IEICE TRANS. INF. & SYST., VOL.E98–D, NO.9 SEPTEMBER 2015

LETTER

Security Enhancement of Medical Imaging via Imperceptible and Robust Watermarking

Manuel CEDILLO HERNANDEZ[†a)], **Antonio CEDILLO HERNANDEZ**[†], **Francisco GARCIA UGALDE**[†], **Mariko NAKANO MIYATAKE**[††], ***Nonmembers***, ***and*** **Hector PEREZ MEANA**[††], ***Member***

SUMMARY In this letter we present an imperceptible and robust watermarking algorithm that uses a cryptographic hash function in the authentication application of digital medical imaging. In the proposed scheme we combine discrete Fourier transform (DFT) and local image masking to detect the watermark after a geometrical distortion and improve its imperceptibility. The image quality is measured by metrics currently used in digital image processing, such as VSNR, SSIM and PSNR.

key words: *digital watermarking, medical imaging, authentication*

1. Introduction

An interesting scheme recently emerged to enhance the security, confidentiality and integrity of digital medical images consisting of the use of digital watermarking in conjunction with cryptographic algorithms [1]. This solution allows the user to verify that the medical images belong to the correct patient and comes from a dependable information source which is an important property of a picture archiving and communication system (PACS) used in healthcare. Medical imaging requires extreme care when it is processed by a watermarking algorithm [2], because the additional information of the watermark may affect the image content and as a consequence it may lead to an erroneous clinical diagnostics. Nowadays, medical imaging infrastructure produces images in digital format through DICOM format (2003 standard for digital imaging and communications in medicine), which is a standard that allows the manipulation, transmission and storage of them [1]. Given the advances in information technologies as well as in security requirements, in order to avoid the undesirable but probable detachment of the image and their electronic patient record [3], we propose the use of a cryptographic hash of the DICOM metadata as the watermark to be embed into the medical images.

This letter proposes an imperceptible and robust watermarking algorithm that improves the scheme proposed in [8] as follows: a) the watermark imperceptibility has been improved without affect the robustness, replacing the integrated optical density concept implemented in [8] by a spatial masking which is described later. b) The new method has been designed to protect medical images against the practical signal processing offered in the tools included on DICOM CD Viewer display interface. Evaluation results provided show the desirable features of the proposed scheme.

Manuscript received January 19, 2015.
Manuscript revised May 14, 2015.
Manuscript publicized May 28, 2015.

[†]The authors are with the Universidad Nacional Autónoma de México (UNAM), Circuito Exterior, Ciudad Universitaria, Coyoacán, 04510 Mexico City, México.
[††]The authors are with the Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhucan, Instituto Politécnico Nacional (IPN), Av. Santa Ana 1000, San Francisco Culhuacan, Coyoacán, 04430 Mexico City, México.
a) E-mail: mcedillohdz@hotmail.com

DOI: 10.1587/transinf.2015EDL8016

2. Proposed Method

The proposed method gives the imperceptible and robust watermarking and is explained in the following steps: *Watermark generation stage*: **1)** Read the DICOM file, extracts the desirable key information from the metadata, e.g., patient name, age, etc., and apply the message digest algorithm RIPEMD-160 [4] to obtain a hash. **2)** Split the binary representation of the cryptographic hash into two parts of the same length (80 bits) and applies an XOR operation between them; obtaining then a watermark pattern W of length $L = 80$ bits that is directly dependent on the DICOM metadata. *Watermark embedding stage*: **1)** Read the original DICOM image $I(x, y)$ in a 8-bit grayscale intensity representation and rescale it into a size of $N_1 \times N_2$, these dimensions will be stored and provided as a secret key K_1 in the extraction stage. **2)** Apply the 2D DFT denoted as $F(u, v)$ to the resized image $I_r(x, y)$ and obtain its magnitude $M(u, v) = |F(u, v)|$ and phase $\mathrm{P}(u, v)$. **3)** Once that Fourier spectrum has been centered, based on the energy distribution in the DFT domain, select a pair of radius r_1 and r_2 around the zero frequency term in $M(u, v)$ and compute its corresponding annular area $A = \pi({r_2}^2 - {r_1}^2)$ that should cover the middle frequency components. Reasons of positioning r_1 and r_2 in the middle frequencies are: a) modifications in the low frequencies of $M(u, v)$ will cause a visible distortion in the spatial domain of the host image, b) modifications in the high frequencies of $M(u, v)$ may affect considerably the robustness against JPEG compression. In order to preserve the robustness respect to JPEG and at the same time keep a high visual quality, the goal then is to find a correct pair of r_1 and r_2. Fortunately there are enough radiuses in the middle frequency of $M(u, v)$ that may satisfy the trade-off between robustness and imperceptibility. These radius values will be stored and provided as a secret key K_2 in the extraction stage. **4)** According to DFT symmetrical properties, consider the 1st and 2nd quadrants of the upper half part

if $(W_i = 0)$ *and* $(d < -\alpha)$ *then*
  None Modification
end
if $(W_i = 0)$ *and* $(d \geq -\alpha)$ *then*
  $M_i'(u_j, v_j) = M_i(u_j, v_j) - (\alpha + d)$
  $M_i'(-u_j, v_j) = M_i(-u_j, v_j) + (\alpha + d)$
end

if $(W_i = 1)$ *and* $(d > \alpha)$ *then*
  None Modification
end
if $(W_i = 1)$ *and* $(d \leq \alpha)$ *then*
  $M_i'(u_j, v_j) = M_i(u_j, v_j) + (\alpha - d)$
  $M_i'(-u_j, v_j) = M_i(-u_j, v_j) - (\alpha - d)$
end

Fig. 1 Pseudo-code of the embedding rules.

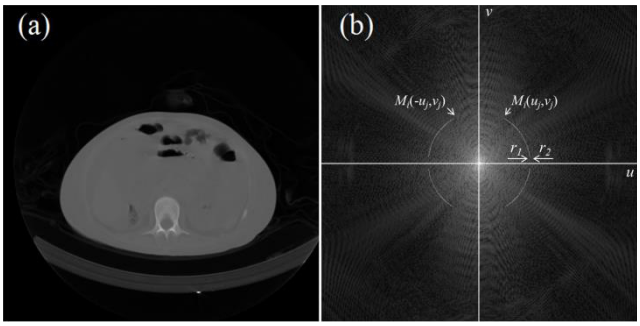

Fig. 2 Modification of DFT magnitude coefficients. a) Original abdomen image. b) Watermarked DFT magnitude of a). A bigger value of the watermark strength α is used with illustrative purposes.

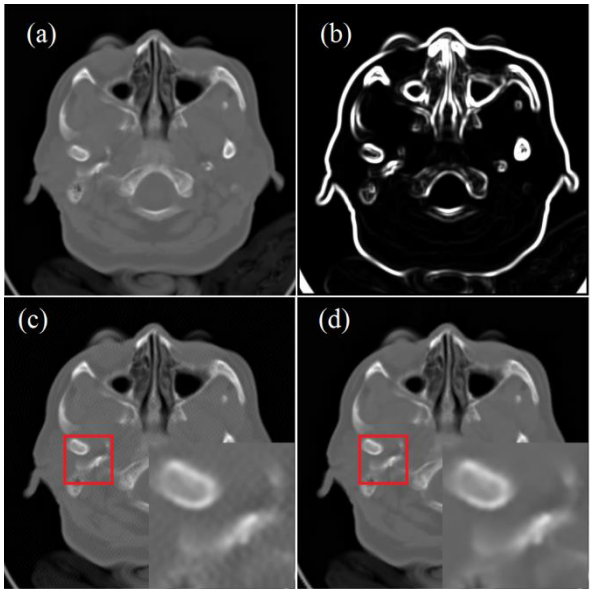

Fig. 3 (a) Original image. (b) Masking image M_σ. (c) Watermarked version without masking. (d) Watermarked version with masking. Zoomed regions from red squares are displayed on lower right corner of (c) and (d) in order to show with more details the masking effect.

of $M(u, v)$, into the area A compute the magnitude difference $d = M_i(u_j, v_j) - M_i(-u_j, v_j)$, where $i = 1, \ldots, L$ denotes an index pointing into the watermark data bits W_i, and j denotes the coordinates into $M(u, v)$. **5)** Considering a watermark strength factor α, modify the DFT middle frequencies magnitudes $M'(u, v)$ as is shown Figs. 1 and 2.

6) In order to produce real values after the DFT magnitude has been modified in **5)**, the lower half part of the corresponding middle frequency band should be modified as well in a symmetrical manner. The watermarked image $I_W(x, y)$ is obtained applying the inverse DFT to the watermarked magnitude $M'(u, v)$ in conjunction with the corresponding non changed original phase $P(u, v)$. Finally the watermarked image $I_W(x, y)$ is rescaled to its original dimensions. Note that, in order to increase the security of the watermarking algorithm, secret keys K_1, K_2, may be renewed randomly in a desirable lapse of time. In this manner, several lots of medical images may be watermarked using different secret keys K_1 and K_2, thus avoiding the estimation of both secret keys by an adversary. In this paper K_1 is given by $N_1 = N_2 = 400$, meanwhile K_2 by $r_1 = 72$ and $r_2 = 74$, however, e.g., a new lot of images could be watermarked by renewed secret keys K_1 ($N_1 = N_2 = 412$) and K_2 ($r_1 = 73$ and $r_2 = 75$), which not would affect the performance of the proposed method. **7)** Improve the imperceptibility implementing a spatial masking [5], as shown in Fig. 3 and given by (1):

$$I_{WM} = (1 - M_\sigma)I + M_\sigma I_W, \quad (1)$$

where M_σ is the masking image, which has values in the interval $[0, 1]$ and gives a measure (for each pixel of the original image I) to its insensitivity to noise [5]. I_{WM} is the final masked and watermarked image and M_σ is given by (2):

$$M_\sigma(x, y) = \frac{1}{M_{\max}} \sum_{(k,l) \in Window} [I(k, l) - \mu_{Window}(k, l)]^2, \quad (2)$$

where $M_{max} = max_{m,n} M_\sigma(m, n)$ is the maximum value of the local variance processed over the whole image, $\mu_{Window}(k, l)$ is the local mean computed in a square window of 9x9 pixels centered at the position (x, y). **8)** Finally, convert I_{WM} to the DICOM native format.

Watermark extraction stage: **1)** Using the secret keys K_1 and K_2 which are known by the extraction stage, replicate the steps 1 to 3 of the embedding stage. **2)** Split the DFT magnitude $M'(u, v)$ into its four quadrants and compute the subtraction operation $D_i = M'_i(u_j, v_j) - M'_i(-u_j, v_j)$ of the 1st and 2nd quadrants of the upper half part of $M'(u, v)$ in the annular area A, where $i = 1, \ldots, L$. **3)** Recover the watermark pattern W' as follows: if $D_i \geq 0$ then $W'_i = 1$, otherwise $W'_i = 0$.

3. Experimental Results

The experimentation was carried out using 150 DICOM files of computed tomography (CT) modality, classified in three types: skull, abdomen and simple skull with 512x512x12 bits grayscale. Empirically the secret key K_1 is given by $N_1 = N_2 = 400$, meanwhile K_2 by $r_1 = 72$ and $r_2 = 74$. The watermark strength factor α used was chosen to 155. The watermark involves the DICOM metadata e.g., patient name, patient age, institution name, station name, patient ID, patient sex, patient birth date, to obtain the 80 bits in total after the watermark generation procedure. In order to

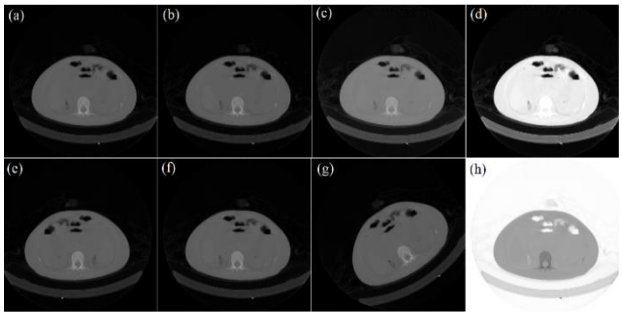

Fig. 4 Different distortions in the watermarked abdomen image.

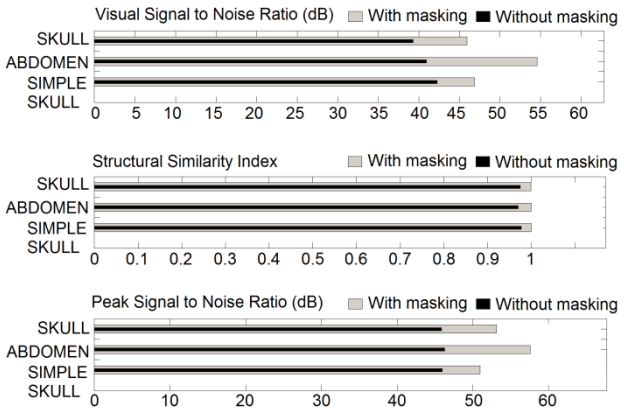

Fig. 5 Average watermark imperceptibility using the VSNR (dB), SSIM and PSNR (dB) metrics.

determine the watermark imperceptibility, we used the well-known VSNR [6], SSIM [7] and PSNR metrics to measure the distortion produced after the embedding process, and we apply the NCC metric to evaluate the similarity between the original watermark W and the extracted watermark W'.

$$PSNR(dB) = 10\log_{10}\left(\frac{N_1 \cdot N_2 \cdot Max\ Pixel\ Value^2}{\sum_{x=1}^{N_1}\sum_{y=1}^{N_2}(I(x,y) - I_{WM}(x,y))^2}\right), \tag{3}$$

$$NCC = \sum_{i=1}^{L}(W_i * W_i')\Big/\sum_{q=1}^{L}|W_i|^2, \tag{4}$$

In Fig. 4 it is shown one of the images used in the experimentation: (a) without distortion, (b) JPEG compression with quality factor 30, (c) contrast, (d) brightness, (e) flipping, (f) JPEG 2000, (g) rotation by 35° and (h) negative version.

In Fig. 5, the watermark imperceptibility in the watermarked images is presented. The watermark robustness after these attacks is given in Table 1. From the results in Fig. 5 and Table 1, we show that our proposed method is imperceptible enough and robust to several attacks while allowing recovering the watermark signal.

Finally, a performance comparison in terms of imperceptibility and robustness with the conventional methods in

Table 1 Average recovered data after several distortions (a)–(h).

Image	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
Simple Skull	100%	93%	90%	89%	100%	100%	88%	100%
Abdomen	100	92%	93%	91%	100%	100%	87%	100%
Skull	100	90%	92%	94%	100%	100%	80%	100%

Table 2 Performance comparison

Parameter	Rodriguez et al. [2]	Das et al. [3]	Proposed method
JPEG lossy	success	100-20	100-25
JPEG 2000	-	success	success
Brightness	success	-	50%
Contrast	success	-	30%
Rotation	0-35°	-	0-360°
Flipping	-	-	horizontal/vertical
PSNR (dB)	≤ 42.3	≤ 35	≥ 49.1
Detection	blind	blind	blind

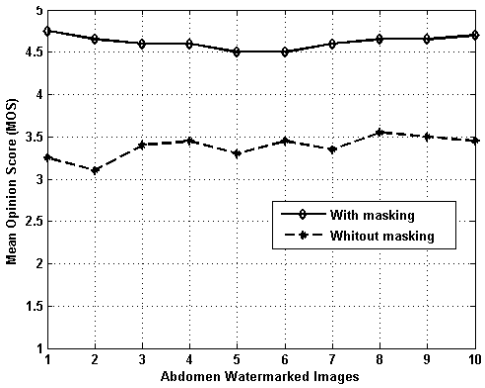

Fig. 6 Average MOS values obtained from ten abdomen images.

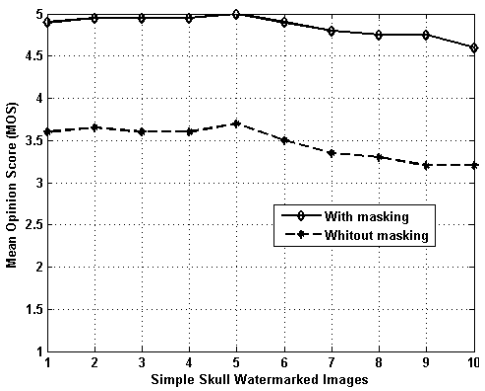

Fig. 7 Average MOS values obtained from ten simple skull images.

[2] and [3] is show in Table 2. Practical signal processing offered in the tools included on DICOM CD Viewer display interface are considered in this comparative. Labels 'success' or 'fail,' are assigned when the tolerance is not reported in the literature. A dash in Table 2 indicates that simulations not were mentioned in the literature.

In order to prove that image quality distortion caused by the proposed method will not affect the correct diagnosis performed by a M.D., a subjective test based on the Mean Opinion Score (MOS) metric was carried out. Our experiments are statistically supported by a medical staff

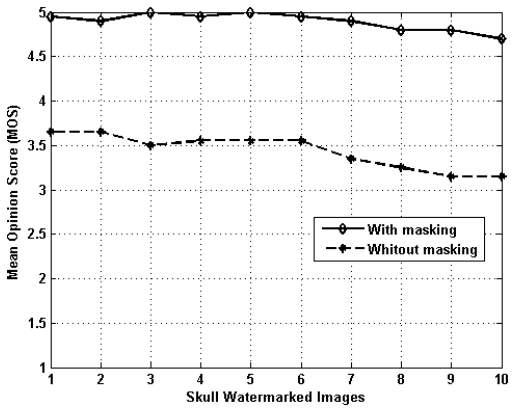

Fig. 8 Average MOS values obtained from ten skull images.

composed by twenty M.D. of different specialties. In Figs. 6, 7 and 8 the average MOS of the ten test watermarked medical images of skull, abdomen and simple skull modalities respectively, with and without masking, are plotted. From the MOS results in Figs. 6, 7 and 8, we conclude that the proposed method allows an accurate diagnosis, preserving a good quality in the watermarked images.

4. Conclusions

In this letter we presented a new and imperceptible watermarking technique applied to medical images that has shown to be robust to several distortions. The watermark has been hashed and ciphered with the RIPEMD-160 algorithm in order to diminish the DICOM metadata size and to add security to the watermarking method. Using a spatial masking it allows to obtain a better imperceptibility in the embedding process, obtaining average VSNR, SSIM and PSNR values greater than 49.10 dB, 0.9996 and 53.90 dB respectively. Because some of the DICOM metadata has been involved in the watermark generation it is created a high dependency with the image data itself preventing the confusion and assuring a robust structure highly recommended for a picture archiving and communication system (PACS) used in healthcare.

Acknowledgments

We thank the PAPIIT IA105215 project from DGAPA in the Universidad Nacional Autónoma de México (UNAM), the Instituto Politécnico Nacional (IPN) of México by the support provided during the realization of this research. We thank the specialists of medical faculty of LaSalle University and the Hospital "Dr. Manuel Gea Gonzalez" of Mexico for the subjective evaluations of the watermarked images obtained using the proposed scheme.

References

[1] G. Coatrieux, C. Quantin, J. Montagner, M. Fassa, F.A. Allaert, and Ch. Roux, "Watermarking medical images with anonymous patient identification to verify authenticity," J. Stud. Health Technol. Inform., vol.136, pp.667–672, 2008.

[2] R. Rodriguez, C. Feregrino, and J. Martinez, "Robust watermarking scheme applied to radiological medical images," IEICE Trans. Inf. & Syst., vol.E91-D, no.3, pp.862–864, March 2008.

[3] S. Das and M.K. Kundu, "Effective management of medical information through a novel blind watermarking technique," J. Med. Syst., vol.36, no.5, pp.3339–3351, Springer, 2012.

[4] B. Schneier, Applied Cryptography, 2nd ed., Wiley, New York, 1996.

[5] F. Bartolini, M. Barni, V. Cappellini, and A. Piva, "Mask building for perceptually hiding frequency embedded watermarks," Proc. International Conference on Image Processing ICIP 98, vol.1, pp.450–454, 4-7 Oct. 1998.

[6] D.M. Chandler and S.S. Hemami, "VSNR: A Wavelet-Based Visual Signal-to-Noise Ratio for Natural Images," IEEE Trans. Image Process., vol.16, no.9, pp.2284–2298, 2007.

[7] Z. Wang, A.C. Bovik, H.R. Sheikh, and E.P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," IEEE Trans. Image Process., vol.13, no.4, pp.600–612, 2004.

[8] M. Cedillo-Hernandez, F. Garcia-Ugalde, M. Nakano-Miyatake, and H. Perez-Meana, "Robust watermarking method in DFT domain for effective management of medical imaging," Signal, Image and Video Processing SIVP Springer, DOI 10.1007/s11760-013-0555-x, 2013.