A Digital Watermarking Algorithm Based on Quantization of the DCT: Application on Medical Imaging

Mohamed Ali Hajjaji, El-Bay Bourennane, Abdellatif Mtibaa, Gilberto Ochoa-Ruiz

A Digital Watermarking Algorithm Based on Quantization of the DCT: Application on Medical Imaging

Mohamed Ali HAJJAJI[1,2], El-Bay BOURENNANE[1], Abdellatif MTIBAA[2], Gilberto OCHOA-RUIZ[1]

[1.] LE2I Laboratory, Burgundy University, Dijon, France.
[2.] Electronics and Microelectronics Laboratory, Monastir University, Tunisia.

mohamedali_hajjaji@etu.u-bourgogne.fr; ebourenn@u-bourgogne.fr; abdellatif.mtibaa@enim.rnu.tn

***Abstract*—The objective of this paper is to elaborate a new watermarking algorithm applied to the medical imaging. This algorithm must be invisible, robust and has a rate, relatively high, integrating data.**

The proposed method uses the standard JPEG compression for the integration of medical data. The insertion block is inserted just after the quantization phase.

To control identification and eventually the correction (if possible) of the inserted data, we use a series of turbocodes to recover the inserted data, after application of several attacks.

The simulation studies are applied on MRI medicals images.

Keywords—Discrete Cosine Transform; series turbocode; Medical image; Quantization; Telemedicine.

I. INTRODUCTION

Medical Imaging is an important and vital tool in diagnostic and management decisions. In this regard, several techniques and imaging modalities (IRM, Echographic, Radiographic, mammography, ultrasound, etc) exist.

On the other hand, with the increasing complexity of diseases, several diagnoses are sometimes insufficient or non-conclusive, leading to the use of several tools, techniques and even physicians in different sites, to achieve a correct diagnostic. This trend is called telemedicine.

An image integrity problem arises with the exchange of data over the Internet, and this is particularly true with medical diagnostics which must be kept private. Therefore, the medical deontology, integrity and confidentiality must be ensured against the appearance of pirates. In this context, several context, several solutions based on the use of access control techniques exist, but they remain insufficient, hence the appearance of the watermarking in order to contribute to the security of medical images shared on the network.

At this step, we propose a watermarking method for medical imaging based on the Discrete Cosine Transform space (DCT) and the Error Correcting Code (ECC) (serial Turbocode).

II. EVALUATION OF WATERMARKING ALGORITHM

For the evaluation of the watermarking algorithm, many criteria are used. The most important are the quality of the image and the robustness of the watermarking scheme against various attacks. The quality of the watermarked image is evaluated with two types of measures [1]:

- Subjective measures;
- Objective measures.

Subjective and objective, that is introduced as follows.

A. Subjective measures

In the case of medical images, the subjective evaluation for image quality is defined by a group of appreciation scale experts. The format distance required is 4 times the height of the screen. Table 1 shows the observations scale of image quality [2] [3] [4].

TABLE I. INDEX OF APPRECIATION SCALE FOR IMAGE QUALITY.

Note	Quality
5	Excellent
4	Good
3	Average
2	Fair
1	Poor

In the case of a large database, this type of evaluation is becoming more expensive.

B. Objective measures

Objective measures are based on the comparison between the received watermarked image and the original image.

From these measures, we find the Peak Signal to Noise Ratio (PSNR), weighted PSNR, the relative entropy, the mean squared error and the average absolute error.

1) *Signal to noise ratio and peak signal to noise ratio*

Among the most important distorting measures in image processing is the Signal to Noise Ratio SNR and the Peak Signal to Noise Ratio PSNR. The SNR and the PSNR are respectively defined by the following formulas:

$$(SNR)_{dB} = 10 \log_{10} \{ [\frac{\sum_{i,j} I^2(i,j)}{\sum_{i,j} [I(i,j) - I_w(i,j)]^2}] \} \quad (1)$$

$$(PSNR)_{dB} = 10 \log_{10} \{ N \times M [\frac{\max I^2(i,j)}{\sum_{i,j} [I(i,j) - I_w(i,j)]^2}] \} \quad (2)$$

2) Weighted peak signal to noise ratio

The Peak Signal to Noise Ratio PSNR is based on comparing pixel to pixel the original image and the received watermarking image. The wPSNR proposed by Voloshy Noviskiand and Al [5] is defined by the following formulas:

$$(wPSNR)_{dB} = 10 \log_{10} \{ \frac{M \times N \max I^2(i,j)}{\sum_{i,j} [\frac{I(i,j) - I_w(i,j)}{1 + \mathrm{var}_I(i,j)}]^2} \} \quad (3)$$

With var(i,j) representing the local variance of pixel(i,j), I(i,j) the intensity value for the pixel(i,j) from the original image and I_w(i,j) the intensity value for the pixel of the image in test. M and N are respectively the height and width of the image.

C. Signature detection tools

The measure of "degree of reliability" detected data, returns to "calculation of distances" between the inserted and detected data. This measure is carried out using the correlation. The correlation of two signals consists to measure them dependence.

The correlation between two images X and Y is to calculate the correlation between two matrices X and Y of the same size by using the following formula:

$$Corr = \frac{\sum_i \sum_j (X_{ij} - \bar{X})(Y_{ij} - \bar{Y})}{\sqrt{\left(\sum_i \sum_j (X_{ij} - \bar{X})^2 \right) \left(\sum_i \sum_j (Y_{ij} - \bar{Y})^2 \right)}} \quad (4)$$

III. ATTACKS TYPES

In order to evaluate the robustness and effectiveness of our watermarking method, it is necessary to investigate the influence of different attacks on image. Many criteria have been explained above, but first we present attack that could be composed into two types [6]: innocent Attacks and malicious attacks.

A. Innocent attacks

During the transmission phase, the image might undergo different modifications, such as filtering, compression, and geometric transformations. These alterations are classified as innocent attacks.

B. Malicious attacks

Malicious attacks prevent the reception of the signature of the watermarked image. These attacks may desynchronize, or even destroy it and this will lead to the loss of coded data. Malicious attacks are concerned with jittering, extra marking attack, copying attack, and mosaics attacks, etc.

IV. PROPOSED WATERMARKING METHOD

The watermarking process is proposed to take advantage of standard JPEG compression. However the phase of the quantization step is the most harmful to the coefficients of the image. We therefore apply the hiding in the DCT components after they are quantified.

Figure 1 shows the overall scheme of our approach watermarking.

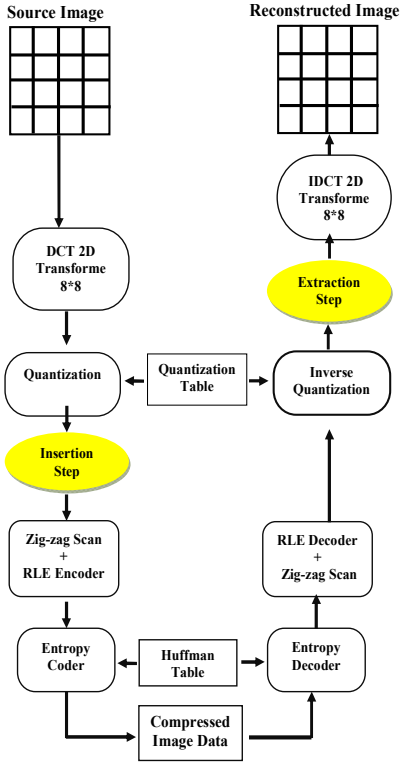

Figure 1. global schema.

As shown in figure 2, the inserting step combines various tools.

- Information about the patient coordinates, medical center and eventually medical diagnostic are introduced;
- The hash [7] function whose purpose is to generate the signature of hospital center ;

- Concatenate the signature and all of the patient record, these information are organized, in data message;
- Coding data message using error correcting codes (ECC), in our contribution the serial turbocode is proposed [8], whose aim is to contribute in data security and to the right data extraction after application of several attacks ;
- Discrete cosines transform space, after application of the quantization step, is the step able to insertion of the watermark.

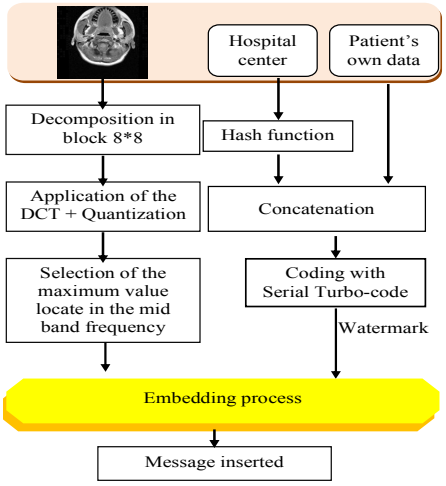

Figure 2. Embedding process.

V. PREPARATION OF WATERMARK

In our work, the totality of substituted message, in the medical image, contains the signature of the hospital center and the data of the patient (Figure 3)

After that, the serial turbo-code is used to contribute to the security and give effectiveness after application of many attacks.

PATIENT RECORD
Hospital center
Patient Ref
Name of the doctor
Age
Adresse
Case History:
Date of admission
Diagnosis

Figure 3. Data patient to insert.

A. Generation of Signature

The proposed hash function used in this work is the SHA-1 hash function.

The SHA-1 is a cryptographic [9] hash approach designed by the NASA in 1995 as a standard information processing tool/algorithm. SHA-1 is a function of this one-way hash. The Secure Hash Algorithm takes a message of less than 264 bits in length and produces a 160-bits message digest which is designed so that it should be computationally expensive to find a text which matches a given hash.

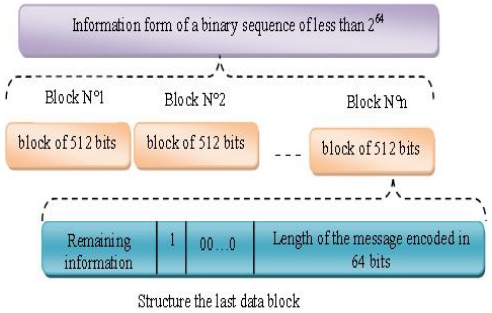

Figure 4. Decomposition of the message into blocks of 512 bits.

The processing is done on the ground totality N block, one after the other to get to the end to find final digital signature.

Figure 5 illustrates the different steps to find the hash of a block M(i).

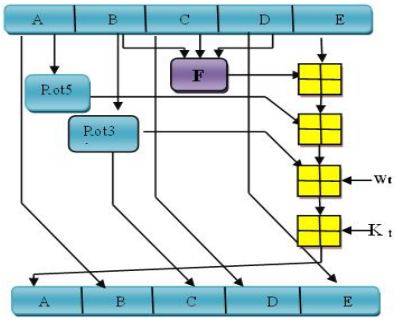

Figure 5. One iteration within the SHA-1 compression function.

With:

- Kt : Constant used in the i^{th} iteration;
- Wt : Word of the message number t in the program;
- F : Describe the functions used in calculating hash values;
- Rot : Describes a rotation with n bits.

VI. PREPARATION OF INSERTION SPACE

A. Selection of the frequency band

The insertion procedure in the field of DCT is quite difficult because the slightest change of certain frequency components of the transformed coefficients can cause significant degradation of the image quality.

Moreover, the inclusion in certain frequency components may be ineffective because the attacks image might undergo, could remove the inserted data.

In order To obtain a more robust watermarking method, the idea is to hide data in perceptually significant components of the image, taking into account the properties of the human visual system (HVS).

For this, it is interesting to select a medium frequency band ensuring good compromise between maximum resistance to attack and minimal degradation of the image quality.

As a result, the mid band frequency is selected as a first choice [10].

B. Selection of pixels carriers of watermark

In a second step, we apply the transformed image a quantization step before selecting pixels to be watermarked.

Indeed, given that the main purpose of insertion in the frequency domain (especially in DCT) is to ensure maximum robustness to JPEG compression, the quantization step is the most harmful alteration to the coefficients of the image.

Therefore, we propose to perform the insertion in the DCT components after they are quantified.

The choice of the quantization matrix was not fortuitous. Indeed, we choose one of the quantization matrices opted by the JPEG compression standard.

In the JPEG standard, numerous tests have led to the adoption in practice of quality factors between 1 (the image is excellent) and 25 (maximum acceptable degradation).

We chose a quantization matrix with a quality factor of 2 (which makes significant changes to the DCT matrix, but minor changes in the image).

The quantization matrix used is the following:

3	5	7	9	11	13	15	17
5	7	9	11	13	15	17	19
7	9	11	13	15	17	19	21
9	11	13	15	17	19	21	23
11	13	15	17	19	21	23	25
13	15	17	19	21	23	25	27
15	17	19	21	23	25	27	29
17	19	21	23	25	27	29	31

Figure 6. Quantization matrix.

In addition to the selection made before about frequency band, we retain only the coefficients belonging to this band and those of greater amplitude.

VII. WATERMARKING SCHEMA DESCRIPTION

Our Watermarking Schema is divided into two steps, insertion step and the detection step. For the insertion phase, it is recommended to:

- Compute the hospital signature center using 160-bit SHA-1 as a hash function;
- Concatenate the signature that contains the patient's information and diagnostic data. This data is transformed into binary message and encoded using the error correcting codes (serial turbocode);
- Apply the DCT on the different blocks (8*8) of the image;
- Apply the quantization step on the different blocks transformed, we chose the mid-range as a first selection. As the second selection, we chose an ordering of the coefficients chosen in descending order;
- In our approach, we propose to insert one bit per block (figure 7), choose the maximum value of frequencies quantified exist in the midrange.

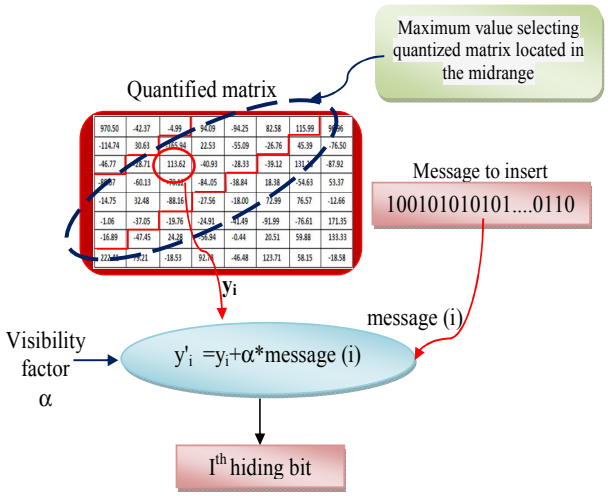

Figure 7. Inserting of one bit.

- Apply the DCT reverse on the different blocks of 8*8 to build the watermarked image.

The detection step consists to follow the reverse steps following previously.

VIII. RESULTS

The proposed approach is evaluated with different IRM images after application of various attacks. The types of attacks applied are:

- JPEG attacks with different rate compression;
- Additive noise attack.

Figure 8 shows measure of PSNR and wPSNR when the visibility coefficient α varies.

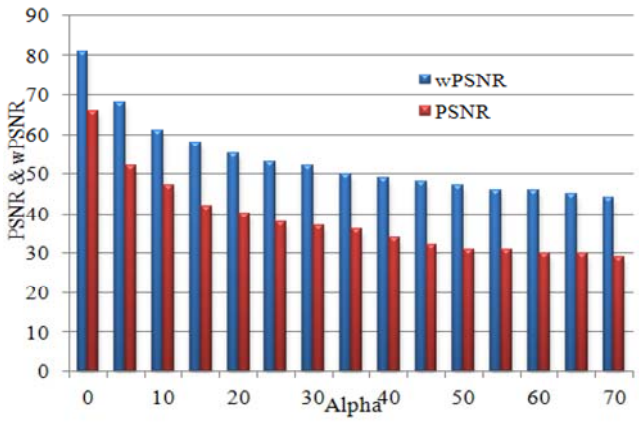

Figure 8. PSNR and wPSNR for MRI image.

Figure 9 shows the quality of MRI watermarked image robustness of our watermarking schema against JPEG attacks with different rate compression.

Concerning the error correcting code (figure 10), many tests show that we are able to correct the occurred errors when the tested images get compression image rate inferior to 90%.

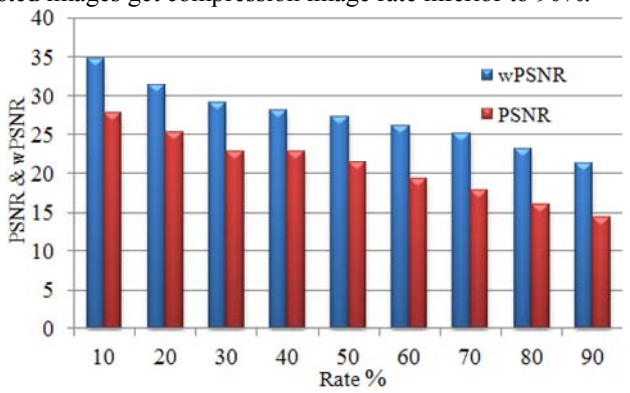

Figure 9. PSNR and wPSNR for MRI image watermarked and compressed.

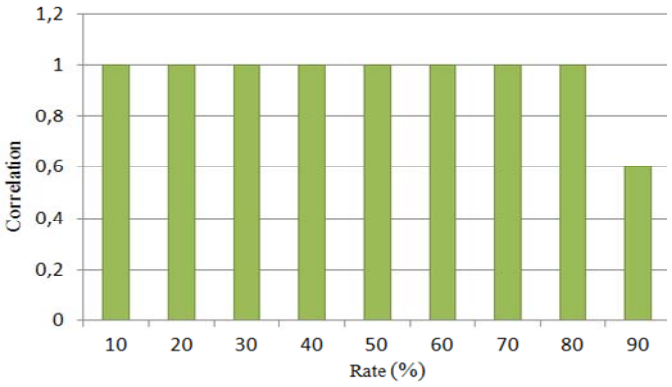

Figure 10. Variation of the correlation value as a function of the compression ratio.

Figure 11 shows the quality (PSNR and wPSNR) of the MRI image after applying a Salt & Pepper noises attack.

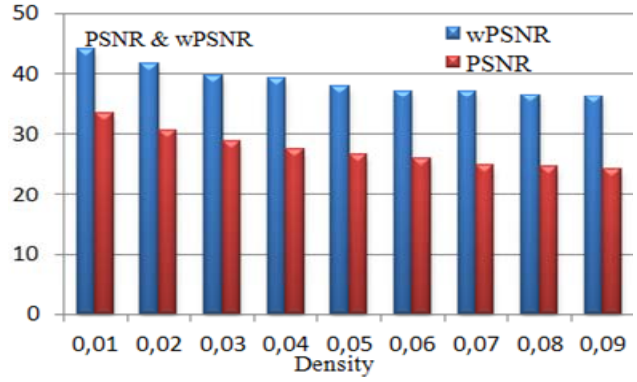

Figure 11. PSNR and wPSNR for MRI images watermarked and attacked by Salt & Pepper noises.

Concerning the robustness, many tests are shown after adding a Salt & Pepper noises attack. Figure 12 shows the correlation factor between the original and the extracted message.

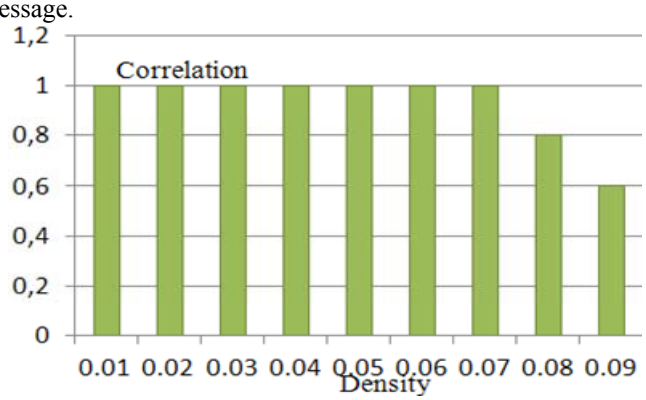

Figure 12. Variation of the correlation value as a function of the impulsionnel noise.

Figure 13 shows the quality of MRI watermarked image robustness of our watermarking schema against median filtering attacks with different windows.

Concerning the error correcting code (figure 14), many tests show that we are able to correct the occurred errors when the tested images get median filtering inferior to 9*9 mask.

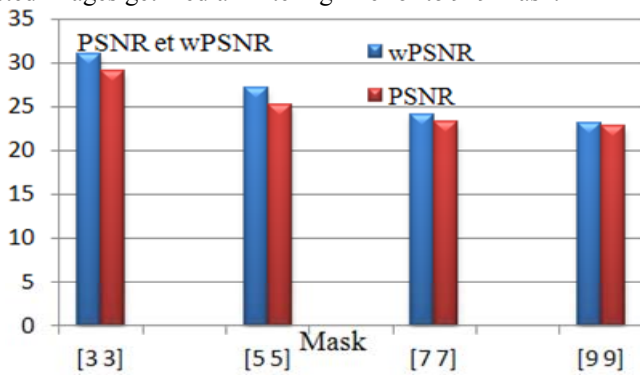

Figure 13. PSNR and wPSNR for MRI images watermarked and attacked by a median filter.

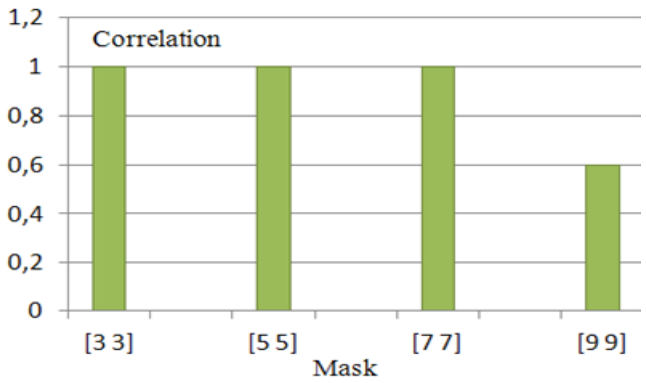

Figure 14. Variation of the correlation value as a function of the median filter.

In what follows, Figure 15 shows the results, in term of visual quality (PSNR and wPSNR), for watermarked test

images attacked by Gaussian noise with zero mean and different variances.

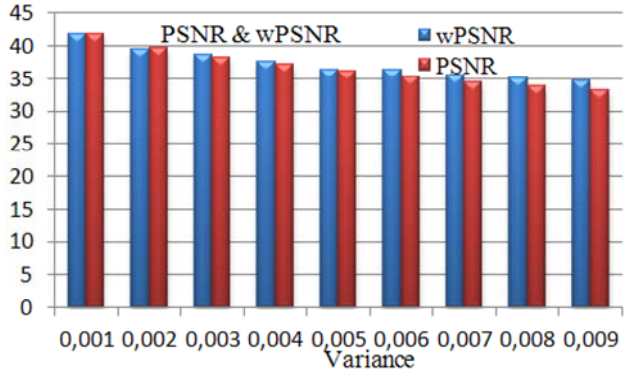

Figure 15. PSNR and wPSNR for MRI images watermarked and attacked by an Gaussian noise.

In the detection phase, and when extract and correct data, these obtained messages underwent alterations. Figure 16 shows the efficiency of our method against attacks by Gaussian noise.

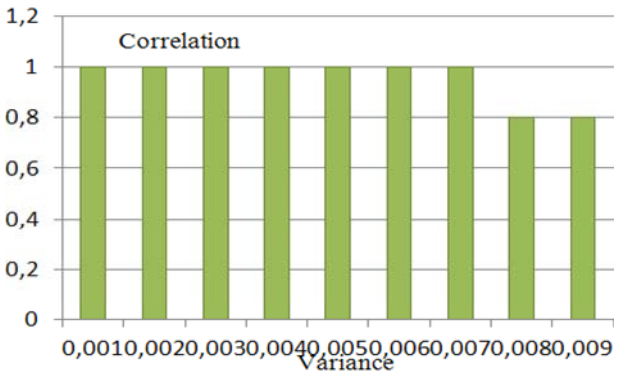

Figure 16. Variation of the correlation value as a function of the Gaussian noise.

IX. CONCLUSIONS

In this paper, we propose a method which deals with medical image watermarking. We aimed at using the DCT space after quantification and the Error Correcting Code. On the other hand, the hash function SHA-1 is used to improve the message integrity and the ECC to increase the security of the message against all types of alterations. The authenticity and the robustness of the received image are verified against different attacks.

To verify the extracted data, we use the correlation technique to extract the data; then we employ the serial turbo-code as an Error Correcting Code, in order to correct the eventual errors that may occur due to different types of attacks.

The insertions of the signature and the patient's recorder using this approach have lead to a good result in terms of image quality of the watermarked image. The robustness of this method is verified for the JPEG compression attack, impulsion noise attack, median filter attack and the Gaussian noise attack.

REFERENCES

[1] M.A. Hajjaji, R. Hajjaji, A. Mibaa and E. Bourennane, "Tatouage des images médicales en vue d'intégrité et de confidentialité des données", fifth Workshop AMINA, 2010, Tunisia.

[2] A. Manoury, "Tatouage d'images numériques par paquets d'ondelettes", Ph.D., university of Nantes, 2001, France.

[3] ITU, "Méthode Recommandation", Union internationale des Télécommunications CCIR 500-4, 1990.

[4] M.A Hajjaji, A. Mtibaa, E. Bourennane, "A Watermarking of Medical Image-New Approach Based On Multi-Layer Method", 33-41, International Journal of Computer Science Issues, Volume 8, Issue 4, July 2011.

[5] P.BAS, "Méthode de tatouage d'images fondé sur le contenu", Ph.D., Thesis at the INP Grenoble, University of Grenoble, 2000,France.

[6] T.Hanène, "Elaboration d'une nouvelle approche de tatouage pour l'indexation des images médicales", Ph.D., University of Rennes 1, 2006, France.

[7] Stephen Gastan. "Channel coding for optical communications". PhD thesis, 2009.

[8] Catherine Douillard ,"Contribution à l'amélioration des performances de systèmes de transmission numériques : Turbo communication et circuits", Habilitation defended in 2004.

[9] "Secure hash standard", Federal Information Processing Standards Publication 180-2, 2002.

[10] Hanène Trichili and al., "Optimizing Image Watermarking Scheme For Better Robustness And More Imperceptibility", 8th World Multiconference on Systemics, Cybernetics and Informatics (SCI 2004).