Multimedia Tools and Applications (2022) 81:14045–14063
https://doi.org/10.1007/s11042-022-12082-0

Multipurpose medical image watermarking for effective security solutions

Rishi Sinhal[1] · Sachin Sharma[2] · Irshad Ahmad Ansari[1] · Varun Bajaj[1]

Received: 15 March 2021 / Revised: 23 November 2021 / Accepted: 4 January 2022 /
Published online: 25 February 2022

Abstract

Digital medical images contain important information regarding patient's health and very useful for diagnosis. Even a small change in medical images (especially in the region of interest (ROI)) can mislead the doctors/practitioners for deciding further treatment. Therefore, the protection of the images against intentional/unintentional tampering, forgery, filtering, compression and other common signal processing attacks are mandatory. This manuscript presents a multipurpose medical image watermarking scheme to offer copyright/ownership protection, tamper detection/localization (for ROI (region of interest) and different segments of RONI (region of non-interest)), and self-recovery of the ROI with 100% reversibility. Initially, the recovery information of the host image's ROI is compressed using LZW (Lempel-Ziv-Welch) algorithm. Afterwards, the robust watermark is embedded into the host image using a transform domain based embedding mechanism. Further, the 256-bit hash keys are generated using SHA-256 algorithm for the ROI and eight RONI regions (i.e. RONI-1 to RONI-8) of the robust watermarked image. The compressed recovery data and hash keys are combined and then embedded into the segmented RONI region of the robust watermarked image using an LSB replacement based fragile watermarking approach. Experimental results show high imperceptibility, high robustness, perfect tamper detection, significant tamper localization, and perfect recovery of the ROI (100% reversibility). The scheme doesn't need original host or watermark information for the extraction process due to the blind nature. The relative analysis demonstrates the superiority of the proposed scheme over existing schemes.

Keywords Medical image watermarking · Ownership verification · Tamper localization · ROI recovery · Reversibility · Blind watermarking

✉ Irshad Ahmad Ansari
irshad@iiitdmj.ac.in

Extended author information available on the last page of the article

1 Introduction

Healthcare facilities are improving these days to facilitate people in a familiar way. The uses of advanced communication technologies and internet have been increased to provide healthcare services to patients. Tele-health, telemedicine and teleradiology are some of the growing fields to provide medical facilities to people without the need to go to the hospitals or clinics. Online consultations with doctors are being common and necessary (during critical times such as COVID-19 pandemic) procedures, further it also help patients to avoid travelling in general cases [4]. The availability of high speed internet and user friendly online platforms makes the sharing of digital data such as voice messages, diagnosis reports, and radiological images (i.e. CT scan, X-ray, MRI etc.) easier along with the online video consultations [30]. It is obvious that the medical images or reports are an important data in terms of deciding future actions for better results. Any modification in digital data (e.g. Medical images) due to signal processing attacks or intentional alterations by attackers can affect diagnosis process that can be hazardous for patients. Specifically, the change in the ROI part of the medical images can be more harmful [10]. Medical images are shared in the same way as the general digital images and therefore the signal or image processing attacks can affect the medical images in a similar fashion. A large number of images are shared/communicated by the people in day-to-day life. Due to easy availability and widespread use of the online medium, digital data security has been an essential and demanding research issue [2, 38]. Data security can be effectively achieved by using Data hiding techniques [20] such as steganography [21, 22], data encryption [23, 42] and digital watermarking [11]. Digital image watermarking [41] offers effective solutions to provide security to digital images against intended or accidental attacks [25, 26].

In the digital image watermarking process [19, 35], the digital information (i.e. watermark) is inserted into the digital image (i.e. host or carrier) in a well-defined algorithmic manner to provide copyright protection [24], tamper detection, proof of ownership, image authentication and restoration etc. Digital image watermarking can be categorized into different types [27]. It is classified as robust, semi-fragile and fragile watermarking based on the robustness [15]; whereas it is categorized as blind, semi-blind and non-blind watermarking based on extraction process [16]. It can also be divided into visible or invisible watermarking based on the imperceptibility of the watermark. Another classification divides the digital watermarking into spatial domain and frequency domain watermarking based on the type of domain used for the process. Generally, robust watermarking is used for copyright protection and ownership identification [32]. Fragile watermarking is preferred for tamper detection, localization and restoration of the tampered region [40]. According to the watermarking literature, frequency domain techniques are preferred for robust watermark insertion because of their effective performance against various signal processing attacks. On the other side, spatial domain approaches are mostly used for fragile watermark insertion. In all these cases, a blind mechanism does not need the original host or watermark at the time of extraction process; but the host or other side information is required for the extraction procedure in case of a non-blind approach [6]. Digital watermarking is an open, ongoing, and challenging research domain in the modern time of digital advancements and progressive teleradiological applications.

As per the literature, Coatrieux et al. [7] presented the importance of watermarking in medical field for providing security solutions such as integrity control and authentication of medical information. The manuscript discussed different scenarios to provide solutions to the security issues and requirements of the medical field with the help of digital watermarking.

Chao et al. [5] proposed a non-blind data hiding method for communicating digital medical information among different hospitals securely. The method combined different types of medical data into a mark image that can be extracted by the authorized personnel at the time of extraction. Nonetheless, the scheme can't be used for tamper localization and self-recovery purposes. Guo and Zhuang [12] introduced a watermarking scheme for the authentication and integrity verification of medical images. The scheme has lossless nature in terms of the recovery of the complete image. However, there is a limitation due to the non-blind nature of the scheme that the original watermark data such as EPR (electronic patient record) is needed for authentication purposes. Das and Kundu [8] offered a blind watermarking scheme using SHA (Secure Hash Algorithm)-256 and AES (advanced encryption standard) encryption for authentication and integrity control of medical images. The scheme has significant parametric results in terms of payload (in bits per pixel) and PSNR, nevertheless the scheme didn't have the ability to protect copyright and recover the tampered portion of the medical image. Eswaraiah and Reddy [9] presented a fragile medical image watermarking scheme for tamper detection and ROI recovery. The scheme embedded the authentication code and the recovery information into the RONI region using an LSB replacement approach. The experimental results proved that the scheme had significant performance in terms of imperceptibility, tamper detection, and ROI recovery; but the scheme didn't provide copyright/ownership protection.

Badshah et al. [3] proposed an LZW compression mechanism-based watermarking scheme for ultrasound medical images. The ROI information and the secret key were combined to get the watermark. This watermark was compressed using the LZW algorithm to reduce the payload. The LSB replacement was performed to embed the compressed watermark information into the RONI region. The scheme has high imperceptibility, significant ROI authentication, and ROI restoration; however, the scheme lacks in the authentication of the embedding region (i.e. RONI). Additionally, the scheme does not provide ownership verification that is an important aspect to confirm the patient's credentials. Parah et al. [28] introduced two medical image watermarking schemes for copyright protection. The schemes were based on block-wise division and DCT transform. The scheme provided satisfactory results in terms of imperceptibility and robustness, however the ability of tamper detection and self-recovery were not achieved. Zear et al. [39] offered a robust watermarking technique for the images related to healthcare. The method used multi-level DWT (Discrete wavelet transform), DCT (Discrete cosine transform), and SVD (Singular value decomposition) for the watermarking process. During embedding, three different watermark were embedded into the host image for verifying information regarding doctor, patient's reports and data integrity. The method reported only ownership/copyright protection. The scheme is not able to provide tamper detection and restoration, which are very essential features for medical images. Swaraja et al. [34] offered a multipurpose watermarking method for medical images for protection of copyrights/ownership, tamper detection, and the recovery of ROI. An optimization algorithm was used to select the embedding region in the RONI for inserting dual watermarks. Although the scheme has multiple features and acceptable results in terms of parametric values, it did not discuss the case of tampered RONI. In case of tampered RONI, the reliability or authenticity of the extracted data should had been investigated because the authentication and the recovery of ROI depends on the reliability of the extracted information. Alshanbari [1] recently proposed a non-blind multipurpose watermarking scheme for medical images using DWT, SVD, and LZW (Lempel-Ziv-Welch) algorithm. Although the imperceptibility is high but robustness results are marginal. Moreover, the scheme provides tamper detection and restoration only for

ROI (region of interest) regions at low tampering rates. Further, the RONI has been selected as the embedding region, but the effect of the tampered embedding region (i.e. RONI) on the ROI recovery has not been discussed.

Since the intentional/unintentional manipulations usually affect the complete image (ROI and RONI) in the same manner, the possibility of modifications in the embedding region can't be ignored. It is also an important fact that the reliability of the extracted watermark depends on the originality of the embedding region (i.e. RONI). Therefore, the authentication of both regions (ROI and RONI) is indispensable against modification due to different signal processing attacks and tampering/forgery. In the proposed work, a recently proposed robust scheme [32] and the fragile scheme [3] are merged in an improved manner to offer an effective multipurpose watermarking scheme for medical images. Due to its multipurpose nature, the scheme includes the features of robust as well as fragile watermarking. It offers copyright protection, tamper detection and localization (for ROI and RONI), and recovery of the ROI. The RONI region is divided into different segments for better tamper localization. Additionally, the scheme does not require the original host data or other side information for watermark extraction because of the blind nature of the scheme. The scheme is able to recover the ROI part (100% reversibility) in case of tampering (excluding embedding region); which can surely be beneficial in medical image watermarking. The prime contribution of the proposed work are as follows:

1) To the best knowledge of authors, the first-ever scheme that offers tamper detection/localization for the ROI as well as the segmented RONI regions.
2) Unlike many existing medical watermarking schemes, the proposed work ensures the authenticity of the embedding region (i.e. RONI), thus it increases the possibility of the ROI recovery even in case of severe tampering.
3) The scheme can recover the ROI with 100% reversibility even after having blind nature.
4) The scheme confirms that the image is not usable for further processing when the embedding region has tampered with. Thus, it alerts timely for further actions related to the patient's health.
5) The scheme offers significant imperceptibility and high robustness against different attacks even after having multipurpose nature.

The successive sections present the proposed scheme, experimental results and discussion, and conclusion respectively.

2 Preliminaries

2.1 LZW (Lempel-Ziv-Welch) algorithm

It is a widely utilized compression algorithm presented in 1984 by Terry Welch [37]. It is lossless in nature, which means there is no data loss while compressing and decompressing the data. It has been utilized in the UNIX utility program (named as 'compress') for faster performance with less storage space. The image file format "GIF" (Graphics interchange format) is also based on the LZW compression algorithm. The LZW technique is structured using a table (which is known as a string table), which maps or converts the input character strings into the codes of fixed- length. This string table commonly has 4096 entries, out of

which the first 256 entries are allocated for representing 8-bit characters (single bytes) from the input data. The remaining entries are used during the encoding process for the repeated sequences of input data. During the decoding process, the data of the compressed (or encoded) version is translated back into characters using the string table [3].

2.2 SHA-256 algorithm

The SHA-256 is an extensively used hash algorithm for cryptographic operations. It is a part of a set of hash functions named as SHA-2, published by NIST (National Institute of Standards and Technology) in 2001 [17, 18]. It is a one-way hash algorithm, which means that the hash key can be generated from the input data but the input data cannot be obtained from the hash key. The SHA-256 has larger digests (hash values) messages having 256-bit length. This feature helps to protect against attacks more effectively. Additionally, it can handle bigger block size of data. In SHA-256, the data is first preprocessed by padding the input data and then the padded input is partitioned into blocks. After setting the initialization values, the hash operation is performed. Finally, the 256-bit hash key (message digest) is obtained [29].

2.3 Slantlet transform

The Slantlet transform is a modified orthogonal form of DWT having superior time localization with two zero moments [31]. Instead of using the concept of filter bank iteration (as in DWT), the slantlet transform framework used diverse filters at each scale. The frequency selectivity of the filter bank is lower. This low frequency selectivity results in better time localization. Due to better time localization feature, the Slantlet transform can provide better edge representation. The Slantlet transform can be utilized for the study of piecewise linear function having discontinuities. It has better ability to model the discontinuous nature and can be used in the image processing applications for the analysis of abrupt changes, texture feature, and the detection of the edges. It is also used in denoising applications very well because it has ability to smoothen the data without compromising the edges [33, 36].

3 Proposed scheme

The proposed scheme comprises of watermark embedding, watermark extraction, tamper detection (ROI and RONI) and the recovery of ROI region (if found tampered) with 100% reversibility. Initially, the host image is divided into ROI and RONI regions. The ROI information is then compressed using LZW compression algorithm, to ensure less memory requirement for embedding. Next, the robust watermark is embedded into the host image using a block wise transform domain approach. Later, the hash keys are generated using SHA-256 algorithm for ROI and segmented RONI regions of robust watermarked image. Subsequently, the fragile watermark is prepared by combining compressed ROI data and hash keys. This fragile watermark is then embedded into the RONI region of the robust watermarked image using LSB replacement approach. During extraction, the robust watermark extraction is performed to verify copyright/ownership. Likewise, the fragile watermark gets extracted and separated into ROI data (i.e. compressed) and hash keys. As similar to embedding process, the hash keys are generated for ROI and RONI parts of the received watermarked image. The extracted and generated hash keys are then compared to detect tampering/forgery. If the ROI

part is found tampered, then it can be recovered using the extracted ROI data (when the RONI part (used for fragile embedding) is not tampered/forged). Similarly, the segmented RONI parts are marked as tampered or not tampered based on the hash keys.

Generally, the watermarking schemes designed for medical imaging focus on the tampering detection and recovery of the ROI region only. It is because the ROI part is used for diagnosis purposes and helps the practitioners/doctors to decide future directions. However, it is important to note that accurate tampering detection and the recovery of ROI are based on the extracted data from the RONI region. If the RONI part (in which the fragile watermark had been inserted during embedding) has been tampered with, then the extracted recovery information cannot be used for the recovery of the ROI region. As it can further result in a faulty diagnosis and may risk the patient's health. Therefore, it is also essential to authenticate the RONI region. Additionally, it would also help in dealing with attacks like fake ownership claims, etc. in the proposed scheme due to the multipurpose nature and dual watermarking approach. The following sub-sections present the proposed scheme in detail.

3.1 Embedding process

The schematic description of the proposed embedding scheme is shown in Fig. 1. At first, select the host image (512 × 512) and divide it into two parts namely ROI and RONI. Convert the pixel values of ROI (100 × 100) into the binary form and organize it in the form of a binary sequence (ROI_{bin}). Compress ROI_{bin}using the LZW algorithm to obtain the compressed binary sequence ($ROI_{compress\ \_\ bin}$). Now, select the robust binary watermark Wat_R(32 × 32 bits) and partitioned the original host image into 8 × 8 size blocks for robust embedding. Select 1024 blocks out of 4096 blocks in a random manner using key (K_1). Now, embed the 1024 robust watermark bits into the selected 1024 blocks sequentially using the following steps. Let us consider that a robust bit is b_r and the 8 × 8 size block is represented as B.

Step 1. Apply Slantlet transform (SLT) on B to generate sub-bands LL, LH, HL and HH.
Step 2. Calculate average intensity $I_1$and I_2 for sub-bands LH and HL respectively.
Step 3. Determine the embedding factor EF_1 and EF_2 using the embedding strength parameter α as per the eq. (1) and (2).

$$EF_1 = \{\alpha - (I_2 - I_1)\}/2 \tag{1}$$

$$EF_2 = \{\alpha - (I_1 - I_2)\}/2 \tag{2}$$

Step 4. Modify LH band using the eq. (3) given as:

$$P_{i,j} = \begin{cases} P_{i,j} - EF1 & when\ b_r = 1\ and\ I_2 - I_1 < \alpha \\ P_{i,j} + EF2 & when\ b_r = 0\ and\ I_1 - I_2 < \alpha \\ P_{i,j} & elsewhere \end{cases} \tag{3}$$

Step 5. Modify HL band using the eq. (4) given as:

$$P_{i,j} = \begin{cases} P_{i,j} + EF1 & when\ b_r = 1\ and\ I_2 - I_1 < \alpha \\ P_{i,j} - EF2 & when\ b_r = 0\ and\ I_1 - I_2 < \alpha \\ P_{i,j} & elsewhere \end{cases} \tag{4}$$

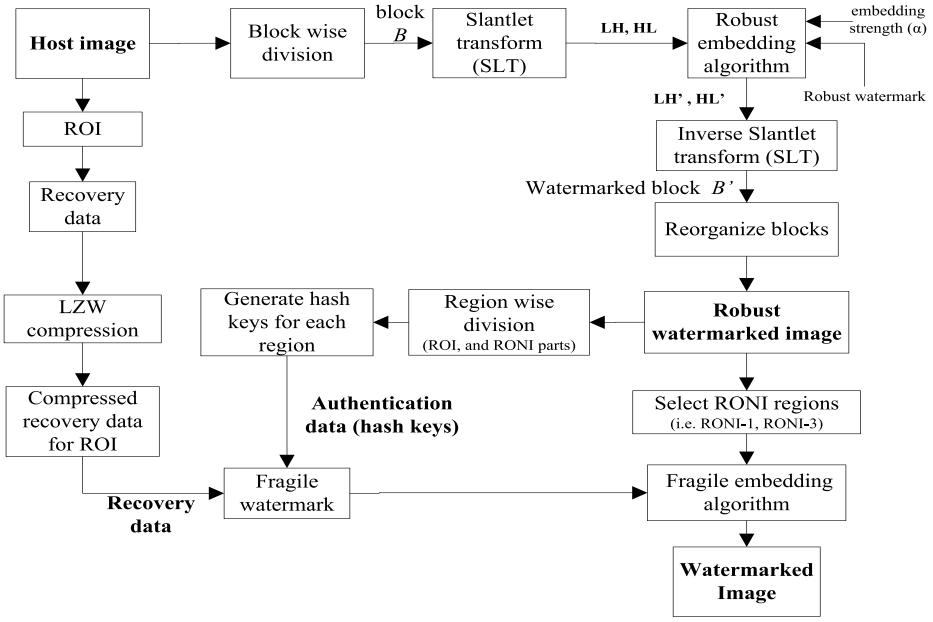


Fig. 1 The proposed watermark embedding process

(Here $P_{i,j}$ denotes the coefficient value at row = i and column = j of block B)

Step 6. Perform inverse Slantlet transform using the modified LH and HL band to get the watermarked block.

At last, recombine the blocks to obtain the robust watermarked image W_{img_r}. The image W_{img_r} will be used as the carrier signal (i.e. image) for fragile watermarking. To prepare the fragile watermark, generate the hash keys (i.e. 256-bit binary sequences) for ROI and RONI parts of W_{img_r}.The illustrative example to generate a 256-bit hash key for a region (e.g. ROI) is shown in Fig. 2. Likewise, the hash keys are obtained for different RONI regions. It is important to note that, the RONI region has been segmented into eight subparts (as shown in Fig. 3) for partial tamper localization. Hence, there is a different hash key for each sub-part of RONI. It would help to understand the tampering area, and confirms the authenticity of the extracted recovery data. Let H_{roi} denotes the hash key for the ROI of the robust watermarked imageW_{img_r}. SimilarlyH_{roni-1}, H_{roni-2}, H_{roni-3}, H_{roni-4}, H_{roni-5}, H_{roni-6}, H_{roni-7} and H_{roni-8}characterize the hash keys for eight non-overlap regions of RONI. Although, one hash key is sufficient to detect tampering in the RONI part but the partitioned RONI helps to detect tampering with partial localization capability. Next, cascade the $ROI_{compress\_bin}$, H_{roi}, H_{roni-1}, H_{roni-2}, H_{roni-3} and H_{roni-4} to produce the complete fragile sequence Wat_F. The following steps are used to embed Wat_F into the robust watermarked image W_{img_r}.

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

Step 2. Convert all the pixel values into binary form.

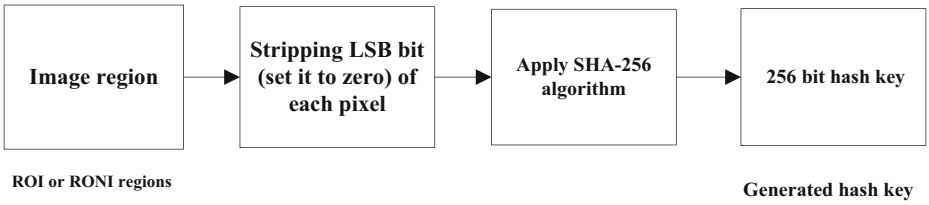


Fig. 2 The process for generating 256-bit hash key for a region (e.g. ROI or other RONI regions)

Step 3. Serially replace the first LSB of all pixels using the bit values of the fragile watermark Wat_F.

Step 4. Convert all pixel values from binary to decimal form. Lastly, the final watermarked image $W_{img\_(r+f)}$ is obtained.

3.2 Extraction process

At the receiver-end, it is always desired that the watermarked image $W_{img_(r+f)}$has not been distorted by intentional/unintentional attacks. However, some common attacks may affect/ modify the image and therefore the effect of these attacks on the performance of the scheme should be analysed carefully.The schematic description of the proposed extraction process is shown in Fig. 4.

1) Robust watermark extraction

The process of extracting the robust watermark information from the received image $W_{img\_(r+f)}$ comprises of the succeeding steps.

Step 1. Divide the image $W_{img\_(r+f)}$ into 8 × 8 size non-overlapping blocks.

Step 2. Select the 1024 blocks (that had been used during embedding) using key (K_1).

Step 3. Choose the first block out of these 1024 blocks and perform SLT transform to get LL, LH, HL, and HH sub-bands.

Step 4. Calculate average intensity values $I_1$and I_2 for LH and HL sub-bands respectively.

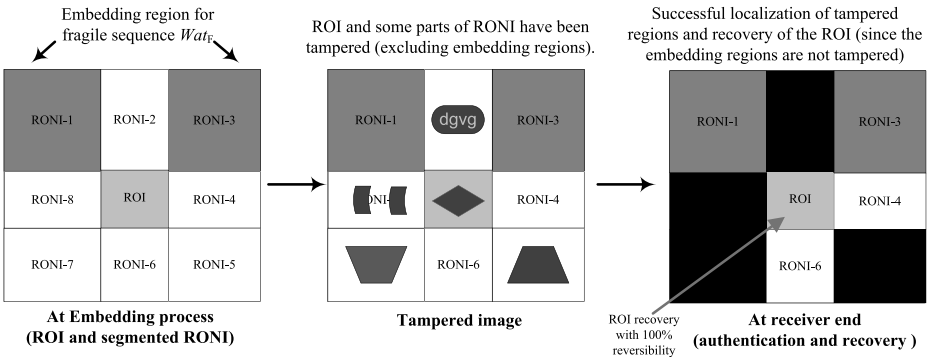


Fig. 3 Benefit of RONI segmentation and partial tamper localization in ROI recovery

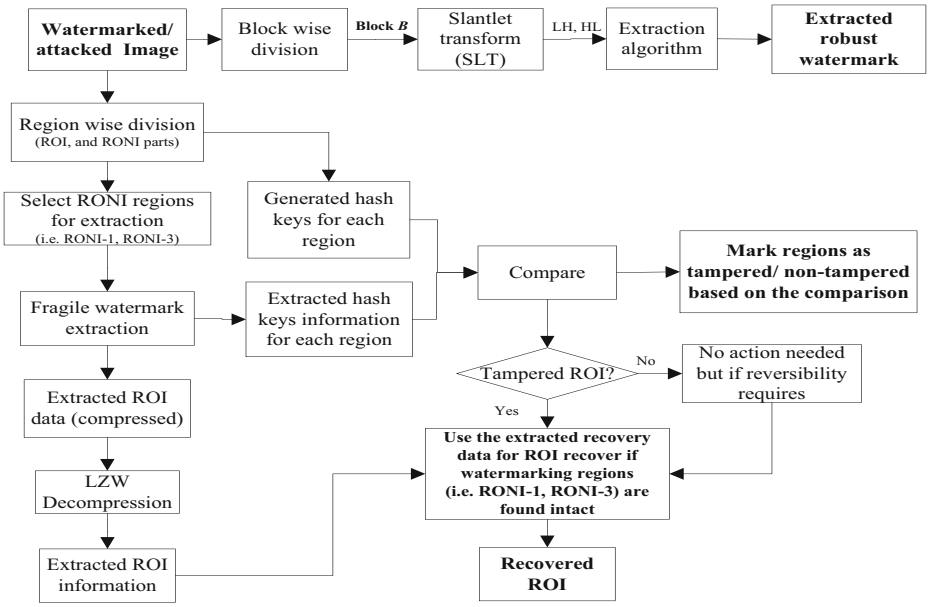


Fig. 4 The proposed watermark extraction process

Step 5. Use the eq. (5) for extracting the bit value b_r.

$$b_r = \begin{cases} 0 & when\ I_1 \geq I_2 \\ 1 & when\ I_1 < I_2 \end{cases} \tag{5}$$

Step 6. Repeat steps 3, 4, and 5 on each selected block to extract the total 1024 bits.
Step 7. Reshape these 1024 bits to 32 × 32 size to obtain the extracted watermark (Wat_{R_ext}).

2) Fragile watermark extraction

The fragile watermark is extracted from the image $W_{img\_(r+f)}$ as follows: Firstly, separate the image into ROI and RONI regions. Afterward, select the n pixels (i.e. used for embedding) and convert them into binary form. Sequentially extract the first LSB bit concerning each pixel and get the extracted fragile sequence Wat_{F_ext}. Now, partition the Wat_{F_ext} sequence to get $ROI_{compress\_bin\_ext}$, H_{roi_ext},H_{roni-1_ext}, H_{roni-2_ext}, H_{roni-3_ext}, H_{roni-4_ext},H_{roni-5_ext}, H_{roni-6_ext}, $H_{roni-7_ext}$and H_{roni-8_ext}. Here, $ROI_{compress\_bin\_ext}$ denotes the extracted ROI recovery information and H_{roi_ext} denotes the 256-bit hash key for the ROI region. H_{roni-1_ext}, H_{roni-2_ext}, H_{roni-3_ext}, H_{roni-4_ext},H_{roni-5_ext}, H_{roni-6_ext}, $H_{roni-7_ext}$and H_{roni-8_ext}represent the extracted hash keys for eight RONI regions.

3.3 Tamper detection and ROI recovery

1) Check for tampering

To detect tampering/alteration in the image $W_{img\_(r+f)}$, get the hash keys for ROI and RONI regions as similar to the embedding process. Let the generated hash keys are H_{roi_new},H_{roni-1_new}, H_{roni-2_new}, H_{roni-3_new}, H_{roni-4_new}, H_{roni-5_new}, H_{roni-6_new}, $H_{roni-7\_}$

$_{new}$and $H_{roni\ -\ 8\ \_\ new}$. Finally, compare the corresponding hash keys to detect tampering. For example, if all analogous bits of $H_{roi\ \_\ ext}$ and $H_{roi\ \_\ new}$ are equal then it confirms that the ROI region has not been tampered with. On the other hand, even if a single bit is not similar to the analogous bit then the complete ROI region can be considered as tampered. Likewise, check the all the eight RONI regions for tampering.

2) ROI recovery

When the ROI region is found tampered, then decompress the binary sequence $ROI_{compress\ \_\ bin\ \_\ ext}$ to get the sequence $ROI_{bin\ \_\ ext}$. Reorganize the $ROI_{bin\ \_\ ext}$ by converting every eight bits into a decimal value in a sequential manner and finally reshape the data as per the size of the ROI region. This way, 100% reversibility in terms of the recovery of the ROI region can be achieved. It should be noted that before recovering ROI, the embedding RONI region (in which the recovery data were stored) should be checked carefully for tampering. The segmentation of the RONI region into eight sub-parts facilitates the tamper localization, which further helps to confirm the precision of the extracted recovery data and hash keys. Since the number of pixels (say N_{pixels}) required for fragile embedding is equal to the length (n) of the fragile sequence Wat_F. Normally, the value of N_{pixels} is relatively small as compared to the complete RONI region of the image. Hence, all segmented RONI regions would not be needed for watermarking. As shown in Fig. 3, RONI-1 and RONI-3 (only when RONI-1 is completely used for embedding) regions have been used for embedding the fragile sequence Wat_F. In that case, tampering in other RONI regions would not affect the extracted fragile sequence $Wat_{F\ \_\ ext}$. Thus, the extracted recovery information still can be used to recover the ROI region with 100% reversibility.

4 Results and discussion

This section presents the experimental analysis of the proposed scheme and its merits over the other existing schemes in the field of medical imaging. From the experimental point of view, 120 medical images from different databases [14] have been used to test the performance of the scheme. However, five medical images are employed to present the experimental and graphical results in this manuscript. In the experiment, the size of the host medical image is 512 × 512, and the robust binary watermark is of size 32 × 32. The size of region of interest (ROI) is 100 × 100, and the remaining part of the image is considered as region of non-interest (RONI). The RONI region is further segmented into eight parts for partial localization of tampering/forgery. The experimental observations have been performed using different watermarking parameters such as PSNR (peak signal to noise ratio), SSIM (structural similarity index), BER (bit error rate), and NC (normalized correlation) [13, 24]. Figure 5 presents the test images and their watermarked versions along with the imperceptibility results in terms of PSNR and SSIM. The robust binary watermark (32 × 32) is also shown in Fig. 4 in succeeding column with robust watermarked images.

As presented in Fig. 5, the watermarked images are highly imperceptible in terms of PSNR, and SSIM. It confirms that the watermark embedding (robust as well as fragile) does not affect the visual quality of the image. For all the test images (120) used in the experiment, the average values of PSNR and SSIM are 40.21 and 0.9984 respectively. On the other side, 25 different attacks (as presented in the next subsection) have been used to check the robustness.

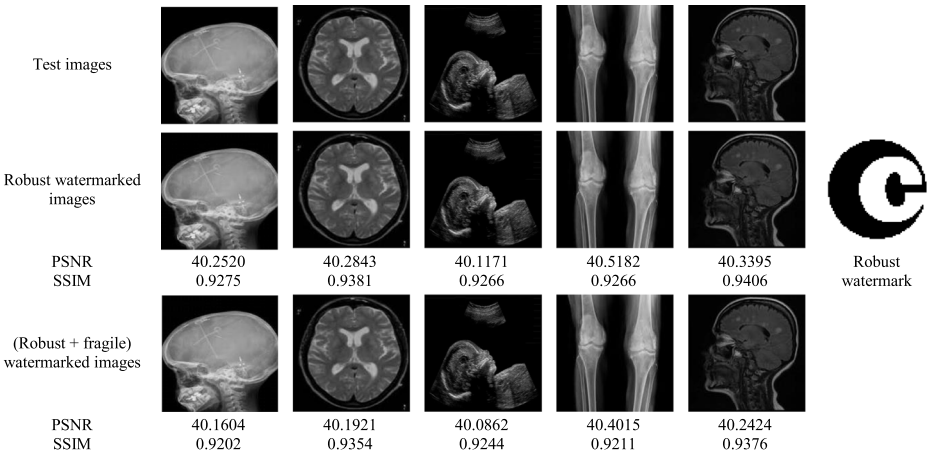


Fig. 5 Host and corresponding watermarked images with imperceptibility results (PSNR, SSIM) and the robust binary watermark

The average BER and NC values are found to be 0.0155 and 0.9603 respectively. This certifies that the scheme has high imperceptibility and robustness for different type of medical images and can surely be helpful in medical image watermarking.

As discussed earlier, the schemes [3, 32] are merged in an improved manner in the proposed work to get better performance with multipurpose nature. Consequently, a comparative analysis given in Table 1 clearly justifies the superiority of the proposed work over [3, 32]. The scheme [32] has a robust nature that can be used only for the robust applications such as source/ownership verification, whereas the scheme [3] has a fragile nature, and can be used for the fragile applications only. On the other hand, the proposed scheme has can be used for both type (robust and fragile) applications effectively with added advantages of region-wise tamper localization.

A relative comparison with the existing medical watermarking schemes in terms of the features and parametric performance has been performed as presented in Table 2. As described in Table 2, existing medical watermarking schemes such as [3, 8, 9] have been proposed to provide tamper detection and restoration features, but they are unable to provide copyright/ ownership protection. Instead, the schemes [28, 39] are unable in providing tampering detection/localization, and restoration. In [1], the multipurpose nature has been provided but

Table 1 Relative comparison with the schemes [3, 32]

S. No.	Characteristics	Sinhal & Ansari [32]	Badshah et al. [3]	Proposed scheme
1	Signal type	Image	Image	Image
2	Scheme type	Robust	Fragile	Robust + Fragile
3	Multipurpose nature	No	No	Yes
4	PSNR (watermarked)	~ 37 dB	~ 51 dB	~ 40 dB
5	Capacity	Low (only robust watermark)	High (Only fragile watermark)	High (Robust + fragile watermark)
6	Robustness	Yes	No	Yes
7	Copyright/ownership verification	Yes	No	Yes
8	Tamper detection ROI	No	Yes	Yes
	RONI	No	No	Yes
9	Region-wise Tamper localization	No	No	Yes
10	Reversibility (for ROI)	No	Yes	Yes

Table 2 Relative comparison with existing medical watermarking schemes

S. No.	Characteristics		Das and Kundu [8]	Eswaraiah and Reddy [9]	Badshah et al. [3]	Parah et al. [28]	Zear et al. [39]	Alshanbari [1]	Proposed scheme
1	Host image type		Medical	Medical	Medical	Medical	Medical	Medical	Medical
2	Scheme type		Fragile	Fragile	Fragile	Robust	Robust	Robust + Fragile	Robust + Fragile
3	Embedding domain		Spatial	Spatial	Spatial	Transform	Transform	Transform + spatial	Transform + spatial
4	Type of extraction		Blind	Blind	Blind	Blind	Non-blind	Non-blind	Blind
5	PSNR (watermarked)		~ 44 dB	~ 50 dB	~ 51 dB	~ 41 dB	~ 33 dB	~ 48 dB	~ 40 dB
6	Capacity		High	High	High	Low	Very high	High	High
7	Robustness		–	–	–	High	High	Poor	High
8	Copyright/ownership verification		No	No	No	Yes	Yes	Yes	Yes
9	Tamper detection	ROI	Yes	Yes	Yes	No	No	Yes	Yes
		RONI	No	No	No	No	No	No	Yes
10	Region-wise Tamper localization		No	No	No	No	No	No	Yes
11	Reversibility (for ROI)		No	Yes (only in case of no attack)	Yes	No	No	Yes	Yes

– denotes that the mentioned characteristic is not provided

it has poor results in terms of robustness. Moreover, the scheme [1] has a non-blind nature that bounds the extraction procedure as it requires additional information (e.g. original host image) for the extraction. In addition, most of the watermarking schemes (as discussed in the manuscript) used RONI as the embedding region but none of them concerned about the authentication of embedding region (i.e. RONI). Since the intentional/unintentional tampering or modification can affect any part of the image. Therefore, the authenticity of the embedding region should be examined carefully.

The proposed work provides an efficient multipurpose scheme with significant parametric performance and additional features. It resolves some of the existing issues in the field of medical image watermarking. The authentication of ROI as well as RONI has been provided in the proposed work. Additionally, the RONI region has been segmented into small subparts to ensure effective region-wise tamper localization. It also increases the possibility of ROI recovery even in case of severe tampering in any part of the image (except the embedding region). Further, the proposed scheme is able to alert about authenticity of the extracted data in case of the tampered embedding region. It can surely help the practitioners to take subsequent treatment related decisions. The relative analysis shows that the proposed scheme has more features with significant parametric values as compared to existing schemes, while having a blind extraction mechanism.

4.1 Robust watermarking results

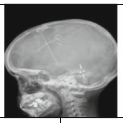
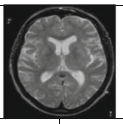
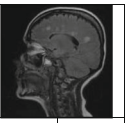
A variety of signal and image processing attacks are applied on the watermarked images before the extraction process to testify the robustness of the scheme. The embedding strength parameter α is set to 15 after thorough experimentation. It gives significant parametric features for imperceptibility and robustness simultaneously. Even though the PSNR >30 dB is considered to be good for images in the literature [3], it has been maintained at ~40 dB in the manuscript for medical images with a little compromise in robustness. The extracted watermarks are of high quality for most of the applied attacks. The obtained parametric results in terms of BER and NC are highly significant. The robustness analysis presented in Table 3 shows that the scheme can sustain different signal processing attacks effectively. Therefore, the proposed blind watermarking scheme can be used for copyright/ ownership verification.

The visual results of the extracted watermark for a test image are also presented in Table 4, which confirms that the visual quality of the extracted watermarks against attacks is good enough. The robustness of the proposed scheme has also been compared with the existing robust watermarking schemes (with same payload = 1024 bits) as shown in Table 5. Some general test images like Lena, Mandrill and Pepper with size 512 × 512 are selected for comparison purpose. Here, it is observed that even after having multipurpose nature, the proposed scheme has superior robustness results for different signal processing attacks. Moreover, the visual quality is also found to be significant with average PSNR value is 39.5 dB and average SSIM value is 0.97. Thus, the proposed scheme gives similar results for different types of images and can be used even for general digital images.

4.2 Fragile watermarking results

Different tampering attacks are applied on the ROI and different parts of the RONI region to investigate the fragile nature of the proposed scheme. Further, the tamper detection and partial localization (region-wise) results are evaluated along with the recovery of the ROI region. In general, the medical image watermarking schemes embed the ROI recovery information into

Table 3 Robustness analysis in terms of BER and NC for test images against different attacks

S. No	Attacks ↓ / Test images →										
		BER	NC	BER	NC	BER	NC	BER	NC	BER	NC
1	No attack	0	1	0	1	0	1	0	1	0	1
2	Speckle (0.005)	0.0010	0.9980	0	1	0	1	0	1	0	1
3	Speckle (0.01)	0	1	0	1	0	1	0	1	0	1
4	Gaussian (0.005)	0.0547	0.8907	0.0420	0.9160	0.0879	0.8244	0.0645	0.8712	0.0352	0.9297
5	Gaussian (0.01)	0.0898	0.8214	0.0879	0.8246	0.1680	0.6643	0.1211	0.7579	0.0947	0.8109
6	Salt & pepper (0.005)	0.0146	0.9707	0.0205	0.959	0.0352	0.9298	0.0195	0.961	0.0146	0.9707
7	Salt & pepper (0.01)	0.0313	0.9375	0.0361	0.9278	0.0508	0.8985	0.0361	0.9282	0.0381	0.9241
8	Average filter 3x3	0.0029	0.9942	0	1	0.0098	0.9805	0.0166	0.9672	0.0020	0.9961
9	Median filter 3x3	0	1	0	1	0.0029	0.9942	0	1	0	1
10	Gaussian filter3x3	0	1	0	1	0	1	0	1	0	1
11	Wiener filter 3x3	0	1	0	1	0	1	0	1	0	1
12	JPEG 50	0.0107	0.9787	0.0049	0.9902	0.0186	0.9635	0.0098	0.9806	0.0059	0.9883
13	JPEG 70	0	1	0	1	0	1	0	1	0	1
14	JPEG 80	0	1	0	1	0	1	0	1	0	1
15	Sharpening (0.2)	0	1	0	1	0	1	0	1	0	1
16	Sharpening (0.8)	0	1	0	1	0	1	0	1	0	1
17	Gamma correction (0.6)	0	1	0	1	0	1	0	1	0	1
18	Gamma correction (0.8)	0	1	0	1	0	1	0	1	0	1
19	Resize (0.5, 2)	0.1465	0.7079	0.1445	0.7146	0.1768	0.6465	0.1357	0.7285	0.1689	0.6621
20	Resize (2, 0.5)	0	1	0	1	0	1	0	1	0	1
21	Crop 5% @ centre	0.0010	0.9980	0.0010	0.9980	0.0010	0.9980	0.0010	0.9980	0.0010	0.9980
22	Adjust contrast @ 20%	0.0010	0.9980	0	1	0	1	0	1	0	1
23	Motion blur (θ=7,Len=10)	0.0068	0.9863	0.0010	0.9980	0.0371	0.9259	0.0107	0.9787	0.0029	0.9941
24	Copy-move (60x60 pixel)	0.0039	0.9922	0.0039	0.9922	0.0049	0.9903	0.0068	0.9863	0.0039	0.9922
25	Copy-paste (60x60 pixel)	0.0049	0.9903	0.0049	0.9902	0.0039	0.9922	0.0049	0.9903	0.0059	0.9883

the RONI region, but investigate the tamper detection, and recovery of the ROI only. With no doubt, it is true that the ROI part is important for further diagnosis by the medical practitioners; but the authentication of RONI is also having importance for verifying the intactness of the extracted data. As the accurate recovery of ROI is based on accuracy of the extracted data, the authentication of RONI region becomes essential. Moreover, the ROI part is a small region as compared to the whole image. Therefore, the complete RONI region is not required for embedding the fragile watermark (recovery data + hash keys). It means that if some part of

Table 4 Extracted watermark information against different attacks

Test images	Extracted watermark for different signal processing attacks							
 Host image	 No attack	 Speckle (0.005)	 Speckle (0.01)	 Gaussian (0.005)	 Gaussian (0.01)	 Salt & pepper (0.005)	 Salt & pepper (0.01)	 Average filter 3x3
 Original watermark	 Median filter 3x3	 Gaussian filter3x3	 Wiener filter 3x3	 JPEG 50	 JPEG 70	 Sharpening (0.2)	 Sharpening (0.8)	 Gamma correction (0.6)
	 Gamma correction (0.8)	 Resize (0.5, 2)	 Resize (2, 0.5)	 Crop 5% @ centre	 Adjust contrast 20%	 Motion blur (θ=7,Len=10)	 Copy-move (60x60 pixel)	 Copy-paste (60x60 pixel)

Table 5 Robustness comparison in terms of BER with existing robust watermarking schemes

Attacks	Lena				Mandrill				Pepper			
	Mehta et al. [17]	Islam and laskar [19]	Islam et al. [20]	Proposed work	Mehta et al. [17]	Islam and laskar [19]	Islam et al. [20]	Proposed work	Mehta et al. [17]	Islam and laskar [19]	Islam et al. [20]	Proposed work
SPN (0.005)	0.06	0.06	0.04	**0.01**	0.05	0.05	0.02	**0.00**	0.06	0.05	0.03	**0.00**
SPN (0.01)	0.12	0.13	0.05	**0.02**	0.10	0.08	0.05	**0.01**	0.12	0.12	0.07	**0.01**
SPN (0.02)	0.16	0.16	0.13	**0.04**	0.18	0.18	0.11	**0.03**	0.20	0.19	0.15	**0.03**
GN (0.001)	0.06	0.05	0.02	**0.00**	0.07	0.06	0.01	**0.00**	0.06	0.47	0.01	**0.00**
GN (0.005)	0.25	0.21	0.11	**0.01**	0.25	0.23	0.11	**0.01**	0.26	0.19	0.14	**0.01**
GN (0.01)	0.36	0.35	0.22	**0.05**	0.33	0.30	0.19	**0.04**	0.36	0.37	0.21	**0.06**
JPEG 50	0.00	0.00	0.01	**0.00**	0.03	0.01	0.01	**0.00**	0.00	0.00	0.00	**0.00**
JPEG 70	0.00	0.00	0.00	**0.00**	0.01	0.00	0.00	**0.00**	0.00	0.00	0.00	**0.00**

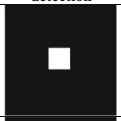
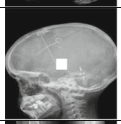
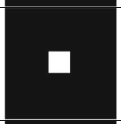
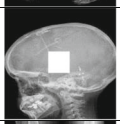
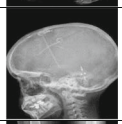
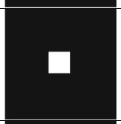
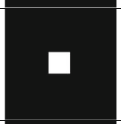
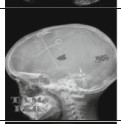
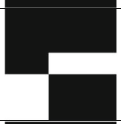
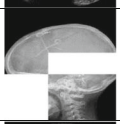
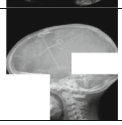
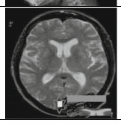
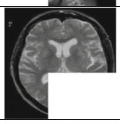
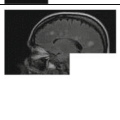
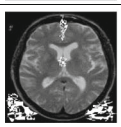
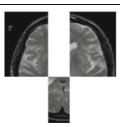
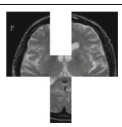
RONI got tampered even then there is a possibility of efficient extraction of embedded data. It can be possible by dividing RONI region into parts and authenticate each part individually. This way, it would be possible to localize tampered region more specifically. The proposed scheme offers authentication of ROI as well as RONI part of the image. The scheme divides RONI part into eight sub-regions for better localization of tampered area. The individual 256-bit hash key is assigned to each sub-region for authentication. Let us consider that the complete watermarked image is of size MxM, in which the ROI (100×100) part is ($m_1 : m_2,\ n_1 : n_2$). The remaining part of the image is considered as RONI region. In the proposed scheme, the eight sub-division of RONI are RONI-1, RONI-2, RONI-3, RONI-4, RONI-5, RONI-6, RONI-7 and RONI-8. To understand the division of RONI part mathematically, the pixel positions of the segmented RONI regions are presented as in the eq. (6).

$$pixel\ cordinates = \begin{cases} (1:(m1-1), 1:(n1-1)) & for\ RONI-1 \\ (1:(m1-1), n1:n2) & for\ RONI-2 \\ (1:(m1-1), (n2+1):512) & for\ RONI-3 \\ (m1:m2, (n2+1):512) & for\ RONI-4 \\ ((m2+1):512, (n2+1):512) & for\ RONI-5 \\ ((m2+1):512, n1:n2) & for\ RONI-6 \\ ((m2+1):512, 1:(n1-1)) & for\ RONI-7 \\ (m1:m2, 1:(n1-1)) & for\ RONI-8 \end{cases} \tag{6}$$

Although the subdivision of RONI region is arbitrary in nature and can be customized as per the situation, yet it can be decided for optimum use of RONI part for watermarking. Thus, even if a large part of RONI (not used for fragile embedding) would be tampered, the ROI can be recovered with 100% reversibility. For the experimental evaluation, the ROI region has pixel co-ordinates ($m_1 : m_2,\ n_1 : n_2$) = (201:300, 201:300). The RONI-1 and RONI-3 have been used for fragile embedding. Therefore, if other RONI regions would be tampered, even then the lossless recovery of the tampered ROI is possible.

As shown in Table 6, different tampering attacks are applied on the test images to verify the performance of the proposed scheme. It is found that the scheme can authenticate ROI and RONI (all four regions) efficiently. The scheme can also recover ROI with 100% reversibility. The only requirement for perfect region-wise tamper detection/ localization and ROI recovery

Table 6 Tamper detection, region-wise localization and ROI recovery for different tampering attacks

S. No.	Attack type	Tampered image	Tamper detection	Image authentication	ROI recovery	Remarks
1	Content removal (small part in ROI)					1) Successful detection and recovery of Tampered ROI with 100% reversibility.
2	Content removal (Large part in ROI)					1)Successful detection and recovery of Tampered ROI with 100% reversibility
3	Copy-paste-A (a portion is copied from the same image and pasted into ROI)					1)Successful detection and recovery of Tampered ROI with 100% reversibility
4	Copy-paste-B (a portion is copied from the other image and pasted into ROI)					1) Successful detection and recovery of Tampered ROI with 100% reversibility
5	Random editing in ROI and RONI (i.e. RONI-4 and RONI-7)					1) Perfect region-wise tamper detection/localization 2) 100% ROI recovery (when ROI as well as a big part of RONI were tampered)
6	Tampering only in RONI (i.e. RONI-5 and RONI-6)				**Not required**	1) Perfect region-wise tamper detection 2) Although ROI recovery is not required, yet it can be done for 100% reversibility.
7	Tampering only in RONI (i.e. RONI-4 and RONI-5, RONI-6 and RONI-7)				**Not required**	1) Perfect region-wise tamper detection/localization 2) Although ROI recovery is not required, yet it can be done for 100% reversibility
8	Tampering in ROI and RONI (i.e. RONI-2, RONI-5 and RONI-7)					1) Perfect region-wise tamper detection 2) Recovery of Tampered ROI with 100% reversibility.

is that the embedding region (i.e. RONI-1 and RONI-3 in the manuscript) should not be tampered. Since the tampering in the embedding region can harm the data and then it cannot be used for recovery purpose. The tamper detection of the RONI with region-wise tamper localization help to authenticate the image more specifically. Additionally, it is able to provide ROI recovery even when RONI (except the embedding region) is tampered. Therefore, the tampering/forgery in the ROI and RONI regions (excluding the region used for embedding) does not interrupt the tamper detection/localization and the ROI recovery with 100% reversibility. Instead, the tampering in the RONI region (used for embedding) alerts that the extracted data has been modified and should not be used for tamper detection, localization, and the self-recovery of the ROI. Thus, the scheme can ensure the doctors/practitioners about the authenticity of the medical image in a better way. The fragile nature of the proposed watermarking framework is investigated as compared to some of the existing fragile schemes as presented in Table 7. It is observed that the fragile mechanism of the proposed framework has significant performance over already existing fragile schemes.

Table 7 The comparison of fragile nature of the proposed scheme with existing fragile watermarking schemes

Fragile Schemes	Characteristics					
	Purpose	Payload	Imperceptibility (PSNR, SSIM)	Blind nature	Tamper localization	ROI recovery
Guo and Zhuang [12]	Data hiding, Image authentication, Restoration	High	~ 57 dB	No	No	Yes
Das and Kundu [8]	Data hiding, Image authentication	High	~ 44 dB	Yes	Yes	No
Eswaraiah and Reddy [9]	Data hiding, Image authentication, Restoration	High	~ 50 dB	Yes	Yes (only for ROI)	Yes (only in case of no attack)
Proposed scheme (only fragile nature)	Data hiding, Image authentication, Restoration	High	~ 57 dB	Yes	Yes	Yes

5 Conclusion

This study proposed a multipurpose and blind image watermarking scheme for medical images. The multiple (robust and fragile) watermarking mechanism provide ability of copyright/ownership protection, tamper detection, region-wise tamper localization and the self-recovery of the ROI part. The robust mechanism is based on block-wise division and slantlet transform, whereas the fragile watermarking used an LSB replacement approach to embed the recovery information of ROI and the authentication keys (i.e. hash keys). The LZW lossless compression technique is used to compress the recovery data before embedding. To authenticate the ROI and different RONI regions, 256-bit hash keys are generated using SHA-256 algorithm. Both the regions (ROI and RONI) get checked for tampering to ensure the integrity of the image. It is important in terms of verifying the extracted information against any intentional/accidental modification. The RONI region is further divided into eight sub-regions to offer region-wise localization capability. The scheme is tested against different signal processing and tampering attacks. Investigational results confirm that the scheme has high robustness, significant imperceptibility, effective tamper detection/localization, and perfect ROI recovery (100% reversibility) capability. The comparison with the other medical watermarking schemes shows the omnipotence of the proposed scheme in terms of parametric results and multipurpose nature. Future work comprises of the improvement in the embedding strategy for better parametric results. The division of the RONI region into sub-regions will also be optimized for better region-wise tamper localization.

Funding This research work was supported by Jagadish Chandra Bose Research Organisation (JCBRO).

Declarations

Conflicts of interest/competing interests There is no conflict of interest.

References

1. Alshanbari HS (2020) Medical image watermarking for ownership & tamper detection. Multimed Tools Appl 80(11):16549–16564
2. Avudaiappan T, Balasubramanian R, Pandiyan SS, Saravanan M, Lakshmanaprabu SK, Shankar K (2018) Medical image security using dual encryption with oppositional based optimization algorithm. J Med Syst 42(11):208
3. Badshah G, Liew SC, Zain JM, Ali M (2016) Watermark compression in medical image watermarking using Lempel-Ziv-Welch (LZW) lossless compression technique. J Digit Imaging 29(2):216–225
4. Casado-Vara R, Corchado J (2019) Distributed e-health wide-world accounting ledger via blockchain. J Intell Fuzzy Syst 36(3):2381–2386
5. Chao HM, Hsu CM, Miaou SG (2002) A data-hiding technique with authentication, integration, and confidentiality for electronic patient records. IEEE Trans Inf Technol Biomed 6(1):46–53
6. Cheung WN (2000) Digital image watermarking in spatial and transform domains. In: 2000 TENCON proceedings. Intelligent systems and Technologies for the new Millennium (cat. No. 00CH37119) (Vol. 3, pp. 374-378). IEEE.
7. Coatrieux G, Maître H, Sankur B, Rolland Y, Collorec R (2000) Relevance of watermarking in medical imaging. In: Proceedings 2000 IEEE EMBS international conference on information technology applications in biomedicine. ITAB-ITIS 2000. Joint meeting third IEEE EMBS international conference on information Technol. IEEE. pp. 250-255
8. Das S, Kundu MK (2013) Effective management of medical information through ROI-lossless fragile image watermarking technique. Comput Methods Prog Biomed 111(3):662–675
9. Eswaraiah R, Sreenivasa Reddy E (2014) Medical image watermarking technique for accurate tamper detection in ROI and exact recovery of ROI. Int J Telemed Appl 2014:1–10
10. Giakoumaki A, Pavlopoulos S, Koutsouris D (2006) Secure and efficient health data management through multiple watermarking on medical images. Med Biol Eng Comput 44(8):619–631
11. Gong LH, Tian C, Zou WP, Zhou NR (2021) Robust and imperceptible watermarking scheme based on canny edge detection and SVD in the contourlet domain. Multimed Tools Appl 80(1):439–461
12. Guo X, Zhuang TG (2009) A region-based lossless watermarking scheme for enhancing security of medical data. J Digit Imaging 22(1):53–64
13. Hore A, Ziou D (2010) Image quality metrics: PSNR vs. SSIM. In 2010 20th international conference on pattern recognition. IEEE. pp. 2366-2369
14. "Image databases," Accessed Sep. 2020. [Online]. Available: http://www.imageprocessingplace.com/root_files_V3/
15. Islam M, Laskar RH (2018) Geometric distortion correction based robust watermarking scheme in LWT-SVD domain with digital watermark extraction using SVM. Multimed Tools Appl 77(11):14407–14434
16. Islam M, Roy A, Laskar RH (2020) SVM-based robust image watermarking technique in LWT domain using different sub-bands. Neural Comput & Applic 32(5):1379–1403
17. Jeong C, Kim Y (2014) Implementation of efficient SHA-256 hash algorithm for secure vehicle communication using FPGA. In: 2014 international SoC design conference (ISOCC). IEEE. pp. 224-225
18. Kammoun M, Elleuchi M, Abid M, BenSaleh MS (2020) FPGA-based implementation of the SHA-256 hash algorithm. In 2020 IEEE international conference on Design & Test of Integrated Micro & Nano-Systems (DTS). IEEE. pp. 1-6
19. Lai CC, Tsai CC (2010) Digital image watermarking using discrete wavelet transform and singular value decomposition. IEEE Trans Instrum Meas 59(11):3060–3063
20. Liao X, Li K, Yin J (2017) Separable data hiding in encrypted image based on compressive sensing and discrete fourier transform. Multimed Tools Appl 76(20):20739–20753
21. Liao X, Guo S, Yin J, Wang H, Li X, Sangaiah AK (2018) New cubic reference table based image steganography. Multimed Tools Appl 77(8):10033–10050
22. Liao X, Yin J, Chen M, Qin Z (2020) Adaptive payload distribution in multiple images steganography based on image texture features. IEEE Trans Dependable Secure Comput:1. https://doi.org/10.1109/TDSC.2020.3004708
23. Luo AW, Gong LH, Zhou NR, Zou WP (2020) Adaptive and blind watermarking scheme based on optimal SVD blocks selection. Multimed Tools Appl 79(1):243–261
24. Mehta R, Rajpal N, Vishwakarma VP (2016) LWT-QR decomposition based robust and efficient image watermarking scheme using Lagrangian SVR. Multimed Tools Appl 75(7):4129–4150
25. Mousavi SM, Naghsh A, Abu-Bakar SAR (2014) Watermarking techniques used in medical images: a survey. J Digit Imaging 27(6):714–729
26. Navas KA, Sasikumar M (2007) Survey of medical image watermarking algorithms. In: Proc. Internation Conf. Sciences of electronics, Technologies of Information and Telecommunications (pp. 25-29).

27. Panchal UH, Srivastava R (2015) A comprehensive survey on digital image watermarking techniques. In: 2015 fifth international conference on communication systems and network technologies. IEEE. pp. 591-595
28. Parah SA, Sheikh JA, Ahad F, Loan NA, Bhat GM (2017) Information hiding in medical images: a robust medical image watermarking system for E-healthcare. Multimed Tools Appl 76(8):10599–10633
29. Rachmawati D, Tarigan JT, Ginting ABC (2018, March) A comparative study of message digest 5 (MD5) and SHA256 algorithm. J Phys Conf Ser 978(1):012116 IOP publishing
30. Ray PP, Dash D, De D (2019) Edge computing for internet of things: a survey, e-healthcare case study and future direction. J Netw Comput Appl 140:1–22
31. Selesnick IW (1999) The slantlet transform. IEEE Trans Signal Process 47(5):1304–1313
32. Sinhal R, Ansari IA (2020) A source and ownership identification framework for Mobile-based messenger applications. In: Pant M, Sharma T, Verma O, Singla R, Sikander A (eds) Soft computing: theories and applications. Advances in Intelligent Systems and Computing, vol 1053. Springer, Singapore. https://doi.org/10.1007/978-981-15-0751-9_89
33. Sinhal R, Ansari IA, Jain DK (2020) Real-time watermark reconstruction for the identification of source information based on deep neural network. J Real-Time Image Proc 17(6):2077–2095
34. Swaraja K, Meenakshi K, Kora P (2020) An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine. Biomed Signal Process Control 55:101665
35. Tang CW, Hang HM (2003) A feature-based robust digital image watermarking scheme. IEEE Trans Signal Process 51(4):950–959
36. Thabit R, Khoo BE (2014) Robust reversible watermarking scheme using Slantlet transform matrix. J Syst Softw 88:74–86
37. Welch TA (1984) A technique for high-performance data compression. Computer 17(06):8–19
38. Zain J, Clarke M (2005) Security in telemedicine: issues in watermarking medical images. Sciences of Electronic, Technologies of Information and Telecommunications, Tunisia.
39. Zear A, Singh AK, Kumar P (2018) A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. Multimed Tools Appl 77(4):4863–4882
40. Zhang X, Wang S (2008) Fragile watermarking with error-free restoration capability. IEEE Trans Multimedia 10(8):1490–1499
41. Zhou NR, Hou WMX, Wen RH, Zou WP (2018) Imperceptible digital watermarking scheme in multiple transform domains. Multimed Tools Appl 77(23):30251–30267
42. Zhou NR, Luo AW, Zou WP (2019) Secure and robust watermark scheme based on multiple transforms and particle swarm optimization algorithm. Multimed Tools Appl 78(2):2507–2523

Affiliations

Rishi Sinhal[1] · Sachin Sharma[2] · Irshad Ahmad Ansari[1] · Varun Bajaj[1]

Rishi Sinhal
rishi.sinhal.jec@gmail.com

Sachin Sharma
sheorajsachin@gmail.com; sachinsharma@jcbrolabs.org

Varun Bajaj
varunb@iiitdmj.ac.in

[1] Electronics and Communication Engineering, PDPM Indian Institute of Information Technology Design and Manufacturing, Jabalpur, MP 482005, India

[2] Research Division, Jagadish Chandra Bose Research Organisation, Gautam Budh Nagar, Uttar Pradesh 203207, India