The Visual Computer
https://doi.org/10.1007/s00371-021-02267-3

ORIGINAL ARTICLE

Secured telemedicine of medical imaging based on dual robust watermarking

David Mata-Mendoza[1] · Manuel Cedillo-Hernandez[1] · Francisco Garcia-Ugalde[2] · Antonio Cedillo-Hernandez[3] · Mariko Nakano-Miyatake[1] · Hector Perez-Meana[1]

Accepted: 19 July 2021

Abstract

Medical information management has progressed in the last few years because of the advances in information technologies. Nowadays, it is possible to share medical images among specialists geographically distant to interpret, discuss, and get improved diagnostics. However, any alteration of transmitted image metadata may lead to issues related to information security, such as detachment and authentication. Detachment refers to link the data of an electronic patient record to an incorrect medical image, while authentication aims to identify the image source. These security problems are critical as they may cause the loss of sensitive data or wrong medical diagnoses. Digital watermarking is an emerging technique that faces these security problems as it allows to embed the metadata directly into the medical image. This paper proposes a hybrid and robust watermarking technique to prevent detachment and authenticate medical images. The quantization index modulation algorithm under dither modulation in conjunction with forwarding error correction is used to embed relevant metadata as a robust-imperceptible watermarking to avoid detachment. The visible-imperceptible watermarking paradigm, whose use is an innovation in medical images, is applied to insert a second watermark in the spatial domain to perform authentication. The experimental results show the contribution of the proposed scheme and its efficiency regarding robustness and imperceptibility.

Keywords Digital watermarking · Information security · DICOM imaging · Authentication · Detachment avoidance

1 Introduction

Currently, most modern medical equipment produces digital images according to the specifications of the Digital Imaging and Communications in Medicine (DICOM) standard [1]. In the beginning, the DICOM standard was used to define services for general management tasks of medical images as well as its corresponding electronic patient record (EPR). A DICOM formatted image consists of a pixel data file with a small header having metadata that links the image to the appropriate EPR. In general terms, the EPR is a log that registers all the activities of a patient such as clinical studies, diagnosis, and prescriptions, among other data [2–17]. Advances in information and communication technologies have permitted the development of more DICOM-based services for convenient access and digital transmission of medical images. Radiology information systems (RIS) and picture archiving and communication systems (PACS) are examples of technologies that fulfill with the DICOM standard and enable the creation of medical applications such as telemedicine, remote diagnostics, e-learning, and telesurgery.

Exchanging medical images and EPR information among health institutions open the possibility of better analysis, diagnosis, and treatment in benefit of a patient's care plan. Digital access to geographically distant medical information can also save patient's time and money. However, this scenario introduces new risks regarding information security that must be mitigated as medical data are highly reserved information. If it is necessary to transmit a medical image

✉ Manuel Cedillo-Hernandez
mcedillohdz@hotmail.com

[1] Instituto Politecnico Nacional SEPI ESIME Culhuacan, Av. Santa Ana 1000 Culhuacan CTM V, 04440 CDMX, Mexico

[2] Facultad de Ingeniería, Universidad Nacional Autonoma de Mexico, C.U., Circuito Exterior,, 04510 CDMX, Mexico

[3] Escuela de Ingeniería Y Ciencias, Tecnologico de Monterrey, Av. Eugenio Garza Sada 2501, 64849 Monterrey, NL, Mexico

Published online: 02 August 2021

to remote equipment, the pixel data and its header must be extracted from the DICOM format and sent separately. Any intentional or unintentional modification in transmitted header metadata may lead to significant information security issues such as detachment and authentication of image source. Detachment refers to unlink the relationship between an EPR and a medical image, while authentication aims to confirm the source of images. These security problems become critical as they may cause the loss of sensitive data or wrong medical diagnoses. During its lifetime, a medical image is transmitted numerous times inside a clinic, hospital, or even, outside, the headquarters. As the metadata are sent separately from medical images, the possibility of metadata corruption increases with each delivery. Thus, a big concern is to design mechanisms to ensure the integrity of header metadata, even in transmissions over insecure networks such as the Internet. The medical health care systems incorporate security mechanisms, such as firewalls, cryptography tools, anti-malware software, and access control, to provide security to their infrastructure [1, 18]. However, these mechanisms are specific-purpose and cannot solve all security issues of medical data, especially those performed to an implementation level.

Digital watermarking is an emerging technique that has been widely used by medical health care systems for improving security. In general terms, digital watermarking methods insert information (i.e., a watermark) to create a trustworthy link between the watermark and the hosting object. A digital watermarking technique is as efficient as the results of its evaluations regarding robustness and imperceptibility. Robustness is a measurement to evaluate if inserted data remain even after severe attacks are performed upon the watermarked image. Further, in case of medical images, it is imperative to preserve almost the same visual quality as the original image to prevent any alteration of medical diagnoses.

In medical image context, research in digital watermarking is usually applied in security problems such as authentication and detachment avoidance [2–17, 19–22], saving bandwidth, captioning, controlling access, indexing, and confidentiality [23–28]. According to human visual perception, digital image watermarking could be classified as *visible* [29], *robust-imperceptible* [30–33], and *visible-imperceptible* [34–37], each of which offers diverse characteristics to design applications with different requirements.

Visible watermarking methods aim to embed a visible pattern called “logo” over the image. Although the objective of these schemes is to insert the watermark unobtrusively, it may not be a suitable option for medical applications as any visual distortion can alter a medical diagnosis, no matter how small they may be.

The main capabilities of *visible watermarking* methods are:

a) Overlap a visible watermark pattern in the image content.
b) Identify ownership.
c) Deterrence against theft.
d) Prohibit unauthorized duplication.
e) Low transparency of image content.
f) Low quality of watermarked image.
g) Not need of explicit extractor/detector.
h) Low robustness.
i) Low computational complexity and
j) Versatility of media content.

The *robust-imperceptible watermarking* is the most explored modality in the scientific literature to find a solution to security issues in medical images [2–17, 19–22]. This modality involves two stages. The first one embeds a signal called “watermark” in an imperceptible manner, obtaining often high visual quality watermarked images. The second stage extracts and detects the watermark signal even though the protected images have experimented changes because of several image processing operations during its transmission or storage, either caused in an intentional or not intentional manner, such as image compression, noise corruption, filtering, or geometric distortions, among others. The aim of this modality is detecting or extracting the watermark signal without any ambiguity, even if the image is severely distorted, i.e., the digital image watermarking algorithm should be the most robust possible against attacks that attempt difficult its recovering tasks.

The main capabilities of *robust-imperceptible watermarking* are:

a) Embed an invisible watermark pattern in the image content.
b) Identify ownership.
c) High transparency of image content.
d) High quality of watermarked image.
e) Need of explicit extractor/detector.
f) High robustness.
g) Often higher computational complexity and
h) Versatility of media content.

Most recent and representative *robust-imperceptible watermarking* works applied to medical imaging reported in the scientific literature [4], are shown in Table 1.

On the other hand, a novel modality of watermarking schemes was recently proposed in the scientific literature with authentication and copyright protection purposes. This technique is known as *visible-imperceptible watermarking* and was first introduced by [34] in 2007. In general terms, *visible-imperceptible watermarking* involves concealing a visible watermark into a digital image, which is not readily perceptible to the naked eye but becomes evident via customized image enhancement operations [34–37]. In other

Table 1 Representative *robust-imperceptible watermarking* approaches applied to medical imaging

Work	Description	Application
[5]	Performed in Contourlet transform domain using Advanced Encryption Standard (AES) algorithm [39] and Bose, Chaudhuri and Hocquenghem (BCH) error correcting, to hide EPR and region of interest (ROI) data	Authentication Indexing
[6] [9]	Performed in discrete Fourier transform (DFT) domain using RIPEMD-160 algorithm [39], integrated optical density [6] and image masking [9], to hide EPR information	Avoid detachment EPR-Image
[7]	Based on discrete wavelet transform (DWT) domain supported by backpropagation neural network and a human visual system criterion to hide small logos	Authentication
[8]	Based on partial differential equation (PDE) criterion to automatically select the embedding region, to conceal logos as well as tamper detection tasks, in DFT-DWT domains	Authentication Integrity
[10]	Watermarking performed in discrete cosine transform (DCT) and DWT frequency domains using singular value decomposition (SVD) to hide binary logos, EPR and patient's data	Authentication
[11]	Based on spatial domain of medical images embedding EPR data into Least Most Significant (LSB) bits of the Region of Non-Interest (RONI)	Authentication
[12]	Performed in spatial domain using criteria of image moment theory, polar mapping, homogeneity, and luminance, to hide EPR data compressed by Huffman method	Confidentiality and Security
[14]	Image medical watermarking based on DWT-SVD in ROI region using Hamming error correcting code (ECC) to embed small binary logos and clinical data	Authentication
[15]	Based on an improved version of DWT domain, SVD and particle swarm optimization (PSO) algorithm, to conceal small binary logos	Authentication
[16]	Watermarking based on DWT and Schur transforms, using Firefly optimized algorithm to embed binary logos in RONI of the medical image	Authentication
[17]	Performed in ROI and RONI regions into the DWT-DCT domains to hide EPR data and binary logos, enhancing the security via message digest MD5 [39] and Rivest–Shamir–Adleman (RSA) [39]	Authentication Confidentiality and Security
[19]	Based on DCT domain and Quantization Index Modulation under Dither Modulation (QIM-DM), using message digest SHA-1 [39], Direct-Sequence Code Division Multiple Access (DS-CDMA), seam carving technique, convolutional encoding and Floyd–Steinberg error diffusion halftoning	Avoid detachment EPR-Image Patient Authentication
[21]	Watermarking based on DWT to hide EPR data into computed tomography images, using a topological reorganization of the coefficients of the LL sub-bands and a zigzag scanning method	Authentication
[22]	Watermarking to embed multiple watermarks in medical images which is based on DWT frequency domain and SVD, in conjunction with error correcting codes and Encryption Then Compression (ETC) technique	Authentication Confidentiality and Security

words, *visible-imperceptible watermarking* inherits valuable properties of the *visible* as well as of the *robust-imperceptible watermarking*, respectively.

In this way, the main capabilities of *visible-imperceptible watermarking* are:

a) Overlap a visible watermark pattern in the image content, which is not readily perceptible to the naked eye.
b) Identify ownership.
c) Deterrence against theft.
d) Prohibit unauthorized duplication.
e) High transparency of image content.
f) High quality of watermarked image.
g) Low need of explicit extractor/detector.
h) High robustness.
i) Low computational complexity and
j) Versatility of media content.

This scheme resembles to real-world watermarks as the revealing stage can be analogous to seeing a bill against different light sources, as shown in Fig. 1.

In this way, motivated by the properties in terms of capacity, imperceptibility, and robustness of the *robust-imperceptible* and *visible-imperceptible* watermarking, respectively, and justified by the necessity to mitigate security issues related to avoid detachment between the EPR and medical images, as well as perform the authentication of the image source in a visual way, in this paper we propose a novel hybrid and robust watermarking algorithm that embeds two different watermarks into the medical image.

Our objective is double: The *robust-imperceptible watermarking* modality is used to insert the first watermark to prevent detachment by using the discrete cosine transform (DCT) domain and the quantization index modulation algorithm under dither modulation (QIM-DM) altogether with a forward error correction (FEC) given by a convolutional encoder. Then, in a second stage, the method embeds a second watermark in the spatial domain by employing the *visible-imperceptible watermarking* paradigm to insert data to identify the origin of the image, i.e., to achieve authentication. Till the date, *visible-imperceptible watermarking* has been used in red–green–blue (RGB) color images [20,

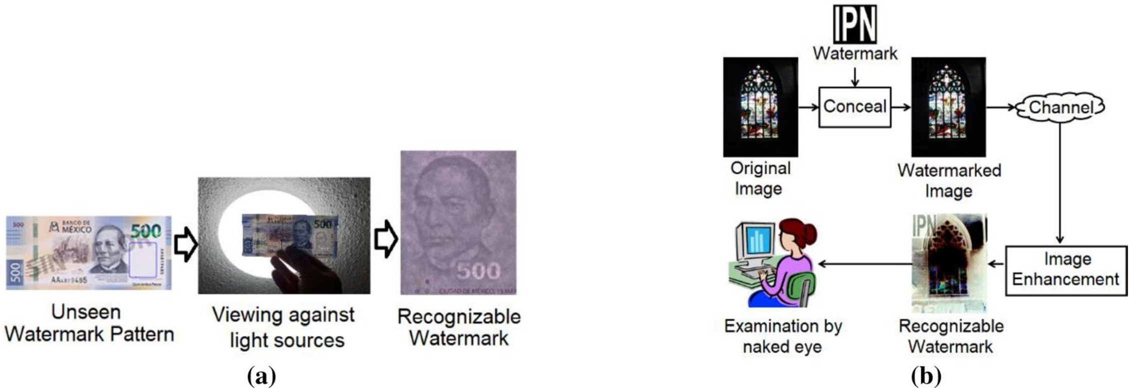


Fig. 1 **a** Real-world watermarking-based bills authentication. **b** *Visible-Imperceptible* watermarking inspired on (**a**)

34–37], 3D images, and video signals [38]. Nevertheless, to the best of our knowledge, this paradigm has not been yet applied to DICOM medical imaging to authentication by a naked eye, using DICOM images with bit depth greater than 8 bits/pixel, making our proposal pioneer in this research field. Watermark imperceptibility is measured by using several visual quality metrics. The experimental results and a comparison with some state-of-the-art proposals show the contribution of the proposed scheme and its efficiency regarding robustness and imperceptibility. Main contributions of the proposed image watermarking scheme are:

- Hybrid and efficient watermarking method for DICOM medical images.
- Authentication via practical exposure of *visible-imperceptible* digital watermarking.
- Avoid detachment between clinical data and medical images using *robust-imperceptible* watermarking.
- High visual quality on the watermarked DICOM images.
- Preserving all intrinsic DICOM data after watermarking method is applied to medical images.
- Versatility for protecting DICOM images with bit depth greater than 8 bit/pixel, which is a crucial aspect in practical scenarios.

The organization of this paper is as follows: Sect. 2 of this paper details the materials and methods employed in the research. The experimental results, including parameter settings, are presented in Sect. 3. Section 4 presents a brief discussion and a comparative analysis with state-of-the-art proposals. Finally, Sect. 5 concludes this work.

2 Material and methods

Figure 2 shows an overview of the architecture of the proposed hybrid watermarking scheme, which is composed of the *robust-imperceptible* and the *visible-imperceptible* watermarking methods.

As shown in Fig. 2, a couple of watermarks: A character string and binary logo are used for detachment and authentication issues, respectively. The *robust-imperceptible* method involves embedding and extraction/detection stages, while the *visible-imperceptible* modality is composed of concealment and exposure procedures. All stages are explained in detail as follows.

2.1 Visible-imperceptible watermarking: concealment stage

For the identification of the image source and verification that the image belongs to the correct patient, the concealment of the logo watermark W_1 is described as follows.

1. Read the original DICOM image I with $N \times M$ pixels in size and select the central pixel $(\hat{x}, \hat{y})$ of the concealment region, denoted CR, that satisfies the condition given by (1), where $n_1 \times n_2$ are the dimensions of CR and of the watermark W_1. The variables (x,y) are spatial coordinates, and wn denotes a window for sliding all pixels of I to find $(\hat{x}, \hat{y})$, $\overline{wn}$ is the mean value of all pixels in wn.

$$(\hat{x}, \hat{y}) = \underset{(x,y)}{\arg\min} \left(\frac{1}{n_1 \cdot n_2} \cdot \sum_{i,j\in\Omega} \left(wn(xt, yt) - \overline{wn} \right)^2 \right), \text{where} \quad \Omega = \begin{cases} xt \in \left[x - \frac{n_1}{2}, x + \frac{n_1}{2} \right] \\ yt \in \left[y - \frac{n_2}{2}, y + \frac{n_2}{2} \right] \end{cases}, \quad x = 1, \ldots, N, \quad y = 1, \ldots, M \quad . \tag{1}$$

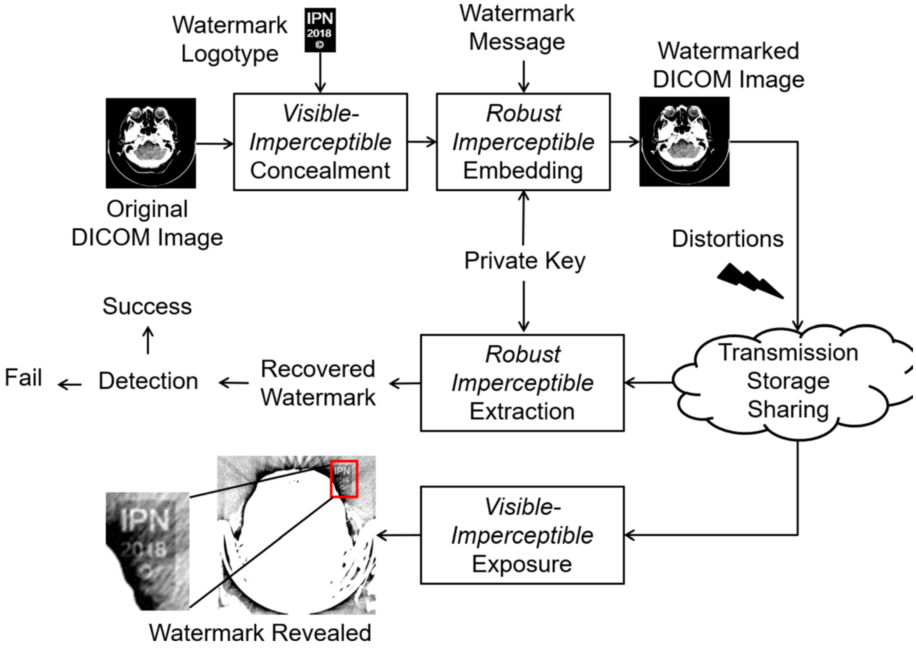


Fig. 2 Architecture of the proposed method

2. Once the concealment region CR is determined, using the information of W_1, of size $n_1 \times n_2$ and binary $\{0, 1\}$ values, the original pixel value, $\mathrm{CR}_o(x,y)$ is modified by (2):

$$\mathrm{CR}_\mathrm{w}(x,y)\begin{cases} \mathrm{CR}_\mathrm{o}(x,y)+\alpha & \text{if} \quad W_1(x,y)=0 \\ \mathrm{CR}_\mathrm{o}(x,y) & \text{if} \quad W_1(x,y)=1 \end{cases} \tag{2}$$

where (x, y) denotes the spatial coordinates, CR_w is the watermarked pixel, and α is a watermark strength factor. The watermarked image resulting in this procedure is denoted as I'.

2.2 Robust-imperceptible watermarking: embedding stage

As mentioned above, detachment refers to unlink the EPR to the corresponding medical image. Moreover, if medical images and related metadata are transmitted separately from each other, the possibility of detachment increases. Such metadata or an identification code must be integrated into the medical image to prevent detachment. In this way, a second watermark W_2 is embedded in the discrete cosine transform domain as follows.

1) Rescale I' to a standard size of $N_1 \times N_2$. The parameters N_1, N_2 will be provided as secret key k_1 in the extraction/detection stage to increase the security of the proposed method.
2) Extract the most critical information from the DICOM image header, e.g., patient, medical and institution data, or another desirable data.
3) Apply a one-way hash function with 160-bit output, such as Secure Hash Algorithm (SHA-1) [39] or RACE Integrity Primitives Evaluation Message Digest (RIPEMD-160) [40, 41] to the data selected in the previous step. Please note that the proposed method can be easily adapted to use another hashing algorithms, obtaining the binary representation, which composing the watermark W_2.
4) To increase the robustness requirements, encode W_2 using a convolutional code proposed in [42]. This operation is used at the extraction/detection stages to perform forward error correction to diminish the bit error rate (BER) in W_2.
5) Segment the rescaled image I' using a block segmentation in the same way of the Joint Photographic Experts Group (JPEG) standard (8×8), and supported by a secret key k_2, B blocks are selected randomly from the image I'. Using the encoded watermark, We and the four-alternating current (AC) coefficients with a low frequency of each B in 2D-DCT domain, embedding We into I', using the QIM-DM algorithm [43] given by (3). The amount of B blocks is determined by $B = \lceil We/4 \rceil$.

$$B_\mathrm{W} = Q\big(B + d(z, SWe_z), \Delta\big) - d(z, SWe_z), \quad z = 1, 2, 3, 4 \tag{3}$$

where B and B_W are the original and watermarked 2D-DCT blocks, respectively, SWe_z is a segmented bit sequence with four bits of the encoded watermark We. The quantification function $Q(X, \Delta)$ is given by (4):

$$Q(X, \Delta) = \left\lfloor \frac{X}{\Delta} \right\rfloor \times \Delta \tag{4}$$

where X implies a couple of dither signals $d(z,0)$ and $d(z,1)$ which are given by (5) and (6), respectively:

$$d(z,0) = -\Delta + (\Delta \cdot p), \tag{5}$$

$$d(z,1) = \begin{cases} d(z,0) + \frac{\Delta}{2}, & \text{if } d(z,0) < 0 \\ d(z,0) - \frac{\Delta}{2}, & \text{otherwise} \end{cases}, \tag{6}$$

where Δ is a step-size of quantification, p is a pseudorandom signal with uniform distribution, the length of p is four. Once encoded watermark We is embedded into the 2D-DCT coefficients of each B block, these are returned to the spatial domain by applying the inverse 2D-IDCT. The resulting image is the watermarked image I'_{w}.

Equation (6), finally, rescales the watermarked image I'_{w} to its original dimensions $N \times M$ and converts it to the DICOM native format.

2.3 Visible-imperceptible watermarking: exposure stage

Given a watermarked image I'_{w}, the revealing process of the watermark W_1 is a non-complex method composed only by one step that helps to prove its authenticity. This process is as follows:

1) Read the watermarked DICOM image I'_{w} and create a grayscale version from its indexed representation by using L gray levels of quantization. The value of L should be adjusted until the watermark logotype W_1 is revealed and perceived by the naked eye. In a practical way, this procedure can be performed using a DICOM viewer application, e.g., the RadiAnt DICOM Viewer© software.

2.4 Robust-imperceptible watermarking: extraction/detection stage

On the other hand, to extract and detect the watermark data bits of W_2, the procedure is:

1. Rescale the watermarked image I'_{w} to the chosen size $N_1 \times N_2$ by using the key k_1, previously defined in the embedding process.
2. Using contents owner's secret key k_2, the B blocks of 8×8 pixels in size are recovered from I'_{w} and then the bits sequence composed by the encoded information is extracted from the B-selected blocks in DCT domain using the QIM-DM extraction algorithm [43]. In this context, from the four AC coefficients with lowest frequencies of each B block, four bits sequence is extracted using (7):

$$\overline{SWe_z} = \arg\min_{l \in \{0,1\}} (c_z - Ds(z,l))^2, \quad z = 1,2,3,4, \tag{7}$$

where $\overline{SWe_z}$ is the zth extracted watermark bit, c_z is the zth watermarked DCT coefficient and $Ds(z, l)$ is a dither signal given by (8) and (9):

$$Ds(z,0) = Q(c_z + d(z,0), \Delta) - d(z,0), \tag{8}$$

$$Ds(z,1) = Q(c_z + d(z,1), \Delta) - d(z,1). \tag{9}$$

where $d(z, l)$, $l = 0$, 1, are given by (5) and (6), and the quantification function $Q(X, \Delta)$ is given by (4). The step-size Δ must be the same value used in robust-imperceptible watermarking embedding stage. Repeat this step for each B block in DCT domain and recover the encoded watermark We'.

3. The retrieved watermark pattern W_2' is then the decoded version of We' employing the error control Viterbi algorithm with hard decision [44].
4. Compute the bit error rate the BER between the original W_2 and the recovered W_2' watermarks, by using the BER metric.
5. Assuming ergodicity [6], the BER is defined as the ratio between the number of incorrectly decoded bits and the total number of embedded bits. Then, a decision threshold value T_{d} must be defined to determine the existence of the watermark W_2 into the watermarked medical image I_{w}. A critical issue concerning to the watermark detection is get a proper value of false alarm probability P_{fa}, which refers to how often a watermarking algorithm detects a watermark in a not watermarked image. Thus, considering a binomial distribution with success probability = 0.5, a false alarm probability P_{fa} is given by (10), and a threshold value T must be adjusted to get a small value of $P_{\mathrm{fa}} = 4.2110 \times 10^{-15}$.

$$P_{\mathrm{fa}} = \sum_{\lambda=T}^{U} \left(\frac{1}{2}\right)^{U} \cdot \left(\frac{U!}{\lambda!(U-\lambda)!}\right), \tag{10}$$

Considering λ as an independent random variable with binomial distribution [45], U as the length of the watermark $W_2 = 160$-bit, and the threshold value $T = 128$-bit, then $T_{\mathrm{d}} = 1 - (T/U) = 0.20$, according to the fact that BER + BCR = 1, where BCR is the bit correct rate. If the BER value between the original W_2 and the recovered W_2' is greater than 20%, the detection process rejects the image either by: (a) DICOM image does not correspond to the EPR metadata or (b) DICOM image is not watermarked. Otherwise, the existence of the watermark W_2 is detected.

3 Results

This section presents the evaluation results of the proposed hybrid efficient watermarking method applied to DICOM images.

3.1 Experimental setup

We consider a set of 100 medical images in DICOM format modality computed tomography (CT) and different types: simple skull, larynx, brain, and abdomen, all of 512×512 in size and 8, 12, and 16 bit/pixel of grayscale resolution, the dataset is provided with copyrights by the Mexican Social Security Institute (Instituto Mexicano del Seguro Social, IMSS). The total payload for watermark W_1 is $62\times89=5518$ data bits. The entire payload for watermark W_2 is related to the size of encoded watermark *We*, which is 552 data bits. The value of the owner's keys k_1 (N_1, N_2), $k_{2,}$ and k_3 is experimentally set and could be renewed periodically to improve the security. The watermark strength factor used in the *visible-imperceptible* watermarking algorithm is $\alpha=8$. The step-size Δ used by the QIM-DM [43] in the *robust-imperceptible* watermarking algorithm is $\Delta=40$. The value of quantization of gray levels is $L=32$ in the exposure stage. However, L value could vary according to the end-user employing a DICOM viewer application, e.g., the RadiAnt DICOM Viewer© software [46]. The parameters for the detection of W_2 are false alarm probability $P_{\mathrm{fa}}=4.21\times10^{-15}$ and decision threshold $T_{\mathrm{d}}=0.20$. The efficiency of the proposed scheme is evaluated in terms of imperceptibility and robustness of the watermarks.

3.2 Parameter settings

A digital watermarking technique is as efficient as the results of its evaluations regarding robustness and imperceptibility. Robustness is a measurement to evaluate if inserted data remain even after severe attacks are performed upon the watermarked image. In the case of medical images, it is imperative to preserve almost the same visual quality as the original image to prevent any alteration of medical diagnoses. In this way, this section shows the configuration of the main parameters used by the proposed robust hybrid watermarking method applied to medical imaging, which are: (a) the watermark strength factor, α, used in the *visible-imperceptible* watermarking algorithm as well as (b) the step-size of quantification, Δ, used by the QIM-DM in the *robust-imperceptible* watermarking algorithm, respectively. Thus, the trade-off between imperceptibility and robustness of the watermark should be evaluated to get the proper values of α and Δ, respectively.

3.2.1 Watermark strength factor α

Considering a medical image in DICOM format on modality CT corresponding to simple skull, a variable watermark strength factor α from 1 to 10, step-size of quantification $\Delta=40$, image corruption by Gaussian noise with mean $\mu=0$, and variance $\sigma^2=0.015$, to determine the proper value of α, the peak signal-to-noise ratio (PSNR) metric was used in this experiment to measure the watermark imperceptibility, and it is given by (11):

$$\mathrm{PSNR(dB)} = 10\log_{10}\left(\frac{\text{Max Pixel Value}^2}{\frac{1}{N\cdot M}\left(\sum_{x=1}^{N}\sum_{y=1}^{M}\left(I(x,y)-I_w(x,y)\right)^2\right)}\right), \tag{11}$$

where $N\times M$ are the original dimensions and I and I_{w} are the original and watermarked images, respectively. Figure 3 shows the PSNR when α is varying from 1 to 10, and Fig. 4 shows the watermark readability with Gaussian noise over the image. Figures 3 and 4 show that a high value of α increases the readability of the watermark W_1, but inversely the imperceptibility requirement decreases for large values of α. Hence, there is a trade-off between the readability and imperceptibility. Figure 3 also shows that for $\alpha=8$ the obtained PSNR is 99.98 dB, which indicates an excellent performance in terms of imperceptibility and at the same time allowing proper watermark readability when typical signal processing attacks are considered, e.g., Gaussian noise, distorts the image.

3.2.2 Step-size of quantification Δ

Considering a DICOM medical image on modality CT and a watermark strength factor $\alpha=8$, Fig. 5a shows the PSNR

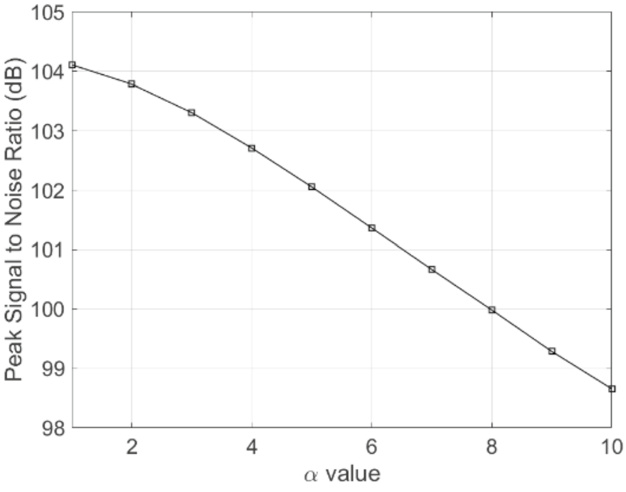


Fig. 3 PSNR obtained with α variable

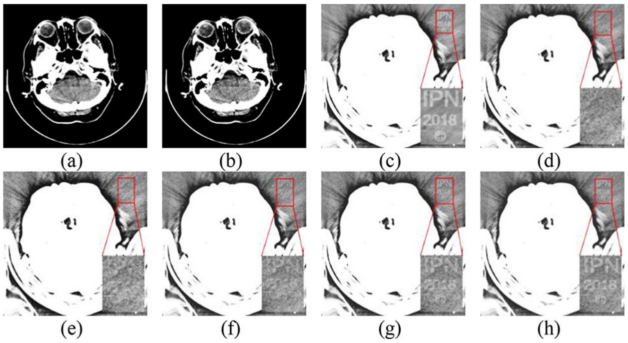


Fig. 4 **a** Watermarked image without distortion. **b** Watermarked image corrupted by Gaussian noise. **c** Watermark exposure without distortion. Watermark readability using image (**b**): **d** $\alpha=1$, **e** $\alpha=3$, **f** $\alpha=5$, **g** $\alpha=7$, and **h** $\alpha=9$

varying the Δ value from 10 to 100 with a not attacked image. Figure 5b shows the watermark robustness in terms of BER when the image is attacked by adding impulsive noise, and the parameter Δ is varying from 10 to 100.

Figure 5a, b shows that a large value of Δ could increase the robustness of the watermark W_2 against signal processing distortions, but the imperceptibility requirement decreases for large values of Δ. Hence, there is also a trade-off between the robustness and imperceptibility. Figure 5a also shows that for $\Delta=40$, the obtained PSNR is 99.59 dB, which indicates outstanding performance in terms of imperceptibility and at the same time allowing proper watermark robustness when the image is distorted by common signal processing attacks, e.g., impulsive noise, obtaining a BER smaller than the decision threshold $T_d=0.20$.

3.3 Watermark imperceptibility

As explained in the previous paragraphs, the proposed medical image watermarking method conceals a watermark logo W_1 in the spatial domain of the image using *visible-imperceptible* watermarking; the second ciphered-encoded watermark W_2 is embedded in the discrete cosine transform domain using QIM-DM modulation in this domain. Therefore, a careful watermark imperceptibility evaluation is compulsory. Using the predefined values $\alpha=8$ and $\Delta=40$, in a first experiment, by using medical images with 8bit/pixel of grayscale resolution, a fair comparison in terms of PSNR is performed considering previous works in [5–7, 9, 10, 12–17, 20, 22]. Table 2 shows the average of the PSNR reported in each proposal and the obtained in our proposed method.

From Table 2, we show that the proposed method outperforms to all previous proposals and only was outperformed by 1.32 dB in [16]. However, the method in [16] is designed to work only on medical images with 8 bit/pixel of grayscale resolution, which can be considered a limiting in scenarios where the image resolutions are higher than 8 bit/pixel. Additionally, an experiment is performed considering medical images with 16 bit/pixel of grayscale resolution, a fair comparison in terms of PSNR is performed regarding previous works in [8, 11, 19, 21], respectively. Table 3 shows the average PSNR reported in [8, 11, 19, 21] as well as the obtained by our proposed method. From Table 3 we

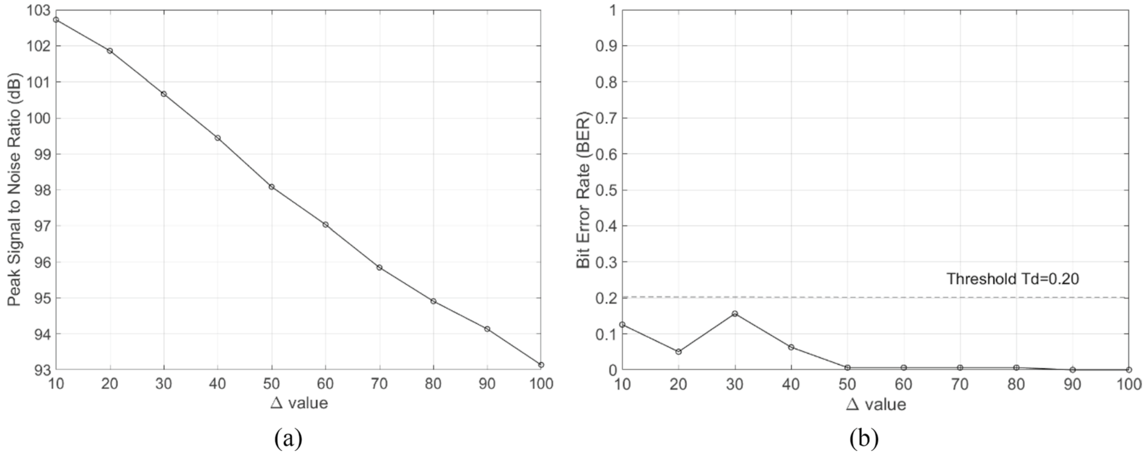


Fig. 5 **a** PSNR with Δ variable. **b** BER after applying impulsive noise with density 0.01 and Δ variable

Table 2 Comparison results in terms of average PSNR in dB considering 8 bit/pixel of grayscale resolution

Method	[5]	[6]	[7]	[9]	[10]	[12]	[13]	[14]	[15]	[16]	[17]	[20]	[22]	This Work
PSNR (dB)	34.36	53.93	34.21	49.10	35.84	40.16	38.66	46.00	45.22	56.23	36.88	41.29	44.19	54.91

Table 3 Comparison results in terms of average PSNR in (dB) considering 16 bit/pixel of grayscale resolution

Method	[8]	[11]	[19]	[21]	Proposed
PSNR (dB)	77.43	46.11	102.00	70.00	99.56

show that the PSNR obtained by our proposed method outperforms to algorithms reported in [8, 11, 21] in terms of watermark imperceptibility, obtaining average PSNR values of 99.56 dB. Although the proposal in [19] outperforms to our proposal by 2.44 dB, the imperceptibility provided by our proposed method is competitive considering that the watermark payload in [19] is only 552 bits; meanwhile, our proposal allows embedding a larger amount of 6070 watermark data bits.

Finally, to visualize the influence of watermarks W_1 and W_2 on the visual quality of the medical images when they are embedded separately and jointly, from a set of 100 medical images in DICOM format with different content (simple skull, larynx, brain, and abdomen) we calculate image quality in terms of the PSNR, structural similarity index (SSIM), Visual Information Fidelity (VIF), mean squared error (MSE), universal quality index (UQI), visual signal-to-noise ratio (VSNR), weighted signal-to-noise ratio (WSNR), and Multi-Scale SSIM Index (MSSIM), [47–49], respectively. Table 4 summarizes the average results of the above metrics. To illustrative purposes, Fig. 6 shows a couple of test images and their watermarked version.

From Table 4 we show that the watermark W_1 (*visible-imperceptible*) is slightly less invasive in the image content compared with the watermark W_2 (*robust-imperceptible*), when are tested in the DICOM images in a separately manner. As expected, metric's values in Table 4 decreased when both watermarks W_1 and W_2 are embedded jointly into the medical images. However, according to the results in Table 4 and Fig. 6, the proposed dual robust watermarking algorithm does not affect the visual quality of DICOM images.

3.4 Watermark robustness

To evaluate the watermark robustness of the proposed method, we use several signal processing and geometrical attacks. We categorize the experimental results according to the watermark modality and its objective, i.e., (a) *Visible-imperceptible* watermarking uses W_1 to authenticate the image source and (b) *Robust-imperceptible* watermarking uses W_2 to avoid detachment between medical image and their corresponding metadata EPR.

3.4.1 Visible-imperceptible watermarking robustness

As mentioned in the above paragraphs, *visible-imperceptible watermarking* involves conceals a visible watermark into a digital image, which is not easily perceptible to the naked eye. The watermark becomes visible in the image via customized image enhancement operations [34–37], which are analogous to the stage of seeing against light sources in a real-world watermarking scenario, e.g., watermark logos into bills [35].

Figure 7 shows the robustness results of W_1 in terms of watermark readability using the image enhancement tool provided by RadiAnt DICOM Viewer© software [46] to expose and authenticate practically the pattern W_1.

Table 4 Analysis of the influence of the watermarks W_1 and W_2 on the visual quality of the medical images when they are embedded separately and jointly

Average	PSNR	SSIM	VIF	MSE	UQI	VSNR	WSNR	MSSIM
Only W_1	103.15	0.9974	0.9960	0.2812	0.9931	47.0287	57.5118	0.9995
Only W_2	102.06	0.9984	0.9892	0.9927	0.9877	49.0082	46.1667	0.9983
W_1 and W_2	99.56	0.9958	0.9856	1.2756	0.9818	49.4592	45.8503	0.9979

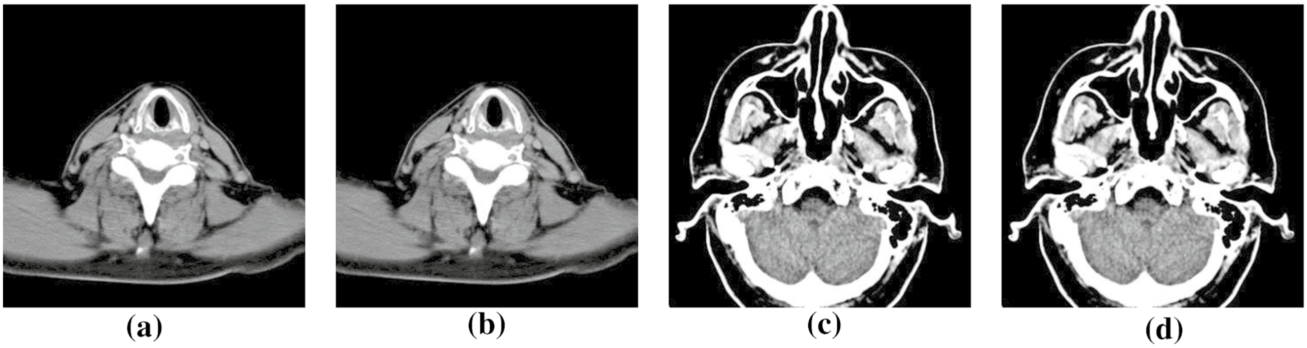


Fig. 6 Original versions (**a**) and (**c**). Correspondingly watermarked medical images (**b**) and (**d**)

According to the results in Fig. 7, we concluded that the proposed method has a good robustness against several aggressive geometric distortions including centered cropping by 100×100 pixels, cropping of 45%, rotation by 45° and 135°, flipping left–right and up–down, aspect ratio change, general affine transformation scaling with scale factor from $fs=0.5$ to 2, translation with crop $x=50$ pixels, $y=50$ pixels, and translation without crop $x=100$ pixels, $y=100$ pixels, and signal processing distortions including image enhancement, filtering, noise corruption, and image compression such as DICOM JPEG/JPEG2000 lossless and lossy compression, respectively, negative, impulsive noise with density = 0.01, Gaussian noise with mean $\mu=0$ and variance $\sigma^2=0.015$, Gamma correction with $\gamma=1.05$ and $\gamma=0.95$, Gaussian filter 7×7, median filter 5×5, average filter 5×5, sharpen, speckle noise with mean $\mu=0$, and variance $\sigma^2=0.05$ as well as histogram equalization. From Fig. 7 we show that in all cases the watermark W_1 was correctly revealed and is easily perceptible to the naked eye by adjusting the L gray levels of quantization using RadiAnt DICOM Viewer© software [46].

3.4.2 Robust-imperceptible watermarking robustness

As mentioned above, we adopted the *robust-imperceptible* watermarking to avoid the detachment issues, embedding the signal W_2 into the discrete cosine transform domain of the image, in such a way that observers are unable of distinguishing the difference between the original and watermarked images by the naked eye. A mandatory requirement of this watermarking modality is that the hidden watermark signal must be robust, i.e., must remain in the image after performing intentional or non-intentional distortions. In this way, invisible watermarking methods can protect the images without affecting their visual quality. Table 5 shows the summary of signal processing and geometric distortions as well as its tolerances applied to watermark W_2.

The detection results are shown in Fig. 8a, b, in terms of average bit error rate (BER) and normalized correlation (NC), respectively. Remembering that, if the BER value is nearer to 0, and the NC value is nearer to 1, indicates that the extracted watermark is more related to the original watermark W_2. From Fig. 8a, b we conclude that W_2 has good robustness against several geometric distortions and signal processing distortions. Robustness against rotation attack is acquired via exhaustive search by several angles' rotation; meanwhile, the secret key k_1 (pair of values N_1 and N_2) is used to resynchronize the detection stage against the rest of geometric attacks. In all cases the watermark W_2 was correctly detected, obtaining average BER values less than the decision threshold $T_{\mathrm{d}}=0.20$ considering a false alarm probability $P_{\mathrm{fa}}=4.2110\times10^{-15}$, and NC values near to 1. The experimental results show that QIM-DM *robust-imperceptible* watermarking in conjunction with the convolutional encoding increases the robustness of the watermark W_2 against several intentional and not intentional attacks.

3.5 Computational complexity (speed)

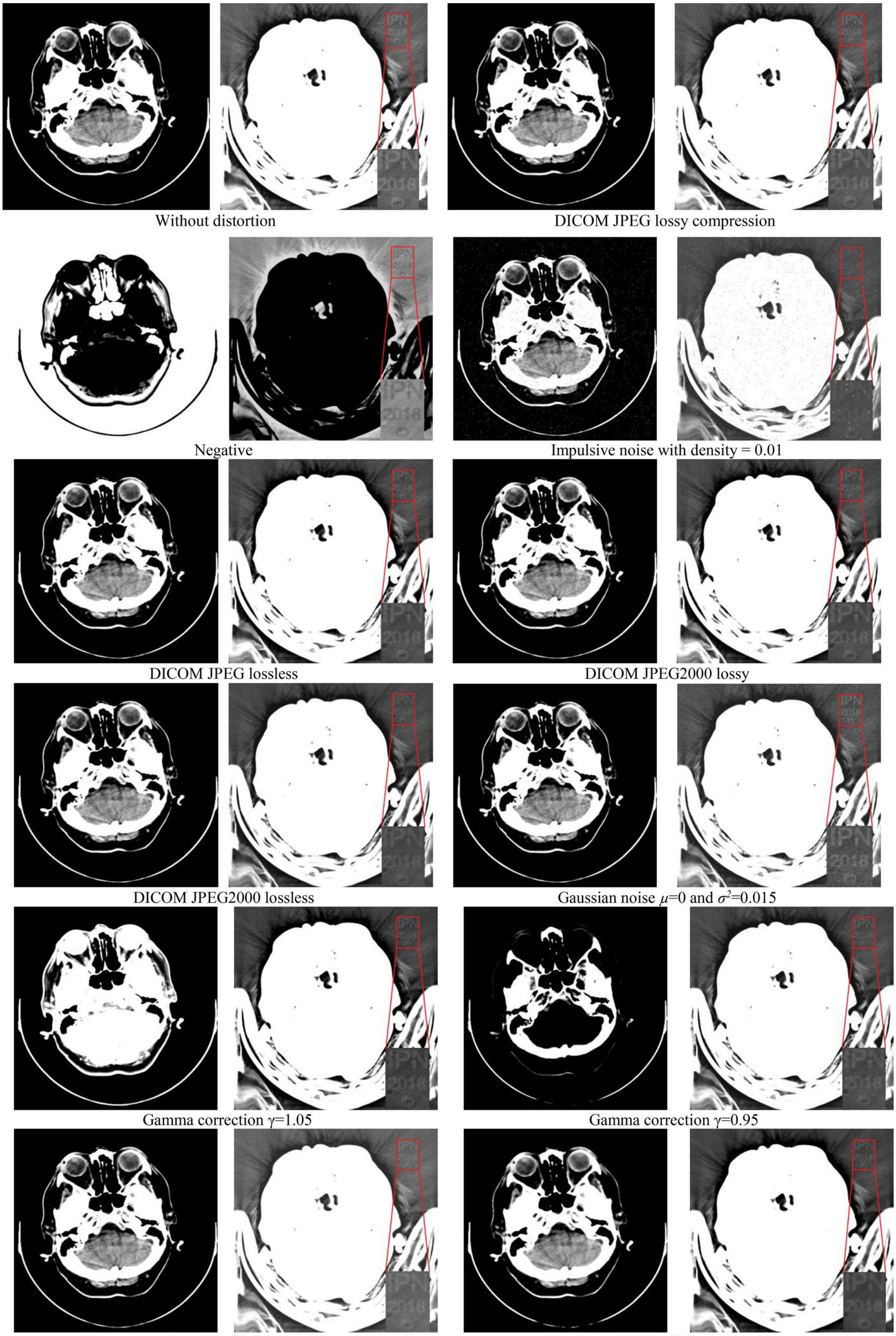
To a reference of the processing time, we employ a personal computer running Windows10© with an Intel© Core i7 processor (1.99 GHz) and 16 GB random access memory (RAM) in which all procedures were implemented using MATLAB© R2017b. Table 6 summarizes the processing time of the main procedures of the proposed method.

From Table 6 we show that the concealment process of W_1 is the process that consumes most computation time, executed in about 4.9 s. This behavior is mainly caused by the sliding of the window in Eq. (1) on all pixels of image I to find the proper region to conceal W_1. This computation time will be increased according to the spatial resolution of the image is increased. On the other hand, the process that consumes less computation time is the exposure process of W_1 which is done in about 0.02 s. An advantage of *visible-imperceptible* regarding to *robust-imperceptible* watermarking is that the computation time of the exposure process is not increased, even though the watermarked image is distorted by any aggressive geometric attack such as rotation or scaling. Finally, the embedding process of W_2 is done in about 0.28 s, while the extraction/detection process of W_2 is executed in about 0.23 s. A disadvantage of robust-imperceptible regarding to visible-imperceptible watermarking is that the computation time of the extraction/detection procedure is increased if the watermarked image is distorted by the rotation attack, because this distortion implies an exhaustive search from 0° to 360° degrees.

4 Discussion

Finally, Table 7 shows a comparison performance by considering the previously reported methods in [5–12, 14–17, 19–22] and our proposal. A grid cell appears with a dash '–', when the authors did not report a criterion or simulation. To the comparative, we consider only relevant criteria, as they are the most essential in the design of a robust digital watermarking algorithm applied to medical images [2–4].

In the sake of brevity, we perform a punctual comparative from Table 7. Although several proposals show the relevant results in terms of imperceptibility, payload, and robustness, some of these such as [5–7, 9, 10, 12–17] design its watermarking algorithms for operating in medical images down-sampled to bit depth of 8 bit/pixel, fact that limits its implementation in practical scenarios, because the conventional bit depths are 10, 12, and 16 bit/pixel according to the DICOM standard [1]. In contrast, the proposal reported in [20] considers in its design the luminance information of



Without distortion

DICOM JPEG lossy compression

Negative

Impulsive noise with density = 0.01

DICOM JPEG lossless

DICOM JPEG2000 lossy

DICOM JPEG2000 lossless

Gaussian noise μ=0 and σ^2=0.015

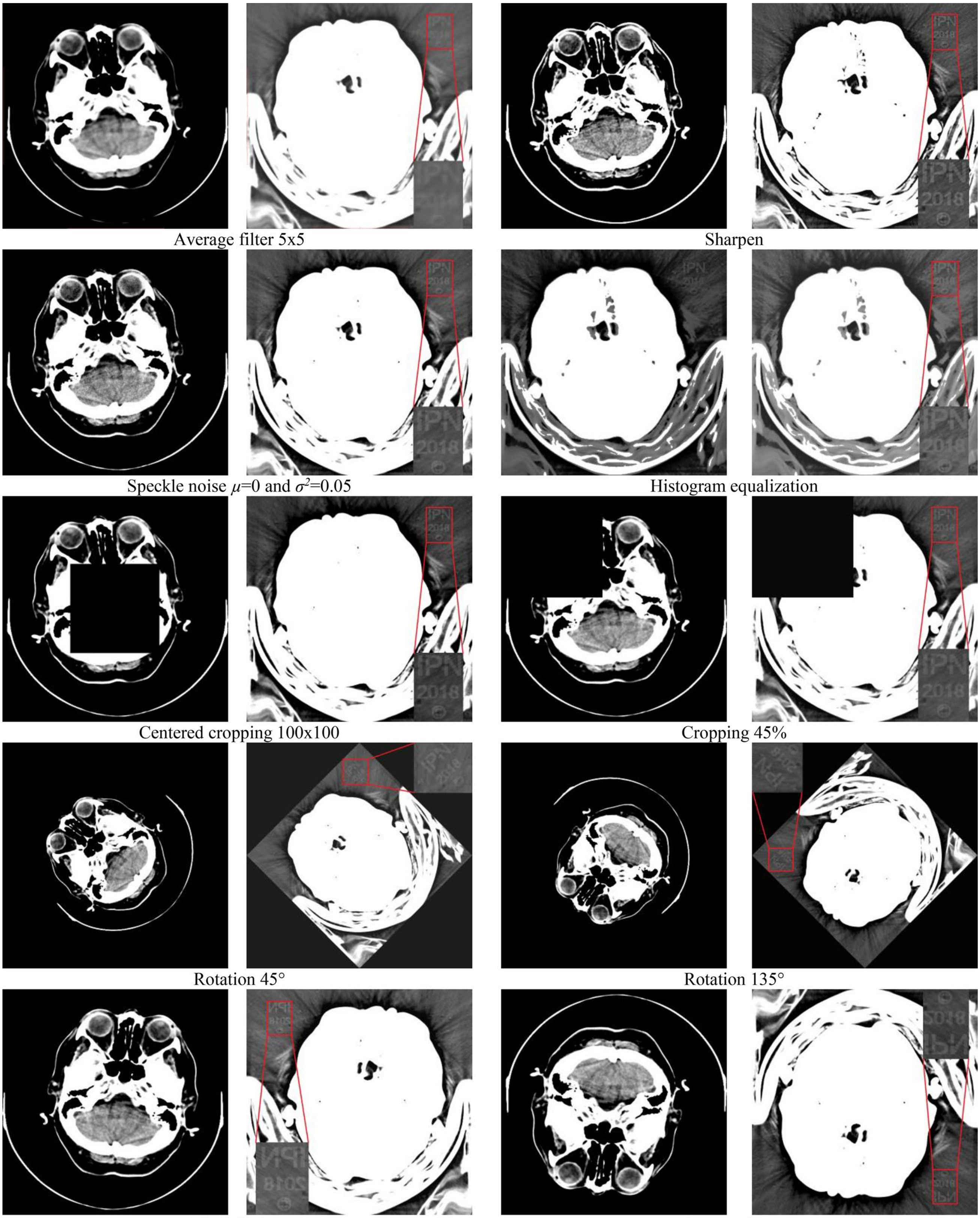
Gamma correction γ=1.05

Gamma correction γ=0.95

Gaussian filter 7x7

Median filter 5x5

Fig. 7 The graphical robustness results of W_1 against signal processing and geometric distortions



Average filter 5x5

Sharpen

Speckle noise μ=0 and σ^2=0.05

Histogram equalization

Centered cropping 100x100

Cropping 45%

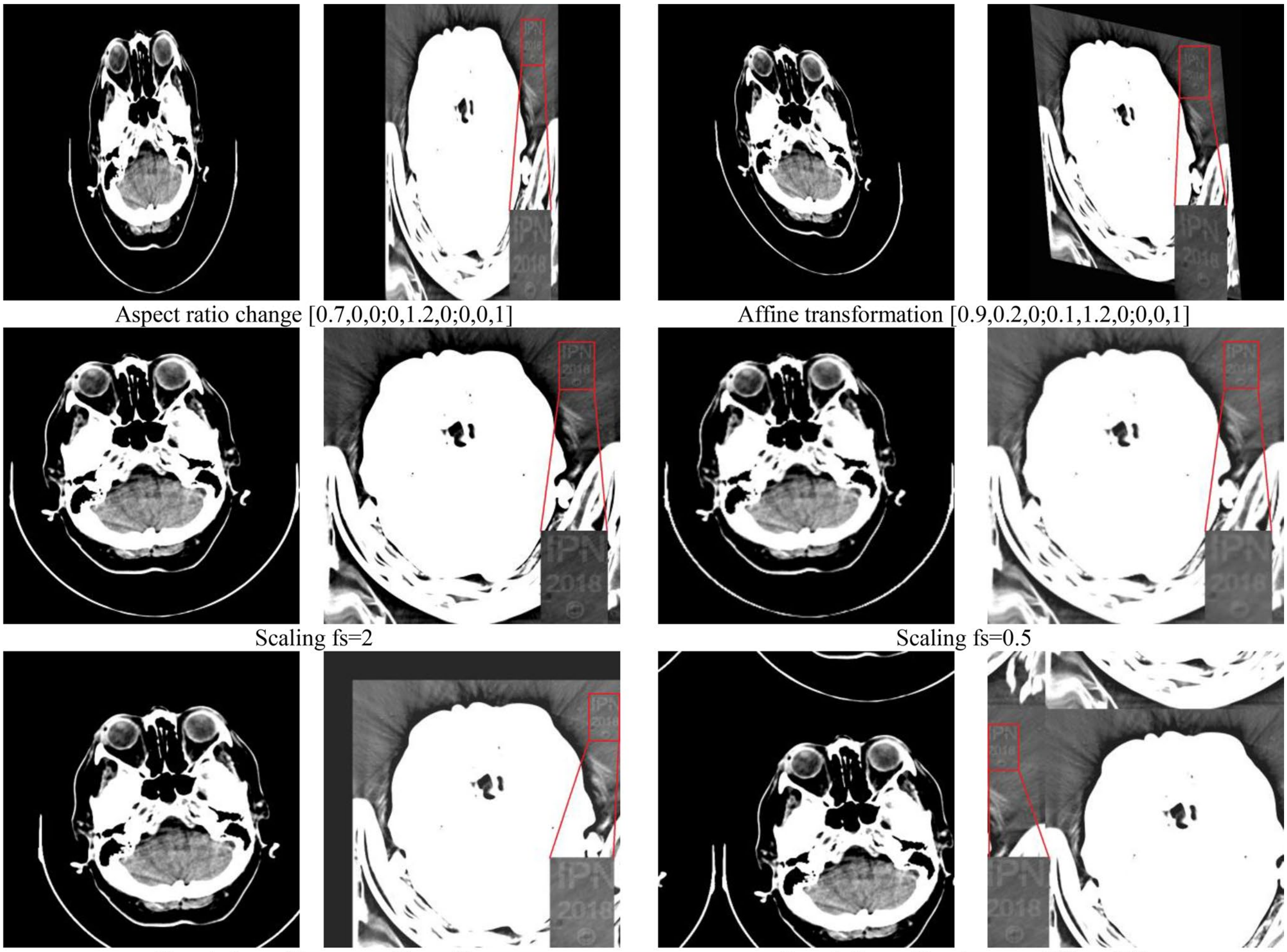
Rotation 45°

Rotation 135°

Flip left-right

Flip up-down

Fig. 7 (continued)



Aspect ratio change [0.7,0,0;0,1.2,0;0,0,1]

Affine transformation [0.9,0.2,0;0.1,1.2,0;0,0,1]

Scaling fs=2

Scaling fs=0.5

Translation with crop x=50, y=50

Translation without crop x=100, y=100

Fig. 7 (continued)

Table 5 Summary of signal processing and geometric distortions applied to W_2

Signal processing distortions and geometric distortions applied to watermark W_2		
(a) Without distortion	(h) Gamma correction γ = 1.05	(o) Centered cropping 100 × 100
(b) DICOM JPEG lossy compression	(i) Gamma correction γ = 0.95	(p) Cropping 45%
(c) Impulsive noise with density = 0.01	(j) Gaussian filter 7 × 7	(q) Rotation 45°
(d) DICOM JPEG lossless	(k) Median filter 3 × 3	(r) Rotation 135°
(e) DICOM JPEG2000 lossy	(l) Sharpen	(s) Aspect ratio change [0.7,0,0;0,1.2,0;0,0,1]
(f) DICOM JPEG2000 lossless	(m) Speckle noise $\mu = 0$ and $\sigma^2 = 0.05$	(t) Scaling fs = 2
(g) Gaussian noise $\mu = 0$ and $\sigma^2 = 0.015$	(n) Histogram equalization	(u) Scaling fs = 0.5

ultrasound (US) images in RGB format with 8 bit/pixel for each color channel, avoiding any down-sampling operation. However, the application of algorithm in [20] is limited only to ultrasound images and is not versatile to operate with bit depths greater than 8 bit/pixel. On the other hand, we found the related works in [8, 11, 19] that consider in its watermarking strategies bit depths greater than 8 bit/pixel, fact that allow its operation in practical scenarios. Our proposed method outperforms to algorithms in [8, 11, 21, 22] in terms of imperceptibility and robustness; and to the work in [19] in terms of payload. Moreover, our proposed method was evaluated considering more metrics of imperceptibility

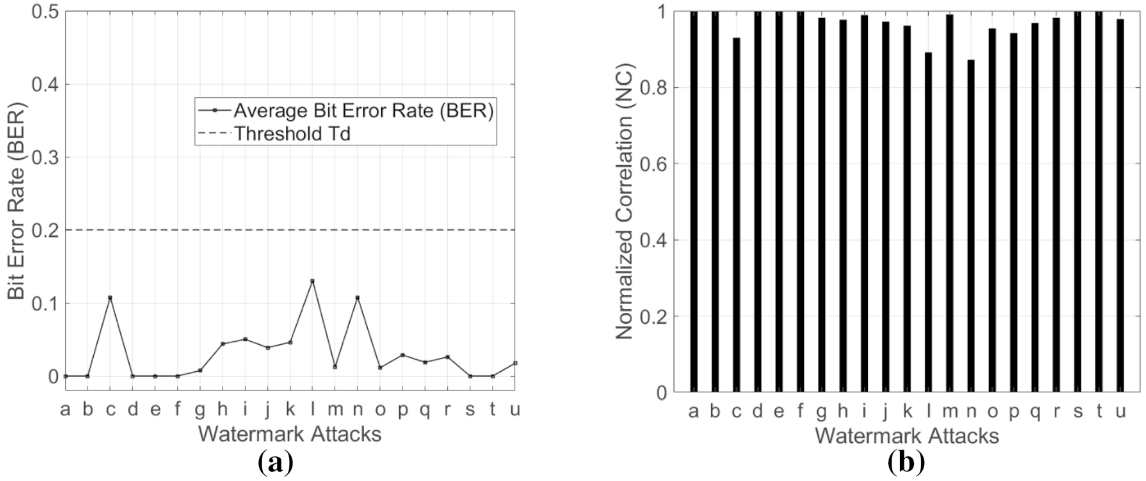


Fig. 8 The robustness results of W_2 against several signal processing and geometrics distortions, in terms of average **a** BER and **b** NC, respectively

Table 6 Computation time of the main procedures of the proposed method

Procedure	Processing time (s)	Stage
Concealment W_1	4.9	Visible-imperceptible
Exposure of W_1	0.02	Visible-imperceptible
Embedding of W_2	0.28	Robust-imperceptible
Extraction/detection W_2	0.23	Robust-imperceptible

and robustness that the reported in current the state of the art. Almost all related works in Table 7 seek embed multiple watermarks to solve one or more issues related to saving bandwidth, captioning, controlling access, indexing, confidentiality, authentication, and detachment avoidance. In this context and considering the above punctual analysis, we show the advantages to implement a hybrid and robust watermarking algorithm that embeds two different watermarks into the DICOM medical images, considering the properties of *visible-imperceptible* and *robust-imperceptible* watermarking modalities, to solve the issues related to the authentication of image source and avoid the detachment between the EPR data and medical image.

5 Conclusion

In this paper, we propose a hybrid digital watermarking scheme that combines the properties of *visible-imperceptible* and *robust-imperceptible* watermarking paradigms to prevent detachment between the EPR data and medical images, as well as perform the authentication of image source of DICOM images. To the best of our knowledge, the *visible-imperceptible* watermarking paradigm has not been applied to DICOM medical imaging to authentication of image source by a naked eye, considering DICOM images with bit-depth greater than 8 bits/pixel, making our proposal pioneer in this research field. The efficiency of the proposed method was confirmed by performing several experiments regarding imperceptibility and robustness. The average visual quality results confirm that the watermarks inserted by the proposed scheme are not perceived by the naked eye and consequently do not produce any distortion, fact that allow the correct issuance of a medical diagnosis. Additionally, the authentication of the image source is not a complex process and is possible to see the logo of the image source by the naked eye once the reveal stage is performed. Regarding robustness, the proposed method was tested by applying extensive experiments to simulate more than twenty geometric and signal processing operations. Finally, we confirm the contribution of the proposed scheme by comparing its performance with state-of-the-art proposals. Our proposal preserves the native DICOM format with the original grayscale resolution, so it is ready for its integration into practical scenarios. Additionally, our method outstands among current proposals regarding robustness and imperceptibility. As future work, we consider improving the embedding strategy without affecting the imperceptibility and robustness obtained hitherto, to other DICOM modalities such as computed radiography (CR), radio fluoroscopy (RF), and magnetic resonance imaging (MRI), among others.

Table 7 Performance comparison

Method	JPEG compression	Watermark payload	Imperceptibility metric	Detection metric	Application	Versatility of bit depth	Geometric attacks	Types of noises
[5]	JPEG lossy JPEG 2000	389 bits	PSNR, weighted peak signal to noise ratio (WPSNR), MSSIM, total perceptual error (TPE) [50]	Subjective criterion	Authentication Indexing	Down-sampled 8bit/pixel	–	Salt and pepper Speckle
[6, 9]	All DICOM compression modes	80 bits	PSNR, SSIM, VIF	BCR	Avoid detachment	Down-sampled 8bit/pixel	Rotation Scaling Translation Cropping	Gaussian Salt and pepper
[7]	–	4096 bits	PSNR	NC	Authentication	Down-sampled 8bit/pixel	–	–
[8]	–	4096 bits	PSNR	NC	Authentication Integrity	12 bit/pixel	–	Gaussian Salt and pepper
[10]	JPEG lossy	65,586 bits	PSNR	NC BER	Authentication	Down-sampled 8bit/pixel	Rotation Scaling Cropping Affine	Gaussian Salt and pepper
[11]	All DICOM compression modes	808 bits	PSNR, SSIM	BER	Authentication	16 bit/pixel	–	Salt and pepper
[12]	JPEG lossy	4800 bits	PSNR, MSE	NCC	Confidentiality and Security	Down-sampled 8bit/pixel	Rotation	–
[14]	JPEG lossy	2046 bits	PSNR, WPSNR, SSIM	NCC BER	Authentication	Down-sampled 8bit/pixel	Scaling Cropping	Gaussian Salt and pepper
[15]	-	4096 bits	PSNR	NC	Authentication	Down-sampled 8bit/pixel	Rotation Scaling	Gaussian Salt and pepper Speckle
[16]	JPEG lossy	22,490 bits	PSNR	NC BER	Authentication	Down-sampled 8bit/pixel	Scaling Rotation Cropping	Gaussian Salt and pepper
[17]	JPEG lossy	65,800 bits	PSNR	NC BER	Authentication Confidentiality and security	Down-sampled 8bit/pixel	Rotation Cropping	Gaussian Salt and pepper Speckle
[19]	All DICOM compression modes	552 bits	PSNR, SSIM, VIF	BER	Avoid detachment Patient authentication	10, 12, and 16 bit/pixel	Rotation Scaling Cropping Aspect ratio Flip	Gaussian Salt and pepper Speckle
[20]	All DICOM compression modes	80 bits	PSNR, SSIM	BER	Authentication Avoid detachment	8 bit/pixel	Rotation Scaling Translation Cropping	Gaussian Salt and pepper Speckle

Table 7 (continued)

Method	JPEG compression	Watermark payload	Imperceptibility metric	Detection metric	Application	Versatility of bit depth	Geometric attacks	Types of noises
[21]	JPEG lossy	3000–4000 bits	PSNR, SSIM, number of pixels changed ratio (NPCR)	NC	Authentication	16 bit/pixel	Scaling Cropping	Gaussian Salt and pepper
[22]	JPEG lossy	65,632 bits	PSNR, SSIM, NPCR, Unified averaged changed intensity (UACI)	BER, NC	Authentication Confidentiality and security	Down-sampled 8bit/pixel	Rotation Cropping	Gaussian Salt and pepper
Proposed method	All DICOM compression modes	6070 bits	PSNR, SSIM, VIF, MSE, UQI VSNR, WSNR, MSSIM	BER, NC Naked eye	Authentication Avoid detachment	10, 12, and 16 bit/pixel	Rotation Scaling Translation Cropping Affine Aspect ratio Flip	Gaussian Salt and pepper Speckle

Acknowledgements Authors thank the Instituto Politecnico Nacional (IPN), the PAPIIT IT-101119 project research from DGAPA in the Universidad Nacional Autonoma de Mexico (UNAM), the Instituto Mexicano del Seguro Social (IMSS) of Mexico as well as the Consejo Nacional de Ciencia y Tecnologia de Mexico (CONACYT) by the support provided during the realization of this research.

References

1. National Electrical Manufacturers Association (NEMA), DICOM Security. 8 Feb 2020. https://www.dicomstandard.org/using/security/
2. Coatrieux, G., Quantin, C., et al.: Watermarking medical images with anonymous patient identification to verify authenticity. In: Studies in Health Technology and Informatics, Vol. 136, pp. 667–672. IOS Press (2008)
3. Qasim, A.F., Meziane, F., Aspin, R.: Digital watermarking: applicability for developing trust in medical imaging workflows state of the art review. Comput. Sci. Rev. **27**, 45–60 (2018). https://doi.org/10.1016/j.cosrev.2017.11.003
4. Mousavi, S.M., Naghsh, A., Abu-Bakar, S.A.R.: Watermarking techniques used in medical images: a survey. J. Digit Imaging **27**, 714–729 (2014). https://doi.org/10.1007/s10278-014-9700-5
5. Das, S., Kundu, M.K.: Effective management of medical information through a novel blind watermarking technique. J. Med Syst. **36**, 3339–3351 (2012). https://doi.org/10.1007/s10916-012-9827-1
6. Cedillo-Hernandez, M., et al.: Robust watermarking method in DFT domain for effective management of medical imaging. SiVP Springer **9**, 1163–1178 (2015). https://doi.org/10.1007/s11760-013-0555-x
7. Kalaivani, K.: An efficient watermarking scheme for medical data security with the aid of neural network. Braz. Archiv. Biol. Technol. 59(spe2), e16161070, 1–12 (2016). https://doi.org/10.1590/1678-4324-2016161070
8. Aherrahrou, N., Tairi, H.: PDE based scheme for multi-modal medical image watermarking. BioMed Eng. OnLine **14**(108), 1–19 (2015). https://doi.org/10.1186/s12938-015-0101-x
9. Cedillo-Hernandez, M., et al.: Security enhancement of medical imaging via imperceptible and robust watermarking. IEICE Trans. Inf. Syst **E98-D5(9)**, 1702–1705 (2015). https://doi.org/10.1587/transinf.2015EDL8016
10. Singh, A.K., Dave, M., Mohan, A.: Hybrid technique for robust and imperceptible multiple watermarking using medical images. Multimed. Tools Appl. **75**, 8381–8401 (2016). https://doi.org/10.1007/s11042-015-2754-7
11. Mousavi, S.M., et al.: A robust medical image watermarking against salt and pepper noise for brain MRI images. Multimed. Tools Appl. **76**, 10313–10342 (2017). https://doi.org/10.1007/s11042-016-3622-9
12. Rodriguez-Colin, R., et al.: A robust watermarking scheme applied to radiological medical images. IEICE Trans. Inf. Syst. **E91-D**(3), 862–864 (2008). https://doi.org/10.1093/ietisy/e91-d.3.862
13. Sharma, A., Singh, A.K., Ghrera, S.P.: Secure hybrid robust watermarking technique for medical images. Procedia Comput. Sci. **70**, 778–784 (2015). https://doi.org/10.1016/j.procs.2015.10.117
14. Thakkar, F.N., Srivastava, V.K.: A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. Multimed. Tools Appl. **76**, 3669–3697 (2017). https://doi.org/10.1007/s11042-016-3928-7
15. Gangadhar, Y., et al.: An evolutionary programming approach for securing medical images using watermarking scheme in invariant discrete wavelet transformation. Biomed. Signal Process. Control **43**, 31–40 (2018). https://doi.org/10.1016/j.bspc.2018.02.007
16. Swaraja, K.: Medical image region-based watermarking for secured telemedicine. Multimed. Tools Appl. **77**(21), 28249–28280 (2018). https://doi.org/10.1007/s11042-018-6020-7
17. Sharma, A., Singh, A.K., Ghrera, S.P.: Robust and secure multiple watermarking for medical images. Wirel. Pers Commun. **92**, 1611–1624 (2017). https://doi.org/10.1007/s11277-016-3625-x
18. Mahesh Selvi, T., Kavitha, V.: A privacy-aware deep learning framework for health recommendation system on analysis of big data. Vis. Comput. (2021). https://doi.org/10.1007/s00371-020-02021-1
19. Cedillo-Hernandez, M., Cedillo-Hernandez, A., Nakano-Miyatake, M., Perez-Meana, H.: Improving the management of medical

imaging by using robust and secure dual watermarking. Biomed. Signal Process. Control **56**, 101695 (2020). https://doi.org/10.1016/j.bspc.2019.101695

20. Nuñez-Ramirez, D., Cedillo-Hernandez, M., Nakano-Miyatake, M., Perez-Meana, H.: Efficient management of ultrasound images using digital watermarking. IEEE Lat. Am. Trans. **18**(08), 1398–1406 (2020). https://doi.org/10.1109/TLA.2020.9111675
21. Kahlessenane, F., Khaldi, A., Kafi, R., et al.: A DWT based watermarking approach for medical image protection. J. Ambient Intell. Human Comput. (2020). https://doi.org/10.1007/s12652-020-02450-9
22. Anand, A., Singh, A.K.: An improved DWT-SVD domain watermarking for medical information security. Comput. Commun. **152**, 72–80 (2020). https://doi.org/10.1016/j.comcom.2020.01.038
23. Swaraja, K., Meenakshi, K., Kora, P.: An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine. Biomed. Signal Process. Control **55**, 101665 (2020). https://doi.org/10.1016/j.bspc.2019.101665
24. Su, G.D., Chang, C.C., Lin, C.C.: Effective self-recovery and tampering localization fragile watermarking for medical images. IEEE Access **8**, 160840–160857 (2020). https://doi.org/10.1109/ACCESS.2020.3019832
25. Geetha, R., Geetha, S.: Efficient high capacity technique to embed EPR information and to detect tampering in medical images. J. Med. Eng. Technol. **44**(2), 55–68 (2020). https://doi.org/10.1080/03091902.2020.1718223
26. Haddad, S., Coatrieux, G., Moreau-Gaudry, A., Cozic, M.: Joint watermarking-encryption-JPEG-LS for medical image reliability control in encrypted and compressed domains. IEEE Trans. Inf. Forensics Secur. **15**, 2556–2569 (2020). https://doi.org/10.1109/TIFS.2020.2972159
27. El-Tokhy, M.S.: Development of optimum watermarking algorithm for radiography images. Comput. Electr. Eng. **89**, 106932 (2021). https://doi.org/10.1016/j.compeleceng.2020.106932
28. Liu, J., et al.: Robust watermarking algorithm for medical volume data in internet of medical things. IEEE Access **8**, 93939–93961 (2020). https://doi.org/10.1109/ACCESS.2020.2995015
29. Gong, Z., Qin, N., Zhang, G.: Visible watermarking in document images using two-stage fuzzy inference system. Vis. Comput. (2021). https://doi.org/10.1007/s00371-020-02045-7
30. Barni, M., Bartolini, F.: Applications. In: Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications, pp. 23–44. CRC Press, Boca Raton (2004). https://doi.org/10.1201/9780203913512
31. Yuan, Z., Su, Q., Liu, D., et al.: A blind image watermarking scheme combining spatial domain and frequency domain. Vis. Comput. (2020). https://doi.org/10.1007/s00371-020-01945-y
32. Liu, D., Su, Q., Yuan, Z., et al.: A color watermarking scheme in frequency domain based on quaternary coding. Vis. Comput. (2020). https://doi.org/10.1007/s00371-020-01991-6
33. Ahmadi, B.B.S., Zhang, G., Wei, S., et al.: An intelligent and blind image watermarking scheme based on hybrid SVD transforms using human visual system characteristics. Vis. Comput. **37**, 385–409 (2021). https://doi.org/10.1007/s00371-020-01808-6
34. Chuang, S.C., Huang, C.H., Wu, J.L.: Unseen visible watermarking. In: IEEE International Conference on Image Processing, 261–264. San Antonio, Texas (2007) https://doi.org/10.1109/ICIP.2007.4379296
35. Huang, C.H., et al.: Unseen visible watermarking: a novel methodology for auxiliary information delivery via visual contents. IEEE Trans. Inf. Forensic Secur. **4**(2), 193–206 (2009). https://doi.org/10.1109/TIFS.2009.2020778
36. Lin, P.Y.: Imperceptible visible watermarking based on post camera histogram operation. J. Syst. Softw. **95**, 194–208 (2014). https://doi.org/10.1016/j.jss.2014.04.038
37. Juarez-Sandoval, U., et al.: Digital image ownership authentication via camouflaged unseen-visible watermarking. Multimed. Tools Appl. **77**(20), 26601–26634 (2018). https://doi.org/10.1007/s11042-018-5881-0
38. Pei, S.C., Wang, Y.Y.: Auxiliary metadata delivery in view synthesis using depth no synthesis error model. IEEE Trans. Multimed. **17**(1), 128–133 (2015). https://doi.org/10.1109/TMM.2014.2368255
39. Schneier, B.: Applied Cryptography, 2nd edn. Wiley, New York (1996)
40. Dobbertin, H., et al.: RIPEMD-160, a strengthened version of RIPEMD. In: Gollmann, D. (ed) Fast Software Encryption, LNCS, vol. 1039, pp. 71–82. Springer, Berlin (1996) https://doi.org/10.1007/3-540-60865-6_44
41. Bosselaers, A., et al.: The RIPEMD-160 cryptographic hash function. Dr. Dobb's J. **22**(1), 24–28 (1997)
42. Sklar, B.: Digital Communications: Fundamentals and Applications, 2nd edn., System View (2001)
43. Chen, B., Wornell, G.W.: Quantization index modulation: a class of provably good method for digital watermarking and information embedding. IEEE Trans. Inf. Theor. **47**(4), 1423–1443 (2001). https://doi.org/10.1109/18.923725
44. Batson, B.H., Moorehead, R.W.: Simulation Results for the Viterbi Decoding Algorithm. NASA-TR-R-396, Technical report (1972)
45. Tang, C.W., Hang, H.M.: A feature-based robust digital image watermarking scheme. IEEE Trans. Signal Process. **51**(4), 950–959 (2003). https://doi.org/10.1109/TSP.2003.809367
46. Medixant. RadiAnt DICOM Viewer [Software]. Version 2020.2. Jul 19, 2020. https://www.radiantviewer.com
47. Wang, Z., et al.: Image quality assessment: from error visibility to structural similarity. IEEE Trans. Image Process **13**(4), 600–612 (2004). https://doi.org/10.1109/TIP.2003.819861
48. Sheikh, H.R., Bovik, A.C.: Image information, and visual quality. IEEE Trans. Image Process **15**(2), 430–444 (2006). https://doi.org/10.1109/TIP.2005.859378
49. Chandler, D.M., Hemami, S.S.: VSNR: a wavelet-based visual signal-to-noise ratio for natural images. IEEE Trans. Image Process. **16**(9), 2284–2298 (2007). https://doi.org/10.1109/TIP.2007.901820
50. Watson, A.B.: DCT quantization matrices visually optimized for individual images. In: Proceedings of SPIE: Human Vision, Visual Processing, and Digital Display IV, vol. 1913, pp. 202–216 (1993) https://doi.org/10.1117/12.152694

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

David Mata-Mendoza was born in Mexico. He received his B.S. and M.S. degrees in the Instituto Politecnico Nacional (IPN) in the years 2018 and 2019, respectively. Currently, he courses the Ph.D degree in Communications and Electronic from the Instituto Politecnico Nacional (IPN). His principal research interests are security information, image processing, watermarking and related fields.

Manuel Cedillo-Hernandez was born in Mexico. He received the B.S. degree in Computer Engineering, the M.S. degree in Microelectronics Engineering and his PhD in Communications and Electronic from the National Polytechnic Institute of Mexico (IPN) in the years 2003, 2006 and 2011, respectively. He has six years of professional experience at Government positions related to IT. From September 2011 to December 2015 he was with the Engineering Faculty of the UNAM where he was a Professor. Currently, he is a full-time researcher at IPN. His principal research interests are image and video processing, watermarking, software development and related fields.

Francisco Garcia-Ugalde was born in Mexico. He received the B.S. degree in 1977, in electronics and electrical system engineering from UNAM, his Diplôme d'Ingénieur from SUPELEC France in 1980, and his PhD in 1982 in information processing from Université de Rennes I, France. Since 1983. Currently he is a full-time professor, and he was appointed to head of the Codification and Security of the Systems Communication Laboratory (CSSCL) in the Engineering Faculty of the National Autonomous University of Mexico (UNAM). His current research interest fields are: Digital filter design tools, analysis and design of digital filters, image and video processing, theory and applications of error control coding, turbo coding, cryptography applications, watermarking, hidden information, parallel processing and data bases.

Antonio Cedillo-Hernandez was born in Mexico. He received the B.S. degree in Computer Engineering, the M.S. degree in Microelectronic Engineering and his PhD in Communications and Electronic from the National Polytechnic Institute of Mexico in the years 2005, 2007 and 2013, respectively. He has about seven years of professional practice in several strategic positions related to IT. Currently, he concluded a postdoctoral position at National Autonomous University of Mexico. His principal research interests are video and image processing, information security, watermarking and related fields.

Mariko Nakano-Miyatake was born in Japan. She received the M.E. degree in 1985, in Electrical Engineering from the University of Electro-Communications, Tokyo Japan, and the PhD degree in Electrical Engineering from Metropolitan Autonomous University (UAM), Mexico City, in 1998. From July 1992 to February 1997 she was at Department of Electrical Engineering in UAM. In February 1997, she joined the Graduate Department of The Mechanical and Electrical Engineering School at National Polytechnic Institute of Mexico, where she is now a professor. Her research interests are in information security, image processing, pattern recognition and related fields.

Hector Perez-Meana was born in Mexico. He received his M.S: Degree on Electrical Engineering from the Electro-Communications University of Tokyo Japan in 1986 and his PhD degree in Electrical Engineering from the Tokyo Institute of Technology, Tokyo, Japan, in 1989. From March 1989 to September 1991, he was a visiting researcher at Fujitsu Laboratories Ltd, Kawasaki, Japan. From September 1991 to February 1997 he was with the Electrical Engineering Department of the UAM where he was a Professor. In February 1997, he joined the Graduate Studies and Research Section of The Mechanical and Electrical Engineering School, of the National Polytechnic Institute of Mexico, where he is now a Professor. His principal research interests are adaptive systems, image processing, pattern recognition, watermarking and related fields.