods by 2.5%, 4%, and 4.5%, respectively.

Furthermore, the proposed system demonstrates improved error rates, achieving an approximately 1.5% lower False Positive Rate (FPR) and a 4% lower False Negative Rate (FNR) when compared to other existing techniques. The performance of the proposed approach surpasses that of current state-of-the-art techniques in both image content localization and tamper detection. Consequently, the devised scheme exhibits exceptional effectiveness across all evaluated metrics: tamper detection, PSNR, SSIM, FPR, and FNR. The proposed algorithm successfully maintains superior visual quality, as indicated by its average PSNR, even when accommodating a greater embedding capacity. Therefore, this research facilitates effective tampered image detection and localization and also enables the accurate recovery of the original image content. Looking ahead, future research efforts may concentrate on developing novel and advanced techniques to further enhance the robustness and security of watermarking schemes against diverse noise and sophisticated filtering attacks.

References

[1] Begum, M., Ferdush, J. and Uddin, M.S., 2021. A Hybrid robust watermarking system based on discrete cosine transform, discrete wavelet transforms, and singular value decomposition. Journal of King Saud University-Computer and Information Sciences.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

[2] Lee, J.E., Seo, Y.H. and Kim, D.W., 2020. Convolutional neural network-based digital image watermarking adaptive to the resolution of image and watermark. Applied Sciences, 10(19), p.6854.

[3] Hemdan, E.E.D., 2021. An efficient and robust watermarking approach based on single value decompression, multi-level DWT, and wavelet fusion with scrambled medical images. Multimedia Tools and Applications, 80(2), pp.1749-1777.

[4] Alam, S., Ahmad, T., Doja, M.N. and Pal, O., 2021. Dual secure robust watermarking scheme based on hybrid optimization algorithm for image security. Personal and Ubiquitous Computing, pp.1-13.

[5] Swaraja, K., Meenakshi, K. and Kora, P., 2020. An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine. Biomedical Signal Processing and Control, 55, p.101665.

[6] Rohilla, T., Kumar, M. and Kumar, R., 2021. Robust digital image watermarking in YCbCr color space using hybrid method. Information Technology in Industry, 9(1), pp.1200-1204.

[7] Zermi, N., Khaldi, A., Kafi, R., Kahlessenane, F. and Euschi, S., 2021. A DWT-SVD based robust digital watermarking for medical image security. Forensic Science International, 320, p.110691.

[8] Mulani, A.O. and Shinde, G.N., An approach for robust digital image watermarking using DWT-PCA.

[9] Liu, D., Su, Q., Yuan, Z. and Zhang, X., 2021. A blind color digital image watermarking method based on image correction and eigenvalue decomposition. Signal Processing: Image Communication, 95, p.116292.

[10] Sehra, K., Raut, S., Mishra, A., Kasturi, P., Wadhera, S., Saxena, G.J. and Saxena, M., 2021. Robust and Secure Digital Image Watermarking Technique Using Arnold Transform and Memristive Chaotic Oscillators. IEEE Access, 9, pp.72465-72483.

[11] Balasamy, K. and Shamia, D., 2021. Feature extraction-based medical image watermarking using fuzzy-based median filter. IETE Journal of Research, pp.1-9.

[12] Singh, P., Devi, K.J., Thakkar, H.K. and Santamaría, J., 2021. Blind and Secured Adaptive Digital Image Watermarking Approach for High Imperceptibility and Robustness. Entropy, 23(12), p.1650.

[13] Hasan, N., Islam, M.S., Chen, W., Kabir, M.A. and Al-Ahmadi, S., 2021. Encryption Based Image Watermarking Algorithm in 2DWT-DCT Domains. Sensors, 21(16), p.5540.

[14] Sharma, S., Sharma, H. and Sharma, J.B., 2021. Artificial bee colony-based perceptually tuned blind color image watermarking in hybrid LWT-DCT domain. Multimedia Tools and Applications, 80(12), pp.18753-18785.

[15] Thanki, R., Kothari, A. and Borra, S., 2021. Hybrid, blind and robust image watermarking: RDWT–NSCT based secure approach for telemedicine applications. Multimedia Tools and Applications, 80(18), pp.27593-27613.

[16] Li, T., Li, J., Liu, J., Huang, M., Chen, Y.W. and Bhatti, U.A., 2022. Robust watermarking algorithm for medical images based on log-polar transform. EURASIP Journal on Wireless Communications and Networking, 2022(1), pp.1-11.

[17] Alzahrani, A., 2022. Enhanced Invisibility and Robustness of Digital Image

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

Watermarking Based on DWT-SVD. Applied Bionics and Biomechanics, 2022.
[18] Nha, P.T., Thanh, T.M. and Phong, N.T., 2022. Consideration of a robust watermarking algorithm for color image using improved QR decomposition. Soft Computing, pp.1-25.
[19] Pei, L., 2022. Research on Digital Image Watermarking Algorithm Based on Scrambling and Singular Value Decomposition. Journal of Mathematics, 2022.
[20] Tayel, M., 2022. A Hybrid Encoded and Adapted-tuned Neural Network for Asset Medical Image Watermarking Technique.
[21] Alhumyani, H., Alrube, I., Alsharif, S., Afifi, A., Ben Amar, C., El-Sayed, H.S. and Faragallah, O.S., 2022. Analytic Beta-Wavelet Transform-Based Digital Image Watermarking for Secure Transmission. CMC-Computers Materials & Continua, 70(3), pp.4657-4673.
[22] Hosny, K.M., Magdi, A., Lashin, N.A., El-Komy, O. and Salah, A., 2022. Robust color image watermarking using multi-core Raspberry pi cluster. Multimedia Tools and Applications, pp.1-20.
[23] Hu, H.T., Hsu, L.Y. and Lee, T.T., 2022. All-round improvement in DCT-based blind image watermarking with visual enhancement via denoising autoencoder. Computers and Electrical Engineering, 100, p.107845.
[24] Soualmi, A., Alti, A. and Laouamer, L., 2022. A novel blind medical image watermarking scheme based on Schur triangulation and chaotic sequence. Concurrency and Computation: Practice and Experience, 34(1), p.e6480.
[25] Sinhal, R., Sharma, S., Ansari, I.A. and Bajaj, V., 2022. Multipurpose medical image watermarking for effective security solutions. Multimedia Tools and Applications, pp.1-19.
[26] Yuan, Z., Zhang, X., Wang, Z. and Yin, Z., 2024. Semi-fragile neural network watermarking for content authentication and tampering localization. Expert Systems with Applications, 236, p.121315.
[27] Zhao, Y., Liu, B., Zhu, T., Ding, M., Yu, X. and Zhou, W., 2024. Proactive image manipulation detection via deep semi-fragile watermark. Neurocomputing, 585, p.127593.
[28] Amrullah, A., Ernawan, F., Raffei, A.F.M. and Chuin, L.S., 2025. TDSF: Two-phase tamper detection in semi-fragile watermarking using two-level integer wavelet transform. Engineering Science and Technology, an International Journal, 61, p.101909.