The Impact of the Concept of the Family Relative Signatures on the Non-Blind Watermarking in the Multiresolution Domain using 9/7 and 5/3 Wavelets

A. Khalfallah and M. S. Bouhlel

Abstract— **Digital watermarking is one of many security tools used to guarantee the intellectual property. There are three kinds of watermarking which differ in terms of the available information at the watermarking extraction step. In this study, we will focus on the non-blind watermarking which allows us to use the original host document, the signed document and the author signature. Unlike the classical watermarking approach which refers to the author by his original mark, the concept of the family relative signatures that refers to the author by a family of signatures made up of the relative daughter signatures. Adopting this concept, a daughter relative signature presents the really inserted signature inside the marked image. Consequently, this signature depends on the inserted mark, the host document and the insertion scheme. The established results present an improvement on the correlation rate and the validation rate in the watermarking process especially when we use the 9/7 wavelet.**

Index Terms— **Family relative signatures, Multiresolution domain, Non-blind image watermarking, 5/3 wavelet, 9/7 wavelet.**

I. Introduction

Information security presents a great worry for humanity. Nowadays, many techniques like cryptography, steganography and watermarking are used to ensure safe data transfer or to prove document ownership. In this work, we will focus on image watermarking. Watermarking is viewed as an imperceptible signal insertion into a digital image [1]. The embedded signal is called signature or mark. Digital watermarking should face up several constraints such as imperceptibility, robustness, insertion capacity, security and complexity.

Watermarking is carried out in two steps. The first step consists of inserting the mark inside the host image. The second step is the mark detection (or extraction). Based on this last step, we can sort out watermarking in three classes. The blind watermarking presents the first watermarking class. Adopting this marking kind, we are authorized to use only the marked image in the detection (or extraction) step [2]. The second watermarking class is called semi-blind watermarking. This kind of digital watermarking allows us to use the author's mark and the host image in the watermarking second step [3]. Finally, the third watermarking class is the non-blind watermarking. This watermarking category enables us to use the original image, the author's mark and watermarked medium in the extraction (or detection) step [4]. In this study, we are interested in the non-blind image watermarking.

At first, watermarking appears as a powerful tool to ensure intellectual propriety [5]. But, the good performance of this security tools and its easy implementation incite researchers to use it for other applications. Now, digital watermarking is used in many fields. In fact, the field of medicine has benefited from the performance of this tool. So, watermarking is used to preserve medical deontology by inserting the medical diagnostic inside the patient's image [6]. The insertion of digital fingerprinting permits to reveal the sources of illegal copies [7] and digital watermarking is used in broadcasting supervision [8]. Finally, specific information could be inserted into the host document to assist its indexation [9] or to check its integrity [10].

In this study, we will present the concept of family relative signatures for non-blind image watermarking and highlight the contribution of this concept on the watermarking performances in the multiresolution field based on the 5/3 and 9/7 wavelets.

Manuscript received October 9, 2001. (Write the date on which you submitted your paper for review.) This work was supported in part by the U.S. Department of Commerce under Grant BS123456 (sponsor and financial support acknowledgment goes here). Paper titles should be written in uppercase and lowercase letters, not all uppercase. Avoid writing long formulas with subscripts in the title; short formulas that identify the elements are fine (e.g., "Nd–Fe–B"). Do not write "(Invited)" in the title. Full names of authors are preferred in the author field, but are not required. Put a space between authors' initials.

F. A. Author is with the National Institute of Standards and Technology, Boulder, CO 80305 USA (corresponding author to provide phone: 303-555-5555; fax: 303-555-5555; e-mail: author@ boulder.nist.gov).

S. B. Author, Jr., was with Rice University, Houston, TX 77005 USA. He is now with the Department of Physics, Colorado State University, Fort Collins, CO 80523 USA (e-mail: author@lamar. colostate.edu).

T. C. Author is with the Electrical Engineering Department, University of Colorado, Boulder, CO 80309 USA, on leave from the National Research Institute for Metals, Tsukuba, Japan (e-mail: author@nrim.go.jp).

II. WATERMARKING IN MULTIRESOLUTION FIELD

Like any signal, an image has many representations. In the spatial domain, the digital image is presented by a matrix. The value of each cell reflects the luminance or the chrominance of the corresponding pixel. The presentation of image's frequency is obtained using the Discrete Cosine Transform (DCT) or the Discrete Fourier Transform (DFT) which highlights the frequency image reparation [11]. However, in the multiresolution field, the image representation highlights simultaneously the spatial and frequency repartition of the image. Therefore, this image representation is frequently used in image processing in JPEG2000 compression [12]. Hence, we will adopt the multiresolution image representation in our non-blind image watermarking approach. To transform an image to this multiresolution field we have to use wavelets.

A. Multiresolution domain by 5/3 wavelet

The 5/3 wavelet is a Gall wavelet based on a three coefficients low-pass filter and five coefficient high-pass filter. It is an integer to integer transform like shown is the equation 1 [13]:

$$\begin{aligned} d[n] &= d_0[n] - \left\lfloor \frac{1}{2}\left(d[n] + d[n-1]\right) \right\rfloor \\ s[n] &= s_0[n] + \left\lfloor \frac{1}{4}\left(d[n] + d[n-1]\right) + \frac{1}{2} \right\rfloor \end{aligned} \qquad (1)$$

This wavelet is frequently used for its conservative feature in PJE2000 compression.

B. Multiresolution domain by 9/7 wavelet

Unlike the 5/3 wavelet, the 9/7 wavelet is a Daubechies wavelet based on a couple of filters. The first one is low-pass filter using seven coefficients. But, the second filter is nine coefficient high-pass filter [13].

$$\begin{aligned} d[n] &= d_0[n] + \left\lfloor \frac{1}{16}\left(\left(s_0[n+2] + s_0[n-1]\right) - 9\left(s_0[n+1] + s_0[n]\right)\right) + \frac{1}{2} \right\rfloor \\ s[n] &= s_0[n] + \left\lfloor \frac{1}{4}\left(d[n] + d[n-1]\right) + \frac{1}{2} \right\rfloor \end{aligned} \qquad (2)$$

Despite, its non-conservative aspect, the 9/7 wavelet is also frequently used on the compression JPEG2000 for its high compression ratio.

C. Watermarking in the multiresolution field using the 5/3 and 9/7 wavelets.

In figure 1, we present the principle of digital image watermarking insertion step.

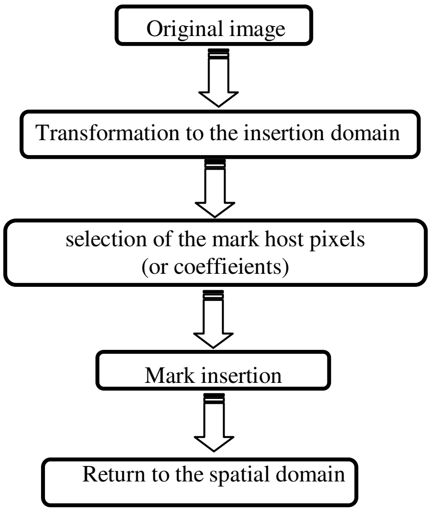

Fig. 1. Insertion scheme

We start by transforming the image into the insertion domain. In our case, it consists of transforming the image to the multiresolution field by the 5/3 or the 9/7 wavelet. Secondly, we select the host coefficients. Then, we insert the signature using an embedding function. Finally, we return to the spatial domain to obtain the watermarked image.

To extract the hidden mark we should transform the image to the insertion domain. Subsequently, we localize the host coefficients applying the insertion selection criteria on the host document. After that, we apply the inverse insertion function into the watermarked image elements to extract the hidden mark.

A validation test could be affected after the detection step. This test consists of comparing the extracted mark to a mark test bank having the same features, of the inserted mark. This bank includes the author referencing mark. The watermarked is called valid if the extracted mark presents the maximum similarity to the author's mark. Otherwise, the watermarked is called invalid.

III. THE CONCEPT OF THE FAMILY RELATIVE SIGNATURES

Classical methods refer to the author by his signature (mark). As known, we are interested in the non-blind watermarking which allows us to use the hidden mark and the original image.

Usually the extracted mark is different from the inserted one. This dissimilarity could be present without applying any distortion to the signed image. This difference is generally due to the insertion scheme. The concept of the family relative signatures profits from our watermarking technique choice. In fact, we adopt the non-blind watermarking. The principle of this approach consists in referring to the author by a family of relative signatures which depends on the author signature, the host image, the insertion function and the insertion domain. Adopting this concept, we name the original author signature "mother signature" or "generator signature". The "family relative signatures" is compound of "daughter relative signatures". This daughter signature is the extracted mark for non-attacked watermarked image. So, this signature depends on the mother signature, the host image and the insertion scheme. It is the really inserted mark. Consequently, the author is referred to by an sample of signatures derived from its original signature. Then, the adoption of the concept of family relative signatures consists of changing the author signature reference from the original signature to the daughter relative signature [14].

IV. Experimental results and discussion

A. Experimental condition and evaluation tools

Along this study, we will use the same signature composed of 512 real. This signature presents the author's signature in the classical approach and the generator signature for the concept of family relative signatures.

The evaluation is performed on a 30 grayscale images database. This image database is made up by 256x256 images of different features. The insertion is carried out on the second decomposition image details of the multiresolution domain (by 5/3 or 9/7 wavelet) using the following embedding function:

$$y_i = x_i\,(1+\alpha w_i) \quad (3)$$

y_i, x_i, α and w_i are respectively the marked host image coefficient, the original host image coefficient, the embedding coefficient strength and the mark element to insert inside the image.

The watermarking performance evaluation is limited in our study to the imperceptibility and the robustness of the embedded mark. In fact, an unnoticeable watermarking presents a PSNR (Peak Signal Ratio) higher than 30 dB. The PSNR is expressed by the following formula:

$$PSNR = 10\log_{10}(X_{max}^2/MSE) = 10\log_{10}(255^2/MSE) \quad (4)$$

Where, X_{max} presents the highest image amplitude. On the other hand, the MSE is the Mean Square Error of the compared images. The MSE formula is:

$$MSE = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m}\left(I_{ij} - I_{ij}^{*}\right)^2}{nm} \quad (5)$$

Where, I and I* are, respectively, the original image and processed watermarked image. n and m present the image matrix size.

The PSNR allows us to quantify the distortion made by the watermark or by any eventual image attack on the signed image.

The watermarking robustness reflects the capacity to detect the inserted mark from an attacked or non attacked signed image. To quantify the watermarking robustness we use a correlation detector. Thus, we will compare the extracted mark to the referring author signature using the correlation.

$$Cor(A,B) = \langle A,B \rangle = \frac{\sum_m\sum_n (A_{mn}-\overline{A})(B_{mn}-\overline{B})}{\sqrt{\left(\sum_m\sum_n (A_{mn}-\overline{A})^2\right)\left(\sum_m\sum_n (B_{mn}-\overline{B})^2\right)}} \quad (6)$$

Accordingly, the watermarking approach is validated if the comparison of the extracted mark to the random 500 signatures database including the referencing author's mark yields to a maximum correlation rate when we compare this last signature to the extracted one.

B. Results and discussions

Firstly, we start by a preliminary evaluation for the watermarking performances without applying any attack to the signed images. According to figure 1, we remark that adopting the family relative signatures concept give a correlation rate equal to 1. This result is due to the construction of the referencing mark. In fact, in this case, the referencing mark is the extracted mark from the non-attacked signed document. Consequently, we obtain the daughter signature in the watermarking extracting step. On the other hand, we remark that using the 5/3 wavelet in classical approaches ensures a better performance in terms of imperceptibility and robustness (Fig. 2 and 3). Figure 3 proves that classical approaches and the concept of family relative signatures ensure the same PSNR. In fact, the CFRS and the classical approach insert the same signature inside the document to watermark. Therefore, the marking imperceptibly depend only on the wavelet used in the insertion scheme. As a result, the family relative signature concept improves the watermarking robustness for the watermarking approach but it preserves the same imperceptibility. Looking to table 1, we can conclude that adopting the concept of family relative signatures in the multiresolution field based on the 5/3 wavelet ensures the best correlation rate and the least distortion of the watermarked image. Moreover, we remark that all approaches ensure a 100% rate validation because they ensure a neat detection of the author referencing signature (Fig. 4).

After that, we apply to the watermarked images some attacks (additive noise, Gaussian noise, cropping and compression). This operation aims at having an objective evaluation of the watermarking approaches. For each technique we illustrate the influence of the attack on the mean correlations (between referencing signature and extracted signature), the validation rate and the mean PSNR (between the original image and attacked signed image). The performance of each watermarking approach depends on the attack intensity and the referring signature. Based on figures 7, 10 and 13, we conclude, that using the 5/3 wavelet guarantees a better watermarking imperceptibility due to the conservative nature of the used wavelet.

Therefore, using the 5/3 wavelet in the classical watermarking ensures a better mean correlation rate between the author's signature and the extracted signature when facing attacks. These attacks could be classified into tow categories. The first attack type is the global attack. This kind of attack affects the whole image like Gaussian noise, compression. The second kind of attacks is partial image attack. This type of attack concerns only some image element like additive noise and cropping.

According to the established results, we remark that, for low intensity attacks, the 5/3 wavelet ensures a better correlation rate compared to the results obtained using the 9/7 wavelet. In fact, when facing these attacks, the extracted mark is distorted by the watermarking, the image attack. So, the non-conservative feature of the 9/7 wavelet adds more distortion to the watermarked images, which explains the better validation rate of classical approach based on the 5/3 wavelet. However, the increase of the attack intensity may change these preliminary results. In fact, the increase of the image partial attack yields a better validation rate for classical watermarking approach based on the 5/3wavelet (Fig. 6 and 12). But, increasing the intensity of the image global attack, the wavelet 9/7 wavelet seems to be better than the 5/3 wavelet according to their validation rate (Fig 9 and 15). In spite of these different validation rates, we remark that the classical watermarking approach based on 5/3 wavelet guaranty a better mean correlation rate between the author's signature and the extracted one (Fig. 5, 8, 11 and 13).

The established results demonstrate that adopting the family relative signatures concept, improves the correlation rate between the referencing mark and the extracted one (Fig. 5, 8, 11 and 13). These results yield to a validation rate improvement (Fig. 6, 9, 12 and 14). In fact, the daughter signature is more robust than the author's signature. These results are due to the referencing signature choice. In case of the family relative signatures concept, the author is referenced by the really inserted mark (daughter mark). However, the classical approach referenced the author by his original signature which could present some distortion in the extraction watermarking step even without applying any attack on the watermarked image.

On the other hand, adopting the concept of family relative signatures, the 9/7 wavelet guarantees a better robustness performance than the 5/3 wavelet when facing any attack. So, unlike the classical watermarking approach where the robustness of the watermarking depends on the wavelet choice and the attack intensity, the concept of family relative signatures ensures better correlation rate and better validation rate when we adopt the 9/7 wavelet in the insertion scheme. However, the use of the 5/3 always ensures a better invisibility performance for the watermarking approach.

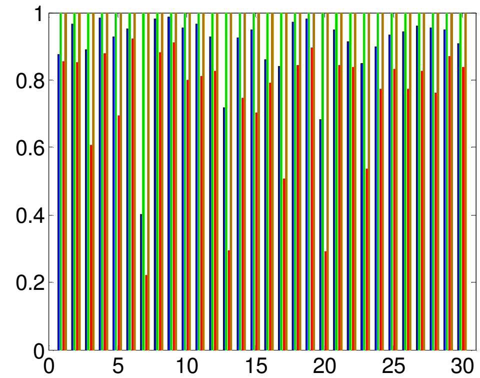

Fig 1. Correlation Vs image number classical watermarking[1] and the family relative signatures concept[2].

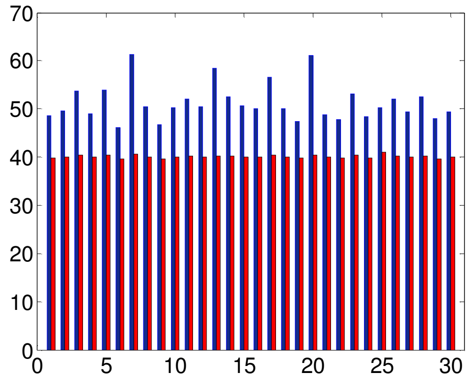

Fig 2. PSNR Vs image number (bleu : watermarking based on 5/3 wavelet ; red :watermarking based on 9/7 wavelet)

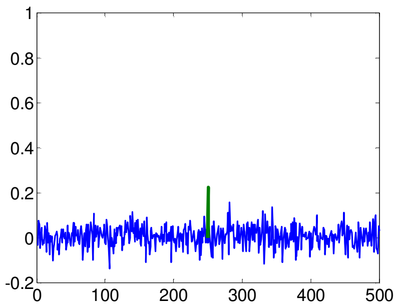

Fig 3. Successful detection for image number 7 : classical watermarking based on 9/7 wavelet (correlation rate = 0.2217).

TABLE I
CLASSICAL WATERMARKING AND THE FAMILY RELATIVE SIGNATURES PERFORMANCES CONCEPT OF THE MULTIRESOLUTION WATERMARKING BASED ON 5/3 AND 9/7 WAVELET

Watermarking type	Wavelet	Mean correlation	Validation rate	Mean PSNR
Classical	5/3	0.9001	100%	51.30
	9/7	0.7408	100%	40.11
RSFC	5/3	1.0000	100%	51.30
	9/7	1.0000	100%	40.11

[1]Bleu: classical watermarking using the 5/3 wavelet; Red: classical watermarking using 9/7 wavelet.
[2]Green: CFRS with 5/3 wavelet; brown: CFRS + 9/7 wavelet.

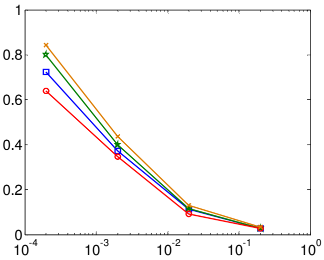

Fig 4. Mean correlation Vs additive noise intensity for classical watermarking and CFRS watermarking in multiresolution domain by 5/3 and 9/7 wavelet.

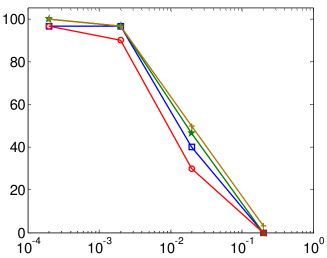

Fig 5. Validation rate Vs additive noise intensity for classical watermarking and CFRS watermarking in multiresolution domain by 5/3 and 9/7 wavelet.

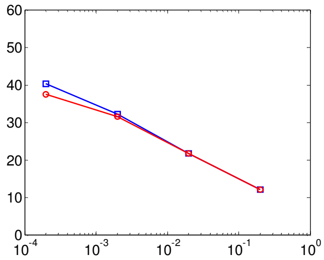

Fig 6. Mean PSNR additive noise intensity (bleu: watermarking based on 5/3 wavelet; red: watermarking based on 9/7 wavelet).

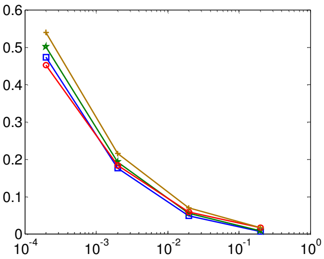

Fig 7. Mean correlation Vs Gaussian noise variance for classical watermarking and CFRS watermarking in multiresolution domain by 5/3 and 9/7 wavelet.

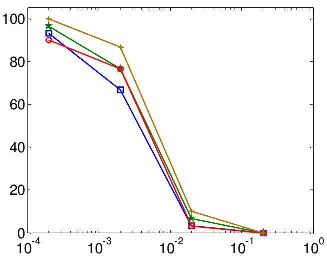

Fig 8. Validation rate Vs Gaussian noise variance for classical watermarking and CFRS watermarking in multiresolution domain by 5/3 and 9/7 wavelet.

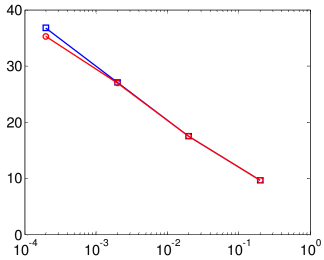

Fig 9. Mean PSNR Vs Gaussian noise variance (bleu: watermarking based on 5/3 wavelet; red: watermarking based on 9/7 wavelet).

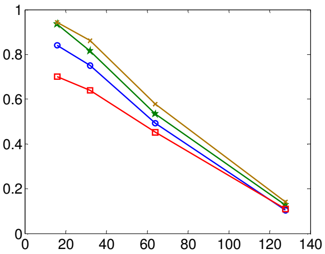

Fig 10. Mean correlation Vs cropping for classical watermarking and CFRS watermarking in multiresolution domain by 5/3 and 9/7 wavelet.

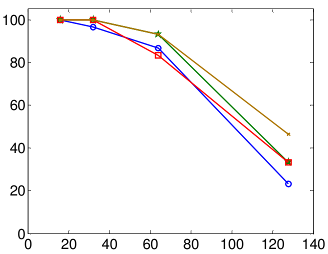

Fig 11. Validation rate Vs cropping for classical watermarking and CFRS watermarking in multiresolution domain by 5/3 and 9/7 wavelet.

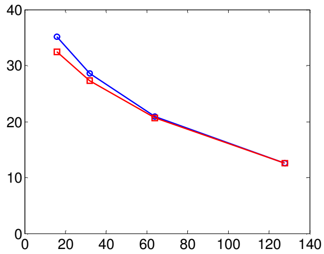

Fig 12. Mean PSNR Vs cropping (bleu: watermarking based on 5/3 wavelet; red: watermarking based on 9/7 wavelet).

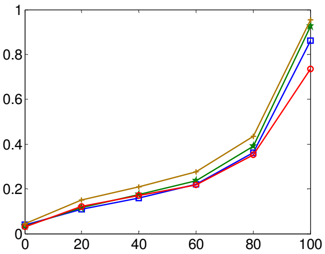

Fig 13. Mean correlation Vs compression quality for classical watermarking and CFRS watermarking in multiresolution domain by 5/3 and 9/7 wavelet.

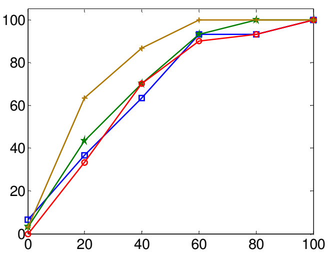

Fig 14. Validation rate Vs compression quality for classical watermarking and CFRS watermarking in multiresolution domain by 5/3 and 9/7 wavelet.

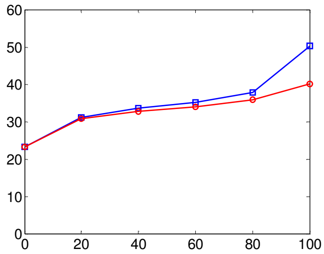

Fig 15. Mean PSNR Vs compression quality (bleu : watermarking based on 5/3 wavelet; red: watermarking based on 9/7 wavelet).

Fig 16. Examples of images from images database

V. Conclusion

In this study, we present a new concept for digital image watermarking. This new approach concerns the extraction step of the watermarking. Unlike the classical approach which refers to the author by the author original signature, the family relative signatures concept refers to the author by the daughter relative signature which is equal to the extracted mark from the non-attacked signed image.

For the classical watermarking, the established results prove that the use of the 5/3 wavelet ensures a better validation rate for non-attacked and low attacked signed images. The increase of the attack intensity on the partial attacked images engenders a better performance for the use of the 5/3 wavelet in classical watermarking. On the other hand, to face high global attacked images, the use of the 9/7 wavelet guarantees a better validation rate for the classical watermarking.

Yet, the adoption of the relative signatures family yields an improvement of the watermarking approach performance. These improvements concern only the correlation rate and validation rate. In fact, the author is referenced by the really inserted mark inside the signed attacked or non-attacked images. Like the classical watermarking, the adoption of the family relative signatures ensures a better imperceptibility for the inserted mark when we use the 5/3 wavelet. However, the use of the 9/7 wavelet certifies for the CFRS a better correlation rate and certainly a better validation rate.

REFERENCES

[1] F. Kammoun, A. Khalfallah and M. S. Bouhlel, “New Scheme of Digital Watermarking Using an Adaptive Embedding Strength Applied on Multiresolution Filed by 9/7 Wavelet”, *Inc. International Journal of Imaging Systems and Technology*, 16: pp 249-257, 2006.

[2] P. H. W. Wong, Oscar C. Au, and Y. M. Yeung, “A Novel Blind Multiple Watermarking Technique for Images”, *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 13, No. 8, pp 813-830, August 2003.

[3] A. Khalfallah, F. Kammoun, M.S. Bouhlel and C. Olivier, “Evaluation du Crypto-tatouage Semi-aveugle par le Chaos dans le Domaine Multirésolution à Base d’Ondelette 9/7”, 9ème Conférence Maghrébine sur les Technologies de l’Information MCSEAI’06, 07-09, Agadir, Maroc, Décembre 2006.

[4] A. Khalfallah, F. Kamoun and M. S. Bouhlel, “Amélioration du tatouage par exploitation d’un coefficient de pondération adapté”, In proceedings of the International Conference: Sciences of Electronic, Technologies of Information and Telecommunications (SETIT 04), TUNISIA, March 15-20, 2004.

[5] P. H. Wong and Nasir Memon, “Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership Verification”, *IEEE Transactions on Image Processing*, Vol. 10, No. 10, pp 1593-1601, October 2001.

[6] C. S. Woo, J. Du and B. Pham, “Multiple Watermark Method for Privacy Control and Tamper Detection in Medical Images”, APRS Workshop on Digital Image Computing (WDIC 2005), ISBN 0-9580255-3-3, Griffith University, Southbank, Brisbane, Australia, 21 Feburuary 2005.

[7] M. Kuribayashi, and H. Tanaka, “Fingerprinting Protocol for Images Based on Additive Homomorphic Property”, *IEEE Transactions on Image Processing*, vol. 14, No. 12, pp 2129-2139, December 2005.

[8] G. Doërr and J. L. Dugelay, “Problématique de la Collusion en Tatouage Attaques et Ripostes”, colloque COmpression et REprésentation des Signaux Audiovisuels (CORESA’05), Rennes, France, 7-8 Novembre 2005.

[9] M. El’arbi, C. Ben Amar and H. Nicolas, “IVTN : Un Environnement d’Indexation de la Vidéo par Tatouage Numérique”, In proceedings of the International Conference Sciences of Electronic, Technologies of Information and Telecommunications (SETIT 07), TUNISIA, March 25-29, 2007.

[10] I. Fourati Kallel, M. Kallel and M. S. Bouhlel, “A Secure fragile Watermarking Algorithm for medical Image Authentication in the DCT Domain”, In proceedings of the IEEE International Conference on Information and Communication Technologies: from Theory to Applications (ICTTA’06), Damascus, Syria, April 24-28, 2006.

[11] M. A. Cody, “The Fast Wavelet Transform Beyond Fourier transforms”, *Dr. Dobb's Journal of Software Tools*, Vol 17, pp 16-28, 1992.

[12] A. Masmoudi and M. S. Bouhlel, “A Proposal for Progressive Authentication and Data Integrity of Jpeg2000 Codestreams”, In proceedings of the IEEE International Conference on Information and Communication Technologies: from Theory to Applications (ICTTA’06), Damascus, Syria, April 24-28, 2006.

[13] M. D. Adams and F. Kossentini, “Reversible Integer-to-Integer Wavelet Transforms for Image Compression: Evaluation and Analysis”, *IEEE Transactions on Image Processing*, Vol 9, N° 6 June 2000.

[14] A. Khalfallah, F. Kamoun and M. S. Bouhlel, “Nouvelle méthode de tatouage dans le domaine multirésolution à base d’ondelette 5/3 : Notion de famille de signatures relatives”, In proceedings of the International Conference: Sciences of Electronic,Technologies of Information and Télécommunications (SETIT 05), TUNISIA, March 15-20, 2004

Dr. Ali Kkhalafallah was born in Rouen (France) in January 1980. He received the Diploma of Engineer on Electricity in 2003, the Diploma of Master on Electronics in 2004 and the Doctorate on Electronics in 2008 from the National Engineering School of Sfax-TUNISIA (ENIS). Currently, he is a research member in the Research Unit of Sciences and Technologies of Image and Telecommunications (SETIT). He is an assistant professor in the Higher Institute of Electronics and Communications of Sfax-TUNISIA (ISECS). His research interests include digital watermarking, cryptography, image fusion, image expansion and image processing. He is member of the organization committee in the international conference: Sciences of Electronic, Technologies of Information and Telecommunication SETIT’05 and the international conference: the International Conference on E-Medical Systems (E-MediSys 2008). He is the organization Chairman of the international conference: Sciences of Electronic, Technologies of Information and Telecommunication SETIT’07 and SETIT'09.

Pr. Mohamed Salim BOUHLEL is the head of the Research Unit of Sciences and Technologies of Image and Telecommunications (SETIT) and the director of the Higher Institute of Electronics and Communications of Sfax-TUNISIA (ISECS). He received in 1999 the golden medal with the special mention of jury in the first International Meeting of Invention, Innovation and Technology (Dubai). He is the Chairman of the international conference: Sciences of Electronic, Technologies of Information and Telecommunication: (SETIT 2003, SETIT 2004, SETIT 2005, SETIT 2007 and SETIT 2009), the Chairman of the international conference: the International Conference on E-Medical Systems (E-MediSys 2007 and E-MediSys 2008) and member of the program committee of a lot of international conferences.