J Inf Process Syst, Vol.11, No.4, pp.495~508, December 2015
http://dx.doi.org/10.3745/JIPS.02.0032

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Robust ROI Watermarking Scheme Based on Visual Cryptography: Application on Mammograms

Meryem Benyoussef*, Samira Mabtoul**, Mohamed El Marraki*, and Driss Aboutajdine*

Abstract

Inthis paper, a novel robust medical images watermarking scheme is proposed. In traditional methods, the added watermark may alter the host medical image in an irreversible manner and may mask subtle details. Consequently, we propose a method for medical image copyright protection that may remedy this problem by embedding the watermark without modifying the original host image. The proposed method is based on the visual cryptography concept and the dominant blocks of wavelet coefficients. The logic in using the blocks dominants map is that local features, such as contours or edges, are unique to each image. The experimental results show that the proposed method can withstand several image processing attacks such as cropping, filtering, compression, etc.

Keywords

Copyright Protection, Mammograms, Medical Image, Robust Watermarking, Visual Cryptography

1. Introduction

The rapid advancement of the Internet and multimedia systems in these last years has led to the creation of many useful applications such as telemedicine, which requires exposing medical data over open networks. But, due to this development, digital media, such as images, video, audio, or text, can be easily distributed, duplicated, and modified. However, in a number of medical applications, special safety and confidentiality is required for medical images, because critical assessments are made based on those images. Therefore, there is a need to provide strict security to ensure only the occurrence of legitimate changes [1].

Digital image watermarking techniques have been developed to protect the intellectual property of a digital image. This is achieved by embedding the copyright information, which is also called "the watermark pattern," into the original image. Copyright protection is achieved by robust watermarking while image authentication is usually achieved by fragile schemes. A fragile watermarking scheme detects any manipulation made to a digital image to guarantee the content integrity while a robust scheme prevents the watermark from being removed unless the quality of the image is greatly reduced.

Manuscript received September 17, 2014; first revision March 19, 2015; second revision June 1, 2015; accepted June 17, 2015; onlinefirst December 7, 2015.
Corresponding Author: Meryem Benyoussef (benyoussef.meryem@gmail.com)
* LRIT, Faculty of Science, Mohammed V University, Rabat, Morocco (Benyoussef.meryem@yahoo.fr, elmarrakimohamed@gmail.com, aboutaj@fsr.ac.ma)
**ENSA, Cadi Ayyad University, Safi, Morocco (mabtoul.samira@gmail.com)

There are a lot of medical image watermarking techniques described in the literature, which we can classify into three schools of thought as explained below.

- Region of interest (ROI) and region of non-interest (RONI) watermarking: In the ROI watermarking techniques, the watermark is embedded in the ROI in such a way that the perceptual quality of the image is not compromised. The watermark information is embedded in the RONI in order to keep the ROI distortion free. This way the diagnosis value of the medical image is not compromised [2,3]. In medical images the RONI generally contains the black background that encircles the ROI.
- Reversible watermarking: The second approach corresponds to reversible watermarking. Once the embedded content is read, the watermark can be removed from the image, which allows for the retrieval of the original image [4].
- Classic watermarking: The third approach consists of using classical watermarking methods while minimizing the distortion. In this case, the watermark replaces some image details, such as the least significant bit of the image [5,6], or some details are lost after lossy image compression [7].

Medical image watermarking techniques can also be grouped into two main categories. In the first one, the watermark is embedded in the spatial domain by directly modifying the pixel intensity of the original image. These algorithms are simple to implement, but can provide less correlation between original and extracted watermarks and less security; hence, anybody can detect these algorithms. In the second category, the watermark is embedded in the transform domain, such as the discrete cosine transform (DCT), discrete Fourier transform (DFT), the discrete wavelet transform (DWT), etc. These methods give more robustness against watermarking attacks because information can be spread over the entire image.

The conventional watermarking systems suffer from the tradeoff between the conflicting requirements of capacity, transparency, and robustness. Zero-watermarking has emerged as a new paradigm of watermarking, which eliminates the imperceptibility issues due to embedding the watermark. This approach does not embed a watermark into the host image physically, whereas it is embedded logically. With the apparition of the concept of visual cryptography (VC), first introduced by Naor and Shamir [8], a new range of zero-watermarking techniques based on this concept have been deployed. However, the major drawback of these schemes is the issue of reliability. This is because the watermark is not embedded physically and due to the fact that the medical images are very similar from one patient to another.

To remedy to this reliability problem, we propose in this paper, a robust ROI watermarking scheme based on the Faber-Schauder DWT transform (FSDWT) and VC concept. In this scheme, we combine VC and FSDWT to benefit from the many characteristics of this transform and from the security of the VC concept and its high protection of medical image content.

The rest of this paper is organized as follows: the concept of visual cryptography and the FSDWT transform are explained in Section 2. In Section 3, we describe the watermark concealing/extracting phases and the reduction procedure. The experimental results and some comparisons are shown in Section 4. Finally, Section 5 concludes this paper.

2. Visual Cryptography and FS-DWT Transform

2.1 Visual Cryptography

VC is a visual secret sharing scheme (VSS) extended for digital images, as proposed by Naor and Shamir [8] in 1994. It involved breaking up the image into n shares using a codebook. These shares are binary images usually presented in transparencies so that each participant can hold a transparency (share). Decryption stacks shares and views the secret image that appears on the stacked shares. The main characteristic of this concept is that it uses the human visual system (HVS) to decrypt a secret image without expensive and complicated decoding process.

The original problem of VC is the special case of a 2 out of 2 visual secret sharing problem, which is the most frequently used. In this scheme, the secret image is divided into two shares that consist of random dots. For each pixel P of the secret image, two blocks of 1×2 pixels are generated in the corresponding location for each share. Therefore, the generated shares have a size of 1s×2s if the original image is 1s×1s in size. If P is white, then the encoder randomly chooses a block of the first two columns in Table 1. If P is black, then the encoder randomly chooses a block of the last two columns in Table 1. Note that if P is white, the two blocks generated are identical, but if P is black, the two blocks are complementary.

In the decryption process, the two shares are stacked together. For a black pixel P, the result is a block with two black sub-pixels. But for a white P, the result is a block with one black sub-pixel and one white sub-pixel. By the HVS, the block with black and white sub-pixels will be recognized as a white pixel and the block with two black sub-pixels will be recognized as a black pixel. Therefore, the secret information can be easily detected when these shares are stacked together.

The decoding of the secret image by the HVS is the interesting feature that has attracted the researchers in adapting this concept for several applications including watermarking. In accordance with cryptography, the security of a crypto-system does not reside in the algorithm, but resides in the secret key; that is, the security will be well maintained, even if the algorithm has been published

Table 1. Codebook of the basic (2,2) visual cryptography

Pixel	□		■	
Probability	**1/2**	**1/2**	**1/2**	**1/2**
Share 1	■□	□■	■□	□■
Share 2	■□	□■	□■	■□
Share 1 ⊗ Share 2	■□	□■	■■	■■

2.2 Image Watermarking Based on Visual Cryptography

The first approach of image watermarking based on VC was proposed by Hwang [9] in 2000. Since the security characteristics of VC, the watermark pattern is difficult to detect or recover from the marked image in an illegal way.

Watermarking methods based on this concept of VC consist, in the embedding process, to create a binary matrix B based on image features. The binary matrix B is used to generate the secret share from

the watermark pattern using a visual cryptography codebook. In the extraction process, the same process is repeated to generate the public share. Finally, this is superimposed on the secret share to recover the ownership label.

Based on Hwang's idea, other related works have been proposed. In these watermarking schemes, the watermark pattern can be either physically embedded into the cover image or not. The first category of schemes, which are similar to traditional methods, are called watermark-embedding schemes [10]. The second category of schemes are called watermark concealing schemes and it is particularly useful in protecting highly sensitive images, since the original image is not altered [9,11-13]. This last feature has attracted us to use this concept for watermarking medical images, due to the high sensitivity of medical image. In this way, our medical images may remain intact and protected from illegitimate changes at the same time. Traditional methods and VC-based watermarking methods embed the watermark pattern in both the spatial domain [9,10,13] and the transform domains [11,12,14].

2.3 FSDWT Transform

The FSDWT has the same construction principle and some identical properties to the Mallat wavelet transform. The main difference is the fact that the FSDWT basis is not orthogonal. This transformation is also well adapted to contour detection as it eliminates the constant and linear correlation of smooth regions [15]. It only uses the first neighboring coefficients and gives more precise edge detection than higher order spline wavelets. The main interest of FSDWT is that this wavelet transform is obtained by lifting scheme formulation with only arithmetic operation and no boundary treatment.

3. Mammograms Preprocessing

Before any image-processing algorithm can be applied to mammograms, image preprocessing is necessary in order to find the orientation of the mammogram, to remove the noise, and to enhance the quality of the image.

Our proposed watermarking method belongs to ROI-based techniques. Therefore, a preprocessing step is required to extract a ROI that contains only the breast tissue in order to limit the undue influence while the features extraction phase in the watermarking process. In particular, mammograms are highly susceptible to the presence of noise, such as the pectoral muscle, a high intensity rectangular label, a low intensity label, tape artifacts, and any other object not belonging to the breast tissue [16]. The types of noises present in a mammogram are represented in Fig. 1.

Preprocessing is not in the scope of this work and this is the reason why we use the images that are preprocessed by the authors of [17].

4. Proposed Watermarking Approach

4.1 Used Techniques

4.1.1 Dominant blocks

Our image watermarking technique is a concealing scheme, which means that the watermark is not

physically embedded into the cover image. In the concealing process, we extracted some image features to construct the secret share. However, medical images are very similar between patients. For this purpose, we used the dominant blocks map consisting of local features such as contours or edges, which are unique to each image, and therefore, can act as a signature of the image.

We used the statistical features of the FSDWT coefficients to select dominant blocks [18]. As shown in Fig. 2, the non-dominant coefficients have amplitude near zero and small deviation values. Indeed, this property can be explained by the number of coefficients in the DWT increasing exponentially when we move up sub-bands, so the concentration of significant value coefficients becomes important in a region that uses a maximum number of scales (i.e., the very shape of region variations).

Dominant blocks can be selected using the following rule:

A block is dominant if $\sigma' \geq T\sigma$, where T is a parameter, σ' and σ, respectively, the standard deviation of the transform coefficients and the local deviation for a given 7×7 block.

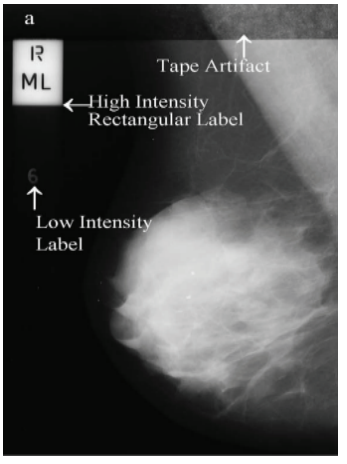


Fig. 1. Types of noise observed in mammogram.

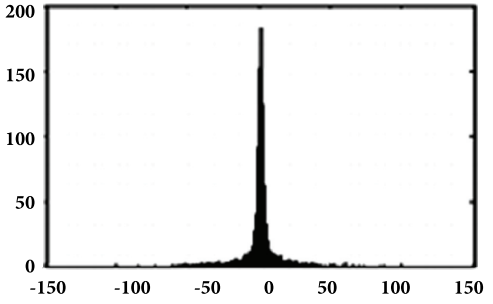


Fig. 2. Histogram of wavelet coefficients.

4.1.2 Reversible Walsh-Hadamard transform

In our image watermarking technique, we generate a binary matrix representing a secret share **SS** and an embedding map **EM** containing the coordinates of the dominant blocks. To merge these two matrixes in a reversible way, we used the reversible Walsh-Hadamard transform of order N=2, which leads to a reconstruction without distortion using the following forward and inverse transform matrices [19]:

$$[RWH]_2 = \begin{pmatrix} 1/2 & 1/2 \\ 1 & -1 \end{pmatrix}, \quad [RWH]_2^{-1} = \begin{pmatrix} 1 & 1/2 \\ 1 & -1/2 \end{pmatrix} \tag{1}$$

The fusion procedure is as follows:

Let (x,y) be the constructed pairs from **EM** and b the binary number from **SS**:

Step 1: Calculate (m,d), where $(m,d)=[RWH]_2(x,y)$

Step 2: Transform the d that corresponds to the difference to a binary number.

$$(d)_2 = d_l \quad d_{l-1} \quad . \quad . \quad d_2 \quad d_1$$

Step 3: Put the bit b as the LSB and calculate d'.

$$(d')_2 = d_l \quad d_{l-1} \quad . \quad . \quad d_2 \quad d_1 \quad b$$

Step 4: Calculate (x', y'), where $(x', y')=[RWH]^{-1}_2 (m, d')$ and replace (x,y) with (x', y').

4.2 Concealing Process

Inputs: Original Image **I** (m×n), Watermark Image **W** (r×c), Secret Key **S**

Outputs: Private Matrix **PM** (r, 2×c)

Step 1: Perform the FSDWT transform on the image **I**, and find all the dominant blocks.

Step 2: Use S as a seed to select random r×c dominant blocks.

Step 3: Construct an embedding map **EM**, such that the entries in the matrix are the positions of the selected dominant blocks obtained in the above step.

Step 4: Construct a feature image **F**, such that the entries in the matrix are the sample averages of the selected dominant blocks. Let F_{avg} be the average of **F**.

Step 5: Construct a binary matrix B:

$$B(x,y) = \begin{cases} 1, & \text{if} \quad F(x,y) \geq F_{avg} \\ 0, & \text{if} \quad F(x,y) < F_{avg} \end{cases} \tag{2}$$

Step 6: Use the bits in matrix **B** to select columns in Table 2 for generating the secret share **SS (r,2xc).**

Step 7: Merge the matrix **EM** with the matrix **SS** using the Reversible Walsh-Hadamard Transform.

Step 8: Use S as a seed to construct a noised private matrix **PM** from the matrix obtained in the above step.

Table 2. Codebook used to generate public and secret share

Pixel	□		■	
Matrix B	0	1	0	1
Public share	■□	□■	■□	□■
Secret share	■□	□■	□■	■□
Public share ⊗ Secret share	■□	□■	■■	■■

4.3 Extracting Process

This watermarking algorithm is blind since the detection process is accomplished without referring to the original image.

Inputs: Attacked Image **I'** (m×n), Secret Key **S**, Private Matrix **PM** (r, 2×c)

Outputs: Watermark Image **W'** (r,2×c)

Step 1: Perform the FSDWT transform on the image **I'**.

Step 2: Use **S** as a seed to denoise the private matrix **PM** and extract the embedding map **EM** and the secret share **SS**.

Step 3: Construct a feature image **F**, such that the entries in the matrix are the sample averages of the dominant blocks. Let F_{avg} be the average of **F**.

Step 4: Construct a binary matrix B:

$$B(x,y)=\begin{cases}1, & \text{if} \quad F(x,y)\geq F_{avg}\\ 0, & \text{if} \quad F(x,y)<F_{avg}\end{cases} \tag{3}$$

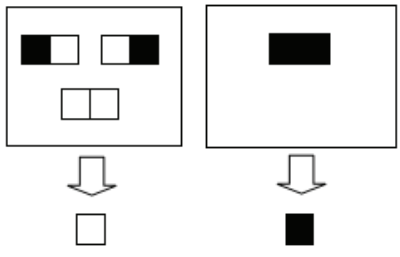
Step 5: Use the bits in matrix **B** to select columns in Table 2 for generating a public share **PS**. Note that the code-block assignment for a public share corresponding to each secret bit is independent of the pixel pair colors in the watermark image.

Step 6: Perform logical OR on the public share **PS** and the secret share **SS** to extract the watermark.

4.4 Reduction Process

Due to the (2,2) VSS scheme used to generate the two shares in our method, the extracted watermark has a size of (r×2c) compared to the original one. To retrieve the original size and to mitigate the noise effect caused by the watermark extraction, which improves the clarity of the extracted watermark, we used a post-process called a "reduction process" that can reduce the redundancy data caused by the VSS scheme. Indeed, this process can perform a function of data reduction as shown in Table 3; that is, a block of data with two pixels located in each group will be transferred into a corresponding pixel. As shown in Table 3, if the block is composed of one black and white pixel or two white pixels then the corresponding pixel is white, but if the block is composed of two black pixels then the corresponding pixel is black.

Table 3. The lookup table of reduction process



5. Experimental Results

In this section, we present some experimental results regarding the proposed method. The experiments are performed using MATLAB R2010a. Our test mammograms are from the MIAS database that are 1024×1024 pixels in size, and the watermark is a binary image representing a hospital logo that is 100×100 pixels in size (Fig. 3).

(a) (b)

Fig. 3. The used images: (a) mammogram and (b) watermark.

5.1 Robustness Test

To test the robustness of the algorithm against attacks, our test images were subjected to the following common attacks: compression, median filter, blurring, salt and pepper noise, cropping, resizing, rotation, and translation.

Watermarking schemes using VC are based on the HVS. Therefore, our first results show a visual comparison between our results and the results of a recent work presenting a watermarking method based on visual cryptography [11], which outperformed many other approaches. Table 4 shows the attacked images and the extracted watermark using our method and [11]'s method. From this table we can visually compare and show the advantage of our method as compared to the watermarking scheme of [11]. We can deduce that our method can provide very good robustness against attacks and we can also prove the efficiency of the proposed reduction process, which can improve the visual quality of the extracted watermark.

To support the previous results, we also measured the similarity between the extracted watermark and the original watermark by the normalized correlation (NC) using Eq. (4), while the peak signal-to-noise ratio (PSNR) using Eq. (5) measures the quality of the attacked images.

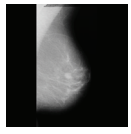
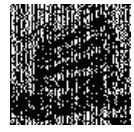
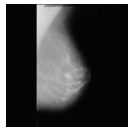
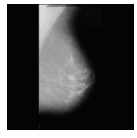
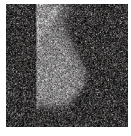
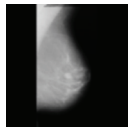
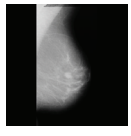
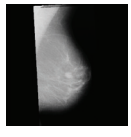
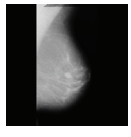
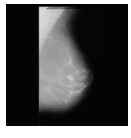
$$NC = \frac{\sum_{i=1}^{r}\sum_{j=1}^{c}\overline{\left(w_{i,j} \oplus w'_{i,j}\right)}}{r \times c} \times 100\ \% \tag{4}$$

$$PSNR = 10 \times \log \frac{255^2}{MSE} \tag{5}$$

$$MSE = \frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(c_{i,j} - c'_{i,j}\right)^2 \tag{6}$$

where, $c_{i,j}$ and $c'_{i,j}$ denote the pixel intensity of the original and attacked images.

Table 4. Experimental results outlining the superiority of the proposed algorithm

Attacks	Attacked images	Results of [11]	Our results
Cropping 15%			
Cropping 50%			
JPEG 40°			
JPEG 10°			
Salt & pepper noise 0.5			
Blurring			
Median filter 3x3			
Rotation 3°			
Scale 50 %			
Translate 20 lines			

In Table 5, we give the PSNR values of the attacked images and the corresponding NC values of the extracted watermark from each one. From this table we can see that even with low PSNR values when the image quality is very degraded, we can retrieve the watermark with a high NC percentage that reflects a very good visual quality and prove the robustness of our method against attacks.

Table 5. Robustness tests against common attacks

Attacks	PSNR (dB)	NC (%)
Cropping 10%	73.56	100.00
Cropping 25%	57.15	100.00
Cropping 50%	22.58	74.14
JPEG 80%	59.70	99.83
JPEG 50%	43.74	99.14
JPEG 10%	52.35	99.84
Salt & pepper noise 0.5	52.49	99.28
Blurring	44.76	97.20
Sharpening	49.52	99.10
Median filter 3×3	61.78	99.93
Median filter 5×5	59.52	99.91
Rotation 3°	34.92	85.59
Rotation 15°	26.24	60.45
Scale 50%	55.32	99.85
Crop 10 lines around	60.29	99.88
Translate 20 lines	29.34	68.88

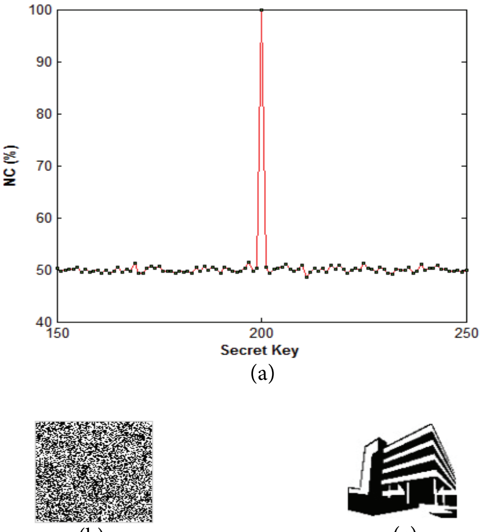
PSNR=peak signal-to-noise ratio, NC=normalized correlation.

5.2 Reliability Test

The second type of simulation helps to evaluate the reliability of the proposed scheme. In the first results, we executed the program with different secret keys to find out if the watermark can be retrieved with false keys.

Fig. 4 shows the NC values of the extracted watermarks and an example of the extracted watermark with false and true keys (200). As we can see from the results, the proposed watermarking scheme is very reliable, since the watermark can be extracted using only the true key.

In the second results, we tested the reliability of the method with different input images. In our method, the watermark is not physically embedded into the cover image. Therefore, we have to prove that the watermark cannot be extracted using a different image in the extraction phase. Table 6 shows the images used in the concealing and extracting schemes, and the watermarks that were extracted using our method and [11]'s method. The results show that our method is more reliable, which is due to the use of the dominant blocks of the FSDWT transform as a feature vector that is different from one image to another. It is also due to using these blocks for concealing the watermark instead of using the hole image, as used in [11]'s scheme.

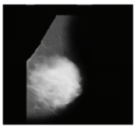
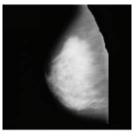
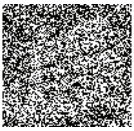
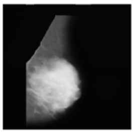
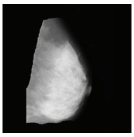
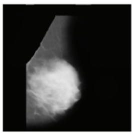
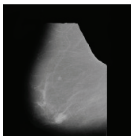
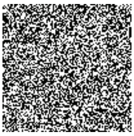
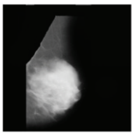
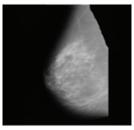
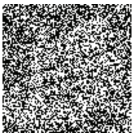
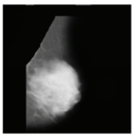
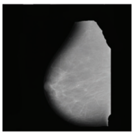
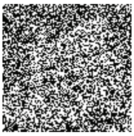
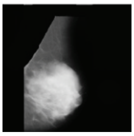
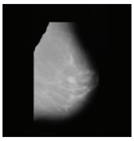
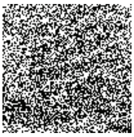


(a)

(b) (c)

Fig. 4. Reliability test: (a) normalized correlation (NC) values of the extracted watermark, (b) an extracted watermark with a false key, and (c) the extracted watermark with the true key (200).

Table 6. Reliability test with different input images

Image used in the concealing process	Image used in the extracting process	Extracted watermark using [11]' method	Extracted watermark using our method
			
			
			
			
			
			

6. Conclusions

This work deals with the development of a robust watermarking scheme for medical images. The purpose of this watermarking method is for copyright protection and the preservation of the confidentiality of patient data in network sharing.

In this method, we mainly focused on VC-based development. The advantage of watermarking methods based on VC is that it allows for the protection of the image by embedding a watermark without altering the cover image. This characteristic is particularly useful in protecting highly sensitive images, such as medical images.

The proposed method has been tested on mammogram images from the MIAS database, and the experimental results show that this method is reliable and can withstand several image processing attacks, such as cropping, filtering, compression, etc.

References

[1] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, and R. Collorec, "Relevance of watermarking in medical imaging," in *Proceedings of 2000 IEEE EMBS International Conference on Information Technology Applications in Biomedicine*, Arlington, VA, 2000, pp. 250-255.

[2] J. H. Wu, R. F. Chang, C. J. Chen, C. L. Wang, T. H. Kuo, W. K. Moon, and D. R. Chen, "Tamper detection and recovery for medical images using near-lossless information hiding technique," *Journal of Digital Imaging*, vol. 21, no. 1, pp. 59-76, 2008.

[3] G. Coatrieux, J. Montagner, H. Huang, and C. Roux, "Mixed reversible and RONI watermarking for medical image reliability protection," in *Proceedings of 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS2007),* Lyon, France, 2007, pp. 5653-5656.

[4] B. Macq and F. Dewey, "Trusted headers for medical images," in *Proceedings of DFG VIII-D II Watermarking Workshop*, Erlangen, Germany, 1999.

[5] D. Anan and U. C. Niranjan, "Watermarking medical images with patient information," in *Proceedings of the 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society,* Hong Kong, 1998, pp. 703-706.

[6] X. Q. Zhou, H. K. Huang, and S. L. Lou, "Authenticity and integrity of digital mammography images," *IEEE Transactions on Medical Imaging*, vol. 20, no. 8, pp. 784-791, 2001.

[7] M. Li, R. Poovendran, and S. Narayanan, "Protecting patient privacy against unauthorized release of medical images in a group communication environment," *Computerized Medical Imaging and Graphics*, vol. 29, no. 5, pp. 367-383, 2005.

[8] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology: EUROCRYPT'94.* Heidelberg: Springer, 1995, pp. 1-12.

[9] R. J. Hwang, "A digital image copyright protection scheme based on visual cryptography," *Tamkang Journal of Science and Engineering*, vol. 3, no. 2, pp. 97-106, 2000.

[10] C. C. Wang, S. C. Tai, and C. S. Yu, "Repeating image watermarking technique by the visual cryptography," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 83, no. 8, pp. 1589-1598, 2000.

[11] B. Surekha and G. N. Swamy, "Sensitive digital image watermarking for copyright protection," *International Journal of Network Security*, vol. 15, no. 2, pp. 113-121, 2013.

[12] M. Benyoussef, S. Mabtoul, M. El Marraki, and D. Aboutajdine, "Blind invisible watermarking technique in DT-CWT domain using visual cryptography," in *Image Analysis and Processing: ICIAP 2013*. Heidelberg: Springer, 2013, pp. 813-822.

[13] A. Sleit and A. Abusitta, "A visual cryptography based watermark technology for individual and group images," *Systemics, Cybernetics and Informatics*, vol. 5, no. 2, pp. 24-32, 2008.

[14] S. Radharani and M. L. Valarmathi, "Multiple watermarking scheme for image authentication and copyright protection using wavelet based texture properties and visual cryptography," *International Journal of Computer Applications*, vol. 23, no. 3, pp. 29-36, 2011.

[15] H. Douzi, D. Mammass, and F. Nouboud, "Faber-Schauder wavelet transformation application to edge detection and image characterization," *Journal of Mathematical Imaging and Vision*, vol. 14, no. 2, pp. 91-102, 2001.

[16] D. N. Ponraj, M. E. Jenifer, P. Poongodi, and J. S. Manoharan, "A survey on the preprocessing techniques of mammogram for the detection of breast cancer," *Journal of Emerging Trends in Computing and Information Sciences*, vol. 2, no. 12, pp. 656-664, 2011.

[17] W. R. Silva and D. Menotti, "Classification of mammograms by the breast composition," in *Proceedings of International Conference on Image Processing, Computer Vision, and Pattern Recognition*, Las Vegas, NV, 2012, pp. 1-6.

[18] H. Douzi and R. Harba, "Watermarking based on the density coefficients of Faber-Schauder wavelets," in *Image and Signal Processing*. Heidelberg: Springer, 2008, pp. 455-462.

[19] H. Sarukhanyan, S. Agaian, K. Egiazarian, and J. Astola, "Reversible Hadamard transforms," *FactaUniversitatis - Series: Electronics and Energetics*, vol. 20, no. 3, pp. 309-330, 2007.

Meryem Benyoussef

She received the Master degree in 2010 in Computer Science and Telecommunication from the Faculty of Science, Mohammed V University, Rabat, Morocco; where she is currently a Doctorate student. Her research interests include watermarking and image processing.

Samira Mabtoul

She obtained her Master degree in Computer Science and Telecommunication in 2005, and her Doctorate degree in engineering science in 2010, both from the Faculty of Science, Mohammed V University, Rabat, Morocco. She works now as an assistant professor at ENSA, Cadi Ayyad University, Safi, Morocco.

Mohamed El Marraki

He received the Doctorate and the Doctorate of the State degrees in algebra and number theory, respectively, from the Bordeaux University, France in 1991, and the Mohammed V-Agdal University, Rabat, Morocco, in 1996; he also received the Doctorate in "dessin d'enfant theory" from the Bordeaux University, France in 2001. He joined Mohammed V University, Rabat, Morocco, in 1996, first as an associate professor and full Professor since 2000, where he is teaching. Over 19 years, he developed teaching and research activities covering various topics of Mathematics, cryptography and graph theory which allow him to advise 5 PhD theses and publish over 60 journal papers and conference communications. Mohamed El Marraki is member of the several "Scientific Program Committee" of the International Conference. He is a member of several mathematical and computer science journals.

Driss Aboutajdine

He received the Doctorate and the Doctorate of the State degrees in signal processing from the Mohammed V-Agdal University, Rabat, Morocco, in 1980 and 1985, respectively. He joined Mohammed V-Agdal University, Rabat, Morocco, in 1978, first as an assistant professor, then as an associate professor in 1985, and full professor since 1990, where he is teaching, Signal/image Processing and Communications. Over 30 years, he developed research activities covering various topics of signal and image processing, wireless communication and pattern recognition which allow him to publish over 300 journal papers and conference communications.