

# Medical image authentication using SLT and IWT schemes

Rasha Thabit<sup>1</sup> · Bee Ee Khoo<sup>1</sup>

Received: 20 March 2015 / Revised: 12 September 2015 / Accepted: 30 October 2015 /  
Published online: 7 November 2015  
© Springer Science+Business Media New York 2015

**Abstract** Over the years, different watermarking techniques have been used for medical image authentication purposes. Some techniques have been presented to detect tampering in the medical image while others can also recover the tampered region after the tamper detection. Many of the previous medical image authentication schemes have successfully achieved their aims; however, the robustness of the authentication scheme against unintentional attacks has not been highlighted sufficiently. This paper presents a new medical image authentication scheme in which the medical image is divided into two regions (i.e., region of interest (ROI) and region of non-interest (RONI)). Then two watermarking methods based on Slantlet transform (SLT) are used to embed data in the ROI and the RONI. The proposed scheme can be used for tamper detection, localization, and recovery in addition to the data hiding. To generate the recovery information of the ROI, a new method has been proposed based on the integer wavelet transform (IWT) coefficients. The experiments that have been conducted to evaluate the proposed authentication scheme proved that it is efficient not only in achieving its main tasks that have been mentioned above but also in having robustness against unintentional attacks (i.e., JPEG compression, additive Gaussian noise (AGN), and salt-and-pepper noise) and that makes it more suitable for the practical applications.

**Keywords** Medical image authentication · ROI-based watermarking · Slantlet transform (SLT) · Integer wavelet transform (IWT)

## 1 Introduction

Digital medical images represent an important kind of media that needs protection against manipulation especially when these images are exchanged through unsecured channels like internet. Different image watermarking schemes have been used to protect medical images where some watermarking schemes have been used for authentication while other schemes

---

✉ Bee Ee Khoo  
beekhoo@usm.my; bekhootan@gmail.com

<sup>1</sup> School of Electrical and Electronic Engineering, Engineering Campus, Universiti Sains Malaysia, 14300 Nibong Tebal, Seberang Perai Selatan, Pulau Pinang, Malaysia

have been used for data hiding [1]. The medical image watermarking schemes can be classified according to their objectives into four major classes that are: (a) schemes for security and privacy control [16, 18], (b) schemes for intactness of the region of interest (ROI) [12–14, 24, 25], (c) schemes for data hiding and tamper detection [7–9, 22], and (d) schemes for tamper detection, localization, and recovery [2, 3, 6, 10, 17, 23, 26, 27].

Some medical image watermarking schemes have been presented to hide the electronic patient's record (EPR) in the medical image in order to avoid the detachment of the medical information from the corresponding image and to provide security and privacy while sharing the medical information [16, 18]. In other medical image watermarking schemes, the image is divided into two parts, one of them is the important part for the diagnosis process, which is called the region of interest (ROI) and the second part called the region of non-interest (RONI). It is important that the watermarking process should not affect the ROI because if this region is distorted it may cause wrong diagnosis [12–14, 24, 25]. To ensure the intactness of the ROI, some authentication schemes embed the data in the RONI and keep the ROI intact [12–14], while other schemes [24, 25] have been proposed for the authentication of the ROI in the medical image. In [24, 25], the image has been divided into two regions (i.e., ROI and RONI) then the SHA-256 hash code for the ROI is calculated and embedded in the Least Significant Bits (LSBs) of the RONI. At the receiver side, the original hash value is extracted from the LSBs of the RONI and then these LSBs are set to zero. The authentication process is conducted by calculating the hash value of the received ROI and comparing it with the original hash value that has been extracted from the RONI. If they are the same, the image is authentic and the ROI is intact. The watermarking schemes in [24, 25] are reversible if the original pixel value has zero in its LSB otherwise the pixel value is irreversible.

Some medical image watermarking schemes have been presented to hide medical information and detect tampering in the medical image. In [22], multiple watermarks have been embedded in the medical image. The patient's information has been embedded in the border of the image using robust watermarking and a fragile watermark has been embedded in the LSBs of the image to detect tampering. In [7, 8], the schemes have been proposed for the health information management that are based on discrete wavelet transform (DWT) and a quantization method to embed the information. The scheme is irreversible and part of the embedded data has robustness against JPEG compression. In [9], a modified difference expansion method has been proposed, which is an improved version of the original difference expansion (DE) method from [21]. In [9], a region of embedding (ROE) has been chosen to prevent generating any distortion in the ROI. The embedded watermark in this scheme includes the patient's data and the hash value for tamper detection.

Some medical image watermarking schemes have been proposed for detecting tampering in the image, localizing the tampered region, and recovering the tampered region. In [26], the medical image has been divided into blocks of  $8 \times 8$  pixels then each block is divided into four sub-blocks of  $4 \times 4$  pixels. For each sub-block the watermark bits have been generated including 2 bits for authentication and 7 bits for recovery. The average of the pixel values in each sub-block has been calculated as recovery information. The generated watermark has been embedded in another block in the image using LSBs. The scheme is irreversible and the embedded watermark is fragile. Thereafter, the authors improved the previous authentication scheme by presenting ROI-based scheme [27] where the authentication process has been conducted for the ROI. The 2 bits for authentication have been embedded in the ROI and the recovery bits have been embedded in the RONI. The scheme is also irreversible and the embedded watermark is fragile but less information has been embedded in the ROI, which gives better visual quality of the watermarked

ROI. In addition, the recovery information has been generated from the average of each  $2 \times 2$  pixels instead of  $4 \times 4$  pixels, which makes the recovered ROI after tampering has better visual quality. In [23], two authentication schemes based on modulo 256 and discrete cosine transform (DCT) have been presented. The first scheme is for authentication and recovery for whole image blocks. The authentication information is generated from the hash value of the image and the recovery information is generated from the JPEG compression of the block. This scheme performs well in detecting the tampered block but because of the limited capacity, high compression rate has been used to reduce the recovery information, which leads to unacceptable recovered blocks as pointed out by the authors themselves [23]. The second scheme in [23] has been suggested to solve the previous problem where the image has been divided into ROI and RONI then the authentication and recovery information has been generated from the ROI only. Therefore, less compression rate can be used to obtain the recovery information and thus the recovered blocks of the ROI have better visual quality. The scheme is not completely reversible because of the preprocessing that has been used to avoid the pixel flipping. In [6], two reversible schemes based on difference expansion technique (DE) have been proposed for the tamper detection and recovery. In these schemes, the image is divided into  $4 \times 4$  blocks and each block is transformed using DE technique. Only smooth blocks (i.e., the blocks with equal pixel values) have been used for the embedding process. In the first scheme, the average of the pixel values in each block has been calculated as recovery information. The second scheme is ROI-based where the pixel values of the ROI have been used as the recovery information. The disadvantage of this scheme is the limitation of the capacity because of using only the smooth blocks. In [2, 3], hybrid watermarking schemes have been proposed to hide patient's data, authenticate ROI, localize tampering in the ROI, and recover the tampered region. In these schemes, the recovery information has been generated from the JPEG2000 compression of the ROI. The patient's data have been embedded in the ROI and the tamper localization and recovery information have been embedded in the RONI. In both schemes, the data have been embedded in the ROI using the modified difference expansion method that has been presented in [9]. In [2], the original difference expansion method from [21] has been used to embed the data in the RONI. In [3], the data has been embedded in the RONI using three-level DWT technique from [11]. The experiments of this technique show that the scheme has robustness against certain level of salt and pepper noise. In [10], another watermarking scheme has been presented for data hiding, tamper localization, and recovery. This scheme used the same procedures that have been proposed in [26] but to make the watermarking process reversible in the ROI, the original LSBs of the ROI have been extracted and embedded in the RONI. The recovery information has been generated from the average of each  $4 \times 4$  block, which leads to recover the tampered blocks of the ROI with low visual quality. The scheme is fragile because of embedding data in the LSBs. In [17], a new fragile medical image watermarking scheme based on a chaotic key and residue number system has been presented. In this scheme, the image is divided into ROI and RONI. The residues of the ROI are calculated using the residue number system in order to be used instead of the original pixel values of the ROI in the watermarked image. The chaotic key has been used as a secret key to choose the locations of embedding the hash value in the RONI. The LSBs of the pixel values in the chosen locations are set to zero and the residues of the ROI are used instead of the original values then the hash value of the image is calculated and embedded in the LSBs of the chosen pixels of the RONI. The hash value has been used to detect tampering at the receiver side, if image is authentic the scheme continue the steps of recovering the original ROI using residue number system and Chinese remainder transform. Thus, the scheme is reversible for the ROI and irreversible for the RONI.

Obviously, there are three aspects that needs to be taken into consideration while implementing a new medical image authentication scheme, which are (a) the tasks that can be performed by the scheme (i.e., data hiding, tamper detection, tamper localization, and tamper recovery), (b) the visual quality of the recovered image after tampering, and (c) the ability of the authentication scheme to withstand the unintentional attacks (i.e., lossy compression and noise). Taking into consideration of these aspects, this paper presents a new ROI-based medical image authentication scheme. First, the medical image is divided into two regions (i.e., ROI and RONI). Then, the information for tamper detection, localization, and recovery are generated from the ROI and embedded in the RONI using robust watermarking scheme based on Slantlet transform. The patient's data are embedded in the ROI using robust reversible watermarking scheme based on Slantlet transform. The recovery information of the ROI has been generated using a new method based on integer wavelet transform coefficients.

The proposed scheme can be used for tamper detection, localization, and recovery, in addition to the data hiding. The ROI has been recovered with good visual quality and the scheme has the ability to withstand the unintentional attacks (i.e., JPEG compression, additive Gaussian noise (AGN), and salt-and-pepper noise). The rest of the paper is organized as follows. Section 2 introduces the proposed medical image authentication scheme. Section 3 presents the results of the experiments that have been conducted to evaluate the proposed scheme. In Section 4, the conclusions of the work are presented.

## 2 The proposed medical image authentication scheme

The ROI is the important part for the diagnosis process in the medical image hence some medical image authentication schemes used reversible watermarking for the ROI to ensure its intactness. The proposed authentication scheme in this paper also depends on this idea. Based on the new researches in the reversible watermarking field, the robust reversible watermarking (RRW) schemes have been suggested as better candidates for the practical applications because they can withstand attacks [4, 5, 19, 20]; therefore, we used RRW for embedding data in the ROI, which is based on our previous work in [20]. The data for tamper detection, localization, and recovery have been embedded in the RONI using a modified version of our previous robust irreversible watermarking scheme that has been implemented in [15]. As explained in section 1, most of the previous tamper detection, localization, and recovery methods reduced the recovery information because of the capacity limitation. In the proposed scheme, a new method based on the integer wavelet transform (IWT) has been suggested to generate the recovery information of the ROI. The proposed algorithm for generating the recovery information is explained in details in the following subsection. Then, the proposed watermarking method for embedding data in the RONI is explained. Thereafter, the procedures of the RRW scheme for the ROI are briefly mentioned (the reader can refer to [20] for more details). Lastly, the complete procedures of the proposed authentication scheme are clarified.

### 2.1 The proposed algorithm for generating the recovery information

The previous authentication schemes proposed some methods to reduce the recovery information. Some of these methods depend on the average of the pixel values in a specific block size. For instance, the schemes in [6, 10, 26] used the average of each  $4 \times 4$  pixels as the recovery information while in [27] the average of each  $2 \times 2$  pixels has been used as the

recovery information. Other schemes used a compressed form of the ROI using JPEG2000 compression such as the methods in [2, 3]. The schemes that are based on the average of the pixel values reduce the quality of the ROI and in some cases, it may be considered as unacceptable. The schemes that are based on the compression of the ROI have better visual quality but the use of the JPEG2000 compression limits the robustness of the scheme because any change in the compressed sequence will cause error in the decoding software of the JPEG2000 compression. In the proposed authentication scheme, a new method has been suggested to generate the recovery information of the ROI, which reduces the recovery information, provides good visual quality of the recovered ROI, and gives a chance to implement a robust authentication scheme. The proposed method depends on the integer wavelet transform. The procedures of generating the recovery information (i.e., the features) and recovering the image from the extracted features are explained as follows.

### 2.1.1 Extracting the features

Consider a grayscale image  $I_m$  of size  $(512 \times 512 \times 8 \text{ bit})$ , the features are extracted using the following steps:

- 1) Calculate the integer wavelet transform (IWT) of the image  $I_m$ . The resulting Approximation (CA), Horizontal (CH), Vertical (CV), and Diagonal (CD) coefficient matrices are in integer form.
- 2) Select the approximation coefficients (CA) to generate the features. Some of the coefficients have negative values and some others have values more than 255. Aiming to obtain a feature that can be presented using 8-bits, an adjustment process has been applied to make the coefficients values in the range [0 to 255] as follows:

$$CA_{new}(i, j) = \begin{cases} 0 & \text{if } CA(i, j) < 0 \\ 255 & \text{if } CA(i, j) > 255 \\ CA(i, j) & \text{if } 0 \leq CA(i, j) \leq 255 \end{cases} .$$

Where  $CA$  is the original approximation coefficients,  $CA_{new}$  is the new approximation coefficients after the adjustment process, and  $(i, j)$  are the coordinates of the coefficient.

- 3) Reshape the matrix of  $CA_{new}$  coefficients to be a single row  $RowCA_{new}$ .
- 4) Convert the sequence of the coefficients in  $RowCA_{new}$  to binary by converting each coefficient to 8-bit binary number then save the binary bits in  $F$ .

### 2.1.2 Recovering the image from the extracted features

The steps of recovering the image from its features are as follows:

- 1) Convert  $F$  from binary to decimal and reshape the row of coefficients to obtain  $CA_{new}$  matrix.
- 2) Consider the Horizontal (CH), Vertical (CV), and Diagonal (CD) coefficients matrices are zeros.
- 3) Apply inverse integer wavelet transform to obtain the recovered image  $RI_m$ .

Experiments have been conducted to choose the wavelet family that can give the best visual quality of the recovered image. Different wavelet families (i.e., 35 wavelet families) have been tested for different medical images. The visual quality has been evaluated by calculating the peak-signal-to-noise ratio (PSNR) between the original medical image and the recovered image from the extracted features. Some of the experimental results that have been obtained are shown in Table 1. From the results it has been found that the proposed method gives the best visual quality of the recovered image using wavelet family Cohen-Daubechies-Feauveau wavelet 3.5 ‘cdf 3.5’. Therefore, the chosen wavelet family for the proposed method will be wavelet cdf 3.5.

Another experiment has been conducted to compare the visual quality of the recovered image using the proposed method with the recovered image using the previous methods that have been suggested in [2, 3, 6, 10, 26, 27]. The comparison has been conducted for the recovered image from the average of the pixel values for each  $2 \times 2$  block, the average of the pixel values for each  $4 \times 4$  block, the JPEG2000 compression, and the proposed feature extraction method using IWT (wavelet family ‘cdf 3.5’). Table 2 shows the results of this experiment, which illustrates that the recovered image using the proposed method has better visual quality in comparison with the previous methods. Figure 1 shows an example of the recovered images obtained by the compared methods, where the regions of interest are zoomed to show the difference clearly.

## 2.2 The proposed algorithm to hide data in the RONI

To provide high data hiding capacity to embed the information in the RONI, this section presents an improved version of the scheme in [15]. The algorithm here depends on using the Slantlet transform matrix [20] instead of the conventional Slantlet transform.

### 2.2.1 Embedding in the RONI

The procedures of the proposed algorithm to embed binary data in a block of size  $(16 \times 16)$  pixels are as follows:

- 1) Transform the image block using SLT matrix as follows:

$$TB = [SLT_{16}]B[SLT_{16}^T].$$

Where  $B$  is the original block,  $TB$  is the transformed block, and  $SLT_{16}$  is the Slantlet transform matrix of size  $16 \times 16$ .

- 2) Divide the coefficients in  $TB$  into 4 subbands (LL, HL, LH, and HH).
- 3) Embed binary data ‘ $b$ ’ by modifying the HL and LH subbands. The watermark bit  $b(i)$  is embedded by manually changing the value of the difference between  $HL(x,y)$  and  $LH(x,y)$ . The rules of the SLT coefficients modification are as follows:

$$\text{If } b(i) = 1 \text{ and } D_1 = HL(x,y) - LH(x,y) < T,$$

( $T$  is a threshold to control watermark invisibility), then increase  $HL(x,y)$  while decrease  $LH(x,y)$  by inserting the watermark.

**Table 1** The visual quality (PSNR (dB)) of the recovered image from the extracted features for different wavelet families

Wavelet name	Test images					
	Image 1	Image 2	Image 3	Image 4	Image 5	Image 6
'haar'	36.649	34.764	35.157	35.518	35.470	35.600
'db2'	38.441	40.138	40.572	40.895	40.933	41.119
'db3'	38.431	39.600	40.003	40.231	40.331	40.560
'db4'	26.460	15.653	15.283	14.662	14.474	14.676
'db5'	27.291	16.046	15.655	15.016	14.823	15.034
'db6'	35.417	38.170	38.300	38.300	38.443	38.497
'db7'	17.287	11.378	11.187	10.787	10.666	10.802
'db8'	32.574	34.189	34.287	34.226	34.360	34.400
'sym2'	38.441	40.138	40.572	40.895	40.933	41.119
'sym3'	20.678	12.895	12.647	12.172	12.027	12.181
'sym4'	40.119	44.830	45.160	45.433	45.446	45.749
'sym5'	38.435	44.665	44.755	44.785	44.832	44.894
'sym6'	31.515	33.390	33.456	33.421	33.527	33.513
'sym7'	33.294	35.010	35.122	35.064	35.234	35.167
'sym8'	19.120	12.190	11.970	11.530	11.396	11.541
'cdf1.1'	36.649	34.764	35.157	35.518	35.470	35.600
'cdf1.3'	36.433	34.536	34.930	35.295	35.244	35.380
'cdf1.5'	36.278	34.418	34.812	35.181	35.129	35.270
'cdf3.1'	39.893	51.407	51.540	51.504	51.519	51.924
'cdf3.3'	40.317	51.529	51.680	51.613	51.644	52.039
'cdf3.5'	40.474	51.655	51.823	51.743	51.799	52.203
'cdf5.1'	36.536	40.525	40.840	40.762	41.085	41.240
'cdf5.3'	35.257	39.088	39.178	39.267	39.506	39.650
'cdf5.5'	37.436	41.306	41.492	41.428	41.751	41.826
'cdf2.2'	39.684	41.187	41.595	41.920	41.967	42.276
'cdf2.4'	39.803	41.398	41.804	42.120	42.176	42.482
'cdf2.6'	39.844	41.451	41.863	42.184	42.243	42.544
'cdf4.2'	38.214	41.461	41.748	41.808	42.026	42.247
'cdf4.4'	38.835	42.414	42.699	42.711	42.904	43.173
'cdf4.6'	39.084	42.840	43.097	43.114	43.309	43.583
'cdf6.2'	32.371	35.004	35.040	35.205	35.278	35.525
'cdf6.4'	33.346	36.497	36.482	36.676	36.728	36.917
'cdf6.6'	33.725	37.043	37.070	37.182	37.285	37.434
'bior4.4'	38.100	25.995	25.191	24.394	24.056	24.580
'bior5.5'	31.300	19.260	18.684	17.941	17.700	18.018
Max. PSNR	40.474	51.655	51.823	51.743	51.799	52.203

$$\begin{cases} HL'(x,y) = HL(x,y) + \frac{(T-D1)}{2} \\ LH'(x,y) = LH(x,y) - \frac{(T-D1)}{2} \end{cases}$$

**Table 2** Comparison of the visual quality of the recovered image for different methods

Image	PSNR (dB)			
	Average 2×2	Average 4×4	JPEG 2000	IWT (cdf3.5)
Image 1	36.6731	31.6142	36.8841	40.4736
Image 2	35.6110	28.5716	38.9219	52.2025
Image 3	33.2378	26.5669	40.2027	44.0007
Image 4	30.1062	23.5957	37.2179	39.0506
Image 5	41.0075	33.9465	41.7425	54.9735
Image 6	32.8499	25.6803	37.5643	46.6089

Else if  $D_1 = HL(x,y) - LH(x,y) \geq T$ , do nothing

If  $b(i) = 0$  and  $D_2 = LH(x,y) - HL(x,y) < T$ , similar operation is done:

$$\begin{cases} HL'(x,y) = HL(x,y) - \frac{(T-D_2)}{2} \\ LH'(x,y) = LH(x,y) + \frac{(T-D_2)}{2} \end{cases}$$

Else if  $D_2 = LH(x,y) - HL(x,y) \geq T$ , do nothing.

This process is repeated to embed a binary sequence of length 64 bits. Thus, each spatial domain block of size  $16 \times 16$  pixels can carry 64 bits.

- 4) Replace the original horizontal and vertical high frequency coefficients with the modified coefficients.
- 5) Apply inverse SLT to obtain the watermarked image using:

$$B_{new} = [SLT_{16}^T] [TB_{new}] [SLT_{16}]$$

Where  $B_{new}$  is the watermarked spatial domain block,  $TB_{new}$  is the watermarked transform domain block, and  $SLT$  is the Slantlet transform matrix. The resultant values in the block  $B_{new}$  are rounded to integer values.

### 2.2.2 Extraction from the RONI

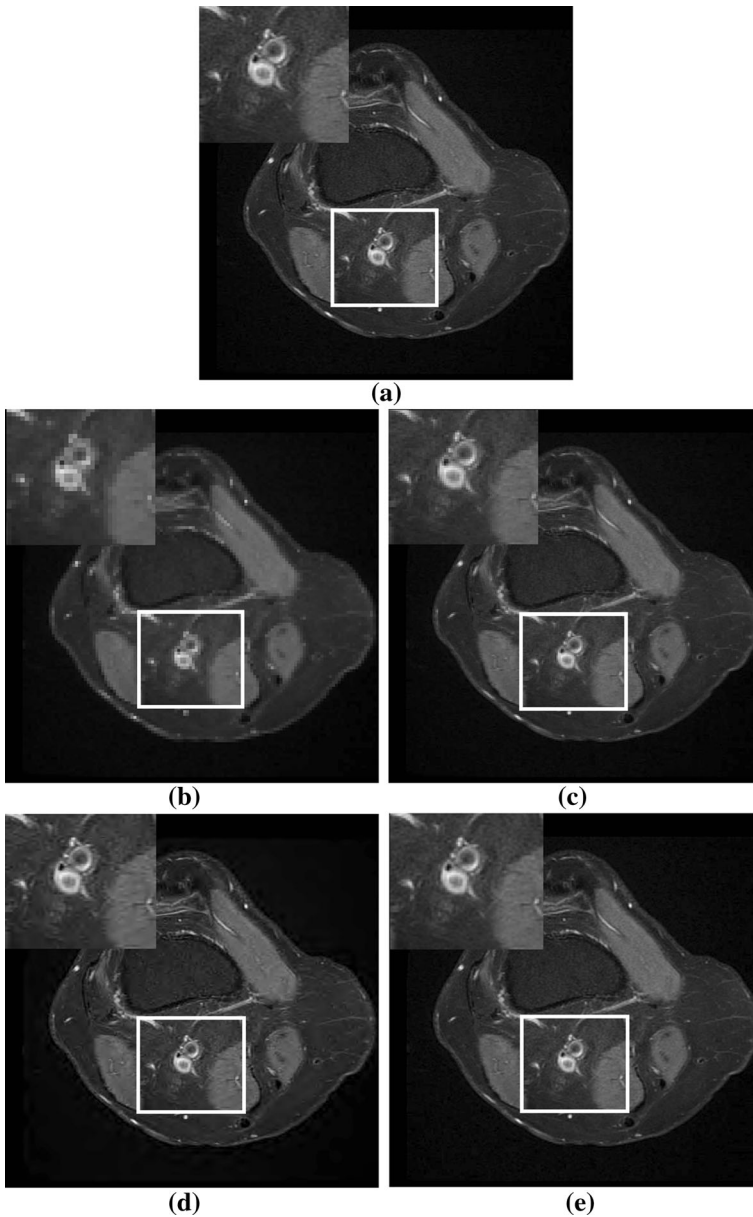
The procedures of extracting the binary data from a block of size  $(16 \times 16)$  pixels are as follows:

- 1) Transform the image block using SLT matrix of size  $16 \times 16$ .
- 2) Divide the coefficients into 4 subbands (LL, HL, LH, and HH).
- 3) Extract the watermark from the selected coefficients as follows:

The selected horizontal and vertical coefficients are  $HL'(x,y)$  and  $LH'(x,y)$ , respectively, the watermark bit  $b'(i)$  can be extracted by:

$$b'(i) = \begin{cases} 1, & \text{if } HL'(x,y) \geq LH'(x,y) \\ 0, & \text{if } LH'(x,y) > HL'(x,y) \end{cases}$$





**Fig. 1** Image1 results for the comparison methods. (a) Original image, recovered images using: (b) Average ( $4 \times 4$ ), (c) Average ( $2 \times 2$ ), (d) JPEG2000, and (e) IWT 'cdf 3.5'. The PSNR values of the recovered images are in Table 2

### 2.3 The robust reversible watermarking for the ROI [20]

The procedures of the watermark embedding and extraction processes are as follows:

### 2.3.1 Embedding procedures

- 1) Divide the image into non-overlapping blocks.
- 2) Transform each block using SLT matrix and divide the resultant coefficients into four subbands (HH, HL, LH, and LL).
- 3) Calculate the mean value of the SLT coefficients in HL subband ( $m^{HL}$ ) and LH subband ( $m^{LH}$ ).
- 4) Define a threshold value (T) to control the visual quality and the robustness, then calculate the modification factors as follows:

$$MF_1 = \frac{T - (m^{HL} - m^{LH})}{2}, \quad MF_2 = \frac{T - (m^{LH} - m^{HL})}{2}$$

- 5) Embed one watermark bit (w) in the each block using the following rules :
  - A) If  $w=1$  and  $(m^{HL} - m^{LH}) \geq T$ , then the block remains without change.
  - B) If  $w=1$  and  $(m^{HL} - m^{LH}) < T$ , then  $MF_1$  is added to  $m^{HL}$  and subtracted from  $m^{LH}$  (i.e.,  $m_{new}^{HL} = m^{HL} + MF_1$  and  $m_{new}^{LH} = m^{LH} - MF_1$ ).
  - C) If  $w=0$  and  $(m^{LH} - m^{HL}) \geq T$ , then the block remains without change.
  - D) If  $w=0$  and  $(m^{LH} - m^{HL}) < T$ , then  $MF_2$  is subtracted from  $m^{HL}$  and added to  $m^{LH}$  (i.e.,  $m_{new}^{HL} = m^{HL} - MF_2$  and  $m_{new}^{LH} = m^{LH} + MF_2$ ).

Because of the reversibility requirements, the difference between the mean values is saved as side information when the mean values are changed to embed the watermark bit.

- 6) Replace the original subbands by the modified subbands and apply the inverse SLT.
- 7) Apply pixel adjustment process to avoid the overflow/ underflow as follows:

$$I'_w(i, j) = \begin{cases} 255, & \text{if } I_w(i, j) > 255 \\ 0, & \text{if } I_w(i, j) < 0 \end{cases}$$

Where  $I_w$  is the watermarked image before pixel adjustment, (i,j) are the coordinates of the value in the image, and  $I'_w(i, j)$  is the modified pixel value.

### 2.3.2 Extraction procedures

- 1) Read the watermarked image and its corresponding side information.
- 2) Return the pixel values that have been adjusted to their locations.
- 3) Divide the image into non-overlapping blocks.
- 4) Transform each block using SLT matrix and divide the resultant SLT coefficients into 4 subbands.
- 5) Calculate the mean values of HL and LH subbands.
- 6) Extract the embedded bit using:

$$w^* = \begin{cases} 1, & \text{if } m^{HL*} \geq m^{LH*} \\ 0, & \text{if } m^{HL*} < m^{LH*} \end{cases} .$$

Where  $w^*$  is the extracted bit,  $m^{HL*}$  is the mean value of the SLT coefficients in HL subband and  $m^{LH*}$  is the mean value of the SLT coefficients in LH subband.

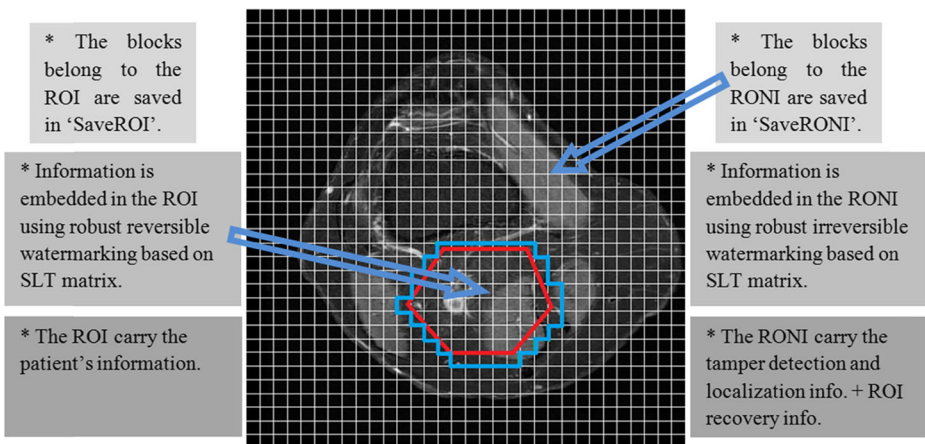
- 7) Recover the original image by applying the inverse of the process that has been applied in the embedding side.

## 2.4 The procedures of the proposed authentication scheme

The following subsections describe the embedding and extraction procedures of the proposed medical image authentication scheme.

### 2.4.1 Embedding procedures

- Step 1: The ROI in the medical image is selected by a polygon as shown in Fig. 2. Then the image is divided into non-overlapping blocks each of size  $16 \times 16$  pixels. The blocks belong to the ROI are extracted and saved in 'SaveROI' and the blocks belong to the RONI are extracted and saved in 'SaveRONI'. The locations of the ROI blocks are saved as a secret key ( $kl$ ) that will be used at the receiver side to mark the ROI blocks.
- Step 2: To generate the tamper detection and localization information, the average of the pixel values for each block in *SaveROI* is calculated and saved in 'AvROI'. Then *AvROI* is converted to binary sequence 'binAv' by converting each average value to 8 bits binary number.
- Step 3: The ROI is represented by a group of adjacent blocks to form an image 'ImROI'. Then the proposed algorithm (section 2.1.1) for generating the recovery information using IWT 'cdf 3.5' is applied to obtain the features of the image *ImROI* and the binary sequence of these features is saved as 'binROI'.
- Step 4: The binary sequences *binAv* and *binROI* are concatenated with each other and the resultant bit stream is coded using the error correction coding BCH (15,11,1) to increase the robustness. The coded binary sequence is saved as 'binSeq'.
- Step 5: The text file of the patient's information is converted to binary and saved as 'binText'.



**Fig. 2** Dividing medical image into ROI and RONI according to the selected ROI. The blocks that are surrounded by the cyan border are selected as the ROI blocks

- Step 6: A process of checking the available capacity in the ROI and the RONI is necessary before proceeding to the next steps. According to the algorithm that have been suggested to embed data in the RONI, each block can carry 64 bits, thus

$$\text{Capacity of RONI} = C_{RONI} = \text{No. of blocks in 'SaveRONI'} \times 64 \text{ bits} .$$

The capacity of *ImROI* of size ( $M \times N$ ) using the RRW from [20] is calculated at transform domain block size ( $2 \times 2$ ) (to obtain the highest embedding capacity) as follows:

$$\text{Capacity of ROI} = C_{ROI} = \frac{1}{16} \times (M \times N) .$$

Now the checking process is as follows:

- If  $C_{RONI} < \text{length}(\text{binSeq})$
  - Then dismiss the embedding procedures and show a message box asking the user to select smaller ROI.
  - If  $C_{ROI} < \text{length}(\text{binText})$
  - Then dismiss the embedding procedures and show a message box asking the user to select larger ROI.
  - If the capacity in both regions is enough to embed the data then continue the embedding procedures.
- Step 7: Start embedding in RONI.

The robust irreversible watermarking algorithm that has been explained in (section 2.2.1) is applied to embed the binary sequence (*binSeq*) in the RONI blocks that have been saved in (*SaveRONI*). Some of blocks required pixel adjustment before embedding data in order to ensure the correct recovery of the embedded data. The pixel values in the block are checked and modified using

$$\text{pixel}_m(i, j) = \begin{cases} 3 & \text{if } \text{pixel}(i, j) \leq 2 \\ 252 & \text{if } \text{pixel}(i, j) \geq 253 \\ \text{pixel}(i, j) & \text{else} \end{cases} .$$

Where  $\text{pixel}_m(i, j)$  is the modified pixel value. The resultant watermarked blocks are saved in '*WRONI*'.

- Step 8: Start embedding in ROI.

The RRW from [20] (section 2.3.1) is applied to embed the binary sequence (*binText*) in the *ImROI* at spatial domain block of size ( $4 \times 4$ ) (i.e., the transform domain block size is  $2 \times 2$ ) to obtain the highest embedding capacity. The algorithm generates some side information that is necessary for the reversibility of the scheme. The watermarked *ImROI* is rearranged as blocks of size ( $16 \times 16$ ) and saved in '*WROI*'.

- Step 9: The watermarked image is obtained by rearranging the blocks of *WROI* and *WRONI*. The watermarked image together with the side information that has been generated from embedding data in the ROI and the secret key (*kI*) are sent to the receiver side.

### 2.4.2 Extraction procedures

- Step 1: Read the watermarked image and the side information.
- Step 2: Mark the ROI and the RONI using  $k1$ .
- Step 3: Divide the image into non-overlapping blocks of size  $(16 \times 16)$  pixels.
- Step 4: Save the blocks of the ROI in '*WROI*' and save the blocks of the RONI in '*WRONI*'. Then the '*WROI*' is represented by a group of adjacent blocks to form an image '*ImWROI*'.
- Step 5: Extract the embedded text from *ImWROI* and recover the original ROI as explained in (section 2.3.2). The recovered ROI is rearranged as blocks of size  $16 \times 16$  pixels and saved in '*RecROI*'. Then the average of the pixel values in each block is calculated and saved in '*Avnew*'.
- Step 6: Extract the binary sequence from the RONI blocks using the extraction procedures that have been explained in (section 2.2.2). Decode the extracted binary sequence using BCH (15,11,1).
- Step 7: From the number of the blocks in *WROI*, one can easily separate the resultant binary sequence into its original parts (i.e., the recovery information part and the tamper detection and localization part). The process is as follows:

Average sequence length =  $AvLen$  = number of blocks in *WROI*  $\times$  8

Recovery sequence length =  $ReLen$  = length of the binary sequence -  $AvLen$

The recovery sequence bits = binary sequence (1 :  $ReLen$ )

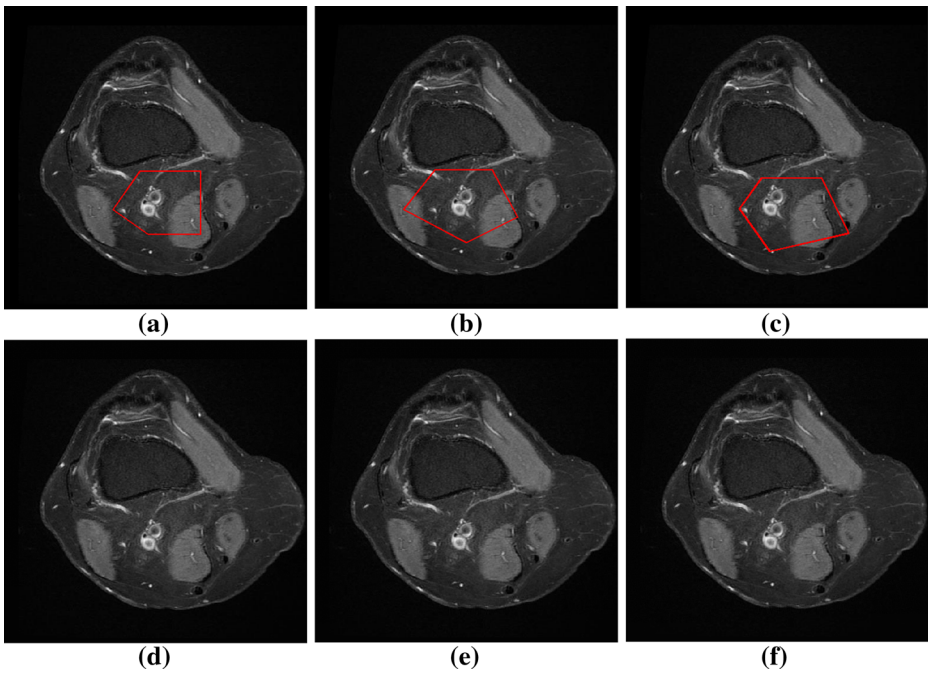
The average sequence bits = binary sequence ( $ReLen + 1$  : end of the binary sequence)

The recovery sequence bits and the average sequence bits are converted from binary to decimal to recover their original values that are named as '*IWTOriginal*' and '*AvOriginal*', respectively.

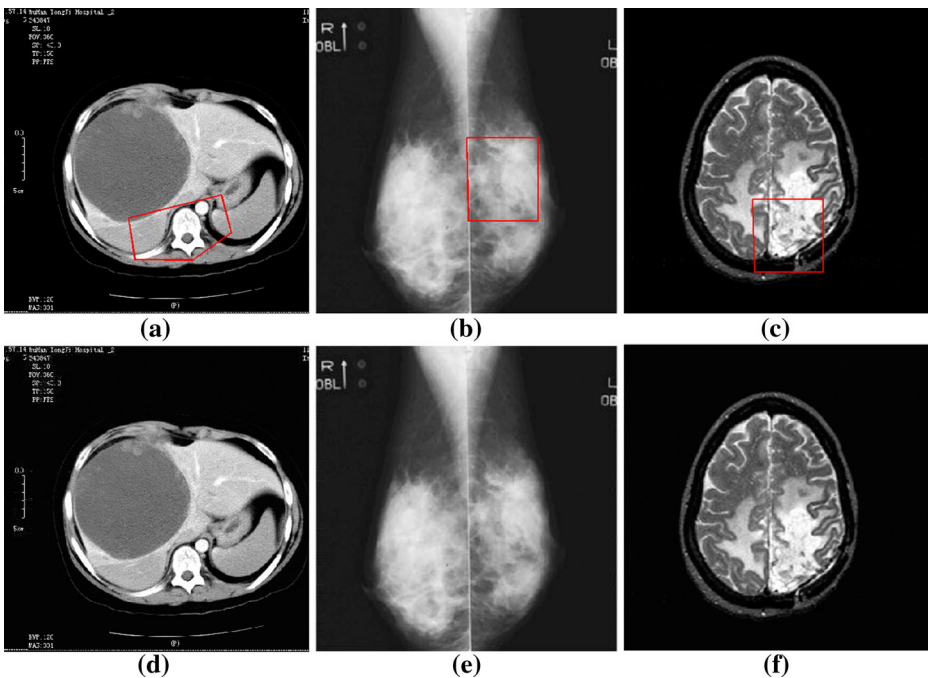
- Step 8: The ROI is tested to ensure its authenticity; the average values of the recovered ROI in '*Avnew*' are compared with the original average values in '*AvOriginal*'. If the values are equal then the image is authentic and the software is ended at this step. Otherwise, if any difference detected, the ROI is considered not authentic and the software must proceed for the tamper localization and recovery steps.
- Step 9: The recovery sequence in '*IWTOriginal*' is used to recover the ROI as explained in (section 2.1.2). The recovered ROI from its features is saved in '*OriginalROI*'.
- Step 10: The average values are compared; if '*Avnew*' and '*AvOriginal*' are not equal then their corresponding block is marked as tampered. Then the tampered block is replaced by its corresponding block in '*OriginalROI*' as a recovery process.

**Table 3** Invisibility test of the proposed authentication scheme

Image	Total capacity (bits)	ROI payload (bits)	RONI payload (bits)	Total payload (bits)	PSNR (dB)
Image 1 region1	62,320	1000	47,552	48,552	42.2544
Image 1 region2	61,840	1000	54,656	55,656	42.0782
Image 1 region3	61,792	1000	55,360	56,360	40.5454
Image2	62,176	1000	49,664	50,664	32.5856
Image3	61,696	1000	56,768	57,768	42.4724
Image4	62,464	1000	45,440	46,440	39.4181



**Fig. 3** Invisibility results for image 1. The original images: (a) Image 1 region1, (b) Image 1 region2, and (c) Image 1 region3. The watermarked images: (d) Image 1 region1, (e) Image 1 region2, and (f) Image 1 region3



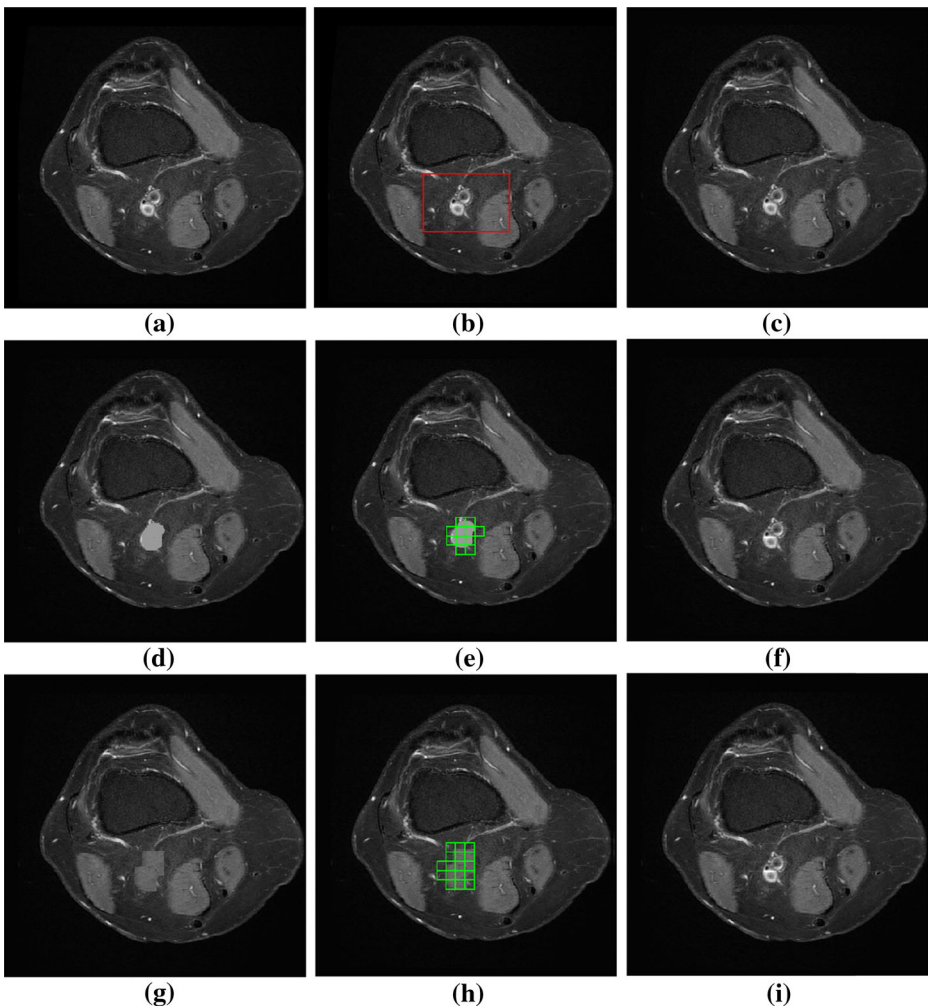
**Fig. 4** Invisibility results for three different images. The original images: (a) Image 2, (b) Image 3, and (c) Image 4. The watermarked images: (d) Image 2, (e) Image 3, and (f) Image 4

### 3 Experimental results and discussion

To test the performance of the proposed authentication scheme, the experiments have been conducted for medical images of size  $(512 \times 512 \times 8 \text{ bits})$ . The experiments and their results are in the following subsections.

#### 3.1 Invisibility test

The binary sequence of the patient's information has been fixed to 1000 bits. The threshold value has been set to  $T=2$  (as an example) for the embedding algorithms in the ROI and the RONI. The results of the visual quality test are in Table 3 where different images have been

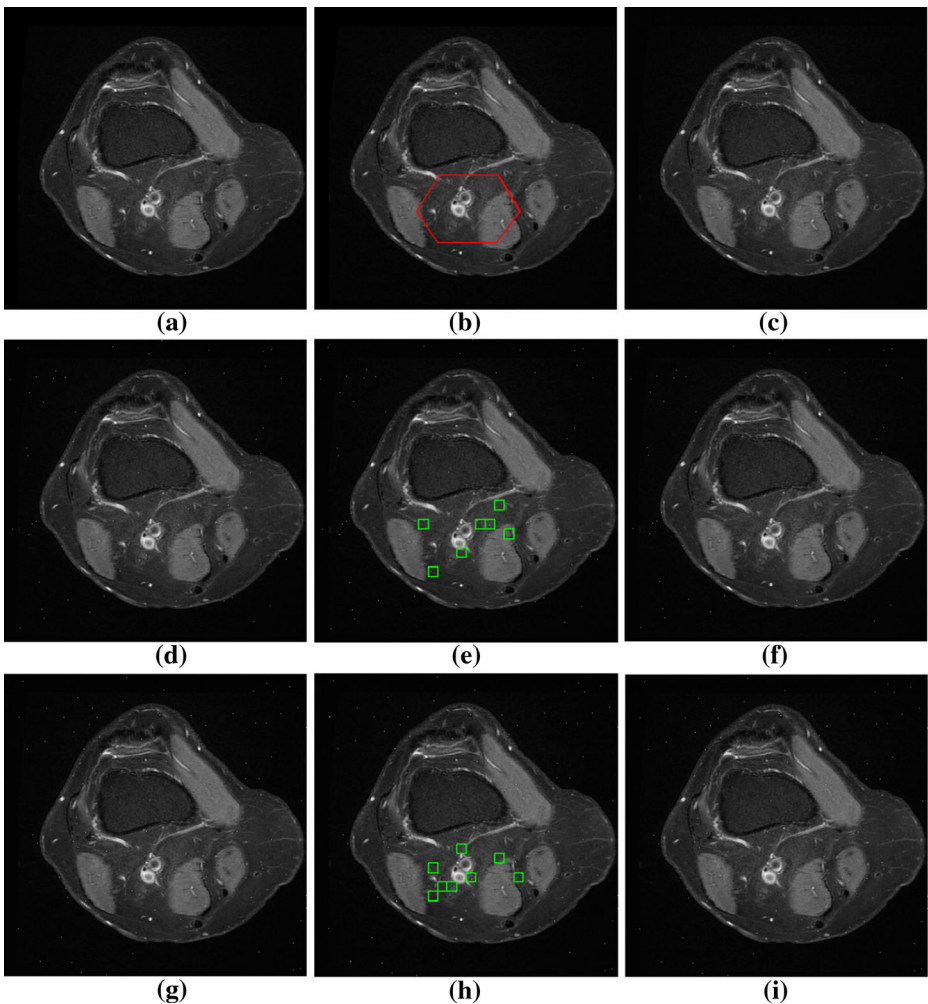


**Fig. 5** Examples to demonstrate tamper localization and recovery. (a) Original image, (b) Selected ROI, (c) Watermarked image, (d) Tamper1 (erasing), (e) Localization of Tamper1, (f) Recovery of Tamper1, (g) Tamper2 (copy & paste), (h) Localization of Tamper2, (i) Recovery of Tamper2

watermarked and one of the test images has been tested for different ROI. Figures 3 and 4 show the original images with the selected ROI and their corresponding watermarked images.

### 3.2 Tamper detection, localization, and recovery test

To demonstrate tamper detection, localization, and recovery, two tampering processes (i.e., erasing and copy & paste) have been imposed on the watermarked image as shown in Fig. 5, which illustrates the localization of the tampered area and the replacement of the tampered blocks with the recovery blocks. As shown in the results, the proposed scheme can successfully detect and recover the tampered area in the ROI.

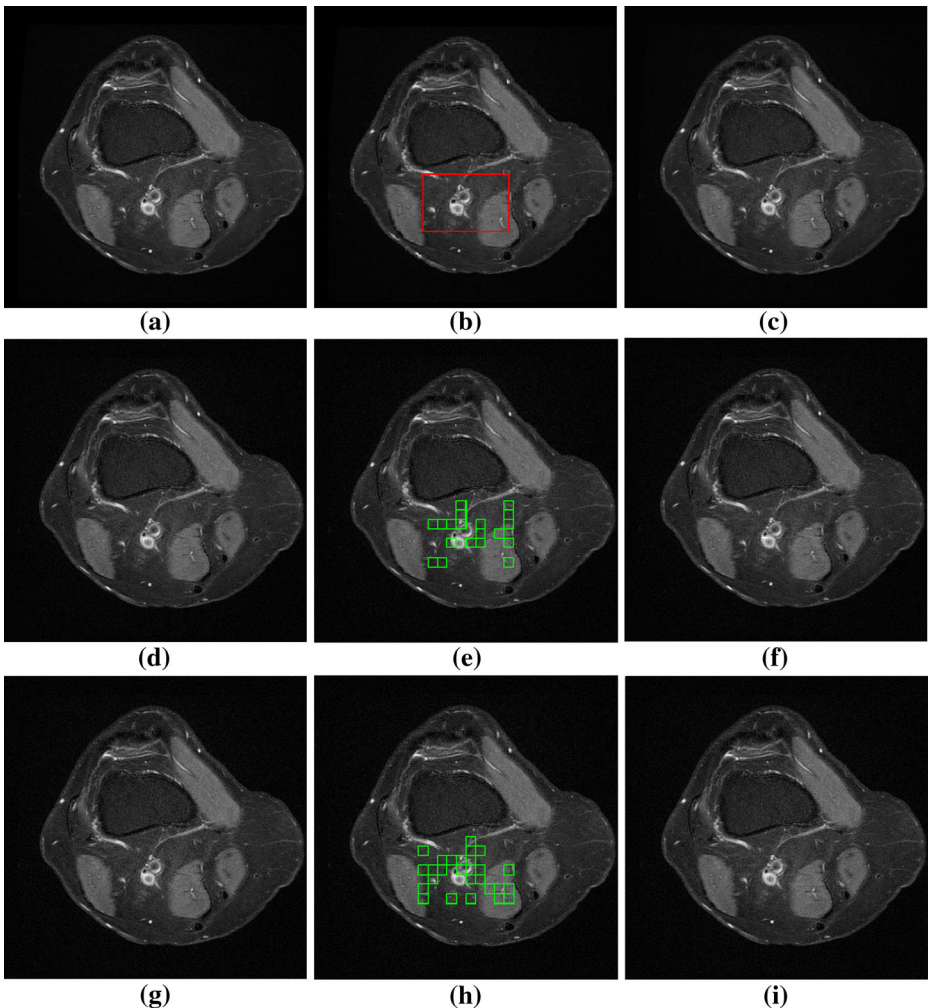


**Fig. 6** Example to demonstrate robustness against salt-and-pepper noise. **(a)** Original image, **(b)** Selected ROI, **(c)** Watermarked image, **(d)** Salt-and-Pepper (0.0005), **(e)** Localization of Salt-and-Pepper (0.0005), **(f)** Recovery of Salt-and-Pepper (0.0005), **(g)** Salt-and-Pepper (0.0008), **(h)** Localization of Salt-and-Pepper (0.0008), **(i)** Recovery of Salt-and-Pepper (0.0008)

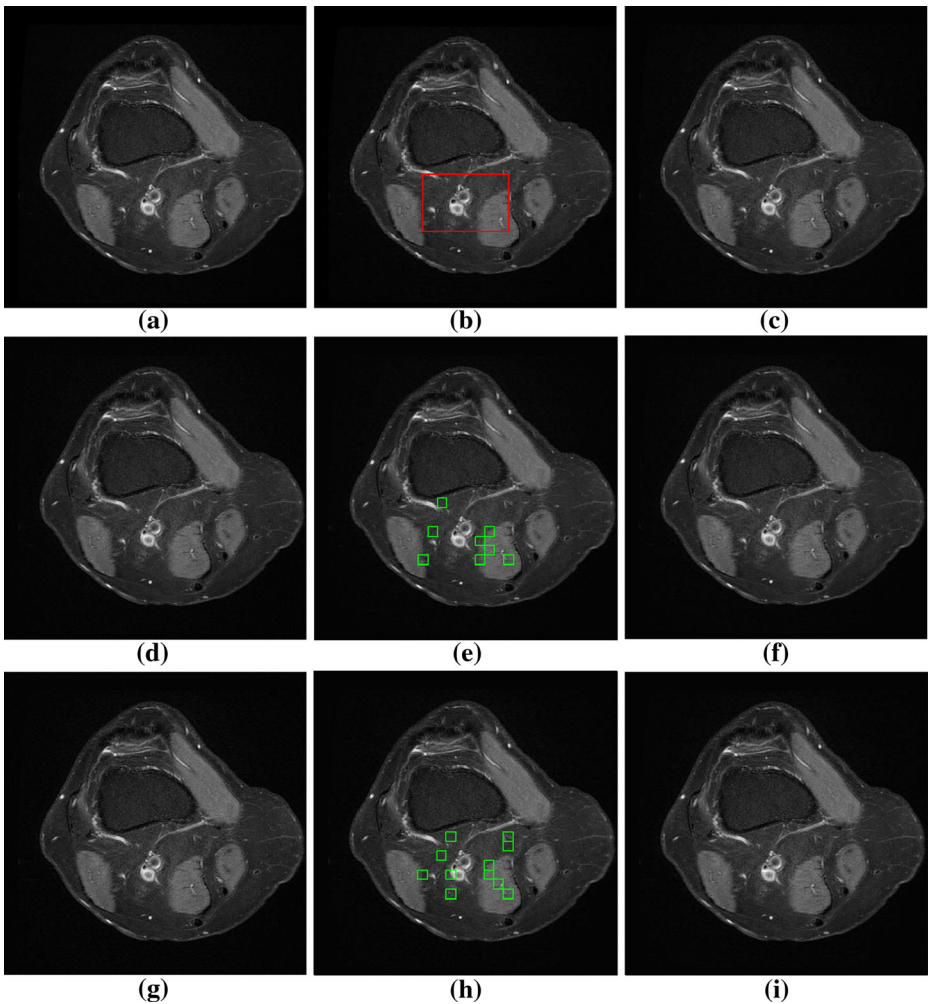


### 3.3 Robustness test

The robustness of the proposed scheme has been tested against unintentional attacks (i.e., adding noise and image compression). Figure 6 shows the robustness of the proposed scheme against salt-and-pepper noise, which illustrates that the scheme can successfully localize the noise, and recover the blocks that have noise. Figure 7 shows the robustness results against AGN and Fig. 8 shows the robustness results against JPEG compression. In addition, the performance of the proposed scheme has been tested when tampering and attacks have been imposed on the watermarked image. Figure 9 shows the results when copy-paste and salt and pepper noise have been occurred. Figure 10 shows the results when copy-paste and JPEG compression have been occurred. As shown in the results, the proposed authentication scheme can localize the tampered area and the attacks in the ROI and can successfully apply the recovery process.



**Fig. 7** Example to demonstrate robustness against AGN noise. (a) Original image, (b) Selected ROI, (c) Watermarked image, (d) AGN (0, 0.0005), (e) Localization of AGN (0, 0.0005), (f) Recovery of AGN (0, 0.0005), (g) AGN (0, 0.0008), (h) Localization of AGN (0, 0.0008), (i) Recovery of AGN (0, 0.0008)

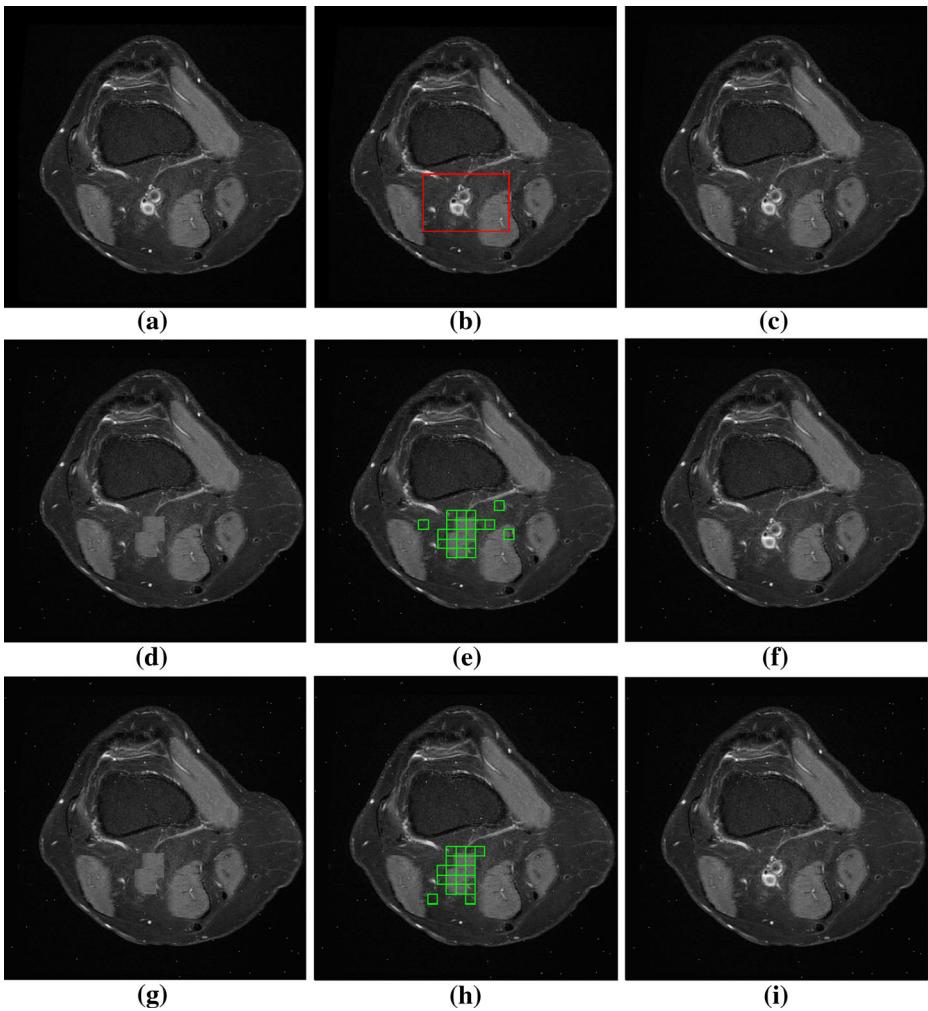


**Fig. 8** Example to demonstrate robustness against JPEG compression. (a) Original image, (b) Selected ROI, (c) Watermarked image, (d) JPEG 80 %, (e) Localization of JPEG 80 %, (f) Recovery of JPEG 80 %, (g) JPEG 70 %, (h) Localization of JPEG 70 %, (i) Recovery of JPEG 70 %

### 3.4 Comparison with previous authentication schemes

The characteristics of the proposed authentication scheme can be summarized as follows:

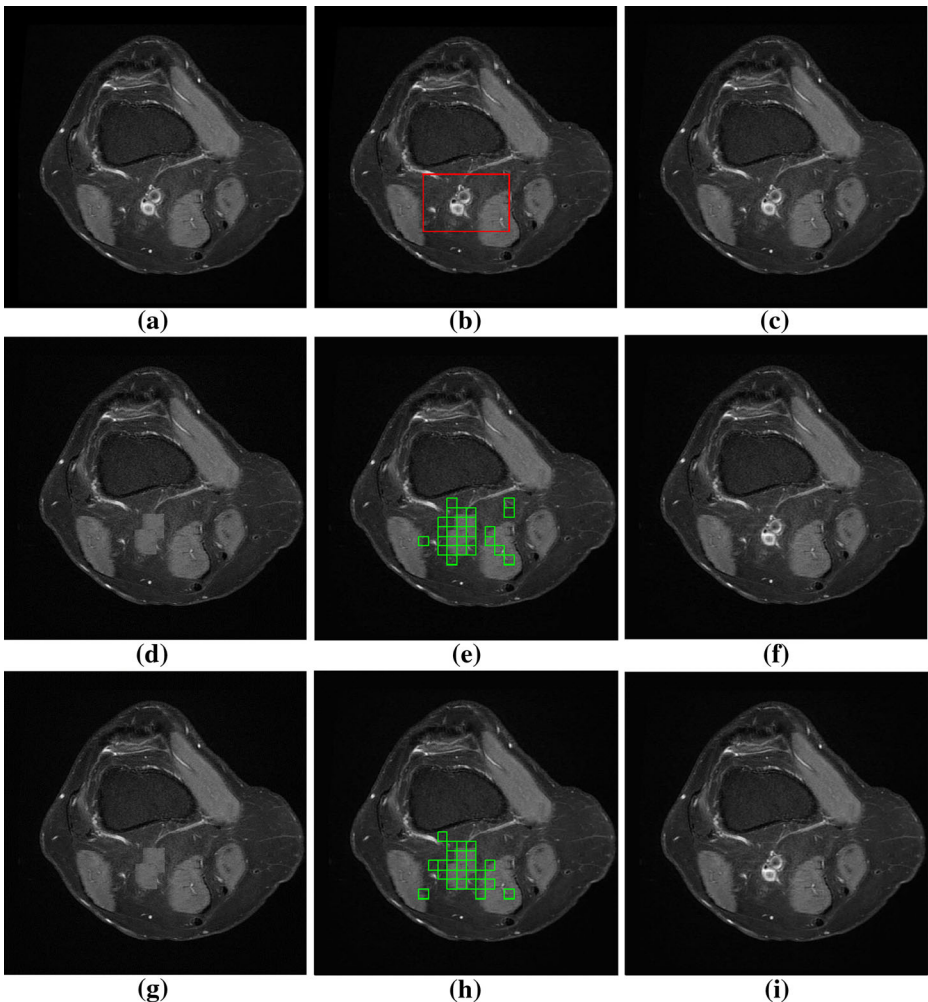
- 1) The scheme can be used for tamper detection, localization, and recovery, in addition to data hiding.
- 2) The ROI can be recovered correctly at the receiver side when the watermarked image does not change.
- 3) The ROI can be recovered with good visual quality when changes are happened in the ROI of the watermarked image.



**Fig. 9** Example 1 to demonstrate the performance when tampering and attack are occurred. (a) Original image, (b) Selected ROI, (c) Watermarked image, (d) copypaste & salt-and-pepper noise (0.0005), (e) Localization of copy-paste & salt-and-pepper noise (0.0005), (f) Recovery of copy-paste & salt-and-pepper noise (0.0005), (g) copy-paste & salt-and-pepper noise (0.0008), (h) Localization of copy-paste & salt-and-pepper noise (0.0008), (i) Recovery of copy-paste & salt-and-pepper noise (0.0008)

- 4) The scheme has robustness against unintentional attacks, which makes the scheme more suitable for the practical applications.

General comparisons between the proposed authentication scheme and the previous authentication schemes are shown in Tables 4 and 5. As shown in the tables, the proposed scheme performs better than the schemes in [7–9, 12, 17, 22, 25] in terms of tamper localization because the schemes in [7–9, 12, 17, 22, 25] can detect tampering in the image but cannot localize the tampered area.



**Fig. 10** Example 2 to demonstrate the performance when tamper and attack are occurred. **(a)** Original image, **(b)** Selected ROI, **(c)** Watermarked image, **(d)** copy-paste & JPEG 80 %, **(e)** Localization of copy-paste & JPEG 80 %, **(f)** Recovery of copy-paste & JPEG 80 %, **(g)** copy-paste & JPEG 70 %, **(h)** Localization of copy-paste & JPEG 70 %, **(i)** Recovery of copy-paste & JPEG 70 %

In terms of tamper recovery, the proposed scheme performs better than the schemes in [7–9, 12, 17, 22, 25] because these schemes cannot recover the tampered area. The schemes in [2, 3, 6, 10, 23, 26, 27] can recover the tampered area but the visual quality of the recovered image using the proposed scheme is better in comparison with [2, 3, 6, 10, 23, 26, 27], which has been proved in the experiments and results of (section 2.1.2, Table 2).

In terms of reversibility, the proposed scheme is better in comparison with the schemes in [7–9, 12, 22, 27] because these schemes are irreversible (i.e., the original image cannot be recovered even when the image does not undergone any attack). In terms of robustness, the proposed scheme is robust against JPEG compression, AGN, and salt & pepper noise; therefore, the proposed scheme is better than all the compared schemes in [2, 3, 6–10, 12,

**Table 4** Comparison 1 between the proposed authentication scheme and the previous authentication schemes

Scheme	Objectives	ROI-based	Embedding technique	Embedded data
Woo et al. (2005) [22]	Authentication and data hiding	×	LSB+DWT	Authentication and patient's data.
Giakoumaki et al. (2006) [7, 8]	Authentication and data hiding	✓	Transform domain DWT	Authentication and patient's data.
Zain and Fauzi (2006) [26]	Authentication	×	Spatial domain LSB	Authentication and recovery data.
Zain and Clarke (2007) [25]	Authentication	✓	Spatial domain LSB	Authentication data.
Zain and Fauzi (2007) [27]	Authentication	✓	Spatial domain LSB	Authentication and recovery data.
Chiang et al. (2008) [6]	Authentication	×	Modified DE	Authentication and recovery data.
Wu et al. (2008) (1) [23]	Authentication	×	Transform domain DCT	Authentication and recovery data.
Wu et al. (2008) (2) [23]	Authentication	✓	Transform domain DCT	Authentication and recovery data.
Guo and Zhuang (2009) [9]	Authentication and data hiding	✓	Modified DE	Authentication and patient's data.
Al-Qershi and Khoo (2009) [2]	Authentication and data hiding	✓	Modified DE+DE	Authentication, recovery, and patient's data.
Memon (2010) [12]	Authentication and data hiding	✓	Spatial domain LSB	Authentication and patient's data.
Al-Qershi and Khoo (2011) [3]	Authentication and data hiding	✓	Modified DE+DWT	Authentication, recovery, and patient's data.
Kulkarni and Patil (2012) [10]	Authentication and data hiding	✓	DE	Authentication, recovery, and patient's data.
Naseem et al. (2013) [17]	Authentication	✓	Spatial domain LSB	Authentication data.
Proposed scheme	Authentication and data hiding	✓	Transform domain SLT	Authentication, recovery, and patient's data.

**Table 5** Comparison 2 between the proposed authentication scheme and the previous authentication schemes

Scheme	Tamper localization	Tamper recovery	Reversibility	Robustness
Woo et al. (2005) [22]	×	×	×	Fragile. Only the data in the border may survive certain attacks
Giakoumaki et al. (2006) [7, 8]	×	×	×	Robust against JPEG compression
Zain and Fauzi (2006) [26]	√	Average of 4×4 blocks	×	Fragile
Zain and Clarke (2007) [25]	×	×	√	Fragile
Zain and Fauzi (2007) [27]	√	Average of 2×2 blocks	×	Fragile
Chiang et al. (2008) [6]	√	Average of 4×4 blocks	√	Fragile
Wu et al. (2008) (1) [23]	√	JPEG compression of the blocks	√	Not tested
Wu et al. (2008) (2) [23]	√	JPEG compression of the blocks	√	Not tested
Guo and Zhuang (2009) [9]	×	×	√	Fragile
Al-Qershi and Khoo (2009) [2]	√	JPEG2000 of the ROI	Only ROI	Fragile
Memon (2010) [12]	×	×	×	Fragile
Al-Qershi and Khoo (2011) [3]	√	JPEG2000 of the ROI	Only ROI	Shows robustness against salt&pepper noise.
Kulkarni and Patil (2012) [10]	√	Average of 4×4 blocks	Only ROI	Fragile
Naseem et al. (2013) [17]	×	×	Only ROI	Fragile
Proposed scheme	√	Selected and modified IWT coefficients of the ROI	Only ROI	Shows robustness against JPEG compression, AGN, and salt & pepper noise.

17, 22, 23, 25–27]. As shown in Table 5, the majority of the previous schemes are fragile while some schemes got robustness against only one type of attacks.

## 4 Conclusions

This paper presents a new medical image authentication scheme based on Slantlet transform watermarking methods. In the proposed scheme, a new method has been suggested to generate the recovery information of the ROI, which is based on the integer wavelet transform coefficients. The proposed method reduces the recovery information, gives good visual quality of the recovered ROI, and provides the ability to implement a robust medical image authentication scheme. A robust reversible watermarking scheme has been used to embed data in the ROI in order to ensure the reversibility of the ROI at the receiver side. A robust irreversible watermarking scheme based on SLT matrix has been used to embed data in the RONI to improve the capacity and give robustness at the same time. The experimental results prove the efficiency of the proposed scheme in detecting and recovering the tampered area in the ROI. The proposed authentication scheme is more suitable for the practical applications in comparison with the previous schemes because it has robustness against unintentional attacks, in addition, it can recover the ROI with good visual quality. The scheme has been implemented

and applied for the medical images that have 8-bit depth. For the future work, some adjustments in the scheme can be conducted to apply it for images with different bit depth (e.g., some medical images have 12-bit depth or 16-bit depth). For instance, in case of 16-bit depth the pixel values range is [0 to 65,535] which should be considered while conducting the adjustments of the scheme. In addition, an extensive study of the IWT coefficients for this type of images should be conducted in order to find out the best type of IWT that can be applied.

## References

1. Abokhdair NO, Manaf ABA (2013) “A review of reversible watermarking properties, applications, and techniques for medical images,” 6th International Conference on Information Technology ICIT, Amman, Jordan
2. Al-Qershi OM, and Khoo BE (2009) “Authentication and data hiding using a reversible ROI-based watermarking scheme for DICOM images,” *Int Conf Med Syst Eng (ICMSE)* 829–834
3. Al-Qershi OM, Khoo BE (2011) Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images. *J Digit Imaging* 24(1):114–125
4. An L, Gao X, Li X, Tao D, Deng C, Li J (2012) Robust reversible watermarking via clustering and enhanced pixel-wise masking. *IEEE Trans Image Process* 21(8):3598–3611
5. An L, Gao X, Yuan Y, Tao D (2012) “Robust lossless data hiding using clustering and statistical quantity histogram. *Neurocomputing* 77(1):1–11
6. Chiang K, Chang-Chien K, Chang R, Yen H (2008) Tamper detection and restoring system for medical images using wavelet-based reversible data embedding. *J Digit Imaging* 21(1):77–90
7. Giakoumaki A, Pavlopoulos S, Koutsouris D (2006) Multiple image watermarking applied to health information management. *IEEE Trans Inf Technol Biomed* 10(4):722–732
8. Giakoumaki A, Pavlopoulos S, Koutsouris D (2006) Secure and efficient health data management through multiple watermarking on medical images. *Med Biol Eng Comput* 44(8):619–631
9. 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
10. Kulkarni MB, Patil RT (2012) Tamper detection & recovery in medical image with secure data hiding using reversible watermarking. *Int J Emerg Technol Adv Eng* 2(3):370–373
11. Kundur D and Hatzinakos D (1999) “Digital watermarking for telltale tamper proofing and authentication,” *Proc IEEE*
12. Memon NA (2010) “Watermarking of medical images for content authentication and copyright protection,” Ph.D. Thesis, Ghulam Ishaq Khan Institute of Engineering Science and Technology
13. Memon NA, Gilani SA (2011) Watermarking of chest CT scan medical images for content authentication. *Int J Comput Math* 88(2):265–280
14. Memon NA, Gilani SAM and Ali A (2009) “Watermarking of chest CT scan medical images for content authentication,” *Int Conf Inform Commun Technol, ICICT* 175–180
15. Mohammed RT and Khoo BE (2012) “Image watermarking using slantlet transform,” *IEEE Symp Indust Electron Applic (ISIEA)* 281–286
16. Mostafa S, El-sheimy N, Tolba A, Abdelkader F, Elhindy H (2010) Wavelet packets-based blind watermarking for medical image management. *Open Biomed Eng J* 4:93–98
17. Naseem MT, Qureshi IM, Cheema TA, Atta-ur-Rahman (2013) Hash based medical image authentication and recovery using chaos and residue number system. *J Basic Appl Sci Res* 3(6):488–495
18. Nayak J, Bhat P, Kumar M, and Acharya U (2004) “Reliable transmission and storage of medical images with patient information using error control codes,” *India Ann Conf, Proc IEEE INDICON* 147–150
19. Thabit R, Khoo BE (2014) Robust reversible watermarking scheme using slantlet transform matrix. *J Syst Softw* 88:74–86
20. Thabit R, Khoo BE (2015) A new robust lossless data hiding scheme and its application to color medical images. *Digit Sign Process* 38:77–94
21. Tian J (2003) Reversible data embedding using a difference expansion. *IEEE Trans Circ Syst Video Technol* 13(8):890–896
22. Woo C, Du J, and Pham B (2005) “Multiple watermark method for privacy control and tamper detection in medical images,” *Proc APRS Workshop Digit Imag Comput Pattern Recognit Imag Med Applic* 43–48
23. Wu J, Chang R, Chen C, Wang C, Kuo T, Moon W, Chen D (2008) Tamper detection and recovery for medical images using near lossless information hiding technique. *J Digit Imaging* 21:59–76

24. Zain J, Baldwin L and Clarke M (2004) “Reversible watermarking for authentication of DICOM images,” Proc 26th Ann Int Conf IEEE Eng Med Biol Soc
25. Zain J, Clarke M (2007) Reversible region of non-interest (RONI) watermarking for authentication of DICOM images. *Int J Comput Sci Network Sec* 7(9):19–28
26. Zain J, and Fauzi A (2006) “Medical image watermarking with tamper detection and recovery,” Proc 28th IEEE EMBS Ann Int Conf 3270–3273
27. Zain J, and Fauzi A (2007) “Evaluation of medical image watermarking with tamper detection and recovery (AW-TDR),” 29th Ann Int Conf IEEE Eng Med Biol Soc (EMBS) 5661–5664



**Rasha Thabit** received her B.Sc. degree in Electronics and Communications Engineering from University of Baghdad, Iraq, in 2006, and M.Sc. degree in Electrical Engineering from University of Baghdad, Iraq, in 2008. She received her Ph.D. degree in Software Engineering from the School of Electrical & Electronic Engineering at Universiti Sains Malaysia (University of Science, Malaysia), in 2015. Her research interest is in the area of data hiding, digital image watermarking, and digital signal processing.



**Bee Ee Khoo** received the B.Tech degree in Quality Control and Instrumentation from Universiti Sains Malaysia in 1993, and Ph.D degree in Electrical Engineering from University of Wales, Swansea in 1998. She is currently Associate Professor at the School of Electrical and Electronic Engineering, Universiti Sains Malaysia. Her current research interests include digital watermarking, computer vision and multimedia forensics.