Multimed Tools Appl (2017) 76:3617–3647
DOI 10.1007/s11042-016-3913-1

Region-based hybrid medical image watermarking for secure telemedicine applications

Priyanka[1] · **Sushila Maheshkar**[1]

Received: 25 April 2016 / Revised: 26 July 2016 / Accepted: 26 August 2016 /
Published online: 14 September 2016

Abstract In this paper we propose a novel region based hybrid medical image watermarking (MIW) scheme to ensure authenticity, integrity and confidentiality of medical images. In this scheme a digital medical image is partitioned into region of interest (ROI) and the region of non interest (RONI). To detect and localize ROI tampering with high accuracy pixel wise positional and relational bits are calculated. Positional bit is calculated with respect to MSBs, row and column of the pixel. Relational bit shows the relation between MSBs. Two original LSBs of each ROI pixel are replace by their corresponding positional and relational bits. Original LSBs of ROI pixels are concatenated and embedded in RONI for ROI recovery in the case of tampering. Multiple watermarks i.e. electronic patient record (EPR), hospitals logo and LSBs of ROI are embedded simultaneously as a robust watermark in RONI using IWT-SVD hybrid transform. The proposed scheme is blind and free from false positive detection. Various experiments have been carried out on different medical imaging modalities to evaluate the performance of the proposed scheme in terms of imperceptibility, robustness, tamper detection, localization, recovery and computation time. ROI tampering is detected and recovered with high accuracy. Thus, the proposed scheme is effective in telemedicine applications.

Keywords Telemdicine · Medical image · Image watermarking · Data hiding · Integer wavelet transform (IWT) · Singular value decomposition (SVD) · Electronic patient record (EPR)

✉ Sushila Maheshkar
sushila_maheshkar@yahoo.com

Priyanka
priyankasingh401@gmail.com

[1] Department of Computer Science and Engineering, Indian School of Mines, Dhanbad Jharkhand, India

1 Introduction

Developments in digital and communication technologies has opened up new opportunities in the field of telemedicine where digital medical images and EPR are transmitted over networks for clinical interpretation and diagnosis [11]. However, transmission over public network is prone to infringement of security, confidentiality, copyright, and integrity. We cannot afford any loss or tampering of medical data as it can lead to mis-diagnosis. Thus security, confidentiality, integrity and authenticity are of prime concern during transmission of medical images through public network and must be simultaneously satisfied [4]. Confidentiality of the transmitted medical images is ensured so that only authorized users can access it. Integrity validates whether the digital medical image is intact or tampered. Authenticity verifies whether the medical image is from the correct source and belongs to the claimed patient. In the present scenario the two major methodologies i.e. cryptography and medical image watermarking are used popularly to meet these requirements [1]. Cryptography-based approach has a major limitation that if the medical image is deciphered, or the digital signature is deleted or lost, then it is difficult to verify integrity and authenticity of the image. Therefore, MIW has come up as a promising solution in this scenario [21]. Digital watermarks such as EPR, signature, hospitals logo or trademark or physician ID can be embedded into the medical image without degrading the visual quality of the medical image to provide confidentiality and authenticity [2]. A fragile or cryptographic hash watermark can be embedded to verify the integrity of medical images. Other than ensuring security, confidentiality and integrity MIW also provides other benefits like avoiding detachment, non-repudiation, controlling access, privacy, captioning, indexing, memory and bandwidth saving [26].

Different medical image modalities such as X-ray, ultrasound, MRI, CT-scan, mammogram, etc. are being used for medical imaging [22]. In medical images, information is non-uniformly distributed across the image. Taking advantage of this fact, region based MIW schemes divide medical image into region of interest (ROI) and region of non-interest (RONI) [41]. ROI contains more informative part of the medical image which is used for the diagnosis. RONI has no significant role in diagnosis. ROI and RONI regions have different characteristics and requirements. Therefore, different types of watermarks are embedded to meet the watermarking goal. Watermarking process should keep the ROI intact as any distortions may cause wrong diagnosis. RONI can be used to embed robust watermarks. Usually ROI/RONI selection is done manually by doctors/radiologists.

In general digital image watermarking is defined as process of embedding watermark into the host/cover image [8]. Watermark embedding is done either in spatial/pixel domain or transform domain [5]. In spatial domain watermarking techniques, the watermark is interleaved by directly modifying the intensity/pixel values of the cover image resulting in low computational complexity. LSB embedding, spread spectrum are some of the popularly used spatial techniques. Spatial techniques are fragile. But this fragility can be advantageous in finding out the distorted area and reproduction of original host image from the distorted one [3]. In transform domain schemes, watermark is inserted by modifying transform coefficients of the cover/host image. DFT, DCT, DWT, IWT, SVD are commonly used transforms. Transform domain techniques are comparatively more robust [21]. Each transform has different characteristics and has different representation of the image. One transform may be robust to one set of attacks and the other transform to the other set of attacks. In the past few decades various spatial domain, transform domain and hybrid MIW scheme has been reported in literature [23, 26]. Related MIW schemes are discussed in detail in Section 2.

Organization of the paper is as follows: Related work is discussed in Section 2. The proposed MIW scheme is explained in detail in Section 3. Section 4 provides experimental results and discussions. Finally, Section 5 concludes the paper.

2 Related work

During the last few years various MIW schemes have been proposed for different objectives. These MIW schemes can be classified as irreversible, reversible and region-based schemes [1]. Irreversible watermarking schemes introduce distortions to the original images by irretrievable watermarking operations such as truncation, quantization or bit replacement. On the other hand, reversible MIW schemes are capable of restoring original pixel values in the watermarked images. But, most of them lack tamper localization functionality and cannot verify integrity of medical images. Region based schemes have tamper localization features which offers integrity for medical images. Region-based watermarking schemes divide the digital medical image into ROI and RONI [24]. ROI and RONI have different characteristics; therefore, we can embed different types of watermarks to accomplish different requirements. Some of the related region based MIW schemes are discussed below.

Naseem et al. [27] proposed a fragile watermarking method using chaotic key and residue number system. The original ROI pixel values are replaced by ROI residue. Hash value is embedded in the RONI at the locations selected by using chaotic key. The LSBs of these pixel values are set to zero. In this scheme ROI is reversible whereas RONI is irreversible. Hajjaji et al. [16] proposed a spatial MIW scheme where EPR and digital signature of hospital data generated by using SHA1 are concatenated. Then it is interleaved in the edge pixels using LSB technique. They used turbo algorithm to check error during transmission. Pandey et al. [28] proposed a multiple MIW scheme for tele-ophthalmology applications using fusion of DWT and SVD. Hash value of the iris portion of the digital eye image is generated using SHA-512. They embedded four watermarks i.e. index, reference watermark, caption, and signature simultaneously. Text and image watermarks are inserted in the RONI. A major drawback of hash code watermark is that it is more time consuming and a slight change in hash code leads to false tamper localization at the receivers side. Solanki and Malik [32], proposed DWT based watermarking scheme. Using RSA encryption algorithm the watermark is encrypted and then embedded in the ROI. However, in this scheme preprocessing is required before actual embedding. Pre-processing adds overhead time. Such cryptographic watermarks are computation-intensive and therefore cannot be used in real-time environments. Amit et al. [33] suggested a multiple watermarking scheme based on DWT-DCT-SVD transform. They have applied simplified encryption technique to increase the security of the text watermark and at the same time save execution time.

Another region based MIW scheme is proposed by Thabit and Khoo [40] for tamper detection, localization, and its recovery. In this scheme ROI feature is extracted using IWT which is further embedded in RONI. This scheme uses Slantlet transform (SLT) for embedding data in ROI and RONI. Authors claim to recover tampered ROI with good visual quality. Memon et al. [25] proposed hybrid watermarking scheme where the medical image is partitioned into ROI and RONI by using vector quantization technique. A fragile watermark is embedded in ROI LSBs. Location map is generated by distributing RONI into blocks of size N $\times$ N. A watermark is embedded in the RONI coefficients. High time complexity required for calculations to generate the location map is bottleneck of this scheme. Singh et al. [34] proposed a DWT-DCT-SVD based scheme. In the embedding process, the host image and watermark image is transformed by DCT-SVD transform. This scheme provides higher imperceptibility and robustness. Another DWT, DCT, and SVD based multiple watermarking scheme is presented by Singh [35]. In this scheme for identity authentication, multiple watermarks are embedded into the same medical image or multimedia data simultaneously. For enhanced security of EPR data is encrypted before embedding into the cover image. Singh et al. [36] proposed secure multiple watermarking scheme using spread-spectrum for medical images. Watermark is embedded using selective DWT coefficients by thresholding the coefficient values of column. Error correcting code (ECC) is applied to the text watermark and binary image of doctor's signature or telemedicine centre name to enhance security. Singh et al. [37] suggested a secure multiple watermarking scheme based on DWT and SVD where the image along with the encrypted and encoded text acts as a watermarks. Guo and Zhuang [14] suggested another MIW scheme based on modified DE for authentication and data hiding. Singh et al. [38] developed a non-blind robust dual MIW scheme based on DWT and SVD using error correcting codes. Text and image watermarks are embedded in radiological image for secure and compact medical data transmission. They advocated use of a hybrid model of two of the ECCs i.e. BCH and repetition code for higher robustness.

Parah et al. [29] presented two different blind MIW algorithms. For embedding the watermark(EPR) relative value of pre-selected DCT coefficients of 8×8 block is used in both the algorithms. In the first algorithm the watermark is embedded in the whole medical image whereas in the second approach watermark is embedded in the RONI only. It lacks ROI tamper detection and recovery features. Moreover, embedding capacity is also low. Wu et al. [17] proposed a reversible data hiding method with contrast enhancement for medical images. Another region-based watermarking scheme is proposed by Al-Haj and Amer [1] using both spatial and frequency domains. Robust watermarks are embedded in RONI to provide confidentiality and authenticity using DWT-SVD transform. Fragile watermark is embedded in ROI of medical image by LSB embedding technique to provide integrity. But, this scheme has limitations of low embedding capacity, low accuracy of tamper detection and high computation time. Table 1 illustrates the comparison of different MIW schemes.

2.1 Motivation and contribution of the proposed work

From the literature review we have two observations. Firstly, most of the SVD based watermarking techniques in existing literature suffers from false positive detection problem [6]. Secondly, many MIW techniques dealing with tamper detection, localization and recovery have low accuracy in tamper detection and poor visual quality of recovered ROI [1, 19, 42]. Intactness of ROI is very important as it is used for diagnosis. Tampered ROI can lead to wrong diagnosis. Therefore, it is very important to detect ROI tampering accurately. Recovery of tampered ROI with good visual quality is another crucial aspect. We are motivated by these issues. The main contribution of our work is as follows:

- False positive free: In false positive problem the fabricated watermark is extracted from an arbitrary image where the embedded watermark is completely different from the extracted watermark. To embed the watermark W, SVD is applied on it. Watermark is decomposed into three matrices as given by Eq. 1.

$$W = U_W S_W V_W^T \tag{1}$$

  Only the singular values matrix of watermark S_W is embedded while the orthogonal matrices U_W and V_W are not embedded. In extraction procedure, only the diagonal

Table 1 Literature review of existing MIW schemes (RB-region based, TL-tamper localization, TR-tamper recovery)

Scheme	Embedding technique	Objective	Embedded data	Reversible	RB	TL	TR
Naseem et al. [27]	LSB method	Authentication	Authentication data	Irreversible-RONI Reversible-ROI	✓	×	×
Thabit and Khoo [40]	SLT, IWT	Authentication, Data hiding	Authentication, recovery data, patient data	Reversible	✓	✓	✓
Al-Haj and Amer [1]	DWT-SVD, LSB method	Authentication, confidentiality, integrity	Authentication, recovery and patient data	Reversible	✓	✓	✓
Hajjaji et al. [16]	LSB method	Confidentiality, integrity	Patient's data, diagonstic data	Irreversible	×	×	×
Memon et al. [25]	IWT	Authentication, confidentiality, integrity, security	Patient's data, doctor's code, LSB of ROI	Reversible	✓	✓	✓
Amit et al. [37]	DWT, Spread spectrum	Authentication, confidentiality, data hiding	doctor's code, image code, patient's identity	Irreversible	×	×	×
Parah et al. [29]	DCT	Confidentiality, and Data hiding	EPR data	Irreversible	×	×	×
Guo and Zhuang [14]	Modified DE	Authentication, and data hiding	Authentication, patient's data	Reversible	✓	×	×
Pandey et al. [28]	DWT, SVD	Authentication, confidentiality and security	Signature, caption, reference watermark, index	Irreversible	×	×	×
Proposed Scheme	IWT-SVD, LSB	Authentication, confidentiality, integrity, security data hiding	patient's data, hospital's logo, recovery data	Irreversible RONI Reversible-ROI	✓	✓	✓

matrix S_W is extracted, whereas U_W and V_W is available at the receiver end. However, the orthogonal matrices U_W and V_W contain the major information about an image. Thus any one can provide a fake pair of orthogonal matrices and claim that his watermark is present in the watermarked image, which causes false positive detection problem as shown in Fig. 1.

Matrix U of SVD has a unique property i.e. all the elements in the first column have very close values. In the same elements of first row of V matrix have close values. By analyzing U, we observe that there is a strong correlation between the $(U_{2,1})$ and $(U_{3,1})$ element [9, 20]. Similarly, $(V_{1,2})$ and $(V_{1,3})$ elements of V matrix are strongly correlated. We have explored this property of SVD to overcome the false positive problem.

- SVD has a notable stability and robustness against the common image manipulation (such as filtering, histogram equalization, noise addition, etc.) and geometric attacks (such as cropping, rotation) etc. Whereas, IWT provides tolerance towards compression algorithms and filtering. IWT-SVD has been used for providing robustness to the watermarks embedded in RONI against these attacks although it may increases computational complexity to some extent.
- Tamper detection, localization and recovery with higher accuracy: pixel-wise positional and relational bits are calculated and embedded in ROI, to detect and localize altered pixels with high precision. Visual quality of recovered pixel is also good.
- Improved performance: In the comparative study of proposed scheme with the other existing techniques in [1, 29], it is observed that the proposed scheme offers superior performance in terms of imperceptibility of watermarked image, robustness, payload, temper detection accuracy and visual quality of recovered ROI.
- Multiple watermarks are embedded simultaneously in the medical image [28]. Multiple watermarks i.e. EPR, hospital logo and ROI LSBs are embedded in the same medical

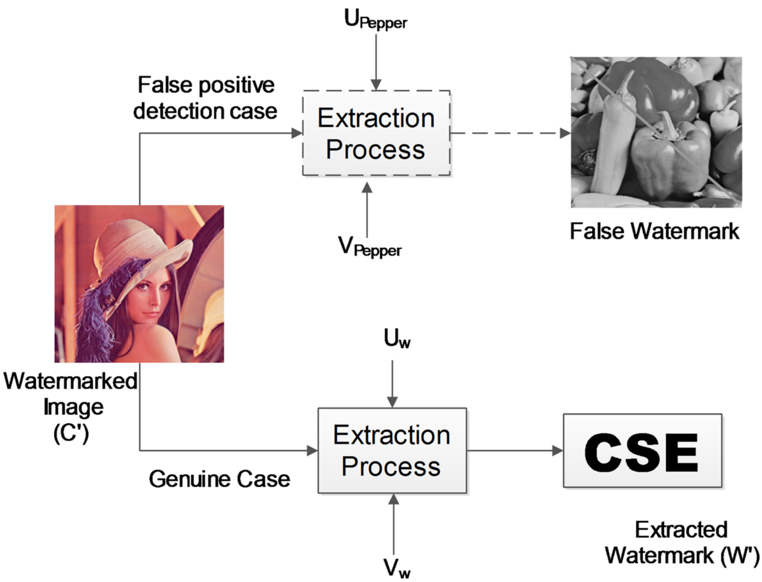

Fig. 1 False positive detection

image simultaneously for providing confidentiality, authentication and integrity respectively. Reduced storage and less bandwidth requirements are the additional benefit that we get as by-product.

3 Proposed technique

The proposed region-based MIW scheme provides confidentiality, authenticity, and integrity for medical images transmitted in telemedicine applications. For embedding the watermarks we firstly divide medical image into ROI and RONI. ROI in medical images can be selected in several ways such as selecting a rectangle or polygon manually by the physician/radiologist, defining a threshold [12], defining seeds [15] or edge detection [23] etc. Mostly, automated ROI detection schemes are specific to a particular image modality and any alterations in the medical image, may yield different ROI boundaries. Keeping the limitations of automated ROI selection in consideration we use manual selection of rectangular ROI by the physician/radiologist. The advantage of representing rectangular ROI is that only two coordinate points i.e. top left and bottom right needed to specified instead of a group of coordinates [23]. The ROI is watermarked in the spatial domain, whereas the RONI is watermarked in the frequency domain using IWT-SVD hybrid transform to achieve different MIW objectives. Spatial techniques are fragile and hence can be used for ROI tamper detection. EPR and hospital logo is embedded in RONI to provide confidentiality and authentication respectively. It is important that these watermarks should be robust. We have used IWT and SVD transform to provide robustness to these watermarks against various signal and geometric attacks. The proposed MIW scheme has four modules i.e. ROI embedding, ROI extraction, RONI embedding and RONI extraction. These modules are discussed in detail in following sub sections.

3.1 ROI embedding

ROI is used for diagnosis. Hence its integrity verification is important. Positional and relational bits are calculated and embedded in ROI pixels using LSB technique for pixel-wise ROI integrity verification as shown in Fig. 2. Original LSBs of ROI pixels are extracted and embedded in RONI to serve as backup for restoring tampered ROI pixels.

3.1.1 Steps for ROI embedding process

Step 1: Extract the LSBs of ROI pixels and concatenate them as a single robust watermark for embedding in the RONI.

Step 2: Calculate the positional bit with respect to its position i.e. row and column. Positional bit is calculated using 6 MSBs of pixel P_i represented as b_a where a ϵ (2...7). P_1 represents bitwise XOR operation between row and pixel value whereas P_2 represents bitwise XOR operation between column and pixel value. P_1 and P_2 is calculated using (2) and (3).

$$P1 = XOR(b^r_{a-2}, b_a) \tag{2}$$

$$P2 = XOR(b^c_{a-2}, b_a) \tag{3}$$

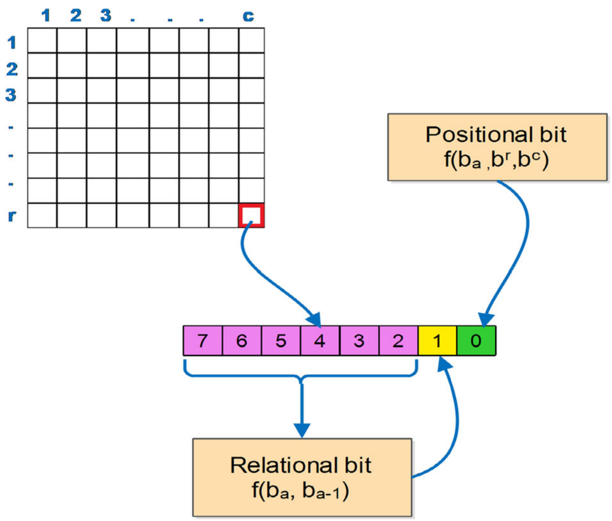

Fig. 2 Embedding of positional and relational bit in ROI pixels

Where a=7,6...2 and b^r and b^c are the binary value of row and column value. Now, calculate positional bit using (4), and embed it in the first LSB of pixel P_i.

$$Positional\ bit = \left\{ \sum_{i=1,2,..6} (P1_i \wedge P2_i) \right\} mod\ 2 \tag{4}$$

Step 3: Relational bit shows the relation between 6 MSBs of P_i. Calculate relational bit using (5) where b_i are the bits of a pixel P_i.

$$Relational\ bit = \left\{ \sum_{i=7,6,..3} (b_i \oplus b_{i-1}) \right\} mod\ 2 \tag{5}$$

Embed the relational bit in the second LSB of pixel P_i.

Step 4: Repeat step 2 and step 3 for each ROI pixel to obtain watermarked ROI'.

3.1.2 Analysis of tampering effects

We analyze the probability of tampering to the watermarked ROI'. Probability of alteration in positional and relational bits due to altered MSBs is calculated as follows:

Positional bit Let b^r and b^c be the binary form of row and column values of ROI'. The total number of possible alterations for any pixel by MSBs is as follows:

$$\alpha_1 = \sum_{i=1,2,..6} {}^6C_i \tag{6}$$

Assume that in a pixel P_i, k bits of the 6 MSBs are altered, then total number of sets of MSBs that affects the positional bit is calculated as follows:

$$\alpha_2 = \sum_{1 \le i \le k} \binom{k}{i} 2^{6-k} \qquad where\ i\ is\ odd \tag{7}$$

Above equation represents those combinations, for which $b^r_{(a-2)}$ and $b^c_{(a-2)}$ is not same for any bit. Therefore, calculate a multiplicative factor to get the actual number of altered set of MSBs. In the image I of size X × Y, if X ≤ 15 or Y ≤ 15 or both are satisfied then, the multiplicative factor γ is calculated by (8).

$$\gamma = 1 - \left[\frac{\{(X-15)+(Y-15)\}}{(X \times Y)} \right] \tag{8}$$

Therefore, the number of pixels, that affects the positional bits, can be obtained by (9).

$$\alpha_3 = \gamma \times \alpha_2 \tag{9}$$

Thus, the probability of alteration in positional bit due to change in pixels is given by (10).

$$Pr_{(p)} = \frac{\alpha_3}{\alpha_1} \tag{10}$$

Relational bit Relational bit can detect alteration in P_i only if the altered pixels contain one altered MSB boundary bit i.e. either 2^{nd} or 7^{th}. Maximum number of possible alterations in MSBs is β_1, given by (11).The total number of combination of MSBs for P_i which exactly contains one boundary bit is given by (11) and (12).

$$\beta_1 = \sum_{i=1,2,3,..6} {}^6C_i - \sum_{i=1,2,3,..5} {}^5C_i \tag{11}$$

$$\beta_2 = \frac{1}{2} \times \sum_{i=1,2,..4} {}^4C_i \tag{12}$$

Hence, the number of pixels which actually affects the relational bits β_3, is calculated as follows:

$$\beta_3 = \beta_1 - \beta_2 \tag{13}$$

Therefore, the probability of changes in relational bit is given by (14).

$$Pr_{(r)} = \frac{\beta_3}{\alpha_1} \tag{14}$$

Now, the probability for a pixel to get detected can be calculated by (15).

$$Pr_{(tot)} = Pr_{(p)} + Pr_{(r)} \tag{15}$$

3.2 ROI extraction

ROI integrity is verified by comparing the calculated and extracted values of positional and relational bits. If the calculated value and extracted values of positional and relational bits matches then the pixels are considered to be intact otherwise tampered. In case of tampering we recover the pixel by using recovery bits extracted from RONI. Steps of ROI extraction is explained below.

Step 1: For all pixels of watermarked ROI', calculate the positional bit using (4). Compare the calculated positional bit with the extracted first LSB of corresponding pixel. If there is match then step 2 is performed. If there is mismatch, mark those pixels as altered one and perform step 3.

Step 2: Calculate the relational bit by using (5). Compare the calculated relational bit with the extracted second LSB of corresponding pixel. If there is mismatch then those pixels will be marked as altered pixel.

Step 3: Replace the two LSBs of pixels with the original ROI LSBs extracted from RONI to get recovered ROI.

3.3 RONI embedding

In the proposed scheme three different robust watermarks i.e. EPR, hospital logo (binary image watermark) and ROI LSBs are embedded as robust watermarks as shown in Fig. 3. RONI is watermarked using IWT-SVD hybrid transform to provide higher robustness and imperceptibility. IWT provides robustness, tolerance to various compression algorithms and filtering. It maps integer to integer and thus avoids fractional computations. It allows construction of lossless retrieval. Wavelet transform have excellent spatial localization, frequency spread, and multi-resolution characteristics, are similar to the theoretical models of the human visual system [39]. SVD provides a good stability and robustness against

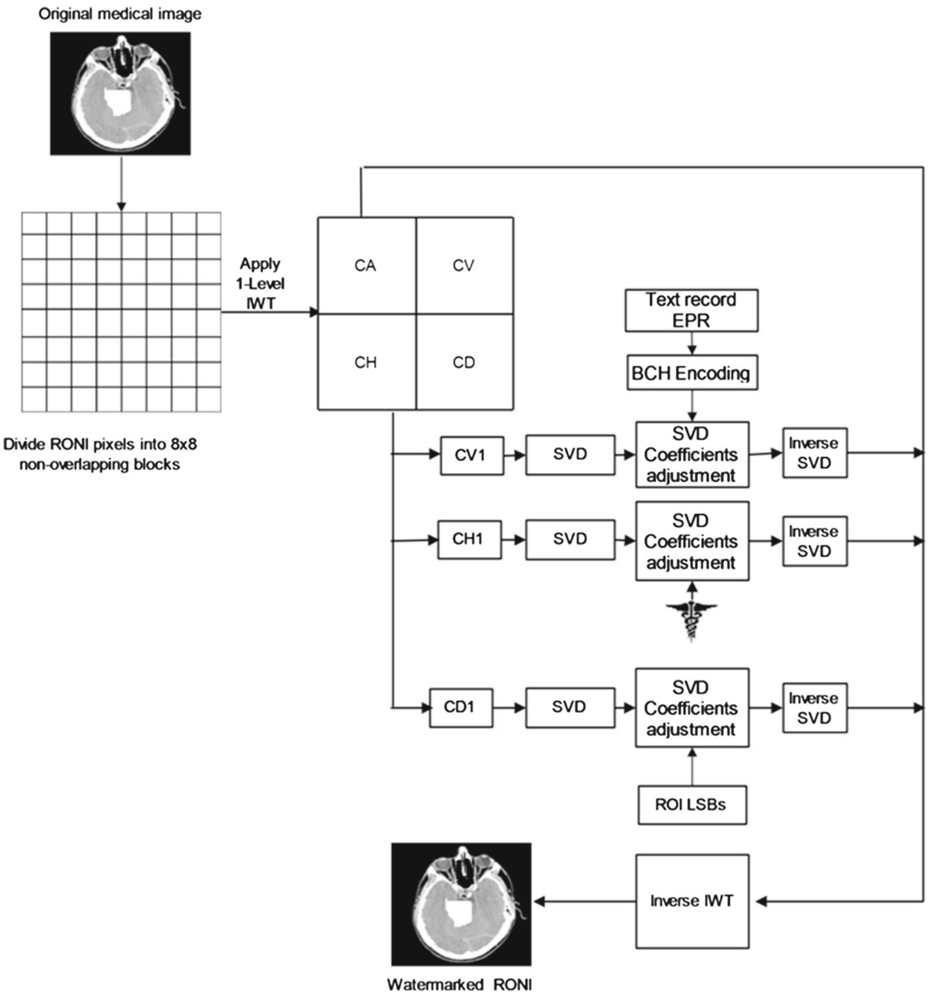

Fig. 3 Block diagram of RONI embedding

the common image manipulation (such as histogram equalization, filtering, noise addition, etc.). RONI pixels are divided into 8 × 8 blocks and IWT is applied to each block. For each block, four sub-bands CA, CV, CH and CD of 4 × 4 is obtained. SVD is applied on CV, CH and CD sub-bands yielding their corresponding U, S and V matrix. Two watermark bits are embedded in a 4 × 4 sub block. First bit is embedded by adjusting second and third element of first column ($U_{2,1}$ and $U_{3,1}$) of U matrix. Whereas, second bit is embedded by adjusting second and third element of first row ($V_{1,2}$ and $V_{1,3}$) of V matrix. There is a strong correlation between ($U_{2,1}$ and $U_{3,1}$) of U matrix and ($V_{1,2}$ and $V_{1,3}$) of V matrix. This property has been explored for embedding watermark bits. We embed watermark bits of EPR, hospital logo and ROI LSBs in CV, CH and CD respectively. For additional security and robustness of EPR we use BCH error correction code. Detail description of RONI embedding process is provided below.

3.3.1 Steps of RONI embedding process

Step 1: Perform BCH encoding (error correction codes) to the 7 bit ASCII representation of text watermark (EPR) bits as follows

$$W_b = BCH(watermark\ bits) \tag{16}$$

Step 2: Convert each of the three robust watermarks i.e. W_b, hospital logo and ROI LSBs in the form of 1-D bit patterns.

Step 3: Divide RONI into 8 × 8 non-overlapping blocks.

Step 4: Apply the 1-level IWT on the 8 × 8 RONI block. Four sub-bands CA, CV, CH and CD of size 4 × 4 are obtained.

Step 5: Apply SVD on CV, CH and CD sub-bands

$$X = U_X S_X V_X^T \qquad where\ X \epsilon (CV, CH, CD) \tag{17}$$

Step 6: Embed two watermark bits each of encoded EPR (W_b), hospital logo and ROI LSBs simultaneously in CV, CH and CD sub-band respectively. One bit each is embedded by adjusting ($U_{2,1}$ and $U_{3,1}$) and ($V_{1,2}$, $V_{1,3}$) coefficients according to the adjustment process explained in algorithm 1.

Step 7: Perform inverse SVD on watermarked U, S_X, and watermarked V matrices for each IWT sub-band.

Step 8: Apply inverse IWT on the sub-bands CA and watermarked CV, CH, CD.

Step 9: Repeat through step 4 to step 8 until all watermark bits are embedded in their respective sub-bands to construct the watermarked RONI.

3.3.2 Algorithm for SVD coefficient adjustment

Watermark bits are embedded by adjusting relations between ($U_{2,1}$ and $U_{3,1}$), ($V_{1,2}$ and $V_{1,3}$) coefficients of U and V matrices. For embedding watermark bit 1, the difference between $U_{2,1}$ and $U_{3,1}$ should be negative and greater than threshold T. To embed watermark bit 0, the difference between $U_{2,1}$ and $U_{3,1}$ should be positive and greater than the threshold T. When these two conditions are violated, SVD coefficients are adjusted according to the Algorithm 1. Similarly, $V_{1,2}$ and $V_{1,3}$ coefficients of V matrix are adjusted for embedding watermark bit. The process of SVD coefficient adjustment is shown in shown in Fig. 4. The flowchart indicating the detailed steps for SVD coefficient adjustment is shown in Fig. 5. Value of threshold T is determined empirically according to the trade off between imperceptibility and robustness. At high threshold, robustness is high but imperceptibility is low.

Algorithm 1 SVD coefficient adjustment

Require: U and V matrix
Ensure: Watermarked U and V matrix

To embed first watermark bit in U matrix
U_{avg}= ($|U_{2,1}|$+ $|U_{3,1}|$)/2
if W=1 **then**
  if $U_{2,1}$ - $U_{3,1}$ <-T **then**
    $U_{2,1} = sign(U_{2,1}) \times (U_{avg} + T/2)$
    $U_{3,1} = sign(U_{3,1}) \times (U_{avg} - T/2)$
  else
    No change
  end if
else if $U_{2,1}$ - $U_{3,1}$ <T **then**
  $U_{2,1} = sign(U_{2,1}) \times (U_{avg} - T/2)$
  $U_{3,1} = sign(U_{3,1}) \times (U_{avg} + T/2)$
else
  No change
end if
where sign(X) presents the sign of X, |X|denotes the absolute value of x.
To embed second watermark bit in V matrix
V_{avg}= ($|V_{1,2}|$+$|V_{1,3}|$)/2
if W=1 **then**
  if $V_{1,2}$ - $V_{1,3}$ <-T **then**
    $V_{1,2} = sign(V_{1,2}) \times (V_{avg} + T/2)$
    $V_{1,3} = sign(V_{1,3}) \times (V_{avg} - T/2)$
  else
    No change
  end if
else if $V_{1,2}$ - $V_{1,3}$ <T **then**
  $V_{1,2} = sign(V_{1,2}) \times (V_{avg} - T/2)$
  $V_{1,3} = sign(V_{1,3}) \times (V_{avg} + T/2)$
else
  No change
end if

3.4 Extraction from RONI

Extraction from RONI is just reverse process of embedding in RONI. Figure 6 shows the block diagram of RONI extraction process. Steps for extraction from RONI is explained below.

Step 1: Divide watermarked RONI into 8 × 8 blocks.
Step 2: Apply 1-level IWT on 8 × 8 RONI block. Four sub-bands CA, CV, CH and CD of size 4 × 4 are obtained.

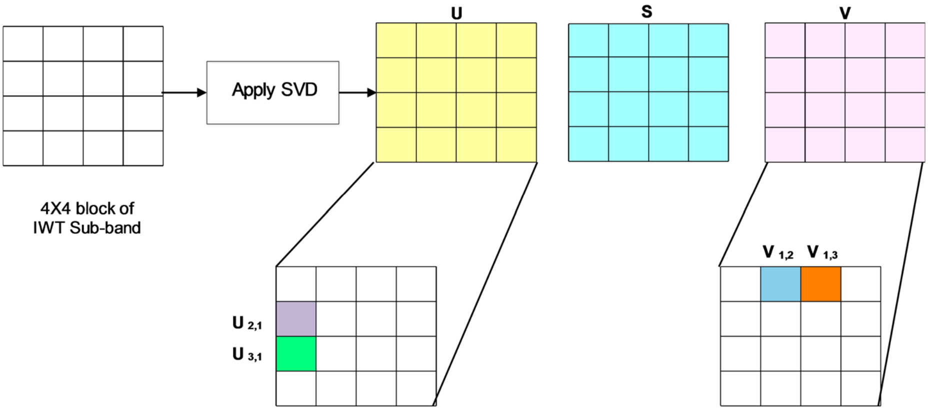

Fig. 4 SVD coefficient adjustment

Step 3: Apply SVD on CV, CH and CD sub-bands as following

$$X = U_X S_X V_X^T \qquad where\ X \epsilon (CV, CH, CD) \tag{18}$$

Step 4: From each sub-band the first watermark bit W_1' is extracted from $(U_{2,1}, U_{3,1})$ coefficients of the U matrix using following relation.

$$W_1' = \begin{cases} 0 & \text{if } U_{2,1} > U_{3,1} \\ 1 & \text{if } U_{2,1} \leq U_{3,1} \end{cases} \tag{19}$$

The second watermark bit W_2' is extracted by applying the following relation between $(V_{1,2}, V_{1,3})$.

$$W_2' = \begin{cases} 0 & \text{if } V_{1,2} > V_{1,3} \\ 1 & \text{if } V_{1,2} \leq V_{1,3} \end{cases} \tag{20}$$

Step 5: Repeat step 2 to step 4, until all watermarked RONI blocks are processed.
Step 6: Reconstruct the three watermarks by cascading relevant watermark bits extracted from the respective sub-bands of all blocks.
Step 7: Perform BCH decoding to the watermark bits extracted from CD sub-band to get the extracted EPR(text watermark).

In the proposed scheme, experimentation is validated on wide range of gray scale medical images of different modalities. However, proposed scheme can be generalized for the color medical images also. We have applied proposed scheme for color medical images using RGB color model. In RGB color model red, green and blue channel can be extracted and treated as a grayscale image. Watermarks are embedded in the blue channel as explained in Sections 3.1 and 3.3. Then the original blue channel in the RGB image is replaced by the

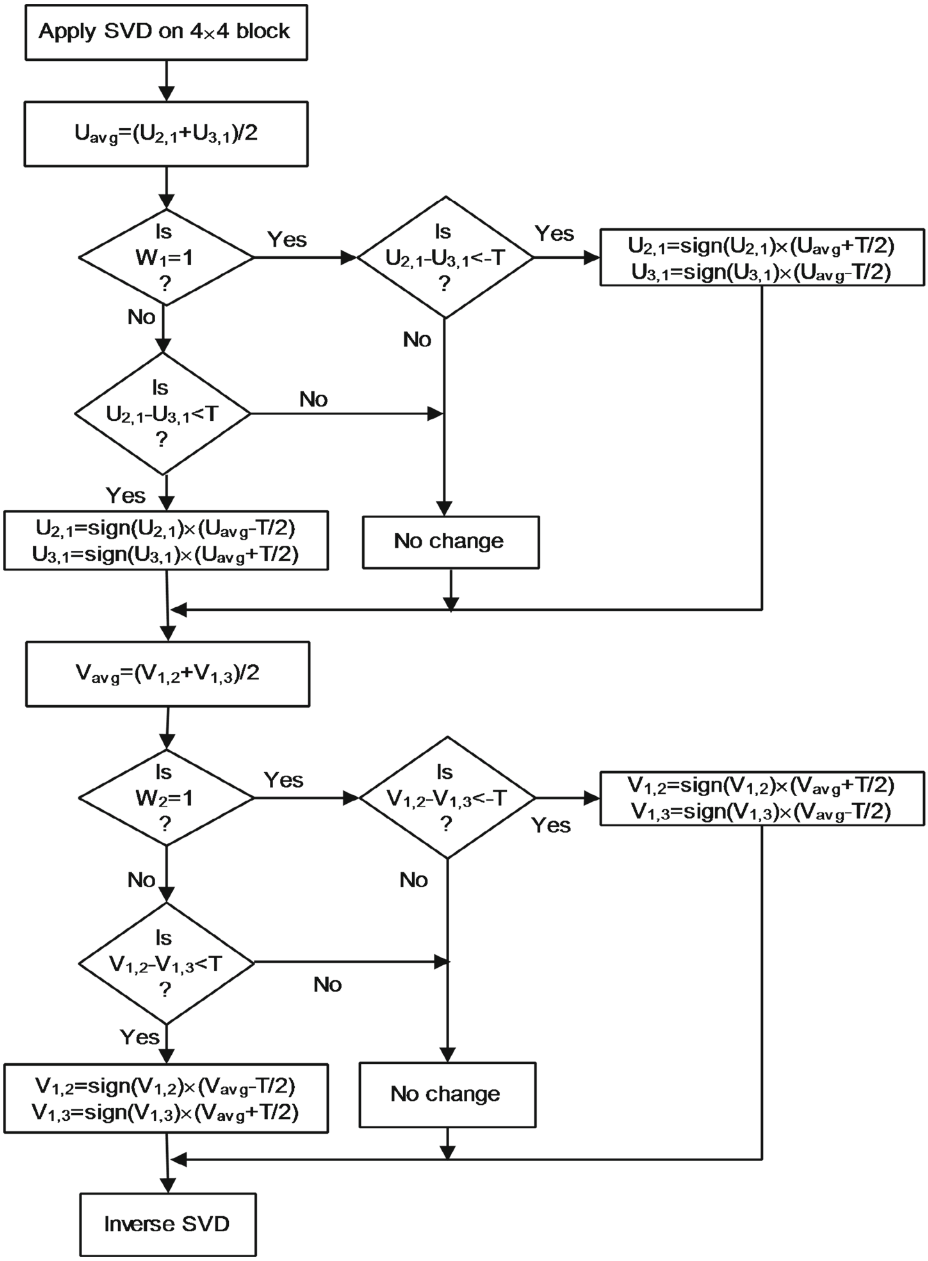

Fig. 5 Flowchart for SVD coefficient adjustment

watermarked blue channel to obtain the watermarked color image. Watermarks are extracted from watermarked blue channel according to the extraction process explained in Sections 3.2 and 3.4.

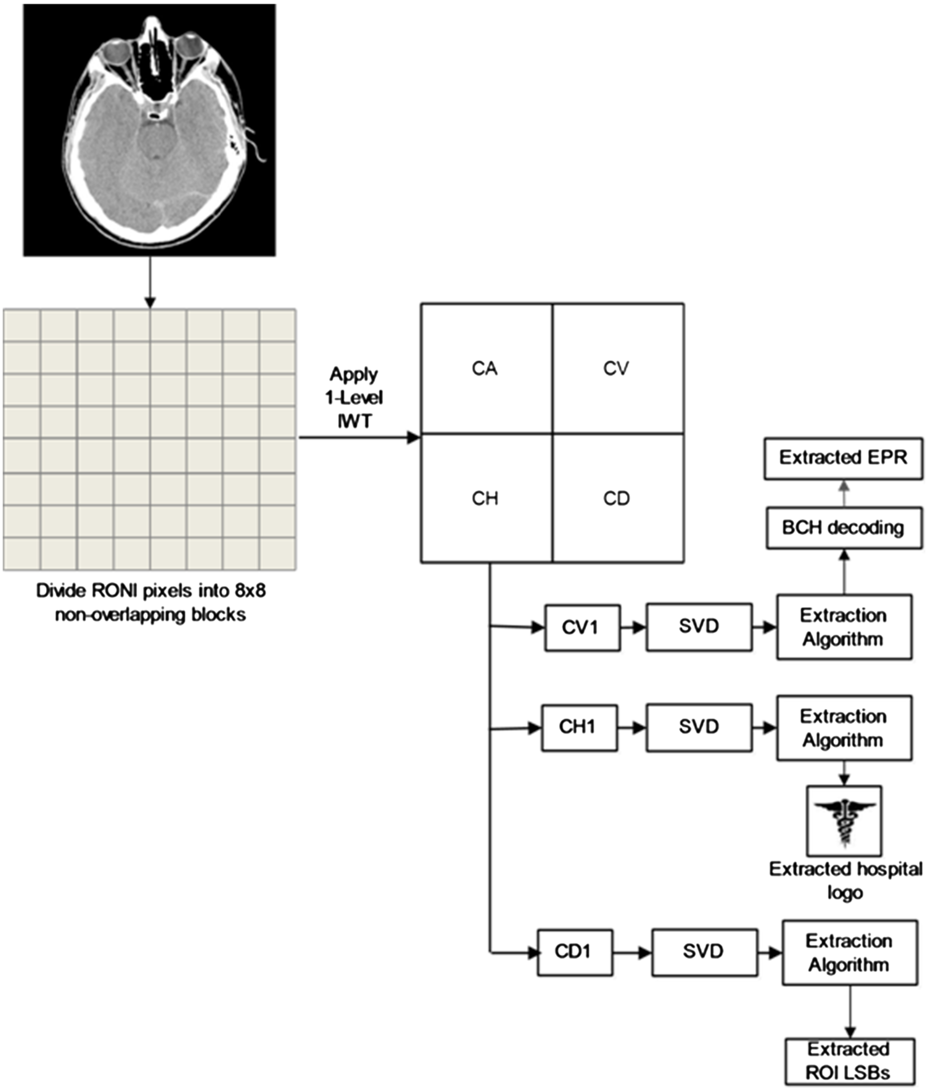

Fig. 6 Block diagram of RONI extraction

4 Experimental Results and Discussions

4.1 Experimental configuration

Experiments have been conducted to evaluate the performance of the proposed scheme in terms of imperceptibility, robustness, time performance, tamper detection and recovery. Experimentation is done using MATLAB R2013a on a PC having Intel core2 Duo, 3.00 GHz, 2GB RAM. Gray scale and color medical images of different modalities have been used as test cover image as shown in Figs. 7 and 8 respectively. All the cover images are of

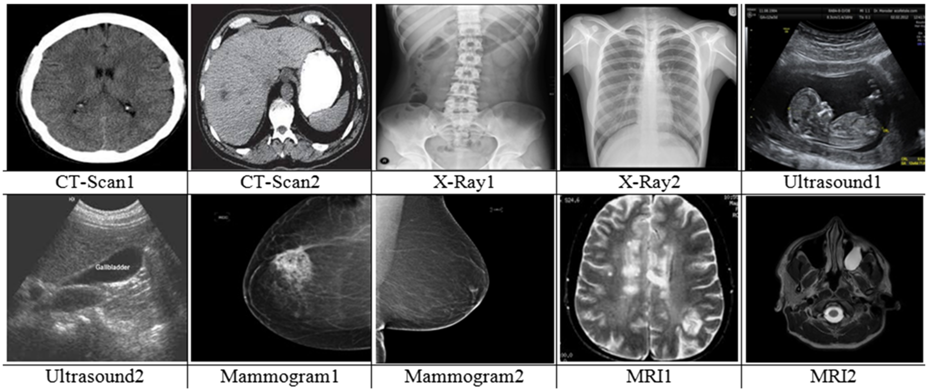

Fig. 7 Grayscale medical cover images of different modalities

size 512 × 512. Binary watermark of hospital logo having size 64 × 32 and EPR of 2048 bits are embedded in the medical images for authenticity and confidentiality respectively as shown in Fig. 9. For all experimentation we have taken threshold T as 0.05.

4.2 Performance measures

The performance of the MIW schemes can be assessed on the basis of imperceptibility, robustness and payload. For objective evaluation of imperceptibility between original and watermarked medical images peak signal-to-noise ratio (PSNR) and structure similarity measure index (SSIM) are used. Normalized correlation (NC) and bit error rate (BER) are used to measure the similarity and differences between original watermark and extracted watermark. Evaluation metrics used to evaluate imperceptibility and robustness of proposed scheme are given in Table 2.

4.3 Imperceptibility test

Imperceptibility is one of the important requirments of MIW scheme. Watermarked image should not have any perceivable distortion as it will be used for diagnosis. Peak signal to-noise ratio (PSNR) and structure similarity measure index (SSIM) are used for objective evaluation of imperceptibility between original and watermarked medical images. Higher the PSNR value, higher is the imperceptibility. Empirically tested threshold value of PSNR is 35dB. From Tables 3 and 4 we can observe that average PSNR value of gray scale and color medical images is about 45dB which is more than the empirical threshold. SSIM value

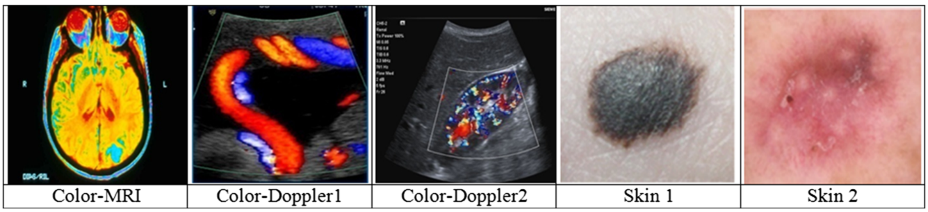

Fig. 8 Color medical cover images of different modalities

	Patient's name_ID_imageID__illness:Priyanka_ISM2705_PXCA1322_Headache
Image Watermark (Hospital Logo)	Electronic Patient Record(EPR)

Fig. 9 Watermarks: Hospital logo, EPR

is about 0.97 which is near to the ideal value indicates that the watermarked images have no significant distortions. PSNR and SSIM values are consistently good for all the tested image modalities therefore it is anticipated that it will yield good imperceptibility with other modalities also. Subjective evaluation of visual quality of watermarked images show no considerable perceivable difference between original and watermarked image as shown in Fig. 10 for gray scale images and Fig. 11 for color images with corresponding PSNR

Table 2 Evaluation metric used for analysis and comparisons

Evaluation metric	Equation	Ideal value
PSNR (Gray scale)	$PSNR = 10log_{10}\left(\frac{255^2 \times M \times N}{\sum_{i=1}^{M}\sum_{j=1}^{N}(I_m(i,j) - I'_m(i,j)^2}\right)$	Infinity
	where $I_m(i,j)$ and $I'_m(i,j)$ are the original & watermarked pixels at (i,j) position respectively. M and N are the dimensions of image I_m	
PSNR (Color)	$PSNR_c = \sum_{i=1}^{3} PSNR_i$	Infinity
	where i=1 is red, i=2 is green and i=3 is blue channel. $PSNR_i$ denotes PSNR of i_{th} channel	
SSIM	$SSIM(x,y) = \left(\frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}\right)$	1
	where μ_x, μ_y are the averages of x and y, σ_x^2, σ_y^2 are the variances and σ_{xy} and covariance for x and y respectively. C_1 and C_2 are balancing constants	
NC	$NC = \left(\frac{\sum_{i=1}^{X}\sum_{j=1}^{Y}(W_o(i,j) \times W_e(i,j))}{\sum_{i=1}^{X}\sum_{j=1}^{Y} W_o^2(i,j))}\right)$	1
	where $W_o(i,j), W_e(i,j)$ are the original and extracted watermark pixels at (i,j) position	
BER	$BER = \frac{Number\ of\ incorrectly\ decoded\ bits}{Total\ number\ of\ bits}$	0

Table 3 PSNR and SSIM of gray scale medical images

Medical image	PSNR(dB)	SSIM	Medical image	PSNR(dB)	SSIM
CT-Scan1	45.8155	0.9680	Ultrasound2	44.2395	0.9725
CT-Scan2	46.0839	0.9718	Mammogram1	46.5825	0.9845
X-ray1	43.8756	0.9635	Mammogram2	45.6137	0.9709
X-ray2	44.3842	0.9819	MRI-1	43.9768	0.9750
Ultrasound1	44.8891	0.9789	MRI-2	43.4132	0.9783
Average	45.0097	0.9728	Average	44.7651	0.9762

values. Objective and subjective evaluations, reveals that the proposed scheme introduced no distortions, thus we can claim that imperceptibility requirement is achieved.

4.4 Robustness test

Robustness is another important requirement of MIW. It is necessary that the watermarks should survive intentional/unintentional attacks with minimum distortion as they will be used for authentication of ownership and originating source and integrity verification. Robustness of the proposed scheme has been tested against various attacks like salt and pepper noise, histogram equalization, JPEG compression, average filtering and cropping attacks.

4.4.1 Robustness against salt and pepper attack

Watermarked medical images have been subjected to salt and pepper noise of varying densities (0.001 and 0.01). NC and BER of image watermark and EPR extracted from different medical images under various intensities of salt and pepper noise is provided in Table 5. In all cases NC values are more than 0.9870 (more than the threshold). Thus, extracted watermarks are clearly visible. BER is 0 in all cases for extracted EPR when noise density is 0.001 and in all other cases it is close to 0. NC and BER values do not vary significantly even at higher noise density which indicates that the proposed scheme is effective at high noise density also. Therefore, from the results of Table 5 it is evident that the proposed scheme effectively resists the salt and pepper attack.

4.4.2 Robustness against JPEG compression

Watermarked images may undergo JPEG compression to reduce media storage and transmission costs. Medical images of different modalities have been tested for JPEG compression under different quality factors. Higher the quality factor lower is the compression and vice versa. Thus, the quality of extracted watermark increases with the increase in quality

Table 4 PSNR and SSIM of color medical images

Medical image	Color-MRI	Doppler1	Doppler2	Skin 1	Skin 2	Average
PSNR(dB)	43. 8809	44.8493	45.3853	44.0628	44.0965	44.5985
SSIM	0.9604	0.9752	0.9816	0.9783	0.9787	0.9748

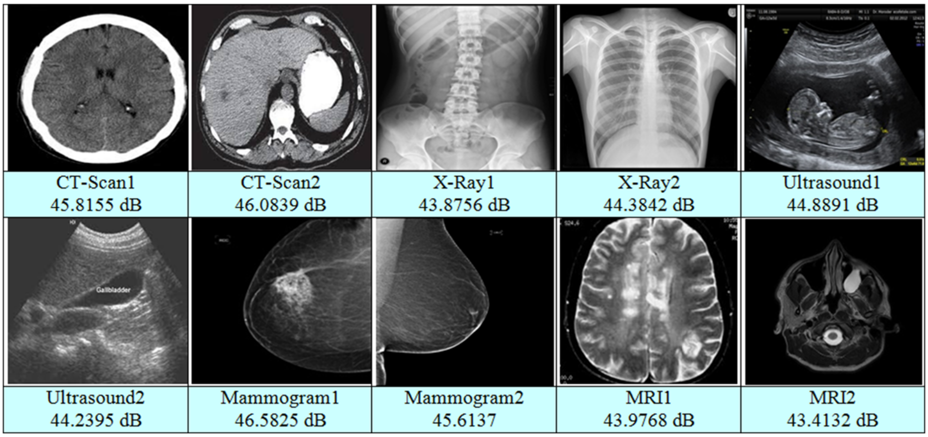

Fig. 10 Watermarked grayscale images with their corresponding PSNR values(dB)

factor as shown in Table 6. It can be observed from Table 6 that the proposed scheme can resist JPEG compression at low quality factor also. NC values are more than the empirical threshold indicating that extracted watermarks are easily distinguishable. BER value decreases with the increase in JPEG quality factor, and approaches to zero when JPEG quality factor is higher than 50. Proposed scheme shows good resistance against JPEG compression.

4.4.3 Robustness against histogram equalization

Histogram equalization attack changes most of the pixel values of image. Under this attack, performance of proposed algorithm is given in Table 7. NC values indicate that the extracted watermarks are distinctly visible. The results in Table 7 shows that the proposed algorithm is effective for the histogram equalization as BER is less than 1.

4.4.4 Average filtering

The watermarked images were subjected to average filtering attack with mask size 3×3 and the results are tabulated in Table 8. The NC value offered by the scheme is quite acceptable and the BER value is closer to 0 as shown in Table 8.

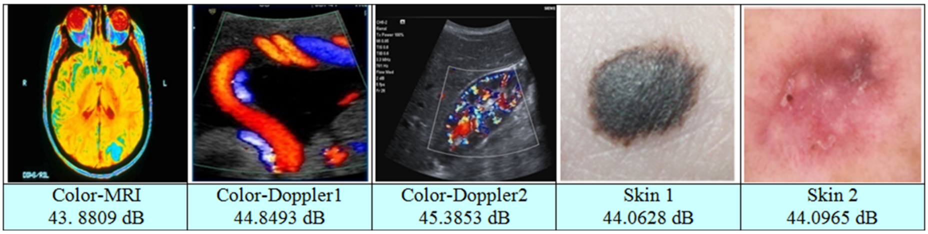

Fig. 11 Watermarked color images with their corresponding PSNR values(dB)

Table 5 NC and BER of image watermark and EPR extracted from different medical images under various intensities of salt and pepper noise

Watermarked image	0.001				0.01			
	Image watermark		EPR		Image watermark		EPR	
	NC	BER	NC	BER	NC	BER	NC	BER
CT-Scan1	0.9924	0.0009	0.9912	0	0.9851	0.0028	0.9783	0.0014
X-Ray 1	0.9898	0.0020	0.9926	0	0.9793	0.0032	0.9796	0.0021
Ultrasound1	0.9937	0.0015	0.9874	0	0.9827	0.0029	0.9815	0.0019
Mammogram 1	0.9961	0.0006	0.9905	0	0.9801	0	0.9741	0.0032
MRI1	0.9942	0.0008	0.9896	0	0.9763	0.0014	0.9811	0.0023
Color-Doppler 1	0.9891	0.0012	0.9794	0	0.9826	0.0027	0.9855	0.0028

4.4.5 Cropping

A cropping attack from top left corner and center is applied on the watermarked medical image using mask size 25 % of dimension of the image. The results obtained after cropping

Table 6 NC and BER of image watermark and EPR extracted from different medical images under various quality factors of JPEG compression

Watermarked image	Quality factor	Image watermark		EPR	
		NC	BER	NC	BER
CT-Scan1	QF=10	0.9151	0.0342	0.8308	0.0635
	QF=50	0.9774	0.0088	0.9759	0
	QF=90	0.9937	0.0020	0.9692	0
X-Ray 1	QF=10	0.9479	0.0088	0.8627	0.0579
	QF=50	0.9850	0.0020	0.9874	0
	QF=90	0.9975	0.0009	1	0
Ultrasound1	QF=10	0.9139	0.0266	0.8824	0.0196
	QF=50	0.9874	0.0068	0.9806	0
	QF=90	0.9916	0.0002	0.9975	0
Mammogram 1	QF=10	0.9230	0.0303	0.8192	0.0361
	QF=50	0.9914	0.0039	0.9813	0
	QF=90	0.9960	0	1	0
MRI1	QF=10	0.9348	0.0246	0.8982	0.0092
	QF=50	0.9871	0.0015	0.9827	0
	QF=90	0.9941	0	0.9975	0
Color-Doppler1	QF=10	0.9330	0.0235	0.8129	0.0069
	QF=50	0.9874	0.0068	0.9838	0
	QF=90	0.9893	0	0.9628	0

Table 7 NC and BER of image watermark and EPR extracted from different medical images under histogram Equalization

Watermarked image	Histogram equalization			
	Image watermark		EPR	
	NC	BER	NC	BER
CT-Scan1	0.8077	0.0591	0.8162	0.0310
X-Ray 1	0.8950	0.0820	0.8038	0.0482
Ultrasound1	0.7792	0.0928	0.7993	0.1316
Mammogram 1	0.8374	0.1854	0.8374	0.0285
MRI1	0.7826	0.0862	0.7826	0.0517
Color-Doppler 1	0.8509	0.0374	0.8342	0.0051

25 % from top left corner and 25 % center in terms of NC and BER is given in Table 9. NC and BER values shows that the proposed scheme sustains both of the cropping attacks.

Most of the popular attacks in image processing has been applied extensively to authenticate the robustness of the proposed scheme in this section. Also, payload of the proposed algorithm is analyzed and experimentally proved that with this payload; all the attacks are sustained. Whereas, other attacks included in the standard watermark benchmarking tools can be studied in future.

4.5 Tamper detection, localization and recovery

Erasing and copy-paste tampering are imposed on the watermarked image to evaluate tamper detection, localization and recovery as shown in Fig. 12. Accuracy of tamper detection is upto 98 % as given in Table 10. It is also evident from the table that PSNR values of recovered image are very close to the PSNR of untampered watermarked image. Subjective evaluation from Fig. 12 further affirms that recovered images have good visual quality. Thus, the proposed scheme successfully meets the ROI integrity requirement with high accuracy.

Table 8 NC and BER of image watermark and EPR extracted from different images under average filtering

Watermarked image	Average filtering (3 × 3)			
	Image watermark		EPR	
	NC	BER	NC	BER
CT-Scan1	0.9876	0.0049	0.9873	0.0031
X-Ray 1	0.9843	0.0009	0.9851	0.0047
Ultrasound1	0.9891	0.0028	0.9793	0.0016
Mammogram 1	0.9816	0.0184	0.9876	0.0052
MRI1	0.9784	0.0086	0.9821	0.0017
Color-Doppler 1	0.9863	0.0008	0.9881	0.0018

Table 9 NC and BER of image watermark and EPR extracted from different images under cropping attack

Watermarked image	Cropping(Top left corner)				Cropping center			
	Image watermark		EPR		Image watermark		EPR	
	NC	BER	NC	BER	NC	BER	NC	BER
CT-Scan1	0.8822	0.1465	0.8563	0.0598	0.8776	0.0049	0.8573	0.0031
X-Ray 1	0.8302	0.0914	0.8872	0.0827	0.8843	0.0109	0.8731	0.0047
Ultrasound1	0.8582	0.0763	0.8275	0.0312	0.8691	0.0028	0.8993	0.0016
Mammogram 1	0.7846	0.1082	0.8426	0.0737	0.8781	0.0184	0. 8976	0.0052
MRI1	0.7988	0.1047	0.8749	0.0833	0.8794	0.0086	0. 8921	0.0138
Color-Doppler 1	0.8279	0.0698	0.7998	0.1008	0.8695	0.0072	0.8652	0.0082

4.6 Time performance

Time performance of the proposed technique is evaluated for gray scale and color medical images of different modalities. From Figs. 13 and 14 it can be observed that the relative time requirements for the watermarking is moderate and regardless of image modality. The prime objective of our scheme is to obtain good imperceptibility, higher robustness, tamper detection and recovery with higher accuracy. Therefore, modest increase in computation time due to SVD can be seen as trade off to achieve these objectives.

4.7 Comparative analysis

To further validate the performance of the proposed scheme, it is compared with existing schemes i.e. Al-Haj and Amer's scheme [1] and Parah et al. scheme [29]. In Al-Haj and Amer's scheme [1] the author had proposed a region based blind scheme using DWT-SVD transform. Local fragile watermark is embedded in ROI of the image using a reversible scheme in the spatial domain to provide integrity. Three robust watermarks are embedded in RONI. Parah et al. [29] proposed two different MIW algorithms using DCT. In both of the algorithms two coefficients of 8×8 DCT block are selected and their magnitudes are compared to embed the watermark/EPR bits. In the first algorithm watermark is embedded in the entire image whereas in the second algorithm watermark is embedded in RONI only.

Table 10 Performance of tamper detection and PSNR value of recovered medical images

Medical image	Altered pixels	Detected pixels	Accuracy (%)	PSNR of Recovered image
CT-Scan1	739	691	93.50	45.1528
X-Ray 1	1047	968	92.45	43.5629
Ultrasound1	859	813	94.64	44.3819
Mammogram1	954	935	98.00	45.8451
MRI1	1415	1389	98.16	43.1639

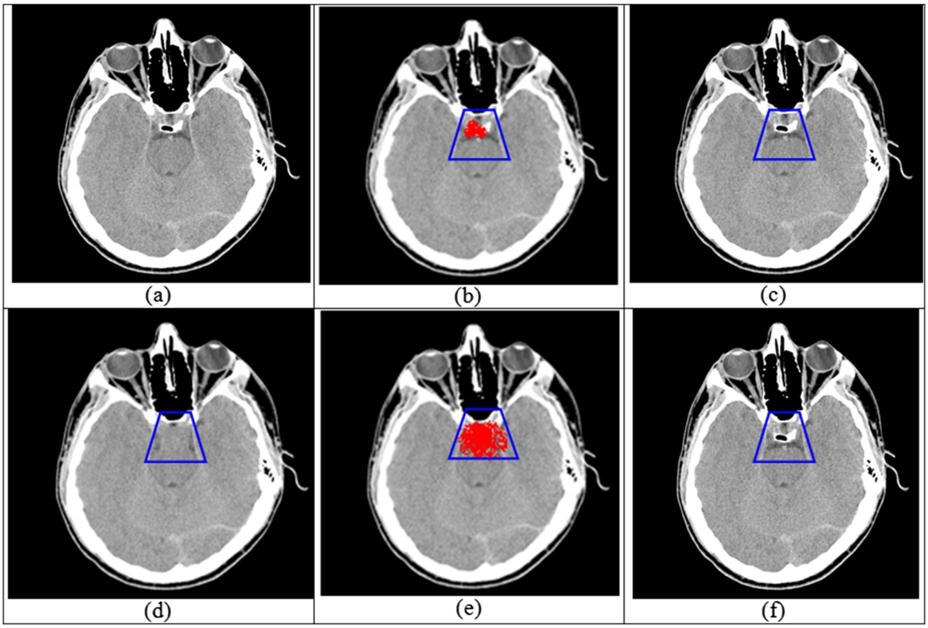

Fig. 12 Tamper localization and recovery. (**a**) Watermarked image (**b**) Localization of erase tampering (**c**) Recovery of erase tampering (**d**) Copy-paste tampering (**e**) Localization of copy & paste tampering (**f**) Recovery of copy-paste tampering

4.7.1 Imperceptibility

The average PSNR acheieved in Al-Haj and Amer's scheme [1] is about 33 dB and in case of Parah et al. [29] it is about 40 dB and 54 dB in the first and second algorithm respectively. Average PSNR of our scheme is higher than Al-Haj and Amer's scheme [1] and the first algorithm of Parah et al. [29]. In the second algorithm of Parah et al. [29] average PSNR is more than our scheme but at the cost of low payload. So, it is concluded that our scheme has better imperceptibility than these existing schemes without sacrificing payload.

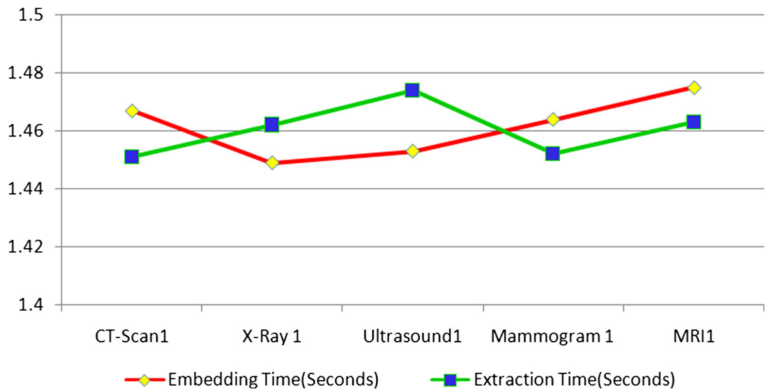

Fig. 13 Embedding and extraction time for *gray*-scale medical images

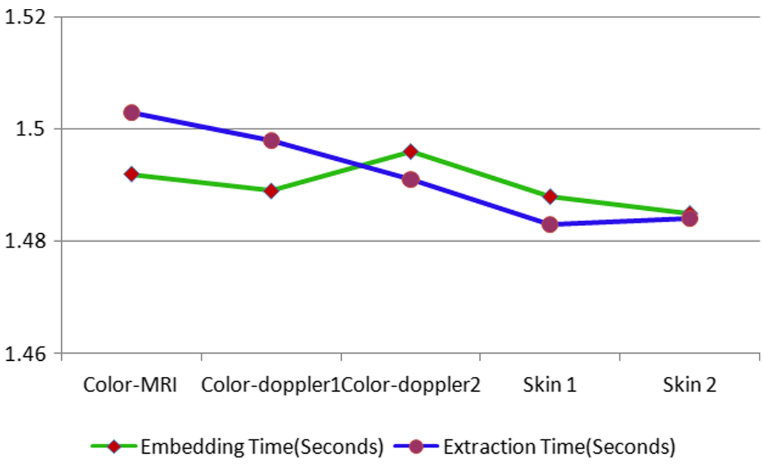

Fig. 14 Embedding and extraction time for color medical images

4.7.2 Robustness

NC and BER values of extracted image watermark and EPR of the proposed scheme is compared with and Al-Haj and Amer [1] in Table 11 under various attacks. It can be observed from Table 11 that NC and BER values of proposed scheme is better than the compared scheme in all attacks. NC value decreases significantly with increase in noise density in Al-Haj and Amer [1] scheme. Also, the quality of extracted watermark deteriorates significantly with decrease in JPEG quality factor. Therefore Al-Haj and Amer [1] scheme cannot be used effectively at high compression ratio and noise densities. The proposed scheme outperforms it in terms of robustness. Besides this tamper detection of Al-Haj and Amer [1] can be easily forged. Whereas, tamper detection and localization is comparatively more accurate in our scheme.

NC and BER values of extracted image watermark and EPR of the proposed scheme is compared with Parah et al. [29] in Table 12. It can be concluded from Table 12 that proposed scheme is more robust than Parah et al. [29] except in histogram equalization which can

Table 11 Comparison of NC and BER of image watermark and EPR extracted from MRI image under various attacks using the proposed scheme and Al-haj and Amer's scheme [1]

Attacks	Proposed scheme				Al-Haj and Amer [1]			
	Image watermark		EPR		Image watermark		EPR	
	NC	BER	NC	BER	NC	BER	NC	BER
Salt and pepper noise (0.001)	0.9942	0.0008	0.9896	0	0.967	0.0038	0.966	0.0019
JPEG compression (QF=80)	0.9927	0	0.9901	0	0.636	0.1000	0.737	0.1382
Gaussian noise (mean=0.1)	0.9725	0.0016	0.9813	0.0008	0.960	0.0462	0.980	0.0485

Table 12 Comparison of NC and BER of image watermark and EPR extracted from CT scan image under various attacks using the proposed scheme and Parah et al. scheme [29]

Attacks	Proposed scheme				Parah et al. [29]			
	Image watermark		EPR		Image watermark		EPR	
	NC	BER	NC	BER	NC	BER	NC	BER
Salt and pepper noise (0.001)	0.9924	0.0009	0.9912	0	0.9652	0.0175	0.9826	0.0162
JPEG compression(QF=80)	0.9948	0.0037	0.9692	0	0.9912	0.0840	0.9794	0.0166
Gaussian noise(mean=0.0001)	0.9813	0.0083	0.9822	0.0019	0.9215	0.0800	0.9534	0.0524
Average Filtering	0.9876	0.0049	0.9873	0.0031	0.9354	0.0654	0.9487	0.0547
Sharpening	0.9861	0.0103	0.9784	0.0084	0.9875	0.0121	0.9525	0.0315
Cropping(Top left 25 %)	0.9822	0.0083	0.9862	0.0041	1	0.0566	0.0008	0.1458

be seen as future improvement work. Parah et al. [29] does not verify integrity of medical images as it lacks feature for tamper detection, localization and recovery.

4.7.3 Payload

The payload of the proposed scheme is compared with the schemes under comparison. In both the algorithms of Parah et al. [29], EPR and authentication watermarks of pre-specified size are embedded. Hence, payload in their scheme is constant i.e. 3072 and 2209 bits in the first and second algorithm respectively. Whereas, the proposed and Al-Haj and Amer scheme [1] embeds ROI LSBs in RONI as recovery bits. But, the size of ROI LSBs are dependent on the manual selection of ROI. Comparison of payload of the proposed scheme and other existing schemes is provided in Table 13. It can be seen that embedding capacity of our scheme is comparatively higher than other schemes.

Table 13 Payload comparison

Scheme	Cover image	EPR (bits)	Authentication watermark	Recovery watermark	Total payload	Embedding capacity (bpp)
Proposed scheme	512 × 512	2048	64 × 32	2048	6144	0.0234
Al-Haj and amers scheme [1]	2048 × 2048	204 × 96	81 × 50	2048	25682	0.0061
Parah et al. 1st scheme [29]	512 × 512	1024	2048	0	3072	0.0117
Parah et al. 2nd scheme [29]	512 × 512	0	2209	0	2209	0.0084

Table 14 Computational complexity of matrix operation/transforms

Matrix operation/transform	Computational complexity	Matrix operation/transform	Computational complexity
1-level 2-D Haar DWT of an $x \times y$ matrix	$O_{HDWT}(4xy)$	Modification of 1-D singular vector	$O_{msv}(y)$
1-level 2-D inverse Haar DWT of an $x \times y$ matrix	$O_{IHDWT}(4xy)$	Mean of an $x \times y$ matrix	$O_{mean}(xy)$
1-level 2-D IWT of an $x \times y$ matrix	$O_{IWT}(2xy)$	Standard deviation of an $x \times y$ matrix	$O_{std}(3xy)$
1-level 2-D inverse IWT of an $x \times y$ matrix	$O_{iIWT}(2xy)$	1-D DCT of an $y \times 1$ vector	$O_{1D-DCT}(2y \log_2 y)$
SVD of an $x \times y$ matrix	$O_{SVD}(2xy^2 + 2y^3)$	1-D inverse DCT of an $y \times 1$ vector	$O_{1D-IDCT}(2y \log_2 y)$
SVD re-composition of an $x \times y$ matrix	$O_{recomp}(2min\{x, y, \}xy)$	Norm of an $y \times 1$ vector	$O_{norm}(2y)$
2-D DCT of an $x \times y$ matrix	$O_{2D-DCT}(2xy \log_2 y + 2yx \log_2 x)$	Gram-Schmidt process of an $x \times y$ matrix	$O_{GS}(2xy^2)$
2-D inverse DCT of an $x \times y$ matrix	$O_{2D-IDCT}(2xy \log_2 y + 2yx \log_2 x)$	Frobenius-norm of an $x \times y$ matrix	$2O_{Forb}(3xy)$

Table 15 Computational complexity comparison

Scheme	Asymptotic estimation	Computed Value
Bao & Ma [7]	$\{O_{HDWT}(4xy)+O_{IHDWT}(4xy)\}\|_{\substack{x=512,\\ y=512}} + (x_l \times x_k)\left\{\begin{array}{c} O_{SVD}(2xy^2+2y^3)+O_{recomp}(2min\{x,y,\}xy) \\ +O_{mean}(xy)+O_{std}(3xy)+O_{norm}(2y) \end{array}\right\}\Bigg\|_{\substack{x_l=64,x_k=64,\\ x=4,y=4}}$	4489216
Su et al. [31]	$\{O_{HDWT}(4xy)+O_{IHDWT}(4xy)\}\|_{\substack{x=512,\\ y=512}} + (x_l \times x_k)\left\{\begin{array}{c} O_{SVD}(2xy^2+2y^3)+O_{recomp}(2min\{x,y,\}xy) \\ +O_{msv}(y)+2O_{Forb}(3xy) \end{array}\right\}\Bigg\|_{\substack{x_l=64,x_k=64,\\ x=4,y=4}}$	4407296
Chang et al. [10]	$\{O_{HDWT}(4xy)+O_{IHDWT}(4xy)\}\|_{\substack{x=512,\\ y=512}} + (x_l \times x_k)\{O_{SVD}(2xy^2+2y^3)+O_{recomp}(2min\{x,y\}xy)\}\Big\|_{\substack{x_l=64,x_k=64,\\ x=4,y=4}}$	4194304
Hu & Hsu [18]	$\{O_{HDWT}(4xy)+O_{IHDWT}(4xy)\}\|_{\substack{x=512,\\ y=512}} + (x_l \times x_k)\left\{\begin{array}{c} O_{SVD}(2xy^2+2y^3)+O_{recomp}(2min\{x,y,\}xy) \\ +O_{1D-DCT}(2y\log_2 y)+O_{1D-DCT}(2y\log_2 y) \\ +O_{GS}(2xy^2)+O_{svadj}(2min\{x,y,\}xy) \end{array}\right\}\Bigg\|_{\substack{x_l=64,x_k=64,\\ x=4,y=4}}$	5373952
Patra et al. [30]	$(x_l \times x_k)\begin{array}{c} O_{2D-DCT}(2xy\log_2 y+2yx\log_2 x)+ \\ O_{2D-IDCT}(2xy\log_2 y+2yx\log_2 x) \end{array}\Bigg\|_{\substack{x_l=64,x_k=64,\\ x=8,y=8}}$	6291456
Proposed scheme	$\frac{M}{x} \times \frac{N}{y}\{O_{IWT}(2xy)+O_{iIWT}(2xy)\}\|_{\substack{M=512,N=512\\ x=8,y=8}} + 3(y_l \times y_k)\left\{\begin{array}{c} O_{SVD}(2xy^2+2y^3)+ \\ O_{recomp}(2min\{x,y,\}xy) \end{array}\right\}\Bigg\|_{\substack{y_l=64,y_k=32,\\ x=4,y=4}}$	3407872

Example:- For illustration, consider that a rectangular ROI region of size 64 × 32 be selected manually in both of the algorithms for fair comparison.

Total selected ROI bits = 64 × 32 = 2048 bits
According to Ali and Amers scheme[3]:
Cover image size = 2048 × 2048 = 4194304 pixels
Size of EPR = 204 × 96 = 19584 bits
Size of authentication watermark = 81 × 50 = 4050 bits
Selected ROI bits = 64 × 32 = 2048 bits
Total payload = 25682 bits

$$\begin{aligned} Embedding\ capacity &= \frac{(Total\ number\ of\ watermark\ bits)}{(Total\ number\ of\ pixels)} \\ &= 25682\ bits/4194304\ pixels \\ &= 0.0061\ bpp \end{aligned}$$

Thus the embedding capacity of Al-Haj and Amers scheme [1] is 0.0061 bpp.
Now, according to our proposed scheme:
Cover image size = 512 × 512 = 262144 pixels
Size of EPR = 2048 bits
Size of authentication watermark = 64 × 32 = 2048 bits
Selected ROI bits = 64 × 32 = 2048 bits
Total payload = 6144 bits

$$\begin{aligned} Embedding\ capacity &= \frac{(Total\ number\ of\ watermark\ bits)}{(Total\ number\ of\ pixels)} \\ &= 25682\ bits/4194304\ pixels \\ &= 0.0234\ bpp \end{aligned}$$

The embedding capacity of proposed scheme is 0.0234 bpp.

4.7.4 Time complexity

Time complexity of an algorithm signifies the total time taken by an algorithm to run as a function of the input size to the problem. Time complexity of the proposed scheme is compared with Bao and Ma [7], Su et al. [31], Chang et al. [10], Hu and Hsu [18] and Patra et al. [30]. Computational complexity of the transformations used popularly in the watermarking schemes is listed in Table 14. Computations involving a single element operation are not taken into account, as it is negligible in the comparison to that of matrix operations. According to the asymptotic estimates shown in Table 14, the transforms and matrix operations required for the schemes under comparison are summed up and tabulated in Table 15. The total number of operations and the sizes of input data for all the schemes under comparison is also specified in Table 15. Most of the computations of the proposed scheme are confined to a matrix of size 4 × 4, thus the overall computational requirement is alleviated. IWT is lifting based transform therefore requires half the number of computations as compared to DWT [13]. Due to these obvious reasons the proposed scheme demands relatively lesser amount of computation as compared to the schemes under comparison developed from the DWT-SVD or DCT framework.

5 Conclusion

This paper presents a new region based MIW scheme using IWT-SVD transform to address the issues of authentication, confidentiality and integrity in tele-medicine. IWT-SVD hybrid transform is applied to include the good stability of SVD and the capability of IWT to preserve a perfect reconstruction, by integer to integer mapping. It also offers high resistance against geometrical and non-geometrical attacks. Proposed scheme is blind and free from false positive problem. From the experimental analysis, it is evident that the proposed scheme has good imperceptibility and higher robustness against most of the attacks such as salt and pepper, histogram equalization, JPEG compression, average filtering and cropping.

Proposed scheme successfully detects and locates tampering with high accuracy. Also, the visual quality of recovered images is very close to the watermarked image. It is tested on gray-scale as well as color medical images and shows consistent results with different medical image modalities. Therefore, it can be applied to 8-bit depth and 24-bit depth medical images of different modalities. Comparative analysis shows that the proposed scheme outperforms the existing schemes and may find potential solution to the telemedicine applications.

Although, most of the common image processing attacks have been applied extensively to authenticate the robustness of the proposed scheme but study of robustness under other attacks included in the standard watermark benchmarking tools can be seen as future work.

References

1. Ali A-H et al (2014) Secured telemedicine using region-based watermarking with tamper localization. J Digit Imaging 27(6):737–750
2. Anusudha K, Venkateswaran N, Valarmathi J (2016) Secured medical image watermarking with dna codec. Multimed Tools Appl:1–22
3. Ansari IA, Pant M, Ahn CW (2015) Svd based fragile watermarking scheme for tamper localization and self-recovery. International Journal of Machine Learning and Cybernetics:1–15
4. Bouslimi D, Coatrieux G (2016) A crypto-watermarking system for ensuring reliability control and traceability of medical images. Signal Process Image Commun 47:160–169
5. Badshah G, Liew S-C, 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
6. Bhatnagar G, QM Jonathan WU, Raman B (2013) A new aspect in robust digital watermarking. Multimed Tools Appl 66(2):179–200
7. Bao P, Ma X (2005) Image adaptive watermarking using wavelet domain singular value decomposition. IEEE Trans Circ Syst Video Technol 15(1):96–102
8. Cox IJ, Miller ML, Bloom JA, Honsinger C (2002) Digital watermarking, vol 1558607145. Springer
9. Chang C-C, Tsai P, Lin C-C (2005) Svd-based digital image watermarking scheme. Pattern Recogn Lett 26(10):1577–1586
10. Chang C-C, Hu Y-S, Lin C-C (2007) A digital watermarking scheme based on singular value decomposition. In: Combinatorics, algorithms, probabilistic and experimental methodologies. Springer, pp 82–93
11. Davie B, Florance V, Friede A, Sheehan J, Sisk JE (2001) Bringing health-care applications to the internet. IEEE Internet Comput 5(3):42–48
12. Das S, Kundu MK (2013) Effective management of medical information through roi-lossless fragile image watermarking technique. Comput Methods Programs Biomed 111(3):662–675
13. Daubechies I, Sweldens W (1998) Factoring wavelet transforms into lifting steps. J Fourier Anal Appl 4(3):247–269
14. Guo X, Zhuang T-G (2009) A region-based lossless watermarking scheme for enhancing security of medical data. J Digit Imaging 22(1):53–64

15. Gunjal BL, Mali SN (2012) Roi based embedded watermarking of medical images for secured communication in telemedicine. Int J Comput Commun Eng 6(48):293–298
16. Hajjaji MA, Mtibaa A, Bourennane E-B (2011) A watermarking of medical image: Method based lsb. International Journal of Computer Science Issues
17. Hao-Tian Wu, Huang J, Shi Y-Q (2015) A reversible data hiding method with contrast enhancement for medical images. J Vis Commun Image Represent 31:146–153
18. Hwai-Tsu HU, Hsu L-Y (2015) Exploring dwt–svd–dct feature parameters for robust multiple watermarking against jpeg and jpeg2000 compression. Comput Electr Eng 41:52–63
19. Jeffery HKWU, Chang R-F, Chen C-J, Wang C-L, Kuo T-H, Moon WK, Chen D-R (2008) Tamper detection and recovery for medical images using near-lossless information hiding technique. J Digit Imaging 21(1):59–76
20. Jia S-L (2014) A novel blind color images watermarking based on svd. Optik-Int J Light Electron Opt 125(12):2868–2874
21. Kumar B, Anand A, Singh SP, Mohan A (2011) High capacity spread-spectrum watermarking for telemedicine applications. World Acad Sci Eng Technol 79:2011
22. Kasban H, El-Bendary MAM, Salama DH A comparative study of medical imaging techniques
23. Mousavi SM, Naghsh A, Abu-Bakar SAR (2014) Watermarking techniques used in medical images: a survey. J Digit Imaging 27(6):714–729
24. Mousavi SM, Naghsh A, Manaf AA, Abu-Bakar SAR (2016) A robust medical image watermarking against salt and pepper noise for brain mri images. Multimedia Tools and Applications:1–30
25. Memon NA, Chaudhry A, Ahmad M, Keerio ZA (2011) Hybrid watermarking of medical images for roi authentication and recovery. Int J Comput Math 88(10):2057–2071
26. Nyeem H, Boles W, Boyd C (2013) A review of medical image watermarking requirements for teleradiology. J Digit Imaging 26(2):326–343
27. Naseem MT, Qureshi M, Cheema A, Rahman A (2013) Hash based medical image authentication and recovery using chaos and residue number system. J Basic Appl Sci Res 3(6):488–495
28. Pandey R, Singh AK, Kumar B, Mohan A (2016) Iris based secure nroi multiple eye image watermarking for teleophthalmology. Multimedia Tools and Applications:1–17
29. Parah SA, Sheikh JA, Ahad F, Loan NA, Mohiuddin Bhat G (2015) Information hiding in medical images: a robust medical image watermarking system for e-healthcare. Multimedia Tools and Applications:1–35
30. Patra JC, Phua JE, Bornand C (2010) A novel dct domain crt-based watermarking scheme for image authentication surviving jpeg compression. Digit Signal Process 20(6):1597–1611
31. Qingtang SU, Niu Y, Zhao Y, Pang S, Liu X (2013) A dual color images watermarking scheme based on the optimized compensation of singular value decomposition. AEU-Int J Electron Commun 67(8):652–664
32. Solanki N, Malik SK (2014) Roi based medical image watermarking with zero distortion and enhanced security. Int J Modern Educ Comput Sci 6(10):40
33. Singh AK, Dave M, Mohan A (2015) Hybrid technique for robust and imperceptible multiple watermarking using medical images. Multimedia Tools and Applications:1–21
34. Singh AK, Dave M, Mohan A (2014) Hybrid technique for robust and imperceptible image watermarking in dwt–dct–svd domain. Nat Acad Sci Lett 37(4):351–358
35. Singh AK (2016) Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images. Multimedia Tools and Applications:1–18
36. Singh AK, Kumar B, Dave M, Mohan A (2015) Multiple watermarking on medical images using selective discrete wavelet transform coefficients. J Med Imaging Health Inf 5(3):607–614
37. Singh AK, Dave M, Mohan A (2015) Robust and secure multiple watermarking in wavelet domain. J Med Imaging Health Inf 5(2):406–414
38. Singh AK, Kumar B, Dave M, Mohan A (2015) Robust and imperceptible dual watermarking for telemedicine applications. Wirel Pers Commun 80(4):1415–1433
39. Singh AK, Dave M, Mohan A (2014) Wavelet based image watermarking: futuristic concepts in information security. Proc Nat Acad Sci India Sect A: Phys Sci 84(3):345–359
40. Thabit R, Khoo BE (2015) Medical image authentication using slt and iwt schemes. Multimedia Tools and Applications:1–24
41. Wakatani A (2002) Digital watermarking for roi medical images by using compressed signature image. In: HICSS. Proceedings of the 35th Annual Hawaii International Conference on System Sciences. IEEE, pp 2043–2048
42. Zain JM, Fauzi ARM (2006) Medical image watermarking with tamper detection and recovery. In: Engineering in Medicine and Biology Society, 2006. EMBS'06. 28th Annual International Conference of the IEEE. IEEE, pp 3270–3273

Sushila Maheshkar was born in India in 1977. She received B.E. in 2003 from Nagpur University, M.Tech in 2007 from RGPV University and Ph.D. degree in 2013 from NIT Allahabad, India. She joined Indian School of Mines, Dhanbad, India, in 2012, where she is currently Assistant Professor. Her main areas of research interest are Digital Image Processing, Digital Image Watermarking, Face Recognition and Image Forensics.

Priyanka Singh was born in India in 1980. She received Master of Computer Applications in 2005 from Magadh University and currently pursuing Ph.D. from the Department of Computer Science and Engineering, Indian School of Mines, Dhanbad, India. Her research interests includes Image processing and Digital image Watermarking.