

# Crypto-Watermarking of Transmitted Medical Images

Ali Al-Haj<sup>1</sup> · Ahmad Mohammad<sup>2</sup> · Alaa' Amer<sup>3</sup>

Published online: 25 August 2016  
© Society for Imaging Informatics in Medicine 2016

**Abstract** Telemedicine is a booming healthcare practice that has facilitated the exchange of medical data and expertise between healthcare entities. However, the widespread use of telemedicine applications requires a secured scheme to guarantee confidentiality and verify authenticity and integrity of exchanged medical data. In this paper, we describe a region-based, crypto-watermarking algorithm capable of providing confidentiality, authenticity, and integrity for medical images of different modalities. The proposed algorithm provides authenticity by embedding robust watermarks in images' region of non-interest using SVD in the DWT domain. Integrity is provided in two levels: strict integrity implemented by a cryptographic hash watermark, and content-based integrity implemented by a symmetric encryption-based tamper localization scheme. Confidentiality is achieved as a byproduct of hiding patient's data in the image. Performance of the algorithm was evaluated with respect to imperceptibility, robustness, capacity, and tamper localization, using different medical images.

The results showed the effectiveness of the algorithm in providing security for telemedicine applications.

**Keywords** Digital watermarking · Telemedicine security · Confidentiality · Authenticity · Integrity · Tamper localization · DICOM standard · DWT · SVD

## Introduction

Digital information systems have been increasingly deployed in modern healthcare environments in the last decades. In fact, many hospital and healthcare centers around the world rely in their operation on hospital information systems (HIS), radiology information systems (RIS), and picture archiving and communication systems (PACS), among many other information and communications technology systems [1–3]. The availability of such systems facilitated sharing medical images and electronic patient records among clinicians and radiologists for telemedicine applications such as teleconsulting, telediagnosis, and telesurgery. Despite such innovative advancements, it is fairly easy for malicious adversary to intercept and tamper transmitted images when public networks are used. It is thus of a paramount importance to implement secured medical transfer schemes in order to achieve the wide range of benefits offered by telemedicine applications [4].

To secure the exchange of medical images between healthcare entities, telemedicine implementations must provide three security services: confidentiality, authenticity, and integrity [5, 6]. Confidentiality ensures that only authorized users have access to the transmitted image, whereas integrity verifies that the received image has not been manipulated by unauthorized users. Authenticity, on the other hand, proves that the received image comes from the correct source and belongs to the correct patient. These three services must be

---

✉ Ali Al-Haj  
ali@psut.edu.jo

Ahmad Mohammad  
atawayha@psut.edu.jo

Alaa' Amer  
searchds@gmail.com

<sup>1</sup> Department of Computer Engineering, King Abdullah II Faculty of Engineering, Princess Sumaya University for Technology, Al-Jubeiha, P.O. BOX 1438, Amman 11941, Jordan

<sup>2</sup> Department of Electrical Engineering, King Abdullah II Faculty of Engineering, Princess Sumaya University for Technology, Al-Jubeiha, P.O. BOX 1438, Amman 11941, Jordan

<sup>3</sup> Ideal Solutions, Ahmad Bin Ali Street, Doha 20851, Qatar

offered simultaneously to achieve reliable and secured telemedicine applications. Currently, cryptography and digital watermarking technologies are used to provide these security services [7, 8].

Cryptography is the approach adopted in the digital imaging and communications in medicine (DICOM) standard which uses symmetric encryption, hashing functions, and digital signatures to provide integrity and authenticity [9–11]. However, a major limitation of pure cryptography is that the loss or deletion of the attached digital signature makes the image untrustworthy and thus it becomes hard to verify its integrity and authenticity. This suggests that cryptography can only be used as a priori protection mechanism. On the other hand, pure watermarking methods achieve security in telemedicine by using robust and fragile watermarks [12–14]. Robust watermarks are characterized by their resistance to common signal processing and malicious attacks; thus, they are appropriate for ownership verification and identity authentication. On the other hand, fragile watermarks do not survive signal processing attacks, making them appropriate for data integrity control and tamper detection.

To utilize the combined benefits of the two approaches, crypto-watermarking algorithms have been proposed in literature to address the security requirements of telemedicine applications [15–18]. In the hybrid approach, watermarking is used as the implementation platform, and integrity and authenticity are implemented using cryptographic watermarks such as hash codes, cyclic redundancy codes (CRCs), and digital signatures. These cryptographic watermarks are embedded as robust or fragile watermarks depending on the required security service. That is, hash codes are commonly used to provide strict integrity of the medical image, whereas CRCs are more appropriately used to detect tampered areas in the image.

Different types of crypto-watermarking methods have been proposed in literature to provide security for exchanged medical images. These methods can be classified into three categories: irreversible methods, reversible methods, and region-based methods. The three types often involve a tradeoff between imperceptibility, robustness, and capacity. The irreversible watermarking methods are lossy in nature as they introduce permanent alterations to the original images even after the extraction of the embedded watermarks [17–19]. Reversible methods, on the other hand, are lossless since they retain the original image after extracting the embedded watermarks [20–25]. The third category is the region-based methods which involve segmenting the original medical image into two areas: region of interest (ROI) and region of non-interest (RONI). Embedding in either region can be done using non-reversible or reversible watermarking techniques [20, 26, 27].

In this paper, we propose a crypto-watermarking algorithm that uses multiple watermarks to provide authenticity, integrity, and confidentiality for medical images exchanged over public networks. The algorithm uses two robust watermarks

representing the patient's personal data and the hospital's logo to implement authenticity. The two watermarks are embedded in the RONI of the image using singular value decomposition (SVD) in the discrete wavelets transform (DWT) domain. A cryptographic watermark representing the hash of the ROI of the image is also embedded in the RONI to provide strict integrity. Additionally, the algorithm provides content-based integrity of the ROI by incorporating a tamper localization scheme. The ROI of the image is encrypted before transmission to achieve confidentiality, and to achieve content-based integrity by localizing tampered blocks at the receiver's side. Therefore, the uniqueness of the proposed algorithm is of twofolds. The first is in providing two levels of integrity verification: strict and content-based integrity of the image ROI, and the second by using symmetric encryption to provide confidentiality and tamper localization of the same region.

The paper is organized as follows. “Literature Survey” section describes recent research work in the area of secured telemedicine. “Image Preprocessing” section describes the process of segmenting the image into ROI/RONI zones and assigning the relevant watermarks to each region. The DWT-SVD watermarking algorithm, which incorporates the localized tamper detection functionality, is described in “Watermarking Procedures” section. Performance of the algorithm is evaluated in “Performance Results Analysis” section. Concluding remarks are given in “Conclusions” section.

## Literature Survey

A few region-based medical image watermarking algorithms with tamper localization functionality have been proposed in literature. Liew et al. [28, 29] proposed a ROI/RONI algorithm in which the ROI is segmented into blocks of  $40 \times 40$  pixels and the RONI into blocks of  $2 \times 2$  pixels. The RONI is further divided into one area for authentication information embedding and one area for recovery information embedding. Tamper localization is implemented by computing the cyclic redundancy check (CRC) and hash functions of the ROI blocks, and embedding the resultant digest values in the form of watermarks in RONI. For recovery, the ROI is compressed using JPEG 2000 and embedded in RONI as a robust watermark using a 3-level DWT.

Al-Qershi and Khoo [30] proposed a scheme that divides the images into a ROI and a RONI. Patient's data are embedded into the ROI using a reversible technique based on difference expansion, while tamper detection and recovery data are embedded into the RONI using a robust technique based on discrete wavelet transform. Tampering is detected locally at the block level by comparing the average value of each block in the ROI with the retrieved average value from the watermark. Tampered blocks are recovered and replaced with a lossy compressed ROI embedded as a watermark.

Guo and Zhuang [31] proposed a watermarking scheme with tamper localization capability based on difference expansion. The scheme introduces the concept of region of authentication (ROA) which can be flexibly partitioned into small regions as an image block or polygonal region in a multilevel hierarchical manner. A hashing function is used to produce digital signatures for each image block, which are then added to the watermark payload. To verify authenticity of the image, the signatures for the ROA are compared to detect any tampering. Tamper localization is implemented using the concept of ROI shading.

Tan et al. [32] proposed dual-layer watermarking scheme in which the tamper localization function was implemented by dividing the original image into  $16 \times 16$  pixel blocks and computing the CRC for each block. Each CRC is embedded into its own block. In the event that the CRC cannot be embedded into its own block, the remaining bits are carried over to the next block. Tampering is localized by extracting the watermark and comparing the CRC of each block. If both CRCs do not match, the block will be identified as being tampered, hence achieving tamper localization.

A major drawback of the proposed algorithms is their extensive usage of cryptographic CRC watermarks to implement the tamper localization functionality. Other than being computation-intensive, the algorithms provide no evidence these cryptographic watermarks were extracted intact at the receiver side. Since a 1-bit change in a CRC or hash code will lead to a false localized tamper detection, extensive use of these cryptographic primitives is considered a major limitation of the proposed algorithms. Another drawback is the lack of evidence about robustness of the watermarks embedded in the RONI. In other words, the robustness of the algorithms was not evaluated properly using standard metrics such as normalized correlation and bit error rates to prove that the cryptographic watermarks could survive attacks such as additive noise and lossy compression.

## Image Preprocessing

A major process in the proposed region-based watermarking algorithm is to separate the image into ROI/RONI regions, transform the segmented image into the frequency domain, and assign the watermarks to the different multi-resolution sub-bands. This process is described in the following subsections.

### ROI/RONI Segmentation

The proposed watermarking algorithm is based on a region-selecting property to allow for localizing tampered regions in manipulated exchanged images. The region-selecting function, performed by a radiologist or a computer aided tool

[33], separates the given medical image into two non-overlapping zones: region of interest (ROI) and region of non-interest (RONI). The ROI zone contains the significant information that the physicians utilize for diagnosis. Therefore, this region may not be used for watermark embedding in order to preserve its integrity and to prevent any compromise on the diagnostic value of the image. Since the RONI zone does not contribute to diagnosis, its integrity does not need to be preserved and thus it can be used for the insertion of robust watermarks. The size and shape of the two regions vary according to the modality and nature of the medical image. Figure 1a shows a generic medical image diagram partitioned into non-overlapping blocks, with the ROI and RONI zones separated by a polygon.

### DWT Sub-band Decomposition

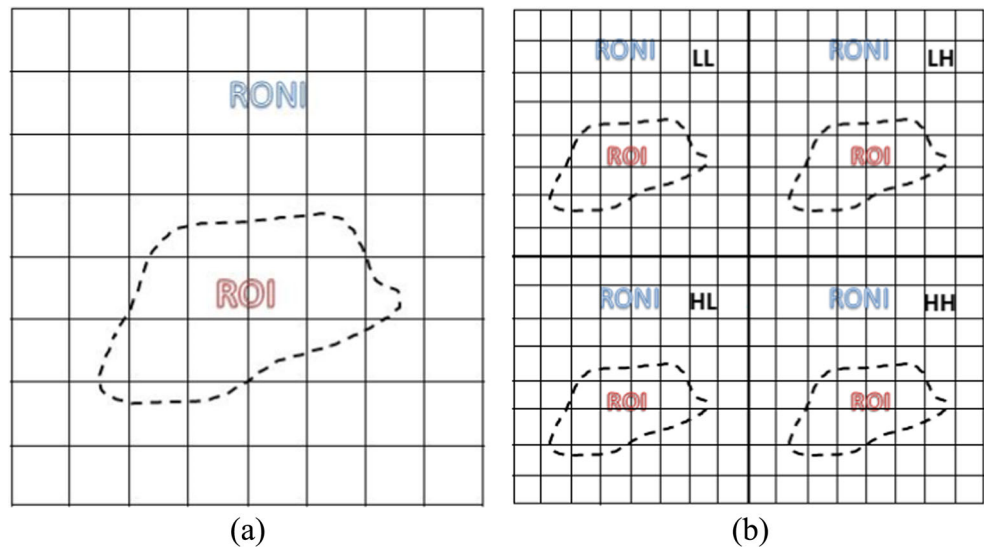
For effective watermarking, the segmented image is transformed into the frequency domain using a 1-level discrete wavelet transform (DWT). Four non-overlapping sub-bands are generated: LL, LH, HL, and HH. The ROI and RONI segmentation in each sub-band is defined by applying the ROI mapping procedure described in [34]. According to this mapping procedure, the ROI coordinates in each sub-band are derived from the spatial domain ROI coordinates based on the spatial self-similarity between the sub-bands. The four sub-bands with their ROI/RONI segmentations are shown in Fig. 1b.

### Watermarks Generation and Assignment

Multiple watermarks are generated to address the different security requirements of medical image transmission. Two watermarks are used to authenticate the ownership and source of origin of the image, and a cryptographic hash watermark is used to verify the strict integrity of the ROI of the image. The three watermarks and their pre-assigned embedding locations are described below.

1. The *patient information watermark* is a  $204 \times 96$  binary image generated from several attributes of a sample patient's record, as shown in Fig. 2a. The 19,584-bit robust watermark serves for image ownership authentication and is embedded in the LH sub-band.
2. The *hospital logo watermark* is an  $81 \times 50$  binary image shown in Fig. 2b. The 4050-bit robust watermark is used to authenticate the source of origin of the image, and it is embedded in the HL sub-band.
3. The *ROI hash watermark* is a SHA-256 digest of the ROI of an MRI brain image. The 256-bit ROI hash watermark is formulated as the 2D image given in Fig. 2c. The watermark is used to verify the strict integrity of the ROI of the image, and is embedded in the HH sub-band.

**Fig. 1** **a** ROI/RONI segmentation and block-based partitioning of a generic medical image diagram. **b** 1-level DWT decomposition of the segmented image



**Watermarking Procedures**

The proposed watermarking algorithm consists of three procedures: watermark embedding, watermark extraction, and integrity verification procedures. The first procedure embeds the authenticity and integrity watermarks into the RONI, while the second extracts the watermarks from the same

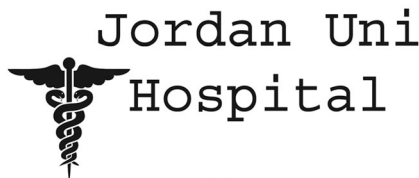
region at the receiving end. The third procedure verifies the integrity of the received image, and detects tampered blocks in the ROI of the image.

**Watermark Embedding Procedure**

The embedding procedure inserts the bit-patterns of the three watermarks in the RONI of each sub-band according to the following assignment: the patient information watermark in the LH sub-band, the hospital logo watermark in the HL sub-band HL, and the *hash watermark* in the HH sub-band. The operational steps of the procedure are depicted in Fig. 3 and described below in detail.

**Patient Name: Hazem Hazem.**  
**Age: 28 years old.**  
**Phone#: 077744500**  
**Insurance#: AC9033T**  
**Patient Illness: Bad headaches**

(a)



(b)



(c)

**Fig. 2** **a** The patient’s information watermark. **b** The hospital logo watermark. **c** The ROI hash watermark

Step 1 (*Block Watermarking*) For each block  $B_i$  in the RONI of the relevant sub-band (LH, HL, or HH), perform Step 1.1~Step 1.3 until all watermark bits are embedded.

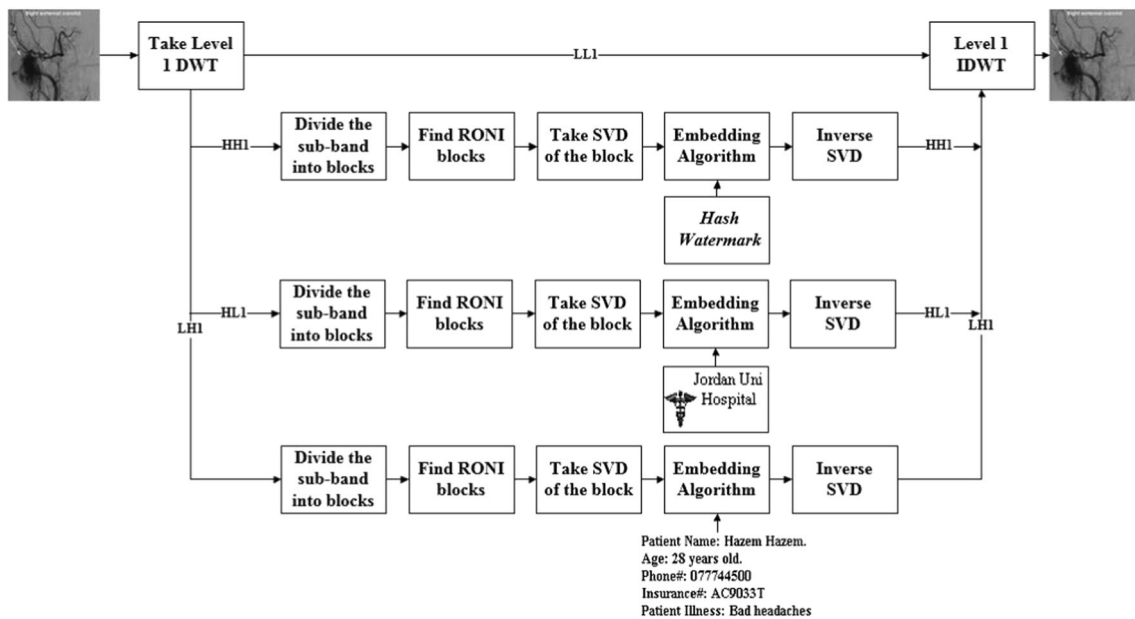
Step 1.1 (*SVD Transformation*). Apply the SVD operator on block  $B_i$ . This results in decomposing the block’s matrix into three independent matrices.

$$B_i = U_{B_i} S_{B_i} V_{B_i}^T \tag{1}$$

Step 1.2 (*LSB Embedding*) Embed a single watermark bit into the upper element of the diagonal matrix  $S_{B_i}$  by substituting the watermark bit  $W_i$  with its least significant bit (LSB).

$$LSB(S_{B_i}(0, 0)) = W_i \tag{2}$$

The LSB substitution is done by taking the integer value of  $S_{B_i}(0,0)$ , preserving the fraction, placing the watermark bit at the LSB position of the integer, and adding the preserved fraction to the modified integer.



**Fig. 3** The RONI watermark embedding procedure

Step 1.3 (*Inverse SVD*) Apply the inverse SVD operator using the modified  $S_{Bi}$ ' matrix to get the watermarked block  $B_i'$ .

$$B_i' = U_{Bi} S_{Bi}' V_{Bi}^T \quad (3)$$

Step 2 (*Inverse DWT*) After embedding the three watermarks in sub-bands  $HL$ ,  $LH$ , and  $HH$ , apply the inverse DWT operation on the whole image to produce the final watermarked image  $I'$ .

### Watermark Extraction Procedure

The proposed algorithm is blind in the sense that it does not require the original medical image in the extraction process. Therefore, the three watermarks are extracted blindly from the LSBs of the watermarked RONI blocks of each sub-band. The procedure is shown in Fig. 4 and described in detail in the steps that follow.

Step 1 (*DWT Decomposition*) Compute the 1-level DWT for the watermarked image  $I'$ . Four non-overlapping sub-bands are produced:  $wLL_1$ ,  $wLH$ ,  $wHL$ , and  $wHH$ .

Step 2 (*ROI/RONI Segmentation*) Define the ROI and RONI zones in each sub-band by applying the ROI mapping procedure described in [34].

Step 3 (*Sub-band Partitioning*) Partition each sub-band into non-overlapping blocks, as shown in Fig. 1b.

Step 4 (*Watermarks Extraction*) For each block  $B_i'$  in the RONI of the relevant sub-band, perform Step 4.1~Step 4.3 until all watermark bits are extracted.

Step 4.1 (*SVD Transformation*) Apply the SVD operator on watermarked block  $B_i'$ . This results in decomposing the block's matrix into three independent matrices.

$$B_i' = U_{Bi} S_{Bi}' V_{Bi}^T \quad (4)$$

Step 4.2 (*LSB Extraction*) Extract the embedded watermark bits from the upper diagonal element of  $S_{Bi}'$  as follows.

$$W_i' = LSB(S_{Bi}'(0, 0)) \quad (5)$$

The LSB extraction is done by taking the integer value of the  $S_{Bi}'$  element and retrieving the watermark bit at the LSB position of the integer.

Step 5 (*Watermarks Reconstruction*) Reconstruct the three watermark patterns by merging all extracted watermark bits from the RONI blocks of each sub-band.

Step 6 (*Image Authentication*) The physicians at the receiving side authenticate the image in terms of ownership and source of origin. The image ownership is authenticated by verifying the extracted patient's information watermark. Similarly, the image source of origin is authenticated by verifying the extracted hospital logo watermark. Authentication is verified if a match exists between the received and expected or reference watermarks.

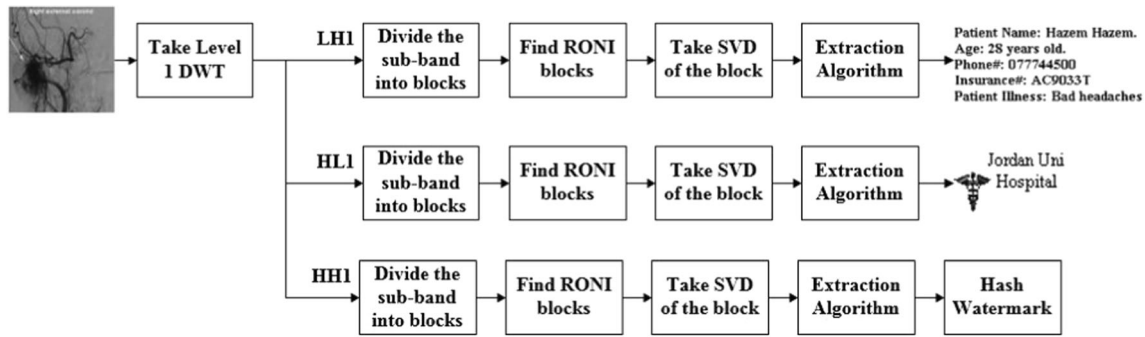


Fig. 4 RONI watermark extraction procedure

**Integrity Verification Procedure**

The physicians at the receiving side have the option of verifying the integrity of the ROI as a whole (strict integrity), or by verifying the integrity of the ROI on block-by-block basis (localized tamper detection). The integrity verification steps are described below.

Step 1 *(Strict Integrity Verification)* Compute the hash value of the ROI of the received watermarked image  $I'$  and compare it with the ROI hash watermark extracted from the RONI. If the correlation between the two hash values is higher than a preset threshold, the integrity of the ROI is verified; otherwise, the ROI is tampered. The process is illustrated in Fig. 5 for an MRI test image.

Step 2 *(Encryption-based localized tamper detection procedure)* The proposed algorithm achieves localized tamper detection using a unique encryption-based detection scheme shown in Fig. 6 and described in Step 2.1.~Step 2.4.

Step 2.1 *(ROI Encryption)* At the sender’s side, encrypt ROI using the standard encryption standard AES-CBS. The encryption process is done as follows.

- a. Formulate the whole ROI into a one-dimensional vector
- b. Divide the vector into blocks of 16 bytes (128 bits) each
- c. Apply AES-CBS on each segment using a zero initialization vector (IV)

Step 2.2 *(ROI Replacement)* Replace the plain ROI in the watermarked image with the encrypted ROI. The

step provides confidentiality for the ROI of the image.

Step 2.3 *(ROI Decryption)* At the receiver’s side, decrypt the ROI using the AES-CBS encryption standard. The decryption is applied on the encrypted 128-bit blocks of the ROI.

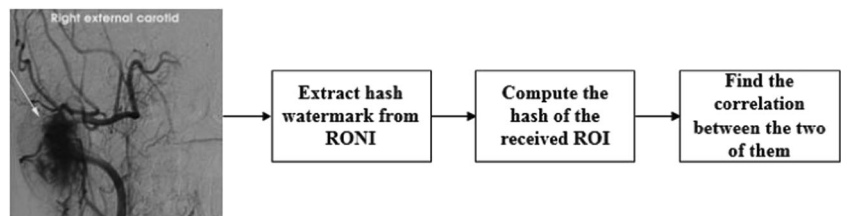
Step 2.4 *(Detection of Tampered Blocks)* A block is considered tampered if the decryption process fails to restore it to its original state. This is by virtue of the avalanche effect of the AES-CBS standard which states that any slight change in the encrypted block will lead to unsuccessful decryption to the original state of the block. The un-decrypted block can be located visually and by performing the following steps:

- a. Compute the difference between the maximum and minimum pixel values within each decrypted ROI block.
- b. Compare the difference value computed for each block against some threshold, empirically found to be 150, which corresponds to half the maximum possible pixel value. If the difference between the maximum and minimum pixel values within the block exceeds the preset threshold, then the block is considered tampered.

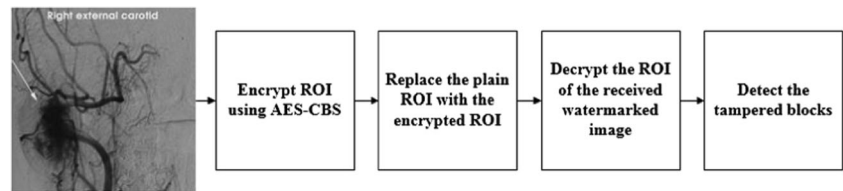
**Performance Results Analysis**

A large set of 8-bit gray-scale medical images have been used to evaluate the performance of the proposed

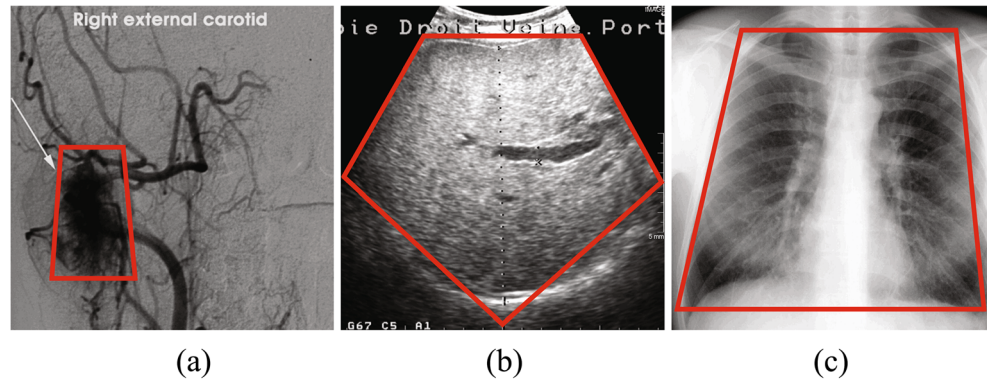
Fig. 5 Strict integrity verification of ROI of the image



**Fig. 6** Localized tamper detection procedure



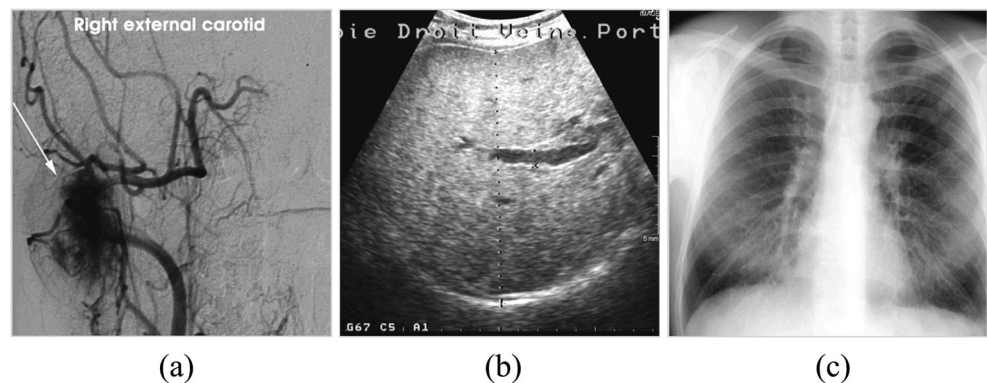
**Fig. 7** Benchmark medical images with ROIs shown in polygons. **a** MRI image, **b** ultrasound image, and **c** X-ray image



algorithm. The test images used for experimentation represent three common modalities (MRI, ultrasound, X-ray) and have different sizes ranging from the standard  $512 \times 512$  pixels to the larger  $2048 \times 2048$  pixels. The simulation results presented in this section have been obtained for the larger  $2048 \times 2048$  images since they provide higher embedding capacities.

Image segmentation of selected test images into ROI and RONI zones is shown in Fig. 7, where polygons encapsulate the ROI of each image. Description of the watermarks embedded in the RONI of each image has been given in “Image Preprocessing” section. Simulation experiments were conducted using MATLAB R2012a running on an AMD Phenom II X4 965 Processor @ 3.40 GHz. Performance results with respect to imperceptibility, robustness, localized tamper detection, and data payload are presented in the following sub-sections.

**Fig. 8** Watermarked benchmarked medical images. **a**. MRI image, **b**. ultrasound image, and **c**. X-ray image



### Imperceptibility Results

A visual subjective comparison between the original images, shown in Fig. 7, and watermarked images, shown in Fig. 8, indicates that high imperceptibility has been achieved by the proposed algorithm. For better assessment, we used the peak signal-to-noise ratio (PSNR) as an imperceptibility objective metric and obtained the following PSNR values: 35.1797, 36.6125, and 35.2988 for the MRI, ultrasound, and X-ray images, respectively.

It is instructive to note here that the achieved PSNR values are a little lower than the recommended 40 dB. However, since the PSNR metric is not an ideal objective evaluation metric, we believe that the subjective evaluation we have done to evaluate the quality of the watermarked images, alongside with the reasonably high PSNR values we obtained, demonstrate the imperceptibility exhibited by the proposed algorithm.

**Table 1** Robustness of the watermarked MRI image against additive Gaussian noise

Watermarked image	Watermarks	Correlation					
		Additive Gaussian noise mean					
		0	0.02	0.04	0.06	0.08	0.1
MRI	Patient information	0.979	0.979	0.979	0.979	0.979	0.98
	Hospital logo	0.961	0.961	0.961	0.961	0.961	0.96
	Hash	1.00	1.00	1.00	1.00	1.00	0.99

**Table 2** Robustness of the watermarked MRI image against additive salt & pepper noise

Watermarked image	Watermarks	Correlation					
		Salt and pepper density					
		0	$1 \times 10^{-6}$	$2 \times 10^{-6}$	$3 \times 10^{-6}$	$4 \times 10^{-6}$	$5 \times 10^{-6}$
MRI	Patient information	0.98	0.98	0.98	0.979	0.979	0.979
	Hospital logo	0.961	0.961	0.961	0.961	0.961	0.96
	Hash	1.00	1.00	1.00	1.00	1.00	1.00

**Robustness Results**

The transmitted medical images may undergo modifications by different types of signal processing operations. This may affect their perceived quality and corrupt the watermarks embedded within their RONIs. Therefore, we evaluated the robustness provided by the proposed algorithm against several signal processing operations: additive Gaussian noise, additive salt and pepper noise, and JPEG compression. The robustness is evaluated using the normalized correlation factor which measures the similarity between the original and extracted watermarks. It is obvious from the robustness results given in Tables 1, 2, and 3 that robustness has been achieved to that extent that authentication and verification can be done with confidence using the extracted watermarks. The *patient information* and hospital logo watermarks can be faithfully used to authenticate the ownership and source of origin of the image, and the *hash watermark* to verify the strict integrity of the ROI of the image. Similar results have been achieved for the X-ray and ultrasound images.

**Table 3** Robustness of the watermarked MRI image against JPEG compression

Watermarked image	Watermarks	Correlation					
		JPEG compression quality					
		100	96	92	88	84	80
MRI	Patient information	0.979	0.977	0.974	0.969	0.966	0.95
	Hospital logo	0.96	0.954	0.931	0.919	0.935	0.891
	Hash	1.00	1.00	1.00	1.00	1.00	0.969

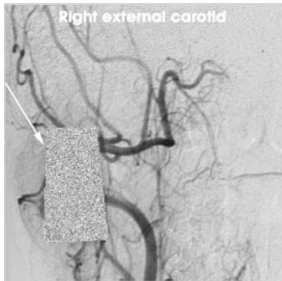
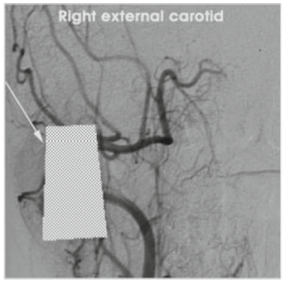
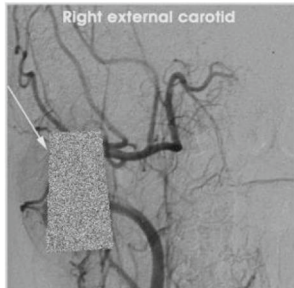
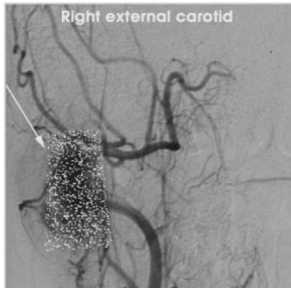
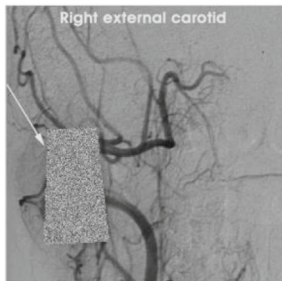
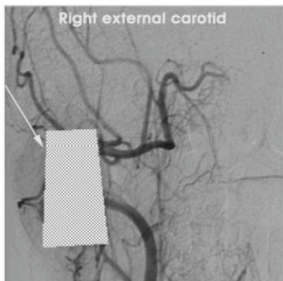
**Tamper Localization Test**

The proposed algorithm achieves content-based integrity of the transmitted image using a tamper detection and localization scheme. The scheme, as described in the previous section, encrypts the ROI of the image using the AES-CBS block cipher, and replaces the plain ROI with the encrypted ROI. At the receiver side, ROI is decrypted block-by-block, where the block size is 128 bits. A block is considered tampered if the decryption process fails to restore the block to its original state. This is by virtue of the avalanche effect inherent in AES-CBS which implies that any slight change in the encrypted block will lead to unsuccessful decryption to the original state of the block. As shown in Table 4, tampering the encrypted ROI using additive white noise, additive salt and pepper noise, and lossy JPEG compression caused the decryption process to produce random output instead of the original ROI.

To show the effectiveness of the tamper localization scheme, we slightly tampered the encrypted ROI by modifying one single bit. As shown in Table 5, the decryption process restored the encrypted ROI to its original state except for the



**Table 4** Effect of severe tampering on the decryption process

	<b>Attacked Encrypted ROI</b>	<b>Decrypted Attacked Encrypted ROI</b>
<b>Gaussian Noise (<math>\mu = 0.3</math>)</b>		
<b>Salt and Pepper Noise (<math>\rho = 0.003</math>)</b>		
<b>JPEG Compression (Q = 80)</b>		

block on which tampering was performed (as indicated by the white circles). To further explore the functionality of the scheme, two distant bits were flipped. As shown in the table, the blocks to which the bits belong were not decrypted correctly. As mentioned earlier, this encryption-based scheme provided tamper localization as well as ROI confidentiality, thus achieving two main requirements of secured telemedicine.

### Data Payload

The embedding capacity provided by the algorithm depends on size of the image, the relative size of ROI and RONI segments, block size, and number of DWT decomposition levels. According to the embedding capacity equation given below,

larger images, smaller block size, and higher DWT levels will provide higher embedding capacity. It is instructive to note here that the capacity equation has been derived in such a way that capacity calculation is confined to three sub-bands (LH, HL, HH), since sub-band (LL) has been excluded from watermark embedding.

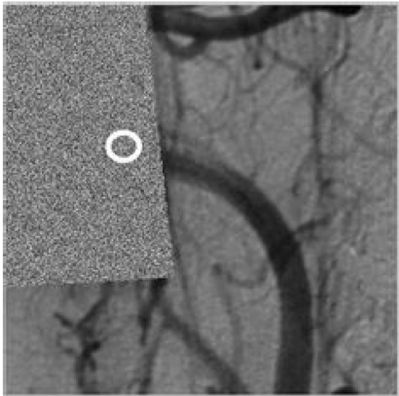
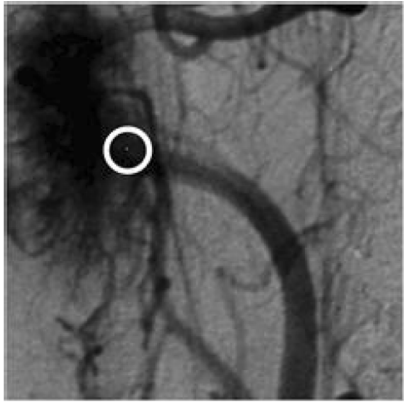
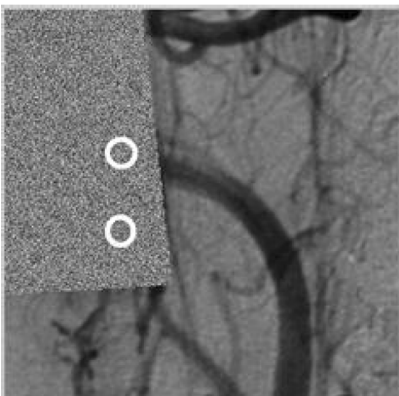
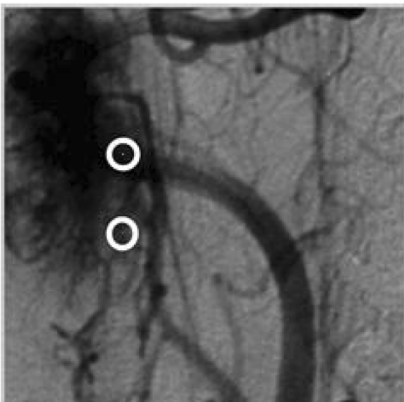
$$C = 3 \times \text{Number of Blocks} \times 4^{\text{DWT Level} - 1} \quad (6)$$

where,

$$\text{Number of Blocks} = \frac{\text{Total Image Size}}{\text{Block Size}} \quad (7)$$

Number of RONI blocks in each of the three medical images and the corresponding embedding capacities are shown in Table 6. The capacities are calculated based on the

**Table 5** Illustration of the tamper localization scheme of the algorithm

Attack Type	Locally Tampered Encrypted ROI	Tampered Block Localization in Decrypted Attacked ROI
<b>1-bit Tampering</b>		
<b>Multiple-bit Tampering</b>		

assumption that the image size is  $2048 \times 2048$ , block size  $8 \times 8$ , and DWT decomposition is performed for one level only. ROI capacities are not included in the table since the ROI of the image is not watermarked in the proposed algorithm.

As shown in Table 7, the available embedding capacity of our region-based watermarking algorithm far exceeds payload capacity needed to embed the watermarks used in the algorithm.

The capacity of a given medical image can be further increased to accommodate larger watermarks by partitioning the original image into blocks with smaller size. As an example,

**Table 6** Available watermark embedding capacity in the RONI

MRI test image	Ultrasound test image	X-ray test image
59,915 blocks	29,528 blocks	20,374 blocks
179,745 bits	88,584 bits	61,122 bits

Table 8 shows the capacity gained by partitioning the  $2048 \times 2048$  MRI image into  $8 \times 8$ ,  $4 \times 4$ , and  $2 \times 2$  blocks. The capacity gain is due to the fact that one single bit only is embedded in each block regardless of its size as we have described in the previous section.

### Comparison with Other Algorithms

In this sub-section, a performance comparison is carried out between the proposed algorithm and other region-based algorithms reported in the literature. The comparisons are made with crypto-watermarking, pure watermarking, and pure cryptographic-based algorithms.

A few region-based crypto-watermarking algorithms with tamper localization functionality have been proposed in the literature [20, 27–30]. One major drawback of the proposed algorithms is the extensive use of cryptographic watermarks, such as CRC-16 and hash codes, to implement the tamper localization functionality. Other than being computationally

**Table 7** Comparison between the available and required payload capacities

Watermark name	Watermark size (bits)	Embedding location (DWT band)	Available capacity (MRI)	Available capacity (US)	Available capacity (X-ray)
Patient's information	19,584	RONI (LH band)	59,915 bits	29,528 bits	20,374 bits
Hospital's logo	4050	RONI (HL band)	59,915 bits	29,528 bits	20,374 bits
ROI hash	256	RONI (HH band)	59,915 bits	29,528 bits	20,374 bits

**Table 8** The available payload capacity as a function of block size

Block size	8 × 8 blocks	4 × 4 blocks	2 × 2 blocks
Number of RONI blocks	59,915 blocks	240,013 blocks	960,718 blocks
Total bit capacity	179,745 bits	720,039 bits	2,882,154 bits
Sub-band bit capacity	59,915 bits	240,013 bits	960,718 bits

intensive, the algorithms provide no evidence that these cryptographic watermarks were extracted intact at the receiver side. Since a 1-bit change in a CRC or hash code will lead to a false localized tamper detection, extensive use of such cryptographic watermarks is considered a major limitation of the proposed algorithms. Moreover, the robustness of the proposed algorithms was not evaluated properly using standard metrics such as normalized correlation and bit error rates to prove that the cryptographic watermarks could survive attacks such additive Gaussian noise and JPEG compression. On the other hand, our encryption-based tamper localization scheme offers confidentiality for the ROI of the image in addition to the accurate localized tamper detection rates. Another limitation in the proposed algorithms is their inefficient ROI recovery schemes. Compressing ROI using the lossy JPEG compression standard, and embedding the compressed file as a recovery watermark in the RONI of the image, is of a limited practical usability. This is by virtue of the fact that the recovered ROI is far from being identical to the original ROI, and thus it may not be appropriate for diagnostic purposes [35]. Similarly, lossless compression, which has been used by some algorithms, may allow for exact recovery of the ROI of the image; however, the time spent in compressing and decompressing the ROI watermark will introduce a computational overhead that will limit its usability. Furthermore, the size of the ROI varies from one modality to another, and thus it is not always guaranteed that the RONI will be large enough

to accommodate the compressed ROI watermark. For these obvious limitations, the recovery feature has not been incorporated in our proposed algorithm.

The proposed algorithm can be compared with pure watermarking methods such as the scheme described in [14]. This scheme provides authenticity to the transmitted medical image using a method similar to the method described in the paper; however, integrity and confidentiality are provided differently. Integrity is provided by embedding local fragile watermarks in the region of interest (ROI) of the image using a reversible scheme in the spatial domain, whereas confidentiality is achieved as a byproduct of hiding the patient's personal data as an authentication robust watermark. As described throughout the paper, the proposed algorithm achieves integrity and confidentiality using more effective methods. The algorithm provides two levels of integrity verification: strict and content-based integrity of the image ROI, and the second by using symmetric encryption to provide confidentiality and tamper localization of the same region.

Finally, when compared with the crypto-based DICOM standard, it is important to emphasize that the proposed algorithm achieves confidentiality, authenticity, and integrity of the transmitted image. Authenticity and integrity are achieved as described in "Image Preprocessing" section, and confidentiality is achieved by virtue of encrypting the ROI before transmission. On the other hand, the Digital Signature Profiles of DICOM's part 3.15 addresses authenticity and

**Table 9** Comparison between the proposed algorithm and the DICOM standard

Algorithm	Confidentiality (header)	Confidentiality (pixels)	Authenticity (header)	Authenticity (pixels)	Integrity (header)	Integrity (pixels)
DICOM standard	√			√		√
Proposed algorithm	√	√	√	√	√	√

integrity of the medical image; however, confidentiality is not addressed in the Basic Application Level Confidentiality Profile of the standard [36]. Moreover, the digital signature stored in the header of the DICOM image provides authenticity and integrity of the image; however, the signature is susceptible to loss or degradation during compression or transmission, thus it may not be always available for verification. As for the header data of the DICOM image, confidentiality is addressed by the DICOM standard; however, authenticity and integrity are not addressed. This is a major limitation of the DICOM standard since the security of the header data of the image is as important as the security of its pixel data of the image. The comparison between the proposed algorithm and the DICOM standard is summarized in Table 9.

## Conclusions

In this paper, we proposed a crypto-watermarking algorithm capable of providing secured exchange of medical images between healthcare entities. The algorithm is based on segmenting the image into a ROI and a RONI zones to preserve the ROI from any distortion that will limit its diagnostic value. Two robust watermarks, representing the patient's personal data and the hospital's logo, are used to implement authenticity in the RONI of the image using singular value decomposition in the discrete wavelets transform domain. A cryptographic hash watermark is also embedded in the RONI to provide strict integrity of the ROI. Additionally, the ROI is encrypted before transmission to achieve confidentiality, and to localize tampered regions at the receiver's side. The uniqueness of the proposed algorithm is of twofolds: providing strict and content-based integrity of the ROI of the image, and using symmetric encryption to provide confidentiality and tamper localization for the ROI. Performance of the algorithm was evaluated using gray-scale medical images of different modalities with respect to imperceptibility, robustness, capacity, and tamper localization. The results showed the effectiveness of the algorithm in providing the desired security requirements of telemedicine applications. Our future research will focus developing new watermarking algorithm to handle multi-slice and multi-frame medical images.

## References

1. Fiaidhi J, Kuziemy C, Mohammed S, Weber J, Topaloglou T: Emerging IT trends in healthcare and well-being. *IT Prof* 18(3):9–13, 2016
2. Saranummi N: In the spotlight: health information systems. *IEEE Rev Biomed Eng* 6:21–23, 2013
3. Huang HK: *PACS and imaging informatics: basic principles and applications*. Wiley-Blackwell, New York, 2010
4. Kocabas O, Soyata T, Aktas M: Emerging security mechanisms for medical cyber physical systems. *IEEE/ACM Trans Comput Biol Bioinform* 13(3):401–416, 2016
5. The Health Insurance Portability and Accountability Act (HIPAA), March 2009. [Online]. Available at: <http://www.hhs.gov/ocr/privacy/index.html>
6. Lee W, et al: A cryptographic key management solution for HIPAA privacy/security regulations. *IEEE Trans Inf Technol Biomed* 12(1):34–41, 2008
7. Schneier B. *Applied cryptography*. Wiley, 1995
8. Mousavi S, Naghsh A, Abu-Bakar S: Watermarking techniques used in medical images: a survey. *J Digit Imaging* 27(6):714–729, 2014
9. Digital Imaging and Communications in Medicine (DICOM) Standard, DICOM. (2006). [Online]. Available: <http://medical.nema.org/dicom/2006/>
10. Al-Haj A: Providing integrity, authenticity, and confidentiality for header and pixel data of DICOM images. *J Digit Imaging* 28(2): 179–187, 2014
11. Al-Haj A, Abandah G, Hussein N: Crypto-based algorithms for secured medical image transmission. *IET Inf Secur* 9(6):365–373, 2015
12. Coatrieux G, Maitre H, Sankur B, Rolland Y, Collorec R: Relevance of watermarking in medical imaging. In: *Proceedings of the IEEE EMBS Conf. on Information Technology Applications in Biomedicine*. USA, 2000, pp. 250–255
13. Nyeem H, Boles W, Boyd C: A review of medical image watermarking requirements for teleradiology. *J Digit Imaging* 26(2):326–343, 2012
14. Al-Haj A, Amer A: Secured telemedicine using region-based watermarking with tamper localization. *J Digit Imaging* 8(3):737–750, 2014
15. Pan W, Coatrieux G, Cuppens-Boulahia N, Cuppens F, Roux C: Medical image integrity control combining digital signature and lossless watermarking. *Data Privacy Manage. Autonom. Spontaneous Sec. (LNCS)*, vol. 5939, 2010, pp. 153–162
16. Zope-Chaudhari S, Venkatachalam P, Buddhiraju K: Secure dissemination and protection of multispectral images using crypto watermarking. *IEEE J Sel Top Appl Earth Observ Remote Sens* 8(11):5388–5394, 2015
17. Al-Haj A, Hussein N, Abandah G: Combining cryptography and digital watermarking for secured transmission of Medical images. In: *Proc. of the IEEE International Conference on Information Management*. UK, 2016
18. Zhou XQ, Huang HK, Lou SL: Authenticity and integrity of digital mammography images. *IEEE Trans Med Imaging* 20(8):784–791, 2001
19. Patel P, Patel Y: Secure and authentic DCT image steganography through DWT-SVD Based Digital Watermarking with RSA Encryption. In: *Proc. of the IEEE fifth International Conference on Communication Systems and Network Technologies*, 2015, pp. 736–739
20. Guo X, Zhuang T: A region-based lossless watermarking scheme for enhancing security of medical data. *J Digit Imaging* 22(1):53–64, 2009
21. Guo X, Zhuang T: Lossless watermarking for verifying the integrity of medical images with tamper localization. *J Digital Imaging* 22(6): 2009
22. Dragoi I, Coltuc D: On local prediction based reversible watermarking. *IEEE Trans Image Process* 124(4):1244–1246, 2015

23. Thodi D, Rodríguez J: Expansion embedding techniques for reversible watermarking. *IEEE Trans Image Process* 16:721–30, 2007
24. Celik M, Sharma G, Tekalp M, Saber E: Lossless generalized-LSB data embedding. *IEEE Trans Image Process* 14:253–266, 2005
25. Su C, Huang J, Shih C, Chen Y: Reversible and embedded watermarking of medical images for telemedicine. In: *Proc. of the first IEEE International Conference on Industrial Networks and Intelligent Systems*. 2015, pp. 145–150
26. Wu J, et al: Tamper detection and recovery for medical images using near-lossless information hiding technique. *J Digit Imaging* 21(1):59–76, 2008
27. Chiang K, Chang K, Chang R, Yen H: Tamper detection and restoring system for medical images using wavelet-based reversible data embedding. *J Digit Imaging* 21:77–90, 2008
28. Liew S, Zain J: Tamper localization and lossless recovery watermarking scheme. *Commun Comput Inf Sci* 179(1):555–566, 2011
29. Liew S, Zain J: Tamper localization and lossless recovery watermarking scheme with ROI segmentation and multilevel authentication. *J Digit Imaging* 24:114–125, 2011
30. Al-Qershi O, Khoo B: Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images. *J Digit Imaging* 24:114–125, 2011
31. Guo X, Zhuang T: Lossless watermarking for verifying the integrity of medical images with tamper localization. *J Digit Imaging* 22(6): 620–628, 2009
32. Tan C, Ng C, Xu X, Poh C, Yong L, Sheah K: Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability. *J Digit Imaging* 24(3):528–540, 2011
33. Mousavi S, Naghsh A, Abu-Bakar S: A heuristic automatic and robust ROI detection method for medical image watermarking. *J Digit Imaging* 28(4):417–427, 2015
34. Su PC, Wang HJ, Kuo CCJ: Digital image watermarking in regions of interest. In: *Proceedings of the IS&T conference on image processing, image quality, image capture systems*. Savannah, Georgia, 1999, pp 295–300
35. Eswarajah R, Reddy E: Robust medical image watermarking technique for accurate detection of tampers inside region of interest and recovering original region of interest. *IET Image Process* 9(8):615–625, 2015
36. *Digital Imaging and Communications in Medicine (DICOM)*, part 15: security profiles ed., National Electrical Manufacturers Association (NEMA), pS 3.15–2001, 2001