Future Technology
Open Access Journal
ISSN 2832-0379

November 2026| Volume 05 | Issue 04 | Pages 169-180

Journal homepage: https://fupubco.com/futech

https://doi.org/10.55670/fpll.futech.5.4.14

Future Publishing LLC

Article

A fragile reversible watermarking technique for medical imaging security using prediction error expansion and Canny edge detection

Asaad F. Qasim*, Ahmed Hussain Ali

Department Studies Planning and Follow-Up Directorate, Ministry of Higher Education and Scientific Research, Baghdad, Iraq

ARTICLE INFO

Article history:
Received 12 April 2026
Received in revised form
09 August 2026
Accepted 01 September 2026

Keywords:
Reversible watermarking, Medical imaging, Prediction error expansion, Authentication, Integrity

*Corresponding author
Email address:
asaad.flayyih@mohesr.edu.iq

DOI: 10.55670/fpll.futech.5.4.14

ABSTRACT

This paper develops a fragile, reversible watermarking technique to detect accidental and intentional alterations in DICOM medical images. A fragile method is adopted to detect any manipulation applied to medical images, while reversibility ensures the recovery of the original unaltered image at extraction. The proposed approach automatically segments medical images into Region of Interest (ROI) and Region of Non-Interest (RONI), extracts authentication data from the DICOM header, and generates a digital signature of the image. The method combines integrity and authentication data and inserts them into the edge areas within the ROI, implementing the Prediction Error Expansion (PEE) technique and Canny edge detection. During extraction, the embedded watermark and the original unmanipulated image are restored without knowing the pixel locations used to hide the watermark data. The method was assessed using twelve 16-bit DICOM images, including MRI and CT, with a 512x512 pixel size. The experimental results yielded an average PSNR of 97.19 dB and an average SSIM of 0.999996, with an average watermark length of 7835 bits per image. The proposed method also fully met the reversibility requirement by recovering both the original unaltered images and the embedded watermark data. Fragility evaluation showed that manipulations of watermarked images can be detected via alterations in the retrieved watermark. The achieved results demonstrate the effectiveness of the proposed technique in maintaining visual image quality while ensuring reversibility, integrity, and authenticity in the conducted experiments.

1. Introduction

In most medical imaging processes, traditional file-based diagnosis methods have largely been replaced by electronic diagnosis systems. Acquisition devices in hospitals generate medical images across modalities such as X-ray, Ultrasound, Magnetic Resonance Imaging (MRI), and Computed Tomography (CT) [1]. These modalities are managed, exchanged, and archived as Digital Imaging and Communications in Medicine (DICOM) within a Hospital Information System (HIS) using a medical imaging technology called Picture Archiving and Communication Systems (PACS) [2]. Sharing digital medical images among hospitals and clinicians has become a common practice in medical settings for many reasons, such as progress monitoring, diagnosis, obtaining expert advice, and treatment planning [3]. In most cases, this sharing occurs within authorized medical imaging workflows; however, malicious cases may involve retrieving medical images from one PACS and transmitting them to another PACS or an external institution. Medical images may be subject to both intentional and unintentional modifications, and detecting these modifications is a significant challenge. It would be impossible to detect many subtle manipulations that contain counterfeit abnormalities by merely viewing the images. Such undetected manipulations may have significant risks to patients during diagnosis and treatment, with potentially life-threatening consequences. Therefore, it is essential to maintain trust in healthcare by ensuring the integrity and authentication of medical images within the local PACS and when transferring them to other hospital systems. In medical imaging, integrity means ensuring that an image has not been manipulated by unauthorized users; authentication means determining an image's source and confirming that it belongs to the correct patient [4]. Two approaches are commonly utilized to verify the authenticity of medical images: digital watermarking and metadata. Metadata represents patient data that links the patient's medical record to the image [5, 6]. In DICOM images, metadata is located in the image header and defines the

patient, image details, and device properties [2]. Current metadata approaches do not provide a robust link between the metadata and the corresponding medical image, as destroying or altering the metadata renders the images untrustworthy. This issue has been addressed by digital watermarking techniques, which can be defined as the process of embedding digital data (watermark) into another digital object. The hidden data can then be extracted/retrieved to verify the integrity and validity of the digital object [7].

In medical fields, manipulating patients' images may undermine trust in their validity. Any slight modification to an image may cause misdiagnosis with potential life-threatening consequences or medicolegal implications. Consequently, regaining the original image after removing the hidden watermark is crucial and must be considered in medical imaging. Lossless or reversible watermarking methods can achieve this requirement by using techniques that precisely retrieve the reference images. Reversible techniques do not generate distortion-free images, but the watermarked image is used as a host for the data, while the restored image is used for medical examination, treatment, intervention planning, etc. [8]. Existing medical image watermarking techniques can be classified into conventional techniques and lossless or reversible techniques. Irreversible methods are unacceptable to doctors because reference images are generally required for diagnosis; hence the need for reversible watermarking. Reversible watermarking approaches can recover the hidden watermark alongside the unchanged image. This technique is a type of digital watermarking that offers a comprehensive framework for image reliability, as the embedding technique certifies image validity, while the reversibility feature maintains visual quality [9]. In this research, we developed a new fragile reversible watermarking technique to provide integrity verification using a fragile digital signature and data authenticity via encoded DICOM metadata. The reference unchanged image can also be reconstructed at the extraction side using a fully reversible watermarking method. The main objectives of this research are: (1) to develop a fragile reversible watermarking method to maintain the integrity and authenticity of medical images; (2) to reduce the noticeable distortion level through embedding watermark bits into edge regions; (3) to remove the overhead related to location map required for reversible watermarking schemes; and (4) to ensure the precise recovery of the original images after extracting the encoded watermark. Based on these objectives, the main contributions of this study are as follows:

- The automatic segmentation of images into Region of Interest (ROI) and Region of Non-Interest (RONI). The ROI section represents the significant portion of the image used for medical investigations and must be kept unaltered. RONI section typically includes the black background and, sometimes, grey-level areas of the image [10].
- Concealing the data within the edges of the ROI, which contain high-frequency data including changes in colour/intensity of pixel values. This makes the degradation less noticeable, as human vision is less sensitive to small changes in edges than in smooth regions.
- Precise recovery of the original images after removing the concealed data, making them ready for use in medical diagnosis and clinical investigations.

The rest of this research is structured as follows. Section 2 reviews and investigates existing medical image watermarking schemes. The embedding and extraction processes are presented in Section 3. The experimental results and comparison with other studies are discussed in Section 4. Finally, a brief conclusion is presented in Section 5.

2. Related work

Existing medical image watermarking can be classified into two sets: conventional techniques and reversible techniques. Whatever method is adopted, digital watermarking should not impact the visual quality of medical images [9].

2.1 Conventional watermarking techniques

Conventional watermarking can be divided into two main groups: spatial domain and frequency domain. Spatial-domain methods directly encode data into the host image by changing pixel values, such as the Least Significant Bits (LSB) of pixels. LSB modification techniques are fast, easy to implement, and offer high capacity, but they cannot withstand attacks such as lossy compression and noise addition [8]. In the frequency domain, transformation methods are applied before hiding the data to provide greater robustness against different attacks. The most common frequency domain methods adopted in digital watermarking are Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) [8]. In medical domains, the original medical image must not be manipulated when using digital watermarking, as no clinician will accept a decision based on a modified image, even if the change is trivial. Therefore, the applied watermarking technique should be reversible. Irreversible methods are unsuitable for medical applications as original unaltered images remain essential for diagnosis and investigations [9].

2.2 Reversible Watermarking Techniques

Reversible watermarking techniques can be broadly categorized into three major groups [11], including compression-based techniques [12,13], histogram modification-based techniques [14-16], and expansion-based techniques [17, 18]. Difference Expansion (DE) reversible watermarking methods generally surpass existing reversible methods in terms of simplicity, hiding capacity, and invisibility [17-19].

Compression-based technique: Reversible watermarking techniques must conceal extra information in the host image alongside the watermark to restore the original, unchanged image at extraction. Consequently, the watermark message size is much larger than in traditional techniques. Increasing hiding capacity can be achieved by compressing the cover image to provide additional space for encoding the data [9]. Celik et al. [13] developed a compression-based watermarking scheme. Firstly, L-level scalar quantization is applied to image pixel values. The pixel remainders are compressed, and the watermark data is encoded into the quantized image to produce the secured image. Then, by quantizing the secured image and decompressing the remainders, the concealed and the original image are recovered during extraction. To increase the hiding payload, Arsalan et al. [12] developed Xuan et al. [20] approach by combining the compounding method with a Genetic Algorithm (GA). The integer wavelet transform converts cover images into the frequency domain. Then, the converted images are divided into pixel blocks, and a threshold is computed for each block. GA is used to obtain the optimal or near-optimal value to manage the embedding process and increase hiding capacity. The compounding operation is performed for all blocks with a value greater than a certain threshold.

Histogram modification-based technique: Generally, lossless watermarking methods cannot resist image operations and attacks. Therefore, histogram modification methods have been introduced to tackle the robustness issue. Embedding techniques based on this type are block-based, making them robust against several image processes. However, the embedding payload is small, and the distortion level is high [9]. Khan and Malik [16] presented a high-capacity reversible watermarking approach based on histogram shifting to provide an area for encoding the watermark. The location map is compressed and inserted into the cover image to reduce image degradation and ensure successful watermark retrieval during extraction. Gao et al. [14] developed a new reversible data-hiding method for medical images to enhance ROI contrast and reduce distortion. Medical images are segmented into ROI and background by adopting Otsu's thresholding technique.

To minimize background degradation caused by histogram shifting, pre-processing and peak-pair expansion are applied only to ROI pixels. Histogram equalization improves the ROI contrast during the hiding process. To detect manipulations, the feature-bit matrix produced from the ROI is encoded into the image background using the LSB technique. Yang et al. [10] reported a data hiding approach for protecting medical images. An adaptive threshold detector segmentation method is adopted to separate the medical images into ROI and RONI. The grayscale values are then stretched to improve the ROI contrast. The data are concealed in the highest bins of the stretched histogram to enhance the ROI's visual quality. The remaining data are concealed in the RONI using the histogram-shifting technique, regardless of the RONI's visual quality, to increase embedding capacity.

Expansion-based technique: In 2003, Tian [21] presented a new technique for reversible watermarking, called Difference Expansion (DE). This approach offers lower complexity and higher payload than previous reversible approaches. The proposed approach selects pixel pairs and embeds a single bit into each pair's difference values using the LSB technique. To improve hiding capacity, Alattar [22] improved the previous approach by concealing 2 bits of data in 3 pixels, and this was further developed by hiding 3 bits of data in 4 pixels [23]. This approach is further generalized by embedding a number of bits in vectors of adjacent pixels instead of pairs, triples, and quads of pixels [24].

The drawback of the DE approach is a reduced embedding payload because it must embed the location of image pixels, called a Location Map (LM), which is encoded alongside the watermark data. This LM is essential to recover the concealed data precisely without any loss. This large auxiliary data reduces capacity and increases the deformation level [8]. Therefore, Qasim et al. [25] developed a reversible system to emphasize the integrity and authenticity of medical images. The proposed method achieved high capacity and low degradation by encoding data into smooth regions within the ROI and removing the need for a large LM. However, encoding data in smooth areas within the ROI may make degradation more noticeable to human vision, as human vision is less sensitive to small modifications in smooth regions than in edges. Bhalerao et al. [26] presented a reversible watermarking method for ROI tamper detection and retrieval. The method merges Prediction Error Expansion (PEE) with histogram shifting to conceal watermark data in both ROI and RONI. Authentication data is encoded in ROI using the PEE technique. The compressed ROI copy is concealed in the RONI using the DE histogram-shifting technique. The drawbacks of the proposed approach are the manual, fixed-size segmentation of the ROI and the need for a location map to recover the original images during extraction. A reversible watermarking technique is proposed by Chidirala and Acharya [27] based on PEE. The proposed technique starts with dividing the grayscale image into two distinct groups: a group of higher-order pixels (a) and a group of lower-order pixels (b). Group (a) contains the tens and hundreds place values, while the values in the units place are stored in group (b).

This grouping shows that many connected pixels share equal values. The higher-order pixel group is utilized to encode data by applying the PEE technique. Tanwar and Panda [11] developed a reversible watermarking algorithm based on the pairwise PEE technique and histogram shifting to maximize the hiding capacity and minimize the degradation. PEE is classified based on the computed variance values of the prediction condition, followed by pairwise data embedding. Arham et al. [28] developed a high-capacity reversible watermarking method based on adaptive 2-bit LSB expansion and pixel shifting. The proposed method classifies pixels into two groups based on their 2-bit LSB values: expandable and non-expandable pixels. Data hiding is performed after shifting the non-expandable pixels to an expandable range. A shifting map records these modifications. Unlike classical reversible watermarking methods that require a location map to reconstruct original images, the proposed approach requires a shifting map to ensure exact retrieval of original images. A reversible watermarking technique is proposed by Arham et al. [29] to certify authentication of medical images while preserving diagnostic quality. The medical image is segmented into three regions: ROI, RONI, and border. Patient data are embedded into the ROI using a multi-layer DE. A semi-fragile watermarking based on 2D-DE is used to conceal watermark data in the RONI for tamper localization and retrieval. Auxiliary data is concealed in the border region using the LSB technique.

Our research proposes a fragile, reversible watermarking technique based on PEE to verify the integrity and authenticity of medical images by developing an algorithm that detects intentional and unintentional changes. Although both the proposed approach and the method presented by Qasim et al. [25] adopt automatic ROI identification and remove the need for a location map, two significant differences distinguish our developed scheme. First, we utilize PEE instead of DE. Second, we encode watermark data in edge regions within the ROI rather than in smooth regions. These two major differences result in lower perceptual distortion in watermarked images.

3. Proposed watermarking scheme

Most reversible watermarking methods require a location map for reversibility, which denotes the location of pixels used in the hiding process. This maximizes the additional overhead for watermarking algorithms [25]. Therefore, we used a PEE-based reversible watermarking technique to avoid the location map for reversibility and reduce additional data. This also increases embedding capacity and reduces distortion of the secured medical image. The proposed scheme comprises four phases: watermark generation, image processing, watermark embedding, and watermark extraction. Figure 1 demonstrates the block diagram of the proposed scheme.

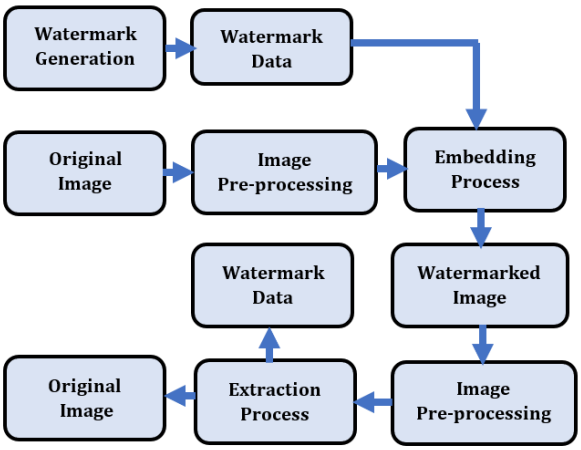

Figure 1. The block diagram of the proposed scheme

3.1 Watermark generation

Many techniques are used to produce watermark data for authentication and integrity purposes [8]. In this research, the metadata and digital signature of DICOM medical images are used as a watermark to confirm authenticity and integrity, respectively. Metadata is placed in the header of DICOM medical images and contains key information about the image and the patient. Table 1 describes an example of the image metadata used in our research. Furthermore, the Message Digest Five (MD5) hash function is used to calculate the image's digital signature. A 128-bit hash code is produced by this function. Any manipulation, intentional or unintentional, to the image changes its hash code. By comparing the original and recovered hash codes, the image manipulation can be detected. The two generated watermarks are merged and then compressed employing Run Length Encoding (RLE) to improve the watermarking imperceptibility and capacity. RLE algorithm is a simple and fast compression method compared to other compression techniques [25]. The steps for generating the watermark data can be described as follows:

- Extract the selected metadata from the header of DICOM medical images.
- Convert the metadata into its corresponding binary representation.
- Concatenate the binary representation of the metadata to form the metadata sequence.
- Use MD5 hash value to calculate the digital signature of the medical image for integrity verification.
- Concatenate the metadata sequence to the digital signature sequence to generate the watermark bits.
- Use RLE to compress the resulting watermark bits and generate the final watermark data.

3.2 Image pre-processing

Image preprocessing is performed on the medical image for ROI segmentation and edge detection. The ROI is identified from the image, and Canny edge detection is applied to the ROI to identify appropriate hiding regions. This process ensures consistent and accurate watermark data hiding.

ROI segmentation: The intensity values of the background in medical images are typically small and approach zero compared to those of the ROI [30]. For this reason, we adopted histogram thresholding to distinguish the image ROI from the RONI based on thresholding values (T). A pixel is considered ROI if its value is greater than T; otherwise, it is treated as part of the RONI. The value of T can be determined automatically or manually [30]. The value of T was determined experimentally and set to 75 after testing several values (25, 50, 75, and 100) on different images and visually evaluating the outcomes. A manual threshold was adopted to ensure reproducible and consistent ROI identification for medical images, since adaptive approaches identify the threshold independently for each image, which may generate variable ROI boundaries and lead to maladjusted edge detection used for data embedding. In addition, quantitative metrics are not applicable in the proposed method, although they can offer an objective assessment when specialist-labelled ROI are defined, because the ROI is defined as the foreground region implemented for hiding watermark data rather than as an anatomical structure defined by clinicians, and expert-labelled ROI are not available for the experimental images. To remove any holes that may appear in the ROI section, morphological functions including erosion, dilation, and hole- filling are applied (Figure 2).

Table 1. An example of metadata extracted from a medical image (The data does not belong to an actual person)

Group	Description	Value
0008,0022	Acquisition Date	20040305
0008,0032	Acquisition Time	214847
0008,0060	Modality	MR
0008,0090	Referring Physician Name	Dr. John Adam
0008,1030	Study Description	MRI Breast
0010,0010	Patient Name	Sarah Boston
0010,0020	Patient ID	111111
0010,0030	Patient Birth Date	01121990
0010,0040	Patient Sex	F
0010,1030	Patient Age	036Y
0018,0015	Body Part Examined	Breast
0028, 0010	Rows	512
0028, 0011	Columns	512
0028, 0100	Bit Allocated	16

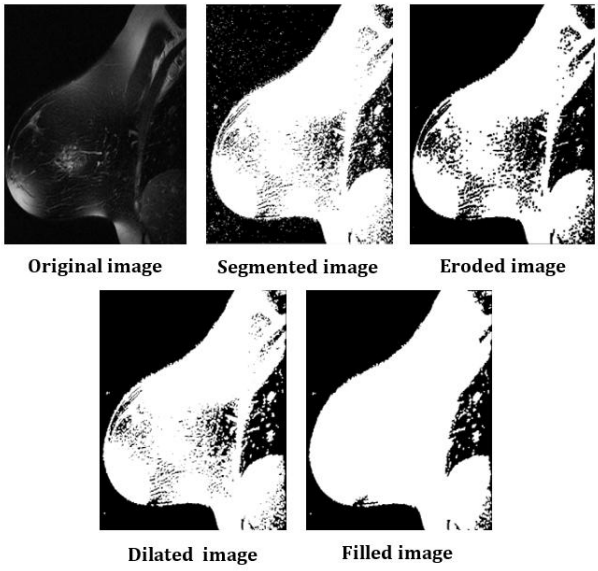

Figure 2. The block diagram of the proposed scheme

The erosion function is applied to minimize the ROI size and maximize the RONI size, while the dilation function is applied to maximize the ROI size. Hole filling automatically fills holes that appear in the RONI, which is surrounded by the ROI's connected borders [31].

Edge detection: Edges are key image features because they capture crucial details. Pixels along edges exhibit noticeable variations in grey levels, making them detectable using certain techniques. Common edge detection methods in image processing include Sobel, Prewitt, Laplacian, and Canny. Among these, Canny is considered the most accurate. It has two different thresholds to detect both thick and thin edges, making it capable of detecting faint edges and resisting noise. If a thin edge is connected to a thick edge, the thin edge is included in the resulting image, which contains the image edges [32]. In this paper, we used the Canny edge operator to detect the edges inside the image ROI. The watermark bits were inserted into the edges, taking advantage of the difficulty of visually detecting changes in these edges. We applied the Canny edge detector available in MATLAB using the 'edge' function with the Canny operator and its default parameter settings to all tested images to guarantee reproducible and consistent edge detection. The result of applying the Canny operator is shown in Figure 3.

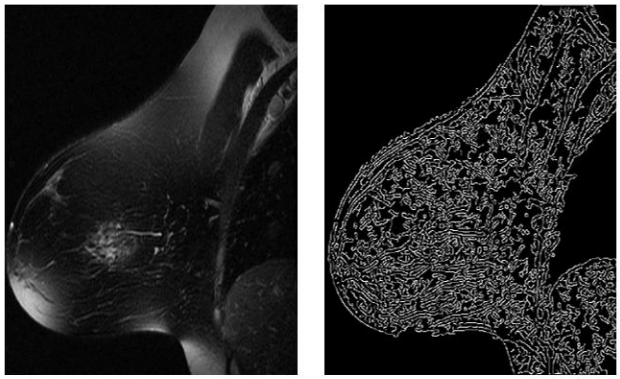

Figure 3. Canny edge detection applied to the ROI of an MRI breast image

The steps of implementing the Canny edge detection technique can be summarized as follows [32]:

Image smoothing: It is done by applying a Gaussian filter with a certain deviation sigma to decrease/remove noise

Identifying gradients: After smoothing, the strength of an edge is determined by calculating the image gradient. Then, the spatial gradient amount of an image is measured by applying the Sobel edge detector. Edges are defined by high-magnitude gradients after applying a Gaussian filter in the horizontal and vertical directions to compute the image gradient.

Edge point determination: Ridges in the gradient magnitude image may occur after performing the edge point identification in step (2); therefore, the algorithm keeps only those pixels on an edge with the largest gradient magnitude. This process is called non-maximal suppression. Then, hysteresis thresholding is applied to identify potential edges using two thresholds, high (Th) and low (Tl). Pixel values greater than Th are considered 'strong' edges, while pixel values between Th and Tl are considered 'weak' edges.

Edge-linking: Finally, the algorithm executes edge-linking by combining weak edges (that are not linked) with strong edges.

3.3 Watermark embedding

Most PEE watermarking techniques require a location map, an array that defines the pixel locations used to conceal watermark bits. This array is mandatory at extraction to regain the embedded data from the watermarked image. This increases the amount of data and, consequently, the level of distortion. Therefore, we used the watermark length and PEE-based reversible watermarking to retrieve both the encoded watermark and the original image without requiring additional data. The watermark bit length is inserted into the RONI by applying a simple DE technique reported by Tian [33].

Edge-blocks Identification: In this research, we developed an approach to encode the data into the edges of the ROI of medical images, which comprise high-frequency data, including changes in colour/intensity of pixel values. This helps reduce visual distortion and improves the invisibility of the encoded data, as human vision is less sensitive to small changes along edges than in smooth regions. The approach divides the segmented medical image into disjoint 2x2 pixel blocks (Figure 4). These 2x2 blocks are considered edge-blocks if at least one pixel within the block lies in the edge region produced by the Canny detector; otherwise, the blocks are considered non-edge-blocks. The hiding capacity of the proposed algorithm depends on the number of available 2x2 edge-blocks within the ROI. One bit of watermark data can be concealed in each selected edge-block. Therefore, the embedding capacity equals the number of eligible edge-blocks for hiding watermark bits.

P1 (i, j)	**P2** (i, j+1)
P3 (i+1, j)	**P4** (i+1, j+1)

Figure 4. A block of 2x2 pixels

Embedding process: The algorithm for embedding watermark data is described as follows:

- After the edge-blocks have been determined as described in the previous section, the top-left pixel (P1) represents the targeted pixel for concealing watermark data. The other three adjacent pixels represent the framework. In the block representation shown in Figure 4, P1 is the target pixel, and P2, P3, and P4 are its framework pixels.
- The predicted value is then calculated using Eq1:

$$\overline{P} = \begin{cases} \max(P2, P3) & if\ P4 \le \min(P2, P3) \\ \min(P2, P3) & if\ P4 \ge \max(P2, P3) \\ P2 + P3 - P4 & othewise \end{cases} \quad (1)$$

- The difference value between the predicted and the original pixel is defined as the prediction error, and it is identified by Eq 2:

$$P(error) = P1 - \overline{P} \quad (2)$$

- The binary form of the prediction error is then shifted left to produce space in its Least Significant Bit (LSB). The watermarking data (w), which is defined as a binary representation, is then placed in the LSB. This process

generates a modified prediction error and can be obtained by applying Eq 3:

$$\overline{P(error)} = 2P(error) + w \quad (3)$$

- The watermarked pixel will be produced by using Eq 4:

$$Pw = \overline{P} + \overline{P(error)} \quad (4)$$

- Finally, by replacing the values of P1 with Pw and keeping the neighboring pixels (P2, P3, P4) without changes, the watermarked image (W_IMG) is constructed. Algorithm 1 demonstrates the embedding process of watermark data.

3.4 Watermark extraction

The algorithm for watermark extraction and image can be described as follows:

- Segment the watermarked image into ROI and RONI as shown in Section 3.2.
- Extract the watermark length from the RONI part.
- Detect the edges within the image ROI as shown in Section 3.2.
- Divide the segmented medical image into non-overlapping blocks of 2x2 and identify the edge-blocks using the technique presented in Section 3.3.
- Calculate the predicted value $\overline{P}$ and the prediction error Pe(error) using Eq 1 and Eq 2, respectively.
- Convert the generated prediction error Pe(error) into binary form. If the LSB of the pixel value is 0, then watermark bit is '0' otherwise, the watermark bit is '1'.
- Retrieve the extracted data and determine the modified prediction error $\overline{\text{Pe(error)}}$ by using Eq 5:

$$\overline{\text{Pe(error)}} = \lfloor (\text{Pe(error)}/2) \rfloor \quad (5)$$

- The extracted pixel $\overline{\text{Pw}}$ can be calculated by applying Eq6:

$$\overline{\text{Pw}} = Pw - \overline{\text{Pe(error)}} \quad (6)$$

- Finally, by swapping the values of Pw with $\overline{\text{Pw}}$ and keeping pixels (P2, P3, P4) values unchanged, the original unmodified image (O_IMG) is retrieved. Algorithm 2 describes the extraction process of watermark data and recovering the original image.

4. Experimental results and discussion

To evaluate the performance of our approach, twelve medical images in various modalities were used. The image size is (512×512 pixels), (16-bit pixel depth), and the format is DICOM. These medical images comprise four brain MRI, four breast MRI, and four CT lung (Figure 5). The images were downloaded from The Cancer Imaging Archive (TCIA) [34], which is a freely available and standardized medical image database. The experimentation was done using MATLAB R2016a installed on PC run with Microsoft Windows 11, 16 GB RAM, and Core ™ i7-1065G7 Intel CPU.

4.1 Performance evaluation

The proposed method is evaluated against three main needs in the medical field: Invisibility/imperceptibility, reversibility, and fragility. Invisibility is the most important feature and shows how much the watermarked image differs from the original. Reversibility confirms that both the original images and the encoded data are precisely recovered at extraction. Fragility is the capability of detecting trivial alterations that occur in medical images.

Algorithm 1. Watermark embedding

Input: Original image (O_IMG), watermark data (w), Edge pixels
Output: Watermarked image (W_IMG)
Identify edge-blocks in original image from detected edge pixels
Compute length of watermark data, Len ← length (w)
Embed Len into RONI.
Initialize watermark counter, i ← 1
For each identified edge-block **do**
Assign the target pixel (P1← top-left pixel)
Assign the neighbouring pixel (P2← right pixel)
Assign the neighbouring pixel (P3← bottom pixel)
Assign the neighbouring pixel (P4← bottom-right pixel)
If P4 ≤ min (P2, P3), $\overline{P}$ ← max (P2, P3) // Compute PE value
Else if P4 ≥ max (P2, P3), $\overline{P}$ ← min (P2, P3)
    Else $\overline{P}$ ← P2+P3-P4
End if
P(error) ← P1 – $\overline{P}$ // Compute prediction error
$\overline{\text{P(error)}}$ ← 2 ∗ P(error) + w(i) // Compute modified PEE
Pw ← $\overline{\text{P}}$ + $\overline{\text{P(error)}}$ // Generate watermarked pixel
P1 ← Pw // Construct watermarked image
i ← i+1 // Get next watermark bit
If i > Len **then** // Check end of watermark
    Exit for
End if
End for

Algorithm 2. Watermark extraction

Input: Watermarked image (W_IMG)
Output: Original image (O_IMG), Watermark data (w)
Segment watermarked image into ROI and RONI
Extract watermark length (Len) from RONI
Detect edges inside the ROI
Identify edge-blocks from the detected edges
Assign integer values to w,x
Initialize watermark counter, i ← 1
For each identified edge-block do
  Assign the target pixel (P1← top-left pixel)
  Assign the neighbouring pixel (P2← right pixel)
  Assign the neighbouring pixel (P3← bottom pixel)
  Assign the neighbouring pixel (P4← bottom-right pixel)
  If P4 ≤ min (P2, P3), $\overline{P}$ ← max (P2, P3) // Compute PE value
    Else if P4 ≥ max (P2, P3), $\overline{P}$ ← min (P2, P3)
    Else $\overline{P}$ ← P2+P3-P4
  End if
  P(error) ← P1 – $\overline{P}$ // Compute prediction error
  x ← LSB of P(error) //Get LSB of computed prediction error
  If x = 0, w ← 0
    Else w ← 1
  End if
  $\overline{\text{Pe(error)}}$ ← ⌊(Pe(error)/2)⌋ // Compute modified PE
  $\overline{\text{Pw}}$ = Pw – $\overline{\text{Pe(error)}}$ // Extract watermarked pixel
  P1 ← $\overline{\text{Pw}}$ // Retrieve original image
  i ← i+1 // Get next watermark bit
  If i > Len then // Check end of watermark
    Exit for
  End if
End for

Invisibility: To evaluate the invisibility of both the original and the watermarked images, Structural Similarity Index (SSIM) and Peak Signal to Noise Ratio (PSNR) were used. In all the following equations, *MN* represents the image size, Io is the original image, and *Iw* is the watermarked image.

- **Peak signal to noise ratio:** This metric is used to compute the distortion level between the original and modified images. A higher PSNR indicates greater invisibility and lower distortion [8].

$$PSNR(I_o, I_w) = log_{10} \frac{MAX_I^2}{MSE} \times 10 \quad (7)$$

where *MAXI* is the highest probable pixel intensity, and MSE is the Mean Squared Error between the original image and the watermarked image.

$$MSE = \frac{1}{MN} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} (I_o(i,j) - I_w(i,j))^2 \quad (8)$$

- **Structural similarity index:** It is used to quantify the degradation in the structural details between the original image and the watermarked image. It compares the similarity of three aspects: structure, luminance, and contrast, and takes range of values between -1 and 1. SSIM value of 1 means that the original and watermarked images are identical [8].

$$SSIM(I_o, I_w) = \frac{(2\mu_{I_o}\mu_{I_w} + x1)(2cov + x2)}{(\mu_{I_o}^2 + \mu_{I_w}^2 + x1)(\sigma_{I_o}^2 + \sigma_{I_w}^2 + x2)}$$

$$\begin{cases} x1 = (y_1 z)^2 & y_1 = 0.01 \\ x2 = (y_2 z)^2 & y_2 = 0.03 \end{cases} \quad (9)$$

Where μ_{I_o} and μ_{I_w} represent the average of the pixels in the reference and modified images, $\sigma_{I_o}^2$ and $\sigma_{I_w}^2$ represent the standard deviation of the pixels of the reference and modified images, *x1* and *x2* are variables to avert imbalance when the denominator approaches 0, *Cov* represent the covariance of watermarked image, and *z* is the dynamic range of pixel intensity.

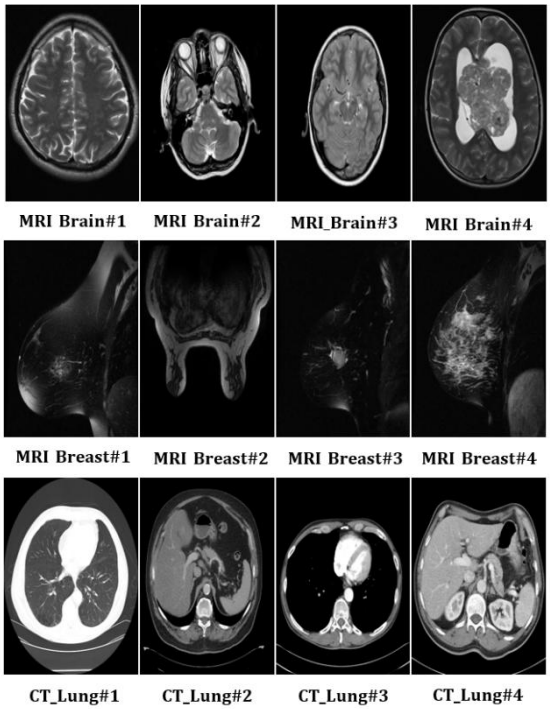

Figure 5. The twelve DICOM medical images used to evaluate the proposed approach

The invisibility and payload capacity of the proposed scheme were evaluated for the twelve medical images as shown in Table 2. PSNR and SSIM values between the original and watermarked images after encoding the watermark data were calculated to measure the amount of distortion. The maximum payload capacity was also defined by computing the number of 2x2 edge blocks within the ROI that can be used for hiding the watermark data. The results show that the values of PSNR are high and the values of SSIM are almost equal to 1. This ensures the key requirement of digital watermarking, which is invisibility. Moreover, across the twelve tested images, the proposed algorithm realized an average PSNR of 97.19±1.73 dB and an average SSIM of 0.999996±0.000010, demonstrating the high similarity between the original and watermarked images. To show the differences between the original and watermarked images, a residual map was produced by computing the absolute pixel-wise difference between the tested images. The generated residual map was amplified by a factor of 20 to enhance the visibility of small changes introduced by watermark encoding. The amplification was used only to enhance visualization and does not represent the actual distortion level of watermarked images (Figure 6).

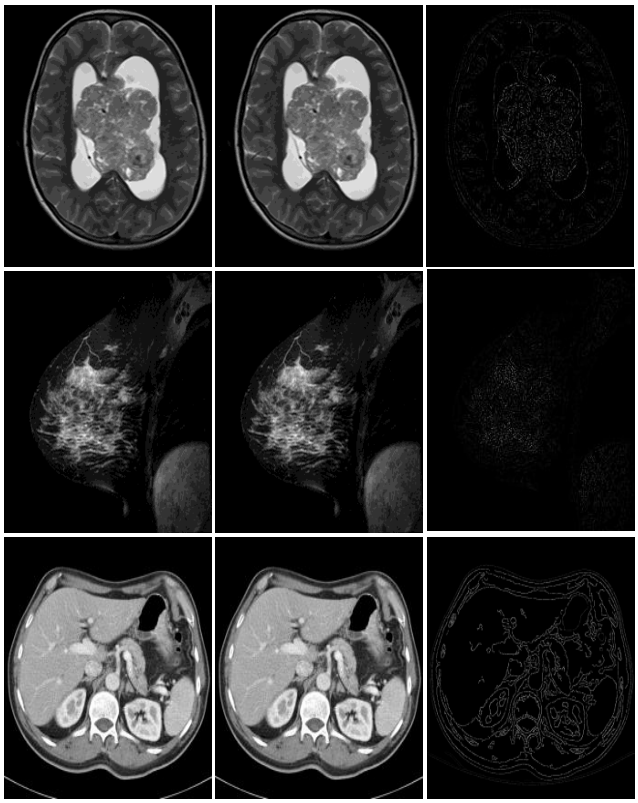

Figure 6. Examples of original and watermarked images after applying the proposed approach. The first column shows the original images, the second column shows the watermarked images, and the third column shows the residual map×20.

Table 2. PSNR and BER values after applying various operations to watermarked images

Medical Image	Watermark length (bits)	Maximum payload (bits)	PSNR (dB)	SSIM
MRI_Brain#1	7556	9096	97.96	1
MRI_Brain#2	7842	10749	96.32	1
MRI_Brain#3	8023	10456	96.50	1
MRI_Brain#4	7288	9899	99.97	1
MRI_Breast#1	7966	13125	98.88	1
MRI_Breast#2	7854	11473	97.43	1
MRI_Breast#3	8322	11996	94.65	0.99998
MRI_Breast#4	7815	11315	98.92	1
CT_Lung#1	7463	11065	97.25	1
CT_Lung#2	7825	8938	96.05	1
CT_Lung#3	8278	9963	94.21	0.99997
CT_Lung#4	7791	9767	98.15	1

Reversibility: To evaluate the reversibility of the proposed system during extraction, we measured the difference between the original and extracted images to ensure image reversibility. Moreover, the similarity between the encoded and extracted watermarks was measured to ensure watermark reversibility. For image reversibility, the PSNR metric was used, while Bit Error Rate (BER) was used for watermark reversibility [8].

$$BER = \frac{EB}{TB} \quad (10)$$

where EB refers to the number of incorrect bits and TB refers to the total number of bits.

The obtained PSNR values between the original and retrieved images were ∞, which means there are no numerical differences in pixel values between the images, as the MSE value is 0. The obtained BER values are 0, meaning the embedded and retrieved watermarks are identical. These results support the reversibility of the proposed algorithm, as both the original unchanged image and the concealed watermark are recovered precisely during extraction.

Fragility: The aim of this study is to verify the integrity and authenticity of medical images. This is achieved only if the original image and the inserted data are recovered exactly during extraction. Any manipulation to the watermarked image, even trivial, must deform the hidden data, resulting in a mismatch between the encoded and retrieved watermarks. To quantify the algorithm's fragility, we used PSNR and BER to measure the similarity between the original and watermarked images, as well as between the original and extracted watermarks, after applying various operations that simulate intentional and unintentional alterations. In addition, we performed common active security attacks that aim to compromise the integrity and authenticity of digital watermarking schemes, including watermark forgery, copy attack, and collusion attack. In the watermark forgery attack, a fake watermark was inserted into the watermarked image. The authentication watermark data produced from one watermarked image was inserted into another medical image to simulate the copy attack. In a collusion attack, two watermarked images are combined to alter the encoded watermark. The resultant PSNR and BER values between the retrieved images and watermark data after applying the operations/attacks confirm the fragility of the algorithm against the applied operations, as the PSNR values are not ∞, and the BER values are not 0 (Table 3). As shown in the results, the intensity adjustment operation produced the lowest PSNR among all tested operations because it changes the entire intensity distribution of the image. Furthermore, clipping and saturation processes may notably modify pixel values, causing a significant reduction in image similarity.

4.2 Comparison with other approaches

The aim of our research is to ensure the authenticity and integrity of medical images by developing a watermarking technique that meets the key requirements of medical imaging: invisibility and reversibility. The integrity and authenticity data were inserted into the edges of the ROI to preserve the significant parts of the image and to decrease visual distortion. The concealed data is recovered during extraction along with the original image, without the need for a location map. Many reversible watermarking schemes were developed in the literature to ensure the integrity and authenticity of digital images [11, 25-27, 29, 35-38]. Some of these schemes are applied to medical images of various modalities and formats. The performance evaluation of our developed technique was compared with several reversible techniques recently presented in the literature using criteria commonly used in medical image watermarking (Table 4).

Table 3. PSNR and BER values after applying various operations to watermarked images

Operations	Watermarked images	PSNR (dB)	BER
Median filter	MRI_Brain#1	71.22	0.3558
Salt and pepper noise (d= 0.0005)	MRI_Breast#4	66.53	0.4028
Gaussian filter (σ =0.5)	CT_Lung#1	73.89	0.4712
Gaussian noise (SNR= 5 dB)	MRI_Brain#3	74.65	0.4325
Rotate (5^0) & cropping	MRI_Breast#3	56.18	0.3955
Crop (95%) & resizing	CT_Lung#3	78.70	0.3856
Adjust brightness (±5)	MRI_Breast#2	80.93	0.2933
Adjust intensity	CT_Lung#2	12.88	0.3745
Watermark forgery	MRI_Brain#4	68.55	0.4131
Copy attack	CT_Lung#4	65.12	0.3914
Collusion attack	MRI_Brain#2	64.73	0.3544

In approaches [26, 29, 35, 38], a pixel-location map is required during extraction to recover the reference image and watermark. This maximizes distortion and reduces the embedding algorithm's capacity. Approach [29] requires a clinician to define the image ROI, and the entire original image

cannot be reconstructed during extraction. In approach [26], the size of ROI is 100x100, which means it can only be applied to specific images. Scheme [36] achieved higher visual image quality compared to other schemes; however, our approach surpassed it in terms of PSNR values. This is due to embedding the data into the ROI edges that are less sensitive to small modifications than smooth regions.

Furthermore, we compared our approach with a well-known approach that achieved a high level of invisibility reported by Qasim et al. [25]. In this research, medical images are automatically divided into ROI and RONI. A fully lossless watermarking technique using the DE method is developed to conceal data in the ROI section using smooth areas. The scheme delivered highly invisible watermarked images with PSNR values ranging from 92.18 to 99.94 dB. For a fair comparison, we applied the algorithm stated in [25] to the same twelve medical images and watermark data used in our research. The ROI was automatically identified before applying the DE-based watermarking process. The comparison was performed using the resulting PSNR values under the same testing conditions to measure distortion. Figures 7-9 clearly show that our approach achieved higher PSNR values for ten of the twelve tested images. However, MRI_Breast#3 and CT_Lung#3 achieved lower PSNR values than the approach in [25]. These two images comprise relatively smaller edge regions compared to their smooth area, which limits the number of edge blocks available for concealing data using the proposed edge-based method. Therefore, the performance superiority of our proposed method depends on the availability of adequate edge regions within the ROI.

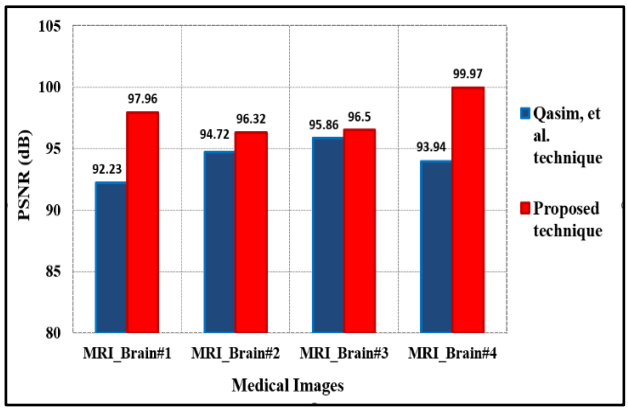

Figure 7. PSNR values for the proposed technique and Qasim, et al. [25] technique after applying the watermark algorithms to MRI brain images

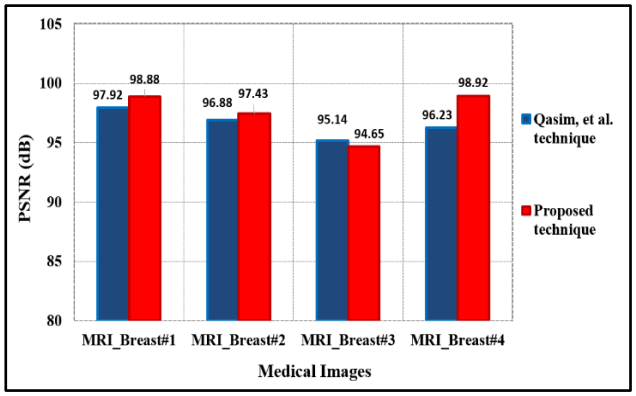

Figure 8. PSNR values for the proposed technique and Qasim, et al. [25] technique after applying the watermark algorithms to MRI breast images

Table 4. Performance comparison of our scheme versus various approaches stated in the literature using various criteria

Scheme	Hiding technique	Hiding region	ROI segmentation	Reversibility	Payload (bits)	Location map (size)	Visual quality
Atta-ur-Rahman, et al. [38]	-Residue Number System (RNS) -Chaotic key	Whole image	No	Entire image	Avg=12100	Not required	Avg.PSNR=71.10dB
Mharakurwa [36]	-DE -NDE	-ROI -RONI	Automatic	Entire image	Avg=23041	Not required	Avg.PSNR=84.29dB Avg. SSIM= 1
Bhalerao, et al. [26]	-DE -Histogram shifting	-ROI -RONI	Static size 100x100 pixels	Entire image	Avg=39322	Required (576 bits)	Avg.PSNR=55.48dB Avg. SSIM= 0.99
Mosco-Garcia, et al. [35]	-PTB -LSB -Checksum insertion	Whole image	No	Entire image	51652	Required (not reported)	PSNR= 67.59dB SSIM= 0.9995
Arham, et al. [29]	-DE -2D-DE	ROI	Manual	Entire image excluding border	10240	Required (not reported)	Avg.PSNR above 38dB Avg. SSIM close to 1
Proposed	-PEE -DE	-ROI -RONI	Automatic	Entire image	Avg=7835	Not required	Avg.PSNR=97.19dB Avg.SSIM= 0.999996

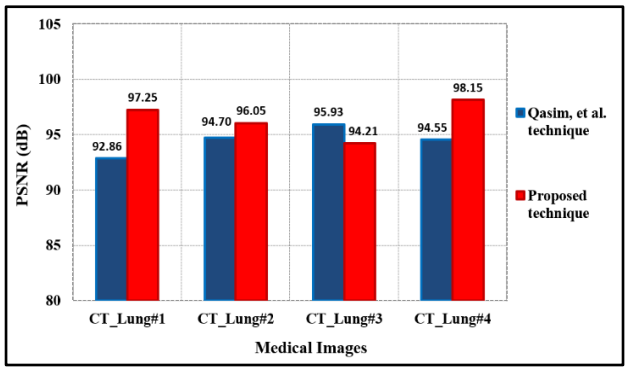

Figure 9. PSNR values for the proposed technique and Qasim, et al. [25] technique after applying the watermark algorithms to CT lung images

5. Conclusion

This paper developed a fragile reversible watermarking method for medical imaging security based on PEE and Canny edge detection. The developed method automatically divides the medical image into ROI and RONI. The integrity and authentication data are compressed and inserted into the Canny-detected edges within the ROI to reduce the noticeable visual distortion in the watermarked image and improve the invisibility of the encoded data. In the extraction process, the exact original image was reconstructed after successfully recovering the hidden data, without needing the location map. This controls and maximizes the embedding level whilst minimizing image distortion. Experimental evaluation on twelve 16-bit DICOM images, comprising brain MRI, breast MRI, and lung CT, achieved high visual quality, with PSNR values ranging from 94.21 to 99.97 dB and SSIM values approaching 1. The fragility experiments ensured the ability to discover intentional and unintentional manipulation. Compared with the ROI-based DE technique, our proposed method achieved higher PSNR values in most tested images. However, the limitation of this research is the relatively small dataset obtained from a single publicly available database, which restricts the generalizability of the results. In addition, we used MD5 for integrity verification, which has known security limitations. For future work, we recommend evaluating the proposed scheme using larger datasets from various sources, including different image sizes, formats, and modalities, and using a stronger hash function such as SHA-256 to improve integrity verification. We also suggest investigating tamper localization and recovery, the robustness-fragility trade-off, and recent DICOM security standards.

Ethical issue

The authors are aware of and comply with best practices in publication ethics, specifically regarding authorship (avoidance of guest authorship), dual submission, manipulation of figures, competing interests, and compliance with research ethics policies. The authors adhere to publication requirements that the submitted work is original and has not been published elsewhere. All survey participants provided informed consent before participating, and the anonymity and confidentiality of all respondents were strictly maintained throughout the research process.

Data availability statement

The manuscript contains all the data. However, additional data will be provided by the corresponding author upon reasonable request.

Conflict of interest

The authors declare no potential conflict of interest.

References

[1] T. M. Godinho, L. M. Silva, and C. Costa, "An automation framework for PACS workflows optimization in shared environments," in 10th Iberian Conference on Information Systems and Technologies (CISTI), Aveiro, Portugal, 2015: IEEE, pp. 1-7, doi:10.1109/CISTI.2015.7170422.

[2] O. S. Pianykh, Digital imaging and communications in medicine (DICOM): a practical introduction and survival guide, 2nd ed ed. 2nd ed. Springer. Berlin, Germany, 2009.doi:https://doi.org/10.1007/978-3-540-74571-6_5.

[3] N. A. Memon, A. Chaudhry, M. Ahmad, and Z. A. Keerio, "Hybrid watermarking of medical images for ROI authentication and recovery," International Journal of Computer Mathematics, vol. 88, no. 10, pp. 2057-2071, 2011, doi: abs/10.1080/00207160.2010.543677.

[4] R. Priya and V. Sadasivam, "A survey on watermarking techniques, requirements, applications for medical images," Journal of Theoretical and Applied Information Technology, vol. 65, no. 1, pp. 103-120, 2014.

[5] S. C. Liew and J. M. Zain, "Tamper localization and lossless recovery watermarking scheme," in Software Engineering and Computer Systems: Springer, 2011, pp. 555-566.doi:https://doi.org/10.1007/978-3-642-22170-5_48.

[6] L. O. M. Kobayashi, S. S. Furuie, and P. S. L. M. Barreto, "Providing integrity and authenticity in DICOM images: a novel approach," IEEE Transactions on Information Technology in Biomedicine, vol. 13, no. 4, pp. 582-589, 2009, doi: 10.1109/TITB.2009.2014751.

[7] J. Guru and H. Damecha, "Digital watermarking classification: a survey," International Journal of Computer Science Trends and Technology (IJCST) vol, vol. 5, pp. 8-13, 2014.

[8] A. F. Qasim, F. Meziane, and R. Aspin, "Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review," Computer Science Review, vol. 27, pp. 45-60, 2018, doi: 10.1016/j.cosrev.2017.11.003.

[9] A. Khan, A. Siddiqa, S. Munib, and S. A. Malik, "A recent survey of reversible watermarking techniques," Information sciences, vol. 279, pp. 251-272, 2014, doi: https://doi.org/10.1016/j.ins.2014.03.118.

[10] Y. Yang, W. Zhang, D. Liang, and N. Yu, "A ROI-based high-capacity reversible data hiding scheme with contrast enhancement for medical images," Multimedia Tools and Applications, vol. 77, no. 14, pp. 18043-18065, 2018, doi: https://doi.org/10.1007/s11042-017-4444-0.

[11] L. Tanwar and J. Panda, "Hybrid reversible watermarking algorithm using histogram shifting and pairwise prediction error expansion," Multimedia Tools and Applications, vol. 83, no. 8, pp. 22075-

22097, 2024, doi: https://doi.org/10.1007/s11042-023-15508-5.
[12] M. Arsalan, S. A. Malik, and A. Khan, "Intelligent reversible watermarking in integer wavelet domain for medical images," Journal of Systems and Software, vol. 85, no. 4, pp. 883-894, 2012, doi: https://doi.org/10.1016/j.jss.2011.11.005.
[13] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," IEEE transactions on image processing, vol. 14, no. 2, pp. 253-266, 2005, doi: 10.1109/TIP.2004.840686.
[14] G. Gao, X. Wan, S. Yao, Z. Cui, C. Zhou, and X. Sun, "Reversible data hiding with contrast enhancement and tamper localization for medical images," Information Sciences, vol. 385, pp. 250-265, 2017, doi: https://doi.org/10.1016/j.ins.2017.01.009.
[15] T.-S. Nguyen, C.-C. Chang, and N.-T. Huynh, "A novel reversible data hiding scheme based on difference-histogram modification and optimal EMD algorithm," Journal of Visual Communication and Image Representation, vol. 33, pp. 389-397, 2015, doi: 10.1016/j.jvcir.2015.10.008.
[16] A. Khan and S. A. Malik, "A high capacity reversible watermarking approach for authenticating images: Exploiting down-sampling, histogram processing, and block selection," Information Sciences, vol. 256, pp. 162-183, 2014, doi: https://doi.org/10.1016/j.ins.2013.07.035.
[17] W. He, K. Zhou, J. Cai, L. Wang, and G. Xiong, "Reversible data hiding using multi-pass pixel value ordering and prediction-error expansion," Journal of Visual Communication and Image Representation, vol. 49, pp. 351-360, 2017, doi: 10.1016/j.jvcir.2017.10.001.
[18] B. Lei, E. L. Tan, S. Chen, D. Ni, T. Wang, and H. Lei, "Reversible watermarking scheme for medical image based on differential evolution," Expert Syst. Appl., vol. 41, no. 7, pp. 3178-3188, 2014. [Online]. Available: http://ac.els-cdn.com/S0957417413009317/1-s2.0-S0957417413009317-main.pdf?_tid=e3850d26-0260-11e6-ab01-00000aab0f6c&acdnat=1460652763_54ccd2807cb900d7165673f21f8bd235.
[19] A. Roček, K. Slavíček, O. Dostál, and M. Javorník, "A new approach to fully-reversible watermarking in medical imaging with breakthrough visibility parameters," Biomedical Signal Processing and Control, vol. 29, pp. 44-52, 2016, doi: https://doi.org/10.1016/j.bspc.2016.05.005.
[20] G. Xuan, C. Yang, Y. Zhen, Y. Q. Shi, and Z. Ni, "Reversible data hiding using integer wavelet transform and companding technique," in International Workshop on Digital Watermarking, 2004: Springer, pp. 115-124, doi: https://doi.org/10.1007/978-3-540-31805-7_10.
[21] J. Tian, "Reversible data embedding using a difference expansion," IEEE transactions on circuits and systems for video technology, vol. 13, no. 8, pp. 890-896, 2003, doi: 10.1109/TCSVT.2003.815962.
[22] A. M. Alattar, "Reversible watermark using difference expansion of triplets," in International Conference on Image Processing (Cat. No.03CH37429), Barcelona, Spain, 2003: IEEE, pp. 501-504, doi: 10.1109/ICIP.2003.1247008.
[23] A. M. Alattar, "Reversible watermark using difference expansion of quads," in International Conference on Acoustics, Speech, and Signal Processing (ICASSP'04), Montreal, Que., Canada, 2004: IEEE, pp. 377-380, doi: 10.1109/ICASSP.2004.1326560.
[24] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," IEEE Transactions on Image Processing, vol. 13, no. 8, pp. 1147-1156, 2004, doi: 10.1109/TIP.2004.828418.
[25] A. F. Qasim, R. Aspin, F. Meziane, and P. Hogg, "ROI-based reversible watermarking scheme for ensuring the integrity and authenticity of DICOM MR images," Multimedia Tools and Applications, vol. 78, no. 12, pp. 16433-16463, 2019, doi: https://doi.org/10.1007/s11042-018-7029-7.
[26] S. Bhalerao, I. A. Ansari, and A. Kumar, "A reversible medical image watermarking for ROI tamper detection and recovery," Circuits, Systems, and Signal Processing, vol. 42, no. 11, pp. 6701-6725, 2023, doi: https://doi.org/10.1007/s00034-023-02416-0.
[27] B. Chidirala and B. Acharya, "Prediction error expansion based reversible watermarking scheme in higher order pixels," Sādhanā, vol. 49, no. 3, p. 227, 2024, doi: https://doi.org/10.1007/s12046-024-02569-x.
[28] A. Arham, S. A. I. Alfarozi, and H. A. Nugroho, "A high-capacity reversible watermarking technique using bit-level expansion and pixel shifting," Communications in Science and Technology, vol. 10, no. 2, pp. 477-492, 2025, doi: 10.21924/cst.
[29] A. Arham, T. B. Adji, S. A. I. Alfarozi, and H. A. Nugroho, "Reversible watermarking for medical images using ROI-based tamper localization and recovery," Franklin Open, p. 100545, 2026, doi: https://doi.org/10.1016/j.fraope.2026.100545.
[30] A. M. Hasan, F. Meziane, and M. A. Kadhim, "Automated segmentation of tumours in MRI brain scans," in Proceedings of the 9th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC), Rome, Italy, 2016, pp. 55-62, doi: 10.5220/0005625900550062.
[31] P. Soille, Morphological image analysis: principles and applications. 2nd ed. Springer. Berlin, Germany, 2013.doi:10.1007/978-3-662-05088-0.
[32] L.-H. Gong, C. Tian, W.-P. Zou, and N.-R. Zhou, "Robust and imperceptible watermarking scheme based on Canny edge detection and SVD in the contourlet domain," Multimedia tools and applications, vol. 80, no. 1, pp. 439-461, 2021, doi: https://doi.org/10.1007/s11042-020-09677-w.
[33] J. Tian, "Reversible watermarking by difference expansion," in Proceedings of workshop on multimedia and security, 2002, pp. 19-22.
[34] A. F. Qasim, F. Meziane, and R. Aspin, "A reversible and imperceptible watermarking scheme for MR

images authentication," in Proceedings of the 24th International Conference on Automation and Computing (ICAC'2018), Newcastle upon Tyne, UK, 2018: IEEE, doi: 10.23919/IConAC.2018.8749000.

[35] J. E. Mosco-Garcia, M. Cedillo-Hernandez, and H. Shouno, "Data Hiding for Clinical Information in DICOM Images via Reversible Halftone Fragile Watermarking," in New Trends in Intelligent Software Methodologies, Tools and Techniques: Proceedings of the 24th International Conference on New Trends in Intelligent Software Methodologies, Tools and Techniques (SoMeT_25), 2025: SAGE Publications 1 Oliver's Yard, 55 City Road, London, EC1Y 1SP, pp. 469-482, doi: https://doi.org/10.3233/FAIA2505.

[36] E. T. Mharakurwa, "A prediction error nonlinear difference expansion reversible watermarking for integrity and authenticity of DICOM medical images," International Journal of Advanced Computer Science and Applications, 2022, doi: 10.14569/IJACSA.2022.0130326.

[37] N. Memon and A. Alzahrani, "Prediction-based reversible watermarking of CT scan images for content authentication and copyright protection. IEEE Access 8, 75448–75462 (2020). Paper," ed, 2020.doi:10.1109/ACCESS.2020.2989175.

[38] Atta-ur-Rahman, K. Sultan, N. Aldhafferi, A. Alqahtani, and M. Mahmud, "Reversible and fragile watermarking for medical images," Computational and mathematical methods in medicine, vol. 2018, pp. 1-7, 2018, doi: https://doi.org/10.1155/2018/3461382.