A Fuzzy Watermarking Approach Based on the Human Visual System

Sameh Oueslati

sameh.oueslati@telecom-bretagne.eu

Faculty of Sciences of Tunis, Department of Physics, Laboratory of Signal Processing, University Tunis El Manar, TUNIS, 1060, TUNISIA.

Adnane Cherif

adnane.cher@fst.rnu.tn

Faculty of Sciences of Tunis, Department of Physics, Laboratory of Signal Processing, University Tunis El Manar, TUNIS, 1060, TUNISIA.

Basel Solaiman

Basel.Solaiman@telecom-bretagne.eu

Higher National School of Telecommunication of Bretagne, Department: Image and Information Processing, Technopole of Brest Iroise, 29285 Brest, FRANCE.

Abstract

The implementation of our watermarking system is based on a hybrid system combining the human visual system (HVS) and the fuzzy inference system (FIS), which always passes through the transcription of human expertise in the form of fuzzy rules expressed in natural language, which allows our watermarking system remain understandable for non expert and become more friendly. The technique discussed in this paper is the use of an advanced approach to the technique of watermark that is the multi-watermark or the watermarking multiple of medical images in the frequency domain. In this approach, the emphasis will be on the safe side and the invisibility while maintaining robustness against a certain target range of attacks. Furthermore, this approach is based on a technique totally blind as we will detail later.

Keywords: Digital watermarking, Fuzzy inference system (FIS), insertion force, The human visual system (HVS), Robustness.

1. INTRODUCTION

The new technologies of information and communication media are likely to make doctors and patients decisive help in finding a better quality of care. But the ease of access afforded by these new technologies poses the problem of the security of information particularly of medical images [10]. The role of security imposed on the medical image is attributed to watermarking [17]. However, its use in the domain of medical image is rare and few studies have been devoted. Even if the watermarking images are generally translated by imperceptible signals, the very fact that it modifies the host image hinders its spread in the hospital [25] [15]. However, in this article a major constraint and a question arose: How should provide a robust watermarking system applied in the medical field?

It is clear that we want it to be tamperproof and must therefore be protected by keys ensuring this security. It is not necessary that it has to be robust to a wide range of attacks as the most robust watermarking that protect the copyrighted images. Indeed, if the patient dares to degrade the watermark, he probably will alter the image also and the authenticity will be suspect at the same time it would degrade the diagnosis.

The work presented in this paper proposes a new watermarking technique based on a fuzzy inference system to extract the knowledge of sensitivity of human eye using the HVS model. The FIS and the HVS handsets are used in this work to automatically determine the insertion force in certain frequency components without being visually perceptible. Like most watermarking algorithms proposed, the invisibility of the watermark is obtained by using different properties of human visual system (HVS).

2. The Human visual system model

To hide the watermark in the image, it is useful to exploit the weaknesses of the human visual system [19, 13, 20, and 4]. However, the study of human perception is not confined only to the understanding of the optical device that represents the eye: Between the visions of the image that is printed on the retina and its interpretation in the human brain. The road is long and involves complex processes that are, todate, far from being fully mastered.

We will try in what follows to present the essential characteristics of human visual system that can be exploited to improve the imperceptible signature and to watermark the image with an adjusted coefficient by its internal dynamics.

We focus here on the sensitivity of brightness, texture and frequency. The HVS model used in this work has been suggested in [1, 2]. This model is also used in many insertion algorithm and detection of the watermark.

2.1 Luminance sensitivity (L_k)

Firstly, the eye is sensitive to contrast, and although the human visual system is capable of detecting small differences of luminance, there is a limit below which the differences are no longer collected [21].

This limit depends on the luminance L_0 of the bottom on which are the components of the image. Indeed, we notice hardly the changes of the image due to watermarking in the areas where the contrast is very important. The brighter the background, the lower the visibility of the embedded signal. Therefore a longer and a stronger embedded signal can be used. The luminance sensitivity is estimated by the following formula:

$$L_k = \left(\frac{V_{DC,k}}{\overline{V_{DC}}}\right)^{\gamma} \tag{1}$$

Where $V_{DC,k}$ is the *DC* coefficient of the DCT of the k^{th} block, $\overline{V_{DC}}$ is the mean value of all $V_{DC,k}$ coefficients of a specific image, and γ is set to 0.649 to control the degree of luminance sensitivity.

2.2 Texture sensitivity (T_k)

The degradations caused by the signature will be very low in the homogeneous areas of the image [3, 23], but may be more intense in highly textured areas for which the eye will not be able to differentiate between the signal from the image and the signal from the signature [8, 5, and 14]. The stronger the texture is less visible is the watermark. The texture sensitivity can be estimated by quantizing the DCT coefficients of an image using the JPEG quantization table. The result is then rounded to nearest integers. The number of non-zero coefficients is then computed. This method can be calculated by the following formula:

$$T_{k} = \sum_{x,y=1}^{N} cond\left(\left[\frac{V_{k}(x,y)}{Q(x,y)}\right]\right)$$
(2)

Where (x, y) represents the location in the k^{th} block. And cond(R) takes the rounded value of R and returns '1' if the value is not equal to zero, '0' otherwise.

2.3 Frequency sensitivity (F_k)

The insertion in the low frequency band of DCT blocks correspond to homogeneous zones in the image features a marking robust but distorts apparently the watermarked image [6, 12, and 16]. Contrariwise, an insertion in the high frequency band corresponding to the contours and abrupt changes of intensity of gray in the image, will characterize an imperceptible marking but fragile. Hence the needs to choose a medium frequency band that provide a compromise between the degradation of image quality and very visible and a maximum resistance to attacks. The sensitivity of frequency is represented by the quantization table (luminance).

3. Fuzzy Inference System (FIS)

In our fuzzy logic approach was a process of insertion well known by a human operator. The goal however is to automate. This is called knowledge by an expert who knows what to do in all cases; Increase the insertion force in less sensitive areas (areas textured) Decrease the strength of integration in sensitive areas (edges and homogeneous areas) ... ect. The fuzzy logic is used in our work, given the uncertainty and the changes in the unknown parameters (insertion force, pixels carrying the signature ...) and the structure of the watermarking system. When human experts are available to provide subjective and qualitative descriptions of behavior of system watermark with words in natural language. The expertise of the operator, often consists of among other simple rules, allows him to manage the system more properly a classical algorithm.

The principle of fuzzy logic approaches the human approach in the sense that the variables treated are not logical variables (within the meaning of the logic for example) but of variable linguistic relatives of human language as « a little, a lot more clearly ... very textured, very homogeneous etc » Moreover, these linguistic variables are processed with rules that refer to some knowledge of system behavior, most often obtained empirically. A fuzzy inference system consists of three blocks as shown in Figure 1. The first floor of fuzzification that converts numeric values to degrees of membership of different fuzzy sets. The second block is the inference engine, consisting of all rules. Finally, a defuzzification stage allows, if necessary, to infer a net worth, from the result of the aggregation rules.

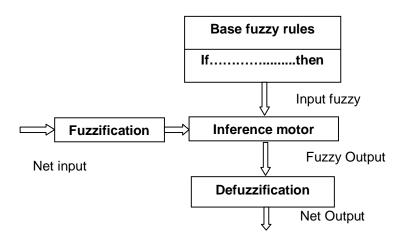


FIGURE 1: A Fuzzy inference system.

In what follows, we will retain only the essential elements to understanding the principle of adjustment of force of insertion in a watermarking system by fuzzy logic; these elements are fuzzy variables, rules of inference, and the membership functions.

3.1 The fuzzy variables

The binary logic has the advantage of simplicity but is rather distant from the logic used naturally by humans. If we represent the same problem using fuzzy logic, variables are not binary but have an infinite number of possible values between the « true» and the « false ».

Note that this representation is much closer to how human's reason, since it can involve concepts such as « smallish, a little, clearer ... highly textured, very homogeneous etc ». This advantage is, of course, at the expense of simplicity of representation. The fuzzy variables have a graduation between these two values.

3.2 Rules of inference

The role of the expert is here because he will fix the rules of the command that will cover only the linguistic values of variables.

We call rules of inference, all fuzzy rules connecting the different variables of a fuzzy system input variables and fuzzy output of this system. These rules come in the form:

- If (condition 1) and / or condition (N) then (action on the outputs).

In terms of artificial intelligence, summarize these rules makes the experience of the expert and they are usually not uniquely definable as each individual creates his own rules. It is necessary to convert quantities into variables crowds. To do this we define two notions.

- The membership functions that define the degree of truth of fuzzy variable depending on the input.

- The fuzzy intervals which determine the number of fuzzy variables.

3.3 The membership functions

It is a relationship between the degree of truth of fuzzy variable and the input correspondent. This is « fuzzification » this is to specify the domain of variation of variables: the universe of discourse, which is divided into intervals (in fuzzy sets or linguistic values). This distribution, which is to determine the number of such securities and distribute them on the domain, is made based on knowledge of the system according to the desired accuracy. The input and output membership functions exploited in this scheme are shown in Fig. 2. It is important to realize that this approach enables the luminance sensitivity (or texture) membership functions to be adjusted in such a manner to best fit the image's properties. In consequence, the approximations of the inferred values are optimized and are used to generate the adaptive strength of the watermark. Although the membership functions used in our algorithm consists of triangular and trapezoidal functions, they are not limited to these forms. We can obviously choose any form for membership functions.

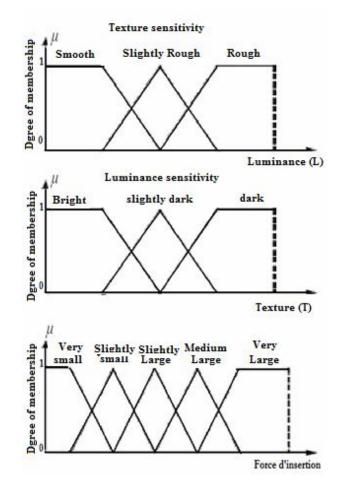


FIGURE 2: Dynamic Membership Functions and mapping of their input/output variables to fuzzy sets

3.4 Defuzzification

On output, the fuzzy system can not provide fuzzy values that can only operate. It is therefore necessary to provide accurate values, the role of the Defuzzification. This step is always done using the membership functions. From the degrees of membership functions, we obtain as many values it has States. It is therefore necessary to provide accurate values, the role of the Defuzzification. This step is always done using the membership functions. From the degrees of membership functions. From the degrees of membership functions. From the degrees of membership functions, we obtain as many values it has States. To determine the exact value to use, you can either keep the maximum, either calculates the weighted average, or to determine center of gravity values. In this work, the inference results are subsequently computed by means of the centroid defuzzification method, where the inferred value i_k of a specific block k of an image is calculated as in Equ. (3), where μ_c is the aggregated resultant membership function of the output fuzzy sets and i_n is the universe of discourse corresponding to the centroid of μ_c .

$$i_{k} = \frac{\sum_{n=1}^{N} \mu_{c}(i_{n})i_{n}}{\sum_{n=1}^{N} \mu_{C}(i_{n})}$$
(3)

In order to compute the adaptive watermark strength, the inferred value i_k is multiplied by the frequency sensitivity as it is shown in the following formula:

$$\alpha_{x,y,k} = F_{x,y} i_k \tag{4}$$

Where $\alpha_{x,y,k}$ the corresponds to the adaptive strength of a watermark at index (x, y) of the k^{th} block of an image. Also, $F_{x,y}$ corresponds to the frequency sensitivity at index (x, y).

4. The Proposed Approach

The FIS and the combined HVS are used in this work as shown in Figure (3), to adjust and determine a way to force automatic insertion. When the watermarking image, it must reflect compromise robustness invisibility. To enhance the robustness against various image distortions that can undergo using an insertion force α which must be below a threshold of visual perceptibility.

This force is not always consistent on all components of the watermark inserted but depends on the characteristics of the zones of insertion (Textured, uniform), because the human eye does not detect changes in low luminance, even better if they are hidden under sudden changes such as edges, contours, textures, etc..This force depends not only on the human visual system (HVS), but also characteristics of the zones of insertion.

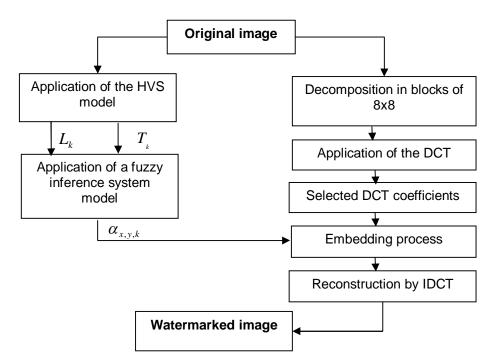


FIGURE 3: Embedding process based on the HVS and FIS

4.1 The Watermark Embedding Process

Among the work of watermarking proposed, algorithm [22], this consists of coding on a pair of frequency values {0, 1}. The use of frequency domain DCT can fulfill not only the invisibility through the study of optimization of the insertion force used, but also security by providing a blind algorithm which use the original image is not essential and the extraction of the mark is through a secret key [24,18,11]. In addition we will target a robust con of specific distortions such as lossy JPEG compression, the approach we propose, makes the coding of several marks in binary on DCT coefficients selected from each block of the image [23]. It proceeds in the following illustration of the stages of the insertion procedure. We proceed by determining the number of

coefficients to be used for coding the mark setting their Cartesian coordinates in the mid-band frequency of each DCT block size (8×8) .

The number of coefficients chosen depends on the size of mark, the level of redundancy of the mark which is reflected by the number of coefficients carry a single mark.

We proceed to a linearization of the mark M = [0,1,1,0,1,1,1,0,0,0..] of size $n = N \times N$. In each block we chose two coefficients of the same value of quantification by JPEG quantization table.

A scan on the blocks selected through the key positions is essential for ordering coefficients as follows:

For i varying from 1:n,

Denotes C_1 and C_2 DCT coefficients and mark holders.

If M(i) = 0 then we check:

If $C_1 \langle C_2$ then $C_1 = C_2$ and $C_2 = C_1$.

So the order becomes $C_1 \rangle C_2$.

- If M(i) = 1 then we check:
- $\text{If} \quad C_1 \geq C_2 \quad \text{then} \ C_1 = C_2 \ \text{and} \ C_2 = C_1 \,.$

So the order becomes $C_1 \langle C_2$.

Thus the entire sequence of binary vector represents a scheduling coefficient holder C_1 and C_2 is applied to characterize the value of the bit up the message blocks identified by the key. The insertion step is then applied as follows:

If $C_1 - C_2 \le \alpha$ and if $C_1 > C_2$ then:

$$\begin{cases} C_1 = C_1 + \frac{\alpha}{2} \\ C_2 = C_2 - \frac{\alpha}{2} \end{cases} \quad \text{Otherwise} \quad \begin{cases} C_1 = C_1 - \frac{\alpha}{2} \\ C_2 = C_2 + \frac{\alpha}{2} \end{cases}$$
(5)

4.2 The Watermark Detection Process

In our approach we have two key insertion markings to secure the site where the mark was introduced. The first key indicates the positions of the two selected coefficients with values of quantification. While the second key relates to the position of the blocks which will carry the marks among the total of all constituent blocks the transformed image. The extraction step is as follows: Compare the values of DCT coefficients to determine if the bit concerned the message was a "0" or "1".

If
$$C_1
angle C_2$$
 and $C_1 - C_2 \ge \alpha$ then $M(i) = 0$

Otherwise M(i) = 1.

Thus we come to remove the marks included in all blocks without using the original image.

5. Validation of the New Approach

For medical images the signature must be imperceptible: The watermarked image should be broadly similar to the original image so as not to lead to a misdiagnosis. The validity of any technical watermark can become more important than testing it against various types of attacks. For this, we chose to subject the medical image watermarked a series of attacks and test the sensitivity of the watermark and its ability to detect any change in the image. After application of each attack, all the marks included are extracted and compared through a study of similarities with the original marks (M and M) to be sure that these marks are not damaged by the attacks applied on the image.

5.1 The correlation coefficient

It measures the ratio of similarity between two images to show the close resemblance between the original mark inserted M and the extracted M'.

More it is close to 1 more likeness is perfect, and vice versa. This similarity measure is given by the following equation:

$$corr = \frac{\sum_{1}^{N} MM'}{\sqrt{\sum_{1}^{N} M^{2} \sum_{1}^{N} M'^{2}}}$$
(6)

5.2 The PSNR (Peak Signal to Noise Ratio)

PSNR, which is presented in equation (7), is an assessment of the decibel difference between the original image and one that is processed. In fact, a PSNR below 30 dB image can be considered untreated, inexploitable.

$$PSNR = 10\log_{10}(\frac{X_{\text{max}}^2}{MSE}) = PSNR = 10\log_{10}(\frac{255^2}{MSE})$$
(7)

Where X_{max} : The maximum luminance. Where MSE is the mean-square error between the original image and the distorted one.

MSE is defined as:

$$MSE = \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} (I_{ij} - I_{ij}^{*})^{2}}{NM}$$
(8)

Where M, N is the size of the image and contains $N \times M$ pixels I is the host image and I^* is the watermarked image.

6. Simulation and Discussion

Regardless of the domain of insertion of the watermark, have a good PSNR is an important requirement especially for medical images, where image quality plays a major role for better use of the image.

This work has been applied to several images of size 256x256 pixels resolution and 8 bits / pixel different. We begin our evaluation by a preliminary study, that is to say, a study without the application of attack on the tagged images.

Figure 4 shows the original medical image and tattooed. We note that the human visual system does not distinguish the difference caused by the marking.

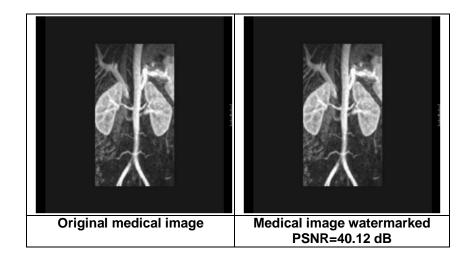


FIGURE 4: Original image and image watermarked.

The first test of robustness for an attack innocent which is compression. The compression algorithms are particularly dangerous for watermarking process. It is through the use of these algorithms do not keep the image that the components essential to their understanding (an invisible mark is obviously not essential). Therefore in the proposed approach, we inserted the signature in places fairly significant image, and it was based on a studied selection of DCT coefficients. We have chosen to apply the watermarked images at different compression ratios as shown in the table below which presents the results of simulations showing the rate of extraction of the similarities after contested mark with the original face of attacks applied.

Index	JPEG compression attack	Correlation values
1	20	0.9245
2	40	0.9482
3	60	0.9691
4	70	0.9825
5	80	1
6	90	1

TABLE 1: Presentation of the correlation values after attack by JPEG compression between the marks extracted and the original.

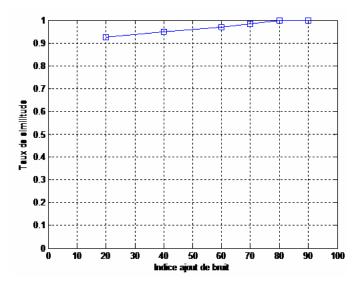


Figure 5: Original image and image watermarked.

The second test of robustness is the median filter that is most used in image processing. This filter replaces the pixel value by the median of its neighbors that exist in the analysis window centered on that pixel. The size of the window set the filter type; the types of filters that are treated in this section are listed in the table below.

TABLE 2: Correlation values after attack by median filter.

Median filter size	3x3	5x5	7x7
Correlation values	0.9158	0.8687	0.7459

The third attack is the application of a noise. This test has three types of noise: additive noise, gaussian noise and speackle noise. Following the application of an additive noise presents results similar rates in Table 3. This noise is measured by the SNR (Signal to Noise Ratio) to measure the quality of the noisy image compared to the original. This parameter is given by:

$$SNR = 10 \times \log_{10} [Var(I_{\rm R}) / Var(I_{\rm R} - I_{\rm 0})]$$
(9)

With I_B the image is noisy and I_0 is the original image. The variance of noise added is equal to X% the variance of the non-noisy image.

Index	Index of adding noise	Correlation values
1	20	0.8542
2	30	0.8093
3	40	0.7845
4	50	0.7285
5	60	0.6523

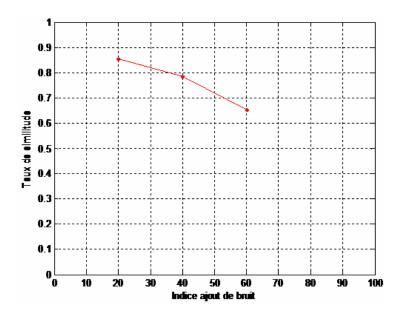


Figure 6: Presentation of correlation values according in the rate of noise.

We tested the robustness of the proposed approach compared to several generations as possible noise by varying each time the type of noise or variance. The PSNR values have their maxima for different variances of the multiplicative noise (speackle) that retains the best quality of the watermarked image. The Gaussian noise gives the lowest values of PSNR (relative to the other two types of noise tested). However, PSNR values are always above 30 dB, which allows the image to be usable as well. Noise "salt and pepper" does not alter too much the image quality digitally, but visually, the images seem to be degraded.

Table 4 summarizes the results established for the watermarked images after applying the three types of noise.

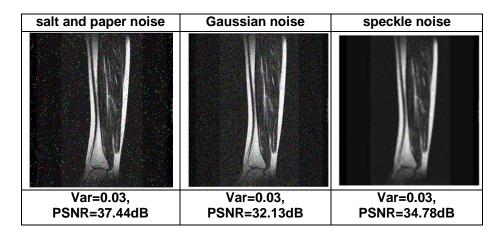


TABLE 4: Image watermarked attacked by different types of noise.

At the end, we evaluate our approach to asynchronous attacks. In what follows we focus on the rotation causes a change in the position of pixels causing a change in the information inserted in the image represented by the mark. The rotation angles used vary between 1° and 5°.

From Figure 7 the large angles of rotation were the most degraded quality digital image. They close the lower rate of similarity values. This degradation affects the holders of the signature involving loss of information.

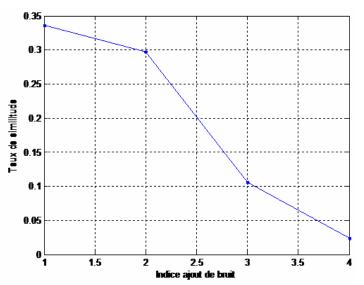


Figure 7: Presentation of correlation values according to the angles of rotation.

By scanning all blocks insertion of the image watermarked we succeeded in extracting the marks inserted in all the blocks used without recourse to the original image.

Note that all tests of medical images in our database, the transposition of the two coefficients by inverting their positions will not affect the image quality and does not introduce changes or visual distortions.

The whole procedure of insertion and extraction applied to the DCT.

This technique improves the safety of blind media tattooed cons of specific distortions such as adding noise or filtering or compression that can occur during transmission or storage.

More, only marked the image used in the process of extraction of patient data that are secured through two key positions indicating the location of coefficients holders and blocks insertion.

Independently of the area of insertion of watermarking, have a good PSNR is an important requirement especially for medical images, where the image quality plays a major role for better use of the image.

The study shows the variation of PSNR and rate of similarity based on different levels of attacks lossy compression, filtering, Median, noise and rotation are presented in Tables (1, 2, 3 and 4) and figures (5, 6 and 7). The marks obtained after the attack type rotation showed a slight similarity with the original image showing that the mark has been inserted damaged by this type of attack used.

7. CONSLUSION & FUTURE WORK

This paper presents a new blind watermarking scheme in the frequency domain based on the HVS and the FIS, which can increase the robustness of watermarking images in terms of quality and confidentiality. This approach of watermarking replacement has positive effects on the robustness of watermarking as it has allowed increasing the coefficient of insertion in certain frequency components without it being visually perceptible. We decided to validate the algorithm against such attacks; filtering, adding noise, rotation and focus here in particular to the JPEG compression. It was proved that the ability of this method is interesting. It resists attacks JPEG acceptable. In contrast, the method proves fragile compared to geometrical attacks. It is not sufficiently reliable to the robustness and security of the watermarking scheme is essential. Although some domains are robust against attacks synchronous, they may submit a weakness

against specific attacks or asynchronous. None of these domains can provide robustness against a wide range of synchronous and asynchronous attacks except through combinations of multiple insertion domains.

8. REFERENCES

- A.B. Watson, "DCT: A technique for visual optimization of DCT quantization matrices for individual images". Society for Information Display Digest of Technical Papers, pp. 946-949, 1993
- 2. N.S. Jayant, J.D. Johnson and R. Safranek. "Signal compression based on models of human perception". Proceedings of IEEE, Volume 81, No. 10, pp. 1385-1422, 1993
- 3. B. Miladi, M. Sayadi and F. Fnaiech. "Textures synthesis methods". International Conference on Electrical Systems and Automatic control, Tunisia, 2010
- S. Zaboli, A. Tabibiazar and R. Safabakhsh. "Entropy-Based image watermarking using DWT and HVS". 3rd International Conference of Sciences of Electronic, Technologies of Information and Telecommunications, Tunisia, 2005
- 5. F.Davoine and S.Pateux. "Tatouage de documents audiovisuels numériques". Livre édition Hermès Lavoisier, traité IC2 Série Traitement du signal et de l'image, (2004).
- 6. Patrick Bas and François Cayre, Natural Watermarking: a secure spread spectrum technique for WOA Information Hiding", pp.1-14, 4437, 2006
- 7. Coatrieux G., Puentes J., Lecornu L., Roux. C., "Compliant secured specialized electronic patient record platform". In D2H2'00, Proceedings of D2H2, Washington, Etats-Unis, 2006
- 8. P. Bas, F. Cayre, B. Mathon. "Techniques sures de tatouage pour l'image". Compression et Représentation des Signaux Audiovisuels, Montpellier, France, 2007
- 9. N. Palluat. "Méthodologie de surveillance dynamique à l'aide des réseaux neuro-fous temporels". PhD Thesis, University of Franche-Comte, 2006
- 10. O. Cadet. "Méthodes d'ondelettes pour la segmentation d'images : Applications à l'imagerie médicale et au tatouage d'images". PhD Thesis at the Polytechnic Institute of Grenoble, 2004
- 11. S. Pereira. "Robust Digital Image Watermarking". PhD Thesis, University of Geneva, 2000
- B. Mathon, P. Bas, F. Cayre. "Practical performance analysis of secure modulations for WOA spread-spectrum based image watermarking". Multimedia and Security Workshop, Dallas, Texas, USA, 2007
- 13. L. Lin, I. J. Cox and G. Doerr. "An efficient algorithm for informed embedding of dirty-paper trellis codes for watermarking". IEEE Int. Conference on Image Processing, 2005
- 14. M. Vincent. "Contribution des filtres LPTV et des techniques d'interpolation au tatouage numérique". PhD Thesis presented in Toulouse, 2006
- 15. A. Westfeld. "A Regression-Based Restoration Technique for Automated Watermark Removal". Multimedia & Security ACM Workshop MMSEC, Oxford, United Kingdom 2008
- 16. C. REY. "Tatouage d'image: Gain en robustesse et intégrité des images". PhD Thesis, University of Avignon and Pays de Vaucluse, 2003
- 17. G. Coatrieux M. Lamard, W.J. Puente, and C. Roux "A low distortion and reversible watermark: Application to angiographic images of the retina". In EMBC'05, Proceedings of Int. Conference of the IEEE-EMBS, p. 2224-2227, Shangaï, Chine, 2005
- 18. A. Zaid. "Compression et tatouage d'images à des fins d'archivage et de transmission : application aux images médicale". Habilitation University El Manar, Tunisia, April 2009
- 19. J.Reichel and M.Kunt. "Performance comparison of masking models based on a new psychovisual test method with natural scenery stimuli". Signal processing: Image communication, 17:807-823, 2002
- 20. M.Kutter and S.Winkler. "A Vision-based Masking Model for Spread-Spectrum Image Watermarking". IEEE Transactions on Image processing, 1(2): 244-250, 2002
- 21. N.sakr et al. "Copyright protection of learning using wavelet objects using wavelet-based watermarking and fuzzy logic, 3rd annual e-learning conference on Intelligent Interactive learning Object". Repositories Montreal. Quebec, Canada, 2006
- 22. J.Zhao, E.Koch. "Towards robust and hidden image copyright labelling". IEEE Workshop on Nonlinear Signal and Image Processing, 1995

- S. Geetha, Siva S. Sivatha Sindhu, N. Kamaraj. "Close Color Pair Signature Ensemble Adaptive Threshold based Steganalysis for LSB Embedding in Digital Images". Transactions on Data Privacy, pp. 140 – 161, 2008
- 24. 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
- 25. G. Coatrieux, H. Maitre. "Images médicales, sécurité et tatouage". Annales des Télécommunications, Numéro Spécial Santé, vol. 58, p. 782-800, 2003