SIViP (2015) 9:1163–1178
DOI 10.1007/s11760-013-0555-x

ORIGINAL PAPER

Robust watermarking method in DFT domain for effective management of medical imaging

Manuel Cedillo-Hernandez · Francisco Garcia-Ugalde · Mariko Nakano-Miyatake · Hector Perez-Meana

Received: 15 December 2012 / Revised: 3 September 2013 / Accepted: 4 September 2013 / Published online: 5 October 2013

Abstract In general, management of medical data is achieved by several issues of medical information such as authentication, security, integrity, privacy, among others. Because medical images and their related electronic patient record (EPR) data are stored separately; the probability of corruption of this information or their detachment from the corresponding EPR data could be very high. Losing data from the corresponding medical image may lead to a wrong diagnostic. Digital watermarking has recently emerged as a suitable solution to solve some of the problems associated with the management of medical images. This paper proposes a robust watermarking method for medical images to avoid their detachment from the corresponding EPR data in which the watermark is embedded using the digital imaging and communications in medicine standard metadata together with cryptographic techniques. In order to provide a high robustness of the watermark while preserving at the same time a high quality of the watermarked images, the generated watermark is embedded into the magnitude of the middle frequencies of the discrete Fourier transform of the original medical image. During the detection process, the watermark data bits are recovered and detected using the bit correct rate criterion. Extensive experiments were carried out, and the performance of the proposed method is evaluated in terms of imperceptibility, payload, robustness and detachment detection. Quantitative evaluation of the watermarked images is performed by using three of the more common metrics: the peak signal-to-noise ratio, structural similarity index and visual information fidelity. Experimental results show the watermark robustness against several of the more aggressive geometric and signal processing distortions. The receiver operating characteristics curves also show the desirable detachment detection performance of the proposed method. A comparison with the previously reported methods with similar purposes respect to the proposed method is also provided.

Keywords Digital watermarking · Discrete Fourier transform · Medical imaging · DICOM imaging · Robust watermarking · Authentication · Detachment detection

M. Cedillo-Hernandez (✉) · F. Garcia-Ugalde
Electrical Engineering Division, Engineering Faculty, National Autonomous University of Mexico, Circuito Exterior, Ciudad Universitaria, Coyoacan, 04510 Mexico City, Mexico
e-mail: mcedillohdz@hotmail.com
URL: http://dps.fi-p.unam.mx/FGU/FGU.html
URL: http://www.posgrados.esimecu.ipn.mx/index.php

F. Garcia-Ugalde
e-mail: fgarciau@unam.mx

M. Nakano-Miyatake · H. Perez-Meana
Mechanical Electrical Engineering School, National Polytechnic Institute of Mexico, Av. Santa Ana 1000, San Francisco Culhuacan, Coyoacan, 04430 Mexico City, Mexico

M. Nakano-Miyatake
e-mail: mnakano@ipn.mx

H. Perez-Meana
e-mail: hmperezm@ipn.mx

1 Introduction

At present, medical imaging infrastructure produces medical images in digital format, and the spread used DICOM format (2003 standard for digital imaging and communications in medicine) [1] is a standard for manipulation, printing, transmission and storage of digital medical images and their related information, e.g., patient's data, medical doctor's data, health care centers, among others [2]. DICOM includes the definition of a file format and a communications protocol based on TCP/IP. The DICOM files may be

exchanged among several equipments that fulfill with the DICOM standard, such as scanners, visualization stations, printers and PACS (Picture Archiving and Communications System). The medical file of a patient is composed by clinical examinations, diagnostics, prescriptions and digital images of several types [1–14] that are stored in the electronic patient record (EPR).

This standardization of medical information and high progress of information technology (IT) provide new ways to store, access and distribute medical data, which are used efficiently in telemedicine, remote diagnostics, etc., allowing good progress in medical care. However, the security issues related to the management of the medical digital information have raised new problems, because the confidentiality of digital patient's data may be more vulnerable than those analog versions. Currently now, several security tools such as firewalls, encryption algorithms, software accreditation and access control are used to provide protection to the confidentiality and integrity of the medical information [1,2]; however, these complementary security tools cannot resolve all security issues of medical information. One of the critical problems that the above-mentioned security tools cannot figure out is the detachment problem of several data of EPR, especially medical images, because in DICOM standard, an image is identified by an attached file and patient's data related to the image are stored separately as metadata. Considering that the detachment of medical images from their corresponding medical data may lead to a wrong diagnostic, this problem must be of critical importance. A suitable solution recently emerged to avoid the detachment problem is the use of digital watermarking techniques [15–19], combined with cryptographic techniques [20]. This solution provides a means to verify that the medical images belong to the correct patient and comes from a dependable information source. Generally, it consists in embedding the ciphered version of the patient's EPR data or an identification code, into the image as a watermark signal.

In the literature, several watermarking-based solutions to hide EPR data with purposes to solve the detachment problem are proposed [10–14]. In this way, authors in [10] propose a watermarking method to hide EPR information and optionally a region of interest (ROI) of the same medical image, obtained and selected manually by the end user. The embedding and extraction procedures are performed in the low-pass sub-bands of the contourlet transform. To increase the security of the method, the EPR data are encrypted using the Advanced Encryption Standard (AES) algorithm [20]. To correct the errors during the extraction stage, a Bose, Chaudhuri and Hocquenghem (BCH) error correcting code is used. The method presents robustness against JPEG and JPEG 2000 compression as well as to impulsive noise contamination and several image filters, such as Gaussian, mean, median, among others. In addition, the work in [11] proposes a multi-watermarking algorithm applied to medical imaging. A caption watermark associated with the EPR data, a signature watermark related to an identification code of the source of the medical image and an index that serves as a keyword for use in medical image databases, is embedded and extracted in 13 sub-bands of the 4-level discrete wavelet transform (DWT) domain. To correct the errors during the extraction stage, a BCH error correcting code is used in the method. The approach considers the robustness against JPEG and JPEG 2000 compression as well as to Gaussian and impulsive noise, sharpening, cropping, low-pass filter and histogram equalization. In [12], the authors propose a contourlet-based dual watermarking scheme applied to DICOM imaging. In a similar manner as in [11], a couple of watermarks are embedded as follows: A caption watermark that gives a permanent link between the patient and the medical data is generated from 230 alphanumeric characters of EPR patient's data that are converted to ASCII code and this in turn is converted to a binary vector to be embedded inside a rectangle in the ROI of the medical image. The second pattern is the signature watermark which is related to an identification code of the source of the medical image as a logo with size 10×40 that is embedded inside a rectangle in the region of non-interest (RONI) that surrounds the rectangular ROI region. The data bits of both watermark patterns are embedded in the singular value decomposition (SVD) of the embedded blocks within low-pass sub-band in contourlet transform with adaptive embedding strength in ROI and RONI regions of the medical image, respectively. The method presents robustness against image filtering such as mean, median, as well as impulsive noise contamination and scaling. To improve the watermark robustness against aggressive attacks such as geometrical distortions, specifically the image rotation, authors of [13] have proposed a method in which the image moment theory is applied and combined with an encryption technique for watermarking of medical images. In order to reduce the amount of embedding data, they compressed the DICOM metadata using a Huffman code. To increase the security, the compressed data are encrypted using the RC4 scheme [20]. From the encrypted data, a bi-dimensional pattern is generated and works as a watermark signal itself. Using the two first-order moments, the image centroid is obtained and established as the origin of a scan operation by applying a polar mapping. The embedding process is done in areas with low homogeneity; it is calculated using the variance (σ^2) of a block of $k \times k$ pixels, scanning the image in a spiral way using the centroid as the origin of this scan. In the detection stage, the watermarked image is scanned in the same spiral way starting from the centroid of the image. Hence, by comparing the grayscale level of the center pixel of an area with the grayscale level of its mean, one watermark data bit is extracted from the area. The method presents robustness against adjustment of brightness and contrast, JPEG

compression and small rotations. Authors in [14] propose a watermarking algorithm based on discrete wavelet packet transform (DWPT) for protecting the EPR information. To generate the watermark pattern, information obtained from the EPR is converted to ASCII code and this in turn is converted to binary data. The resulting binary data are encoded using the error correcting code BCH and are embedded in two sub-band with middle energy from the two-level DWPT. A reference image composed by a binary logo of the medical center is used to embed the watermark according to the embedding rules. The scheme is robust against Gaussian noise, gamma correction, histogram equalization, contrast adjustment, rotation, sharpen, median filter and JPEG lossy compression.

In this paper, we propose an effective and robust watermarking method applied to medical imaging, where detachment of the medical image from the EPR information can be avoided using watermark data. The proposed method combines DICOM metadata and encryption techniques to produce a watermark pattern; it is embedded into the magnitude of the middle frequencies of DFT of the original medical image in order to preserve a high image quality.

After the embedding process, the watermarked medical image preserves the DICOM format and its original dimensions. During the detection stage, at the same time that the medical image comes from dependable information source, the watermark data bits are recovered and detected using the BCR criterion to prove the correspondence between the image and the EPR information. The watermarked image quality is measured with well-known metrics used in image processing such as the PSNR, SSIM and VIF. The experimental results show the watermark robustness against several geometric and signal processing distortions; also, it confirms that the proposed scheme provides a correct correspondence between the medical image and its related metadata.

The rest of this paper is organized as follows. Section 2 describes the watermark generation, embedding and detection process of the proposed algorithm. The experimental results including comparison with previous reported watermarking algorithms are presented in Sect. 3. Finally, Sect. 4 concludes this work.

2 Proposed algorithm

The main steps of the proposed watermarking method consist of the watermark generation, embedding and detection process. General diagrams of each stage are shown in Figs. 1, 2 and 3, respectively.

2.1 Watermark generation

The watermark generation is described as follows:

1. Read the DICOM file and extract the key information from the DICOM metadata, e.g., patient name, patient age, institution name, station name, patient ID, patient sex, patient birth date.
2. Apply the RACE Integrity Primitives Evaluation Message Digest RIPEMD-160 [21,22] to the DICOM metadata selected in the previous step. We would like to note that our proposed method may be easily adapted to the use of others message digest algorithms for example the Tiger/160 or HAVAL [20].
3. Once the hash sequence is obtained, convert the 40 hexadecimal digits to its 160 bits binary representation.
4. Split the binary representation into two blocks of 80 bits each one and apply an XOR operation between this two blocks, according to (1):

$$W_m = b_k \oplus b_l, \tag{1}$$

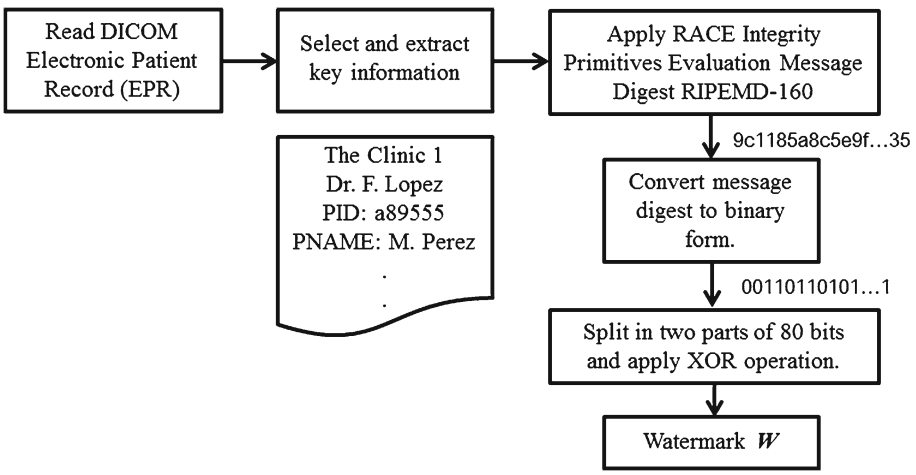


Fig. 1 General diagram of the watermarking generation process

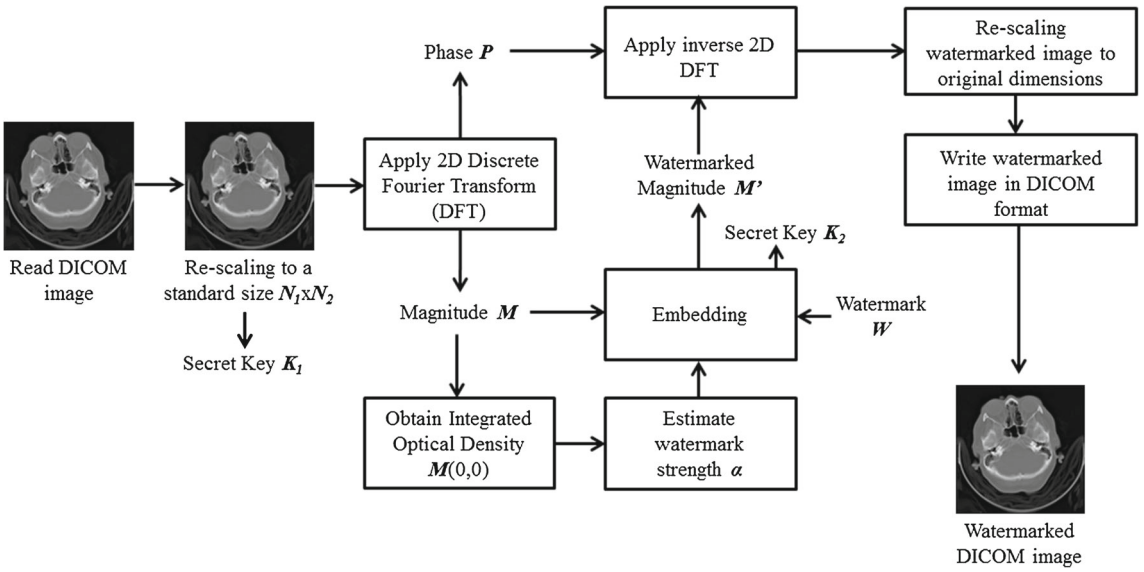
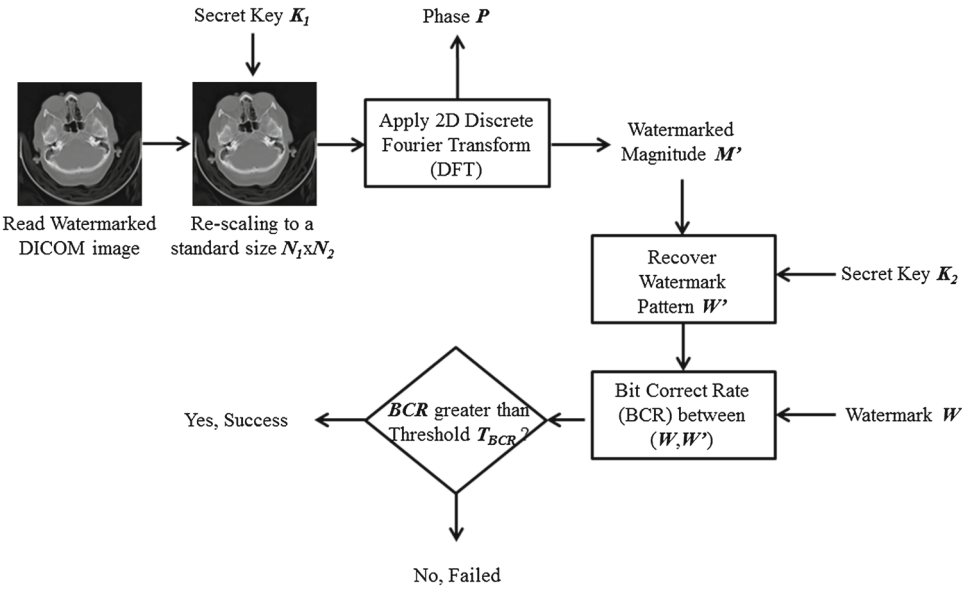


Fig. 2 General diagram of the watermark embedding process

Fig. 3 General diagram of the watermark detection process



where $m, k = 1, \ldots 80$ and $l = 81, \ldots 160$, b denotes the kth and the lth bits from each block, respectively, and W corresponds to the result of the XOR operation denoted by $\oplus$.

5. In this manner by its computation the resulting 80 bits of the watermark pattern W of length $L = 80$ bits are directly dependent on the key information of the DICOM metadata.

2.2 Watermarking embedding process

The watermark embedding process is described in the following steps:

1. Read the original DICOM image $I(x, y)$ in a grayscale intensity and rescale it to a standard size of $N_1 \times N_2$.
2. Apply the 2D DFT to the original resized image $I(x, y)$ of size $N_1 \times N_2$ given by (2):

$$F(u, v) = \sum_{x=1}^{N_1} \sum_{y=1}^{N_2} I(x, y) e^{-j2\pi(f_1 x/N_1 + f_2 y/N_2)}, \qquad (2)$$

and obtain the magnitude $M(u, v) = |F(u, v)|$ and phase $P(u, v)$ of $F(u, v)$ components. In order to increase the security of the proposed method, N_1, N_2 values will be provided also as secret key K_1 in the detection stage. The secret key K_1 shown in Fig. 2 has to be known by the watermark detector.

By the properties of the DFT, the translations in the spatial domain do not affect the magnitude of the DFT transform, as shown in (3):

$$|\mathrm{DFT}\,[I(x+x_1, y+y_1)]| = M(u, v). \tag{3}$$

Concerning the scaling in the spatial domain, it causes an inverse scaling in the frequency domain, see (4):

$$\mathrm{DFT}\,[I(\rho x, \rho y)] = \frac{1}{\rho} F\left(\frac{u}{\rho}, \frac{v}{\rho}\right). \tag{4}$$

where ρ is the scaling factor. And rotation in the spatial domain causes the same rotation in the frequency domain, (5):

$$\begin{aligned}&\mathrm{DFT}\,[I(x\cos\theta - y\sin\theta, x\sin\theta + y\cos\theta)]\\ &= F(u\cos\theta - v\sin\theta, u\sin\theta + v\cos\theta)\end{aligned} \tag{5}$$

Thus, selecting the DFT domain to embed the watermark W has a certain number of advantages for rotation, scaling and translation (RST) invariance as well as watermark robustness against common signal processing. Although some attacks may be considered unusual in the medical imaging field, e.g., pixel translation with cropping attack, the proposed algorithm is designed to be robust against a wide range of intentional or non-intentional distortions.

3. Considering that the distortion caused by the watermark embedding may affect the image contents and it may lead to an erroneous medical diagnostics, the watermark strength must be carefully evaluated. In order to measure any perceptual distortions, the integrated optical density, which describes the appearance of an image, is obtained. The integrated optical density is strongly characterized by the radial frequency portrait of the DFT such that the concentration of large coefficients near the DFT origin depends on the existence of large and smooth image components, often belonging to smooth object surfaces or background. Note that nearly every image will have a significant peak at the DFT origin (unless it is very dark), since from (6), $M(0, 0)$ is the accumulated intensity of the image (integrated optical density) [23]:

$$M(0,0) = \sum_{x=1}^{N_1}\sum_{y=1}^{N_2} I(x, y). \tag{6}$$

4. Once that the integrated optical density is obtained, the watermark strength α is calculated by (7):

$$\alpha = M(0,0)/\beta, \tag{7}$$

where $M(0, 0)$ denotes the integrated optical density given by (6) and β is an adaptive value dependent on the medical image type, i.e., computed radiography (CR), radio fluoroscopy (RF), magnetic resonance (MR) and computed tomography (CT).

5. Based on the energy distribution in the DFT domain, the watermark embedding is carried out by selecting a pair of radius r_1 and r_2 in $F(u, v)$ and its corresponding annular area $A = \pi(r_2^2 - r_1^2)$ between r_1 and r_2 what should cover the middle frequency components in the DFT domain around the zero frequency term; the reason of positioning this area in the middle frequencies is because modifications in the magnitude of low frequencies of the DFT will cause a visible distortion in the spatial domain of the image. And on the other hand, modifications of the magnitudes of the high frequencies may affect considerably the JPEG lossy compression quality. Thus, the embedding of the watermark pattern in the middle frequencies band must preserve the robustness respect to the JPEG compression and at the same time preserves a high degree of imperceptibility. Based on these arguments, the goal is to find the correct pair of radius r_1 and r_2. Fortunately, there are enough radiuses in the middle frequencies band that may satisfy the trade-off between robustness and imperceptibility; in this band of frequencies, one couple of values may be selected randomly in order to increase the security of the proposed method, and the chosen values will be provided as a secret key K_2 in the detection stage. Then the secret key K_2 shown in Fig. 2 is also known by the watermark detector.
6. Considering the four quadrants of the DFT magnitude, select the middle frequencies band. So that to ensure the correct watermark embedding of robustness and imperceptibility, the condition $(A/4) \geq L$ should be satisfied, where A indicates the annular area between r_1 and r_2 and L is the watermark length.
7. In the annular region compute the magnitude difference denoted by d between the magnitude coefficients from the first and the second quadrants of the upper half part of the DFT magnitude, respectively, $d = M_i(u_j, v_j) - M_i(-u_j, v_j)$, where $j = 1, \ldots, L$ denotes an index pointing to the watermark data bits, as shown in Fig. 4.
8. Once the difference d is calculated, consider a watermark strength parameter α in order to modify the DFT middle frequencies magnitudes in a controlled manner as follows: If the watermark data bit $w_i = 0$ and $d < (-\alpha)$, then $M_i(u_j, v_j)$, $M_i(-u_j, v_j)$ will not be modified. On the other hand, if $d \geq (-\alpha)$, then $M_i(u_j, v_j)$, $M_i(-u_j, v_j)$ are modified according to (8):

$$\begin{aligned}M_i'(u_j, v_j) &= M_i(u_j, v_j) - (\alpha + d)\\ M_i'(-u_j, v_j) &= M_i(-u_j, v_j) + (\alpha + d),\end{aligned} \tag{8}$$

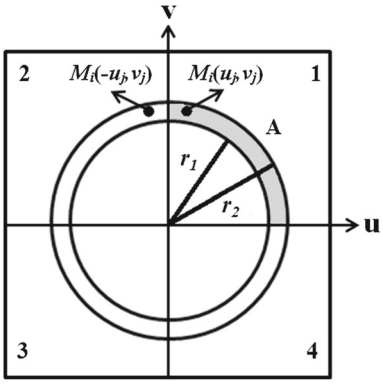


Fig. 4 Modification of DFT magnitude coefficients, shading region denotes condition $(A/4) \geq L$

In these equations, the difference d is added to the watermark strength α in order to force the compliance of the condition $d < (-\alpha)$ when $w_i = 0$, providing a large enough margin between $M_i'(u_j, v_j)$ and $M_i'(-u_j, v_j)$ in order to preserve $d < (-\alpha)$ after that the watermarked medical image is processed by a common signal processing or a geometric distortion.

If the watermark data bit $w_i = 1$ and $d > \alpha$, then $M_i(u_j, v_j)$, $M_i(-u_j, v_j)$ will not be modified. On the other hand, if $d \leq \alpha$, then $M_i(u_j, v_j)$, $M_i(-u_j, v_j)$ are modified according to (9):

$$\begin{aligned} M_i'(u_j, v_j) &= M_i(u_j, v_j) + (\alpha - d) \\ M_i'(-u_j, v_j) &= M_i(-u_j, v_j) - (\alpha - d), \end{aligned} \tag{9}$$

where the difference d is subtracted from the watermark strength α in order to force the compliance of the condition $d > \alpha$ when $w_i = 1$, providing a large enough margin between $M_i'(u_j, v_j)$ and $M_i'(-u_j, v_j)$ in order to preserve $d > \alpha$ after that the watermarked medical image is processed by a common signal processing or a geometric distortion. In (8) and (9), $i = 1, \ldots, L$ denotes an index pointing to the corresponding w_i watermark data bits, $M_i(u_j, v_j)$, and $M_i(-u_j, v_j)$ denotes the original magnitude coefficients. And $M_i'(u_j, v_j)$ and $M_i'(-u_j, v_j)$ denote the watermarked magnitude coefficients. A larger value of α would increase the robustness of the watermark, on the other hand, the watermark imperceptibility is less affected with a small value of α. Hence, there is a trade-off between robustness and imperceptibility. According to DFT symmetrical properties in order to produce real values after the DFT magnitude is modified, the watermark was embedded into the upper half part of the middle frequencies of the DFT magnitude coefficients, and by consequence, the lower half part of the middle frequency band should be modified symmetrically. These DFT symmetrical properties allows the correct detection of the watermark when the watermarked image is rotated, because while the secret key K_1 keeps a standard size of $N_1 \times N_2$, the secret key K_2 provides the correct pair of radius r_1 and r_2, and both are known in the watermark detector. It is just needed an exhaustive search in the range $[-\pi, \pi]$ in order to detect the watermark. By repeating the above-mentioned procedure, the total L watermark data bits can be embedded in the annular region.

9. The watermarked image $I'(x, y)$ is obtained applying the inverse DFT (IDFT) to the watermarked magnitude $M'(u, v)$ in conjunction with the corresponding original phase $P(u, v)$ as shown (10).

$$I' = \text{IDFT}(F'), \quad F' = (M', P). \tag{10}$$

10. Finally, rescaling the watermarked image $I'(x, y)$ to its original dimensions and converts it to the DICOM native format.

2.3 Watermark detection process

The watermark detection process is described in the following steps:

1. Read the DICOM watermarked image $I'(x, y)$ in grayscale intensity and using the secret key K_1 that provides the same pair of values N_1 and N_2 used in the frequency domain embedding process, rescale it to the chosen size $N_1 \times N_2$.
2. Obtain the bi-dimensional DFT transform $F'(u, v)$ of the watermarked image $I'(x, y)$. Then the watermarked magnitude $M'(u, v) = |F'(u, v)|$ and the phase $P(u, v)$ are obtained from $F'(u, v)$.
3. Using the secret key K_2 that provides the same pair of radiuses r_1 and r_2 used in the frequency domain embedding process compute the annular area A.
4. Split the DFT magnitude $M'(u, v)$ in its four quadrants in the frequency domain and compute the subtraction operation $s_i = M_i'(u_j, v_j) - M_i'(-u_j, v_j)$ of the first and second quadrants of the upper half part of the watermarked DFT magnitude in the annular region A.
5. Recover the watermark pattern W' using the *sign* function as follows: if $sign(s_i)$ is '+' or '0,' then $w_i' = 1$, otherwise $w_i' = 0$, where $i = 1, \ldots, L$. Remember that L is the watermark length in the annular region A.
6. Applying the watermark generation procedure computes the original watermark pattern W using the same key information from the corresponding DICOM metadata. According to (11) calculate the bit correct rate (BCR) for binary data [24] between the original and the recovered watermark patterns W and W', respectively.

$$\mathrm{BCR} = \frac{L - \sum_{i=1}^{L} W_i \oplus W_i'}{L}, \tag{11}$$

where $L = 80$ is the watermark length and $\oplus$ denotes a module 2 addition, or XOR operation.

7. Assuming ergodicity, the BCR is defined as the ratio between the number of correctly decoded bits and the total number of embedded bits. A threshold value T_{BCR} must be defined to determine when the watermark W is present or not in the medical image. In order to formalize the computation of this threshold, we consider a binomial distribution with success probability equal to 0.5, then the false alarm probability P_{fa} for L bits embedded watermark data is given by (12), and a threshold value T must be provided in order to P_{fa} becomes smaller than a predetermined value [25].

$$P_{\mathrm{fa}} = \sum_{z=T}^{L} \left(\frac{1}{2}\right)^{L} \cdot \left(\frac{L!}{z!(L-z)!}\right), \tag{12}$$

where L is the total number of watermark data bits, whose value is empirically set to 80 and based on the Bernoulli trials assumption, z is independent random variable with binomial distribution [25]. When $T = 60$, the false alarm probability must be less than $P_{\mathrm{fa}} = 4.29 \times 10^{-6}$; this value satisfies the requirements of most watermarking applications for a reliable detection [25], and then an adequate threshold value is $T_{\mathrm{BCR}} = T/L = 60/80 = 0.75$. Recall by the inclusion–exclusion probability principle that the addition of the bit error rate (BER) and the bit correct rate (BCR) must be equal to 1.

8. Finally, if the BCR value is greater than the threshold value T_{BCR}, the watermark pattern is detected and the medical image is considered belonging to the right patient and that it corresponds to the correct metadata. Otherwise, if the BCR is less than 75 % (less than 60 correct bits), the detection process rejects the image because it does not correspond to the metadata or because the image is not watermarked.

3 Experimental results and comparisons

This section presents the evaluation results of the proposed watermarking method applied to medical imaging, using a set of 100 medical images in DICOM format and different types: CR, RF, MR and CT. The set of CR images is composed by several thorax images; RF by several abdomen and esophagus images, MR by skull, brain and shoulder images and finally, CT by simple skull, brain and abdomen images. The test key information obtained from DICOM metadata to compose the watermark pattern W of size $L = 80$ bits consist of patient name, patient age, institution name, station name, patient ID, patient sex and patient birth date. Empirically, the pair of scaling values and radiuses have been set to $N_1 = N_2 = 512$, $r_1 = 80$ and $r_2 = 81$, and these values are provided as secret keys K_1 and K_2, respectively, in the detection stage. Depending on the medical image type, the watermark strength α is estimated to achieve the required imperceptibility and robustness using the accumulated intensity of the image $M(0, 0)$ and β as given in (6). In order to have a reference to the processing time, we precise that our experiments are carried out on a personal computer running win7© with an AMD© Athlon processor (2.7Ghz) and 4GB RAM in which the embedding and extracting procedures were implemented using MATLAB© 7.10. In our system, the embedding process is done in about 8.89 s, while the detection process in about 5.87 s.

The performance of the proposed algorithm has been evaluated in terms of watermark imperceptibility, payload and robustness. Also the false positive and false negative errors when the integrity of combination of medical image and metadata is confirmed have been measured.

3.1 Watermark imperceptibility

Figure 5 shows the original DICOM images (left column) together with their watermarked versions (right column). Figure 5a corresponds to a grayscale CR image with 4,280 × 3,520 × 10 bits. Figure 5b shows a grayscale RF image with 1,024 × 1,024 × 10 bits. Figure 5c, d corresponds to grayscale CT and MR images with 512 × 512 × 12 and 256 × 256 × 12 bits, respectively. For illustrative purposes, all figures presented in this section are grayscale rescaled and down-sampled to 8 bits per pixel.

Using the parameters $L = 80$, $r_1 = 80$ and $r_2 = 81$ and a variable watermark strength α from 20 to 100, the watermark imperceptibility was evaluated in terms of PSNR, VIF [26] and SSIM [27] given by (13), (14) and (15), respectively.

$$\mathrm{PSNR\ (dB)} = 10 \log_{10} \left(\frac{N_1 \cdot N_2 \cdot \mathrm{Max\ Pixel\ Value}^2}{\sum_{x=1}^{N_1} \sum_{y=1}^{N_2} (I(x, y) - I'(x, y))^2} \right), \tag{13}$$

$$\mathrm{VIF} = \frac{\sum_{k \in \mathrm{channels}} I(\vec{C}^{Z,k}; \vec{G}^{Z,k} | s^{Z,k})}{\sum_{k \in \mathrm{channels}} I(\vec{C}^{Z,k}; \vec{E}^{Z,k} | s^{Z,k})}, \tag{14}$$

In (14), the addition is on the channels of interest, $\vec{C}^{Z,k}$ represents Z elements of the random field RF C_k that describes the coefficients of the channel k, and so on [26]. E and G denote the visual signal at the output of the human visual system model (HVS) of the original and the watermarked images, respectively, from which the brain extracts cognitive information. $I(\vec{C}^{Z,k}; \vec{E}^{Z,k} | s^{Z,k})$ and $I(\vec{C}^{Z,k}; \vec{G}^{Z,k} | s^{Z,k})$ correspond to the information that can be ideally extracted by the

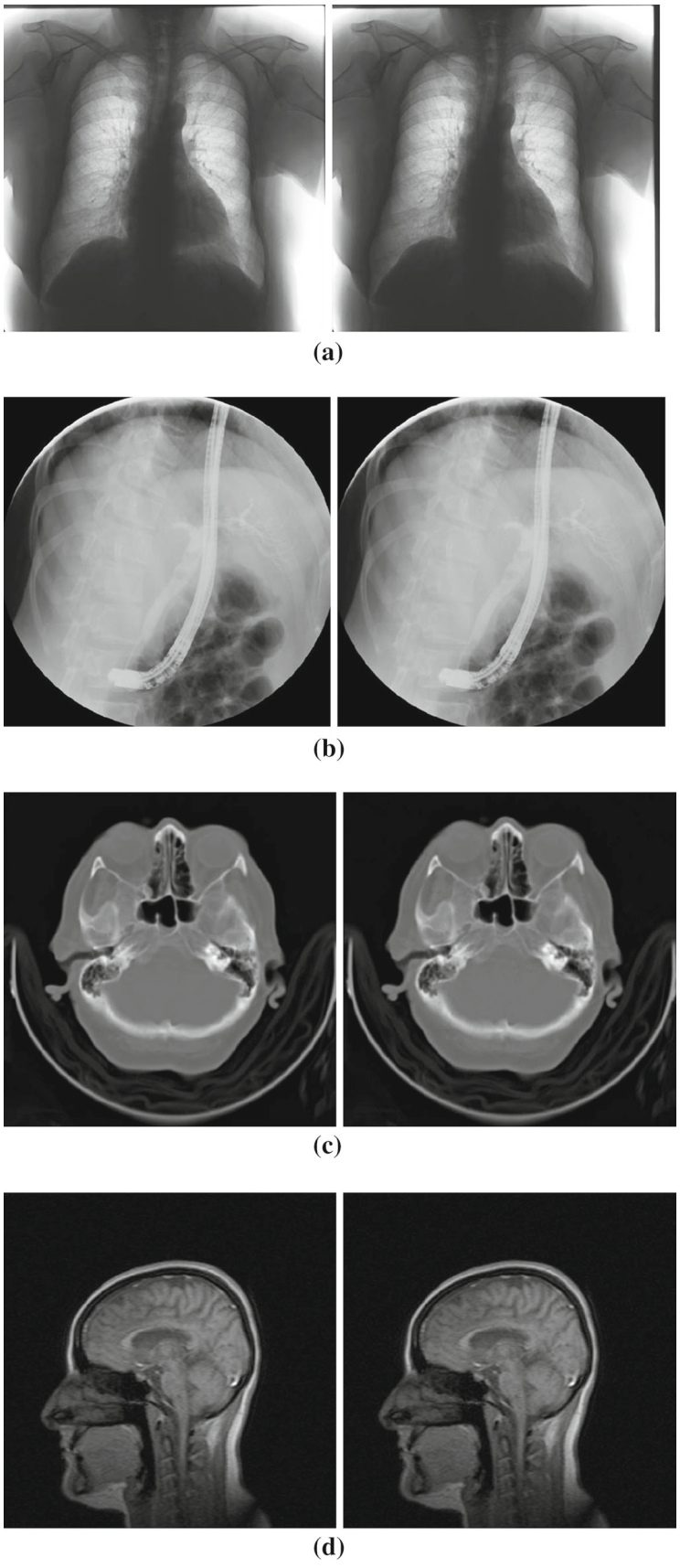


Fig. 5 Original test DICOM images (*left*) together with their watermarked versions (*right*). **a** Computed radiography (CR) PSNR = 53.12 dB, SSIM = 0.9978, VIF = 0.9663. **b** Radio fluoroscopy (RF) PSNR = 51.40 dB, SSIM = 0.9913, VIF = 0.9618. **c** Computed tomography (CT) PSNR = 53.26 dB, SSIM = 0.9976, VIF = 0.9513. **d** Magnetic resonance (MR) PSNR = 49.48 dB, SSIM = 0.9876, VIF = 0.9643

brain from a particular channel in the original and the watermarked medical images, respectively [26].

$$\mathrm{SSIM}(I, I') = \frac{(2\mu_I\mu_{I'} + C_1)(2\sigma_{I_I'} + C_2)}{(\mu_I^2 + \mu_{I'}^2 + C_1)(\sigma_I^2 + \sigma_{I'}^2 + C_2)}. \quad (15)$$

In (15), I and I' are the original and the watermarked medical images, respectively, and C_1 and C_2 are small constant values [27].

As it is known in the literature, the VIF value reflects perceptual distortions more precisely than the PSNR. The range of VIF values is [0, 1], and the closer value to 1 represents the better fidelity respect to the original image. Also, it is well known in the literature that the SSIM value reflects perceptual distortions more precisely than the PSNR. The range of SSIM values is [0, 1], and the closer value to 1 represents the better quality respect to the original image, a value of 1 corresponds to the case when the original and the reference image are the same. In Fig. 6, the average (a) PSNR, (b) SSIM and (c) VIF values are plotted with variable watermark strength α ranging from 20 to 100.

As shown in Fig. 6a–c, with a smaller value of α, the watermark imperceptibility is increased; however, its robustness may be sacrificed. Hence, there is a trade-off between robustness and imperceptibility. Although it may be considered that an acceptable PSNR value is above 45 dB with $\alpha = 100$, a value of the watermark strength α greater than 60 produces a small perceptible noise effect in the image. This effect is observed in the upper left region of a zoomed CR image shown in Fig. 7. Considering special attention that must be paid for medical images, the empirically determined values of α are set as follows: set $\alpha = 20$ for computed radiography (CR) images, $\alpha = 40$ for radio fluoroscopy (RF) images, $\alpha = 30$ for computed tomography (CT) images and $\alpha = 60$ for magnetic resonance (MR) images.

Table 1 shows in summary the average PSNR, SSIM and VIF values obtained in the test images according to the classification mentioned above and their respective watermark strength mentioned above, i.e., $\alpha = 20$ for CR, $\alpha = 40$ for RF, $\alpha = 30$ for CT and $\alpha = 60$ for MR imaging.

From Table 1, it follows that the proposed scheme provides a fairly good fidelity of the watermarked image, achieving the PSNR, SSIM and VIF values greater than 49 dB, 0.98 and 0.95, respectively. The imperceptibility performance is compared with that reported by algorithm [13], which is one of the most robust watermarking algorithms published applied to medical imaging with similar purposes as our proposed scheme. To get a proper comparison, we consider a homogeneous format of DICOM grayscale images of $512 \times 512 \times 8$ bits. The images used in both algorithms (ours and that proposed in [13]) are 100 images for each category CR, RF, CT and MR. The comparison results are shown in Table 2.

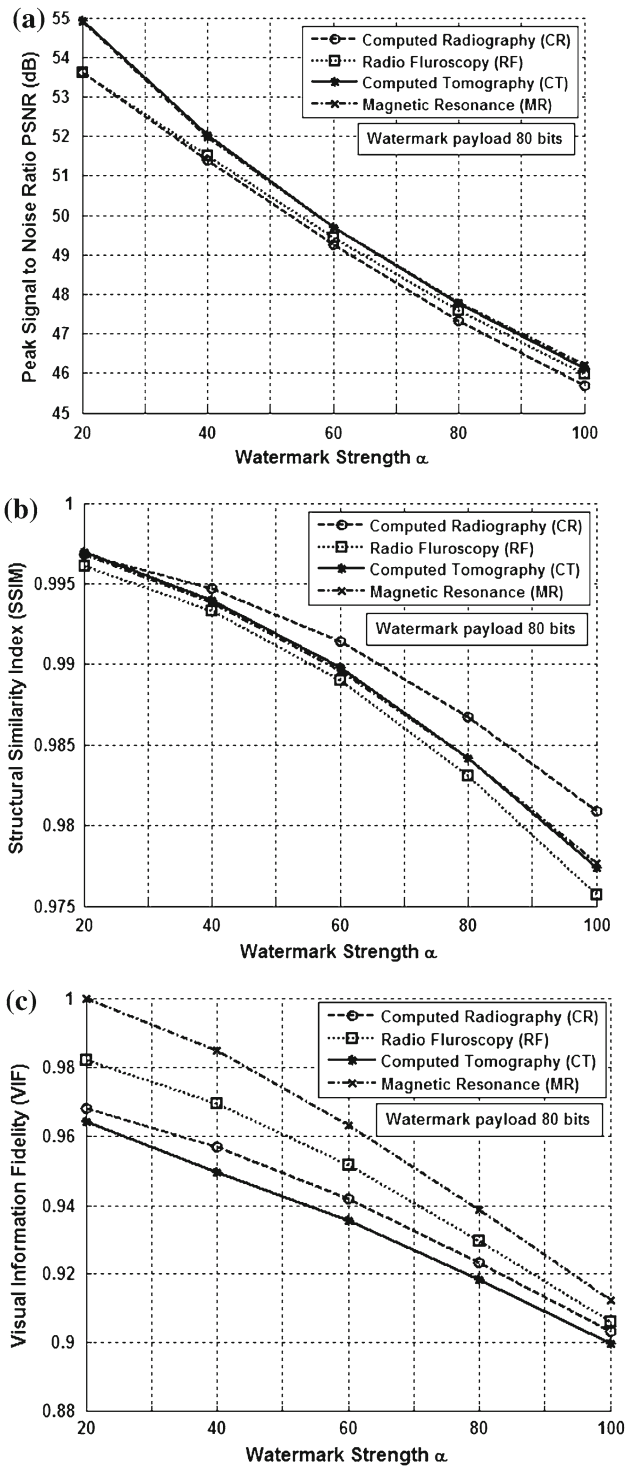


Fig. 6 Average **a** PSNR (dB), **b** SSIM and **c** VIF obtained with different watermark strength α from 20 to 100

From Table 2, it follows that the proposed scheme provides a fairly good fidelity of the watermarked image, achieving a PSNR greater than 50 dB, avoiding the perceptual distortions in the medical images that may affect the image content and as consequence it may lead to an erroneous clinical diagnostics.

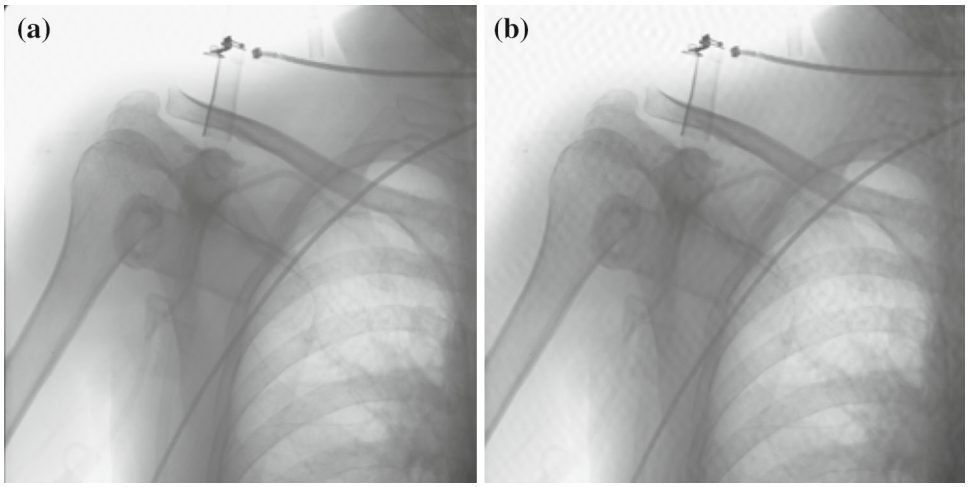


Fig. 7 Perceptible noise effect, **a** watermarked image with $\alpha = 20$ and PSNR = 54.29 dB. **b** Watermarked image with $\alpha = 100$ and PSNR = 46.54 dB

Table 1 Average watermark imperceptibility using PSNR (dB), SSIM and VIF metrics

DICOM image	PSNR (dB)	SSIM	VIF
Computed radiography	53.62	0.9968	0.9683
Radio fluoroscopy	51.52	0.9933	0.9698
Computed tomography	53.03	0.9940	0.9596
Magnetic resonance	49.68	0.9896	0.9631

Table 2 Average comparative results of imperceptibility using the PSNR (dB) metric

DICOM image	Proposed method	Method in [13]
Computed tomography	53.93	42.08
Radio fluoroscopy	52.62	39.15
Computed radiography	55.12	38.26
Magnetic resonance	50.33	43.91

3.2 Watermark payload

Considering fixed values of watermark strength as follows: $\alpha = 20$ for computed radiography (CR) images, $\alpha = 40$ for radio fluoroscopy (RF) images, $\alpha = 30$ for computed tomography (CT) images and $\alpha = 60$ for magnetic resonance (MR) images, in conjunction with a pair of radiuses $r_1 = 80$ and $r_2 = 81$ and a variable value of L ranging from 16 to 256 bits, in Fig. 8a–c we show that a large value of L would increase the payload of the watermarking method; however, the imperceptibility of the watermarking algorithm in terms of PSNR, SSIM and VIF metrics would decrease for large L, causing perceptual distortions that may affect the image quality and the medical diagnostics.

Hence, there is a trade-off between payload and imperceptibility. From Fig. 8a, we show that although it may be considered that an acceptable PSNR is above 44 dB with $L = 256$, a value of the watermark length L greater than 80 causes a small perceptible noise effect in the image. To illustrative purposes, this effect is observed in the center region of a zoomed CT and RF sample images shown in Figs. 9 and 10, respectively. From Fig. 9b, we show the perceptible noise effect in the gray regions of the CT image in comparison with Fig. 9a. In the same way occurs with RF sample image, from Fig. 10b, we show the perceptible noise effect in the plain regions of the RF image in comparison with Fig. 9a. In an analog manner, this effect is present in MR and CR images, respectively. According to this behavior, L =16–80 are considered a suitable set of values. In order to preserve the trade-off between payload–robustness–imperceptibility, and obtaining the maximum watermark payload, in the proposed watermarking method, we have adopted the value $L = 80$ in conjunction with the others embedding parameters.

3.3 Watermark robustness

To evaluate the watermark robustness of the proposed algorithm, several geometrical distortions, DICOM compression modes and common signal processing reported in the medical imaging fields are applied to the watermarked images. The robustness performance is compared with that reported by the algorithm [13]. Again, to get a proper comparison, we consider a homogeneous format of DICOM grayscale images of $512 \times 512 \times 8$ bits. The images used in both algorithms (ours and that proposed in [13]) are 100 images for each category CR, RF, CT and MR. Table 3 shows the average BCR obtained after applying the above-mentioned distortions to the watermarked DICOM images in both algorithms. In Table 3, *italic letters* indicate failure detection against the distortion.

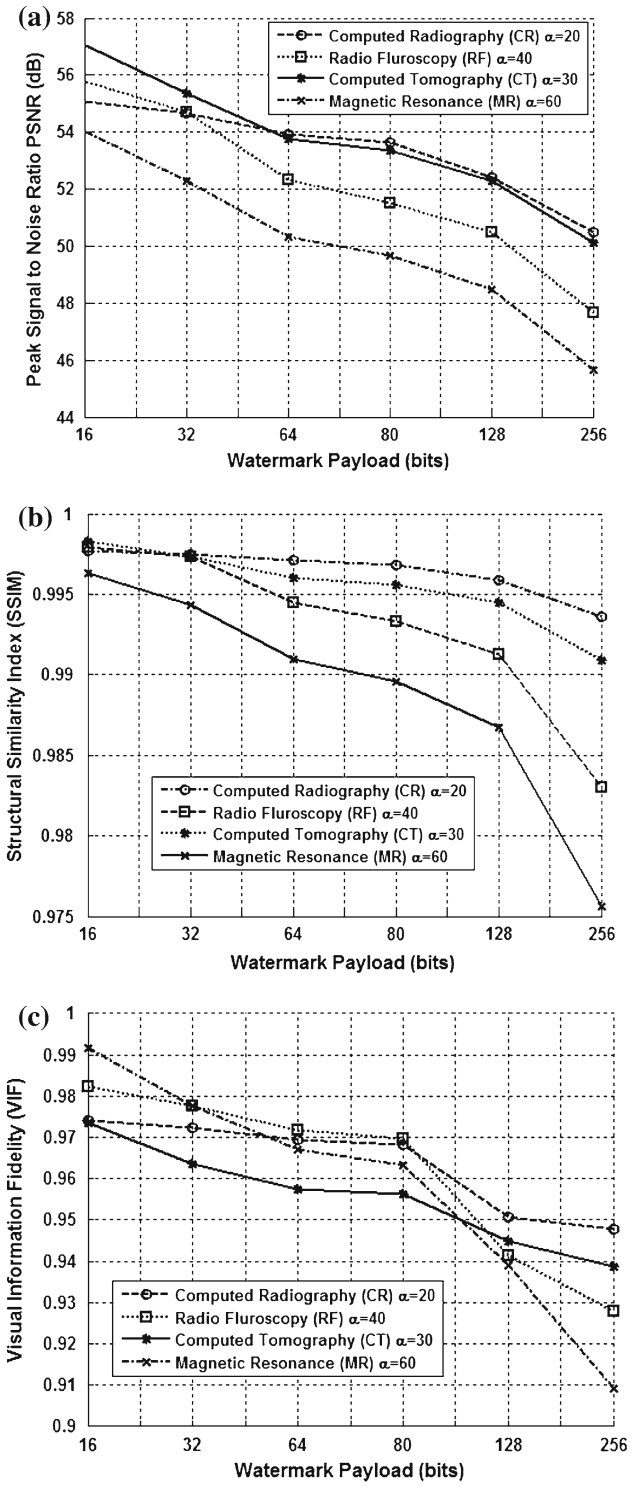


Fig. 8 Average **a** PSNR (dB), **b** SSIM and **c** VIF obtained with variable watermark length L from 16 to 256

3.3.1 Geometric distortions

From Table 3, we can observe that the embedded watermark signal in our proposed method is sufficiently robust to all rotation angles, translation with cropping attack and aggressive scaling with a scaling factor of 0.4 and 1.5, obtaining BCR values greater than or equal to 0.91, 0.96 and 0.98, respectively. In all cases, in the proposed method, we have obtained the BCR values greater than the predefined threshold value $T_{\mathrm{BCR}} = 0.75$, calculated as mentioned in Sect. 2.3 and used to determine whether the watermark W is present or not into the watermarked medical image. Meanwhile, from Table 3, we can observe that the embedded watermark signal in [13] presents weak robustness against rotation greater than 35°, translation with cropping attack and aggressive scaling with a scaling factor of 0.4 and 1.5. Although some attacks may be considered unusual in the medical imaging context, e.g., pixel translation with cropping attack, the proposed algorithm is designed to be robust against a wide range of intentional or non-intentional distortions.

3.3.2 DICOM compression modes and JPEG 2000

From Table 3, we can observe that the embedded watermark signal in our proposed method is sufficiently robust against DICOM standard image compression schemes, i.e., JPEG Lossless, run-length encoding (RLE) and JPEG lossy compression with quality factor QF = 50, which is a standard quality factor in DICOM standard, as well as to JPEG 2000 lossy and lossless compression, obtaining the BCR values equals to 1 for all compression schemes except in JPEG lossy compression mode, which values are greater than or equals to 0.96. From Table 3, we can also observe that the embedded watermark signal in [13] is robust against DICOM JPEG Lossless, RLE and JPEG 2000, obtaining BCR values equals to 1. However, this method presents weak robustness against JPEG lossy compression with QF = 50.

3.3.3 Signal processing

From Table 3, we can observe that the embedded watermark signal in our proposed method is sufficiently robust against common signal processing such as Gaussian noise contamination with $\mu = 0$, variance $\sigma^2 = 0.001$ and signal-to-noise ratio SNR = 41.82, 30.85, 19.33 and 13.49 dB, for CR, RF, CT and MR, respectively, impulsive noise with density=0.001, median and sharpness filtering with 3×3 window size, as well as contrast and brightness changes. In all cases, we have obtained the BCR values greater than the predefined threshold value $T_{\mathrm{BCR}} = 0.75$. From Table 3, we can also observe that the embedded watermark signal in [13] presents weak robustness against Gaussian noise and median filtering.

In Fig. 11, watermarked images after some attacks given in Table 3 are shown.

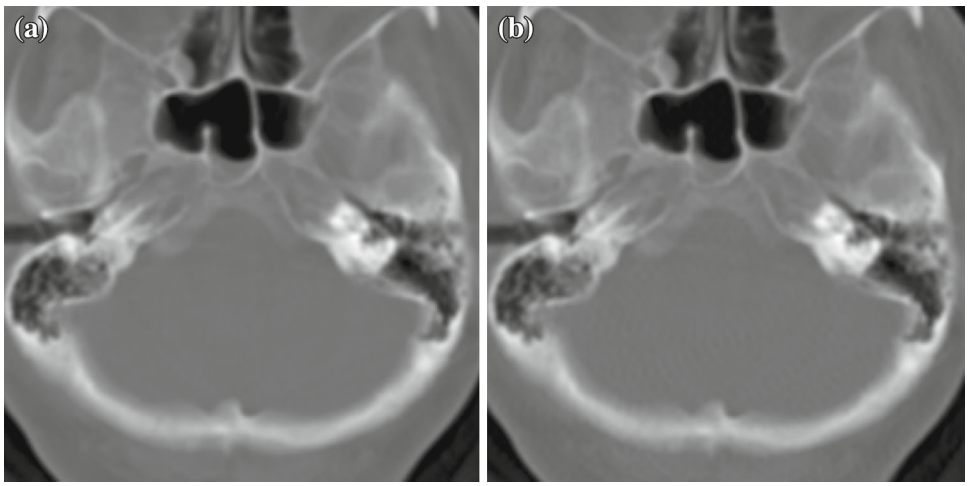


Fig. 9 Perceptible noise effect in gray regions of the CT images, **a** watermarked CT image with $\alpha = 30$ and $L = 80$, PSNR = 53.36 dB. **b** Watermarked CT image with $\alpha = 30$ and $L = 256$, PSNR = 50.14 dB

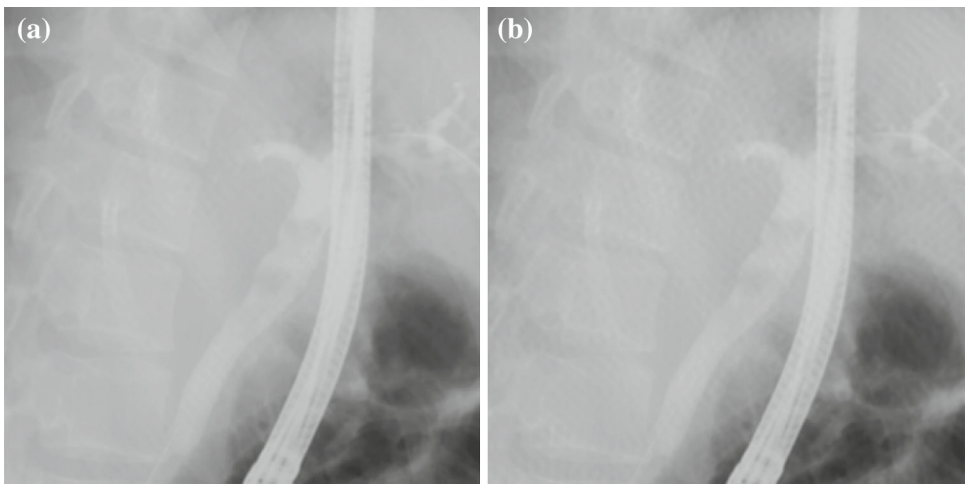


Fig. 10 Perceptible noise effect in plain regions of the RF images, **a** watermarked RF image with $\alpha = 40$ and $L = 80$, PSNR = 51.50 dB. **b** Watermarked RF image with $\alpha = 40$ and $L = 256$, PSNR = 47.65 dB

3.4 Detector performance

Considering the false alarm probability as the probability of detect erroneously a detachment when actually the watermarked image and their corresponding metadata are right corresponded, and the false rejection probability as the probability that the detector cannot detect a detachment when the watermarked image and the metadata do not correspond, the ROC curves are obtained and plotted under each attack. To perform a fair comparison between our algorithm and the proposed in [13], Gaussian noise with $\mu = 0$ and variance $\sigma^2 = 0.001$, 3×3 median filtering and JPEG lossy compression with QF = 50 are considered in both cases. These comparisons are shown in Figs. 12, 13 and 14, respectively.

From Fig. 12, we show that the method in [13] has a detection probability equals to 0.5584; meanwhile, our proposed method has a detection probability equals to 0.8422, when $P_{\text{fa}} = 4.29 \times 10^{-6}$. From Fig. 13, it follows that the method in [13] provides a detection probability of 0.0001; meanwhile, our proposed method has a detection probability equals to 1, when $P_{\text{fa}} = 4.29 \times 10^{-6}$. Finally, from Fig. 14, it follows that the method in [13] has a detection probability equal to 0.4568; meanwhile, our proposed method has a detection probability equal to 0.9996, when $P_{\text{fa}} = 4.29 \times 10^{-6}$. According to these results, our proposed algorithm presents a good detection performance avoiding the detachment from the corresponding EPR data and generally outperforms to the method presented in [13].

Finally, a comparison performance in terms of imperceptibility and robustness with the previously reported methods in [10–12] and [14] is show in Table 4. Table 4 presents also the tolerance under distortions and designates the capacity to resist as either 'detected' or 'fail,' when the tolerance is not given in detail by the other four methods above mentioned. A grid cell is marked with a dash for attack simulations not mentioned in the literature. In this way, a comparison with

Table 3 Average BCR obtained from CR, RF, CT and MR test watermarked images after geometric and signal processing distortions

Distortion	Proposed method				Method in [13]			
	CR	RF	CT	MR	CR	RF	CT	MR
Without distortion	1	1	1	1	1	1	1	1
DICOM JPEG lossless	1	1	1	1	1	1	1	1
DICOM RLE	1	1	1	1	1	1	1	1
DICOM JPEG lossy QF = 50	1	0.98	0.96	0.98	*0.61*	*0.64*	*0.60*	*0.62*
JPEG 2000 lossy	1	1	1	1	1	1	1	1
JPEG 2000 lossless	1	1	1	1	1	1	1	1
Sharpening 3 × 3	1	1	0.96	1	0.92	0.89	0.90	0.88
Gaussian noise (0,0.001)	1	0.95	0.87	0.92	*0.74*	*0.71*	*0.66*	*0.70*
Median filter 3 × 3	1	1	0.96	1	*0.49*	*0.50*	*0.51*	*0.49*
Bright reduction	1	0.98	0.92	0.92	0.92	0.87	0.86	0.86
Contrast enhanced	0.98	1	0.98	0.96	0.91	0.90	0.88	0.89
Impulsive noise density = 0.001	0.98	1	0.92	0.96	0.92	0.89	0.91	0.87
Gaussian filter 3 × 3	1	1	0.96	1	0.90	0.85	0.89	0.83
Histogram equalization	0.98	0.95	0.96	0.92	0.89	0.83	0.86	0.89
Translation $x = 25$, $y = 25$ with cropping	1	0.89	1	0.98	*0.52*	*0.50*	*0.48*	*0.50*
Rotation 35°	0.92	0.91	1	0.96	0.82	0.83	0.87	0.85
Rotation 75° with auto-crop	0.91	0.92	0.96	0.95	*0.61*	*0.69*	*0.60*	*0.65*
Scaling 1.5	1	1	1	1	*0.62*	*0.60*	*0.62*	*0.49*
Scaling 0.4	1	1	1	0.96	*0.73*	*0.70*	*0.74*	*0.69*

[10] reveals that our proposed method is more imperceptible in terms of PSNR metric, getting values greater than or equals to 49 dB; meanwhile, in [10], the PSNR values are less than 35 dB. The method in [10] is less robust that our proposed method because uses a subjective criterion to measure the robustness of the algorithm, which is essentially based only on a maximum acceptable modification amount in the watermarked medical image. Thus, the conventional metrics to measure the robustness in digital watermarking algorithms such as Normalized Correlation (NC), BER or BCR are discarded for the authors. This subjective criterion makes that the algorithm in [10] take into account only a few set of signal processing operations, neglecting the geometric distortions such as scaling and rotation, which not affect the quality of the medical images but may be used by the medical staff (in a non-intentional manner to remove the watermark) in order to observe with more detail certain regions of the medical images. Thereby, the method in [10] presents weak robustness against geometric distortions, because the extraction stage is desynchronized and the EPR data are not be recovered correctly. Thus, our proposed method outperforms the method proposed in [10] against geometric distortions, avoiding perfectly detachment problem when the medical image is rotated or scaled. Moreover, a comparison with [11] reveals that our proposed watermarked method is more imperceptible in terms of PSNR metric, obtaining values greater than or equals to 49 dB; meanwhile, in [11], the PSNR values are less than 34 dB. The method presented in [11] uses a non-blind detection; in consequence, the original medical image is needed for extracting in a correct manner the watermark and this fact limits their application in real life environments. Meanwhile, our proposed algorithm employs a blind detection, which makes it suitable for real life applications. Additionally, a comparison with the algorithm in [12] reveals that our proposed method is slightly more imperceptible in terms of PSNR metric, obtaining values greater than or equals to 49 dB; meanwhile, in [12], the PSNR values obtained from the whole image are less than 47 dB. Although the method in [12] presents robustness against filtering, impulsive noise contamination and scaling is outperformed by our proposed method in robustness terms against image compression including DICOM JPEG lossy with QF = 50 and JPEG 2000 lossy–lossless, which are common signal processing operations used to save storage space in databases or hard disks. Finally, the method proposed in [14] has less imperceptibility obtaining PSNR values less than 40 dB; meanwhile, our proposed method obtains values greater than or equals to 49 dB. The watermarking algorithm presented in [14] is less secured and needs a reference image for blind extraction and detection of the watermark. Meantime, in our proposed method, we only need the secret keys K_1 and K_2 during the watermark detection process. The scheme in [14]

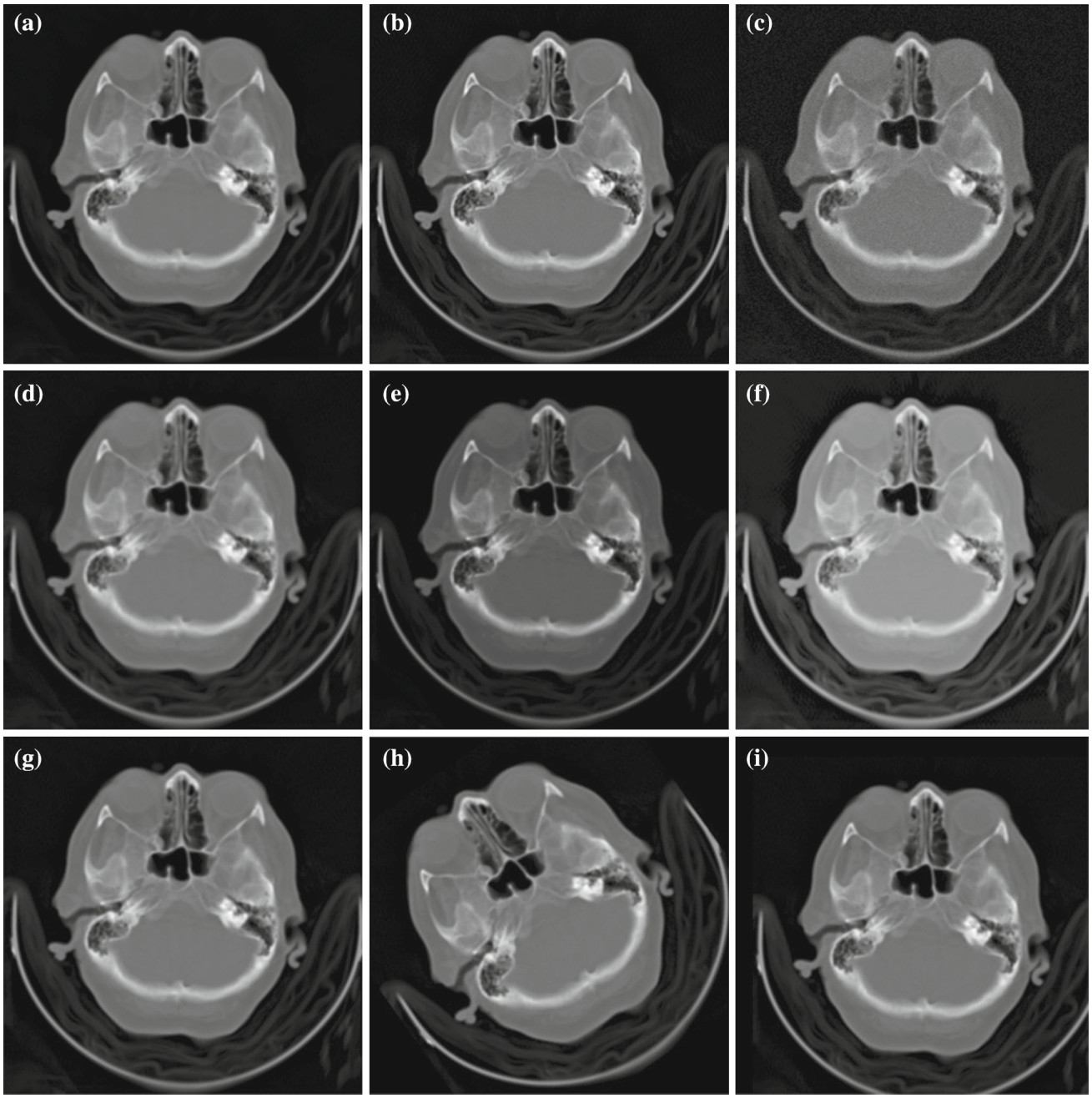


Fig. 11 Different attacks in the watermarked image. **a** DICOM JPEG lossy. **b** Sharpening 3×3. **c** Gaussian noise $\mu = 0$, $\sigma^2 = 0.001$. **d** Median filter 3×3. **e** Bright reduction. **f** Contrast enhanced. **g** Gaussian filter by 3×3. **h** Rotation by 35°. **i** Translation $x = 25$, $y = 25$ with cropping

is robust against several signal processing distortions, including one geometric distortion composed by rotation. However, its tolerance against JPEG compression is up to QF = 60 and rotation up to 5°, meantime, our proposed method is robust against several DICOM JPEG compression modes including JPEG lossy with QF = 50 as well as JPEG 2000 lossy and lossless. Moreover, our proposed scheme is designed to support all rotation angles and other aggressive geometric distortions.

4 Conclusions and future work

Because medical images and their related EPR are stored separately; the probability of corruption of this information or their detachment from the corresponding EPR is very high. Losing a data from the corresponding medical image may lead to a wrong diagnostic. Using a digital watermarking technique, the digest of this separate data can be embedded into the corresponding medical image as a watermark

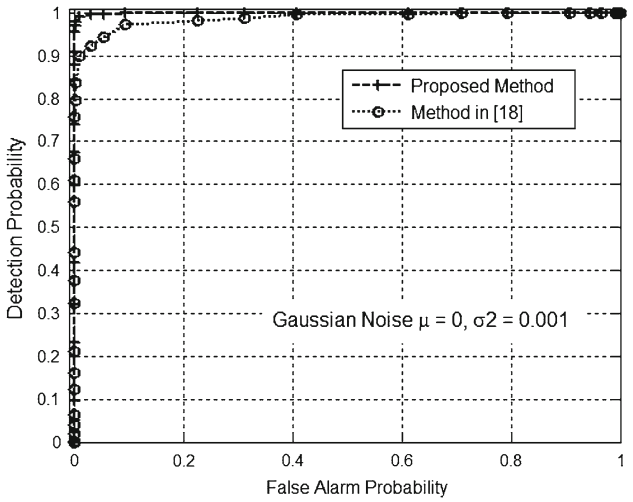


Fig. 12 ROC curves for Gaussian noise attack with $\mu = 0$ and variance $\sigma^2 = 0.001$

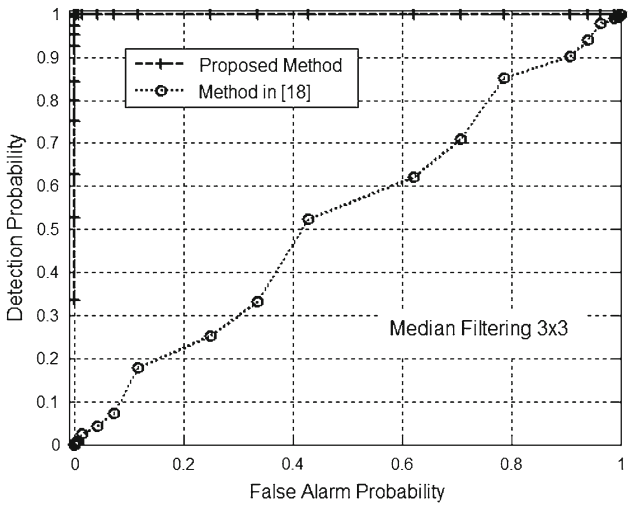


Fig. 13 ROC curves for median filtering attack with window size 3×3

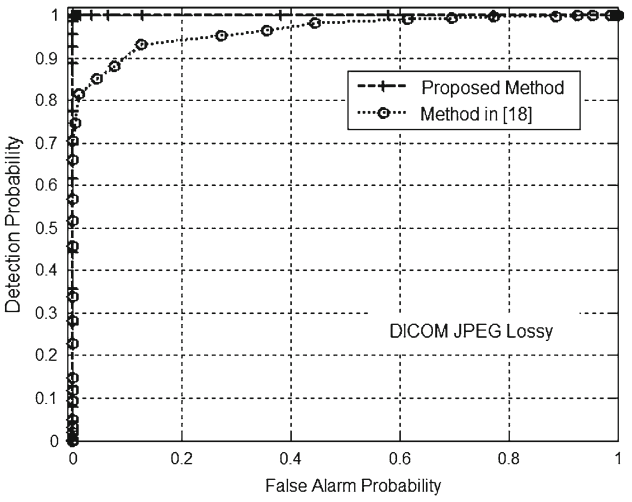


Fig. 14 ROC curves for DICOM JPEG lossy compression mode

sequence, reducing the risk of detachment. In this paper, we have presented a robust DFT-based watermarking method applied to several types of DICOM medical images to avoid detachment of the EPR information from the medical image under analysis. The computational results using CR, RF, CT and MR images have a good performance from robustness and imperceptibility points of view. Evaluation results show that the proposed algorithm is robust against geometric distortions and common signal processing operations, including DICOM standard image compression modes. The proposed method avoids a wrong diagnostic caused by image degradation, preserving the imperceptibility requirement for medical images, achieving a PSNR, SSIM and VIF values greater than 49 dB, 0.98 and 0.95, respectively. Also simulation results show that the proposed algorithm avoids perfectly detachment problem. Given its relative compact design, the proposed watermarking algorithm can be applied to the medical images at the same time of acquisition. In summary, from the comparison results, we can conclude that the proposed algorithm outperforms the algorithms proposed in [10–14] in

Table 4 Performance comparison

Comparison	Das et al. [10] (contourlet transform)	Manasrah et al. [11] (discrete wavelet transform)	Rahimi et al. [12] (contourlet transform)	Mostafa et al. [14] (discrete wavelet packet transform)	Proposed method (discrete Fourier transform)
JPEG lossy (quality factor)	Detected	Detected	–	60–100	20–100
Scaling	–	–	0.5–0.75	–	0.4–2
Rotation	–	–	–	−5°, 5°	0°–360°
Imperceptibility (dB)	PSNR $\leq$ 35	PSNR $\leq$ 34	PSNR $\leq$ 47	PSNR $\leq$ 40	PSNR $\geq$ 49
Detection metric	Subjective criterion	Correlation	BER, NC	BER, NC	BCR
Original image	Not need, blind detection	Needed, non-blind detection	Not need, blind detection	Reference image for blind detection	Not need, blind detection

terms of imperceptibility and robustness, which are one of the most efficient algorithms recently proposed in the literature with the same purpose. As a future scope of the proposed method is considered to improve the embedding strategy without affect the imperceptibility and robustness obtained hitherto, replacing the one-way by two-way hash function, in order to be able to restore the original EPR data. Until now, our proposed method is capable of avoiding perfectly the detachment problem even when the watermarked medical image is distorted by signal processing and aggressive geometric distortions; however, as a drawback, the method proposed does not restore the EPR data to their text original format.

Acknowledgments We thank the Post-Doctoral Scholarships Program and PAPIIT IN-112513 project from DGAPA in the National Autonomous University of Mexico (UNAM) and the National Polytechnic Institute (IPN) of Mexico by the support provided during the realization of this research. The authors also thank the Mexican Institute Social Security (IMSS) for providing us the medical images used to carry out this research work.

References

1. Coatrieux, G., Maître, H., Sankur, B., Rolland, Y., Collorec, R.: Relevance of watermarking in medical imaging. In: IEEE-embs Information Technology Applications in, Biomedicine, pp. 250–255 (2000)
2. Coatrieux, G., Quantin, C., Montagner, J., Fassa, M., Allaert, F.A., Roux, Ch.: Watermarking medical images with anonymous patient identification to verify authenticity. J. Stud. Health Technol. Inform. **136**, 667–672 (2008)
3. Navas, K.A., Sasikumar, M.: Survey of medical image watermarking algorithms. In: Proceedings of the Internation Conference Sciences of Electronics, Technologies of Information and Telecommunications, pp. 25–29 (2007)
4. Zain, J.M., Fauzi. A.R., Aziz. A.: Clinical evaluation of watermarked medical images. In: Proceedings of the 28th IEEE EMBS Annual International Conference, pp. 5459–5462 (2006)
5. Guo, X., Zhuang, T.G.: A region-based lossless watermarking scheme for enhancing security of medical data. J. Digit. Imaging **22**(1), 53–64 (2009)
6. Nergui, M., Acharya, U.S., Acharya, U.R., Yu, W.: Reliable and robust transmission and storage techniques for medical images with patient information. J. Med. Syst. **34**(6), 1129–1139 (2010)
7. Wu, J.H., Chang, R.F., Chen, C.J., Wang, C.L., Kuo, T.H., Moon, W.K., Chen, D.-R.: Tamper detection and recovery for medical images using near-lossless information hiding technique. J. Digit. Imaging **21**(1), 59–76 (2008)
8. Osamah, M., Al-Qershi, O., Khoo, B.E.: Authentication and data hiding using a reversible ROI-based watermarking scheme for DICOM images. Int. J. Inf. Commun. Eng. **5**(2), 801–806 (2009)
9. Zain, J.M., Fauzi, A.R.M.: Medical image watermarking with tamper detection and recovery. In: Proceedings of the 28th IEEE EMBS Annual International Conference, pp. 3270–3273 (2006)
10. Das, S., Kundu, M.K.: Effective management of medical information through a novel blind watermarking technique. J. Med. Syst. **36**, 3339–3351 (2012)
11. Manasrah, T., Al-Haj, A.: Management of medical images using wavelets-based multi-watermarking algorithm. In: International Conference on Innovations in Information Technology (IIT 2008), pp. 697–701 (2008). doi:10.1109/INNOVATIONS.2008.4781697
12. Rahimi, F., Rabbani, H.: A dual adaptive watermarking scheme in contourlet domain for DICOM images. Biomed. Eng. Online **10**(53), 1–18 (2011)
13. Rodriguez, R., Feregrino, C., Martinez, J.: Robust watermarking scheme applied to radiological medical images. IEICE Trans. Inf. Syst. **91**(3), 862–864 (2008)
14. Mostafa, S.A.K., El-sheimy, N., Tolba, A.S., Abdelkader, F.M., Elhindy, H.M.: Wavelet packets-based blind watermarking for medical image management. Open Biomed. Eng. J. **4**, 93–98 (2010)
15. Barni, M., Bartolini, F.: Data hiding for fighting piracy. IEEE Signal Process. Mag. **21**(2), 28–39 (2004)
16. Lacy, J., Quackenbush, S., Reibman, A., Snyder, J.: Intellectual property protection systems and digital watermarking. Opt. Express **3**, 478–484 (1998)
17. Langelaar, G.C., Setyawan, I., Lagendijk, R.L.: Watermarking digital image and video data. IEEE Signal Process. Mag. **17**, 20–46 (2000)
18. Barni, M., Bartolini, F.: Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications. Marcel Dekker, New York (2004)
19. Mintzer, F., Braudaway, G.W., Yeung, M.M.: Effective and ineffective digital watermarks. In: IEEE International Conference on Image Processing, pp. 9–12 (1997)
20. Schneier, B.: Applied Cryptography, 2nd edn. Wiley, New York (1996)
21. Dobbertin, H., Bosselaers, A., Preneel, B.: RIPEMD-160, a strengthened version of RIPEMD. In: Gollmann, D. (ed.) Fast Software Encryption, LNCS, vol. 1039, pp. 71–82. Springer, Berlin (1996). doi:10.1007/3-540-60865-6_44
22. Bosselaers, A., Dobbertin, H., Preneel, B.: The RIPEMD-160 cryptographic hash function. Dr. Dobb's J. **22**(1), 24–28 (January 1997)
23. Bovik, A.C.: Handbook of Image and Video Processing. Academic Press, New York (2005)
24. Okman, O., Akar, G.: Quantization index modulation-based image watermarking using digital holography. J. Opt. Soc. Am. A **24**, 243–252 (2007)
25. Tang, C.W., Hang, H.M.: A feature-based robust digital image watermarking scheme. IEEE Trans. Signal Process. **51**(4), 950–959 (2003)
26. Sheikh, H.R., Bovik, A.C.: Image information and visual quality. IEEE Trans. Image Process. **15**(2), 430–444 (2006)
27. Wang, Z., Bovik, A.C., Sheikh, H.R., Simoncelli, E.P.: Image quality assessment: from error visibility to structural similarity. IEEE Trans. Image Process. **13**(4), 600–612 (2004)