J Digit Imaging (2014) 27:737–750
DOI 10.1007/s10278-014-9709-9

Secured Telemedicine Using Region-Based Watermarking with Tamper Localization

Ali Al-Haj · Alaa' Amer

Published online: 30 May 2014

Abstract Medical images exchanged over public networks require a methodology to provide confidentiality for the image, authenticity of the image ownership and source of origin, and image integrity verification. To provide these three security requirements, we propose in this paper a region-based algorithm based on multiple watermarking in the frequency and spatial domains. Confidentiality and authenticity are provided by embedding robust watermarks in the region-of-non-interest (RONI) of the image using a blind scheme in the discrete wavelet transform and singular value decomposition domain (DWT-SVD). On the other hand, 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. The integrity provided by the proposed algorithm is implemented on a block-level of the partitioned-image, thus enabling localized detection of tampered regions. The algorithm was evaluated with respect to imperceptibility, robustness, capacity, and tamper localization capability, using MRI, Ultrasound, and X-ray gray-scale medical images. Performance results demonstrate the effectiveness of the proposed algorithm in providing the required security services for telemedicine applications.

Keywords Telemedicine · Confidentiality · Authenticity · Integrity · Tamper localization · Medical image transmission · DWT · SVD · Watermarking

A. Al-Haj (✉)
Department of Computer Engineering, King Abdullah II Faculty of Engineering, Princess Sumaya University for Technology, Al-Jubeiha, PO Box 1438, Amman 11941, Jordan
e-mail: ali@psut.edu.jo

A. Amer
Ideal Solutions, Ahmad Bin Ali Street, Doha 20851, Qatar
e-mail: alaa.mamer@gmail.com

Introduction

The recent innovations in information and communication technologies have boosted the quality of health-care services and introduced new effective medical practices. One such unique practice is telemedicine, which has enabled the exchange of medical images and electronic health records among physicians and hospitals around the world. Indeed, telemedicine nowadays plays an increasingly important role in modern health-care applications such as telediagnosis, telesurgery, and distant learning [1]. However, the effectiveness of telemedicine applications requires a secured transmission of medical records since current communication networking technologies make it easy for intruders to intercept and tamper medical images while being exchanged over public networks [2].

To provide secured exchange of medical images between health-care entities, three requirements must be simultaneously satisfied: confidentiality, authenticity, and integrity [3]. While confidentiality ensures that only entitled users have access to the transmitted image, integrity verifies that the image has not been modified, and authenticity ensures that the image belongs to the claimed patient and comes from the correct source. Currently, cryptography and digital watermarking are the two major technologies that are used to provide the three security requirements. Cryptography-based methods use symmetric encryption, hashing, and digital signatures [4–6], while watermarking-based methods use robust and fragile watermarks [7].

Cryptography is the standard approach of achieving security in information systems; thus, it has been the only approach to provide security for telemedicine applications for many years [8]. As a matter of fact, cryptography is used in the Digital Imaging and Communications in Medicine (DICOM) standard which defines a technical framework for application entities involved in the exchange of medical data [9]. In

particular, part 15 and supplement 142 of the standard recommend the use of triple DES and AES symmetric encryption standards and digital signatures to achieve security for the exchanged images [10]. However, a major limitation of the cryptographic-based DICOM approach is that once the medical image is deciphered, or the digital signature is deleted or lost, the image is no longer protected, and it becomes hard to verify its integrity and authenticity.

Digital watermarking is currently the limestone technology in the field of digital intellectual property and information security [11]. The focus of this data-hiding technology has been to provide copyright protection for digital multimedia documents consisting of images, audio, and video objects [12]. Therefore, it is believed that digital watermarking has the potential to provide exchanged medial images with confidentiality protection, origin and ownership authentication, and data integrity [13]. Indeed, watermarking could provide medical confidentiality by embedding the patient's personal data into the associated image in the form of a permanent robust watermark. Similarly, authenticity can be provided by embedding into the image a robust watermark containing the physician's or the hospital's identification code. Finally, watermarking provides the means to verify the integrity of exchanged images using fragile or cryptographic hash watermarks [14].

Three types of watermarking methods have been proposed for medical image watermarking; irreversible methods, reversible methods, and region-based methods [15]. Irreversible watermarking methods are not acceptable in the medical field since the distortions caused to the original images by the watermarking process involve non-invertible operations such as bit replacement, truncation, or quantization. Reversible watermarking methods, on the other hand, restore the watermarked images to their original pixel values, thus allowing for accurate medical diagnosis. However, most reversible watermarking algorithms lack the tamper localization functionality which is a desired property in the integrity verification of medical images. The third type, region-based watermarking methods, involves segmenting the original image into two separate areas; region-of-interest (ROI) and region-of-non-interest (RONI). The two regions have different characteristics; thus, different watermarks can be embedded to achieve different security requirements. Moreover, the region-based methods posses the tamper localization functionality which provides content-based integrity for exchanged medical images.

In this paper, we describe a region-based watermarking algorithm capable of providing confidentiality, and verifying authenticity and integrity, for medical images exchanged in telemedicine applications. The algorithm uses multiple watermarks to meet these security requirements. For authenticity, the algorithm uses two robust watermarks representing the patient's personal data and the hospital's logo. For content-based integrity, the algorithm uses randomly generated local fragile watermarks to detect ROI blocks that have been tampered. The robust watermarks are embedded in the RONI using a blind transform-based scheme, and the local fragile watermarks are embedded in the ROI using least significant bit (LSB)-based spatial-domain scheme. Confidentiality is achieved as a by-product of hiding the patient's personal data as an authentication robust watermark.

A few related region-based medical image watermarking algorithms with tamper localization capabilities have been proposed in literature. These algorithms use cyclic redundancy check (CRC) and hash codes as watermarks to implement the tamper localization functionality. Such cryptographic watermarks are computationally intensive which prevents their use in real-time environments. Moreover, any slight change in an embedded CRC or hash code watermark will lead to false localized tamper detection at the receiver's side. To overcome these limitations, our proposed algorithm uses randomly generated local fragile watermarks, instead of cryptographic primitives, to achieve the tamper localization functionality without computational overhead and false localized tamper detection. The remaining of the paper is organized as follows. "Related Work" section is a literature survey of recent related work. The proposed algorithm is described in detail in "The Proposed Algorithm" section. Evaluation results are presented in "Performance Evaluation Results" section. Discussion and concluding remarks are given in "Discussion and Concluding Remarks" section.

Related Work

Different types of watermarking methods have been proposed in literature to provide the security services required for telemedicine applications. These methods can be classified into three categories: irreversible methods, reversible methods, and region-based methods. Some recently proposed methods are described hereafter.

Irreversible watermarking methods are lossy in nature since they introduce permanent alterations to the original image pixels even after the extraction of the hidden watermarks. Chao [16] proposed a discrete cosine transform (DCT)-based technique capable of hiding medical data into the quantized DCT coefficients of the transformed image. Zhou [17] demonstrated that authenticity and integrity can be verified for digital mammography images by replacing the LSB of one random pixel of the mammogram by one bit of the digital envelope bit stream. Irreversible methods are generally not acceptable in the medical field because the watermarking-induced image distortions are caused by non-invertible operations such as bit replacement, truncation, or quantization. Therefore, irreversible distortions may lead to incorrect diagnosis and treatment with life threatening consequences.

Reversible watermarking ensures that alterations introduced during the embedding process can be removed from the image, thus restoring the original pixels for accurate diagnosis. This lossless type of watermarking has drawn the interest of the medical imaging community. De Vleeschouwer [18] applied a circular interpretation of bijective transformations to embed data in a lossless manner. Tan [19] proposed a high-capacity lossless scheme based on the difference expansion of pairs of pixel values. The scheme was the basis of similar schemes introduced by Guo [20], Alattar [21], and Thodi [22]. The reversibility of the scheme presented by Celic [23, 24] was achieved by compressing quantization residues, whereas Zhou [25] achieved reversibility by compressing the LSBs of random image pixels. These proposed reversible schemes are effective in the standard image watermarking applications; however, they bring inconvenience for medical applications since the embedding-induced distortion becomes distributed in the whole medical image.

Region-based watermarking methods separate medical images into two parts: region-of-interest (ROI) and region-of-non-interest (RONI). A few related region-based medical image watermarking algorithms with tamper localization functionality have been proposed in literature. Liew et al. [26, 27] proposed a region-based algorithm in which tamper localization is implemented by computing CRC and hash functions of ROI blocks and embedding the resultant digest values in the form of watermarks in RONI. Al-Qershi and Khoo [28] proposed a scheme that implements tamper localization by comparing the average value of each block in ROI with the retrieved average value from the watermark. Guo and Zhuang [29] proposed a watermarking scheme with tamper localization based on difference expansion. Tamper localization of this scheme is implemented using the concept of ROI shading. All proposed algorithms use CRC and hash codes watermarks to implement the tamper localization functionality. A major limitation of using CRC and hash codes as watermarks is that they are computation-intensive, thus preventing their use in real-time environments. Moreover, any slight change in a CRC or a hash code watermark will lead to false localized tamper detection at the receiver's side.

The Proposed Algorithm

In this section, we describe a region-based watermarking algorithm which provides the security requirements of confidentiality, authenticity, and integrity for medical images exchanged in telemedicine applications. The algorithm consists of three modules: image preprocessing, watermarks generation, and ROI/RONI watermarking. The ROI is watermarked in the spatial domain using irreversible watermarking, whereas the RONI is watermarked in the frequency domain using a discrete wavelet transform and singular value decomposition (DWT-SVD) hybrid transform. Tamper localization functionality is incorporated in the algorithm to allow for content-based integrity verification of the ROI region. The three modules are explained in detail in what follows.

Image Segmentation

The proposed algorithm is based on the assumption that medical images can invariably be separated into two zones: ROI (region-of-interest) and RONI (region-of-non-interest). The ROI of the image contains the significant information that the physicians utilize for the diagnosis. It is also the region whose integrity must be strictly controlled since the modification of even one bit may not be tolerated. On the other hand, the RONI of the image does not contribute to the diagnosis process and thus can be used for robust watermark insertion. The image-dependent ROI can be defined by a polygon drawn by a radiologist or a computer-aided selection tool. An additional preprocessing step is to partition the image into non-overlapping blocks to facilitate watermark embedding and to increase embedding capacity. An example of ROI/RONI image segmentation and block-based partitioning is shown in Fig. 1.

Authenticity and Integrity Watermarks

The proposed algorithm makes use of two robust watermarks for ownership and source of origin authentication, one fragile watermark for ROI integrity verification, and one robust watermark to store the least significant bits (LSBs) of the

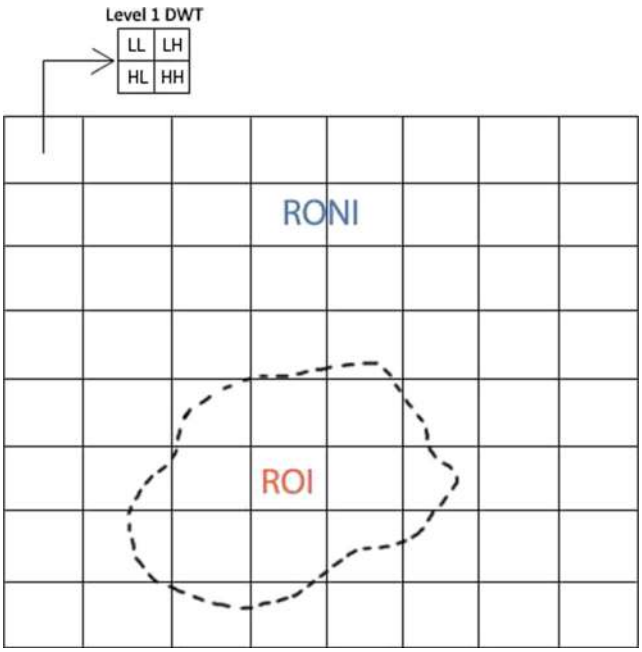

Fig. 1 ROI/RONI segmentation and block-based partitioning of medical images

ROI in order to implement the tamper localization functionality.

The three robust watermarks are described as follows. The *patient's information watermark* is a 204×96 binary image generated from several private patient's attributes as shown in Fig. 2a. The 19,584-bit robust watermark serves for the authentication of image ownership. The *hospital logo watermark* is 81×50 binary image shown in Fig. 2b. The 4,050-bit robust watermark serves for the authentication of the source of origin of the image. The *ROI LSBs watermark* is a robust watermark embedded in the RONI and extracted at the receiver's side to restore the original LSBs of ROI after integrity verification. The watermark is formed by concatenating the LSBs of selected pixels in each ROI block. Therefore, the actual size of this watermark depends on the size of the ROI, number of partitioned ROI blocks, and number of fragile bits embedded in each ROI block.

The *local ROI fragile watermarks* are pn-sequences generated to implement the tamper localization functionality of the algorithm. Integrity of each ROI block is verified by a local fragile watermark whose size depends on the size of the block.

ROI/RONI Watermarking Procedures

Watermarks embedding and extraction procedures are described here for the ROI and RONI segments. Embedding of the fragile watermark in the ROI is described first, followed by a description of embedding the robust watermarks in the RONI. Extraction is done in the reverse order where robust watermarks are extracted from the RONI first. ROI embedding and extraction procedures implement the tamper localization functionality incorporated in the proposed algorithm.

ROI Embedding Procedure

For localized tamper detection, the integrity of each block in the ROI must be verified. This necessitates embedding a local fragile watermark in each block as described below and depicted in the block diagram shown in Fig. 3.

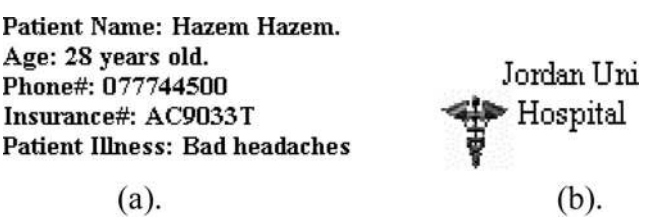

Fig. 2 Authentication watermarks. **a** The patient's information watermark. **b** The hospital logo watermark

Step 1. (Save LSBs of Selected ROI Pixels) Extract the LSBs of randomly selected ROI pixels. The extracted LSBs are concatenated as a single robust watermark for embedding in the RONI. If the ROI block is small, and the RONI bit-capacity is sufficiently large, LSBs of all pixels in the block are extracted.

Step 2. (Embed Local Fragile Watermarks) Embed the bit pattern of the fragile watermark in the same locations of the extracted LSBs.

Step 3. (Produce Watermarked ROI) Replace the original ROI blocks with the watermarked blocks. The ROI of the image is now watermarked.

RONI Embedding Procedure

Embedding of the three robust watermarks in the RONI of the image is depicted in Fig. 4 and described in detail in the steps that follow.

Step 1. (Watermark Formulation) Formulate each of the three robust watermarks in the form of one-dimensional bit patterns.

Step 2. (Embedding in RONI Blocks) For each block in RONI, perform step 2.1~step 2.6 in order to embed the bit patterns of the three robust watermarks.

Step 2.1. (DWT Decomposition) Compute the 1-level DWT for the block. This operation generates four non-overlapping sub-bands [***LL***, ***HL***, ***LH***, ***HH***]. Each sub-band is a matrix of DWT coefficients at a specific resolution.

Step 2.2. Embed the watermark bit patterns in the sub-bands of the RONI block according to the following assignment: ROI LSBs watermark in the HH sub-band, patient's information watermark in the LH sub-band, and the hospital logo watermark in the HL sub-band.

Step 2.3. (SVD Transformation) Apply the SVD operator on the X sub-band of the block. This results in decomposing the block's coefficient matrix into three independent matrices as given in Eq. (1).

$$\boldsymbol{X} = \boldsymbol{U}_X \boldsymbol{S}_X \boldsymbol{V}^T{}_X \tag{1}$$

where $\boldsymbol{X}$ refers to the HL, LH, or HH sub-bands, depending on which watermark is being processed.

Step 2.4. (LSB Embedding) Embed a single watermark bit into upper element of the diagonal matrix $\boldsymbol{S}_X$ by substituting

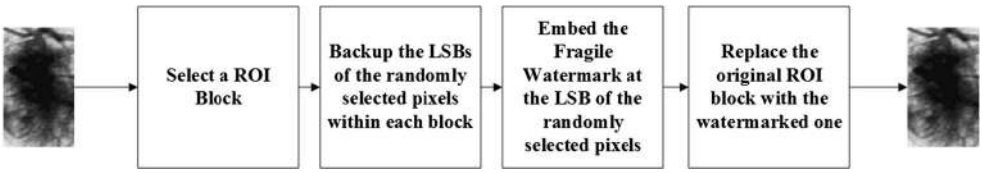

Fig. 3 ROI watermark embedding procedure

the watermark bit W_i with the least significant bit (LSB) of that element.

$$LSB\left(S_{Xi}(0,0) = W_i \right. \tag{2}$$

Step 2.5. (Inverse SVD) Apply the inverse SVD operator on the modified S_X matrix (S_X') to get the modified coefficient matrix X'.

$$X' = U_X S_X' V_X{}^T \tag{3}$$

Step 2.6. (Inverse DWT) Apply inverse DWT on the block after the assigned watermark bits have been embedded in the three sub-bands HL, LH, and HH. With this operation, the block is considered watermarked.

Step 3. Construct the final watermarked medical image I' by merging all watermarked RONI blocks.

RONI Extraction Procedure

The proposed algorithm is blind in the sense that it does not require the original medical image in the extraction process. Therefore, we can extract the robust watermarks directly from the DWT-SVD transformed RONI blocks as depicted in Fig. 5 and described in detail in the steps that follow.

Step 1. (Extraction From RONI Block) For each RONI block in the watermarked medical image I', perform step 1.1~step 1.5 in order to extract the watermark bits.

Step 1.1. (DWT Decomposition) Compute the 1-level DWT for the block. This operation generates four non-overlapping sub-bands [*wLL*, *wHL*, *wLH*, *wHH*].

Step 1.2. (SVD Transformation) Apply the SVD operator on the X sub-band of the block. This results in decomposing the block's coefficient matrix into three independent matrices.

$$X_w = U_{Xw} S_{Xw} V^T{}_{Xw} \tag{4}$$

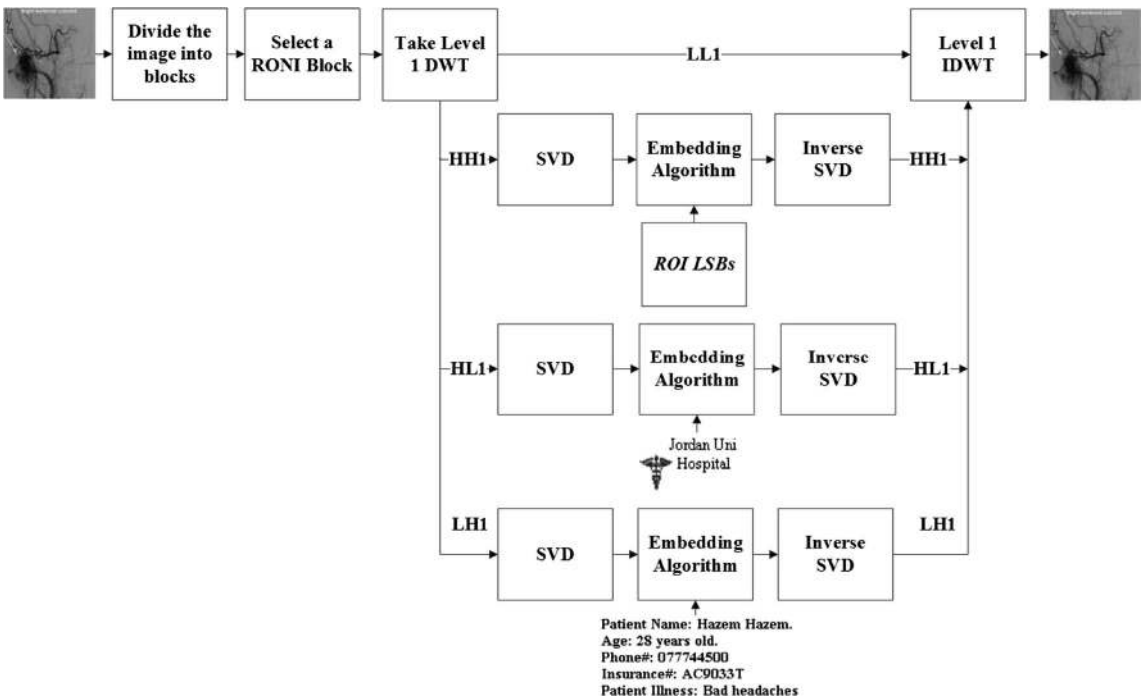

Fig. 4 RONI watermark embedding procedure

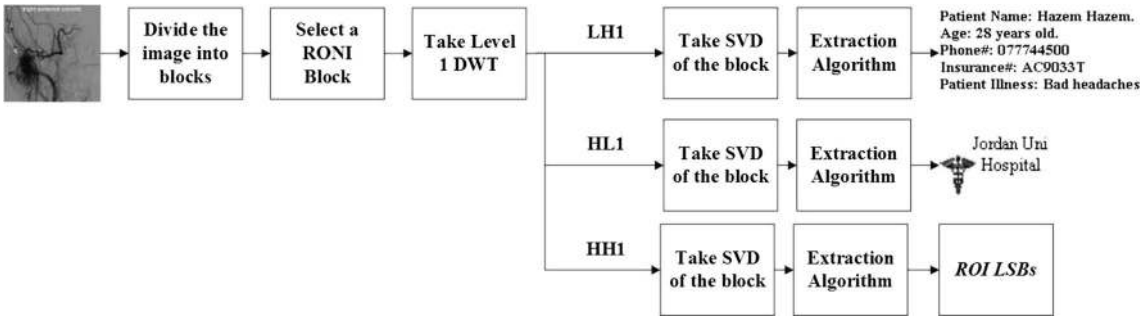

Fig. 5 RONI watermark extraction procedure

Step 1.3. (LSB Extraction) Extract the embedded watermark bit from the upper diagonal element of $\boldsymbol{S}_{\boldsymbol{Xw}}$.

$$\boldsymbol{W}_{\mathbf{i}}^{'} = \boldsymbol{LSB}\left(\boldsymbol{S}_{\boldsymbol{Xw}i}(0,0)\right) \tag{5}$$

Step 2. (Watermarks Reconstruction) Reconstruct the three watermarks by cascading relevant watermark bits extracted from the ***wX*** sub-bands of all blocks.

Step 3. (Authentication) Authentication of the ownership and source of origin of the received image is verified as follows:

Step 3.1. (Image Ownership Authentication) Authenticate the ownership of the image by comparing the original and extracted patient's information watermark*s*. If a match exists, the image ownership is authenticated.

Step 3.2. (Source of Origin Authentication) Authenticate the source of origin of the image by comparing the original and the extracted hospital logo watermark*s*. If a match exists, the source of origin of the image is authenticated.

ROI Extraction Procedure

This procedure performs localized tamper detection as shown in Fig. 6. For each block in ROI, perform the following steps.

Step 1. (Local Watermark Extraction) Extract the local fragile watermark from the LSBs of the same pixels used in embedding.

Step 2. (Local Tamper Detection) Compare the extracted block's watermark with the block's reference fragile watermark. A mismatch indicates that the block has been tampered.

Step 3. (Restore Original ROI) Restore the original LSBs of the block from the robust ROI LSBs watermark.

Performance Evaluation Results

In this section, we present the performance results of the proposed algorithm with respect to imperceptibility, robustness, embedding capacity, tamper localization, and execution time. Extensive experimentation has been carried out on gray-scale medical images of three modalities: MRI, Ultrasound, and X-ray. All test images are 2,048× 2,048 pixels and have been partitioned into 2×2 blocks. Figure 7 shows three test images, representing the three modalities, with the ROI of each image indicated by a polygon. All simulation experiments were done using MATLAB R2012a running on an AMD Phenom II X4 965 Processor at 3.40 GHz.

Imperceptibility

Imperceptibility ensures that the quality of the watermarked image is not perceivably distorted. The three watermarked benchmark images are shown in Fig. 8. An immediate subjective evaluation of the perceptual quality of the images reveals no visual difference with their original counterparts shown in Fig. 7. For objective evaluation, we used the peak

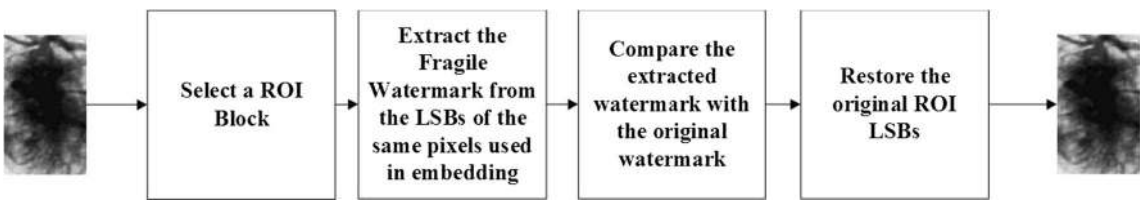

Fig. 6 ROI watermark extraction procedure

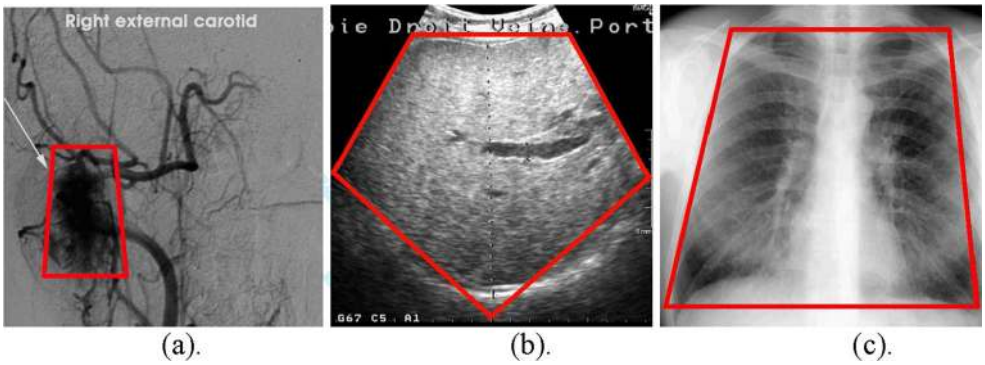

Fig. 7 ROI/RONI segmented benchmark medical images. **a** MRI image. (**b**) Ultrasound image. **c** X-ray image

signal to noise ratio (PSNR) metric and obtained the values 32.9232, 34.0424, and 34.1107 for the MRI, Ultrasound, and X-ray images, respectively. Based on the subjective and objective evaluations, it can be said that the watermarks in the medical images introduced no distortions, thus achieving the imperceptibility requirement.

Robustness

Robustness is a vital requirement for effective digital watermarking. It measures the capability of watermarking techniques to protect the embedded robust watermarks from removal or degradation. To simulate the possible attacks that a transmitted image may undergo, we measured robustness of the algorithm against three commonly simulated attacks: Gaussian noise, salt and pepper noise, and JPEG compression. Robustness is measured for the patient's information watermark embedded in the LH sub-bands of the RONI and for the hospital logo watermark embedded in the HL sub-bands of the RONI. It is important that the two watermarks survive the attacks with the least possible distortion since they are both needed to authenticate the ownership and source of origin of the image.

We applied the three attacks on the watermarked MRI image and measured robustness using the normalized correlation factor (ρ) and the bit error rate (*BER*) metrics. Both metrics measure the similarity between the original and extracted watermarks. The correlation factor is computed according to Eq. (6).

$$\rho\left(w,\widehat{w}\right)=\frac{\sum_{i=1}^{N} w_i\widehat{w}_i}{\sqrt{\sum_{i=1}^{N} w_i^2}\sqrt{\sum_{i=1}^{N} \widehat{w}_i^{\,2}}} \tag{6}$$

where N is the number of pixels in watermark, w and $\widehat{w}$ are the original and extracted watermarks, respectively. The correlation factor ρ may take values between 0 (random relationship) to 1 (perfect linear relationship). On the other hand, the bit error rate (BER) is computed according to Eq. (7).

$$BER=\frac{100}{1}\sum_{n=0}^{l-1}\left\{\begin{array}{ll}1, & W'_n=W_n\\ 0, & W'_n\neq W_n\end{array}\right\} \tag{7}$$

where $\boldsymbol{l}$ is the watermark length, $\boldsymbol{W_n}$ is the $\boldsymbol{n}$th bit of the embedded watermark and $\boldsymbol{W'_n}$ is the $\boldsymbol{n}$th bit of the extracted watermark.

The normalized correlation values are given in Tables 1, 2, and 3, alongside with the extracted watermarks. The corresponding bit error rates have also been plotted in Figs. 9, 10, and 11. Robustness against the two noise types, Gaussian noise and salt and pepper noise, is apparent from the high

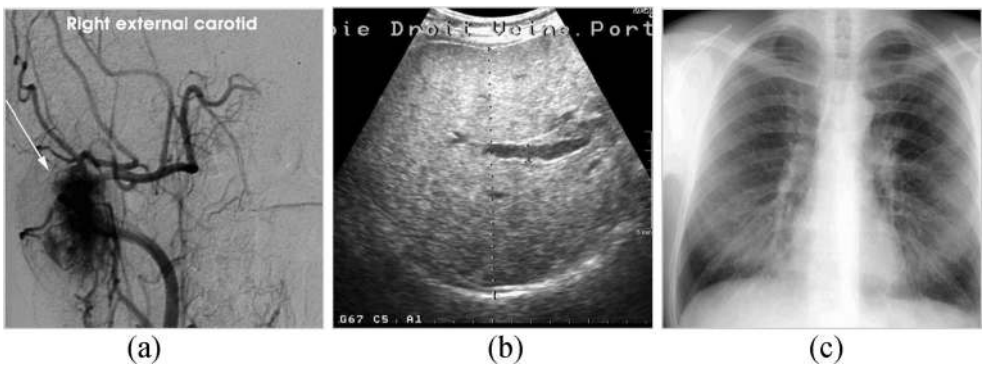

Fig. 8 Watermarked **a** MRI image, **b** Ultrasound image, and **c** X-ray image

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

Watermarked image	Watermarks	Correlation and extracted watermarks			
		Gaussian noise mean			
		0	0.02	0.06	0.1
MRI	Patient information	0.979 Patient name: Hazem Hazem. Age: 28 years old. Phone#: 077744500 Insurance#: AC9033T Patient illness: Bad headaches	0.979 Patient name: Hazem Hazem. Age: 28 years old. Phone#: 077744500 Insurance#: AC9033T Patient illness: Bad headaches	0.979 Patient name: Hazem Hazem. Age: 28 years old. Phone#: 077744500 Insurance#: AC9033T Patient illness: Bad headaches	0.980 Patient name: Hazem Hazem. Age: 28 years old. Phone#: 077744500 Insurance#: AC9033T Patient illness: Bad headaches
	Hospital logo	0.961 Jordan Uni Hospital	0.961 Jordan Uni Hospital	0.961 Jordan Uni Hospital	0.960 Jordan Uni Hospital

correlation values, quality of the extracted watermarks, and the low bit error rates. On the other hand, relatively lower correlation values and higher bit error rates have been obtained for the JPEG lossy compression attack. However, this should not be of a major concern since in practice, a medical image is compressed using lossless compression methods to avoid diagnostic errors; a lossy algorithm may induce. In conclusion, it can be said that robustness has been achieved to the extent that authentication and verification can be done with confidence.

Embedding Capacity

The embedding capacity provided by the algorithm depends on size of the image, size of the ROI and RONI segments, size of image partitioning blocks, and number of DWT decomposition levels. According to the embedding capacity formula given in Eq. (8), larger images, smaller block size, and higher DWT levels will increase the maximum available embedding capacity.

$$C = 3 * Number\ of\ Blocks * 4^{DWT\ Level-1} \tag{8}$$

where

$$Number\ of\ Blocks = \frac{Total\ Image\ Size}{Block\ Size} \tag{9}$$

The capacity equation (Eq. 8) has been derived such that the LL sub-band was excluded from watermark embedding since embedding in this band may have an adverse effect on the quality and imperceptibility of the watermarked images. To find the available bit-capacity in the ROI and RONI segments, the number of blocks in both regions is counted

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

Watermarked image	Watermarks	Correlation and extracted watermarks			
		Salt and pepper noise density			
		0	0.0002	0.0006	0.001
MRI	Patient information	0.995 Patient name: Hazem Hazem. Age: 28 years old. Phone#: 077744500 Insurance#: AC9033T Patient illness: Bad headaches	0.989 Patient name: Hazem Hazem. Age: 28 years old. Phone#: 077744500 Insurance#: AC9033T Patient illness: Bad headaches	0.978 Patient name: Hazem Hazem. Age: 28 years old. Phone#: 077744500 Insurance#: AC9033T Patient illness: Bad headaches	0.966 Patient name: Hazem Hazem. Age: 28 years old. Phone#: 077744500 Insurance#: AC9033T Patient illness: Bad headaches
	Hospital logo	1.000 Jordan Uni Hospital	0.991 Jordan Uni Hospital	0.981 Jordan Uni Hospital	0.967 Jordan Uni Hospital

Table 3 Robustness of the watermarked MRI image against JPEG compression

Watermarked image	Watermarks	Correlation and extracted watermarks			
		JPEG compression quality factor			
		100	96	88	80
MRI	Patient information	0.973 Patient name: Hazem Hazem. Age: 28 years old. Phone#: 077744500 Insurance#: AC9033T Patient illness: Bad headaches	0.867 Patient name: Hazem Hazem. Age: 28 years old. Phone#: 077744500 Insurance#: AC9033T Patient illness: Bad headaches	0.762 Patient name: Hazem Hazem. Age: 28 years old. Phone#: 077744500 Insurance#: AC9033T Patient illness: Bad headaches	0.737 Patient name: Hazem Hazem. Age: 28 years old. Phone#: 077744500 Insurance#: AC9033T Patient illness: Bad headaches
	Hospital logo	0.973 Jordan Uni Hospital	0.873 Jordan Uni Hospital	0.759 Jordan Uni Hospital	0.636 Jordan Uni Hospital

before applying the capacity equation. Table 4 gives the maximum available capacities under the following assumptions: 2,048×2,048 image size, 2×2 block size, and 1-level DWT. The 2×2 block size has been chosen in order to provide the maximum watermarking capacity. Larger blocks decrease the maximum available capacity since one single bit is embedded in each DWT-SVD transformed block regardless of its size, as explained in the previous section. Larger blocks, on the other hand, have the benefit of reducing watermarking time as will be shown elsewhere in this section.

Table 4 gives as well the maximum bit-capacity of the two regions. As described in the previous section, three bits are embedded in each RONI block (one bit per sub-band). Therefore, the total embedding capacity for the RONI is computed by multiplying number of RONI blocks by three. As for the ROI, the maximum bit-size of the fragile watermark that can be accommodated is equal to the total number of ROI blocks multiplied by number of pixels in each block.

Referring to Table 4, it is important to mention that the number of blocks in the RONI and ROI segments were counted, rather than computed, since it depends on the size and shape of the ROI of the image, which is in turn determined by a physician. As shown in Fig. 7, the ROI of the MRI image is relatively small; thus, number of ROI blocks is much smaller than number of RONI blocks. On the other hand, the ROI of the Ultrasound image is much bigger than its RONI; thus, less RONI blocks are available for embedding the three robust watermarks, as given in Table 4.

Table 5 gives a comparison between the maximum bit-capacity provided by the algorithm and the payload required by the different watermarks. As shown in the table, the available ROI/RONI embedding capacities far exceed the total bit requirements of the watermarks used in the algorithm.

Tamper Localization

Based on the localized tamper detection scheme of the proposed algorithm, the integrity of the ROI segment of the image is verified by checking the integrity of each single block in ROI, and not by considering the strict integrity of ROI as a

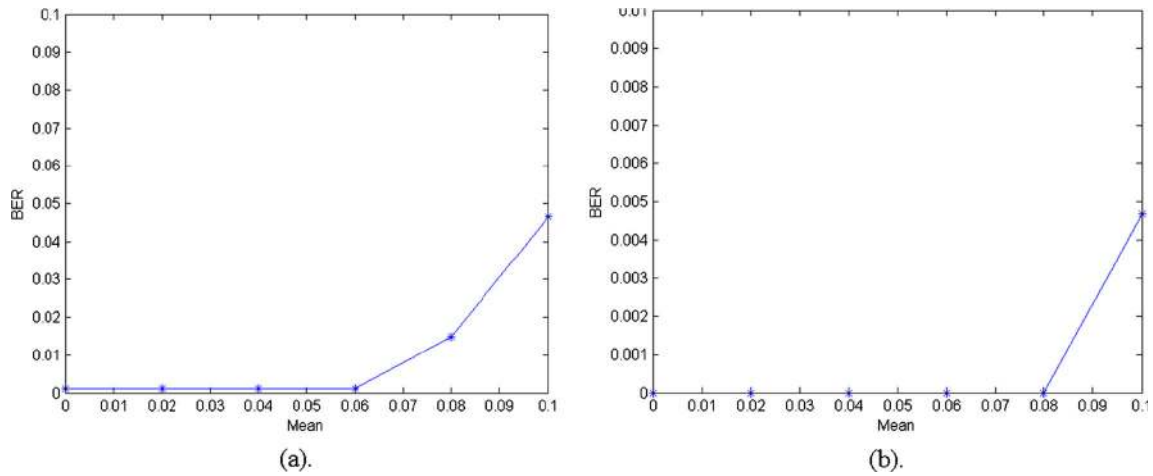

Fig. 9 Robustness against Gaussian noise measured using BER for **a** the patient's information watermark and **b** the hospital logo watermark

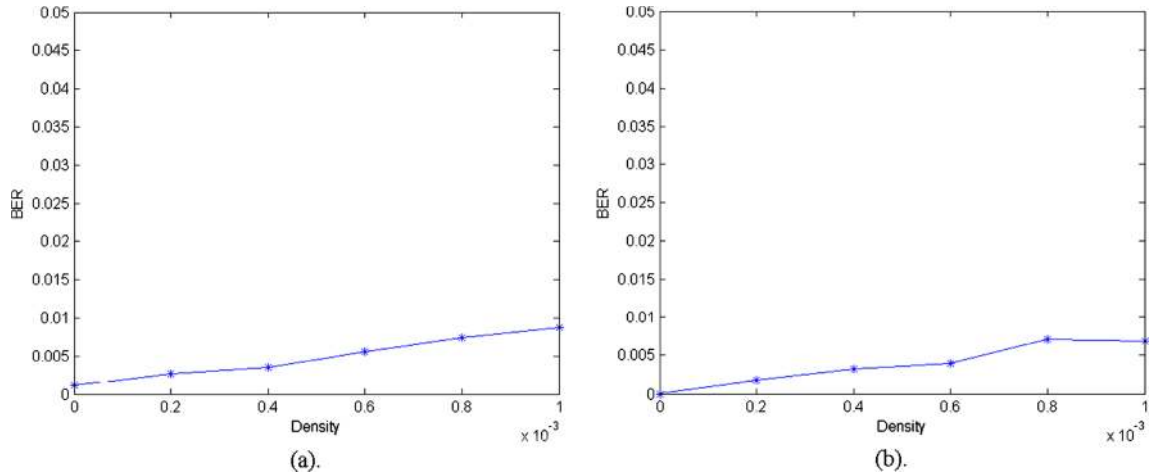

Fig. 10 Robustness against salt and pepper noise measured using BER for **a** the patient's information watermark and the **b** the hospital logo watermark

whole. For each block, the extracted local fragile watermark is compared with the original reference watermark of the block. If a match exists, the integrity of the block is verified; otherwise, the block is considered tampered. The capability of the algorithm to detect and localize tampered blocks is demonstrated in Fig. 12 which shows localization of a manually tampered 2×2 block. The granularity of tamper localization can also be controlled by varying the size of the block, as shown in the same figure.

The Ultrasound and X-ray images shown in Fig. 7 have much larger ROIs compared with the ROI of the MRI image. Nonetheless, tamper localization for large ROIs can still be implemented using our proposed scheme. As described earlier, the ROI pixels of the MRI image have been all watermarked in block, since their LSBs were accommodated and stored as a robust watermark in the HH band of the RONI blocks. However, for the Ultrasound image, only 24 % of its ROI pixels can be watermarked as determined by the maximum bit-capacity of the HH band in the RONI blocks. Similarly, for the X-ray image, only 12 % of its ROI pixels can be watermarked as determined by the maximum bit-capacity of the HH band in the RONI blocks. Table 6 gives a comparison between the three modalities with respect to the percentage of ROI pixels that can be watermarked based on 2×2 blocks.

A zoomed snapshot for localized tamper detection of the Ultrasound and X-images is given in Fig. 13. Multiple ROI blocks were tampered manually and localized by the proposed scheme, as indicated by the white circles.

Time Performance

Medical image watermarking schemes developed for secured telemedicine applications may eventually be incorporated in hospitals' information systems. It is therefore important to measure the time taken to execute the watermark embedding and extraction procedures, as well as the time required to process the tamper localization function. The results given in Fig. 14 show that the spent in embedding the watermarks is much higher than the time spent in the extraction process. Moreover, the results show that the runtime for the tamper

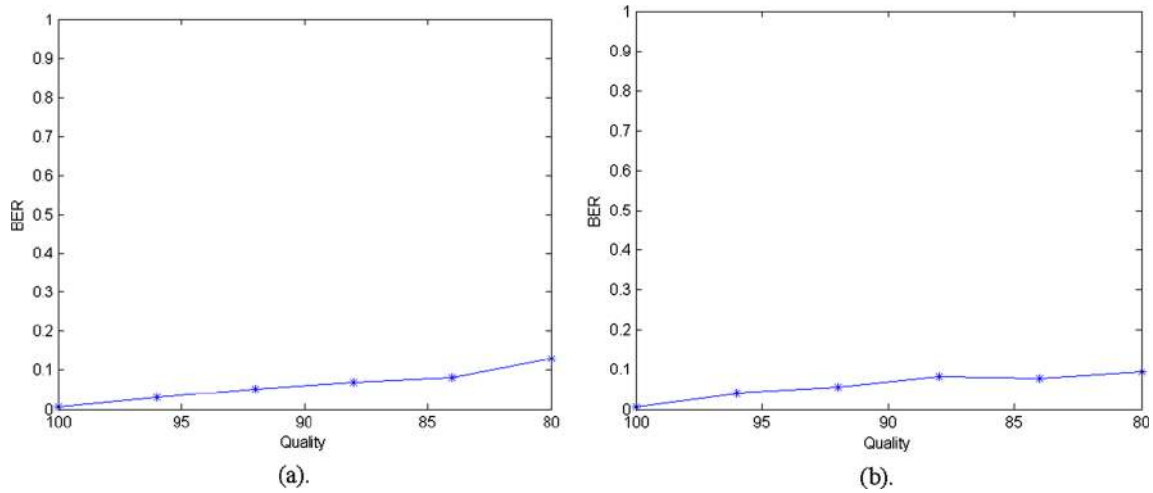

Fig. 11 Robustness against JPEG compression measured using BER for **a** the patient's information watermark and **b** the hospital logo watermark

Table 4 Available watermark embedding capacity provided by the algorithm

	MRI test image	Ultrasound test image	X-ray test image
RONI maximum blocks	960,718 blocks	518,708 blocks	342,614 blocks
ROI maximum blocks	87,876 blocks	529,868 blocks	705,962 blocks
RONI maximum capacity	2,882,154 bits	1,556,124 bits	1,027,842 bits
ROI maximum capacity	351,504 bits	2,119,472 bits	2,823,848 bits

localization function (ROI embedding and extraction) is relatively low when compared to the total runtime.

The total execution time could be drastically reduced if larger blocks were used for the watermarking process. As shown in Fig. 14, the total execution time for the 2×2 blocks is the highest when compared with the time spent using larger block size. However, the 2×2 blocks were used by the algorithm for two reasons; first, they provided the highest bit-capacity, and second, they achieved the best tamper localization. Nonetheless, since the block size is an adjustable parameter, the data hider may choose to use blocks larger than 2×2 if the execution time is of a major concern when compared to capacity and tamper localization requirements. Finally, it is important to note that the time performance has been measured for the MRI test image only. However, the achieved results demonstrate the relative time requirements of the watermarking procedures regardless of image modality.

Discussion and Concluding Remarks

In this paper, we described a region-based watermarking algorithm capable of providing confidentiality and verifying authenticity and integrity for medical images of different modalities. The algorithm uses multiple watermarks to meet these security requirements. For authenticity, the algorithm uses two robust watermarks representing the patient's personal data and the logo of the hospital representing the source of the image. For integrity verification, the algorithm uses a sequence of randomly generated local fragile watermarks to identify and localize tampered blocks. The robust watermarks are embedded in the RONI using a DWT-SVD-based irreversible embedding scheme, and the local fragile watermarks are embedded in the ROI using reversible, LSB-based, spatial-domain scheme. Reversibility is achieved by a third robust watermark holding LSBs of the watermarked ROI pixels. The watermark is embedded in the RONI at the sender's side and extracted at the receiver's side to restore the original LSBs. Confidentiality is achieved by the algorithm as by-product of embedding the patient's private data and hospital information watermarks in the RONI.

Performance of the algorithm was evaluated with respect to imperceptibility, robustness, embedding capacity, block-based tamper localization, and execution time. Experiments were carried out using MRI, Ultrasound, and X-ray gray-scale images. The results showed the effectiveness of the algorithm in providing the authenticity and integrity control requirements. Moreover, the ROI/RONI separation of the original image provided the algorithm with the ability to control integrity of the exchanged images by incorporating the tamper detection and localization function in the watermarking process. Effectiveness of the tamper localization scheme was also evaluated with respect to different varying parameters such as granularity and image modality.

A few related region-based medical image watermarking algorithm with tamper localization functionality have been proposed in literature. Liew [26, 27] proposed a ROI/RONI region-based algorithm in which the ROI is segmented into blocks of 40×40 pixels and the RONI into blocks of 2×2 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 the RONI. For

Table 5 Comparison between the available and required payload capacities

Watermark type and name	Watermark size (bits)	Embedding location (DWT band)	Available capacity (MRI)	Available capacity (Ultrasound)	Available capacity (X-ray)
Patient's information	19,584 bits	RONI (LH band)	960,718 bits	518,708 bits	342,614 bits
Hospital's logo	4,050 bits	RONI (HL band)	960,718 bits	518,708 bits	342,614 bits
ROI LSBs watermark	depends on ROI	RONI (HH band)	960,718 bits	518,708 bits	342,614 bits
ROI fragile watermark	depends on ROI	ROI region	351,504 bits	2,119,472 bits	2,823,848 bits

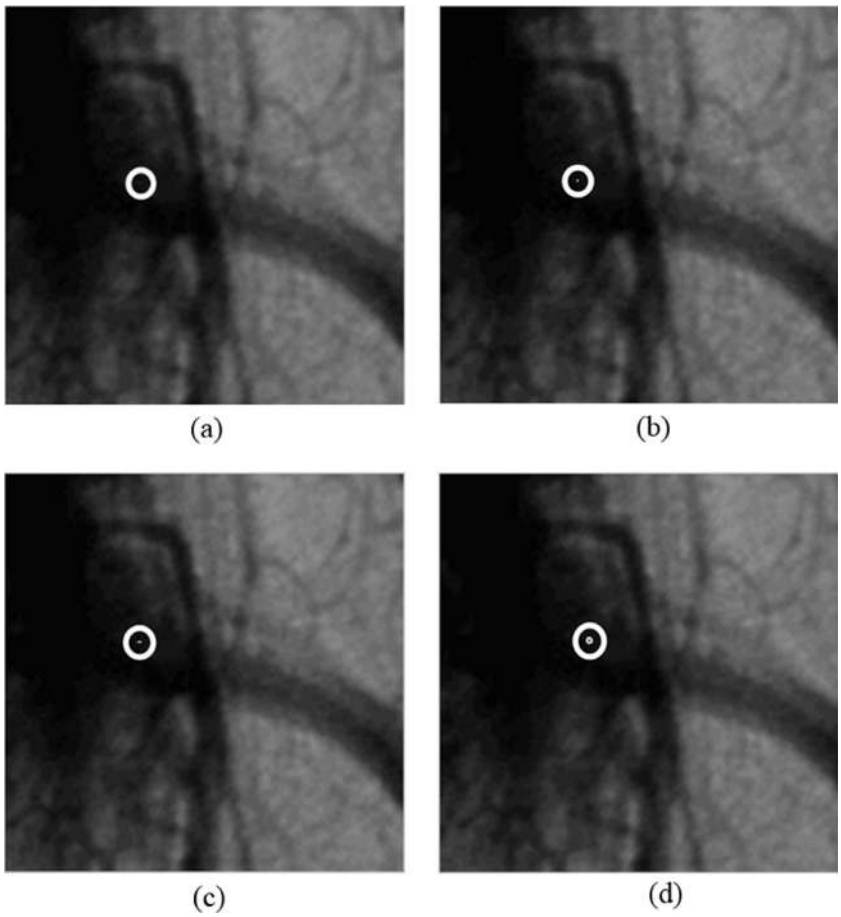

Fig. 12 Block-based tamper localization for the MRI image

recovery, the ROI is compressed using JPEG2000 and embedded in the RONI as a robust watermark using a 3-level DWT.

Al-Qershi and Khoo [28] proposed a scheme that divides the image 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 the discrete wavelet transform. Tamper localization is done by comparing the average value of each block in the ROI with the retrieved average value from the watermark. Tampered blocks are recovered using lossy compressed ROI.

Guo and Zhuang [29] proposed a watermarking scheme with tamper localization 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 the 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 [19] proposed dual-layer watermarking scheme in which the tamper localization function was implemented by dividing the original image into 16×16 pixel blocks and computing the cyclic redundancy check (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

Table 6 Percentage of watermarked ROI pixels

Block size	MRI image	Ultrasound image	X-ray image
Number of RONI bits (HH)	960,718 bits	518,708 bits	342,614 bits
Number of ROI blocks	87,858 blocks	529,868 blocks	705,962 blocks
Number of ROI bits	231,432 bits	2,119,472 bits	2,823,848 bits
Percentage of watermarked ROI pixels	100 %	24 %	12 %

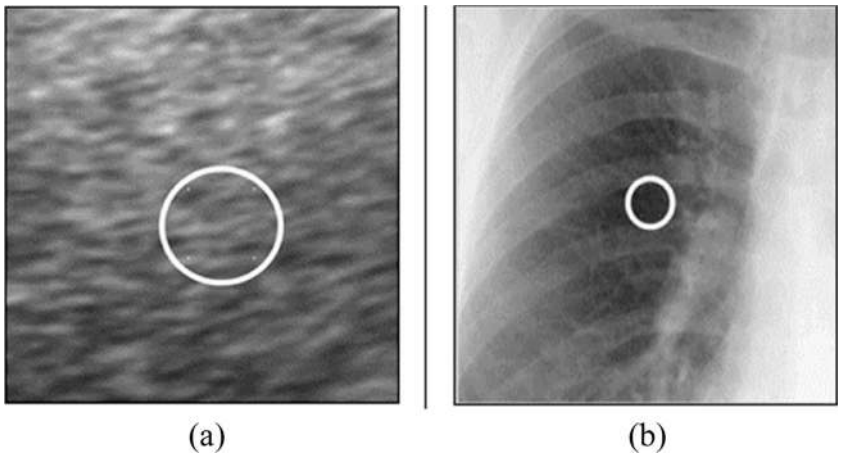

Fig. 13 Block-based tamper localization for the Ultrasound and X-ray images

will be identified as being tampered, hence achieving tamper localization.

A major drawback of the above published algorithms is their extensive use of cryptographic primitives, such as CRC-16 and hash codes, as watermarks. Other than being computationally intensive, the algorithms provide no evidence that these cryptographic watermarks were extracted intact at the receiver's side. Moreover, the robustness of those algorithms was not evaluated properly to prove that the cryptographic watermarks could survive attacks such as additive Gaussian noise and JPEG compression. Since a 1-bit change in a CRC or hash code will lead to false localized tamper detection, extensive use of cryptographic primitives is considered a major limitation of the algorithms. On the other hand, the local fragile watermarks used in our proposed algorithm achieve the tamper localization functionality; however, the computational overhead and false detection rates are reduced.

Another limitation in the reported algorithms is their ROI recovery feature. Compressing the ROI using the lossy JPEG compression standard and embedding the compressed file as a recovery watermark in the RONI is of a limited practical use. This is due to the fact that the recovered ROI is very likely to be far from being identical to the original ROI; thus, it may not be appropriate for diagnostic purposes. On the other hand, lossless compression used by some algorithms may allow for exact recovery of the ROI; however, the time spent in compressing and decompressing the ROI watermark is excessively high. Furthermore, the size of the ROI part of the image varies from one modality to another; 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.

Finally, it is instructive to note that the proposed algorithm was evaluated using standard medical images. However, DICOM images could be used as well. The patient's attributes in the DICOM header could be used totally or partially to construct the patient's information watermark. Embedding

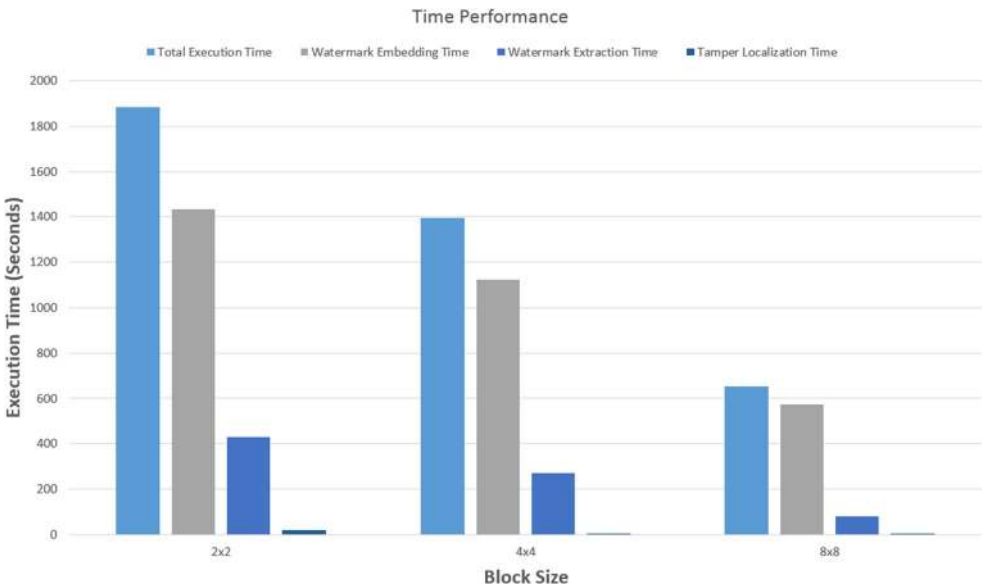

Fig. 14 Time performance of the proposed watermarking algorithm

this watermark in the RONI of the image offers the required confidentiality and prevents the loss or manipulation of the patient's header data.

References

1. Davie B, Florence V, Friede A, Sheehan J, Sisk J: Bringing health-care applications to the internet. IEEE Internet Comput 5(3):42–46, 2001
2. McEvoy F, Svalastoga E: Security of patient and study data associated with DICOM images when transferred using compact disc media. J Digit Imaging 22(1):65–70, 2007
3. Norcen R, Podesser M, Pommer A, Schmidt HP, Uhl A: Confidential storage and transmission of medical image data. Comput Biol Med 33:277–292, 2003
4. Kobayashi L, Furuie S, Barreto P: Providing integrity and authenticity in DICOM images: a novel approach. IEEE Trans Inf Technol Biomed 13(4):582–589, 2009
5. Rodrigues JM,Puech W, Fiorio C: Lossless crypto-data hiding in medical images without increasing the original image size. In: Proc. 2nd Int. Conf. Adv. Med. Signal Inf. Process., Sep. 2004, pp 358–365
6. Bernarding J, Thiel A, Grzesik A: A JAVA-based DICOM server with integration of clinical findings and DICOM-conform data encryption. Int J Med Inform 64:429–438, 2001
7. 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. Arlington, USA, Nov. 2000, pp 250–255
8. Stallings W: Cryptography and Network Security—Principles and Practice. Prentice-Hall, Englewood Cliffs, 1999
9. Digital Imaging and Communications in Medicine (DICOM) Standard, DICOM: 2006. [Online]. Available: http://medical.nema.org/dicom/2006/
10. Digital Imaging and Communications in Medicine (DICOM): part 15: security profiles ed., National Electrical Manufacturers Association (NEMA), 2001, pS 3.15–2001
11. Cox IJ, Miller ML, Bloom JA: Digital Watermarking. Morgan Kaufmann, San Francisco, 2002, pp 26–36
12. Hartung F, Kutter M: Multimedia watermarking techniques. In: Proc. IEEE, vol. 87, no. 7, pp 1069–1107, July 2006
13. Coatrieux G, Lecornu L, Sankur B, Roux Ch: A review of image watermarking applications in healthcare. Porc. of IEEE-EMBC Conf., New York, USA, 2006, pp 4691–4694
14. Coatrieux G, Quantin C, Montagner J, Fassa M, Allaert FA, Roux Ch: "Watermarking medical images with anonymous patient identification to verify authenticity," Studies Health Technol. Inf 136:667–672, 2008
15. Coatrieux G, Maitre H, Sankur B: Strict integrity control of biomedical images. In: Proc. SPIE Security Watermarking Multimedia Contents III, SPIE 2001, vol. 4314, San Jose, CA January 2001, pp 229–240
16. Chao H, Hsu C, Miaou S: A data-hiding technique with authentication, integration, and confidentiality for electronic patient records. IEEE Trans Inf Technol Biomed 6(1):46–53, 2002
17. Zhou XQ, Huang HK, Lou SL: Authenticity and integrity of digital mammography images. IEEE Trans Med Imaging 20(8):784–791, 2001
18. De Vleeschouwer C, Delaigle J, Macq B: Circular interpretation of bijective transformations in lossless watermarking for media asset management. IEEE Trans Multimed 5:97–105, 2003
19. 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
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. Alattar A: Reversible watermark using the difference expansion of a generalized integer transform. IEEE Trans Image Process 13:1147–1156, 2004
22. Thodi D, Rodríguez J: Expansion embedding techniques for reversible watermarking. IEEE Trans Image Process 16:721–730, 2007
23. Celik M, Sharma G, Tekalp M, Saber E: Lossless generalized-LSB data embedding. IEEE Trans Image Process 14:253–266, 2005
24. Celik MU M, Sharma G, Tekalp A: Lossless watermarking for image authentication: a new framework and an implementation. IEEE Trans Image Process 15:1042–1049, 2006
25. Zhou Z, Huang H, Liu B: Digital signature embedding (DSE) for medical image integrity in a data grid off-site backup archive. Proc SPIE 5748:306–317, 2005
26. Liew S, Zain J: Tamper localization and lossless recovery watermarking scheme. Commun Comput Inf Sci 179(1):555–566, 2011
27. Liew S, Way S, Zain J: Tamper localization and lossless recovery watermarking scheme with ROI Segmentation and Multilevel Authentication. J Digit Imaging 24:114–125, 2012
28. Osamah M, Khoo B: Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images. J Digit Imaging 24:114–125, 2011
29. Guo X, Zhuang T: Lossless watermarking for verifying the integrity of medical images with tamper localization. J Digit Imaging 22(6): 620–628, 2009