

Received January 4, 2022, accepted January 10, 2022, date of publication January 14, 2022, date of current version January 26, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3143801

Region-Based Hybrid Medical Image Watermarking Scheme for Robust and Secured Transmission in IoMT

PRIYANKA SINGH¹, K. JYOTHSNA DEVI¹, HIREN KUMAR THAKKAR², (Member, IEEE), AND KETAN KOTECHA³

¹Department of Computer Science and Engineering, SRM University AP, Amaravati 522502, India

²Department of Computer Engineering, Marwadi University, Rajkot, Gujarat 360006, India

³Symbiosis Center for Applied Artificial Intelligence, Symbiosis International University, Pune, Maharashtra 412115, India

Corresponding authors: Ketan Kotecha (head@scaai.siu.edu.in) and Hiren Kumar Thakkar (iamhiren@gmail.com)

This work was supported by the Symbiosis International University.

ABSTRACT With the growth in Internet and digital technology, Internet of Medical Things (IoMT) and Telemedicine have become buzzwords in healthcare. A large number of medical images and information is shared through a public network in these applications. This paper proposes a region-based hybrid Medical Image Watermarking (MIW) scheme to ensure the authenticity, authorization, integrity, and confidentiality of the medical images transmitted through a public network in IoMT. In the proposed scheme, medical images are partitioned into Region of Interest (RoI) and Region of Non-Interest (RoNI). To ascertain integrity of RoI, tamper detection and recovery bits are embedded in RoI in the medical image. RoI is watermarked using adaptive Least Significant Bit (LSB) substitution with respect to the hiding capacity map for higher RoI imperceptibility and accuracy in tamper detection and recovery. Electronic Patient Record (EPR) is compressed using Huffman coding and encrypted using a pseudo-random key (secret key) to provide higher confidentiality and payload. QR code of hospital logo, Encrypted EPR, and RoI recovery bits are interleaved in RoNI using Discrete Wavelet Transform-Singular Value Decomposition (DWT-SVD) hybrid transforms to achieve a robust watermark. The proposed scheme is tested under various geometric and non-geometric attacks such as filtering, compression, rotation, salt and pepper noise and shearing. The evaluation results demonstrate that the proposed scheme has high imperceptibility, robustness, security, payload, tamper detection, and recovery accuracy under image processing attacks. Therefore, the proposed scheme can be used in the transmission of medical images and EPR in IoMT. Relevance of the proposed scheme is established by its superior performance in comparison to some of the popular existing schemes.

INDEX TERMS DWT-SVD, Internet of Medical Things (IoMT), structural saliency map, hiding capacity map, pseudo random key, medical image watermarking.

I. INTRODUCTION

In this internet era, medical images and patient information is widely transmitted through a public transmission channel in Internet of Medical Things (IoMT) applications. While sharing medical images or electronic patient record (EPR) through a public network, they can get tampered or manipulated, leading to the wrong diagnosis by the medical consultants. Similarly, one can easily claim false ownership of the medical images [1]. Confidentiality of the patient record is also a major concern. Thus, it is very important

The associate editor coordinating the review of this manuscript and approving it for publication was Ludovico Minati¹.

to ensure authenticity, authorization, integrity, and confidentiality of the information during transmission [2]. Medical Image Watermarking (MIW) is one of the most popular approaches to address these issues [3]. For diagnosis, the whole medical image is not used by the medical consultant. Therefore, a medical image can be segmented into a Region of Interest (RoI) and a region of Non-Interest (RoNI) [4]. RoI is used for diagnostic purpose, and RoNI is not important for diagnosis. It is important to ensure the integrity and higher imperceptibility for RoI. Therefore, EPR, hospital logo (or any other authentication information), and tamper detection/recovery information can be embedded as a robust and invisible watermark in RoNI. The Imperceptibility of

RoNI can be compromised to ensure higher robustness for the watermark embedded in RoNI. Watermark can be extracted from RoNI to track ownership (authenticity), tamper detection/recovery (integrity), authorization, and confidentiality of the information when it is needed [5]. Spatial, frequency or hybrid domain [6] MIW techniques can be used to insert authentication information into the host medical image. The Least Significant Bit (LSB) watermarking technique is one of the spatial domain techniques used to embed watermark by directly altering the LSB of pixels in the host image. LSB is a fragile watermark technique, so it can be used for tamper detection in RoI [7]. High imperceptibility can be achieved by adaptive LSB substitution. Frequency domain watermarking techniques show higher robustness, hence can be used to embed authentication and patient information in RoNI [8]. This paper proposes a region-based hybrid MIW scheme using hybrid domain watermark techniques for higher imperceptibility, security, tamper detection/recovery accuracy, and authentication, even under intentional/unintentional attacks. The proposed scheme ensures authenticity, authorization, integrity, and confidentiality of the medical data. The remaining sections of this paper are organized as follows: Section II analyses the related work, Section III describes the proposed scheme in detail, Section IV presents discussion on simulation results, followed by conclusion and future enhancements in Section V.

II. RELATED WORK

During the past decade, there has been a lot of research in MIW using spatial, frequency and hybrid domain techniques for the secure transmission of medical image and EPR in IoMT. Reversible MIW schemes are explored to ensure high imperceptibility and integrity of medical image [10], [13], [22], [23] using spatial domain techniques. Generally, reversible watermarking techniques (spatial domain), are imperceptible and can be used for integrity verification, but they are less robust. The schemes proposed in [10]–[13], [22], [23], [25] have high imperceptibility but are vulnerable to some image processing attacks. Hence, researchers have suggested frequency domain watermarking schemes such as SVD [17], Schur [24] and hybrid transform schemes using DWT - SVD [6], [16], [25], Redundant discrete wavelet transform (RDWT) - SVD - HT [9], DWT - Schur [11], FdCuT - DCT [14], FD - DCT [18] to achieve high imperceptibility as well as high robustness. The schemes proposed in [6], [9], [11], [12], [14]–[17], [22], [24], [25] have achieved high imperceptibility and robustness but lacks in ensuring integrity of the transmitted data. Integrity (tamper detection and recovery) is one of the important requirement for medical image transmission to ensure that the receiver has received intact medical image. To ensure integrity, schemes in [6], [10], [13], [18], [23] implemented localised tamper detection and recovery techniques. However, there is scope of improvement in the accuracy rate of tamper detection and recovery. Confidentiality and security of EPR watermark is also necessary for applications such as Telemedicine, IoMT, e-healthcare

services. In majority of existing MIW schemes, watermark security is either ignored or less focused. MIW schemes presented in [10]–[15] have less focused on watermark security. Arnold map is applied for security of the watermark in [16], [17], but it has low security. Further, schemes in [9], [24], [25], use chaotic map for watermark security. But, chaotic maps suffers from hyper tuning parameter issue. Scheme in [23] and [18] use RC4 and FD for watermark security respectively. Despite the fact that the techniques presented in [9], [18], [23] have achieved high imperceptibility, robustness, and security but has high computational cost. Digital image watermarking schemes proposed in [29]–[31], embeds tamper detection, localization and recovery information in the digital image. These schemes achieve higher imperceptibility and embedding capacity but at the cost of robustness. These schemes have achieved higher tamper detection and localization accuracy but may not be suitable for MIW, as the embedding is done in the entire image which may affect the visual quality of RoI in medical images. Region-based MIW approaches are also proposed, as they effectively use the non-diagnosis (RoNI) portion for watermark embedding without compromising the integrity of the diagnosis-relevant portion (RoI) [10], [12].

Motivation and contribution: The related work review reveals that a good amount of research has been done to securely transmit medical data through the Internet using the MIW approach. However, some challenges need to be addressed. Here, a region based hybrid MIW scheme is proposed to address the mentioned challenges. The proposed MIW scheme is motivated by Swaraja *et al.* [11], Hanan [6], Kumar & Jha [18] and its contributions are as follows:

- 1) **High EPR security and payload at low computational cost:** The proposed scheme ensures EPR security by using the compression-then-encryption approach. First, EPR is compressed by using Huffman coding. EPR compression provides security and increases the payload. Further, the compressed EPR is encrypted using a unique pseudo-random key (PRK) to make EPR highly secure. Divide-And-Conquer (DAC) and Mersenne Twister (MT) random number generator is used to generate PRK having time complexity of $O(n \log n)$. Encrypted EPR is embedded as a watermark in RoNI.
- 2) **High RoI imperceptibility:** RoI is watermarked according to the hiding capacity map (H_{map}) to ensure higher RoI imperceptibility. Tamper detection information is embedded in RoI by using adaptive LSB in the spatial domain. This approach is more secure than the conventional LSB embedding technique.
- 3) **High RoI tamper detection and recovery accuracy:** Block wise parity and authentication bit is computed for detecting and localizing RoI tampering. Parity and authentication bits are embedded in the adjacent block in a cylindrical manner. Original LSBs are embedded as a robust watermark in RoNI, further used to

recover original RoI. Tamper detection accuracy of the proposed scheme, is more than 97% for various medical images. Also, PSNR of the recovered images is more than 40dB indicating high imperceptibility of recovered images. Thus, the proposed scheme provides higher accuracy in RoI tamper detection, localization and recovery.

- 4) **Precise medical image authentication:** Generally, a hospital logo is embedded in the medical image for its authentication, but that can be easily forged. Hence, in the proposed scheme, the QR code of the hospital logo is interleaved in the medical image to avoid authentication forgery.

III. PROPOSED WORK

Here, a region-based MIW scheme is proposed to ensure authenticity, integrity, confidentiality and security of medical images with high imperceptibility and robustness. In the proposed scheme, the medical cover image (C) of size $M \times N$ is segmented into RoI (Region of Interest) and RoNI (Region of Non-Interest). After medical image segmentation, tamper detection and recovery information is embedded in RoI using adaptive LSB with respect to H_{map} . Encrypted EPR, QR code of hospital logo and RoI recovery bits (ROIRB) are embedded in RoNI using DWT-SVD. Watermarked RoI and RoNI are combined to get watermarked medical image C' . Watermarks are extracted from C' for authentication, tamper detection and recovery. EPR is also retrieved from C' . Block diagram of the proposed watermark embedding and extraction scheme (RoI and RoNI) are shown in Figure 1 and Figure 14 respectively. The proposed scheme is elucidated as follows:

A. RoI AND RoNI SEGMENTATION

RoI and RoNI can be segmented manually or with the help of automated segmentation tools [26]–[28]. However, automated segmentation tools are image modality dependent, computationally expensive and less accurate at marking RoI than manual approaches [38]. Therefore, manual segmentation of RoI (by the radiologist or physician) is considered in the proposed scheme. An irregular shape ROI is manually marked by the radiologist/physician in the medical image as shown in Figure 2 (i). Following steps are performed to mark a rectangular RoI in the proposed scheme:

- Step 1: For a $M \times N$ medical image, draw $M \times N$ grid lines (M horizontal lines and N vertical lines) to completely cover the image, where each pixel occupies one grid cell as shown in Figure 2 (ii).
- Step 2: Find the maximum RoI (marked manually) pixel point (P_1, P_2, P_3, P_4) in all four directions. P_1, P_2, P_3 and P_4 are the maximum pixel position along the top-left, top-right, bottom-right and bottom-left grid lines respectively as shown in Figure 2 (ii).
- Step 3: Finally, connect the points (P_1, P_2), (P_2, P_3), (P_3, P_4), and (P_4, P_1) to form an enclosing rectangle as shown in Figure 2 (iii), the resulting rectangular region is

the ROI of the medical cover image, and the rest of the region is the RONI.

After RoI and RONI segmentation of medical cover image, RoI embedding is done as explained in following sub-section.

B. RoI EMBEDDING AND EXTRACTION

RoI has a key role in making diagnostic decisions; thus ensuring high RoI imperceptibility and integrity is crucial. In the proposed scheme, RoI is watermarked using adaptive LSB substitution (spatial domain) for tamper detection, localization and recovery. Block-wise tamper detection and recovery bits are embedded in RoI concerning H_{map} to provide high imperceptibility and security. The following subsection explains the H_{map} generation.

1) HIDING CAPACITY MAP (H_{map}) GENERATION

The hiding capacity map represents the maximum number of bits that can be interleaved into each pixel without sacrificing imperceptibility. The proposed scheme generates H_{map} from the structural saliency map (S_{map}). According to the information theory an image can be divided into two parts i.e. novelty (innovation) and redundant parts [20]. The novelty part of an image is unaffected by any image modifications. A log or log-log spectrum can be used to extract the novelty of an image. The proposed scheme extracts the novelty part of an image using the log spectrum representation [51]–[53]. Saliency map uses the novelty part of the image, which is independent of the image, and redundant information cannot be suppressed by the coding system [20], [40]. Thus, the structural saliency map generated for the original RoI and watermarked RoI (attacked) will be identical, and subsequently H_{map} will also be identical. H_{map} generation process is presented in Algorithm 1. The pixel values in the S_{map} range from 0 to 1, indicating the nature of RoI pixel as flat to busy. In S_{map} , 0 indicates flat zone and 1 indicates busy zone. Human Visual System (HVS) is less sensitive to the changes in a busy zone than the flat zone. Therefore, the busy zone pixels have been chosen to hide the maximum amount of RoI tamper detection and recovery bits (TDRB). To achieve higher imperceptibility for RoI, only 1-bit LSB substitution is considered in flat zone where $0.25 \geq S_{map}(i, j) \geq 0$, whereas 4-bit LSB substitution done in busy zone where $1 \geq S_{map}(i, j) > 0.75$. The range of S_{map} value is divided into four continuous intervals for determining the embedding capacity of pixel as shown in Algorithm 1. Generation of H_{map} from corresponding S_{map} for RoI is explained with an example in Figure 3. The following subsection explains the RoI embedding corresponding to (H_{map}).

2) RoI EMBEDDING

In the proposed scheme, TDRB is embedded in RoI using adaptive LSB substitution using H_{map} where a maximum of 4 bits can be embedded in each pixel. First, RoI is divided into 6×6 non-overlapping blocks referred to as main block (MB),

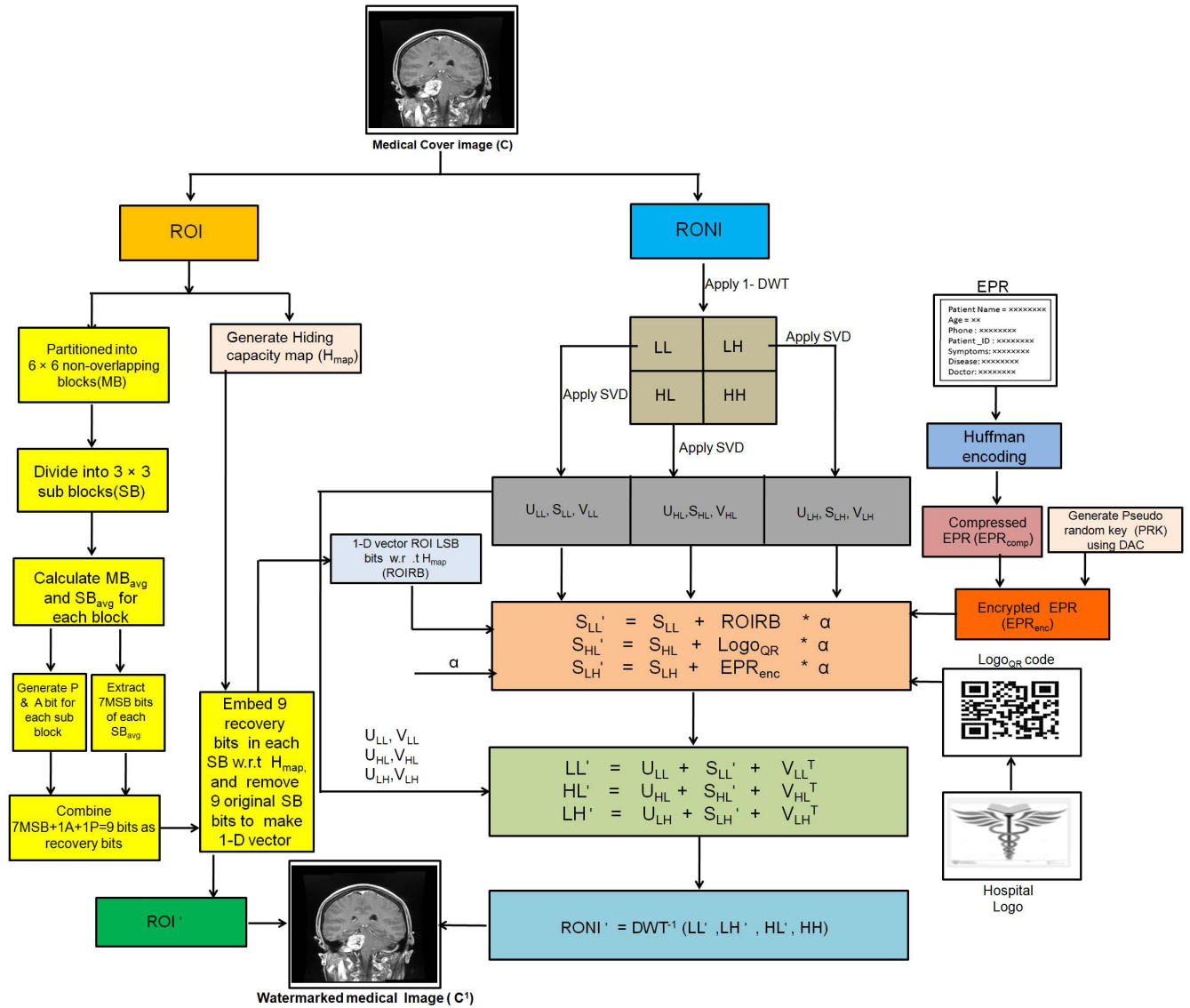


FIGURE 1. Block diagram for the proposed watermark embedding process.

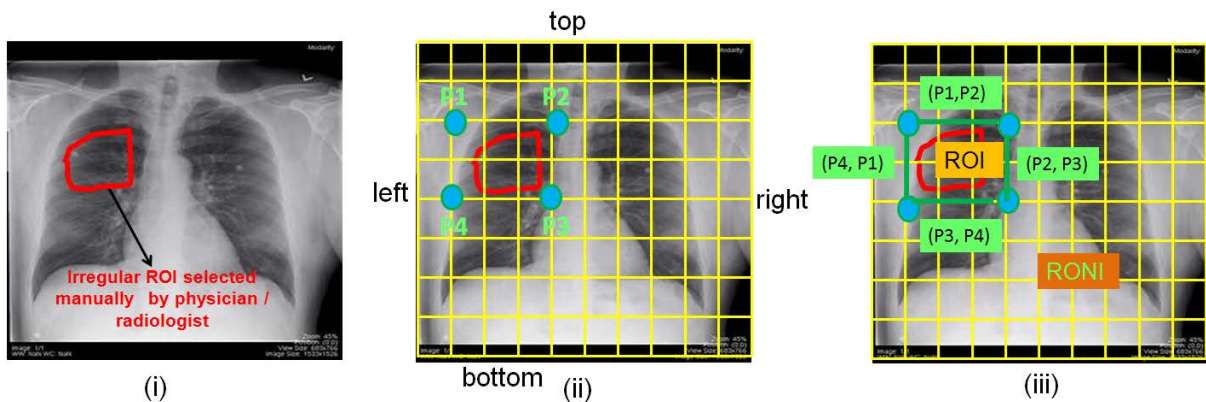


FIGURE 2. Roi and RoNI segmentation.

which is further divided into 3×3 non-overlapping called as sub blocks (SB) as shown in Figure 4.

Further, main block pixel average (MB_{avg}) and sub block pixel average (SB_{avg}) for each 6×6 block in ROI is calculated

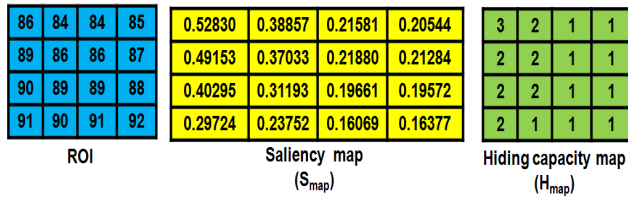


FIGURE 3. S_{map} and H_{map} Generation for RoI.

Algorithm 1 Hiding Capacity Map (H_{map}) Generation

Require: RoI

Ensure: H_{map}

- 1: Apply the FFT (Fast Fourier Transform) on the RoI.
- 2: Apply log spectra to FFT coefficients to get log-amplitude spectrum and phase angle.
- 3: Apply a median filter to the original log-amplitude spectrum to smooth it out even more.
- 4: Further subtract smoothed spectrum from the original log spectrum resulting in residuals of the spectrum.
- 5: Finally, invert the combined residuals of the spectrum and phase angle to get the S_{map} .
- 6: Use following threshold to generate H_{map} from S_{map} :

$$H_{map}(i, j) = \begin{cases} 4 & \text{if } 1.00 \geq S_{map}(i, j) > 0.75 \\ 3 & \text{if } 0.75 \geq S_{map}(i, j) > 0.50 \\ 2 & \text{if } 0.50 \geq S_{map}(i, j) > 0.25 \\ 1 & \text{if } 0.25 \geq S_{map}(i, j) \geq 0 \end{cases}$$

where i is the row and j is the column indices of H_{map} and S_{map} .

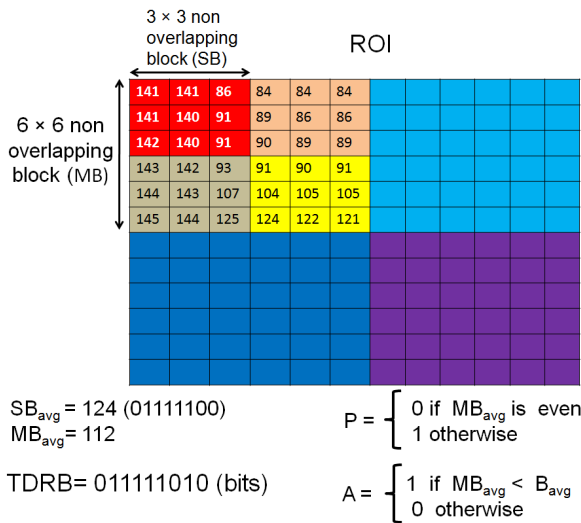


FIGURE 4. Partitioning of RoI into main block (MB) and sub block (SB), 9-bit Tamper detection and recovery bit (TDRB) vector.

using Eq. 1 and Eq. 2, respectively.

$$MB_{avg} = \left\lceil \left(\frac{\text{Sum of all the pixel values in the MB}}{\text{Total number of pixels in MB}} \right) \right\rceil \quad (1)$$

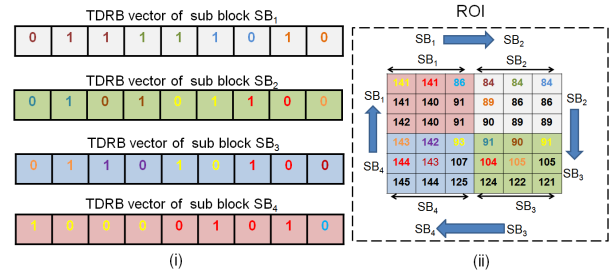


FIGURE 5. One-to-one mapping of sub block (SB) for TDRB embedding.

$$SB_{avg} = \left\lceil \left(\frac{\text{Sum of all of the pixel values in the SB}}{\text{Total number of pixels in SB}} \right) \right\rceil \quad (2)$$

For tamper detection, authentication (A) and parity (P) bits are determined for each SB from SB_{avg} and MB_{avg} using Eq. 3 and Eq. 4.

$$\text{Parity bit}(P) = \begin{cases} 0 & \text{if } MB_{avg} \text{ is even} \\ 1 & \text{otherwise} \end{cases} \quad (3)$$

$$\text{Authentication bit}(A) = \begin{cases} 1 & \text{if } MB_{avg} < SB_{avg} \\ 0 & \text{otherwise} \end{cases} \quad (4)$$

Further, 7 MSB of SB_{avg} , A and P bits are appended to form a 9-bit TDRB vector for a given SB. TDRB vector of an SB is embedded in the other SB using a one-to-one mapping process as given in Eq. 5.

$$\bar{SB}_N = [(L \times SB_N) \bmod T] + 1 \quad (5)$$

where SB_N is the N^{th} sub-block. SB is numbered in raster scan fashion and \bar{SB}_N is the mapped sub-block for a given SB_N ($N \in 1, 2, 3 \dots T$). T is the number of blocks in RoI. L is the biggest prime number between $0 - T/2$. TDRB of SB is embedded in a circular order; for, e.g. if the total number of blocks are 4, then TDRB will be embedded in a circular manner, i.e. $SB_1 \rightarrow SB_2 \rightarrow SB_3 \rightarrow SB_4 \rightarrow SB_1$ as shown in Figure 5. TDRB (9-bits) of a SB_N is embedded in \bar{SB}_N where ($N = 1, 2, 3, 4$) by using adaptive LSB substitution according to the H_{map} as shown in Figure 6 to get watermarked RoI (RoI'). Before the embedding in \bar{SB}_N , the original LSB of \bar{SB}_N (w.r.t H_{map}) are appended to a 1-D vector RIORB (RoI recovery bits). Further, RIORB is embedded in RoNI for tamper recovery at the receiver end.

3) ROI EXTRACTION

Before making any diagnostic decisions, integrity of ROI should be ensured to avoid wrong diagnosis. For this, the watermarked medical image is partitioned into ROI' and $RoNI'$ to extract integrity check watermarks for tamper detection and recovery. Firstly, H_{map} is generated for ROI' as explained in section III-B1. Authentication (A), parity (P) bit and 7 MSB are extracted for a 3×3 SB from the respective \bar{SB}_N according to H_{map} . Further, authentication (A') and parity (P') bit for each 3×3 ROI' SB is calculated using

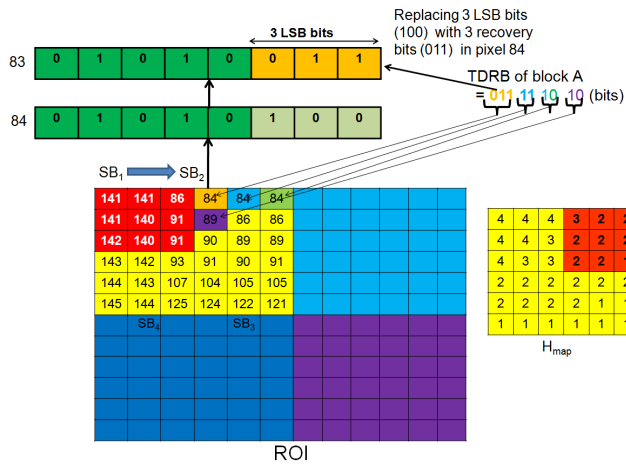


FIGURE 6. ROI Embedding (adaptive LSB substitution w.r. to H_{map}).

Eq. 1, Eq. 2, Eq. 3 and Eq. 4. To localize the tampering, for each sub block, (A') and (P') are compared with the extracted (A) and (P). If the computed and extracted authentication and parity bits are equal, then it indicates that the ROI' sub block is intact otherwise tampered. The tampered sub block is recovered by replacing 7 MSBs of all pixels of SB with the MSB extracted from mapped SB_N. And the original LSBs of the pixels are restored from ROI_{RB} extracted from RoNI' as explained in sub-section III-E2. This process is carried out for each sub block to detect, localize and recover ROI tampering. The flowchart of tamper detection and recovery is shown in Figure 7.

C. EPR ENCRYPTION AND DECRYPTION

EPR may contain patient's confidential information and must be kept secure while it is transmitted via a global communication channel. High payload is also a major requirement in smart healthcare systems such as Telemedicine, and IoMT. In the proposed scheme compression and cryptographic approach is used to achieve high security and payload for EPR. Firstly, EPR is compressed using Huffman coding and then encrypted by using pseudo random key (PRK) at the sender's side. PRK is a secret key which is shared by the certified authority/sender to the receiver of the watermarked medical image. At the receiver end, encrypted EPR is extracted from the watermarked medical image followed by decryption (using PRK received secretly) and decompression (using Huffman coding). The overall encryption and decryption process is shown as flowchart in Figure. 8. The process is explained in following subsections:

1) EPR COMPRESSION

The proposed scheme employs lossless compression technique for EPR compression, to circumvent any loss of information. There are various lossless compression techniques such as Huffman coding, LZW, RLE, bit plane coding, and arithmetic coding. Considering the computational cost and

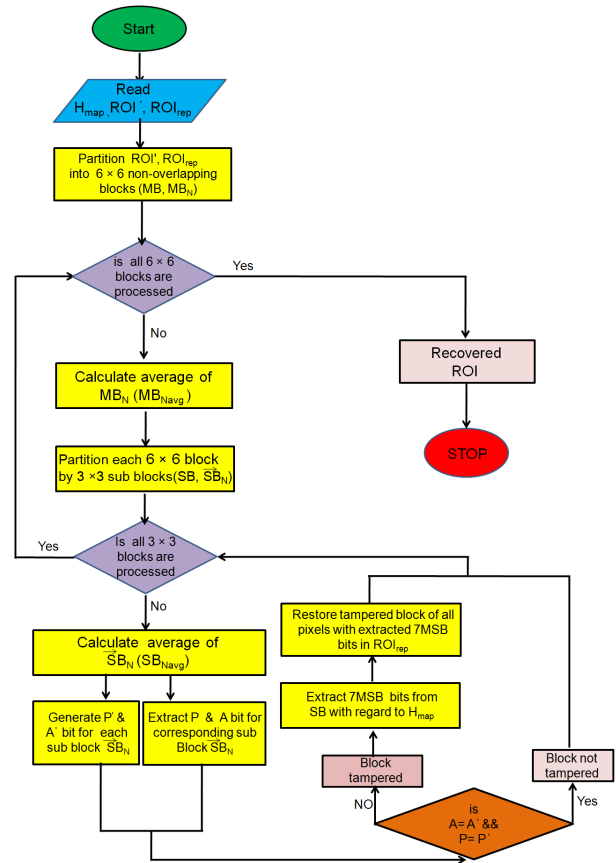


FIGURE 7. Tamper detection and recovery.

compression ratio, Huffman coding is more suitable for medical image watermarking [42]–[44]. EPR is compressed by using Huffman coding to get EPR_{comp} which is further encrypted as explained in following subsection.

2) EPR ENCRYPTION

EPR_{comp} pixels are shuffled with respect to PRK in order to obtain the encrypted EPR (EPR_{enc}) as shown in Figure 9. PRK is generated using Divide-and-Conquer (DAC) algorithm, where the data or information is recursively sub-divided into smaller problems and then combine all sub-divisions to develop a solution. The size of PRK is equal to the size of EPR_{comp}, which implies that if, the size of EPR_{comp} is N × N then the size of PRK will also be N × N. To generate PRK, a vector (V) of size N × N is considered. Another vector Z of size N × N is initialized with values from 1 to N × N. Values in Z is randomized by using DAC. A random pivot point (P) is selected and the vector Z is divided into two vectors (sub intervals) called left and right sub-vectors. The selected random position is appended to the PRK vector. This process is recursively repeated until the left and right sub-vectors are empty, as shown in Figure. 10.

To, elevate the effectiveness of the proposed encryption, pivot positions are randomly generated by using Mersenne Twister (MT) pseudo random number generator. MT can

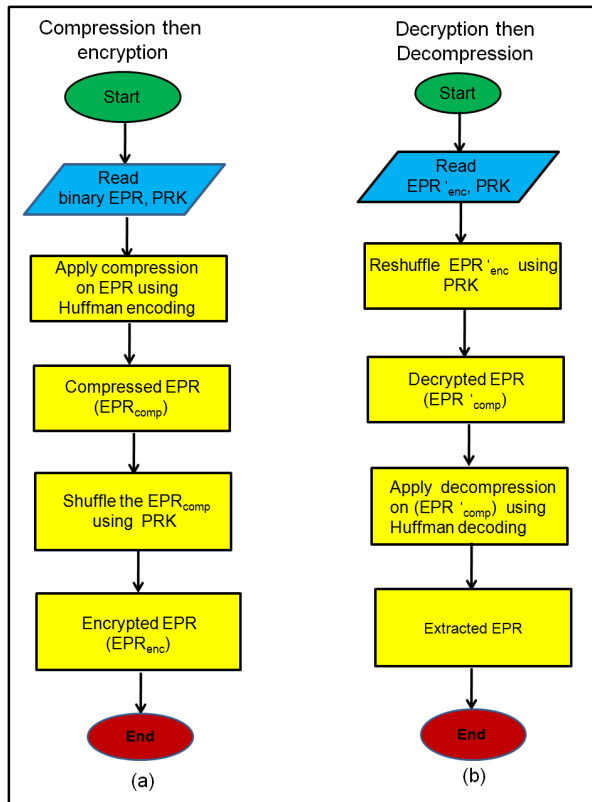


FIGURE 8. (a) Encryption process (b) Decryption Process.

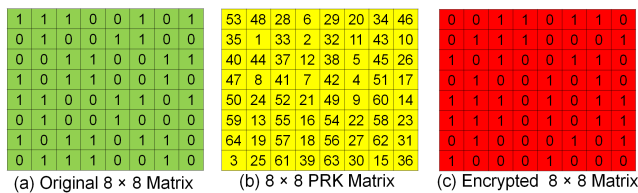


FIGURE 9. Watermark encryption using PRK.

generate longer series without repetition within a range of $[0, 2^p - 1]$, where p is the Mersenne prime of 19937 [21]. Also, MT generator takes less time to generate larger series and is approximately twenty times faster than the hardware-implemented processor-based RDRAND instruction set. The total computational cost to generation of pseudo random key in this approach is $O(n \log n)$, where n is the total size of watermark [39]. The process of PRK vector is explained with an example in Figure 11. Finally, PRK vector is converted into matrix of size $N \times N$ in a raster scan order to get PRK matrix. EPR pixel are shuffled according to the PRK matrix to obtain encrypted EPR (EPR_{enc}). The total number of different possible, PRK generated is $(M/4 \times N/4)!$. Hence, it is difficult for the attacker to guess the original key. If the watermark size is increased, the number of possible PRK also increases.

3) KEY MANAGEMENT

In the proposed scheme, a unique secret key (PRK) is generated for every pair of cover image-watermark embedding.

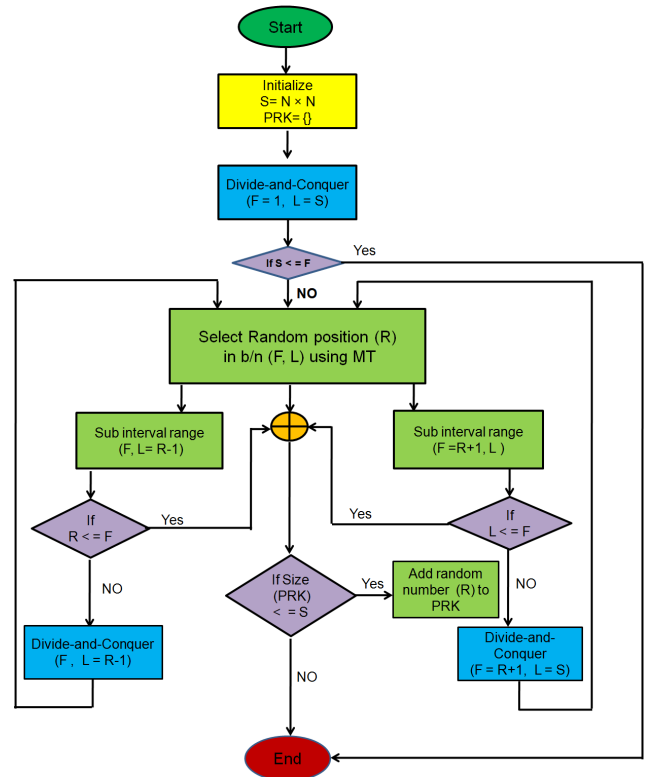


FIGURE 10. DAC for pseudo random key generation.

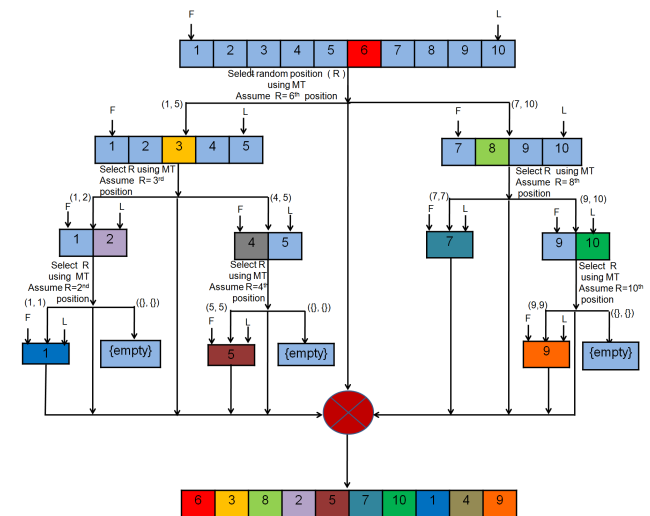


FIGURE 11. Example for Pseudo random key generation using DAC.

This approach is less vulnerable in comparison to using a common single secret key for all images. Here, for key management, the unique PRK is registered and saved with the third party or certified authority [48], responsible for sharing the key with the receiver. This also avoid attacks where the attacker embeds false watermark and generate own secret keys [49], [50].

4) EPR DECRYPTION

EPR decryption is the reverse process of watermark encryption. Encrypted EPR (EPR_{enc}) is extracted from the

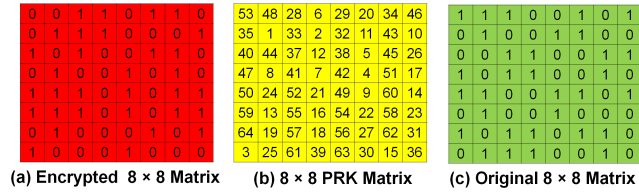


FIGURE 12. Watermark decryption with respect to pseudo random key.

watermarked medical image. EPR'_{enc} is decrypted by shuffling the pixel positions concerning PRK received secretly from the certified authority/sender. The process of decryption with respect to PRK is depicted in Figure 12. Further, decrypted EPR is decompressed by using Huffman coding to get extracted EPR.

D. QR CODE OF HOSPITAL LOGO

In the proposed scheme, QR code of hospital logo ($Logo_{QR}$) is embedded in RoNI for authentication. $Logo_{QR}$ is generated by using Zxing QR code generator available at [54]. $Logo_{QR}$ embedding avoids logo counterfeiting.

E. RoNI EMBEDDING AND EXTRACTION

The proposed scheme utilizes RoNI for robust watermark embedding by taking advantage of the fact that, RoNI is less significant in making diagnostic decisions. Three binary watermarks, i.e. QR code of hospital logo (medical image authentication information), compressed and encrypted EPR_{enc} (confidentiality), and ROIRB (tamper recovery information) are embedded in spectral-domain using DWT-SVD hybrid transform. DWT-SVD hybrid transform is proposed to achieve high robustness against the majority of attacks. DWT transform is robust to scaling, compression and filtering attacks [32], [33]. Whereas SVD transform is robust against geometrical attacks (e.g. rotation, cropping, etc.) and common image processing attacks (e.g. histogram equalization, noise addition, filtering, etc.) [34]–[37]. RoNI embedding is explained as follows:

1) RoNI EMBEDDING

For RoNI embedding, 1-level DWT is applied on RoNI, giving four sub-bands (LL, LH, HL, and HH). LL sub-band constitute image approximation. HL and LH sub-bands incorporate facet information in unique directions (horizontal, vertical). Whereas the HH sub-band consists of high-level image information, any insertions to the HH causes distortions in the cover image. Hence, to ensure high imperceptibility, LL, LH and HL sub-bands are considered for embedding. Further, LL, LH and HL sub-band are decomposed into corresponding unitary (U, V) and singular (S) matrices, i.e. LL (U_{LL}, S_{LL}, V_{LL}), LH (U_{LH}, S_{LH}, V_{LH}) and, HL (U_{HL}, S_{HL}, V_{HL}) by applying SVD. Singular matrices contains less significant image information [41], therefore, the three watermarks i.e. ROIRB, EPR_{enc} and $Logo_{QR}$ are embedded in S_{LL}, S_{LH} and S_{HL} respectively. For embed-

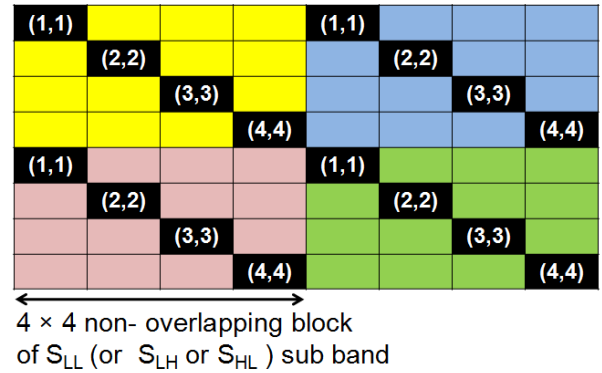


FIGURE 13. Diagonal positions in 4×4 non-overlapping block of S_{LL} or S_{LH} or S_{HL} .

ding watermarks in singular matrices, S_{LL}, S_{LH} and S_{HL} are further partitioned into 4×4 non-overlapping blocks for higher robustness and security [41] as shown in Figure 13. Watermarks are embedded in a diagonal position in S_{LL}, S_{LH} and S_{HL} using a randomly chosen scaling factor (α). Four watermark bits are inserted in each 4×4 non-overlapping block to achieve higher embedding capacity and imperceptibility. Finally, inverse SVD and DWT transform is applied to obtain watermarked RoNI ($RoNI'$). Algorithmic steps for RoNI embedding are shown in Algorithm 2. RoNI extraction is the reverse process of RoNI embedding, as explained below.

Algorithm 2 RoNI Embedding Process

Require: RoNI (R), ROIRB, $Logo_{QR}$, and EPR_{enc}

Ensure: Watermarked RoNI ($RoNI'$)

- 1: Applying 1-level DWT on R, yielding LL, LH, HL and HH subbands.
- 2: Apply SVD transform on LL, LH, HL , to further decompose them into $(U_{LL}, S_{LL}, V_{LL}), (U_{LH}, S_{LH}, V_{LH})$ and (U_{HL}, S_{HL}, V_{HL}) matrices respectively.
- 3: Divide S_{LL}, S_{LH} and S_{HL} into 4×4 non-overlapping blocks.
- 4: Select diagonal positions in 4×4 non-overlapping block for watermarks embedding. Embed ROIRB, EPR_{enc} and $Logo_{QR}$ in S_{LL1}, S_{LH} and S_{HL} respectively as shown below: $S'_{LL}(i, i) = S_{LL}(i, i) + \alpha \times ROIRB S'_{LH}(i, i) = S_{LH}(i, i) + \alpha \times EPR_{enc} S'_{HL}(i, i) = S_{HL}(i, i) + \alpha \times Logo_{QR}$ where α is watermark strengthening parameter, $i = 1, 2, 3, 4$ and S'_{LL}, S'_{LH} and S'_{HL} are watermarked singular matrix.
- 5: Apply inverse SVD followed by inverse DWT to obtain watermarked RoNI ($RoNI'$).

Watermarked RoI and RoNI are combined together to obtain watermarked medical image (C'). The proposed MIW scheme can be implemented for color medical images also. For color medical images, red, green and blue channels are extracted (using RGB color model). Changes in blue channel

induces less distortion in the image. Using this fact, watermark is inserted in blue channel by treating it as grayscale image. After embedding, watermarked blue, red and green channels are concatenated to get the watermarked color medical image.

2) RoNI EXTRACTION

For watermark extraction from RoNI, 1-level DWT is applied on the watermarked RoNI ($RoNI'$) giving 4 sub-bands (LL^1, LH^1, HL^1 , and HH^1). LL^1, LH^1 and HL^1 sub-bands are considered for extraction since, robust watermarks are embedded in LL, LH and HL sub-bands. Further, SVD decomposition is applied on HL^1 sub-bands to get corresponding unitary and singular matrices, i.e. $HL^1 (U_{HL}^1, S_{HL}^1, V_{HL}^1)$. S_{HL}^1 is partitioned into 4×4 non-overlapping blocks. QR code of hospital logo is extracted from the 4×4 non-overlapping blocks of S_{HL}^1 using following relation: $Logo_{QR}' = (S_{HL}^1(i,i) - S_{HL}(i,i)) / \alpha$ Where $i=1,2,3,4$. $S_{HL}(i,i)$ and scaling factor (α) are the side information.

QR code of hospital logo is extracted and converted into corresponding hospital logo. Extracted hospital logo is used for authentication verification. If authentication is successful then further extraction of $ROIRB'$ and EPR'_{enc} is carried out otherwise extraction process is aborted. After, successful authentication, EPR extraction and tamper detection and recovery process is carried out by applying SVD on LL^1 and LH^1 sub-bands to obtain corresponding unitary and singular matrices, i.e. $LL^1 (U_{LL}^1, S_{LL}^1, V_{LL}^1)$ and $LH^1 (U_{LH}^1, S_{LH}^1, V_{LH}^1)$. Singular matrices S_{LL}^1 and S_{LH}^1 are partitioned into 4×4 non-overlapping blocks. The two watermarks i.e. $ROIRB'$ and EPR'_{enc} are extracted from diagonal position of 4×4 non-overlapping blocks in S_{LL}^1 and S_{LH}^1 respectively using scaling factor (α) to extract two watermarks by using following equation:

$ROIRB' = S_{LL}^1(i,i) - S_{LL}(i,i) / \alpha$ $EPR'_{enc} = S_{LH}^1(i,i) - S_{LH}(i,i) / \alpha$ Further, $ROIRB'$ is used for tamper recovery to ensure integrity of RoI. EPR'_{enc} is decrypted to obtain extracted EPR. The proposed scheme is blind watermarking because the watermark can be extracted without requiring the original cover image. Algorithmic steps for RoNI extraction are shown in Algorithm 3.

IV. SIMULATION RESULTS AND DISCUSSION

Simulation has been performed to investigate the performance and relevance of the proposed scheme in the current state of the art. Simulation results and discussion is presented in this section. Grayscale and color cover images (512×512) of various modalities have been taken from OPENi [55], USC-SIPI [56], Kaggle [57], [58] and STARE [59] dataset as shown in Figure 15 and Figure 17. EPR and hospital logo images are taken as binary watermark each of size 64×64 .

A. IMPERCEPTIBILITY TEST

In telemedicine, diagnosis depends largely on the visual quality of a medical image. Thus, higher imperceptibility is one of the important requirements for MIW. Subjective

Algorithm 3 RoNI Extraction Process

Require: Watermarked RoNI ($RoNI'$), α , S_{LL} , S_{LH} , S_{HL}

Ensure: $ROIRB'$, EPR'_{enc} , hospital logo

- 1: Obtain LL^1, LH^1, HL^1 , and HH^1 subbands by applying 1-level DWT to $RoNI'$.
- 2: Apply SVD transform on HL^1 , to further decompose them into $U_{HL}^1, S_{HL}^1, V_{HL}^1$ matrices respectively.
- 3: Divide S_{HL}^1 into 4×4 non-overlapping blocks. Select diagonal positions in 4×4 non-overlapping block for $Logo_{QR}'$ extraction. Extract $Logo_{QR}'$ from S_{HL}^1 as shown below: $Logo_{QR}' = S_{HL}^1(i,i) - S_{HL}(i,i) / \alpha$ where $i=1,2,3,4$.
- 4: Convert extracted $Logo_{QR}'$ into hospital logo. Further verify authentication of extracted hospital logo. if authentication is successful goto step 5, otherwise goto step 8.
- 5: Apply SVD transform on LL^1 and LH^1 , to further decompose them into $(U_{LL}^1, S_{LL}^1, V_{LL}^1)$ and $(U_{LH}^1, S_{LH}^1, V_{LH}^1)$ matrices respectively.
- 6: Divide S_{LL}^1 and S_{LH}^1 into 4×4 non-overlapping blocks.
- 7: Select diagonal positions in 4×4 non-overlapping block for $ROIRB'$ and EPR'_{enc} extraction. Extract $ROIRB'$ and EPR'_{enc} from S_{LL}^1, S_{LH}^1 as shown below: $ROIRB' = S_{LL}^1(i,i) - S_{LL}(i,i) / \alpha$ $EPR'_{enc} = S_{LH}^1(i,i) - S_{LH}(i,i) / \alpha$ where $i=1,2,3,4$.
- 8: Abort extraction process

and objective evaluation is carried out to study the imperceptibility performance of the proposed scheme. Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index Metric (SSIM) metrics are used for objective evaluation of imperceptibility. PSNR and SSIM can be mathematically represented as in Eq. 6 and Eq. 7.

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE} \right)$$

$$\text{where, } MSE = \frac{1}{M \times M} \sum_{r=1}^M \sum_{c=1}^M [C(r, c) - C^1(c, r)]^2 \quad (6)$$

$$SSIM = [l(C, C^1)^\alpha \cdot b(C, C^1)^\beta \cdot s(C, C^1)^\gamma] \quad (7)$$

$$l(C, C^1) = \frac{2\mu_c * \mu_{c^1} + p1}{\mu_{c^2} + \mu_{c^1} + p1} \quad (8)$$

$$b(C, C^1) = \frac{2\sigma_c * \sigma_{c^1} + p2}{\sigma_{c^2} * \sigma_{c^1} + p2} \quad (9)$$

$$s(C, C^1) = \frac{\sigma_{cc^1} + p3}{\sigma_c * \sigma_{c^1} + p3} \quad (10)$$

Here, $l(C, C^1)$, $b(C, C^1)$, and $s(C, C^1)$ can be represented as Eq. 8, Eq. 9, and Eq. 10, respectively. Where C is the cover image, C^1 is the watermarked image, μ_c, μ_{c^1} is mean of C, C^1 respectively. σ_c, σ_{c^1} is the variance of C and C^1 , σ_{cc^1} is the co-variance of C and C^1 , $p1 = (x1, v)^2$, $p2 = (x2, v)^2$, $p3 = p2/2$, $x1 = 0.001$ and $x2 = 0.003$, $v = (2M - 1)$, $\alpha, \beta, \gamma = 1$ [19].

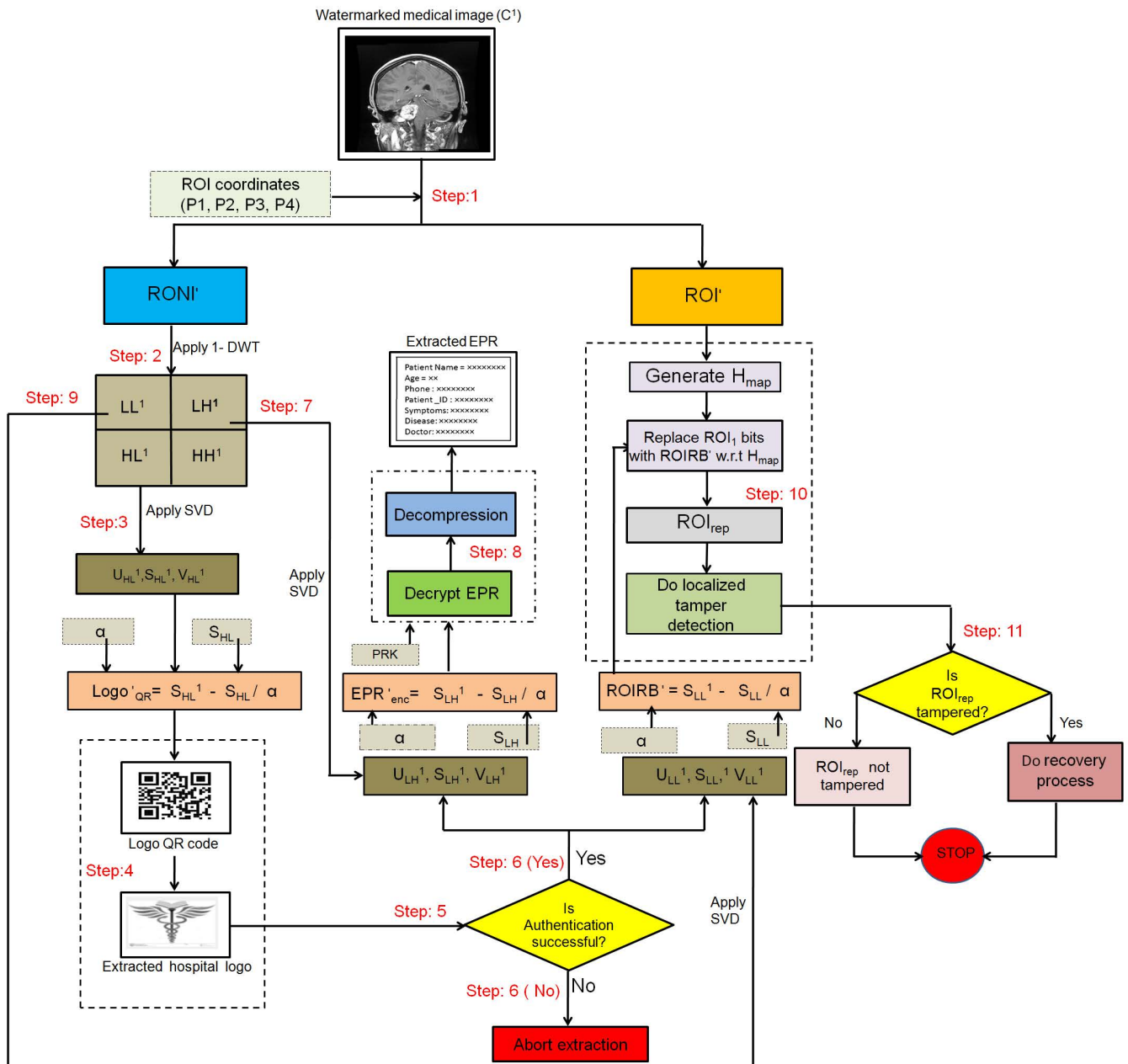


FIGURE 14. Block diagram for the proposed watermark extraction process.

Imperceptibility performance of the proposed MIW scheme is studied for different types of medical images as shown in Figure 15 and the corresponding watermarked images ($\alpha = 0.001$) and extracted watermarks (EPR and hospital logo) are shown in Figure 16. Watermarked images have no significant distortion perceived by HVS. The extracted watermarks under zero attack is distinctly visible as in Figure 16. Also, the imperceptibility performance is studied in terms of PSNR and SSIM, with different scaling factor ($\alpha = 0.001, 0.01$ and 0.1) and the results are tabulated in Table 1. It can be studied from Table 1 that the

PSNR values for all images are more than 40 dB. In general, visual quality of watermarked image is considered to be good, if $PSNR \geq 35$ dB [46], [47]. Also, there is no much variation in PSNR values with the variation in scaling factor. SSIM value is very close to the ideal value for all images modalities indicating that the proposed scheme can be used for watermarking majority of medical images. The average PSNR and SSIM values for gray-scale medical images are 45.93 dB and 0.9234 respectively for $\alpha = 0.001$. Similarly, average PSNR and SSIM values for colour medical images are 47.29 dB and 0.9503, respectively. Further, the effect

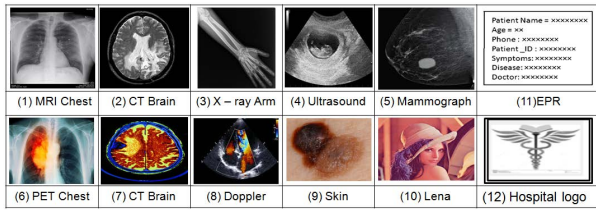


FIGURE 15. Test cover images: Gray-scale images (1-5) { MRI Chest (2) CT Brain (3) X-ray Arm (4) Ultrasound (5) Mammograph} Color images (6-10) {(6) PET Chest (7) CT Brain (8) Doppler (9) Skin (10) Lena} (11) EPR Watermark (12) Hospital Logo.

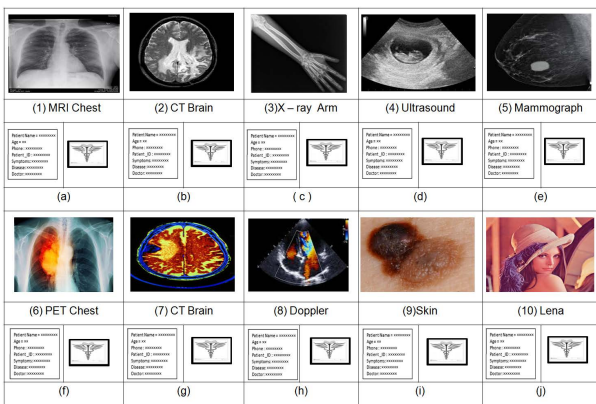


FIGURE 16. Watermarked images and corresponding extracted watermark under zero attack ($\alpha = 0.001$): Gray-scale watermarked images (1– 5), Color watermarked images (6–10), Corresponding extracted watermark image (a–j).

of variation in scaling factor on imperceptibility was also studied. PSNR and SSIM values for different scaling factor ($\alpha = 0.001, 0.01$ and 0.1) has been presented in Table 1. The average PSNR value is 45.92 dB, and the average SSIM is 0.9188 for grayscale medical images when $\alpha = 0.01$. Similarly, the average PSNR and SSIM values are 51.17 dB and 0.9708 for colour medical images. Average PSNR values for grayscale and color images are 45.95 dB and 47.42 dB respectively, whereas average SSIM for grayscale and color images are 0.9195 and 0.9505 respectively when $\alpha = 0.1$. Hence, the proposed scheme demonstrates higher imperceptibility even with the high scaling factor ($\alpha = 0.1$). From Table 1, it can be stated that there is no significant variation in PSNR and SSIM values with the increase in scaling factor.

Imperceptibility performance evaluation was further extended for five images each of brain MRI, CT scan, ultrasound, Doppler, X-ray chest, Mammograph, skin, retina, PET brain and general images as shown in Figure 17 and results are presented in Table 2. PSNR and SSIM values for all the images of different modalities shown in Table 2 are more than 35 dB indicating good visual quality of watermarked images. From Table 1 and Table 2 it can be observed that the proposed scheme has good visual quality for medical images of various modalities.

Further, subjective evaluation of imperceptibility performance is also done for the proposed MIW scheme using Mean Opinion Score (MOS) [45]. To provide MOS, watermarked images are manually compared with the original images from various angles by a set of observers (using HVS). Each observer provides a score to the watermarked image between 0 and 10. The lowest score is 0 representing the lowest visual quality and 10 representing the highest visual quality. For each watermarked image, a normalised MOS is calculated as the average score given by the observers by using Eq. 11.

$$MOS_i = \frac{1}{N_{Ob}} \sum_{j=1}^{N_{Ob}} MOS_{score}(i,j) \tag{11}$$

where MOS_i is the mean opinion score of i^{th} image, N_{Ob} is the number of observers and $MOS_{score}(i,j)$ is the score for i^{th} image given by N_{Ob}^j observer.

Twenty persons compared the visual difference between original and watermarked images and provided individual score (between 0 and 10) for each image. MOS score is calculated using Eq.11 and is tabulated in Table 1 and Table 2. MOS is greater than 9.5 for all images with variation in scaling factor, indicating higher imperceptibility is achieved by the proposed scheme. Subjective evaluation of watermarked images shows that no observable distortion is induced by the proposed MIW scheme. The proposed MIW scheme ensures higher imperceptibility for medical images of different modalities is substantiated by subjective and objective evaluation.

B. ROBUSTNESS TEST

In the proposed MIW, the authentication, authorization, patient’s record and RoI recovery information are embedded as a watermark in the medical image. Thus, higher watermark robustness becomes indispensable for MIW to facilitate correct diagnosis. Robustness of the proposed scheme has been simulated and studied under various common attacks for different scaling factors. Normalized Correlation (NC) and Bit Error Rate (BER) are taken as robustness metrics. NC represents the similarity between embedded and extracted watermarks, whereas; BER estimates the number of bits by which the embedded and extracted watermark differs. The mathematical representation for NC and BE are shown in Eq. 12 and Eq. 13 respectively.

$$NC = \frac{\sum_{r=1}^N \sum_{c=1}^N [Wt(r, c) - Wt^1(r, c)]^2}{\sqrt{\left[\sum_{r=1}^N \sum_{c=1}^N Wt(r, c)^2 \right]} \times \sqrt{\left[\sum_{r=1}^N \sum_{c=1}^N Wt^1(r, c)^2 \right]}} \tag{12}$$

where $Wt(r,c)$ and $Wt^1(r, c)$ are original and extracted watermarks.

$$BER = \frac{EB}{TB} \tag{13}$$

TABLE 1. PSNR, SSIM, MOS for gray-scale and color images ($\alpha = 0.001, \alpha = 0.01, \alpha = 0.1$).

Grayscale Image	$\alpha = 0.001$			$\alpha = 0.01$			$\alpha = 0.1$		
	PSNR	SSIM	MOS	PSNR	SSIM	MOS	PSNR	SSIM	MOS
MRI Chest	43.30	0.9247	9.86	43.30	0.9247	9.83	43.32	0.9247	9.75
CT Brain	43.23	0.9122	9.91	42.05	0.9039	9.89	43.25	0.9042	9.83
X-ray Arm	41.96	0.9138	9.83	40.89	0.8938	9.72	42.01	0.9024	9.69
Ultrasound	45.91	0.9493	9.64	45.90	0.9491	9.61	45.93	0.9492	9.58
Mammograph	55.24	0.9168	9.82	55.24	0.9168	9.79	55.26	0.9171	9.77
Average	45.93	0.9234	9.81	45.92	0.9188	9.76	45.95	0.9195	9.72
Color Image	PSNR	SSIM	MOS	PSNR	SSIM	MOS	PSNR	SSIM	MOS
PET Chest	49.31	0.9922	9.93	49.30	0.9971	9.89	49.52	0.9923	9.87
CT Brain	51.06	0.8963	9.92	55.09	0.9163	9.91	51.42	0.8966	9.89
Doppler	47.39	0.9384	9.89	47.39	0.9418	9.90	47.43	0.9388	9.87
Skin	44.95	0.9258	9.88	59.82	0.9999	9.86	44.98	0.9259	9.89
Lena	43.75	0.9989	9.79	43.74	0.9989	9.76	43.79	0.9992	9.82
Average	47.29	0.9503	9.88	51.17	0.9708	9.87	47.42	0.9505	9.86

where

$$EB = \begin{cases} counter + 1 & \text{if } \sum_{r=1}^N \sum_{c=1}^N Wt(r, c) \neq Wt^1(r, c) \\ 0 & \text{otherwise} \end{cases}$$

$$TB = N \times N$$

where EB represents incorrectly decoded bits in an extracted watermark, TB is the total number of bits and the initial value of counter=0.

Extracted watermark from watermarked medical images under zero attacks is shown in Fig. 16. As discussed earlier, from the subjective evaluation of extracted watermark from Fig. 16, it is observed that the embedded and extracted watermarks are similar. Robustness of the proposed scheme for 50 images of different modalities under zero attack when $\alpha = 0.001$ is presented in Table 2. It can be observed from Table 2 that for EPR and hospital logo, $NC \simeq 1$ and $BER \simeq 0$ i.e. close to the ideal values, for all images. This observation indicates that the proposed scheme is robust for different image modalities under zero attack when $\alpha = 0.001$. Robustness performance of the proposed scheme for different scaling factors ($\alpha = 0.001, 0.01$ and 0.1) under zero attack is also examined and NC and BER values are presented Table 3. From Table 3, it is observed that there is no significant variation in NC and BER values for the extracted EPR and hospital logo with different scaling factors. Watermarks are extracted successfully (under zero attack) with high scaling factor values.

Further, the robustness of the proposed scheme is evaluated under different attacks such as noising, filtering, compression and geometrical attacks on different medical images. NC and BER values of EPR and hospital logo, for MRI Chest, X-ray Arm and CT Brain images under different attacks are shown in Table 4. Results for MRI Chest, X-ray Arm and CT Brain images are only presented in Table 4 for ease of reference. From Table 4, it can be observed that the proposed scheme is highly robust against Gaussian filter, Weiner filter, Unmask filter, Butter Worth filter, sharpening translate, and JPEG compression (QF = 30, 50, 70 and 90) attack as NC and

BER values are close to the ideal value. Also, it shows fair robustness against Salt & Pepper noise, Median filter, shearing, rotation, translate, resize and histogram equalization as NC and BER values are more than the threshold values. It is observed from Table 4 that for all the compression, QF, NC and BER are near to the ideal value. Robustness of the proposed scheme under different attacks with the variation in scaling factor is also analyzed, and results for MRI chest image are presented in Table 5. Analysis of NC and BER values for EPR and hospital logo from Table 5 reveals that the suggested MIW scheme is robust against the most of attacks. There is no significant degradation in the robustness performance of the suggested scheme when $\alpha = 0.1$. Simulation results for different attacks affirm that the proposed scheme shows higher robustness against most attacks.

C. SECURITY KEY TEST

Confidentiality of EPR is a very important requirement for telemedicine applications. As discussed in the previous section, the original EPR is encrypted using a pseudo-random key to ensure higher confidentiality and security. The security performance of the proposed scheme has been evaluated in terms of SSIM and NC for encrypted and decrypted watermark. In Figure. 18 test binary watermark images, corresponding encrypted and decrypted image along with their SSIM and NC value has been presented. It is observed from Figure. 18 that SSIM and NC values of encrypted images are almost equal to 0, indicating that the encrypted image is very different from the original one. In contrast, SSIM and NC values of decrypted images are 1 (ideal value), indicating that the decrypted image is exactly similar to the original image. Hence, it is difficult to guess the original watermark even if the attacker is able to extract the encrypted watermark.

Further, security performance has been evaluated in terms of Correlation Coefficient (CC). The CC values (horizontal, vertical and diagonal direction) of the encrypted and decrypted image has been tabulated in Table 6. The correlation between the original watermark image and encrypted

TABLE 2. PSNR, SSIM, MOS, NC and BER (EPR and hospital logo) for 50 test cover images under zero attack taken from OPENI [55], USC-SIPI [56], Kaggle [57], [58], STARE [59] with $\alpha = 0.001$.

Image	PSNR	SSIM	MOS	EPR		Hospital logo		
				NC	BER	NC	BER	
MRI brain images	Image1	43.32	0.8646	9.85	0.9999	0	0.9999	0
	Image2	43.82	0.9496	9.59	0.9999	0	0.9998	0
	Image3	48.22	0.8755	9.72	0.9999	0	1	0
	Image4	44.49	0.8540	9.51	0.9999	0	0.9999	0
	Image5	43.54	0.9665	9.63	1	0	0.9999	0
CT Images	Image1	44.29	0.8542	9.82	0.9999	0	1	0
	Image2	39.90	0.8398	9.88	1	0	1	0
	Image3	37.44	0.8882	9.82	1	0	1	0
	Image4	38.62	0.8174	9.92	0.9999	0	0.9999	0
	Image5	38.57	0.8008	9.72	0.9998	0.0002	0.9997	0.0004
Ultrasound	Image1	37.13	0.8728	9.62	0.9999	0	0.9999	0
	Image2	38.82	0.8395	9.59	0.9999	0	0.9999	0
	Image3	38.93	0.8398	9.81	0.9999	0	1	0
	Image4	38.17	0.8926	9.79	0.9999	0	0.9999	0
	Image5	39.01	0.8455	9.83	0.9999	0	0.9999	0
Doppler	Image1	39.72	0.9683	9.72	0.9999	0	0.9998	0.0002
	Image2	40.39	0.9714	9.80	0.9999	0	0.9999	0
	Image3	40.93	0.8493	9.85	0.9999	0	1	0
	Image4	41.00	0.8762	9.73	0.9999	0	0.9999	0
	Image5	42.91	0.9934	9.74	1	0	0.9999	0
X - ray Chest	Image1	45.81	0.9884	9.86	0.9999	0	0.9999	0
	Image2	45.46	0.9889	9.84	0.9999	0	0.9999	0
	Image3	42.39	0.9884	9.92	1	0	1	0
	Image4	44.83	0.9875	9.92	1	0	1	0
	Image5	44.29	0.9862	9.91	1	0	0.9999	0
Mammograph	Image1	48.13	0.9118	9.73	1	0	1	0
	Image2	38.79	0.8908	9.71	0.9999	0	0.9999	0
	Image3	51.24	0.9789	9.74	0.9999	0	1	0
	Image4	41.62	0.9123	9.82	1	0	1	0
	Image5	47.31	0.8524	9.85	0.9999	0	0.9999	0
Skin	Image1	50.71	0.9973	9.92	0.9999	0	1	0
	Image2	61.09	0.9961	9.89	1	0	0.9999	0
	Image3	47.99	0.9980	9.87	0.9998	0.0002	0.9999	0
	Image4	55.27	0.9985	9.85	0.9999	0	0.9999	0
	Image5	50.34	0.9986	9.91	0.9999	0	0.9999	0
Retina	Image1	47.87	0.9906	9.93	1	0	0.9999	0
	Image2	54.59	0.9941	9.87	1	0	1	0
	Image3	66.56	0.9884	9.64	0.9999	0	0.9999	0
	Image4	49.45	0.9725	9.83	0.9999	0	0.9999	0
	Image5	45.92	0.9075	9.69	1	0	0.9999	0
PET Brain	Image1	38.46	0.9730	9.59	0.9997	0.0004	0.9992	0.0002
	Image2	40.47	0.8162	9.68	0.9999	0	1	0
	Image3	39.43	0.7763	9.63	0.9998	0.0002	0.9999	0
	Image4	39.37	0.9616	9.69	0.9999	0	0.9999	0
	Image5	37.93	0.7873	9.73	0.9999	0	0.9999	0
General Images	misc_4.2.03	38.00	0.9908	9.94	0.9998	0.0002	0.9998	0.0002
	misc_4.2.07	39.71	0.9840	9.93	0.9998	0.0002	0.9997	0.0004
	misc_4.1.05	45.69	0.9933	9.87	0.9999	0	0.9999	0
	misc_5.3.01	39.46	0.9732	9.83	0.9998	0.0002	0.9999	0
	Barbara	42.35	0.9788	9.91	0.9999	0	1	0
Average	43.99	0.9244	9.78	0.9999	0	0.9813	0	

watermark image is less than 0.4, and for decrypted watermark image, correlation is 1 for all test images as shown in Table 6. It further validates that the proposed scheme has very high and effective watermark security.

The sensitivity of generated PRK is also evaluated by changing bits of PRK. Even a 1-bit difference in PRK

leads to unsuccessful decryption of the encrypted watermark. Correlation between encrypted images obtained by using a generated PRK and with a 1-bit difference in the generated PRK has been computed and presented in Table 7. It is observed from Table 7 that CC values, on average, is lesser than 0.4, indicating that even a change in 1 bit will give an

TABLE 3. NC, BER for gray-scale and color images ($\alpha = 0.001, \alpha = 0.01, \alpha = 0.1$).

Grayscale Image	$\alpha = 0.001$				$\alpha = 0.01$				$\alpha = 0.1$			
	EPR		Hospital logo		EPR		Hospital logo		EPR		Hospital logo	
	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER
MRI Chest	0.9999	0	0.9999	0	0.9997	0	0.9997	0.0002	0.9917	0.0154	0.9915	0.0156
CT Brain	0.9999	0	0.9999	0	0.9996	0	0.9997	0	0.9920	0.0144	0.9923	0.0142
X-ray ARM	1	0	1	0	1	0	0.9999	0	0.9917	0.0054	0.9921	0.0051
Leg	0.9999	0	0.9999	0	0.9999	0	0.9999	0	0.9919	0.0129	0.9924	0.0125
Wrist	0.9998	0	0.9998	0.0002	1	0	0.9999	0	0.9907	0.0090	0.9909	0.0089
Average	0.9999	0	0.9999	0	0.9998	0	0.9998	0	0.9916	0.0114	0.9918	0.0112
Color Image	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER
Chest	0.9999	0	0.9998	0.0002	0.9997	0	0.9996	0.0004	0.9996	0.0006	0.9994	0.0010
Arm	0.9998	0	0.9998	0	0.9996	0.0004	0.9997	0.0004	0.9995	0.0004	0.9996	0.0008
Legs	0.9997	0	0.9997	0.0002	0.9993	0.0024	0.9994	0.0020	0.9991	0.0026	0.9992	0.0025
Forearm	0.9997	0	0.9997	0	0.9974	0.0042	0.9972	0.0043	0.9992	0.0012	0.9993	0.0011
Wrist	0.9999	0	0.9999	0	0.9997	0	0.9998	0	0.9996	0.0004	0.9995	0.0006
Average	0.9998	0	0.9998	0	0.9987	0.0014	0.9991	0.0010	0.9998	0.0010	0.9994	0.0012

TABLE 4. NC and BER values under various attacks for MRI Chest, X-ray arm and CT brain images.

Attacks	MRI Chest				X - ray Arm				CT Brain			
	EPR		Hospital logo		EPR		Hospital logo		EPR		Hospital logo	
	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER
Salt and Pepper Noise (0.002)	0.8730	0.0142	0.8729	0.0143	0.8042	0.0194	0.8040	0.0195	0.7934	0.0261	0.7942	0.0260
Median Filter (3 by 3)	0.8868	0.0415	0.8866	0.0417	0.8743	0.0321	0.8741	0.0323	0.8996	0.0195	0.9021	0.0181
Gaussian Filter (3 by 3)	0.9999	0	0.9999	0	0.9999	0	0.9999	0	0.9999	0	0.9999	0
Weiner Filter (3 by 3)	0.9553	0.0149	0.9555	0.0148	0.9472	0.0241	0.9473	0.0240	0.9343	0.0159	0.9391	0.0151
Unmask Filter	0.9676	0.1738	0.9679	0.1737	0.9521	0.1942	0.9520	0.1944	0.9534	0.1943	0.9521	0.2013
Butter worth Filter (3 by 3)	0.9999	0	0.9999	0	0.9999	0	0.9999	0	0.9999	0	0.9999	0
Sharpening	0.9745	0.1241	0.9744	0.1242	0.9625	0.0978	0.9626	0.0976	0.9689	0.0893	0.9683	0.0895
Shear (x-shear)	0.8294	0.0284	0.8301	0.0282	0.8832	0.0265	0.8840	0.0261	0.8983	0.0241	0.9021	0.0136
Rotation (10)	0.8496	0.0284	0.8499	0.0283	0.8721	0.0214	0.8729	0.0211	0.8542	0.0274	0.8619	0.0192
Translate	0.9040	0.0149	0.9041	0.0148	0.8831	0.0231	0.8891	0.0226	0.8963	0.0342	0.8952	0.0302
Resize (320 320)	0.8321	0.0198	0.8328	0.0196	0.8986	0.0141	0.8971	0.0201	0.8632	0.0185	0.8595	0.0203
Histogram equalization	0.8881	0.0159	0.8882	0.0157	0.8943	0.0131	0.8937	0.0182	0.9004	0.0142	0.9006	0.0141
JPEG compression (QF=90)	0.9974	0.0034	0.9982	0.0034	0.9983	0.0023	0.9986	0.0021	0.9982	0.0019	0.9988	0.0017
JPEG compression (QF=70)	0.9927	0.0103	0.9939	0.0101	0.9932	0.0101	0.9941	0.0114	0.9943	0.0105	0.9939	0.0113
JPEG compression (QF=50)	0.9918	0.0137	0.9926	0.0132	0.9782	0.0189	0.9792	0.0172	0.9689	0.0215	0.9682	0.0216
JPEG compression (QF=30)	0.9614	0.0173	0.9651	0.0163	0.9598	0.0182	0.9596	0.0181	0.9498	0.1023	0.9491	0.1082

TABLE 5. NC and BER values under various attacks with different α for MRI Chest.

Attacks	0.001				0.01				0.1			
	EPR		Hospital logo		EPR		Hospital logo		EPR		Hospital logo	
	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER
Salt and Pepper Noise (0.002)	0.8730	0.0142	0.8729	0.0143	0.8724	0.0140	0.8802	0.0102	0.8125	0.0182	0.8121	0.0180
Median Filter (3 by 3)	0.8868	0.0415	0.8866	0.0417	0.8864	0.0420	0.8892	0.0403	0.8859	0.0426	0.8892	0.0417
Gaussian Filter (3 by 3)	0.9999	0	0.9999	0	0.9999	0	0.9999	0	0.9999	0	0.9999	0
Weiner Filter (3 by 3)	0.9553	0.0149	0.9555	0.0148	0.9551	0.0153	0.9531	0.0192	0.9544	0.0246	0.9541	0.0241
Unmask Filter	0.9676	0.1738	0.9679	0.1737	0.9672	0.1742	0.9696	0.1691	0.9668	0.1725	0.9662	0.1720
Butter worth Filter (3 by 3)	0.9999	0	0.9999	0	0.9999	0	0.9999	0	0.9999	0	0.9999	0
Sharpening	0.9745	0.1242	0.9744	0.1242	0.9741	0.0284	0.9743	0.0283	0.9738	0.0288	0.9735	0.0287
Shear (x-shear)	0.8294	0.0284	0.8301	0.0282	0.8291	0.0288	0.8282	0.0287	0.8283	0.0319	0.8280	0.0316
Rotation (10)	0.8496	0.0284	0.8499	0.0283	0.8493	0.0288	0.8501	0.0272	0.8488	0.0293	0.8501	0.0281
Translate	0.9040	0.0149	0.9041	0.0148	0.9037	0.0153	0.9035	0.0152	0.9025	0.0264	0.9022	0.0263
Resize (320 320)	0.8321	0.0198	0.8328	0.0196	0.8318	0.0193	0.8302	0.0223	0.8312	0.0184	0.8309	0.0181
Histogram equalization	0.8881	0.0159	0.8882	0.0157	0.8874	0.0166	0.8872	0.0165	0.8861	0.0241	0.8857	0.0239

entirely different encrypted image. Also, if there is even a single bit change in the pseudo-random key, decryption is unsuccessful. In Figure 19, it is seen that with the correct

pseudo-random key, an exact watermark can be obtained by decryption indicated by subjective and objective evaluation as SSIM and NC is 1 for all test watermark images. Whereas

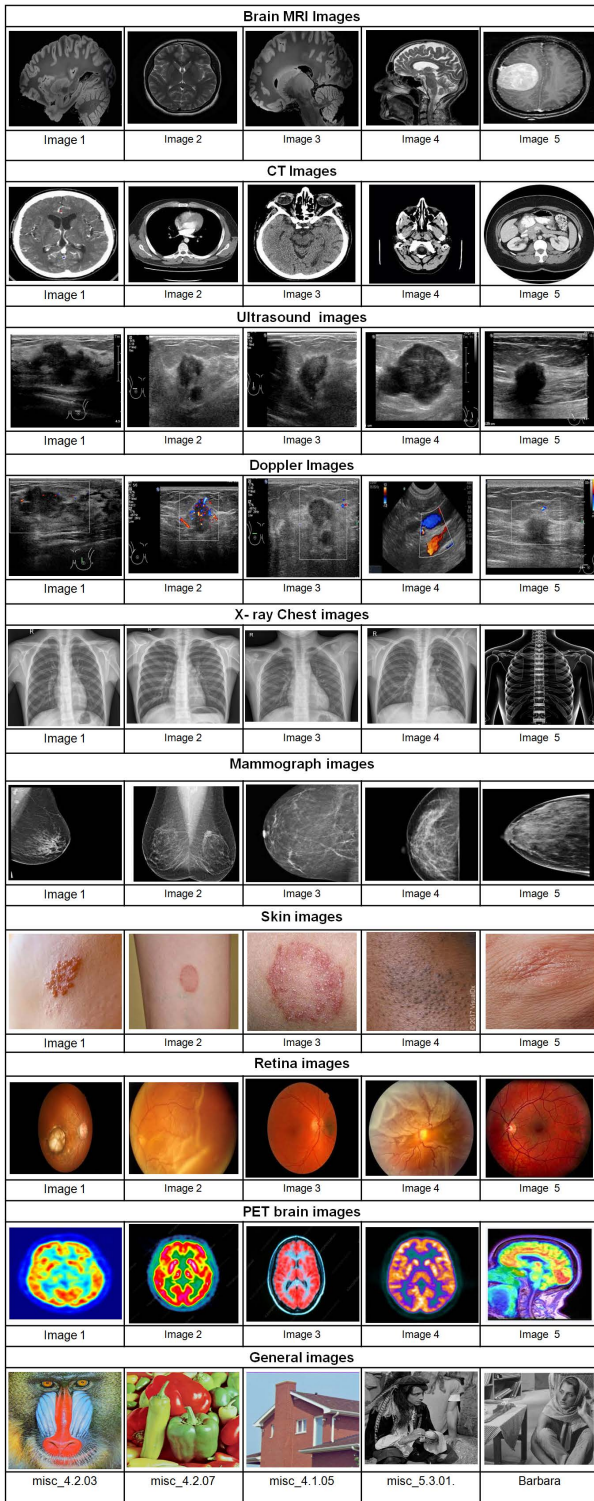


FIGURE 17. 50 Medical cover images (brain MRI, CT scan, ultrasound, Doppler, X-ray chest, Mammograph, skin, retina, PET brain and general images) taken from OPENI [55], USC-SIPI [56], Kaggle [57], [58] and STARE [59].

decryption is unsuccessful even if there is a variation of 1 bit in pseudo-random key as indicated by SSIM and NC values almost equal to 0 as in Figure 19.

Original	Encrypted	Decrypted
<p>Patient Name = xxxxxxxx Age = xx Phone : xxxxxxxx Patient_ID : xxxxxxxx Symptoms: xxxxxxxx Disease: xxxxxxxx Doctor: xxxxxxxx</p>	<p>SSIM=0.0003 NC = 0.0002</p>	<p>Patient Name = xxxxxxxx Age = xx Phone : xxxxxxxx Patient_ID : xxxxxxxx Symptoms: xxxxxxxx Disease: xxxxxxxx Doctor: xxxxxxxx</p> <p>SSIM = 1 NC=1</p>
<p>MRI Chest</p>	<p>SSIM=0.0002 NC = 0.0003</p>	<p>SSIM = 1 NC=1</p>
<p>Lena</p>	<p>SSIM=0.0006 NC = 0.0001</p>	<p>SSIM = 1 NC=1</p>

FIGURE 18. SSIM and NC values for encrypted and decrypted EPR, binary images (MRI chest and Lena.)

TABLE 6. Correlation Coefficient (CC) of encrypted and decrypted EPR and binary image using CC (H- Horizontal, V-Vertical, D-Diagonal.)

Test Images (binary)	CC of original and encrypted images			CC of original and decrypted images		
	H	V	D	H	V	D
EPR	0.0620	0.2308	0.2731	1	1	1
X-Ray Arm	0.1877	0.2409	0.1911	1	1	1
MRI Chest	0.3910	0.4159	0.4251	1	1	1
Ultrasound	0.3926	0.4625	0.4237	1	1	1
Skin	0.3300	0.4290	0.4876	1	1	1
Lena	0.3607	0.3950	0.3801	1	1	1

TABLE 7. Security test of encrypted watermark using CC with one bit differ in key.

Test Images (binary)	Correlation of two encrypted images		
	Horizontal	Vertical	Diagonal
EPR	0.2083	0.2427	0.2467
MRI Chest	0.4392	0.4571	0.4603
Skin	0.3441	0.2901	0.3133
X-ray Arm	0.3794	0.3791	0.3406
Lena	0.4706	0.4325	0.3899
Ultrasound	0.4051	0.4595	0.4273

Further, the security performance of the proposed scheme has been tested using differential measures like Number of Pixel Changing Rate (NPCR), Unified Averaged Changed Intensity (UACI). NPCR and UACI can be mathematically expressed as follows:

$$NPCR(EI^1, EI^2) = \sum_{r=1}^N \sum_{c=1}^N \frac{DI(r, c)}{TP} \times 100\%$$

$$DI(r, c) = \begin{cases} 0 & \text{if } EI^1(r, c) = EI^2(r, c) \\ 1 & \text{if } EI^1(r, c) \neq EI^2(r, c) \end{cases}$$

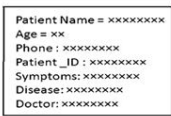








Original	Decrypted using same key	Decrypted using 1 bit differ in key
 <p>Patient Name = xxxxxxxx Age = xx Phone : xxxxxxxx Patient_ID : xxxxxxxx Symptoms: xxxxxxxx Disease: xxxxxxxx Doctor: xxxxxxxx</p> <p>EPR</p>	 <p>Patient Name = xxxxxxxx Age = xx Phone : xxxxxxxx Patient_ID : xxxxxxxx Symptoms: xxxxxxxx Disease: xxxxxxxx Doctor: xxxxxxxx</p> <p>SSIM = 1 NC=1</p>	 <p>SSIM = 0.0025 NC = 0.0387</p>
 <p>MRI Chest</p>	 <p>SSIM = 1 NC=1</p>	 <p>SSIM = 0.0068 NC = 0.0512</p>
 <p>Lena</p>	 <p>SSIM = 1 NC=1</p>	 <p>SSIM = 0.0081 NC = 0.1865</p>

FIGURE 19. Performance of secret key with 1 bit differ in key interms of robustness.

TABLE 8. Performance of NPCR(%) and UACI(%) tests.

Image	NPCR%	UACI%
EPR	96.85	32.98
MRI Chest	97.01	31.24
CT Brain	97.03	33.67
X-ray Arm	96.23	31.90
Lena	95.92	31.23
Average	96.61	32.20

$$UACI(EI^1, EI^2) = \sum_{r=1}^N \sum_{c=1}^N \frac{|EI^1 - EI^2|}{LF * TP} \times 100\%$$

where EI^1, EI^2 are cipher images with one bit difference in PRK. TP is the total number of pixels in encrypted image, and FP is the highest supported pixel value(for grayscale images, it is 255).

NPCR and UACI for the proposed scheme are shown in Table 8. For five test images, the average NPCR value is 96.61, and the UACI value is 32.30, nearly equal to the ideal value. Hence, it concluded that the proposed random key approach is highly secure.

D. TAMPER DETECTION AND RECOVERY

The integrity of the medical images, especially for RoI, is very important for correct diagnosis. The effectiveness of the proposed scheme in tamper detection and recovery has been examined. Copy-paste tampering has been applied on 10% of the watermarked image (considering it as RoI). Figure 20 shows the original watermarked images; copy-paste tampered image, tamper detected region and the recovered image. Similarly, Figure 21. shows the original watermarked images, erase tampered images, tamper detected region and the recovered image. It can be observed from Figure 20, and

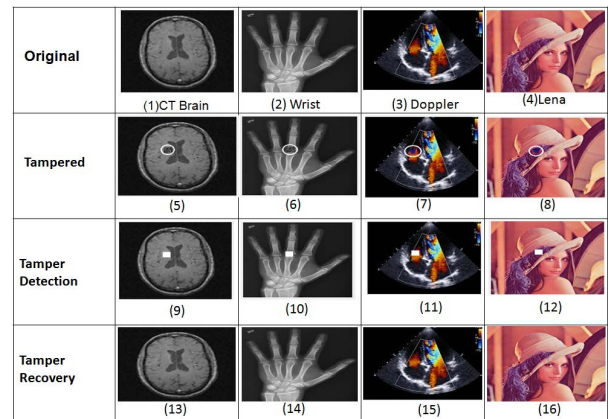


FIGURE 20. Original watermarked images (1-4), Copy-paste tampered images (5 - 8), Tamper detected area marked with white pixels (9 - 12), Recovered images (13 - 16).

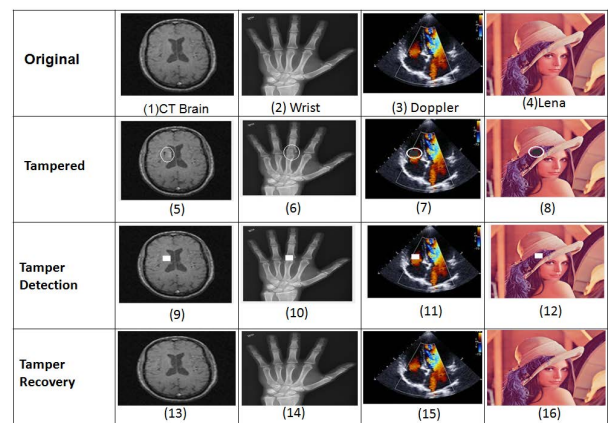


FIGURE 21. Original watermarked images from (1 - 4), Erase tampered images(5 - 8), Tamper detected images (9-12), Recovered images (13 - 16).

TABLE 9. Recovered images tamper detection accuracy rate (%) and PSNR.

Grayscale Image	PSNR	Accuracy	Color Image	PSNR	Accuracy
MRI Chest	42.92	98.32	PET Chest	48.63	97.82
CT Brain	41.56	97.97	CT Brain	49.72	97.82
X-ray Arm	40.05	97.67	Doppler	46.21	97.45
Ultrasound	44.48	98.02	Skin	43.05	98.01
Mammograph	53.96	97.13	Lena	41.31	97.43

Figure 21 that the tampered area is accurately detected, localized and recovered. The effectiveness of tamper detection and recovery of the proposed scheme has been measured in terms of accuracy rate and PSNR, respectively, and the results are shown in Table 9. The tamper detection accuracy rate is more than 97%. PSNR of the watermarked and recovered image with respect to the original image is almost equal indicating high visual quality of recovered images. Hence, it is claimed that the proposed scheme can detect and recover tampering for different image modalities.

TABLE 10. Compression ratio, saving % using LZW, RLE and Huffman coding for different size of watermark (in pixels).

Size	Compression ratio			Saving %		
	LZW	RLE	Huffman	LZW	RLE	Huffman
250 × 250	2.90	3.09	3.59	65.57	67.73	72.20
128 × 128	2.25	1.95	2.78	55.64	48.82	64.06
64 × 64	3.50	3.16	4.14	71.45	68.40	75.92

TABLE 11. Computational cost of the major expensive steps in the proposed scheme.

Operations	Computational cost
H_{map} Generation	$\mathcal{O}(\log M) + \mathcal{O}(M \log M) + \mathcal{O}(MN)$ $= \mathcal{O}(MN)$
EPR Encryption	$\mathcal{O}(X \log X)$
EPR Compression/decompression	$\mathcal{O}(X \log X)$
1-level 2D DWT	$\mathcal{O}(2MN)$
1-level 2D inverse DWT	$\mathcal{O}(2MN)$
SVD Decomposition	$\mathcal{O}(2MN^2 + 2N^3)$
SVD Re-composition	$\mathcal{O}(2 \min [M, N] MN)$

E. COMPRESSION PERFORMANCE TEST

In the proposed scheme, Huffman coding is used for EPR compression. Compression ratio and saving% is calculated using equations Eq. 14 and Eq. 15 respectively, for LZW, RLE, and Huffman coding and presented in Table 10.

$$\text{Compression ratio} = \frac{S_{uc}}{S_c} \tag{14}$$

$$\text{Saving\%} = \left(1 - \frac{S_c}{S_{uc}}\right) \times 100 \tag{15}$$

where S_{uc} and S_c are EPR before and after compression respectively.

Compression ratio and saving% of commonly used lossless compression technique i.e. LZW, RLE and Huffman coding is computed and compared in Table 10 to study the effectiveness of Huffman coding for EPR compression in the proposed scheme. From Table 10, it can be studied that Huffman coding reduces more number of pixels as compared to LZW and RLE. Compression ratio and saving% of Huffman coding is higher for all the three test cases. This observation supports the effectiveness of Huffman coding for EPR compression.

F. COMPUTATIONAL COST

In this section the computational cost of the proposed scheme is analysed. For a medical cover image ($M \times N$) and EPR ($X \times X$), the computational cost (Γ) of major expensive steps involved, are shown in Table 11. Considering only expensive steps, the computational cost of the proposed scheme is calculated as follows:

$$\begin{aligned} \Gamma &= \mathcal{O}(MN) + \mathcal{O}(X \log X) + \mathcal{O}(2MN) + \mathcal{O}(2MN) \\ &\quad + \mathcal{O}(2MN^2 + 2N^3) + \mathcal{O}(2 \min[M, N] MN) \\ &= \mathcal{O}(MN^2) \end{aligned} \tag{16}$$

The computational cost of the proposed MIW scheme is $\mathcal{O}(MN^2)$ as shown in Eq. 16. The proposed EPR encryp-

TABLE 12. Encryption and decryption time in seconds.

Binary image	Encryption time (seconds)	Decryption time (seconds)
EPR	0.030719	0.009780
MRI Chest	0.026908	0.009671
Lena	0.028732	0.009746

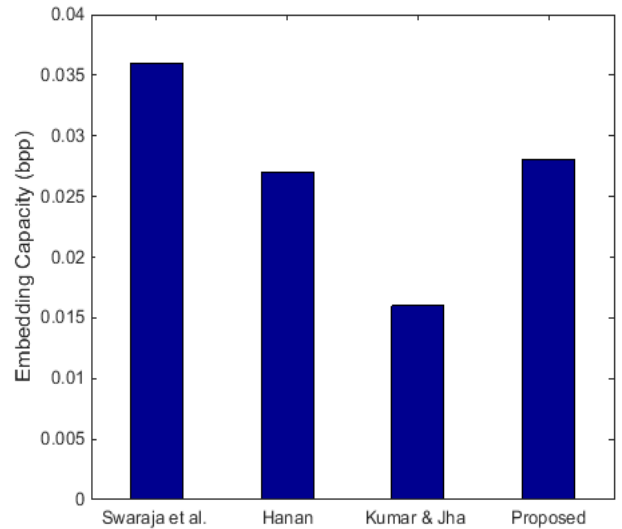


FIGURE 22. Performance comparison of embedding capacity of proposed scheme against Swaraja et al. [11], Hanan. [6] and Kumar & Jha. [18] schemes.

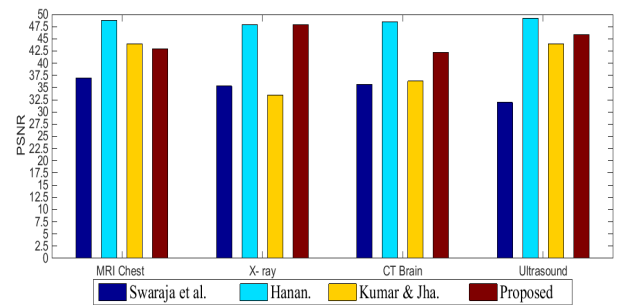


FIGURE 23. Performance comparison of imperceptibility of proposed scheme against Swaraja et al. [11], Hanan et al. [6] and Kumar et al. [18] schemes.

tion and decryption scheme has low computational cost of $\mathcal{O}(X \log X)$ and $\mathcal{O}(X \log X)$. Run-time of the proposed EPR encryption and decryption was studied using an Intel i5 processor, 2.00 GHz, 4 GB RAM and tabulated in Table 12. It can be observed that encryption and decryption time is quite low, nearly 0.03s and 0.01s respectively for all test cases. Also, the run-time for watermark embedding in grayscale and color images are less than 0.16s and 0.5s respectively. Similarly extraction time for grayscale and color image is nearly 0.09s and 0.13s respectively as shown in Table 13. From the analysis, it is observed that the proposed scheme has acceptable computational cost.

TABLE 13. Watermark embedding and extraction time of the proposed scheme.

Grayscale Image	Embedding Time (Seconds)	Extraction Time (Seconds)	Color Image	Embedding Time (Seconds)	Extraction Time (Seconds)
MRI Chest	0.141457	0.087668	PET Chest	0.441881	0.131850
CT Brain	0.132324	0.087665	CT Brain	0.439738	0.131127
X-ray Arm	0.131535	0.096715	Doppler	0.446561	0.124672
Ultrasound	0.130669	0.085257	Skin	0.435533	0.132074
Mammograph	0.156970	0.088384	Lena	0.492796	0.129381

TABLE 14. Comparison analysis of proposed scheme with state of art techniques.

Specifications	Swaraja <i>et al.</i> [11]	Hanan [6]	Kumar & Jha [18]	Proposed
Environment	Blind	Blind	Blind	Blind
Embedding Domain	DWT + Schur	DWT + SVD	DCT	DWT +SVD
Authentication	Yes	Yes	No	Yes
Tamper detection	Yes	Yes	No	Yes
Security	Low	Low	Low	High
Embedding capacity(bpp)	0.036	0.027	0.016	0.028

TABLE 15. Performance comparison of proposed scheme with respect to Swaraja *et al.* [11], Hanan. [6] and Kumar & Jha [18].

Scheme	MRI Chest		X-ray		CT Brain		Ultrasound	
	PSNR	NC	PSNR	NC	PSNR	NC	PSNR	NC
Swaraj <i>et al.</i> [11]	36.99	1	35.33	0.96	35.18	0.97	34.83	1
Hanan.[6]	48.37	0.92	47.93	0.88	48.52	0.88	49.19	0.80
Kumar & Jha. [18]	44.00	0.95	33.47	0.99	36.35	0.93	43.99	0.99
Proposed	43.30	0.99	41.96	1	43.23	0.99	45.91	0.99

G. COMPARATIVE ANALYSIS

To further establish the relevance of the proposed scheme in the current state of the art, a comparative analysis of the proposed schemes is done with some of the recent and popular MIW schemes proposed by Swaraja *et al.* [11], Hanan [6], and Kumar & Jha [18]. Swaraja *et al.* [11] have proposed a blind MIW using DWT+ Schur and PSBFO optimization. They have used LZW compression to achieve high embedding capacity and security. Hanan [6] has also proposed a blind MIW scheme using DWT+SVD and LZW compression. Whereas Kumar & Jha [18] have used DCT and fractional differentiator (FD) in their blind MIW scheme. The overview of the schemes in comparison is shown in Table 14. It is observed from Table 14 that the scheme proposed in [18] has not taken authentication and tamper detection into account, which is very important in MIW. Security of the proposed scheme is higher as than [6], [11], [18] which is further discussed in detail in this section. Embedding capacity is also higher than [6], [18] as shown in Figure 22. Comparison of imperceptibility and robustness under zero attack for different medical images, i.e. MRI Chest, X-ray and CT Brain and Ultrasound, is presented in Table 15. It can be observed from Table 15 that the PSNR values of the proposed scheme are higher than Swaraja *et al.* [11] and Kumar & Jha [18] schemes, but lower than Hanan [6] scheme. It is also observed from Figure 23. Table 15 shows that the proposed scheme has a higher NC value than other schemes in comparison.

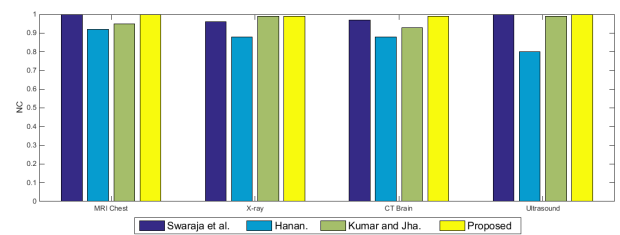


FIGURE 24. Performance comparison of robustness under zero attack of proposed scheme against Swaraja *et al.* [11], Hanan [6] and Kumar & Jha [18] schemes.

Comparison of NC value for all schemes has also been shown in Figure 24. From this observation, it is concluded that the proposed scheme has higher robustness and imperceptibility for different image modalities than its counterparts. Hanan [6] scheme has higher imperceptibility than the proposed scheme but under performs in terms of robustness.

The robustness of the proposed scheme is compared with the schemes under comparison for various attacks on the X-ray image and shown in Table 16. The proposed scheme has higher robustness than schemes in [6], [11], [18] under JPEG compression, Gaussian filtering and Weiner filtering. From Table 16, it is observed that the performance of the proposed scheme under the median filter is at par with its counterparts. The proposed scheme can resist salt & pepper noise and shearing attacks as the NC values are 0.87 and 0.89,

TABLE 16. Robustness comparison (NC) for [6], [11], [18] and the proposed scheme under different attacks.

Attacks	Swaraja et al. [11]	Hanan [6]	Kumar & Jha [18]	Proposed
JPEG compression	0.99	0.90	0.98	0.99
Salt & Pepper	0.98	0.79	0.82	0.87
Shearing	0.92	0.90	0.98	0.89
Gaussian Filter	0.89	0.91	0.99	1
Median Filter	0.88	0.91	0.87	0.89
Weiner Filter	0.90	0.80	0.86	0.95

respectively, more than the threshold value but lagging behind the schemes in comparison, which can be seen as the scope of improvement in future work.

Further, the security of the proposed scheme is compared with related schemes in comparison. Swaraja *et al.* [11], and Hanan. [6] have used LZW (Lempel–Ziv–Welch) compression algorithm for watermark compression and confidentiality. Generally, compression is used to reduce file size and increase the data transfer rate through the internet. Compression techniques do not meet security parameters such as secret, authentication, integrity and non-rejection. In addition to that, LZW compression approach has some limitations, such as high computational latency, dictionary overhead. Hence, watermark security and confidentiality in the schemes proposed in [6], [11] is limited. Kumar & Jha. [18] proposed a cryptography based secure scheme. Here the pseudo-random key is generated using DSSS (Direct Spread Spectrum Sequence) with an initial seed value. Based on this seed value entire key sequence is generated, this is the bottleneck of Kumar & Jha. [18], and it is quite easy for the attacker to break the sequence. Cryptography approaches are good for security, that prevent data from tapping. In the proposed scheme, security is achieved by a cryptography approach using mathematical theory and algorithms to generate the pseudo-random key. It is difficult for attackers to guess the PRK generated by the proposed scheme. This discussion asserts that the proposed MIW scheme is more secure than the counterpart schemes.

Comparative analysis shows that the proposed scheme has higher imperceptibility for gray-scales and colour medical images than its counterparts. The proposed scheme has higher / similar robustness against common attacks. The security of the proposed scheme is very high as compared to other schemes. Also, the proposed scheme surpasses other schemes in terms of tamper detection and recovery accuracy. Hence, from simulation results and comparative analysis, it is claimed that the proposed scheme has superior performance to the existing schemes.

V. CONCLUSION

In this study, a MIW scheme is proposed to facilitate medical image and EPR communication in IoMT. The RoI recovery bits, encrypted EPR and hospital logo QR code is embedded into the RoNI to ensure integrity of RoI, confidentiality of

ERP and ownership authentication. The scheme is successful at maintaining imperceptibility of the medical image, robustness, tamper detection and security. The proposed scheme is tested with various attacks such as filtering, compression, geometric and noising and the experimental results demonstrate that robustness is achieved for majority of attacks. The proposed tamper detection and recovery algorithm is able to achieve more than 97% accuracy for efficient tamper detection and recovery in RoI. High confidentiality and payload of EPR with low computational cost is provided by pseudo random key and Huffman coding. The proposed scheme can be used for grayscale as well as color medical images of different modalities as indicated by the experimental results. Robustness for attacks such as salt and pepper noise, rotation and shear can be improved in future work. Further, in future we wish to optimize scaling factor using optimization approaches like Soft Computing, Nature inspired optimizations techniques.

REFERENCES

- [1] M. Begum and M. S. Uddin, "Analysis of digital image watermarking techniques through hybrid methods," *Adv. Multimedia*, vol. 2020, pp. 1–12, Aug. 2020.
- [2] C. Rey and J.-L. Dugelay, "A survey of watermarking algorithms for image authentication," *EURASIP J. Adv. Signal Process.*, vol. 2002, no. 6, Dec. 2002, Art. no. 218932.
- [3] Q. Su and B. Chen, "Robust color image watermarking technique in the spatial domain," *Soft Comput.*, vol. 22, no. 1, pp. 91–106, 2018.
- [4] M. Rathod and J. Khanapuri, "A comparative study of transform domain methods for image resolution enhancement of satellite image," in *Proc. 11th Int. Conf. Intell. Syst. Control (ISCO)*, Coimbatore, India, 2017, pp. 287–291.
- [5] L. Singh, A. K. Singh, and P. K. Singh, "Secure data hiding techniques: A survey," *Multimedia Tools Appl.*, vol. 79, no. 23, pp. 15901–15921, 2020.
- [6] H. S. Alshanbari, "Medical image watermarking for ownership & tamper detection," *Multimedia Tools Appl.*, vol. 80, no. 11, pp. 16549–16564, May 2021.
- [7] P. N. Faoziyah, F. P. Permana, T. A. B. Wirayuda, and U. N. Wisesty, "Tamper detection and recovery of medical image watermarking using modified LSB and Huffman compression," in *Proc. 2nd Int. Conf. Informat. Appl. (ICIA)*, Lodz, Poland, Sep. 2013, pp. 129–132.
- [8] B. Hassan, R. Ahmed, B. Li, and O. Hassan, "An imperceptible medical image watermarking framework for automated diagnosis of retinal pathologies in an eHealth arrangement," *IEEE Access*, vol. 7, pp. 69758–69775, 2019.
- [9] P. Khare and V. K. Srivastava, "A secured and robust medical image watermarking approach for protecting integrity of medical images," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 2, Feb. 2021, Art. no. e3918.
- [10] R. Eswaraiah and E. Sreenivasa Reddy, "Medical image watermarking technique for accurate tamper detection in ROI and exact recovery of ROI," *Int. J. Telemed. Appl.*, vol. 2014, Jan. 2014, Art. no. 13.
- [11] K. Swaraja, K. Meenakshi, and P. Kora, "An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine," *Biomed. Signal Process. Control*, vol. 55, Jan. 2020, Art. no. 101665.
- [12] F. Sabbane and H. Tairi, "Medical image watermarking technique based on polynomial decomposition," *Multimedia Tools Appl.*, vol. 78, no. 23, pp. 34129–34155, Dec. 2019.
- [13] T. A. BW and F. P. Permana, "Medical image watermarking with tamper detection and recovery using reversible watermarking with LSB modification and run length encoding (RLE) compression," in *Proc. IEEE Int. Conf. Commun., Netw. Satell. (ComNetSat)*, Jul. 2012, pp. 167–171.
- [14] R. Thanki, S. Borra, V. Dwivedi, and K. Borisagar, "An efficient medical image watermarking scheme based on FDCuT–DCT," *Int. J. Eng. Sci. Technol.*, vol. 20, no. 4, pp. 1366–1379, Aug. 2017.

- [15] M. Sharma, "Medical image watermarking technique in the application of E-diagnosis using M-Ary modulation," *Proc. Comput. Sci.*, vol. 85, pp. 648–655, Jan. 2016.
- [16] C. Kumar, A. K. Singh, and P. Kumar, "Dual watermarking: An approach for securing digital documents," *Multimedia Tools Appl.*, vol. 79, pp. 1–16, Dec. 2019.
- [17] A. Shehab, M. Elhoseny, K. Muhammad, A. K. Sangaiah, P. Yang, H. Huang, and G. Hou, "Secure and robust fragile watermarking scheme for medical images," *IEEE Access*, vol. 6, pp. 10269–10278, 2018.
- [18] S. Kumar and R. K. Jha, "FD-based detector for medical image watermarking," *IET Image Process.*, vol. 13, no. 10, pp. 1773–1782, Aug. 2019.
- [19] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004.
- [20] X. Hou and L. Zhang, "Saliency detection: A spectral residual approach," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jun. 2007, pp. 1–8.
- [21] A. Jagannatham, "Mersenne Twister—A pseudo random number generator and its variants," Dept. Elect. Comput. Eng., George Mason Univ., Fairfax, VA, USA, Tech. Rep. 14718336, 2008.
- [22] A. Nagm and M. S. Elwan, "Protection of the patient data against intentional attacks using a hybrid robust watermarking code," *PeerJ Comput. Sci.*, vol. 7, p. e400, Mar. 2021.
- [23] S. A. Parah, J. A. Kaw, P. Bellavista, N. A. Loan, G. M. Bhat, K. Muhammad, and V. H. C. de Albuquerque, "Efficient security and authentication for edge-based Internet of Medical Things," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15652–15662, Nov. 2021.
- [24] A. Soualmi, A. Alti, and L. Laouamer, "A novel blind medical image watermarking scheme based on Schur triangulation and chaotic sequence," *Concurrency Comput., Pract. Exper.*, vol. 34, no. 1, Jan. 2022, Art. no. e6480.
- [25] K. Balasamy and S. Suganyadevi, "A fuzzy based ROI selection for encryption and watermarking in medical image using DWT and SVD," *Multimedia Tools Appl.*, vol. 80, no. 5, pp. 7167–7186, Feb. 2021.
- [26] N. Sharma, A. Ray, K. Shukla, S. Sharma, S. Pradhan, A. Srivastva, and L. Aggarwal, "Automated medical image segmentation techniques," *J. Med. Phys.*, vol. 35, no. 1, p. 3, 2010.
- [27] K. K. Roy and A. Phadikar, "Automated medical image segmentation: A survey," *Comput., Commun. Manuf.*, vol. 1, pp. 1–5, 2014, Art. no. 45784192.
- [28] D. L. Pham, C. Xu, and J. L. Prince, "Current methods in medical image segmentation," *Annu. Rev. Biomed. Eng., Annu. Rev.*, vol. 2, no. 1, pp. 315–337, 2000.
- [29] V. Rajput and I. A. Ansari, "Image tamper detection and self-recovery using multiple median watermarking," *Multimedia Tools Appl.*, vol. 79, nos. 47–48, pp. 35519–35535, Dec. 2020, doi: 10.1007/s11042-019-07971-w.
- [30] S. Prasad and A. K. Pal, "A tamper detection suitable fragile watermarking scheme based on novel payload embedding strategy," *Multimedia Tools Appl.*, vol. 79, nos. 3–4, pp. 1673–1705, Jan. 2020, doi: 10.1007/s11042-019-08144-5.
- [31] S. Bhalerao, I. A. Ansari, and A. Kumar, "A secure image watermarking for tamper detection and localization," *J. Ambient Intell. Hum. Comput.*, vol. 12, no. 1, pp. 1057–1068, Jan. 2021.
- [32] S. M. M. Islam, R. Debnath, and S. K. A. Hossain, "DWT based digital watermarking technique and its robustness on image rotation, scaling, JPEG compression, cropping and multiple watermarking," in *Proc. Int. Conf. Inf. Commun. Technol.*, Mar. 2007, pp. 246–249.
- [33] H. Daren, L. Jiufen, H. Jiwu, and L. Hongmei, "A DWT-based image watermarking algorithm," in *Proc. IEEE Int. Conf. Multimedia Expo*, Aug. 2001, p. 80.
- [34] M. Ali, C. W. Ahn, and M. Pant, "A robust image watermarking technique using SVD and differential evolution in DCT domain," *Optik*, vol. 125, no. 1, pp. 428–434, Jan. 2014.
- [35] C.-C. Lai and C.-C. Tsai, "Digital image watermarking using discrete wavelet transform and singular value decomposition," *IEEE Trans. Instrum. Meas.*, vol. 59, no. 11, pp. 3060–3063, Nov. 2010.
- [36] S. B. B. Ahmadi, G. Zhang, and S. Wei, "Robust and hybrid SVD-based image watermarking schemes," *Multimedia Tools Appl.*, vol. 79, pp. 1075–1117, Jan. 2020.
- [37] R. K. Singh, D. K. Shaw, and J. Sahoo, "A secure and robust block based DWT-SVD image watermarking approach," *J. Inf. Optim. Sci.*, vol. 38, no. 6, pp. 911–925, Aug. 2017.
- [38] C. M. A. Rahman, "Automatic RoI selection for multi-modal medical images," M.S. thesis, Dept. Elect., Electron. Commun. Eng., Mil. Inst. Sci. Technol., Dhaka, Bangladesh, 2020.
- [39] J. L. Bentley and M. I. Shamos, "Divide and conquer for linear expected time," Dept. Comput. Sci., Carnegie-Mellon Univ., Pittsburgh, PA, USA, Tech. Rep., 1977, vol. 7.2.
- [40] A. D. Andrushia and R. Thangarajan, "An efficient visual saliency detection model based on Ripplet transform," *Sādhanā*, vol. 42, no. 5, pp. 671–685, May 2017.
- [41] S. Maheshkar, "Region-based hybrid medical image watermarking for secure telemedicine applications," *Multimedia Tools Appl.*, vol. 76, no. 3, pp. 3617–3647, Feb. 2017.
- [42] A. B. Jambek and N. A. Khairi, "Performance comparison of Huffman and Lempel–Ziv Welch data compression for wireless sensor node application," *Amer. J. Appl. Sci.*, vol. 11, no. 1, pp. 119–126, Jan. 2014.
- [43] C. Raghavendra, S. Sivasubramanian, and A. Kumaravel, "Improved image compression using effective lossless compression technique," *Cluster Comput.*, vol. 22, no. S2, pp. 3911–3916, Mar. 2019.
- [44] V. Punitha and P. Kalavathi, "Analysis of file formats and lossless compression techniques for medical images," *Int. J. Sci. Res. Comput.*, vol. 2, no. 1, pp. 1–6, 2020.
- [45] P. Cignoni, M. Corsini, and G. Ranzuglia, "MeshLab: An open-source 3D mesh processing system," *Ercim news*, vol. 73, pp. 45–46, Jan. 2008.
- [46] D. Liu, Z. Yuan, and Q. Su, "A blind color image watermarking scheme with variable steps based on Schur decomposition," *Multimedia Tools Appl.*, vol. 79, nos. 11–12, pp. 7491–7513, Mar. 2020.
- [47] M. Moosazadeh and G. Ekbatanifard, "A new DCT-based robust image watermarking method using teaching-learning-based optimization," *J. Inf. Secur. Appl.*, vol. 47, pp. 28–38, Aug. 2019.
- [48] X. Wu and W. Sun, "Robust copyright protection scheme for digital images using overlapping DCT and SVD," *Appl. Soft Comput.*, vol. 13, pp. 1170–1182, Feb. 2013.
- [49] S. Rawat and B. Raman, "A blind watermarking algorithm based on fractional Fourier transform and visual cryptography," *Signal Process.*, vol. 92, no. 6, pp. 1480–1491, Jun. 2012.
- [50] M. Ali, C. W. Ahn, and M. Pant, "An efficient lossless robust watermarking scheme by integrating redistributed invariant wavelet and fractional Fourier transforms," *Multimedia Tools Appl.*, vol. 77, no. 10, pp. 11751–11773, May 2018.
- [51] A. Torralba, "Modeling global scene factors in attention," *J. Opt. Soc. Amer. A, Opt. Image Sci.*, vol. 20, no. 7, pp. 1407–1418, 2003.
- [52] A. Torralba and A. Oliva, "Depth estimation from image structure," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 24, no. 9, pp. 1226–1238, Sep. 2002.
- [53] A. Torralba and A. Oliva, "Statistics of natural image categories," *Network*, vol. 14, no. 3, pp. 391–412, Aug. 2003.
- [54] (Sep. 2012). *Zxing*. Accessed: Sep. 2021. [Online]. Available: <http://zxing.appspot.com/generator>
- [55] Accessed: May 2021. [Online]. Available: <https://openi.nlm.nih.gov/>
- [56] Accessed: May 2021. [Online]. Available: <https://sipi.usc.edu/database/>
- [57] Accessed: May 2021. [Online]. Available: <https://www.kaggle.com/>
- [58] Accessed: Sep. 2021. [Online]. Available: <http://www.onlinemedicalimages.com/>
- [59] Accessed: Sep. 2021. [Online]. Available: <http://cecas.clemson.edu/~ahoover/stare/>

• • •