Biomedical Signal Processing and Control 56 (2020) 101695

Contents lists available at ScienceDirect

Biomedical Signal Processing and Control

journal homepage: www.elsevier.com/locate/bspc

Improving the management of medical imaging by using robust and secure dual watermarking

M. Cedillo-Hernandez[a,*], A. Cedillo-Hernandez[b], M. Nakano-Miyatake[a], H. Perez-Meana[a]

[a] Instituto Politecnico Nacional SEPI ESIME Culhuacan, Avenida Santa Ana 951, San Francisco Culhuacan, Culhuacan CTM V, C.P. 04260, Coyoacan, Ciudad de Mexico, Mexico
[b] Universidad Politecnica Metropolitana de Hidalgo, Ex Hacienda San Javier, Boulevard Acceso a Tolcayuca 1009, 43860, Tolcayuca, Hidalgo, Mexico

ARTICLE INFO

Article history:
Received 28 June 2019
Received in revised form 9 September 2019
Accepted 5 October 2019

Keywords:
Digital watermarking
Image processing
Information security
DICOM imaging
Authentication
Detachment detection

ABSTRACT

Nowadays, the management of medical imaging could be affected by several issues related to information security. Among others, a critical issue is related to information authentication. A promissory way to solve this issue is the use of digital watermarking to improve the management of medical imaging. In this paper, we propose a robust and secure medical image watermarking method that involves *invisible* and *zero* watermarking techniques that provide a proper link between clinical information, medical image, and patient identity. Concealing an encoded and encrypted watermark signal in the frequency domain of the medical image, the *invisible* watermarking component avoids the detachment between the medical images and their corresponding electronic patient record. Based on a modified spread spectrum technique, the response of the *invisible* watermarking detector and the watermark information, the *zero* watermarking stage authenticates in a confidential form the identity of the patient. Experimental results show the effectiveness of the proposed method in terms of transparency, security, reliability, and robustness of the watermark against several image processing operations. A comparison with state of the art proposals with similar purposes to the proposed method is also provided. The presented work may find applications in the secure and effective management of medical imaging.

1. Introduction

Due to its relevance in clinical diagnosis, treatment, research, and other commercial and non-commercial applications of public and private organizations; medical information is highly valuable and delicate by nature. In recent years the fast and significant advances in terms of information technologies (IT) have generated a large number of changes to conceptual and application-level into the paradigm of medical information management. The modern and integrated healthcare systems such as Hospital Information System (HIS) and Picture Archiving and Communication System (PACS) among others; provides easy access, manipulation, and distribution of medical data [1–3]. There are several reasons for the interchange of medical information, e.g. telemedicine applications where we found teleconsultation, telediagnosis, and telesurgery with aims of e-learning of the medical staff. On the other hand, the Electronic Patient Record (EPR) has replaced the ineffective paradigm of the medical record in hardcopy format. Usually, EPR contains diagnosis reports, medical images, and biomedical signals, among other information, however, also could contain medical record such as demographic data, results of medical testing, treatments, medical prescriptions, among others, which are by definition highly confidential [3,4]. These advances in the technology of medical information management have brought as a consequence new risks by the inappropriate use of the medical information, given the facility with which the digital data could be manipulated and distributed.

In a medical image context, these have unique features and requirements that moreover of the ethics and legal aspects, should be preserved to define the allowed operations on the medical information so that it does not cause a degradation level on the image that can generate a wrong medical diagnosis [5]. Thus, it is imperative to improve its security. In this way moreover of security improvement, is needs the design of suitable medical image storage and distribution systems, with controlled and restricted access to medical imaging, preserving unaltered the requirements of authentication, integrity, and confidentiality of medical data, with aims of

[*] Corresponding author.
E-mail addresses: mcedilloh@ipn.mx (M. Cedillo-Hernandez), acedillo@upmh.edu.mx (A. Cedillo-Hernandez).

https://doi.org/10.1016/j.bspc.2019.101695
1746-8094/© 2019 Elsevier Ltd. All rights reserved.

efficient management [6]. However, the management of medical imaging could be affected by several issues related to information security. Among others, critical problems are concerned with the way to authenticate applications focusing on image source verification, validation that the medical image belongs to the proper patient as well as avoiding the detachment between the medical images and their corresponding EPR [6–8]. A promissory way to solve the above security issues consists of design and integrate a solution based on digital watermarking [9–12] to improve the management and security of medical imaging [1,2,5,7,8]. In general terms, the conventional digital watermarking allows concealing data in several formats such as binary logo, pseudorandom patterns or text into an image either visible or invisible manner. Initially, the primary motivation of digital watermarking was the copyright protection and ownership authentication of the multimedia data [9–12], however, over the years have been extended to a wide range of applications among which stands out the related to the protection of medical images that fulfill with the international standard Digital Imaging and Communications in Medicine (DICOM) [13].

In this context, this paper proposes a hybrid watermarking algorithm composed of a couple of *invisible* watermarking and *zero* watermarking complementary methods, with purposes of improving the management of medical imaging. Several testing were carried out in terms of imperceptibility, robustness, and security. The visual quality of the protected images is measured using the peak signal to noise ratio (PSNR), structural similarity index (SSIM) and visual information fidelity (VIF). Experimental results confirm the efficiency of the proposed method in terms of transparency, security, and robustness of the watermark against several image processing operations. A comparison with state of the art proposals with similar purposes to the proposed method is also provided. The organization of the proposed paper is as follows. In Section 2 we explain the contribution and a general description of this work. In Section 3 we show a compilation that contains the most recent and related works with this proposal. In Section 4 we explain in a detailed manner the different stages that composing the proposed algorithm. Section 5 shows the experimental results and discussion. Finally, Section 6 concludes this work.

2. The most important contribution of the work

Digital watermarking has the potential of being a value-added tool in order to confront several problems associated with the medical data management, among which we can mention: a) avoid detachment between image and corresponding EPR, b) authentication, c) bandwidth saving, d) confidentiality and security, e) integrity control, f) indexation and g) labeling. According to the application context, a digital watermarking method for medical imaging can be *invisible* and *distortion-free* watermarking. *Invisible* watermarking consists of two main stages, one to embed a small signal called "watermark" into the image content and other to detect or recover the watermark signal from the protected image [1,2,5–25], remaining hidden the watermark to any unauthorized user and should be resistant to any attempt to suppress it [1]. Generally, an algorithm of this category should be accomplishing three main requirements which are: robustness, enough payload, and imperceptibility. An essential challenge in the design of these algorithms is preserving a balanced trade-off between the three watermarking requirements because medical staff is very strict with the visual quality of the images. As a consequence, a limitation of *invisible* watermarking in a context of medical imaging is its constrained capacity in terms of watermark payload; however, with few watermark data bits often offer high visual quality as well as high robustness against several geometric and common signal processing distortions [9–12].

On the other hand, in the literature, we can find two kinds of *distortion-free* watermarking techniques. The first one is known as reversible watermarking, in which once the watermark sequence is detected or extracted from the watermarked image, the original undistorted host image can be recovered [27]. However, generally speaking, the reversible watermarking techniques cannot provide sufficient robustness of watermark sequence to conventional signal processing tasks, such as JPEG compression and noise contamination. The second distortion-free watermarking technique is known as *zero* watermarking, in which the watermark sequence is not embedded physically into the host image, instead is logically linked with the host image keeping the host image intact [28–30,45–48]. In this way, some inherent features are extracted from the host image and are linked with an owner's watermark sequence to generate via or-exclusive operation a "*zero* watermark code," which is stored safely. The protected images by a *zero* watermarking algorithm are transmitted through any insecure public communication channels, and the owner can verify his ownership by using the *zero* watermark code and the inherent feature extracted from the image under analysis. Thus, in the *zero* watermarking technique, the extraction of robust intrinsic features of the host image is the most critical issue for their desirable performance. However, another significant and not least important issue happens when an image is analyzed by two or more *zero* watermarking algorithms since this fact will cause a severe controversy and ambiguity at the moment of claim the ownership authentication. Since every *zero* watermarking algorithm is in an equal condition of employ it's *zero* watermark code and extract the inherent features from the same image, as a consequence all *zero* watermarking algorithms that analyzing the same image could claim as their property. In a medical image context, this fact could carry several and serious authentication issues.

Table 1 summarizes the novelties and contributions in the proposed hybrid watermarking algorithm composed by *invisible watermarking* + *zero-watermarking* techniques versus *invisible* and *zero* watermarking approaches.

According to the advantages and disadvantages of the *invisible* and *zero* watermarking mentioned above into a medical imaging context, this paper proposes a hybrid watermarking algorithm composed by both modalities. In this way, an integrated solution is intended and designed with authentication purposes focusing on image source verification, validation that the medical image belongs to the proper patient as well as avoiding the detachment between the medical images and its correspondent electronic patient record. The architecture proposed hybrid watermarking algorithm is shown in Fig. 1.

On the one hand, the *invisible* watermarking based on the discrete cosine transform (DCT) domain employs the quantization index modulation under dither modulation (QIM-DM) technique [32] to embed and extract a watermark signal (clinical data of the patient). The watermark is then ciphered by using the message digest algorithm SHA-1 [26], and coded by a convolutional coder [31] and Viterbi decoder [36]; this architecture enables image source verification and avoiding detachment between the medical images and its correspondent EPR. Thus, only few watermark data bits are needed to accomplish the above aims, preserving a balance between imperceptibility and robustness. Additionally, to increase the watermark payload and validates that the medical image belongs to proper patient; we propose a *zero* watermarking that is applied in a non-conventional way. Our proposal does not extract inherent features from medical image; instead, only if the detection result of the *invisible* watermarking is success, it is obtained a customized key data set from the EPR. Then, it is ciphered by a one-way hash function SHA-1 [26] and processed via direct-sequence code division multiple access (DS-CDMA) [33] and a seam-carving image technique [34], to increase the payload

Table 1
Novelties and contributions in proposed hybrid watermarking algorithm.

Parameter	Invisible Watermarking	Zero Watermarking	Proposed hybrid method (*invisible* + *zero* watermarking)
Data Payload (Capacity)	Low, due to tradeoff imperceptibility-robustness-payload	High	High
Quality of watermarked medical image	Often high	Unaltered image	High
Robustness	High	Often high	High
Need of explicit extractor/detector	Yes	No	Yes
Need of inherent features extractor	No	Yes	No
Ambiguity	No, Due to the knowledge of the exact algorithms for embedding and extracting the invisible and unremovable watermark.	Yes, Since the image under analysis is unwatermarked and unaltered, if two or more zero-watermarking algorithms analyzing a given medical image, all could claim this as their property.	No, a) Due to the knowledge of the exact algorithms for embedding and extracting the invisible and unremovable watermark. b) Zero-watermarking increases the data payload and is not dependable on the inherent image features extractor.

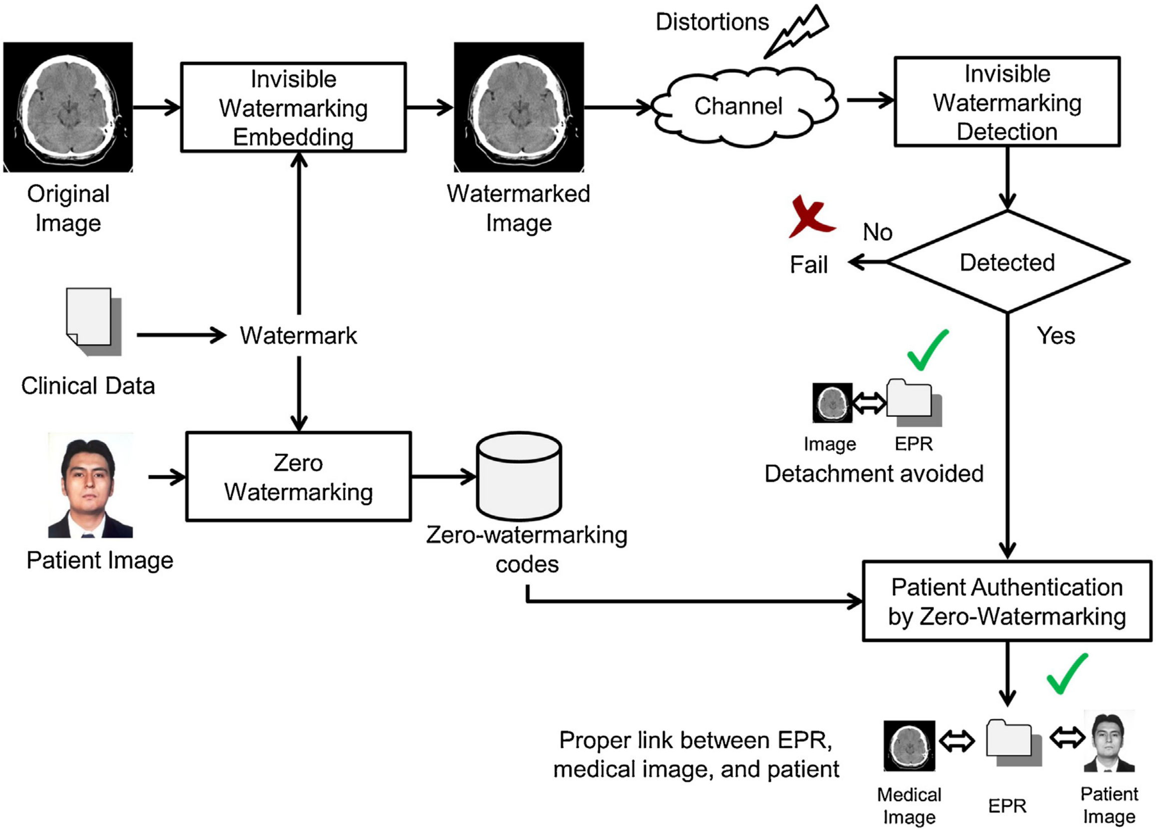


Fig. 1. Architecture of the proposed method.

and the security of the proposed *zero* watermarking methods. The result of this process is a feature pattern. Finally, to obtain the "*zero* watermark code," we employ a *xor* operation between the feature pattern and a halftone photograph of the patient obtained by the Floyd-Steinberg error diffusion halftoning method [35]. This strategy accomplishes with the aims of image source verification, validation that the medical image belongs to proper patient, avoiding any ambiguity and establishing an appropriate link between EPR, medical image, and patient.

3. Related works

Several methods for invisible watermarking applied to medical images have been proposed in the scientific literature [14–25,40–44]. In the following paragraphs, to the best of our knowledge, we explain a brief review of the most recent representative proposals. Sharma et al. in [15] propose a robust watermarking algorithm for medical images, which embed watermarks into the region of interest (ROI) and region of non-interest (RONI) respectively. The embedding domain used in [15] is a combination of two frequency domains, particularly the discrete wavelet transform (DWT) and DCT transforms. Two watermarks are used in the experiments, the first one is a binary logo of 256 × 256 in size, and the second one is a string of characters extracted from the EPR data. The algorithm is designed for patient identity verification purposes. The security of the watermarking method is enhanced using the message-digest (MD5) and Rivest-Shamir-Adleman (RSA) algorithms [26], applied to the watermarks before of the embedding stage. To improve the robustness of the proposed method, the Hamming error correction code is adopted. The method is evaluated from the points of view of robustness using the metrics bit error rate (BER) and normalized correlation (NC), and imperceptibility employing the PSNR metric. For your part, Mousavi et al. in [16] design a watermarking method with high robustness against

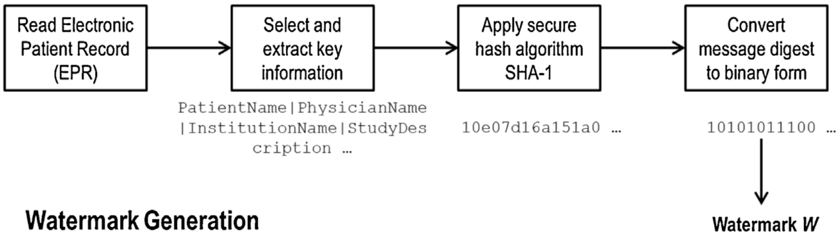

Read Electronic Patient Record (EPR)
Select and extract key information
Apply secure hash algorithm SHA-1
Convert message digest to binary form
PatientName|PhysicianName |InstitutionName|StudyDescription …
10e07d16a151a0 …
10101011100 …
Watermark Generation
Watermark W

Fig. 2. Watermark *W* generation procedure.

impulsive noise for brain magnetic resonance images (MRI). The watermark data bits extracted from the EPR are embedded in the spatial domain of RONI using channel coding and noise filtering methods. The visual quality of watermarked images is evaluated using PSNR and SSIM, and the accuracy of the extracted watermark is assessed using the BER metric. On the other hand, Thakkar et al. in [17] propose an invisible watermarking for telemedicine applications that is based on the frequency domain of the ROI of medical image, using DWT domain and the singular value decomposition (SVD) method. Two watermarks in logotype and string formats respectively are embedded into the image with purposes of authentication and identification of the original medical image. The Hamming error correcting code (ECC) is used to enhance the robustness of the method. The algorithm is applied to several modalities of medical images like X-ray, CT, and mammography. The watermark imperceptibility is measured using PSNR meanwhile the robustness is assessed with BER and NCC. For his part, Swaraja K. in [18] proposes a watermarking algorithm based on RONI of the medical images to conceal a couple of watermarking in logo format with aims of authenticity and validation of the original source for the interchange of medical images in telemedicine applications. The method is performed in a hybrid embedding domain composed by DWT and Schur transforms respectively. To enhance the trade-off imperceptibility-robustness, the Firefly optimization algorithm is adopted in the proposal. The watermarking method is tested on MRI, X-ray and Ultrasound modalities of medical images. The scheme is evaluated in terms of robustness using BER and normalized correlation (NC), imperceptibility employing PSNR and watermark payload. Gangadhar et al. in [19] propose an invisible watermarking method applied to medical images based on an improved discrete wavelet transform (IDWT) and SVD in order to get more robustness against signal processing distortions. In the same way that Swaraja K. [18], the authors in [19] adopts an optimization algorithm called particle swarm optimization (PSO) to enhance the trade-off imperceptibility-robustness. The watermark used in the experimental results is a binary logo which is embedded in the low frequencies of IDWT transform. NC and PSNR metrics are considered to evaluate the robustness and transparency of the watermark respectively. Chauhan et al. [40] propose an adaptive watermarking method based on the Mexican hat wavelet and spread spectrum which conceals a watermark of 50 × 9 in size, into CT images with authentication purposes. After the medical images are shared or transmitted, the watermark is extracted using Cauchy statistical model. The imperceptibility of the watermark is measured with PSNR meanwhile the robustness with NC. For your part, Thakur et al. [41] propose an invisible watermarking based on a hybrid strategy that employs a combination of DWT, DCT, and SVD for tasks of authentication, annotation, and identification. To increase the security of the algorithm, the authors apply chaotic encryption to the watermarked medical image. The visual quality of the image is measured with PSNR and SSIM metrics. The watermark robustness is tested using NC metric. The size of the watermark is 256 × 256. On the other hand, Surekah Borra et al. [42] presents an invisible medical image watermarking technique based on finite Ridgelet transform (FRT) and SVD in conjunction with Arnold scrambling. The algorithm is applied to two modalities of medical images, particularly X-ray and CT. The size of watermarks embedded into the medical content is 64 × 64, the imperceptibility is measured with PSNR, and the robustness is evaluated with NC. For your part, Assini et al. [43] propose a technique of medical image watermarking based on the combination of the stationary wavelet transform (SWT) and the fast Walsh-Hadamard transform (FWHT), to conceal watermarks of 512 × 512 in size with authentication purposes. The proposal is applied to CT, magnetic resonance angiography (MRA), MRI and X-Ray imaging. The method is evaluated from the imperceptibility and robustness points of view, using PSNR and NC respectively. Finally, Singh in [44] presents an invisible watermarking method based on lifting wavelet transform (LWT) and DCT in conjunction with message-digest algorithm MD5 and Bose–Chaudhuri–Hocquenghem (BCH) error-correcting code, oriented to telehealth applications. The method embeds watermarks of 64 × 64 and 80 in size respectively. The metric to measure the watermark imperceptibility is PSNR; meanwhile, the robustness is measured using BER and NC metrics.

4. Proposed method

The architecture of the proposed hybrid watermarking algorithm is composed by five stages; the first one is related to watermark generation, second and third one belongs to embedding and extraction/detection stages of the *invisible* watermarking, and the *zero* watermarking scheme is composed by the *zero* watermark code generation and authentication stages respectively. Each one is described in a detailed manner in the following paragraphs.

4.1. Watermark generation

In the sake of brevity and avoiding redundancy, we summarize the steps to generate the watermark pattern *W*, which is employed in the rest of the four stages and its procedure is illustrated in Fig. 2. In this way, to generate the watermark *W*:

Step 1- 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. This extraction could be customized according to desirable information.

Step 2- Apply the secure hash algorithm SHA-1 [26] to the DICOM data selected in the previous step. We would like to note that our proposed method may be easily adapted to the use of different message digest algorithms.

Step 3- Once the hash sequence is obtained convert the 40 hexadecimal digits to its 160 bits binary representation, which compose the watermark *W*.

4.2. Invisible watermarking: embedding algorithm

Embedding a watermark in the frequency domain of the DICOM image preserving its original bit-depth gives a certain number of robust properties with respect to geometric distortions and common signal processing. In this way, for image source verification and the same time avoiding the detachment between the medical

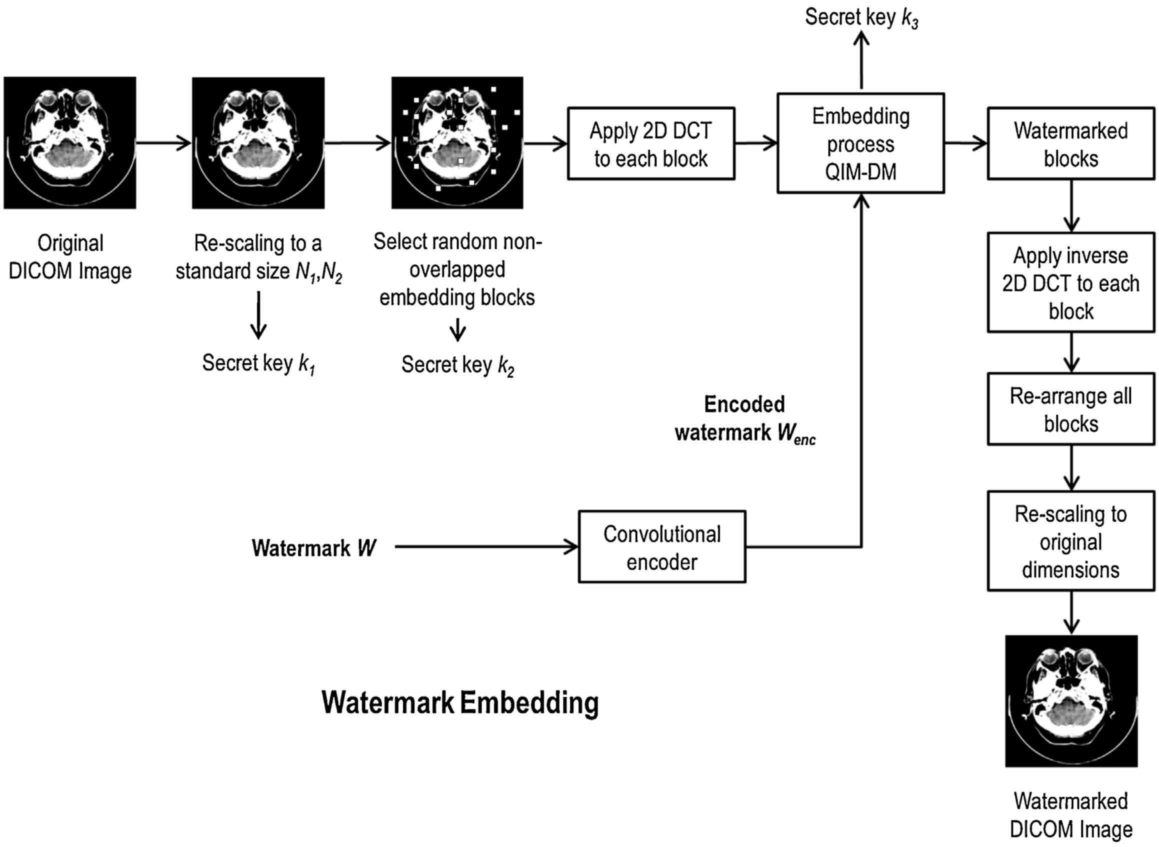


Fig. 3. Embedding procedure of the *invisible* watermarking.

images and its correspondent EPR, the embedding procedure of the watermark W is shown in Fig. 3 and described as follows.

Step 1- Read the original DICOM image, denoted as I and rescale it to a standard size of $N_1 \times N_2$. In order to increase the security of the proposed method, N_1, N_2 values will be provided as secret key k_1 in the extraction/detection stage.

Step 2- Encode W using a convolutional code [31] with code rate = 1/3, constraint length K = 5, free distance d_{free} = 12 and the generator polynomials g_1 = [11111], g_2 = [11011] and g_3 = [10101]. The redundant bits are used at the receiver to perform forward error correction to achieve a lower BER. The output of this step is the encoded watermark W_{enc}.

Step 3- Using a secret key k_2, B blocks of 8 × 8 pixels in size are selected randomly from the re-scaled image I. The amount of blocks A_B needed to embed groups of 4 bits of the encoded pattern W_{enc} into the image I' is obtained by (1):

$$A_B = length(W_{enc})/4 \quad , \tag{1}$$

Step 4- Divide W_{enc} in sub-sequences S_j, where j = 1,. . . A_B, composed of 4 bits each one. Then, each B_j block is transformed by the DCT transform. In this way each S_j is embedded into the 4 alternating currents (AC) coefficients with lowest frequencies of each B_j in the 2D DCT domain, using the QIM-DM algorithm [32] given by (2):

$$\begin{aligned} & if\ S_j(z) = 0 \\ & \quad Cw_z = \left\lfloor \frac{(Co_z + d(z,0))}{\Delta} \right\rfloor \cdot \Delta - d(z,0) \\ & else \\ & \quad Cw_z = \left\lfloor \frac{(Co_z + d(z,1))}{\Delta} \right\rfloor \cdot \Delta - d(z,1) \quad , \end{aligned} \tag{2}$$

where Co and Cw are the original and watermarked coefficient respectively in each B_j block, j = 1,. . . A_B, z = 1,2,3,4 and Δ is a step-size of quantification. The dither signals $d(z,0)$ and $d(z,1)$ are given by (3) and (4) respectively:

$$d(z,0) = -\Delta + (\Delta \cdot p) \quad , \tag{3}$$

$$d(z,1) = \begin{cases} d(z,0) + \dfrac{\Delta}{2}, & \rightarrow \quad if\ d(z,0) < 0 \\ d(z,0) - \dfrac{\Delta}{2}, & \rightarrow \quad otherwise \end{cases} \quad , \tag{4}$$

where Δ is a step-size of quantification, p is a pseudo-random signal with uniform distribution generated by a secret key k_3, the size of p is the length of z. Once all encoded bits W_{enc} are embedded into the DCT coefficients of each B_j block, the watermarked DCT coefficients are returned to the spatial domain applying the inverse 2D DCT. The resulting image is the protected image denoted as I_w.

Step 5- Finally, rescaling the protected image I_w to its original dimensions $N \times M$ and converts it to the DICOM native format.

4.3. Invisible watermarking: extraction/detection algorithm

Given a watermarked image, I_w, to extract and detect the presence or absence of the watermark W, the procedure is shown in Fig. 4 and explained as follows:

Step 1- Supported by the secret key k_1, rescale the protected image I_w to the chosen size $N_1 \times N_2$.

Step 2- Using the secret key k_2, the B blocks of 8 × 8 pixels in size are recovered from I_w. The encoded information is extracted from the B blocks in DCT domain using the QIM-DM extraction algorithm [32], given by (5):

$$d1_z = (Cw_z - Q1_z)^2, \quad d2_z = (Cw_z - Q2_z)^2 \quad , \tag{5}$$

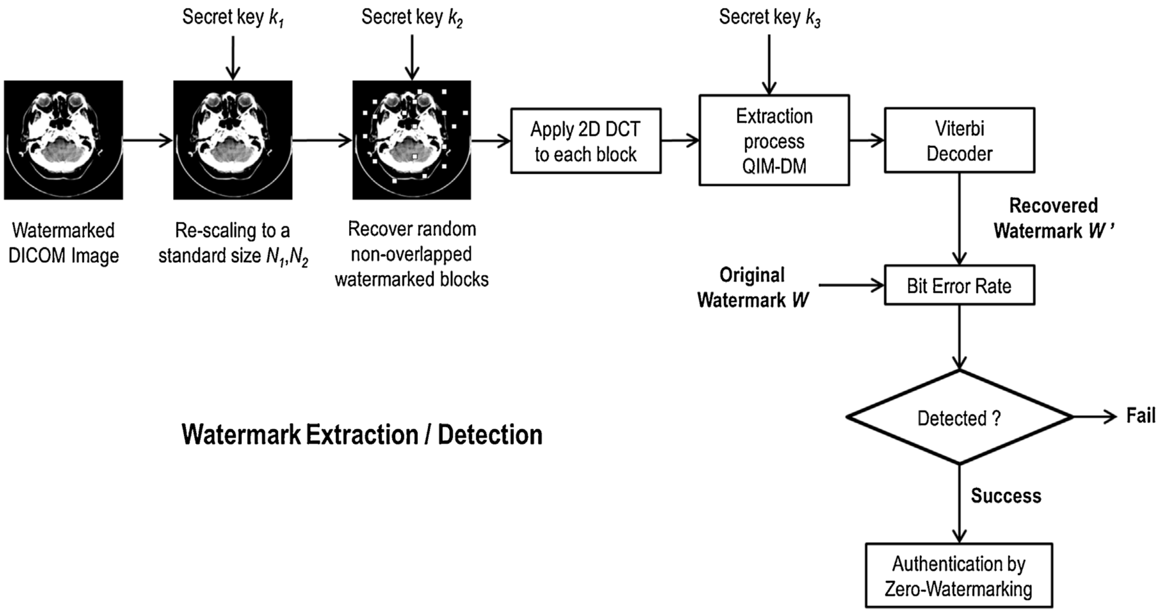

Secret key k_1
Secret key k_2
Secret key k_3
Watermarked DICOM Image
Re-scaling to a standard size N_1,N_2
Recover random non-overlapped watermarked blocks
Apply 2D DCT to each block
Extraction process QIM-DM
Viterbi Decoder
Recovered Watermark W'
Original Watermark W
Bit Error Rate
Detected ?
Fail
Success
Authentication by Zero-Watermarking
Watermark Extraction / Detection

Fig. 4. Extraction/Detection procedure of the *invisible* watermarking.

where *d1* and *d2* are a pair of distances, z = 1,2,3,4, *Cw* are the watermarked DCT coefficients and *Q1*, *Q2* is a pair of quantizators given by (6):

$$Q1_z = \left\lfloor \frac{(Cw_z + d(z,0))}{\Delta} \right\rfloor \cdot \Delta - d(z,0) \quad ,$$
$$Q2_z = \left\lfloor \frac{(Cw_z + d(z,1))}{\Delta} \right\rfloor \cdot \Delta - d(z,1) \quad , \qquad (6)$$

where Δ is the step-size of quantification used in the embedding procedure; $d(z,0)$ and $d(z,1)$ are given by (3) and (4) supported by the secret key k_3, respectively. Once that *d1* and *d2* are obtained, to extract an encoded watermark data bit we use the decision rule in (7):

$$\begin{aligned} &\text{if } d1_z < d2_z \quad \text{then } we' = 0 \\ &\qquad\qquad\qquad \text{else } we' = 1 \end{aligned} \qquad (7)$$

Repeat this step iteratively for each B_j block in DCT domain, where j = 1,. . . A_B, and recover the encoded watermark W_{enc}'.

Step 3- The decoding of W_{enc}' is performed using the Viterbi algorithm with hard decision [36], obtaining the recovered watermark *W*'.

Step 4- Once that *W*' was extracted from the DCT domain, compute the BER between the original *W* and the recovered *W*' watermarks.

Step 5- A decision threshold value T_d must be defined to determine if *W* is present or not into the I_w. Considering a binomial distribution with success probability equal to 0.5, a false alarm probability P_{fa} for *L* watermark data bits is given by (8), where a threshold value *T* must be controlled in order to get a smaller value of P_{fa} than a predetermined one.

$$P_{fa} = \sum_{\lambda=T}^{L} \left(\frac{1}{2}\right)^L \cdot \left(\frac{L!}{\lambda!(L-\lambda)!}\right) \quad , \qquad (8)$$

where L = 160 is the length of *W*. Based on the Bernoulli trials assumption, λ is an independent random variable with binomial distribution [37]. The false alarm probability must be less than 10^{-15} which is set to satisfy the requirements of most watermarking applications for a reliable detection [37], and then an adequate decision threshold value T_d is defined by (9):

$$T_d = 1 - \left(\frac{T}{L}\right) \quad , \qquad (9)$$

From (9), considering L = 160 and T = 128, then T_d = 0.20, according to the fact that BER + the bit correct rate (BCR) must be equal to 1. If the BER value between *W* and *W*' is greater than 20%, the detection process considers the absence of *W*, otherwise, *W* is detected in a successful manner, verifying the image source and the same time, the detachment between the medical image and its correspondent EPR is avoided. If *W* is detected in a successful manner, then we proceed to the authentication of the patient via *zero* watermarking technique, which is explained in the following paragraphs.

4.4. Zero-watermarking: code generation algorithm

Once confirmed the presence of *W* into watermarked medical image I_w, we proceed to the authentication of the patient via *zero* watermarking technique, whose code generation algorithm is shown in Fig. 5 and explained in detail as follows.

Step 1- Given a patient image with a bit-depth of 24 bit/pixel, first this is converted a grayscale with a bit-depth of 8 bit/pixel and consequently is down-sampled via the error diffusion halftoning method reported by Floyd-Steinberg in [35]. Fig. 6(a) shows the Floyd–Steinberg error diffusion method, where Q is the quantification process that transforms a grayscale value $i(x,y)$ of dimensions *n* x *m* in size into a binary one denoted by $b(x,y)$ using a threshold value T_b = 128 that corresponds to the half value of 8 bits/pixel grayscale. In general terms, the error sequence $e(x,y)$ is the difference between $u(x,y)$, $b(x,y)$, and is introduced to the 2D-filter *H*, whose coefficients are shown in Fig. 6(a); the black circle in the coefficients means the current pixel. The coefficients of *H* represent the diffusion ratio of $e(x,y)$ produced by *Q* to the neighbor pixels (only four future neighbors in a raster scan manner are considered). Thus, we use Floyd-Steinberg coefficients to generate halftone image I_H. Fig. 6(b) shows an example of this step.

Step 2- As mentioned in Section 2, our inherent feature for the proposed *zero* watermarking method is directly linked to the clinical data of a patient in order to avoid any ambiguity and establishing a proper link between EPR, medical image, and patient. In

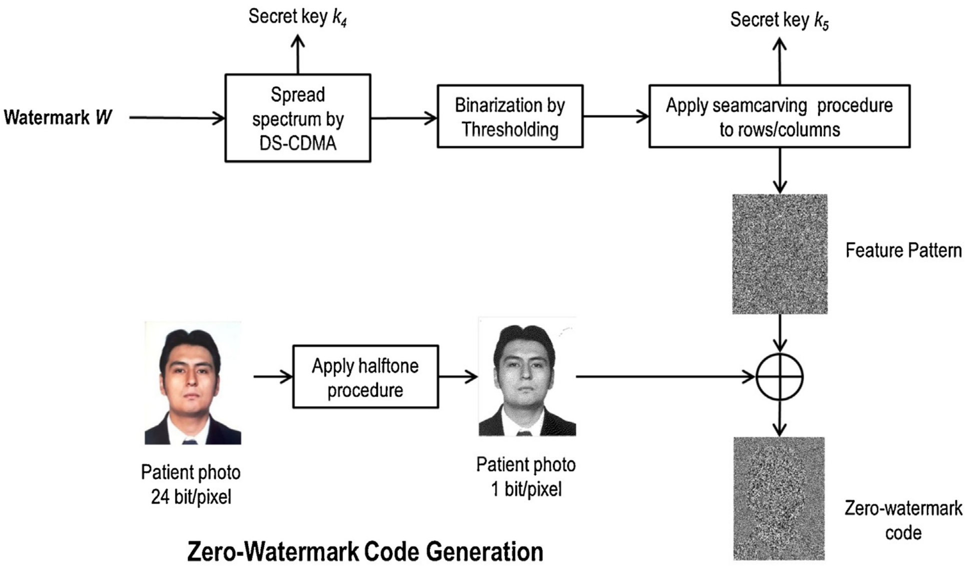

Secret key k_4
Watermark W
Spread spectrum by DS-CDMA
Binarization by Thresholding
Secret key k_5
Apply seamcarving procedure to rows/columns
Feature Pattern
Apply halftone procedure
Patient photo 24 bit/pixel
Patient photo 1 bit/pixel
Zero-watermark code
Zero-Watermark Code Generation

Fig. 5. *Zero* watermark code generation procedure.

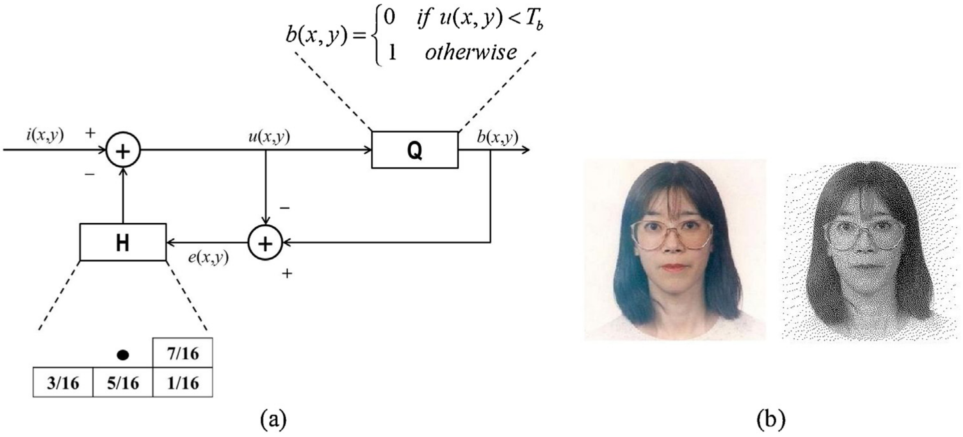

$b(x,y)=\begin{cases}0 & if\ u(x,y)<T_b\\ 1 & otherwise\end{cases}$
i(x,y)
+
−
u(x,y)
Q
b(x,y)
−
H
e(x,y)
+
●
7/16
3/16
5/16
1/16
(a)
(b)

Fig. 6. a) Halftoning method by Floyd-Steinberg [35], b) Input-Output of the halftoning procedure.

this way, using the binary information of W and the spread spectrum DS-CDMA [33], for each watermark data bit W_l, $l = 1,\ldots L$, a 2D pseudorandom pattern G_l composed by $\{-1,1\}$ with predefined dimensions p x q, is assigned according to a secret key k_4, given by (10).

$$\begin{matrix} +G_l & if\ W_l = 0 \\ -G_l & if\ W_l = 1 \end{matrix}. \qquad (10)$$

After that, the sum of all 2D pseudorandom patterns G_l defines a 2D feature pattern P, given by (11).

$$P = \sum_{l=1}^{L} \pm G_l, \qquad (11)$$

where the sign (±) of each G_l is dependent of W_l value as defined in (10).

Step 3- Apply a binarization procedure to 2D pattern P, given by (12)

$$\begin{matrix} P(x,y) = 1 & if\ \ P(x,y) > 0 \\ P(x,y) = 0 & otherwise \end{matrix}. \qquad (12)$$

Step 4- To increase the security of the 2D feature pattern P, we apply the seam carving procedure proposed in [34] to the signal P with predefined dimensions p x q, the energy function ef of the seam carving algorithm is defined by (13):

$$ef(P) = |\frac{\partial}{\partial_x}P| + |\frac{\partial}{\partial_y}P|, \qquad (13)$$

The energy value of each pixel depends on the other eight neighbor pixels. Then the optimal seam is computed, employing (14):

$$S_{r,c}\{\begin{matrix} E_{0,j} & if\ r = 0 \\ E_{i,j} + \min(S_{r-1,c-1}, S_{r-1,c}, S_{r-1,c+1}) & otherwise \end{matrix}, \qquad (14)$$

where E is the energy map, S is the seam map and r and c indicate row and column position. In general terms, seam carving is an effective technique for adaptive resizing the images by gracefully carving-out or inserting pixels at different locations, removing or duplicating a "seam", which is composed by an optimal connected path of pixels having the lowest energy in an image from top to bottom for horizontal adjustment or left to right for vertical adjustment. This method is able to preserve the important content in an image as well as the global visual effect. In the sake of brevity, for interested readers, the details of seam carving procedure could be consulted in [34].

The "seams" in vertical and horizontal directions compose the secret key k_5 and could be renewed periodically to preserve the

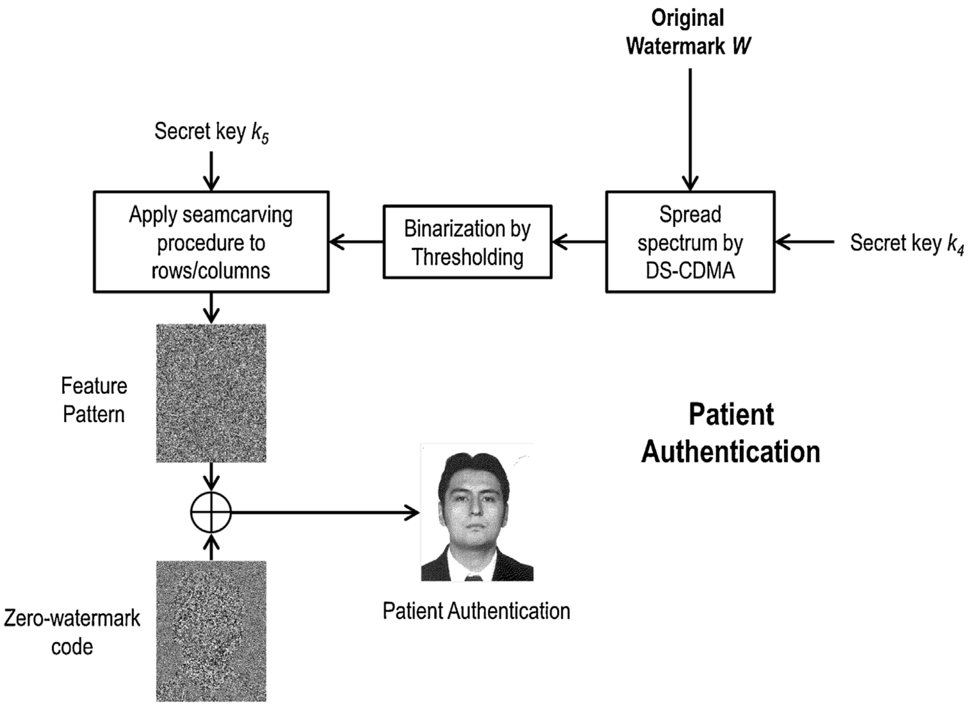


Fig. 7. Patient authentication procedure.

security of the *zero* watermarking method. In this way, the resized pattern *P* of size *p* x *q*, is denoted as F_P whose dimensions are now *n* x *m*. The security of F_P is dependable of a set of elements composed by the watermark data bits *W* as well as the secret keys k_4 and k_5.

Note that the seam carving procedure is adopted in our proposed method to increase the security of the 2D feature pattern *P* against malicious attacks that trying estimating it, desynchronizing it geometrically in vertical and horizontal orientations respectively.

Step 5- Finally, with the information of the feature pattern F_P and the halftone image I_H, using an or-exclusive operation, we obtain the code *zero* watermark *ZW*.

4.5. Zero-watermarking: patient authentication

Once the *zero* watermark code *ZW* is obtained and stored safely, the procedure to authenticate a patient, once confirmed the presence of *W* into watermarked medical image I_w, is shown in Fig. 7 and is described as follows.

Step 1- Supported by the watermark data bits *W* and the secret keys k_4 and k_5, obtain the feature pattern F_P whose procedure is described in the sub-section D of this Section 4.

Step 2- Finally, with the information of the feature pattern F_P and the code *zero* watermark *ZW*, using an or-exclusive operation we obtain the patient authentication in a visual manner.

5. Experimental results

This section presents the evaluation results of the proposed hybrid watermarking method applied to medical imaging, using a set of: a) 310 medical images in DICOM format modality CT (Computed Tomography) and different types: simple skull, larynx, brain and abdomen images, all of 512 × 512 in size and 12 bit-depth of grayscale resolution; b) 124 medical images in DICOM format modality RF (Radio-Fluoroscopy) and different types: esophagus, abdomen and urography images, all of 1024 × 1024 in size and 10 bit-depth of grayscale resolution. Fig. 8 shows a set of test images. A summary of the several parameters used in the proposed algorithm is shown in Table 2. The experimental results are carried out on a personal computer running Windows10© with an Intel© Core i7 processor (1.99 GHz) and 16GB RAM in which all procedures were implemented using MATLAB© R2017b. The performance of the proposed algorithm has been evaluated in terms of imperceptibility, security, and robustness. In the following sub-sections we explain the criteria to determine the proper value of the step-size of quantification Δ and its influence on the trade-off imperceptibility-robustness.

5.1. Invisible watermarking: setting of the step-size of quantification Δ

In this section, we show the configuration of the step-size of quantification, Δ, used by the QIM-DM in the proposed hybrid watermarking algorithm.

Considering the whole medical image datasets in DICOM format on modality CT and RF respectively, a variable step-size of quantification Δ from 10 to 100, an distortion composed by Gaussian noise with $\mu = 0$, $\sigma^2 = 0.0028$ for CT modality and $\mu = 0$, $\sigma^2 = 0.0022$ for RF modality, to determine the proper value of Δ, the robustness against Gaussian noise is measured employing BER metric and a decision threshold $T_d = 0.20$. In Fig. 9(a) and (b) shows an example of CT and RF images corrupted with Gaussian noise. In Fig. 9(c) and (d) we show the watermark robustness in terms of average BER varying Δ value from 10 to 100 for CT and RF modalities respectively.

Fig. 9(c) and (d) shows that Δ> = 40 to CT, Δ> = 80 to RF, could increase the robustness of the watermark *W* against common signal processing distortions obtaining BER smaller than the decision threshold $T_d = 0.20$, but the imperceptibility requirement decreases for large values of Δ. Hence, there is a trade-off between the robustness and imperceptibility, which we will discuss in the following section.

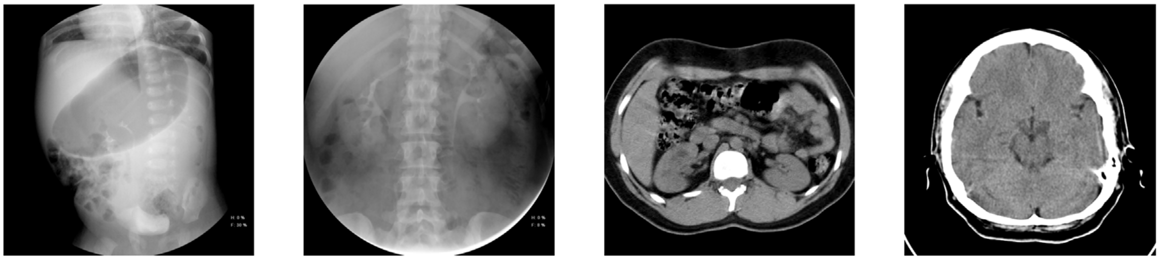
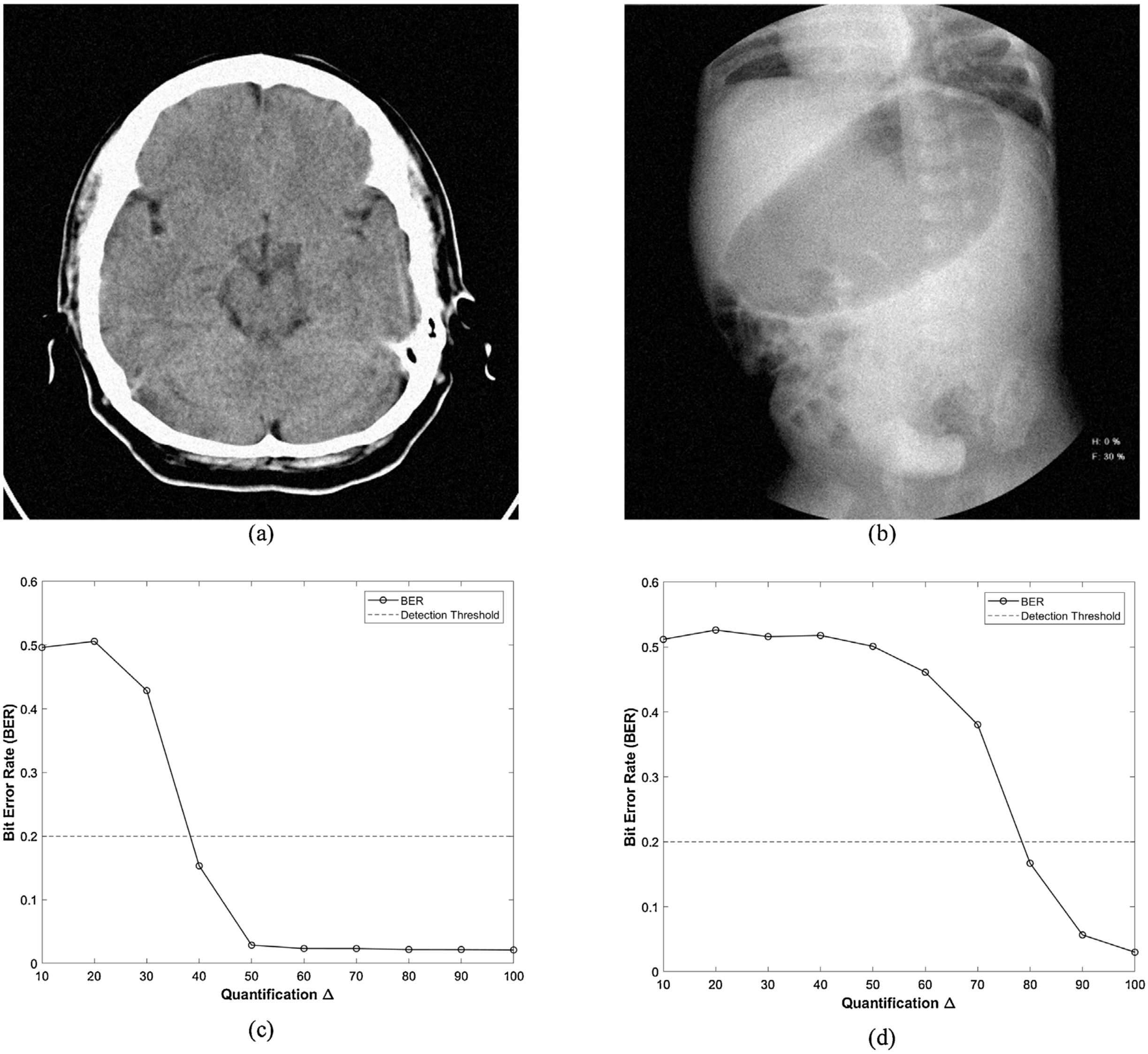


Fig. 8. Example of test images used in the experiments.

Table 2
Summary of the parameters used in the proposed method.

Parameter	Value
Secret key k_1 (N_1, N_2)	N_1, N_2 = 500 for CT images, N_1, N_2 = 1000 for RF images (can be renewed periodically)
Watermark W	160 bits when SHA-1 is applied to key information extracted from EPR data
Convolutional code	Code rate = 1/3. Constraint length K = 5. Free distance d_{free} = 12. Generator polynomials g_1 = [11111], g_2 = [11011], g_3 = [10101]
Secret key k_2, k_3	Defined by the content owner's
Step-size of quantification Δ	Δ = 40 for CT images, Δ = 80 for RF images
Decision threshold value T_d	T_d = 0.20
Dimensions n, m	Size of the patient's image n, m = 256
Secret key k_4 (p,q)	Defined by the content owner's
Secret key k_5	Seams in vertical and horizontal directions, defined by the content owner's (can be renewed periodically)



(a)

(b)

(c)

(d)

Fig. 9. Watermark robustness against Gaussian noise.

5.2. Invisible watermarking: watermark imperceptibility evaluation

As explained in the previous paragraphs, the proposed hybrid watermarking method applied to medical imaging embeds a ciphered-encoded watermark W in the frequency domain using QIM-DM modulation in the DCT domain. Therefore, a careful watermark imperceptibility evaluation is compulsory. Using a variable step-size of quantification Δ from 10 to 100, the watermark imperceptibility was evaluated in terms of the PSNR, SSIM [38] and VIF [39] image quality metrics defined by (15), (16) and (17), respectively.

$$PSNR(dB) = 10\log_{10}\left(\frac{Max\,Pixel\,Value^2}{\frac{1}{N\cdot M}\left(\sum_{x=1}^{N}\sum_{y=1}^{M}(I(x,y)-I_w(x,y))^2\right)}\right), \quad (15)$$

$$SSIM(I, I_w) = \frac{(2\mu_I\mu_{Iw}+C_1)(2\sigma_{I\,Iw}+C_2)}{(\mu_I^2+\mu_{Iw}^2+C_1)(\sigma_I^2+\sigma_{Iw}^2+C_2)}. \quad (16)$$

In (15) and (16) I and I_w are the original and the watermarked medical images respectively. In (16) C_1 and C_2 are small constant values [38]. The SSIM value reflects perceptual distortions more precisely than the PSNR value. The range of SSIM values is [0,1], and values closer to 1 represent better quality with respect to the original image. A value of 1 indicates that the original and the reference image are the same.

$$VIF = \frac{\sum\limits_{t\,\in\,channels} I(\vec{C}^{R,t};\vec{F}^{R,t}|s^{R,t})}{\sum\limits_{t\,\in\,channels} I(\vec{C}^{R,t};\vec{E}^{R,t}|s^{R,t})}. \quad (17)$$

As it is known in the literature [39], the VIF value reflects perceptual distortions more precisely than the PSNR metric. The range of VIF values is [0,1], and a closer value to 1 represents a better fidelity respect to the original image. Interested readers could refer to [39] to obtain more details about VIF metric. Fig. 10 shows the imperceptibility results to CT and RF datasets respectively, in terms of average values of PSNR, SSIM, and VIF respectively.

From Fig. 10(a)–(c) shows that the imperceptibility requirement decreases for large values of Δ in terms of PSNR, SSIM and VIF, however, large values of Δ increases the robustness of the watermark W against signal processing distortions. As mentioned in the above section, there is a trade-off between the robustness and imperceptibility. Fig. 11 shows the visual distortion using several values of Δ in CT and RF modalities. Fig. 11(a)–(c) corresponds to CT using values $\Delta = 40$, 80 and 120 respectively; meanwhile Fig. 11(d)–(f) corresponds to RF using values $\Delta = 80$, 100 and 150 values respectively. In Fig. 11 the regions marked in red shows the visual distortions caused by the increment of value of Δ.

Based in the robustness results obtained in the above section against Gaussian noise image corruption, which is considered an aggressive attack for *invisible* watermarking methods based on QIM-DM in DCT domain [32], and considering the behavior shown Fig. 10, we set $\Delta = 40$ for CT modality and $\Delta = 80$ for RF as the optimal values to obtain an equilibrium of the trade-off between the robustness and imperceptibility, obtaining BER smaller than the decision threshold $T_d = 0.20$ and PSNR > 100 dB, SSIM and VIF closer values to 1.

Table 3
Robustness the proposed method in terms of average BER for CT.

Distortions	Computed Tomography 12 bit/pixel Bit Error Rate
Non-watermarked	*0.5283*
Without distortion	0
Compression DICOM JPEG lossy	0.0047
Compression DICOM JPEG lossless	0
Compression DICOM JPEG2000 lossy	0.0055
Compression DICOM JPEG2000 lossless	0
Compression DICOM RLE	0
Impulsive noise density 0.008	0.1392
Impulsive noise density 0.005	0.0788
Gaussian noise $\mu = 0$, $\sigma^2 = 0.0018$	0.0503
Gaussian noise $\mu = 0$, $\sigma^2 = 0.0028$	0.1534
Speckle noise 0.007	0.1531
Gamma correction $\gamma = 1.1$	0.0680
Gamma correction $\gamma = 0.9$	0.1381
Gaussian filter 3 x 3	0.0284
Median filter 3 x 3	0.0955
Average filter 3 x 3	0.1942
Sharpening	0.1288
Brightness reduced	0.1574
Centered cropping 100 x 100	0.0590
Centered cropping 50 x 50	0.0110
Cropping 25%	0.0089
Cropping 45%	0.0449
Cropping 55%	0.1116
Rotation with auto-crop 15°	0.1041
Rotation with auto-crop 45°	0.1289
Rotation with auto-crop 135°	0.1289
Flipping up-down	0
Flipping right-left	0
Aspect ratio change [0.7,0,0;0,1.2,0;0,0,1]	0.1447
Scaling 0.5	0.1812
Scaling 2	0.0273
Scaling 3	0.0197

5.3. Invisible watermarking: watermark robustness testing

In this paper, the *invisible* watermarking is adopted for purposes of image source verification as well as to avoid the detachment between the medical images and its correspondent EPR. Thus, only few watermark data bits are needed to accomplish the above aims, preserving an equilibrium between the imperceptibility and robustness, in such a way that observers are unable of distinguishing the difference between the original and watermarked DICOM images by the naked eye. A mandatory requirement to *invisible* watermarking is that the hidden watermark signal W must be robust, i.e., must remain in the image after intentional or non-intentional distortions are performed. Considering the whole medical image datasets in DICOM format on modality CT and RF respectively, Tables 3 and 4 show the average detection results considering several geometric and signal processing distortions, using the metric BER to determine the presence or absence of the watermark W. Results in Tables 3 and 4 show the robustness provided by the several elements that compose the stage of *invisible* watermarking. In this way, the robustness against geometric attacks such as scaling and aspect ratio change is improved by the secret key k_1 (N_1, N_2), allowing rescale the image I_w to a predefined standard size. For your part, in order to confront aggressive distortions such as image cropping, the convolutional encoder has a key role because includes redundant bits which are used at the receiver to perform forward error correction to achieve a lower BER. Against image rotation, the watermark data bits are recovered by an exhaustive search from 0° to 360°. Moreover, the QIM-DM watermarking in DCT domain with $z = 1,2,3,4$, allows obtain an improved robustness against the above mentioned attacks as well as against signal processing distortions such as all DICOM compression modalities, image corruption

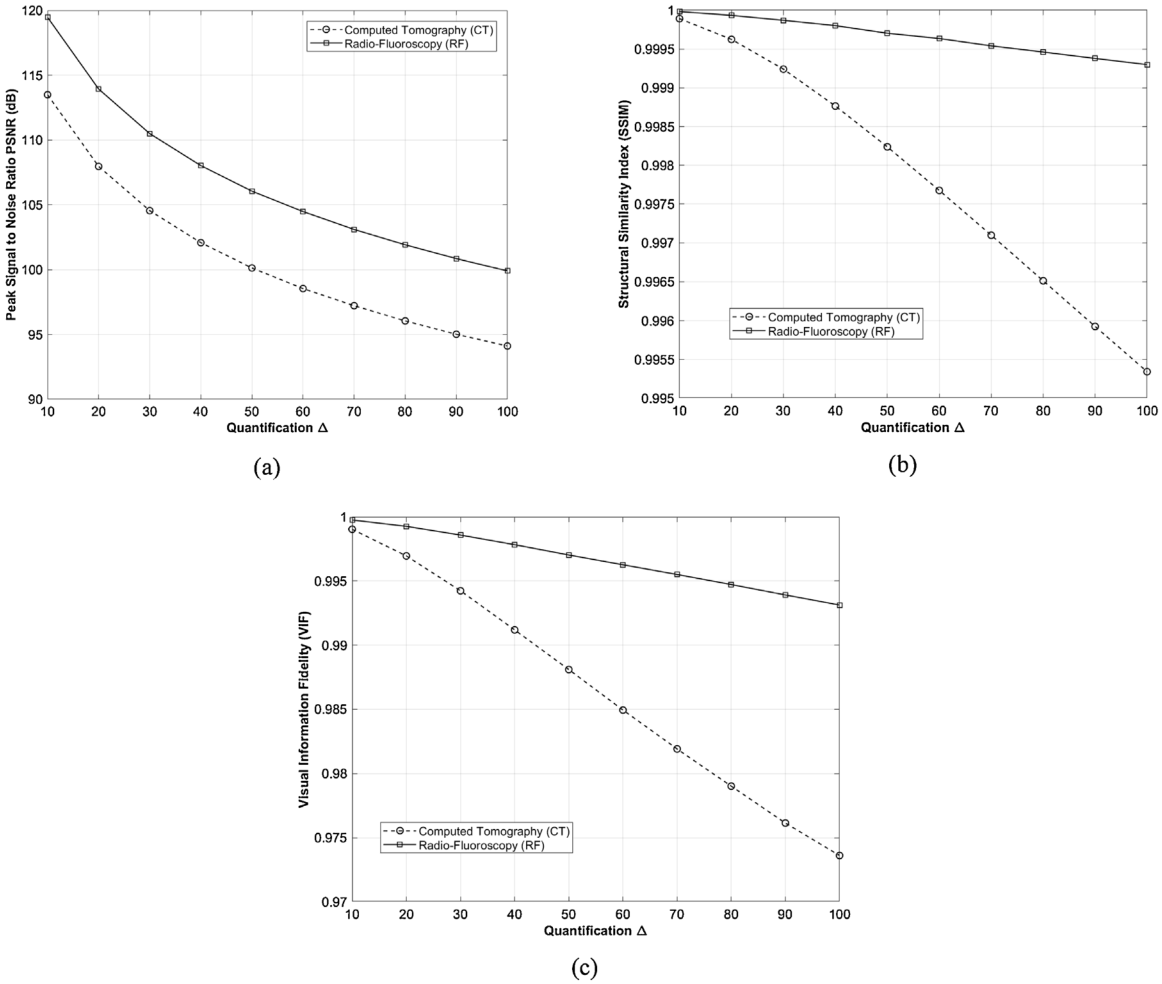


Fig. 10. Average PSNR, SSIM, and VIF for CT and RF imaging.

by Gaussian, speckle and impulsive noises, filtering, sharpening, brightness, gamma correction and flipping, obtaining in all cases BER smaller than the decision threshold $T_d = 0.20$.

5.4. Zero-watermarking: authentication reliability

As mentioned above, to increase the watermark payload and validates that the medical image belongs to proper patient, we propose a *zero* watermarking that accomplish with the aims of image source verification, validation that the medical image belongs to proper patient, avoiding any ambiguity and establishing a proper link between EPR, medical image, and patient. Therefore, a careful authentication reliability evaluation is compulsory. In all testing of this section, it is assumed that the watermark W has been detected, as shown in Fig. 1. Considering a variable set of pseudo-random sequences to spread spectrum DS-CDMA, and fixed values to the SHA-1 digest and secret key k_5, in Fig. 12 we show the average BER obtained on 10,000 trials where the trial number 5000 contains the DS-CDMA pseudo-random correct sequences obtaining BER = 0 confirming the patient authentication in all CT and RF datasets respectively.

From Fig. 12 we show that the security of the proposed *zero* watermarking algorithm is ensured since considering a watermark length of W equals to 160 given by SHA-1 and the fact that the seed to generate each pseudo-random sequence is in the range $[0, 2^{16}-1]$; then we have $C^{160}_{2^{16}-1}$ possible combinations to estimate the correct seeds employed by the DS-CDMA spread spectrum. Moreover, we need to consider that although an adversary will achieve estimate all DS-CDMA seeds, our *zero* watermarking proposed algorithm does not depend only on this parameter, and we need other two complementary security elements which are evaluated as follows. In this way, considering 10,000 different messages digests SHA-1 that causes 10,000 unique *zero* watermarking codes, and fixed values to DS-CDMA seeds and secret key k_5 respectively. In Fig. 13 we show the average BER obtained on 10,000 trials where the trial number 5000 contains the correct message digest SHA-1 obtaining BER = 0, again confirming the security and the patient authentication in a successful manner on all CT and RF datasets respectively. We would like to note that our proposed method may be easily adapted to the use of others algorithms that eventually could replace SHA-1, such as RIPEMD-160, Tiger, or WHIRLPOOL [26].

A third experiment contemplates fixed values to DS-CDMA seeds and SHA-1 message digest respectively, and variable values for the secret key k_5 composed by the seams in vertical and horizontal directions, defined by the content owner's, which can be renewed periodically in order to increase the security of the proposed *zero* watermarking method. In Fig. 14 we show the average BER obtained on 10,000 trials where the trial number 5000 contains the correct secret key k_5 obtaining BER = 0, again confirming the security and the patient authentication in a successful manner on all CT and RF datasets respectively. Note that the seam carving procedure is adopted in our proposed method to increase the security of the 2D feature pattern P into the zero-watermarking algorithm,

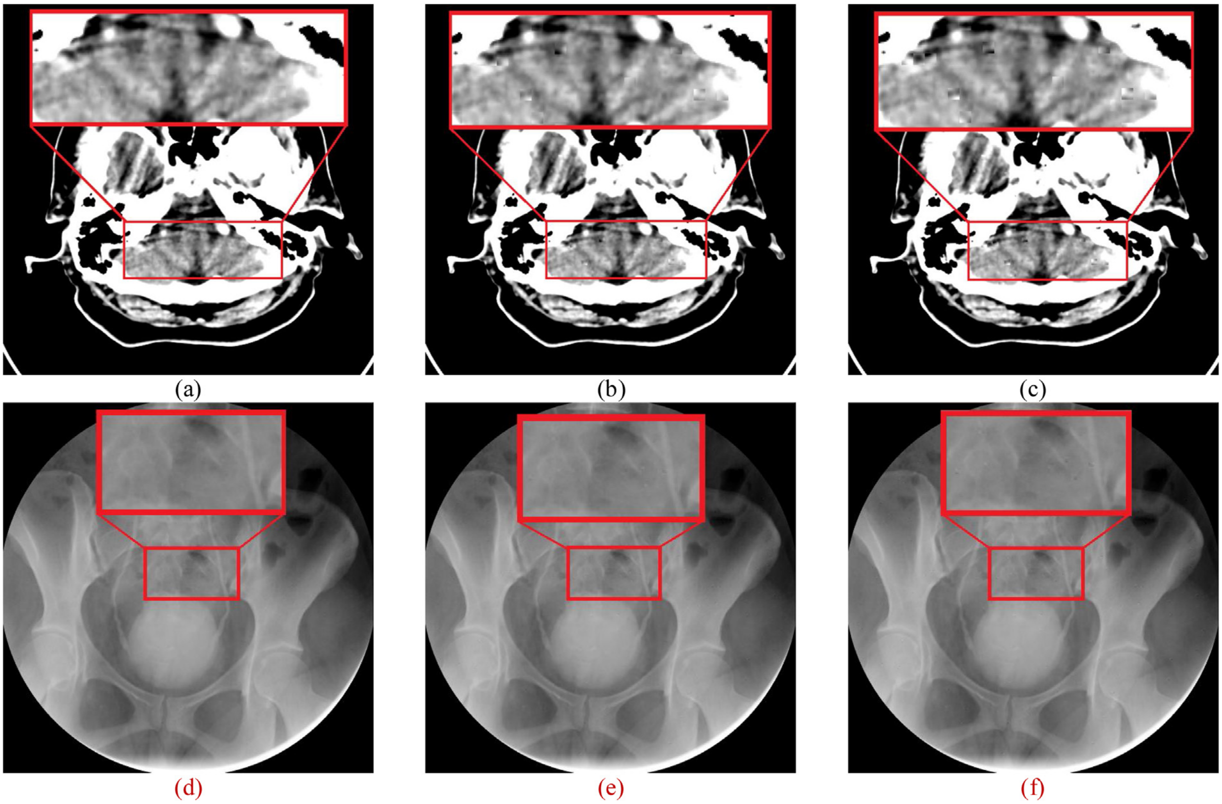


Fig. 11. Visual distortions caused by the increment of the value Δ.

Table 4
Robustness the proposed method in terms of average BER for RF.

Distortions	Radio fluoroscopy 10 bit/pixel Bit Error Rate
Non-watermarked	*0.5031*
Without distortion	0
Compression DICOM JPEG lossy	0
Compression DICOM JPEG lossless	0
Compression DICOM JPEG2000 lossy	0.0001
Compression DICOM JPEG2000 lossless	0
Compression DICOM RLE	0
Impulsive noise density 0.009	0.1748
Impulsive noise density 0.005	0.0596
Gaussian noise $\mu = 0, \sigma^2 = 0.001$	0.0044
Gaussian noise $\mu = 0, \sigma^2 = 0.0022$	0.1670
Speckle noise 0.005	0.1263
Gamma correction $\gamma = 1.25$	0.0507
Gamma correction $\gamma = 0.75$	0.1091
Gaussian filter 7 x 7	0.0023
Median filter 3 x 3	0.0023
Average filter 3 x 3	0.0034
Sharpening	0.0005
Brightness reduced	0.1510
Centered cropping 100 x 100	0.0051
Centered cropping 50 x 50	0.0024
Cropping 25%	0
Cropping 45%	0.0275
Cropping 55%	0.1508
Rotation with auto-crop 15°	0.0042
Rotation with auto-crop 45°	0.0143
Rotation with auto-crop 135°	0.0143
Flipping up-down	0
Flipping right-left	0
Aspect ratio change [0.7,0,0;0,1.2,0;0,0,1]	0.0016
Scaling 0.5	0.0295
Scaling 2	0.0019
Scaling 3	0.0008

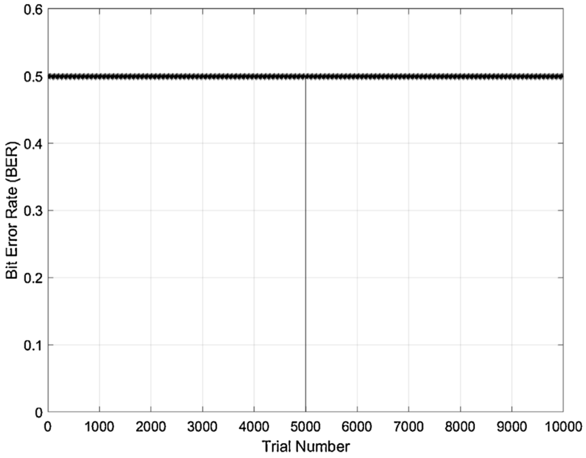


Fig. 12. Average BER with variable pseudo-random sequences to spread spectrum DS-CDMA.

against malicious attacks that trying estimating it, desynchronizing it geometrically in vertical and horizontal orientations respectively.

With illustrative purposes, Fig. 15 shows an example of the output of patient authentication stage in the *zero* watermarking algorithm, considering wrong and accurate values to DS-CDMA seeds, message digest SHA-1, and secret key k_5 respectively.

5.5. Performance comparison

In our best knowledge, until the write of this paper, we not found related works that consider a hybrid design as the proposed in this work, which is composed of *invisible* watermarking and *zero* watermarking techniques. In this way, we try carried out an equitable comparison performance relative to those most recent representa-

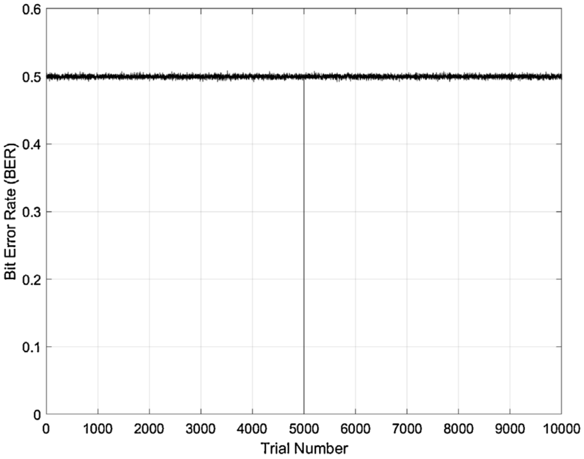


Fig. 13. Average BER with variable message digests SHA-1.

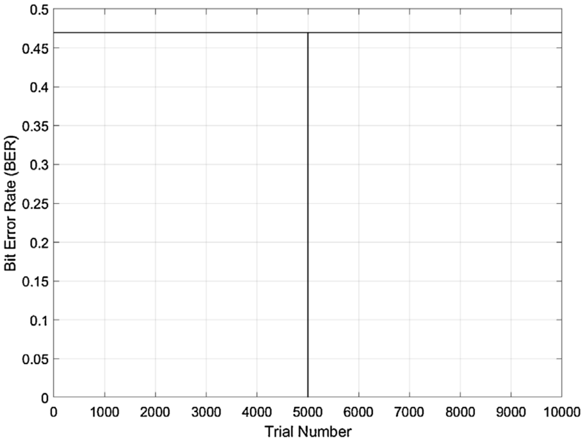


Fig. 14. Average BER with variable secret key k_5.

tive proposals [15–19,40–44] with similar purpose and application to our proposed method, which is shown in Table 5. A grid cell is marked with a dash, '-' for simulations or criterions not mentioned in the literature. To fair comparison, only relevant criteria were considered, because are the most essential in the design of a robust digital watermarking algorithm applied to medical images [1,5].

In the sake of brevity, the comparative is performed in terms of imperceptibility, payload and robustness, respectively.

In this way, from Table 5 we show that all proposals measure the visual quality of the watermarked images with PSNR metric, however some works such as [16,17] and [41] consider the SSIM index as an additional imperceptibility metric. Our proposed method measures the visual quality in a stricter manner employing PSNR, SSIM and VIF metrics. Considering a grayscale resolution of 8 bit/pixel, our proposed method obtains average PSNR = 59.05 dB, outperforming to all proposals in [15–19] and [40–44], moreover, if we consider the original resolution of 12 and 10 bit/pixel for CT and RF modalities, our proposed method obtains PSNR greater than 100 dB.

In terms of payload, our proposal outperforms to the methods reported in [16–19] and [40,42,44]; and is competitive with [15,41,43], because this employing a hybrid watermarking algorithm composed by a couple of *invisible* watermarking and *zero* watermarking complementary methods that ensure a payload of at least 66,088 bits, amount that could be adjusted in increasing or decreasing manner according to the size of the patient image, preserving the high visual quality of the medical image.

In terms of watermark robustness, from Table 5 we show that to measure this requirement, the watermarking methods employ either BER or NC or both. Against image compression, in Table 4 we show that only the method in [16] and our proposed method are robust against all DICOM compression modes: JPEG and JPEG2000 lossy and lossless respectively, as well as against DICOM RLE. The rest of the proposals [15,17,18,40–44] only consider the JPEG lossy compression except the work in [19] that not reports robustness against any image compression algorithm. Against image noise, our and all proposals, except the reported work in [43], are competitive because consider the three most popular noises which are Gaussian, impulsive (salt&pepper) and speckle; tolerances for our proposal were reported in Tables 3 and 4. Against geometric attacks, our proposal considers a wide range of distortions such as rotation by several angles, scaling, global and centered cropping, aspect ratio change and vertical/horizontal flipping. Thus, our method outperforms to all algorithms in Table 5, which consider only a few geometric distortions [15,17–19,41–44] or well none [16,40].

According to the performance analysis, there is an aspect that is necessary to specify, which refers to the hybrid design of the proposed method in this paper. In this way, not to depend on an inherent image feature extractor and the same time conceal an invisible and non-removable watermark on the medical image content, the literature relative to *zero* watermarking is excluded in the performance analysis. To fair comparison, we only consider digital watermarking algorithms reported previously into the scientific literature that accomplishes the following properties: a) same or similar purpose/application that the proposed in the present work, b) keep an invisible and non-removable watermark into the medical image content.

As mentioned in Table 1, a problematic found in the *zero* watermarking algorithms is the ambiguity at the moment of its application on a medical image. The effectivity of these algorithms strongly depends on an inherent feature extraction to the image content that not necessary is related to the clinical data

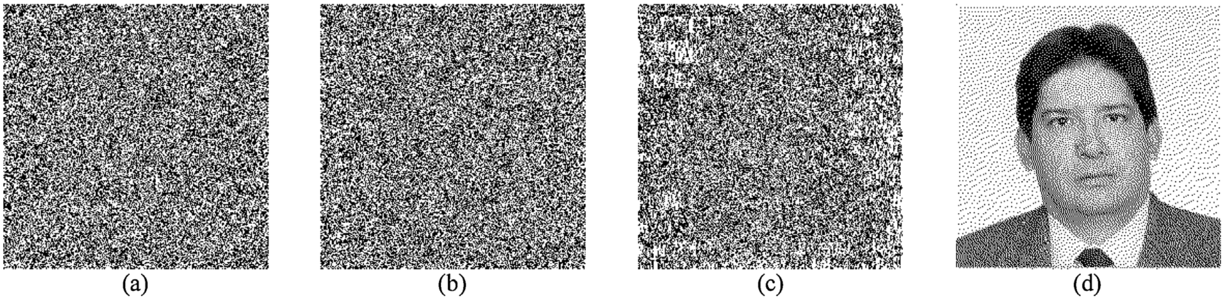


Fig. 15. (a) Wrong value to DS-CDMA seeds, accurate values of SHA-1 message digest and secret key k_5, (b) Wrong SHA-1 message digest, accurate values of DS-CDMA seeds and secret key k_5, (c) Wrong secret key k_5, accurate values of DS-CDMA seeds and SHA-1 message digest, (d) Accurate values of DS-CDMA seed, SHA-1 message digest and secret key k_5.

Table 5
Performance comparison.

Comparison	Image Compression	Watermark Payload (bits)	Imperceptibility Metric	Detection Metric	Application	Average PSNR (dB)	Geometric Attacks	Types of Noises
Method								
[15]	JPEG lossy	65,800	PSNR	NC BER	- Authentication - Confidentiality and Security	36.88	Rotation Cropping	Gaussian Salt & Pepper Speckle
[16]	All DICOM compression modes	808	PSNR SSIM	BER	- Authentication	46.11	–	Salt & Pepper
[17]	JPEG lossy	2,046	PSNR WPSNR SSIM	NC BER	- Authentication	46.00	Scaling Cropping	Gaussian Salt & Pepper
[18]	JPEG lossy	22,490	PSNR	NC BER	- Authentication	56.23	Scaling Rotation Cropping	Gaussian Salt & Pepper
[19]	–	4,096	PSNR	NC	- Authentication	45.22	Rotation Scaling	Gaussian Salt & Pepper Speckle
[40]	JPEG lossy	450	PSNR	NC	- Authentication	43.99	–	Gaussian Salt & Pepper Poisson
[41]	JPEG lossy	65,536	PSNR SSIM	NC	- Authentication -Annotation	35.52	Rotation Scaling Cropping	Gaussian Salt & Pepper
[42]	JPEG lossy	4096	PSNR	NC	- Authentication	42.95	Cropping	Gaussian Salt & Pepper Speckle
[43]	JPEG lossy	262,144	PSNR	NC	- Authentication	47.75	Rotation Scaling	–
[44]	JPEG lossy	4,176	PSNR	NC BER	- Authentication - Confidentiality	36.01	Rotation Scaling	Gaussian Salt & Pepper Speckle
Proposed Method	All DICOM compression modes	$(n\cdot m)+W_{enc}$ = $(256\cdot 256)$ + 552 = 66,088	PSNR SSIM VIF	BER	- Authentication -Avoid detachment	(8bit-depth) = 59.05 (12 and 10 bit-depth) = 102.00	Rotation Scaling Cropping Aspect Ratio Flip	Gaussian Salt & Pepper Speckle

and patient identity, causing that any *zero* watermarking methods are in conditions of claim the medical image under analysis as its property. On the other hand, the *invisible* watermarking proposals reported in Table 5 have the drawback of the tradeoff between imperceptibility-payload, because if the watermark size is increased the robustness could improve, but the visual quality of the medical image is severely affected. In the medical context, the watermark imperceptibility is very strict and should be preserved as best as possible. In the proposed method, the watermark *W* is generated using clinical data from EPR, which replaces the inherent feature extraction used by the conventional *zero* watermarking, allowing a proper link between clinical data, medical image and patient identity, whose effectiveness depend mainly of the robustness of the watermark *W* against intentional and not intentional distortions applied to the medical image.

The comparison shown in Table 5 reveals that almost all algorithms reported in the literature [15,17,18,40–44] are designed to operate only on DICOM images with 8 bits/pixel bit-depth grayscale resolution, meanwhile [16] works on 16 bits/pixel and [19] is versatile in the handling of bit-depth grayscale resolution. Design medical image watermarking algorithms for operating on fix grayscale resolution may be inconvenient in practical scenarios because usually the DICOM modalities handling several bit-depth grayscale resolutions commonly between 8, 10, 12 and 16 bits respectively. Our proposal, in the same way, that [19], has the versatility to operate with several bit depths.

Another important aspect is the watermark robustness against lossy and lossless image compression algorithms, in this context, almost all related works [15,17,18,40–44] orient their efforts to increase the robustness against JPEG lossy compression algorithm, others not include the image compression in their set of robustness testing [19] and only the related work in [16] consider all DICOM compression modes in their experiment. Again, design medical image watermarking algorithms robust only against JPEG lossy may be inconvenient in practical scenarios, where the DICOM viewer's tools have in their repertory image compression algorithms such as lossy and lossless JPEG2000. Our proposal, in the same way, that [16], considers in its design the robustness against all DICOM image compression modes.

Finally, the application of our proposed method accomplishes with the aims of image source verification, validation that the medical image belongs to proper patient, avoiding any ambiguity and establishing a proper link between EPR, medical image, and patient.

6. Conclusions

Due to its relevance in clinical diagnosis, treatment, research and other commercial and non-commercial applications of public and private organizations; medical information is highly valuable and delicate by nature. Digital watermarking has the potential to be a value-added tool to confront several information security issues associated with medical imaging management. This paper proposes a hybrid watermarking algorithm composed by a couple of *invisible* watermarking and *zero* watermarking complementary methods, applied to DICOM images in RF and CT modalities. This strategy accomplishes with the aims of image source verification, validation that the medical image belongs to proper patient, avoiding any ambiguity and establishing a proper link between EPR, medical image, and patient. Moreover, this paper solves a critical issue that happens when a medical image is analyzed by two or more *zero* watermarking algorithms, since this fact will causes a serious controversy and ambiguity at the moment of authentication, because each *zero* watermarking algorithm is in equal conditions of employ its *zero* watermark code and extract its inherent features from the same image, as consequence all *zero* watermarking algorithms that analyzing the same image could claim as their property. In a medical image context, this fact could carry several and serious authentication issues. Experimental results show that the proposed *zero* watermarking is reliable and secure. On the other hand, the component of *invisible* watermarking shows high robustness against all DICOM image compression modes, filtering, image noise, image enhancement as well as geometric distortions. The visual quality of the DICOM images was preserved obtaining PSNR values greater than 100 dB and evaluated in a stricter manner employing other metrics based on the human visual system such as SSIM and VIF, obtaining for both values nearest to 1. The comparative with the current state of the art reveals a better performance of the proposed work in terms of imperceptibility, robustness, and payload. As future work, we consider extending the application to other DICOM imaging modalities such as X-ray, resonance magnetic, ultrasound, among others.

Acknowledgments

Authors thank the Instituto Politecnico Nacional (IPN) as well as the Consejo Nacional de Ciencia y Tecnologia de Mexico (CONACYT) by the support provided during the realization of this research.

Declaration of Competing Interest

The authors declare that there are no conflicts of interest.

References

[1] G. Coatrieux, H. Maître, B. Sankur, Y. Rolland, R. Collorec, Relevance of watermarking in medical imaging, IEEE-embs information technology applications in, Biomedicine (2000) 250–255, http://dx.doi.org/10.1109/ITAB.2000.892396.

[2] G. Coatrieux, C. Quantin, J. Montagner, M. Fassa, F.A. Allaert, Ch. Roux, Watermarking Medical Images With Anonymous Patient Identification to Verify Authenticity in Studies in Health Technology and Informatics, vol. 136, IOS Press, 2008, pp. 667–672.

[3] S. Kaihara, Realization of the computerized patient record; relevance and unsolved problems, Int. J. Med. Inform. 1 (49) (1998) 1–8.

[4] E.L. Siegel, R.M. Kolodner, Filmless Radiology, Springer, New York, 1999.

[5] H. Nyeem, W. Boles, C. Boyd, A review of medical image watermarking requirements for teleradiology, J. Digit. Imaging 26 (2) (2013) 326–343, http://dx.doi.org/10.1007/s10278-012-9527-x.

[6] A.F. Qasim, F. Meziane, Rob Aspin, Digital watermarking: applicability for developing trust in medical imaging workflows state of the art review, Comput. Sci. Rev. 27 (2018) 45–60, http://dx.doi.org/10.1016/j.cosrev.2017.11.003.

[7] S.M. Mousavi, A. Naghsh, S.A.R. Abu-Bakar, Watermarking techniques used in medical images: a survey, J. Digit. Imaging 27 (2014) 714–729, http://dx.doi.org/10.1007/s10278-014-9700-5.

[8] S. Das, M.K. Kundu, Effective management of medical information through a novel blind watermarking technique, J. Med. Syst. 36 (2012) 3339–3351, http://dx.doi.org/10.1007/s10916-012-9827-1.

[9] M. Barni, F. Bartolini, Applications, in: Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications, CRC Press, Boca Raton, 2004, pp. 23–44, http://dx.doi.org/10.1201/9780203913512.

[10] P. Bas, T. Furon, F. Cayre, G. Doërr, B. Mathon, A quick tour of watermarking techniques, in: Watermarking Security Fundamentals, Secure Design and Attacks, Springer Briefs in Electrical and Computer Engineering, Springer, Singapore, 2016, pp. 13–31, http://dx.doi.org/10.1007/978-981-10-0506-0.

[11] M. Barni, I. Cox, T. Kalker, H.J. Kim, Digital Watermarking, 2005, http://dx.doi.org/10.1007/11551492.

[12] I. Cox, M. Miller, J. Bloom, Applications and properties, in: Digital Watermarking, Morgan Kaufmann Publishers, USA, 2002, pp. 11–39 https://www.elsevier.com/books/digital-watermarking/cox/978-1-55860-714-9.

[13] DICOM Standard, 2019, https://www.dicomstandard.org/. (Accessed June 2019).

[14] A.K. Singh, M. Dave, A. Mohan, Hybrid technique for robust and imperceptible multiple watermarking using medical images, Multimed. Tools Appl. 75 (2016) 8381–8401, http://dx.doi.org/10.1007/s11042-015-2754-7.

[15] A. Sharma, A.K. Singh, S.P. Ghrera, Robust and secure multiple watermarking for medical images, Wireless Pers. Commun. 92 (2017) 1611–1624, http://dx.doi.org/10.1007/s11277-016-3625-x.

[16] S.M. Mousavi, A. Naghsh, A.A. Manaf, S.A.R. Abu-Bakar, A robust medical image watermarking against salt and pepper noise for brain MRI images, Multimed. Tools Appl. 76 (2017) 10313–10342, http://dx.doi.org/10.1007/s11042-016-3622-9.

[17] F.N. Thakkar, V.K. Srivastava, A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications, Multimed. Tools Appl. 76 (2017) 3669–3697, http://dx.doi.org/10.1007/s11042-016-3928-7.

[18] K. Swaraja, Medical image region based watermarking for secured telemedicine, Multimed. Tools Appl. 77 (21) (2018) 28249–28280, http://dx.doi.org/10.1007/s11042-018-6020-7.

[19] Y. Gangadhar, V.S. Giridhar Akula, P. Chenna Reddy, An evolutionary programming approach for securing medical images using watermarking scheme in invariant discrete wavelet transformation, Biomed. Signal Process. Control 43 (2018) 31–40, http://dx.doi.org/10.1016/j.bspc.2018.02.007.

[20] M. Cedillo-Hernandez, F. Garcia-Ugalde, M. Nakano-Miyatake, H. Perez-Meana, Robust watermarking method in DFT domain for effective management of medical imaging, SIViP 9 (2015) 1163–1178, http://dx.doi.org/10.1007/s11760-013-0555-x.

[21] K. Kalaivani, An efficient watermarking scheme for medical data security with the aid of neural network, Braz. Arch. Biol. Technol. 59 (spe2) (2016), e16161070, http://dx.doi.org/10.1590/1678-4324-2016161070, 1–12.

[22] N. Aherrahrou, H. Tairi, PDE based scheme for multi-modal medical image watermarking, Biomed. Eng. Online 14 (108) (2015) 1–19, http://dx.doi.org/10.1186/s12938-015-0101-x.

[23] M. Cedillo-Hernandez, A. Cedillo-Hernandez, F. Garcia-Ugalde, M. Nakano-Miyatake, H. Perez-Meana, Security enhancement of medical imaging via imperceptible and robust watermarking, IEICE Trans. Inf. Syst. E98-D (9) (2015) 1702–1705, http://dx.doi.org/10.1587/transinf.2015EDL8016.

[24] R. Rodriguez-Colin, C. Feregrino-Uribe, J.A. Martinez-Villanueva, Robust watermarking scheme applied to radiological medical images, IEICE Trans. Inf. Syst. E91-D (3) (2008) 862–3864, http://dx.doi.org/10.1093/ietisy/e91-d.3.862.

[25] A. Sharma, A.K. Singh, S.P. Ghrera, Secure hybrid robust watermarking technique for medical images, Procedia Comput. Sci. 70 (2015) 778–784, http://dx.doi.org/10.1016/j.procs.2015.10.117.

[26] C. Paar, J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, Springer-Verlag, Berlin Heidelberg, 2010, http://dx.doi.org/10.1007/978-3-642-04101-3.

[27] L. Yuling, Q. Xinxin, X. Guojiangn, A ROI-based reversible data hiding scheme in encrypted medical images, J. Vis. Commun. Image Represent. 39 (2016) 51–57, http://dx.doi.org/10.1016/j.jvcir.2016.05.008.

[28] W. Chunpeng, W. Xingyuan, X. Zhiqiu, Z. Chuan, Ternary radial harmonic Fourier moments based robust stereo image zero-watermarking algorithm, Inf. Sci. 470 (2019) 109–120, http://dx.doi.org/10.1016/j.ins.2018.08.028.

[29] X. Zhiqiu, W. Xingyuan, Z. Wenjie, L. Rui, W. Chunpeng, Z. Chuan, Color medical image lossless watermarking using chaotic system and accurate quaternion polar harmonic transforms, Signal Process. 157 (2019) 108–118, http://dx.doi.org/10.1016/j.sigpro.2018.11.011.

[30] J. Liu, J. Li, J. Ma, N. Sadiq, U.A. Bhatti, Y. Ai, A robust multi-watermarking algorithm for medical images based on DTCWT-DCT and Henon Map, Appl. Sci. 9 (4) (2019) 700, http://dx.doi.org/10.3390/app9040700.

[31] B. Sklar, Digital Communications: Fundamentals and Applications, second edition, System View, 2001.

[32] B. Chen, G.W. Wornell, Quantization index modulation: a class of provably good method for watermarking and information embedding, IEEE Trans. Inf. Theor. 47 (4) (2001) 1423–1443, http://dx.doi.org/10.1109/18.923725.

[33] M. Cedillo-Hernandez, A. Cedillo-Hernandez, F. Garcia-Ugalde, M. Nakano-Miyatake, H. Perez-Meana, Digital color images ownership authentication via efficient and robust watermarking in a hybrid domain, Radioeng. J. 26 (2) (2017) 536–551, http://dx.doi.org/10.13164/re.2017.0536.

[34] M. Hashemzadeh, B. Asheghi, N. Farajzadeh, Content-aware image resizing: an improved and shadow-preserving seam carving method, Signal Process. 155 (2019) 233–246, http://dx.doi.org/10.1016/j.sigpro.2018.09.037.

[35] M. Mese, P. Vaidyanathan, Recent advances in digital halftoning and inverse halftoning methods, IEEE Trans. Circuits Syst. I 49 (6) (2002) 790–805, http://dx.doi.org/10.1109/TCSI.2002.1010034.

[36] B.H. Batson, R.W. Moorehead, Simulation Results for the Viterbi Decoding Algorithm. NASA-TR-R-396, Technical Report, 1972.

[37] C.W. Tang, H.M. Hang, A feature-based robust digital image watermarking scheme, IEEE Trans. Signal Process. 51 (4) (2003) 950–959, http://dx.doi.org/10.1109/TSP.2003.809367.

[38] Z. Wang, A.C. Bovik, H.R. Sheikh, E.P. Simoncelli, Image quality assessment: from error visibility to structural similarity, IEEE Trans. Image Process. 13 (4) (2004) 600–612, http://dx.doi.org/10.1109/TIP.2003.819861.

[39] H.R. Sheikh, A.C. Bovik, Image information and visual quality, IEEE Trans. Image Process. 15 (2) (2006) 430–444, http://dx.doi.org/10.1109/TIP.2005.859378.

[40] D.S. Chauhan, A.K. Singh, A. Adarsh, B. Kumar, J.P. Saini, Combining Mexican hat wavelet and spread spectrum for adaptive watermarking and its statistical detection using medical images, Multimed. Tools Appl. 78 (10) (2019) 12647–12661, http://dx.doi.org/10.1007/s11042-017-5348-8.

[41] S. Thakur, A. Kumar Singh, S. Prakash Ghrera, M. Elhoseny, Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications, Multimed. Tools Appl. 78 (3) (2019) 3457–3470, http://dx.doi.org/10.1007/s11042-018-6263-3.

[42] K.S. Surekah Borra, C.U. Rohit Thanki, A FRT-SVD based blind medical watermarking technique for telemedicine applications, Int. J. Digit. Crime Forensics 11 (2) (2019) 13–33, http://dx.doi.org/10.4018/IJDCF.2019040102.

[43] I. Assini, A. Badri, K. Safi, A. Sahel, A. Baghdad, Robust watermarking for medical image against geometric and compression attacks, in: F. Khoukhi, M. Bahaj, M. Ezziyyani (Eds.), Smart Data and Computational Intelligence. AIT2S 2018. Lecture Notes in Networks and Systems, vol. 66, 2019, pp. 97–103, http://dx.doi.org/10.1007/978-3-030-11914-0_10.

[44] A.K. Singh, Robust and distortion control dual watermarking in LWT domain using DCT and error correction code for color medical image, Multimed. Tools Appl. (2019) 1–11, http://dx.doi.org/10.1007/s11042-018-7115-x (in press).

[45] X. Wu, J. Li, R. Tu, J. Cheng, U. Aslam Bhatti, J. Ma, Contourlet-DCT based multiple robust watermarkings for medical images, Multimed. Tools Appl. 78 (7) (2019) 8463–8480, http://dx.doi.org/10.1007/s11042-018-6877-5.

[46] Z. Ali, M. Imran, S. McClean, N. Khan, M. Shoaib, Protection of records and data authentication based on secret shares and watermarking, Future Gener. Comput. Syst. 98 (2019) 331–341, http://dx.doi.org/10.1016/j.future.2019.01.050.

[47] T.-Y. Fan, H.-C. Chao, B.-C. Chieu, Lossless medical image watermarking method based on significant difference of cellular automata transform coefficient, Signal Process. Image Commun. 70 (2019) 174–183, http://dx.doi.org/10.1016/j.image.2018.09.015.

[48] R. Bamal, S.S. Kasana, Dual hybrid medical watermarking using walsh-slantlet transform, Multimed. Tools Appl. 78 (13) (2019) 17899–17927, http://dx.doi.org/10.1007/s11042-018-6820-9.