ROI-based fragile watermarking for medical image tamper detection

Article *in* International Journal of High Performance Computing and Networking · January 2019

DOI: 10.1504/IJHPCN.2019.097508

CITATIONS
40

READS
561

2 authors:

Nour El Houda Golea
University of Batna 1
5 PUBLICATIONS **51** CITATIONS
SEE PROFILE

Kamal Eddine Melkemi
University of Batna2
30 PUBLICATIONS **274** CITATIONS
SEE PROFILE

ROI-based fragile watermarking for medical image tamper detection

Nour El-Houda Goléa*

Department of Computer Science,
University of Batna 2, Algeria
Email: golea.nour@gmail.com
*Corresponding author

Kamal Eddine Melkemi

Department of Computer Science,
University of Biskra, Algeria
Email: melkemi2002@yahoo.com

Abstract: In this paper, we propose a region of interest (ROI) based fragile watermarking scheme for medical image tamper detection. The proposed methodology is inspired by network transmission where the transmitted message is divided into packets and redundant information is added to treat errors. In fact, the cyclic redundancy check code (CRC) is one of the most crucial error detecting checking tools used in various digital communication systems. Consequently, the region of interest to be protected is considered as a message to be transmitted without errors. Thus, the CRC code is based on a standard polynomial generator CRC-32 with more particular mathematical properties and is performed on each packet to generate a watermark to be inserted in spatial domain. At the reception end, the watermark is extracted to detect errors. Results of experiments show the validity of the proposed approach in terms of imperceptibility and efficiency to detect reliable and strong attacks.

Keywords: region of interest; ROI; fragile watermarking; medical image watermarking; tamper detection; error detecting code; EDC; cyclic redundancy check code; CRC; spatial domain watermarking; least significant bits; LSBs; computing and networking; network transmission.

Reference to this paper should be made as follows: Goléa, N.E-H. and Melkemi, K.E. (2019) 'ROI-based fragile watermarking for medical image tamper detection', *Int. J. High Performance Computing and Networking*, Vol. 13, No. 2, pp.199–210.

Biographical notes: Nour El-Houda Goléa graduated in Computer Science Engineer since June 2007 at the University of Batna. She received her MS in Computer Science from the University of Batna, Algeria, in July 2010. She is working toward her PhD in Computer Science at the University of Batna. Here current research interests include image watermarking, evolutionary approaches and optimisation.

Kamal Eddine Melkemi received his PhD in Computer Science in 2006, from the University of Constantine, Algeria, in 2006. He is currently a Professor of Computer Science at the University of Biskra, Algeria. He is also a member of the applied mathematics laboratory, University of Biskra, Algeria. His research activities are related to image processing, pattern recognition, shape matching and retrieval, evolutionary algorithms, artificial life. He is also interested in machine learning, and evolutionary algorithms.

1 Introduction

Nowadays, the transition to the digital world facilitates and accelerates data processing, storage and transmission through networks. Medical technologies are also influenced by the digitisation process where different medical devices produce medical images, which are converted to digital format. Being easy to use and modified, intellectual property rights of digital contents can be violated illegally. For this reason, a pattern of bits called the watermark can be inserted into images in order to attain different security issues. This approach is called digital watermarking (Pizzolante et al., 2014; Castiglione et al., 2015).

In order to embed watermark, two different categories of techniques are proposed in literature: the first one named spatial domain in which the watermark is embedded directly in pixels of original image (Ansari et al., 2016; Yang et al., 2008). The second one called transform domain where the watermark is embedded in coefficients of image transformation (Hu and Chen, 2013; Kejgir and Kokare, 2014; Fan and Tsao, 2007).

According to the field of application, watermarking schemes are classified into robust, fragile and semi-fragile. Robust watermarking schemes are applicable for copyright protection (Su and Chen, 2017; Kejgir and Kokare, 2014) whereas fragile and semi-fragile schemes are employed for image authentication and integrity. Fragile watermarking must be sensitive both to malicious attacks and to accidental content alteration and it is very desirable that it can detect corrupted areas such as in the case of medical images (Ansari et al., 2016; Singh and Agarwal, 2016).

In this paper, we propose a novel fragile watermarking approach using error detecting code (EDC) to achieve the region of interest (ROI) integrity and tamper detection. ROI is the part containing the important information to diagnosis. Usually, the information of ROI tamper detection and recovery are stored in region of non-interest (RONI) that accepts some visual quality degradation (Al-Qershi and Khoo, 2009, 2010; Eswaraiah and Reddy, 2014).

The proposed scheme is inspired by network transmission, in which the message to be transmitted is divided into packets of fixed size and redundant information is added to each packet to treat errors. Depending on communication channel features, two strategies have been performed in practice: the forward error correction (FEC), strategy and the automatic repeat request (ARQ) strategy. The FEC strategy uses the error correcting codes (ECC) to correct errors caused by channels that make many errors (such as wireless links). However, the ARQ is based on EDC that allow the receiver to detect that an error has occurred and it requests a retransmission. This last strategy is used in the case of fibre or high-quality channel where errors appear occasionally and error detection and retransmission are usually more efficient (Tanenbaum, 2003). Generally, ARQ technique is preferred in practice for the reason that the needed redundant information size is smaller than in the case of FEC. This last one is especially used when retransmission is hard to applicable (Ramabadran and Gaitonde, 1988). Cyclic redundancy check (CRC) code is known as one of most useful and powerful EDC used in various digital communication systems (Crow et al., 1997; Koopman, 2002).

In order to obtain a high ROI tamper detection capability, we project the concept of CRC code on medical images. Consequently, the ROI is considered as a message to be transmitted without errors. So, it must be decomposed on packets of fixed size (16 pixels) and CRC encoder is based on a standard polynomial generator CRC-32 with more particular mathematical properties and is performed on each packet to generate a checksum of size 32 bits considering as a watermark to be inserted in 1st and 2nd least significant bits (LSBs) of the corresponding packet. At the reception end, the watermark is extracted and appended on each corresponding packet and CRC decoder is performed on this new sequence to detect errors. Depending on the degree of alteration and the interest of the packet, the receiver can ask the sender to retransmit only the corrupted packets.

The remainder of this paper is organised as follows: Section 2 gives a state of art on some related works. The principle of CRC is reported in Section 3. Our proposed scheme is presented in Section 4. In Section 5, the experimental results are described and analysed. Finally, we draw the conclusions of our work in Section 6.

2 Related works

Codes theory is attractive for image watermarking research. Hence, several code-based watermarking approaches are proposed and diverse EDC or ECC are used such as Reed Solomon (RS), Hamming (Ham), Bose-Chaudhuri-Hocquenghen (BCH), etc. Table 1 presents a literature summary of different code-based watermarking approaches. We can see from Table 1 that all the proposed image watermarking schemes perform different types of codes on the signature or on some features of image. In the case of medical image, codes are performed to attain the robustness of patient information called also electronic patient record (EPR). The proposed methodology is to apply one of the most useful EDC directly on the ROI pixels to obtain the integrity purpose.

Generally, the design of watermarking systems for integrity and tamper detection is based on fragile models (Castiglione et al., 2015; Ansari et al., 2016; Singh and Agarwal, 2016; Kim et al., 2017). Recently, various fragile watermarking methods are focused on ROI medical image integrity and several of them are block-based and the average of each block is used as tampered and recovery information (Liew et al., 2010; Tjokorda Agung, 2012). Indeed, tamper detection fails when the values of pixels are altered without changing the average of block. Eswaraiah and Reddy (2014) resolve this problem by using average and variance of each block. In this scheme, the hash of ROI is calculated to detect the tamper and this information is embedded in LSBs of border pixels. The pixels of each block in ROI are inserted in LSBs of a corresponding block in RONI. At the extraction, the hash value of ROI is compared with extracted hash value. If there are not equal, only tampered blocks are recovered. The tampered blocks are marked based on the average and variance of each block. The main disadvantages of this scheme are:

1 False negative: tamper detection information is embedded separately in RONI. So, if some blocks in ROI are not tampered and their corresponding blocks in RONI are tampered, they are marked as tampered blocks.

2 Much information must be used as tamper detection (hash of ROI, average and variance).

3 Loss in detection when rounding floating average and variance values to integer.

Indeed, tamper detection cannot be 100% accurate.

Table 1 Literature summary of different codes based watermarking techniques

Scheme	*Adopt medical image*	*Type*	*Code*	*Information encoded by code*	*Embedding domain*
Lee and Won (2000)	No	Fragile	RS	Generated signature	Spatial
Terzija and Geisselhardt (2004)	No	Robust	RS	The watermark message (text)	Frequency
Lin et al. (2004)	No	Fragile	CRC	Generated signature.	Spatial
Nayak et al. (2004)	Yes	Robust	RS	Patient information	Spatial
Zhou et al. (2004)	No	Semi-fragile	BCH	Signature extracted from image	Frequency
Chemak et al. (2007)	Yes	Robust	Turbo code	Patient information	Frequency
Qi and Qi (2007)	No	Robust	Ham	The watermark message (text)	Frequency
Nayak et al. (2009)	Yes	Robust	RS, BCH, ham	Patient information	Spatial
Al-Qershi and Khoo (2009)	Yes	Fragile	RS	Patient information and signature	Spatial
Mostafa et al. (2010)	Yes	Robust	BCH	Patient information	Frequency
Hajjaji et al. (2011)	Yes	Robust	BCH	Patient information	Frequency
Kumar et al. (2015)	Yes	Robust	BCH	Patient information	Frequency

For these reasons, we propose to generate the watermark dependently on each pixel in ROI and embed this information directly in LSBs of ROI to preserve a high quality. The watermark is generated using the concept of CRC and a standard generator polynomial of degree 32 (CRC-32) that is employed to achieve a good tamper detection capability.

In the literature some effective medical image watermarking techniques are designed for a special images type such as: Pizzolante et al. (2014) for protecting microscopy images and Castiglione et al. (2015, 2017) for functional magnetic resonance imaging images. We introduce in this paper, a watermarking method that can work on different modalities with different size.

3 Cyclic redundancy check code

CRC code is one of the most crucial error checking techniques used in various digital communication systems and data storage devices such as a disk drive.

The implementation of the CRC requires choosing a polynomial called the generator polynomial of reference often named $G(x)$ that is known to the transmitter and receiver. The transmitter performs the encoding procedure on the message stream to generate a certain number of check bits called a checksum. This checksum is appended to the message being transmitted. At the reception, the receiver performs the decoding procedure, to verify that the checksum is valid.

A CRC code with symbols from Galois field $GF(2)$ (with two elements 0 and 1) is noted $CRC(n, k)$ where:

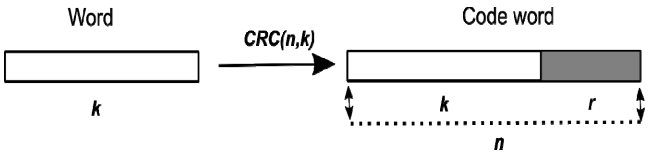
- n: length of the code word (message + checksum).
- k: length of the word (or message).
- $r = n - k$: the checksum.

Figure 1 shows a schematic representation of $CRC(n, k)$ code.

The $CRC(n, k)$ code represents the binary message $M = \{m_1, m_2, \ldots, m_n\}$ to be transmitted as a polynomial $M(x)$ using the following equation:

$$M(x) = \sum_{i=1}^{k} m_i x^{k-i} \tag{1}$$

Figure 1 Schematic representation of $CRC(n, k)$ code



For example, the message $M = \{1101\}$ is represented by $M(x) = x^3 + x^2 + 1$. The transmitter generates a checksum of length r by representing the data stream as a polynomial $M(x)$, multiplying $M(x)$ by x^r and dividing the result by $G(x)$ of degree r. The rest of the division is the checksum which is appended to the polynomial $M(x)$ and transmitted. At the receiver end, the complete transmitted polynomial is then divided by the same $G(x)$. If the result of this division has no remainder R, there are no transmission errors (Tanenbaum, 2003). Algorithms 1 and 3 report the encoding and decoding procedures.

Algorithm 1 CRC encoder procedure

Input:

M: message to be transmitted;

G(x): generator polynomial of degree r.

Output:

M': message with checksum.

Steps:

1 Represent the message M as a polynomial $M(x)$ by performing equation (1).

2 Calculate $M(x) \times x^r$ which is equivalent to appended r zeros bits to the k-bit message.

3 Compute $\frac{M(x) \times x^r}{G(x)}$.

4 The remainder of division $R(x)$ is the generated checksum.

5 Appended the remainder $R(x)$ at the end of $M(x)$.

6 The message being transmitted is $M' = M + R$.

Figure 2 Example of $CRC(7, 4)$ encoder using $G(x) = x^3 + 1$ (see online version for colours)

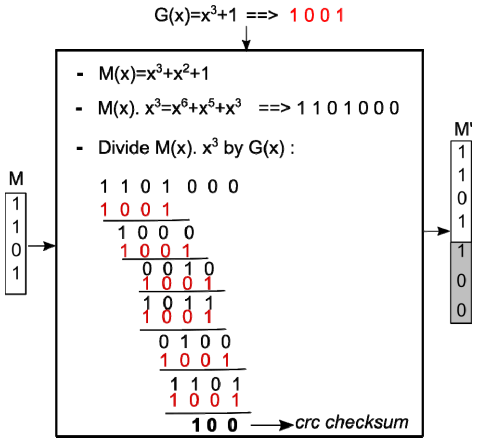


Figure 2 illustrates an example of $CRC(7, 4)$ encoder. Suppose $M = \{1101\}$ the message to be transmitted and $G(x) = x^3 + 1$, which is 1001. Firstly, M is represented as polynomial $M(x) = x^3 + x^2 + 1$. Secondly, multiplying $M(x)$ by x^3 is equivalent to appended three zeros at the end of $M(x)$. Thus, $M(x) \times x^3$ is 1101000. Finally, we have to divide 1101000 by 1001 using modulo-2 arithmetic which is just exclusive-OR operator. At the reception, we propose two scenarios: the first one is without errors and the second one is with errors. These scenarios are illustrated in Figure 3.

Algorithm 2 CRC decoder procedure

Input:

M'': received message;

$G(x)$: generator polynomial of degree r.

Output:

Remainder of division.

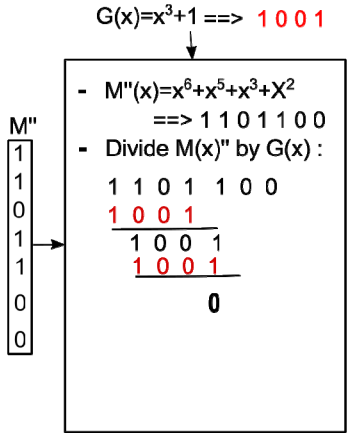
Steps:

1 Represent the message M'' as a polynomial $M''(x)$.

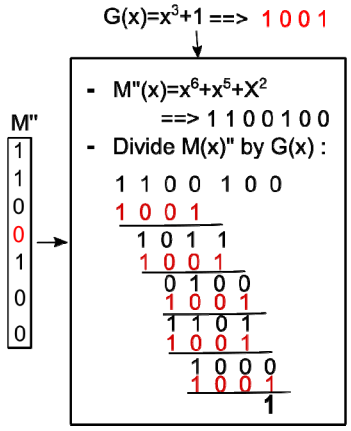
2 Calculate $\frac{M''(x) \times x^r}{G(x)}$.

3 If the remainder is null then the message is not corrupted else it is.

Figure 3 Example of $CRC(7, 4)$ decoder using the same generator $G(x) = x^3 + 1$, (a) scenario without error (b) scenario with error (see online version for colours)



(a)



(b)

The performance of a CRC code is dependent on the choice of a good generator polynomial $G(x)$. Typically, in real applications the degree r of $G(x)$ is between 8 and 32. Table 2 lists standards generator polynomial proved that have many good properties (Ramabadran and Gaitonde, 1988).

Table 2 Generator polynomials of some standard CRC codes

Common name	*Degree*	*Polynomial*
LRCC-8	8	$x^8 + 1$
CRC-12	12	$x^{12} + x^{11} + x^3 + x^2 + x + 1$
CRC-16	16	$x^{16} + x^{15} + x^2 + 1$
CRC-CCITT	16	$x^{16} + x^{12} + x^5 + 1$
LRCC-16	16	$x^{16} + 1$
CRC-32	32	$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

Source: Ramabadran and Gaitonde (1988)

The CRC-32 polynomial used in the IEEE 802.3 (Ethernet) network standard is known to be grossly sub-optimal and very efficient to detect different types of errors (Crow et al., 1997; Koopman, 2002). Since, we have inspired the use of CRC-32 on Internet applications for the digital watermarking.

4 Proposed approach

In this section we described our proposed scheme, which is decomposed from two stages: watermark generation and embedding stage and the tamper detection stage. The first stage performs the CRC encoder procedure to generate a watermark that will be embedding in LSBs. At the second stage, the watermark is extracted and *CRC decoder* procedure is performed to detect tampered packets.

4.1 Watermark generation and embedding algorithm

Algorithm 3 highlights the details of our scheme. In particular, the scheme generates a watermark using the CRC encoder and embedded it to the LSB of each pixel in ROI. The first step effectuated by Algorithm 3 is the segmentation of original image f into two regions: ROI and RONI. Segmentation can be done manually or automatically. The latter is generally intended for a specific medical modality. For example, the approach proposed in Liu et al. (2015) is efficient mass segmentation in mammograms. In order to apply our approach for different modalities, we propose to give freedom to the user to select the ROI. This region is defined as polygon shape because it is not regular in the most of cases. The coordinates of the vertices of this polygon are stored in vector $Vert_{roi}$ and encrypted using a secret key Key_1 to create $Vert_{Encry}$ which is used later in the detection process. Figure 4 illustrates an example of constructing the vector $Vert_{roi}$. For the simplicity of description, we have focused on single ROI. The same algorithms can extend on multiple ROIs. Subsequently, the pixels of extracted ROI are stored in vector *roi* that will be permuting using the second secret key Key_2. This permuted vector is decomposed on packets P_i of 16 pixels, where i is the number of packets. The six mean significant bits (MSBs) of each packet are concatenated to create a binary vector M_{P_i} of size 16 × 6. An example of packet P_i and vector M_{P_i} is shown in Figure 5. A $CRC(128, 96)$ encoder is performed at each vector M_{P_i} to create a checksum of size 32. The generated checksum is the watermark W that will be embedded in spatial domain (1st and 2nd LSBs) of each corresponding pixel to reconstruct the watermarked ROI noted ROI_w. Finally, the watermarked image is created by combining ROI_w and RONI. Figure 6 illustrates the block diagram of watermark generation and embedding.

Algorithm 3 Watermark generation and embedding procedure

Input:

f: original medical image.

Key_1 and Key_2: secret keys.

Output:

f_w: watermarked image;

$Vert_{Encry}$: Encrypted vertices of ROI.

Steps:

1 The user selects manually the ROI from the original image f.

2 The coordinates of vertices of ROI are stored in vector $Vert_{roi}$. The size of this vector is $2 \times N$ where N is the number of vertices. The vector $Vert_{roi}$ is encrypted using pseudo random number Key_1 to return the vector $Vert_{Encry}$.

3 The pixels of ROI are stored in vector *roi* which is randomly permuted using a key Key_2.

4 Decompose the permuted vector on packets P_i of fixed size (16 pixels).

5 For each packet P_i do:

Extract the six bits MSBs form each pixel.

Concatenate these bits together to create a vector M_{P_i} of size 16 × 6.

Perform $CRC(128, 96)$ encoder at M_{P_i} using the standard generator polynomial CRC-32.

A generated checksum is the watermark W_{P_i}

Embedding each two bits of W_{P_i} in 1st and 2nd LSBs of the corresponding pixel to create the watermarked packet P_i^w.

6 Reconstruct roi_w by using the watermarked packets P_i^w.

7 Combine RONI and ROI_w to create the watermarked image.

Figure 4 Example of vector $Vert_{roi}$ (see online version for colours)

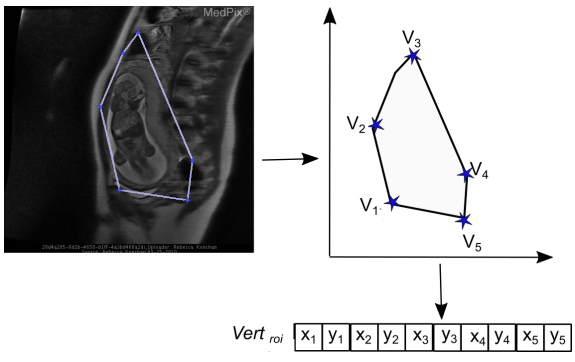
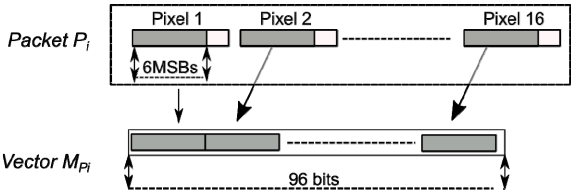


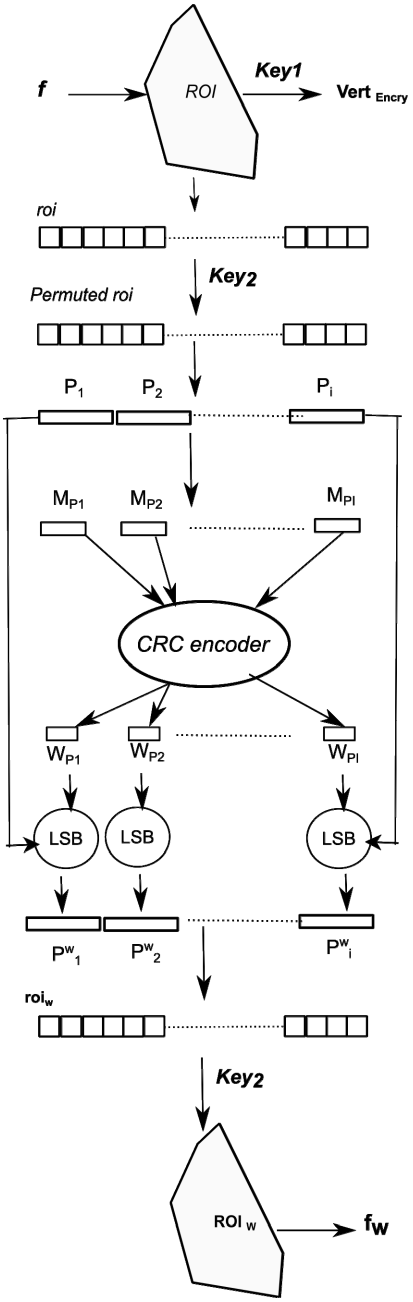
Figure 5 Example of constructing packet P_i and vector M_{P_i}



4.2 Tamper detection algorithm

The extraction and tamper detection is just inverse of embedding and generation process. The details are reported in Algorithm 4.

Figure 6 Block diagram of watermark generation and embedding



5 Simulation and experimental results

In this section, we focus on evaluating the effectiveness of the proposed scheme in terms of imperceptibility and capability of tamper detection. Consequently, tests have been separated into two parts: the first one is for testing the imperceptibility property and second one is for evaluating the fragility (or capabilities of tamper detection) to malicious manipulations.

Algorithm 4 Extraction and tamper detection procedure

Input:

fw: watermarked image.

Key_1 and Key_2: secret keys.

$Vert_{Encry}$: Encrypted vertices of ROI.

Output:

Tamper detection map (TDM);

Steps:

1 Extract the vertices of ROI by Decrypting $Vert_{Encry}$ using Key_1.

2 Extracted vertices are used to decompose the watermarked image into ROI and RONI.

3 The pixels of ROI are stored in vector roi_w.

4 Randomly permute the vector roi_w using Key_2.

5 Decompose the permuted vector on packets P_i^w of fixed size (16 pixels).

6 For each packet P_i^w do:

Extract the six bits MSBs form each pixel.

Concatenate these bits together to create a vector M'_{P_i} of size 16 × 6.

Extract the two bits LSB of each pixels to create the extracted watermark W'_{P_i}.

Append the W'_{P_i} at the end of M'_{P_i} to create the vector W'_{P_i} as shown in Figure 7.

Perform $CRC(128, 96)$ decoder at these sequence using the generator polynomial of degree 32.

If the remainder is null than

$TDM = 1$ which indicates that the packet is not tampered

Else

$TDM = 0$: the packet is corrupted.

Figure 7 Example of extracting the watermark W'_{P_i} and constructing the vector WM_{P_i}

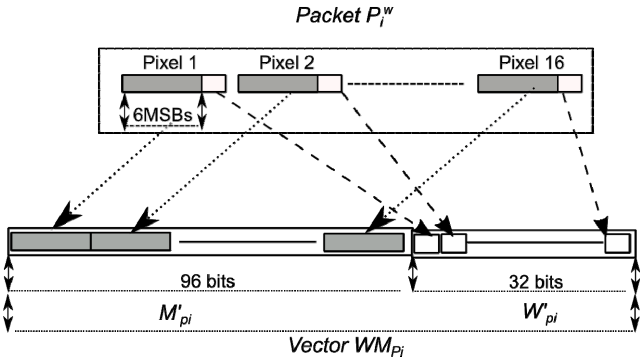
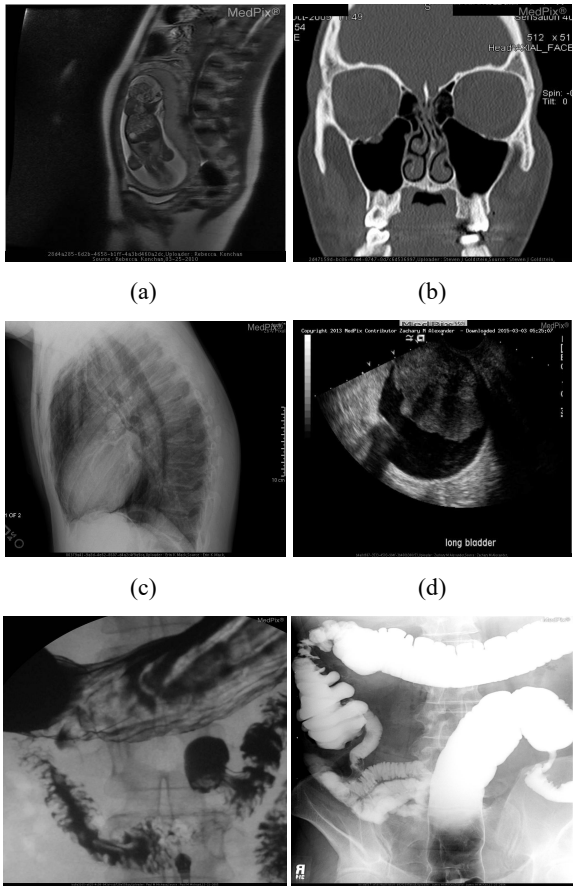


Figure 8 Original medical images, (a) MRI scan (b) CT (c) XR (d) US (e) UGI (f) BE



(a) (b)

(c) (d)

(e) (f)

Experiments are performed on a dataset composed by six different medical image modalities: computed tomography (CT), magnetic resonance imaging (MRI), ultrasound (US), X-ray (XR), upper gastrointestinal series (UGI) and barium enema (BE). These images are downloaded from the free online medical image database (MedPix, 2017) and they are shown in Figure 8.

Table 3 reports the size of different tested images and corresponding selected ROI size.

Table 3 Description of different dataset employed in experiments

Modality	*Size of image*	*Size ROI (%)*
MRI	513 × 512	15
CT	571 × 500	25
XR	637 × 760	43
US	720 × 960	9
UGI	1,024 × 1,085	43
BE	1,001 × 1,200	63

In our experiments, a laptop computer with an Intel i3 CPU 2.GHZ, 4 GB RAM, Windows 7 is used as the computing platform.

5.1 Imperceptibility analysis

The imperceptibility property means that the process of embedding the watermark should not perceptually degrade original image quality. Figure 9 shows selected ROI and the watermarked images f_w.

In order to test the quality of watermarked images two mathematical metrics are used: peak signal to noise ratio (PSNR) and structural similarity metric index (SSIM).

The PSNR estimates the distortion between two images f and f_w. The SSIM evaluates the similarity between them and its values are $\in$ [–1, 1]. The value 1 means that the original and watermarked images are similar. Suppose N_1 and N_2 are height and width of images, PSNR and SSIM are defined as (Roček et al., 2016):

$$PSNR = 10\log_{10}\left(\frac{N_1 \times N_2 \times \max\left(f(i,j)\right)^2}{\sum_{i=1}^{N_1}\sum_{j=1}^{N_2}\left(f(i,j)-f_w(i,j)\right)^2}\right). \tag{2}$$

$$SSIM = \frac{\left(2\times\mu_f\times\mu_{f_w}+C_1\right)\left(2\times\sigma_{ff_w}+C_2\right)}{\left(\mu_f^2+\mu_{f_w}^2+C_1\right)\left(\sigma_f^2+\sigma_{fw}^2+C_2\right)}. \tag{3}$$

where μ_f and μ_{f_w} are the local means, σ_f, σ_{f_w} are the standard deviations and σ_{ff_w} is the covariance. C_1 and C_2 are constants included to avoid a null denominator when $\mu_f^2+\mu_{fw}^2=0$ and/or $\sigma_f^2+\sigma_{f_w}^2=0$.

Table 4 is providing the imperceptibility comparison of proposed scheme with Eswaraiah and Reddy (2014).

Table 4 Quality of the watermarked images through PSNR and SSIM

Modality	*Our scheme*		*Eswaraiah and Reddy (2014)*	
	PSNR	*SSIM*	*PSNR*	*SSIM*
MRI	55.5628	0.9969	50.1560	0.9839
CT	56.0244	0.9965	-	-
XR	50.8052	0.9882	-	-
US	57.8021	0.9970	52.4634	0.9824
UGI	50.8508	0.9861	-	-
BE	48.0818	0.9815	-	-

The results reported in Table 4 show satisfactory results of the proposed scheme. In every case the PSNR values are greater than 48 dB and SIMM are greater than 0.98 and they are best than Eswaraiah scheme. In the case of CT, XR, UGI and BE modalities, Eswaraiah scheme does not work because the ROI size are greater than 25%.

Another approach also was used to estimate the imperceptibility which is the histogram plot that allows to observe the tonal distribution of an image. Therefore, by comparing the histograms of the original and watermarked images, we can judge the imperceptibility (Musrrat et al., 2015). From histogram plots in Figure 10, we can see that they are superimposed which indicate that the difference between the original and watermarked images is non-noticeable to human visual system.

Figure 9 Selected ROI and watermarked images, (a) MRI scan (b) CT (c) XR (d) US (e) UGI (f) BE (see online version for colours)

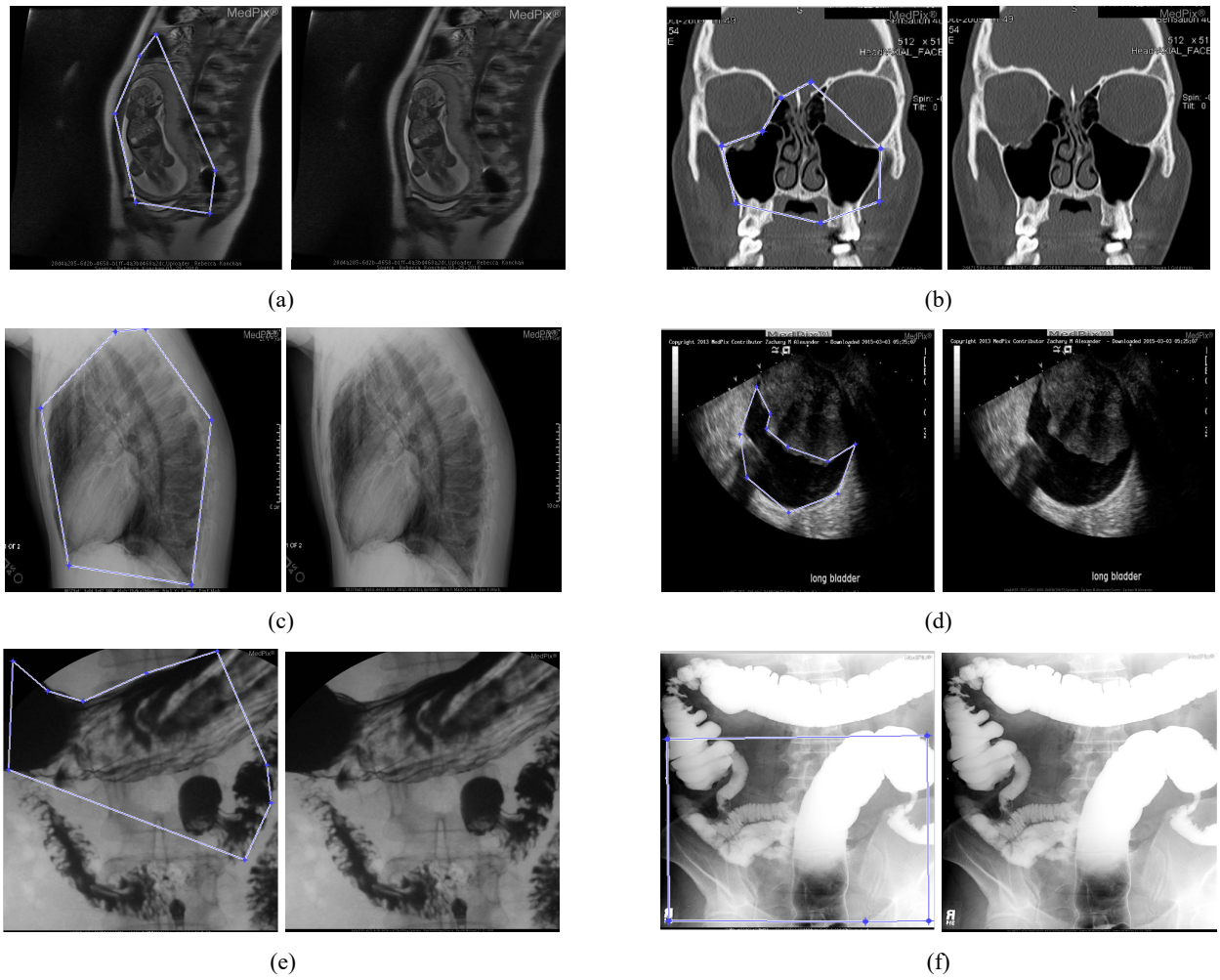


Figure 10 Imperceptibility presentation through histograms for different modalities, (a) MRI scan (b) CT (c) XR (d) US (e) UGI (f) BE (see online version for colours)

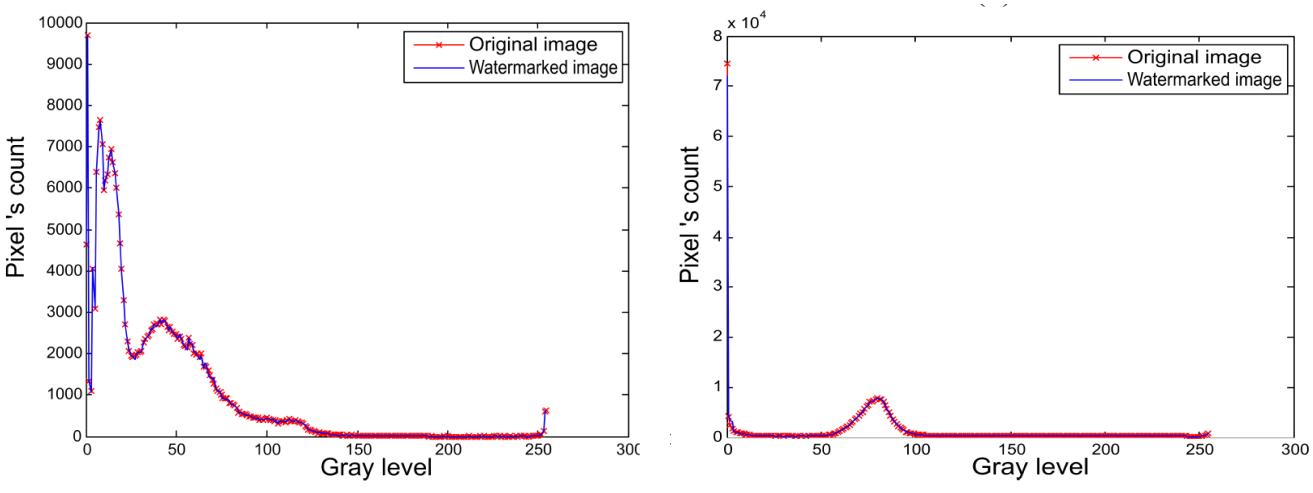


Figure 10 Imperceptibility presentation through histograms for different modalities, (a) MRI scan (b) CT (c) XR (d) US (e) UGI (f) BE (continued) (see online version for colours)

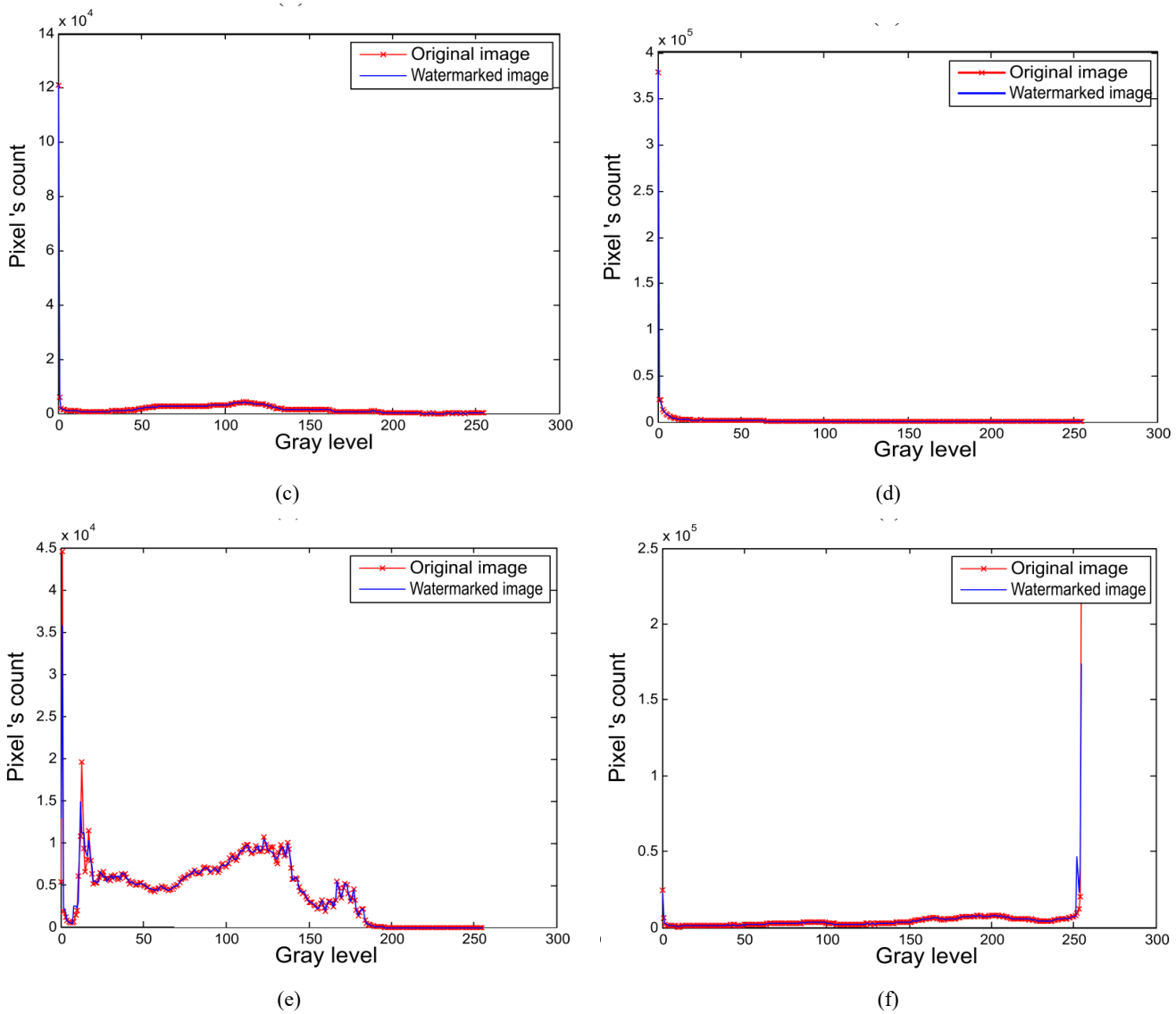
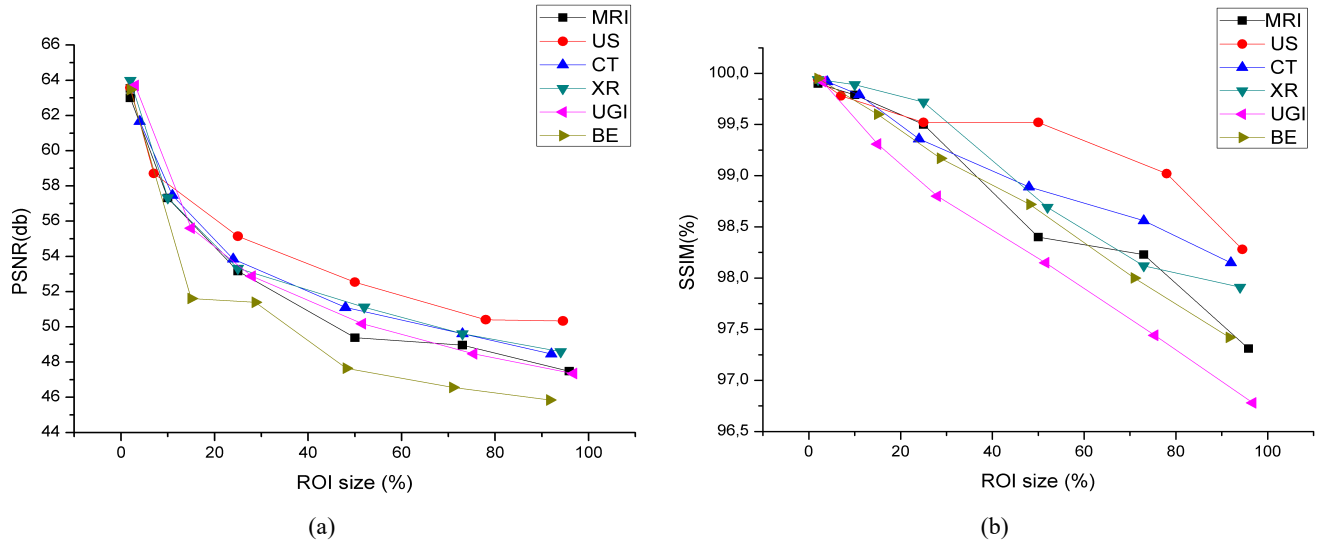


Figure 11 Impact of increasing ROI size on the quality of watermarked images, (a) PSNR plots (b) SSIM plots (see online version for colours)



We evaluate also the impact of increasing the ROI size on the quality of the watermarked image. The results are showed in Figure 11. Form PSNR plots, we can observe that the PSNR values are very good (are in the range of 60 db) for small size of ROI and it still good by increasing the ROI size. When the ROI size is 100% of original image (all image is considered as ROI) the PSNR is equal to 46 db which is considered also as a good. The SSIM plots indicate also that by increasing the ROI size the SSIM values range between 0.96 and 1.

5.2 Correctness and fragility analysis

To examine the efficiency of the proposed approach to detect the alteration, we compute the tamper detection rate *TD* using the following equation:

$$TD = \frac{Number\ of\ tampered\ \ packets\ detected}{Actual\ tampered\ number\ of\ \ packets} \times 100. \qquad (4)$$

The variation of tamper detection of different tampered modalities with respect to tampering percentage is presented in Figure 12. From Figure 12, it is quite evident that the proposed methods detect 100% tampered packets independently on tampering percentage and it performs quite similarly with different modalities.

Figure 12 Variation of tamper detection rate of different tampered modalities with respect to tampered packets percentage (see online version for colours)

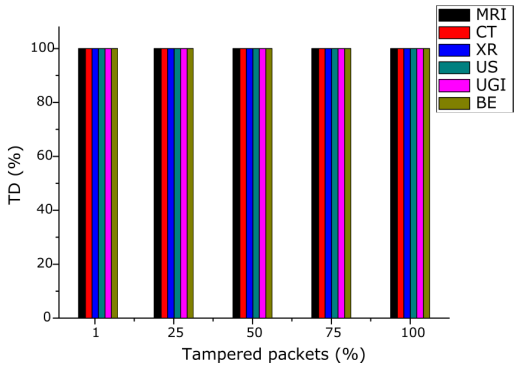


Figure 13 Tamper detection at the packet level (see online version for colours)

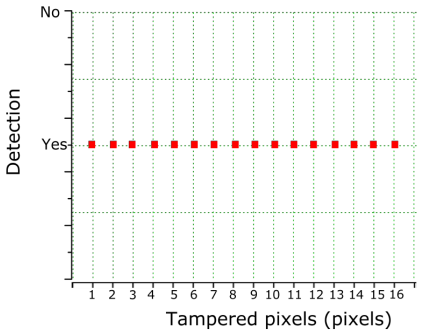
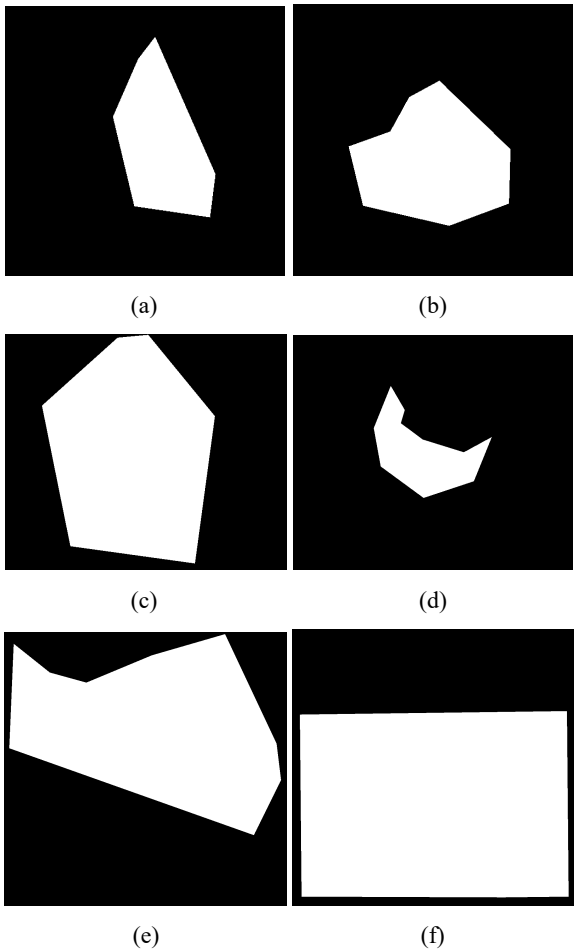


Figure 14 Tamper detection map extracted from watermarked images without any attacks, (a) MRI scan (b) CT (c) XR (d) US (e) UGI (f) BE



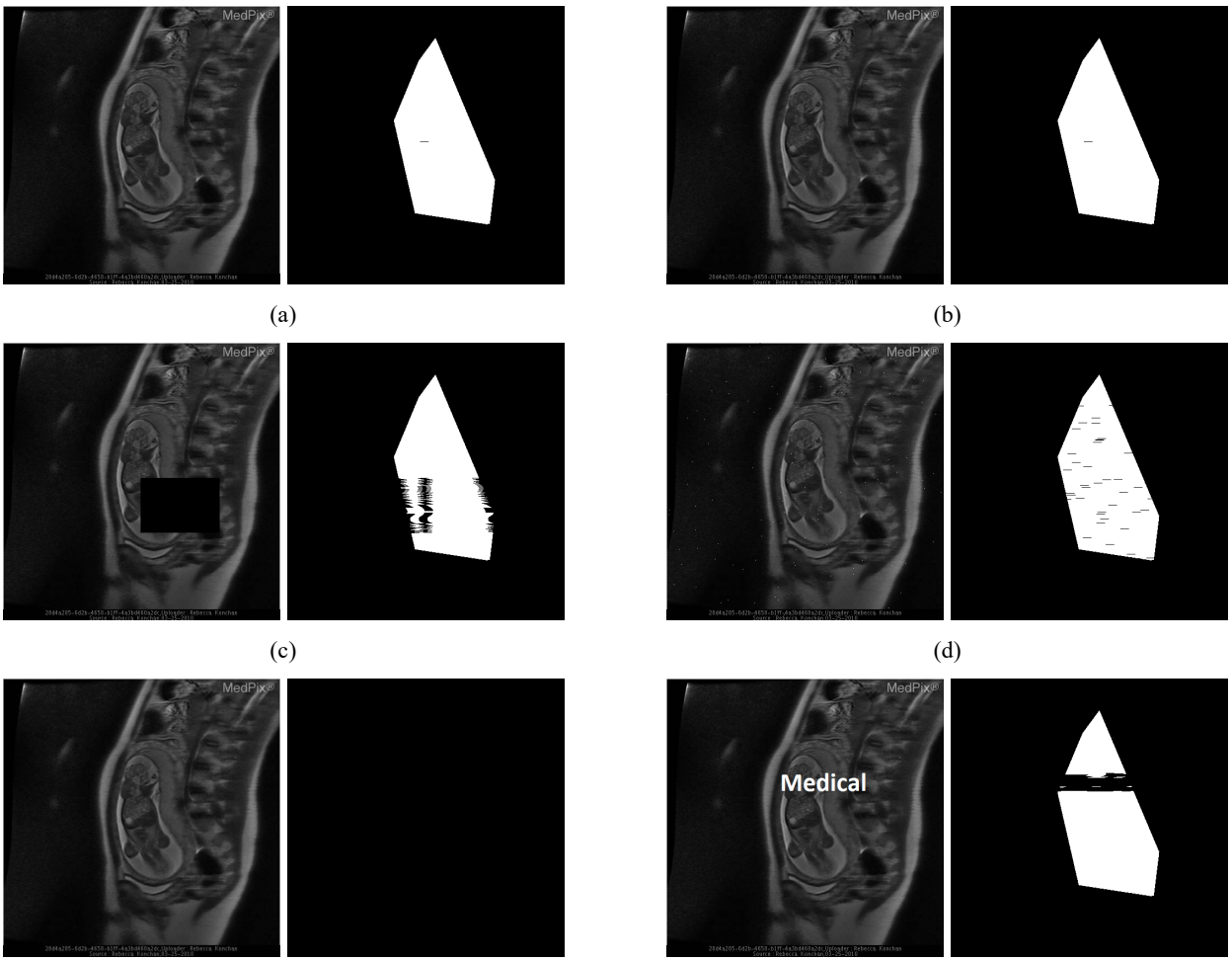
We also test the detection capability at the packet level. Hence, we estimate the capability of detecting that packet is tampered or not with a respect of number of tampered pixels in packet (from 1 pixel to 16 pixels). Figure 13 shows the detection capability at the packet level.

To visually present the correctness and fragility of the proposed scheme, we use tamper detection map (TDM) image to indicate the corrupted packets in ROI. Black pixels in TDM illustrate the corrupted pixels. Figure 14 illustrates the tamper detection map extracted from different watermarked images without any attacks.

To highlight the fragility of our method, we have taken into account several kinds of image watermarking attacks. Figure 15 shows the attacked images and their corresponding extracted TDM.

It is clear that the proposed approach is able to detect reliable attacks (like one bit and one pixel alteration) and strong attacks that alter several or all pixels (like noise and filter).

Figure 15 Fragility against attacks, (a) one bit corrupted (b) one pixel corrupted (c) cropping attacks (d) salt and peppers noise (e) Gaussian noise (f) text copy



(a) (b) (c) (d) (e) (f)

6 Conclusions

In this paper, we propose a ROI-based fragile watermarking scheme for medical images tamper detection. First, the user selects the ROI to be protected. Next, this region is decomposed on packets and CRC encoder procedure is performed on each packet to generate the checksum considered as a watermark to be embedded in LSBs of each corresponding pixel in ROI. At the reception, the receiver extracts the watermark and performs the CRC decoder to detect the tampered pixels.

The performance of our method depends on the degree of generator polynomial. We have chosen the standard generator of degree 32 (CRC-32) which is known from its good capability to detect errors. Experimental results show that our scheme gives a good compromise between imperceptibility and fragility.

In future work, we try to combine the CRC with correcting code like Reed Solomon to recover the ROI.

References

Al-Qershi, O.M. and Khoo, B. (2009) 'Authentication and data hiding using a reversible ROI-based watermarking scheme for DICOM images', in *Proceedings of International Conference on Medical Systems Engineering (ICMSE)*, pp.829–834.

Al-Qershi, O.M. and Khoo, B.E. (2010) 'ROI-based tamper detection and recovery for medical images using reversible watermarking technique', in *2010 IEEE International Conference on Information Theory and Information Security (ICITIS)*, IEEE, pp.151–155.

Ansari, I.A., Pant, M. and Ahn, C.W. (2016) 'SVD based fragile watermarking scheme for tamper localization and self-recovery', *International Journal of Machine Learning and Cybernetics*, Vol. 7, No. 6, pp.1225–1239.

Castiglione, A., De Santis, A., Pizzolante, R., Castiglione, A., Loia, V. and Palmieri, F. (2015) 'On the protection of fMRI images in multi-domain environments', in *2015 IEEE 29th International Conference on Advanced Information Networking and Applications (AINA)*, IEEE, pp.476–481.

Castiglione, A., Pizzolante, R., Palmieri, F., Masucci, B., Carpentieri, B., Santis, A.D. and Castiglione, A. (2017) 'On-board formatindependent security of functional magnetic resonance images', *ACM Transactions on Embedded Computing Systems (TECS)*, Vol. 16, No. 2, p.56.

Chemak, C., Bouhlel, M-S. and Lapayre, J-C. (2007) 'A new scheme of image watermarking based on 5/3 wavelet decomposition and turbo-code', *WSEAS Transaction on Biology and Biomedicine*, Vol. 4, No. 4, pp.45–52.

Crow, B.P., Widjaja, I., Kim, J.G. and Sakai, P.T. (1997) 'IEEE 802.11 wireless local area networks', *IEEE Communications Magazine*, Vol. 35, No. 9, pp.116–126.

Eswaraiah, R. and Reddy, E.S. (2014) 'Medical image watermarking technique for accurate tamper detection in ROI and exact recovery of ROI', *Int. J. Telemedicine Appl.*, Vol. No. 13, pp.1–10.

Fan, Y-C. and Tsao, H-W. (2007) 'A dual pyramid watermarking for JPEG-2000', *International Journal of High Performance Computing and Networking*, Vol. 5, Nos. 1–2, pp.84–96.

Hajjaji, M.A., Mtibaa, A. and Bourennane, E-B. (2011) 'A watermarking of medical image: new approach based on 'multi-layer' method', *International Journal of Computer Science Issues*, Vol. 8, No. 2, pp.33–41.

Hu, W-C. and Chen, W-H. (2013) 'Effective forgery detection using dct+ svd-based watermarking for region of interest in key frames of vision-based surveillance', *International Journal of Computational Science and Engineering*, Vol. 8, No. 4, pp.297–305.

Kejgir, S.G. and Kokare, M.B. (2014) 'Robust multichannel colour image watermarking using lifting wavelet transform with singular value decomposition', *International Journal of Computational Science and Engineering*, Vol. 9, No. 4, pp.371–385.

Kim, C., Shin, D. and Yang, C-N. (2017) 'Self-embedding fragile watermarking scheme to restoration of a tampered image using AMBTC', *Personal and Ubiquitous Computing*, pp.1–12 [online] http://www.link.springer.com/journal/779/onlineFirst/page/2.

Koopman, P. (2002) '32-bit cyclic redundancy codes for internet applications', in *International Conference on Dependable Systems and Networks*, *DSN*, IEEE, pp.459–468.

Kumar, B., Kumar, S.B. and Chauhan, D.S. (2015) 'Wavelet based imperceptible medical image watermarking using spreadspectrum', in *2015 38th International Conference on Telecommunications and Signal Processing (TSP)*, pp.1–5.

Lee, J. and Won, C.S. (2000) 'A watermarking sequence using parities of error control coding for image authentication and correction', *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 2, pp.313–317.

Liew, S-C., Liew, S-W. and Zain, J.M. (2010) 'Reversible medical image watermarking for tamper detection and recovery with run length encoding compression', *World Academy of Science, Engineering and Technology*, Vol. 72, pp.799–803.

Lin, P-L., Huang, P-W. and Peng, A-W. (2004) 'A fragile watermarking scheme for image authentication with localization and recovery', in *IEEE Sixth International Symposium on Multimedia Software Engineering*, pp.146–153.

Liu, F., Gong, Z., Chen, Y. and Gu, Y. (2015) 'Segmentation of mass in mammograms by a novel integrated active contour method', *International Journal of Computational Science and Engineering*, Vol. 11, No. 2, pp.207–215.

MedPix (2017) *Department of Radiology and Radiological Sciences, Uniformed Services University of Health Sciences (USUHS)*.

Mostafa, S.A.K., El-Sheimy, N., Tolba, A.S., Abdelkader, F.M. and Elhindy, H.M. (2010) 'Wavelet packets-based blind watermarking for medical image management', *Open Biomedical Engineering Journal*, Vol. 4, pp.93–98.

Musrrat, A., Chang, A.W., Millie, P. and Patrick, S. (2015) 'An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony', *Information Sciences*, Vol. 301, pp.44–60.

Nayak, J., Bhat, P.S., Kumar, M.S. and Acharya, U.R. (2004) 'Reliable transmission and storage of medical images with patient information using error control codes', in *First India Annual Conference, Proceedings of the IEEE INDICON*, pp.147–150.

Nayak, J., Subbanna Bhat, P., Acharya, U.R. and Sathish Kumar, M. (2009) 'Efficient storage and transmission of digital fundus images with patient information using reversible watermarking technique and error control codes', *Journal of Medical Systems*, Vol. 33, No. 3, pp.163–171.

Pizzolante, R., Castiglione, A., Carpentieri, B., De Santis, A. and Castiglione, A. (2014) 'Protection of microscopy images through digital watermarking techniques', in *International Conference on Intelligent Networking and Collaborative Systems (INCoS)*, IEEE, pp.65–72.

Qi, X. and Qi, J. (2007) 'A robust content-based digital image watermarking scheme', *Signal Processing*, Vol. 87, No. 6, pp.1264–1280.

Ramabadran, T.V. and Gaitonde, S.S. (1988) 'A tutorial on CRC computations', *IEEE Micro*, Vol. 8, No. 4, pp.62–75.

Roček, A., Slavíček, K., Dostál, O. and Javorník, M. (2016) 'A new approach to fully-reversible watermarking in medical imaging with breakthrough visibility parameters', *Biomedical Signal Processing and Control*, 29 August, pp.44–52.

Singh, P. and Agarwal, S. (2016) 'An efficient fragile watermarking scheme with multilevel tamper detection and recovery based on dynamic domain selection', *Multimedia Tools and Applications*, Vol. 75, No. 14, pp.8165–8194.

Su, Q. and Chen, B. (2017) 'Robust color image watermarking technique in the spatial domain', *Soft Computing*, pp.1–16 [online] http://www.link.springer.com/journal/500/onlineFirst/page/22.

Tanenbaum, A. (2003) *Computer Networks*, 4th ed., Pearson Education International, The Netherlands.

Terzija, N. and Geisselhardt, W. (2004) 'Digital image watermarking using complex wavelet transform', in *Proceedings of the 2004 Workshop on Multimedia and Security*, ACM, New York, NY, USA, pp.193–198.

Tjokorda Agung, B.W. and Adiwijaya, F. (2012) 'Medical image watermarking with tamper detection and recovery using reversible watermarking with LSB modification and run length encoding (RLE) compression', in *2012 International Conference on Communication, Networks and Satellite (ComNetSat)*, IEEE, pp.167–171.

Yang, C-H., Weng, C-Y., Wang, S-J. and Sun, H-M. (2008) 'Adaptive data hiding in edge areas of images with spatial LSB domain systems', *IEEE Transactions on Information Forensics and Security*, Vol. 3, No. 3, pp.488–497.

Zhou, X., Duan, X. and Wang, D. (2004) 'A semi-fragile watermark scheme for image authentication', in *Proceedings 10th International Multimedia Modelling Conference*, pp.374–377.