Multiple Binary Images Watermarking in Spatial and Frequency Domains

Sameh Oueslati, Adnane Cherif, and Bassel Solaiman

***Abstract*—Watermarking is used for the protection of intellectual property, data integrity, and data authentication. This paper proposes a novel method for image watermarking based on embedding multiples watermarks in different domains of the image representation (spatial and DCT domains), without any distortion of the watermarked image. In the spatial domain, the processing method is based on study of segmentation by fuzzy c-means clustering method that outputs the zones of watermark embedding and respectively the associated appropriate embedding gain factors. However in the DCT domain a proper choice of the DCT coefficients based on the quantization JPEG table in the middle frequencies band is carried out. Several watermarks were embedded in these two domains in order to take advantage of the spatial domain robustness against different asynchronous attacks, associated to the DCT domain robustness against jpeg compression and some other signal processing distortions. Experimental results show that the proposed method is robust against a large set of synchronous and asynchronous image attacks such as filtering, lossy compression, cropping and rotation attack.**

***Index Terms*—Image watermarking, multi-domains, multi-watermark, insertion force, fuzzy c-mean (FCM)**

I. Introduction

Watermarking is a technique to identify the rightful ownership of multimedia data. When the ownership of data is in question, the watermark can be extracted to prove the copyright [1], [2]. The watermarking techniques proposed in the literature fall in two categories: spatial-domain methods [3], [4] and transform-domain methods [5] Many techniques have been proposed in the spatial domain, such as the LSB (least significant bit) insertion method [6], the patchwork method, and the texture block coding method [7]. For the human visual perception, the small changes in gray values are regarded as noise, The LSB method has a major disadvantage that the least significant bits may be easily destroyed such as randomly flipping the lower bits or lossy compression. Transform-domain methods, such as the Fourier transform [8], discrete cosine transform [9], or discrete wavelet transform [10], are based on spatial transformation, and process the coefficients in the frequency domain for hiding data. Therefore, how to select the best frequency portions of the image for hiding watermark is an important and difficult topic. After the inverse transformation, the hidden data is scattered around the spatial image. The transform-domain method is more robust than the spatial-domain method against compression, cropping, and jittering. The robustness is maintained at the price of imperceptibility in the transform domain.

In [11], a pseudorandom Gaussian sequence is embedded into the largest 1000 AC coefficients in the DCT domain. This method is robust to common image processing and geometric distortions.

In [12] and [13], the proposed DCT/DWT methods embed a binary visual watermark by modulating the middle-frequency components. These two methods are also robust to common image operations; but geometric transformations are still challenges.

In [14], the authors utilize SVD to embed two different types of watermarks, a Gaussian sequence and a binary image, respectively. This scheme could resist against rotation, cropping, and several malicious attacks. In this work a new image watermarking approach is proposed. Based on a multiple domain watermarking with several watermarks embedding in the spatial and frequency domains of the image representation. The number of embedded watermarks reached the eleven.

This paper is organized as follows: Section II details the multi-insertion method proposed in the fields of space and DCT: the segmentation study conducted and the automatic determination of the insertion force. In Section IV, we introduce the robustness of this technique against different attacks, and to test the capacity to detect the embedded watermark. And finally, we conclude our article.

II. The Proposed Method

In this paper we propose to exploit the robustness of respectively the spatial and frequency domain in the same time. A set of watermarks is embedded in the DCT frequency domain in different selected blocks coefficients with respect to the JPEG quantization values table. The choice of these coefficients is based on a strategy to minimize the vulnerability of the embedding scheme by the redundancy of the different embedded watermarks. In the same time, based on fuzzy clustering technique, a second set of watermarks is embedded in the spatial domain.

This embedding approach proves that the watermarked image become more robust mutually to the jpeg compression and wide kinds of synchronous and asynchronous attacks. In addition because of the recurrence resulting from the multiple embedded watermarks in these two domains, at least all or

Manuscript received November 18, 2012; revised January 23, 2013.

S. Oueslati is with the Faculty of Sciences of Tunis, Department of Physics, Laboratory of Signal Processing, Tunis, 1060, Tunisia (e-mail: Sameh.oueslati@telecom-bretagne.eu).

A. Cherif is with the Department of Physics, Laboratory of Signal Processing, Faculty of Sciences of Tunis, 1060, Tunisia (e-mail: adnane.cher@fst.rnu.tn).

B. Solaiman is with the Higher National School of Telecommunication of Bretagne, Department: Image and Information Processing, Technopole of Brest Iroise, 29285 Brest, France (e-mail: Basel.solaiman@telecom-bretagne.eu).

DOI: 10.7763/IJCTE.2013.V5.757

some of these inserted watermarks survived in each of the applied attacks.

A. Watermarks Presentation

The watermarks are presented as different binary images, containing data about the authors, research group, university name…etc with P ×P size described as the following:

$$M_L = \{M_L(i,j), 0 \le i, j \le P\} M \in \{0,1\} L \in .\{1,2......,L_{\max}\} \quad (1)$$

M_L denotes the binary watermark of index L. The maximum number of the watermarks having to be inserted is noted $L_{\max}$. P is chosen equal 32, and $L_{\max}$ is equal to 5 in the frequency domain and 6 in the spatial domain.

B. DCT Watermark Embedding

The first step of our watermarking scheme is to embed multiple watermarks in the frequency domain. Let I^{DCT} be the transformed image into the DCT domain presented as an 8×8 DCT blocks with respect to the image size. The DCT coefficients where the watermark bits will be encoded are chosen from the medium frequency band of the transformed blocks in order to provide additional resistance to lossy compression while avoiding significant modifications or distortions to the cover image. Instead of chosen arbitrarily the coefficients locations, we can increase the robustness to compression by basing our choice on the recommended JPEG table [15]. In fact if two locations are chosen as they present identical quantization values, any scaling of the first coefficient will scale the second by the same factor preserving their relative size. On the other hand to augment the survivel chances of the embedded watermarks against a large set of attacks and reduces the probability of detection errors, an additional gain factor denoted α is used in the watermark embedding process. Some criteria are presented for the choice of K as shown in Equation (2), in order to respect the threshold of the watermark imperceptibility shown by the image distortion.

$$C_1(i_1,\ j_1) - C_2(i_2, j_2) \ge K \quad (2)$$

C_1, C_2 are the DCT coefficients, $(i_1,\ j_1)$, (i_2, j_2) are respectively the positions of the two selected Coefficients with same quantization values and K is the gain factor resultant from this equation. The embedding procedure is as follows.

$$I_t^{DCT}(i,j) = I^{DCT} + KM_L(i,j), 0 \le i, j \le P \quad (3)$$

where + denotes the operation of watermarks adding to selected coefficients of 8×8 blocks represented by I^{DCT}, M_L are the embedded watermarks. By applying an inverse DCT transform, we obtain a spatial representation of a watermarked matrix image called $I_M{}^S$.

C. Determination Zones of Insertion by Method Fuzzy C-Means

FCM is an unsupervised clustering technique which has been utilized in a wide variety of image processing applications such as medical imaging [16] and remote sensing [17]. In fact, an image can be represented in terms of pixels, which are associated with a location and a gray level value. It can also be represented by its derivatives, e.g., regions with statistical features like Average grayscale value, Standard deviation, Variance, Entropy, Skewness, Kurtosis.

The first step consists to characterize each image pixel by a feature vector. Features can be extracted from regions masked by $(n \times n)$ window. Second step is used to cluster the feature vectors into several classes with every class corresponding to one region in the segmented image [18]. Using this method, the proposed technique doesn't allow a wrong classification output. Window $(n \times n)$ pixels is used to browse the DCT watermarked image to identify and mark the different existing zones. The original is automatically classified and marked with different colors as shown in Fig. 1 and Fig. 2. The spatial embedding procedure is preceded by a step of determining the insertion zones. Indeed, a heterogeneous image is composed by different zones (homogeneous textures, low intensity...). This diversity implies that the insertion in these different zones may not be identical. These aspects have been implemented in the next section; so the key point to embed a watermark is to determine where the watermark can be embedded and how much the strength can be added to.

D. Spatial Embedding Procedure

Six watermarks are used to be inserted into different zones with different gain. Because of the binary used watermarks, the embedding procedure derived from the Weber's law and shown by Equation 4 is considered as adding a percent of the pixel value to itself, this percent will varies of course with this value. In this way, the values of the added pixels belonging to the watermarks are not fixing; in fact the embedded watermark is variable from a pixel to another in order to preserve the homogeny of the image. This embedding procedure can be justified by the fact that HVS does not perceive equal changes in images equally, but visual sensitivity is nearly constant with respect to relative changes in an image.

$$(I_M(i,j) - I(i,j))/|I(i,j)| = cte \quad (4)$$

The general shape of the insertion procedure takes into account that the image was previously marked in the DCT frequency domain by a set of labels introduced as the following equation:

$$I^S_{MML}(i,j) = I^S_{M,L}(i,j)[1 + KM_L(i,j)] \quad (5)$$

where L denotes the watermark index $L \in \{1,2,......L_{\max}\}$. In this equation I^S_{MM} denotes the double watermarked image in the spatial and frequency domain, $I^S{}_{MML}$ is the watermarked image by L watermarks in the two domains, $I^S_{M,L}$ is the frequency watermarked image going to be watermarked in the second time by the watermark number $L \in \{1,2,......L_{\max}\}$ and K is the variable gain factor. The total embedded watermarks in the spatial and frequency domain are then considered equal to eleven, five in the frequency domain and six in the spatial domain.

Different other images are used in the carried experiments in all the watermarking process, with different classified zones numbers as shown in Fig. 1 and Fig. 2. These Figs show medical images with textures. Fig. 1 partitioned into four zones where the watermark can be embedded with several different gain factors. Fig. 2 is divided into three different zones. In each image the position where the watermarks have to be embedded change with the different zones.

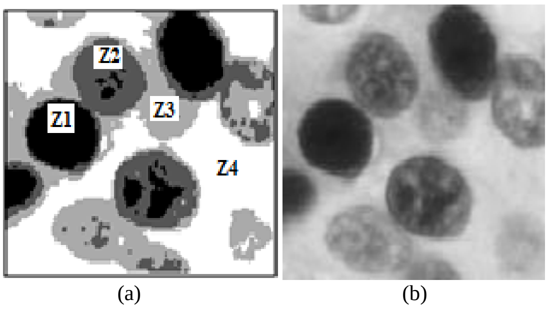

Fig. 1. (a) Original image, (b) Four classified zones.

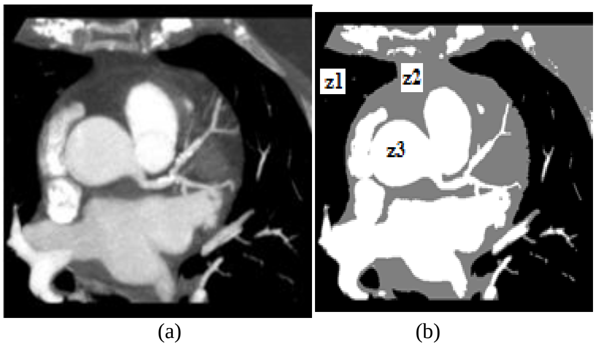

Fig. 2. (a) Original image, (b) Three classified zones.

E. Watermarks Detection

The detection procedure is performed in one of two domains, if the signature extracted satisfactory we can stop the detection process. In the opposite case where the signature is different from that extracted inserted. We move to another domain to perform a second detection procedure. One the signatures is detected we can choose the best, or reconstruct a more complete signature from those extracted.

III. Robustness Against Attacks

A. Performance Metrics

A watermarking scheme is evaluated based on two critical yet conflicting performance metrics:

1) Imperceptibility 2) the robustness to attacks that aim to eliminate watermarks.

Imperceptibility measures*:* Peak Signal to Noise Ratio (PSNR) is a widely used measure of fidelity (similarity between the original and the distorted image). Values over 30 dB in PSNR are acceptable in terms of degradation, which means no significant degradation is observed by the human eye. PSNR is defined as:

$$PSNR = 10\log_{10}\left(\frac{X^2_{\max}}{MSE}\right) = PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \quad (6)$$

$X_{\max}$: The maximum luminance, MSE is the mean-square error between the original image and the distorted one. To evaluate robustness, the watermark is extracted from a test image that underwent modifications, and correlation between the test watermark and the reference watermark is calculated. Normalized correlation, sim in [7], is used in this paper and is defined as:

$$sim(X, X^*) = \frac{X.X^*}{\sqrt{X^*.X^*}}, \quad (7)$$

where X and X^* are the original and reconstructed watermark sequence, respectively.

B. Experimental Results and Discussion

After concluding the watermarking process, we will test our algorithm by applying different attacks on the watermarked image as: JPEG compression, filtering, noises, cropping and rotation attacks. The tests performed to validate our hybrid approach are on images of size 256 x 256 grayscale. Respectively after each applied attack, the recovered watermark is compared with a set of 800 random watermarks containing the original one. We proved in all the experiments, the higher one corresponds to this computed between the original and the recovered watermark and there are no other similarities with other watermarks.

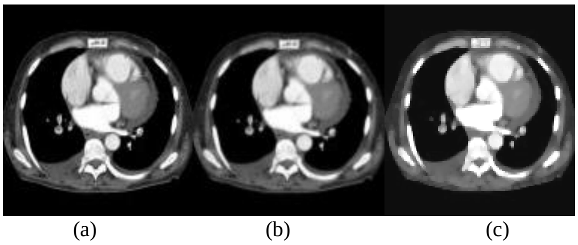

Fig. 3. The watermarked image introduced to various attacks: (a) JPEG compression (with quality factor 60%) of the watermarked image, (b) Watermarked image attacked by Gaussian filter, (c) Watermarked image after median filtering with a 3×3 windows.

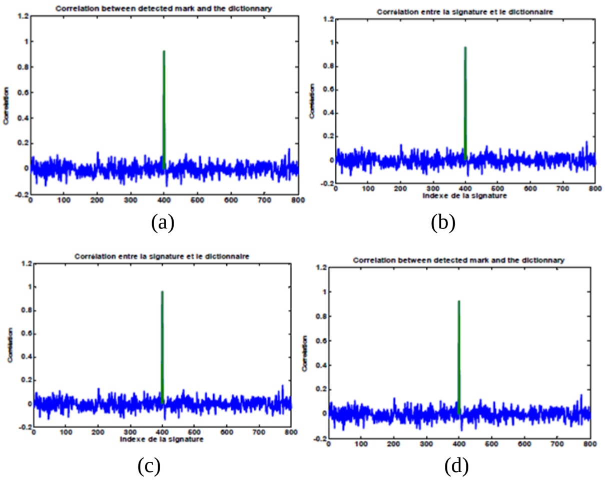

Fig. 4. Watermark detector response of attacked by JPEG compression of quality 60, (b) Watermark detector response of attacked by Gaussian noise (0.03), (c) Watermark detector response of attacked by Gaussian filler, (d) Watermark detector response of attacked median filtering with a 3x3 window.

1) *JPEG compression attack*

The JPEG compression is one of the standard attacks that a watermarking system should be resistance to. The measured PSNR between original images and watermarked image Attacked by different rate of compression (90%, 70%, 50%, 30%, 10%) are shown in Fig. 5.

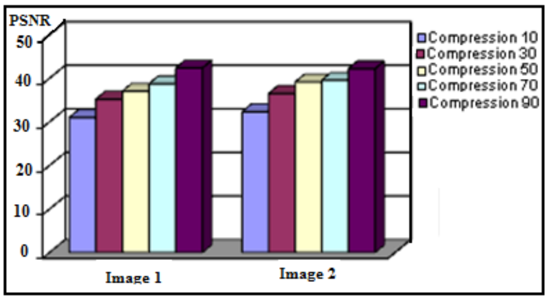

Fig. 5. Mean values of PSNR between the original images and watermarked images attacked by different rate of compression.

When compared with other methods more robustness and watermark embedding capacity are noted. In addition, when compared with [19], [20], this method proved its efficiency for the high amount of embedded data and a better robustness against different geometrical attacks As shown in Fig. 9, our proposed algorithm is highly more robust to JPEG compression when compared with different well known algorithms in the DCT and spatial domains such as Kutter, Cox, Koch, Langelaar, Bruyndonckx, and Fririch algorithms [21], [22], [24]-[26].

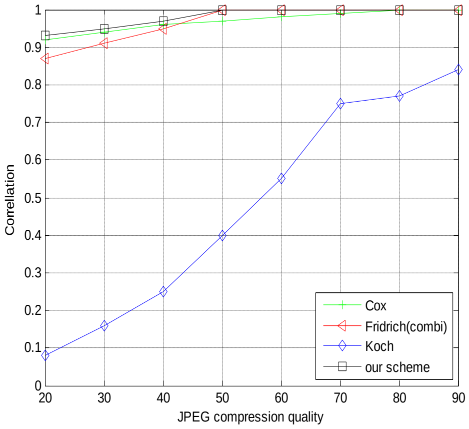

Fig. 6. Comparison with algorithms in DCT domain.

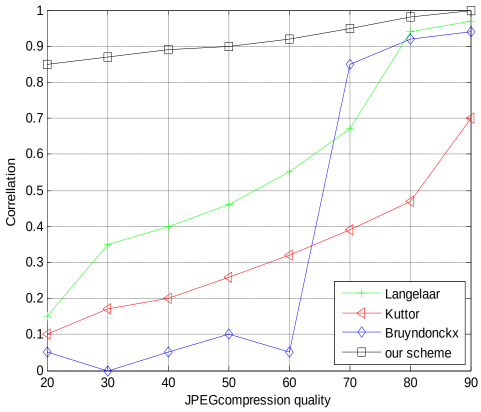

Fig. 7. Comparison with algorithms in spatial domain.

2) *Attack by adding noise*

It is quite relevant to evaluate the robustness of the suggested method against Noise. In fact, we have tested our new approach using 10 different Noises generations and by modifying variances at each time. The watermark detector response when the watermarked image is introduced to additive Gaussian noise with different variance values is shown in Fig. 4(b). From the Fig. 8, we can observe values of PSNR that are always higher than 30 dB. This makes it obvious that the image quality is good and these new Watermarked images algorithm is powerful to keep image fidelity even after Noise attack.

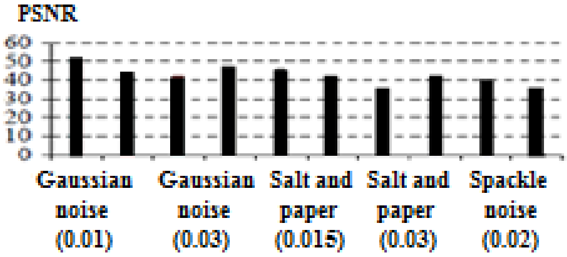

Fig. 8. Mean values of PSNR images Watermarked and attacked by different Types of Noises.

Note that the equation is centered using a center tab stop. We have tested the robustness of our proposed method face to Gaussian filter Fig. 4(c) displays the watermark detector response when the watermarked image is attacked by Gaussian filter.

3) *Geometric transformations attacks*

The tested geometric transforms are rotation and Cropping. We present in the following the means of PSNR for several test images related to the tested attacks: The cropping with different sizes (15×15, 25×25 and 65×65) and the different rotation angles (5, 15 and 20).

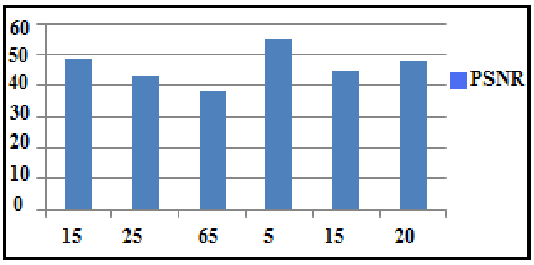

Fig. 9. Means values of PSNR for several test images watermarked and attacked by geometric transformations.

IV. Conclusion

In this paper a novel image watermarking approach based on a multiple domain watermarking with several watermarks embedding in the spatial and frequency domains. The simulation results proved that the proposed technique is robust against different synchronous and asynchronous attacks such as JPEG compression, different filtering and geometrical transformations.

In the watermark detection process we proved that between the embedded watermarks, a different watermark has survived to a large set of the applied attacks kinds. In addition, the redundancy caused by the multiple insertions has not altered our algorithm robustness. High correlations values after the attacked watermarked image are found in all the applied attacks kinds.

ACKNOWLEDGMENT

The authors express gratitude to Dr. REZGUI Haythem and Dr. AZAIEZ Mustapha clinic from the MANAR II of Tunisia, for helping and being in assistance.

REFERENCES

[1] K. Nima and M. Seyed, “A Robust image watermarking in the ridgelet domain using universally optimum decoder,” *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 20, no. 3, pp. 396-406, 2010.

[2] S. Srdjan and O. Irena, “An application of multidimensional time-frequency analysis as base for the unified watermarking approach,” *IEEE Transactions on Image Processing*, vol. 19, no. 3, pp. 736-745, 2010.

[3] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, “A DCT domain system for robust image watermarking,” *Signal Processing*, vol. 66, no. 3, pp. 357-372, 1998.

[4] S. Oueslati, A. Cherif, and B. Solaiman “Maximizing strength of digital Watermarks Using Fuzzy Logic,” *Signal and Image Processing: An International Journal (SIPIJ),* vol. 1, no. 2, pp. 112-124, December 2010.

[5] O. Azza, *Compression et Tatouage D’Images a Des Fins D’Archivage et de Transmission : Application Aux Images Médicales*, Habilitation University, Tunis El Manar, 2009.

[6] S. Saha and R. Vemuri, “How do image statistics impact lossy coding performance,” *Information Technology,* pp. 42-47, 2000.

[7] R. Gonzalez and R. Woods, *Digital Image Processing,* Addision Wesley, New York, USA, 1981.

[8] S. Jun and S. Mohammad, “Fragility and robustness of binary-phase-only-filter-based fragile/semi-fragile Digital image watermarking,” *IEEE Transactions on Instrumentation and Measurement,* vol. 57, no. 3, pp. 595-606, 2008.

[9] A. Philippe, “Digitalisation Sécurisée d'objets 3D : Application aux formes et aux lignes de style de chaussures,” Thesis Presented to the Academy of Montpellier University of Montpellier, 2008.

[10] A. Mohammad and S. Ebrahim, “Robust scaling-based image watermarking using maximum-likelihood decoder with optimum strength factor,” *IEEE Transactions on Multimedia*, vol. 11, no. 5, pp. 822-833, 2009.

[11] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” *IEEE Transactions on* Image *Processing.* vol. 6, no. 12, pp. 1673-1687, 1997.

[12] C. T. Hsu and J. L. Wu, “Hidden digital watermarks in images,” *IEEE Transactions on Image Processing.* vol. 8, no. 1, pp. 58-68, 1999.

[13] C. T. Hsu and J. L. Wu, “Multiresolution watermarking for digital images,” *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing,* vol. 45, no. 8, pp. 1097-1101. 1998.

[14] R. Z. Liu and T. N. Tan, “An SVD-based watermarking scheme for protecting rightful ownership,” *IEEE Transactions on Multimedia.* vol. 4, no. 1, pp. 121-128, 2002.

[15] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*, Morgan Kaufmann, 1999.

[16] K. Hsiang, C. M. Jang and L. C. Chih, “Model-Free Functional MRI Analysis Using Kohonen Clustering Neural Networks and Fuzzy C-Means,” *IEEE Transactions on medical imaging,* vol. 18, no. 12, 1999.

[17] W. Chumsamrong, P. Thitimajshima, and Y. Rangsanseri, “Syntetic aperture radar (SAR) image segmentation using a new modified fuzzy c-means algorithm,” in *Proceedings of Geoscience and Remote Sensing Symposium,* vol. 2, pp. 624-626, 2000.

[18] J. C. Bezdek, “Pattern recognition with fuzzy objective function algorithms,” *Pleunum,* New York, 1981.

[19] Z. Dawei, C. Grong, and L. Wenbo, “A chaos based robust wavelet-domain watermarking algorithm,” *Science Direct Journal,* 2004.

[20] B. S. Kim, J. G. Choi, C. H. Park, J. U. Won, D. M. Kwak, S. K. Oh, C. R. Koh, and K. H. Park, “Robust digital image watermarking method against geometrical attacks,” *Real Time Imaging Journal,* vol. 9, no. 2, pp. 139-149, 2003.

[21] O. Bruyndonckx, J. Quisquater, and B. Macq, “Spatial method for copyright labeling of digital images,” *IEEE* Workshop *on* Non-*linear Signal and Image Processing*, Thessaloniki, Greece, pp. 456-459, 1995.

[22] J. Fridrich, “Combining low-frequency and spread spectrum watermarking,” in *Proc. the SPIE Symposium on Optical Science, Engineering and Instrumentation,* San Diego, USA, 1998.

[23] M. Kutter, F. Jordan, and F. Bossen, “Digital signature of color images using amplitude modulation,” editor, in *Proc. the SPIE Conference on Storage and Retrieval for Image and Video Databases*, San Jose, USA, vol. 2952, pp. 518 - 526, 1997.

[24] W. Chumsamrong, P. Thitimajshima, and Y. Rangsanseri, “Syntetic aperture radar (SAR) image segmentation using a new modified fuzzy c-means algorithm,” in *Proceedings of Geoscience and Remote Sensing Symposium,* vol. 2, pp. 624-626, 2000.

[25] G. C. Langelaar, R. L. Lagendijk, and J. Biemond, “Robust labeling methods for copy protection of images,” in *Proc. the SPIE Conference on Storage and Retrieval for Image and Video Databases,* San Jose, USA, vol. 3022, 1997.

Sameh Oueslati is a researcher at the Image and Information Processing Department Higher National School of Telecommunications of Bretagne she is also in signal processing laboratory at the University of Sciences of Tunis - Tunisia (FST). Degree in electronics and she received a Masters degree in 2006 from the University of Sciences of Tunis. She is currently a PhD student at the Faculty of Sciences of Tunis of where she is a contractual assistant. His research interests include information hiding and image processing, digital watermarking, database security. She can be contacted at: sameh.oueslati@telecom-bretagne.eu

Adnane Cherif obtained his engineering diploma in 1988 from the Engineering Faculty of Tunis and his Ph.D. in electrical engineering and electronics in 1997. Actually he is a professor at the Science Faculty of Tunis, responsible for the Signal Processing Laboratory. He participated in several research and cooperation projects, and is the author of more than 60 international communications and publications. He can be contacted at adnene.cher@fst.rmu.tn

Bassel Solaiman is a telecom engineer, who holds a Ph.D. and HDR in Information Processing, University of Rennes I, He is currently professor and Head of Image and Information Processing from the Higher National School of Telecommunication of Bretagne in Brest, France. His research interests include, among others, on different approaches to treatment and Information Fusion and have been the subject of numerous publications. He can be contacted at bassel.solaimane@telecom-bretagne.eu