A Digital Watermarking Algorithm Based on DCT: Application on Medical Image

Mohamed Ali Hajjaji, Sondes Laajili, Abdellatif Mtibaa, El-Bey Bourennane

A Digital Watermarking Algorithm Based on DCT: Application on Medical Image

Mohamed Ali Hajjaji[#1], Sondes Laajili[#2], Abdellatif Mtibaa[#3], El-bey Bourennane[*4],

[#]National *Engineering School of Monastir - TUNISIA*

[1]mohamedali_hajjaji@etu.u-bourgogne.fr

[2]sondesinfo@gmail.com

[3]abdellatif.mtibaa@enim.rnu.tn

[*]*LE2I Laboratory, Burgundy University, Dijon, France*

[4]ebourenn@u-bourgogne.fr

***Abstract*—This work is a presentation of a new approach of robust watermarking applied in medical domain such as telemedicine hence the need to keep the visual aspect of medical images and other conservation of the various data substituted. For hiding information, the proposed method uses the Discrete Cosine Transform (DCT) space.**

To control identification and eventually the correction (if possible) of the data inserted, it should be noted that we used the series turbocode to recover the data inserted and after application of several attacks.

***Keywords*— discrete cosine transform, series turbocode, Medical image, SHA-1, Telemedicine.**

I. Introduction

The evolution of information technology and communication domain offer to the medical sector many opportunities to practise the medicine at distance in order to enhance the quality of life and increase the efficiency of medical services. This practice named "Telemedicine" offers access to patient's records and medical images [1] [2], when these sites are protected by controlling access rights, security is never absolute.

At this step, the watermarking [3] contributes to keep secret to many data own to the patient and the keeping quality of the image. The major problem for the watermarking applied on medical images is on the one hand, to preserve the image quality (the least modification of data contained in images implies a misdiagnosis), and on the other hand, to extracting of the totality of the data after many attacks (the least modification of data extracted implies a misdiagnosis).

In this context, we propose a watermarking method applied on the medical images.

The proposed spaces in this system use the discrete cosine transform (DCT).

II. Evaluation of Watermarking Algorithm

For the evaluation of the watermarking algorithm, many criteria are used. The most important are being 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 [4].

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 [5] [6] [7].

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 [8] 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 will be explained above, but first we present attack that could be composed into two types [9]:

- Innocent Attacks;
- Malicious attacks.

A. Innocent attacks

During the transmission phase, the image undergoes different treatments such as filtering, compression, and geometric transformations. These treatments 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

As shown in figure 1, the proposed method presented in this work combine various tools.

- Information about the patient coordinates, medical center and eventually medical diagnostic are introduced;
- The hash [10] 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 [11], whose aim is to contribute in data security and to the right data extraction after application of several attacks ;
- Discrete cosines transform (DCT) as insertion space.

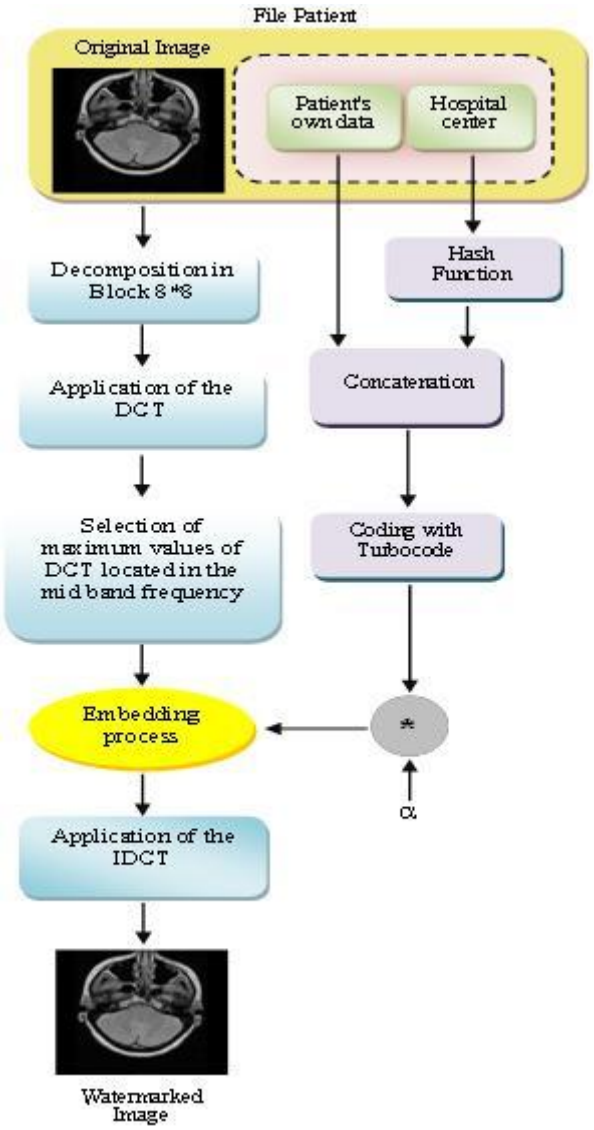

Fig. 1 Embedding process

V. Preparation of Watermark

In our work, the totality of message substituted, in the medical image, contains the signature of the hospital center and the data of the patient.

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

A. Generation of Signature

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

The SHA-1 is a cryptographic [12] hash approach designed by NASA in 1995 as a standard information processing. SHA-1 is a function of this one-way hash. The Secure Hash Algorithm takes a message of less than 2^{64} 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.

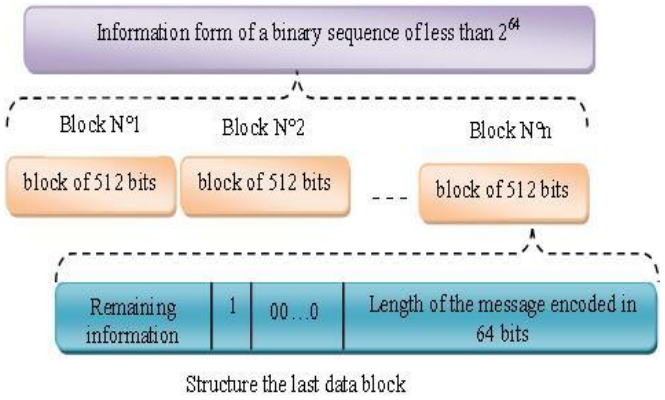

Fig. 2 Decomposition of the message into blocks of 512 bits

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

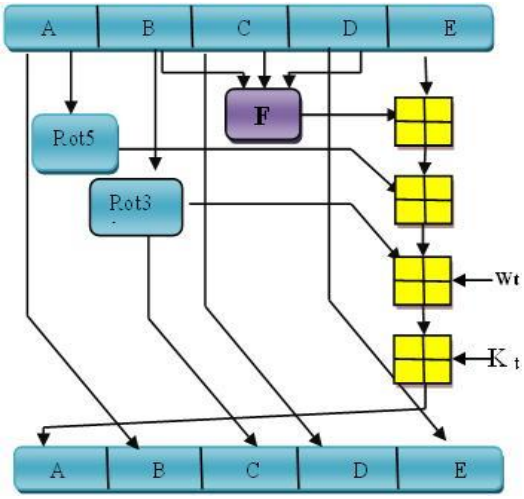

Fig. 3 One iteration within the SHA-1 compression function

With:

- Kt : Constant used in the i^{eme} 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.

B. Error Correcting Code: Serial "Turbocode"

The concept of Turbocode, recently introduced, is approximated to the notion of concatenation of many types of Error Correcting Codes. Indeed, a turbocode is to concatenate two or many ECC generally convolutional separated by an interleaver block. Recalling that a convolutional code is to consider data as an infinite sequence of symbols that must go through a number of memory equal to m+1 on the way to generate a sequence of coded symbols.

For the serial "Turbocode", the idea is to concatenate two or many convolutional codes in serie. These codes are usually separated by an interleaver block. This architecture allows course to break the error packets whose origin is within the decoder in order to facilitate the work of the other decoder said "Exterior".

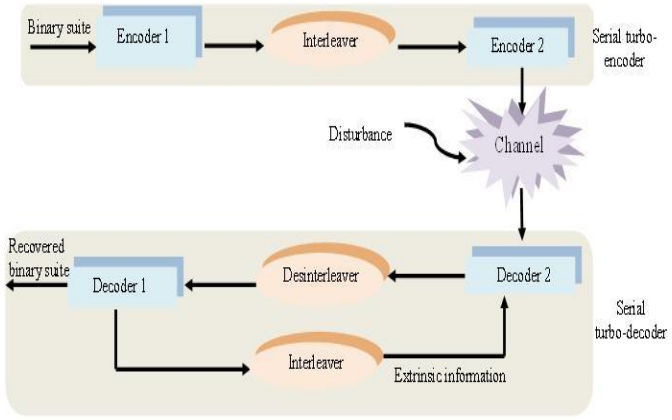

Fig. 4 Serial "Turbocode" diagram

The extrinsic information presented in the diagram above refers to a data set called data of reliability. It is exchanged between the decoders at the end of the correction to improve over the iterations [13].

VI. Preparation of Insertion Space: DCT Space

Discrete Cosines Transform (DCT) [14] is the transformation of choice in the context of image processing. It is the transformation which is by far the most currently used in JPEG compression standards.

The expression of the DCT is:

$$F(k,l)=\frac{2}{N}a(k)a(l)\sum_{m=0}^{N-1}\sum_{n=0}^{N-1}f(m,n)\cos\left[\frac{(2m+1)k\pi}{2N}\right]\cos\left[\frac{(2n+1)l\pi}{2N}\right] \quad (5)$$

with $a(0)=\sqrt{2}/2$ When $k\neq 0$ and $a(k)=1$

The main advantage of the DCT is that it provides good localization of different frequency.

Figure 5 shows the localization of different frequency applied in the portion 8*8 of an image.

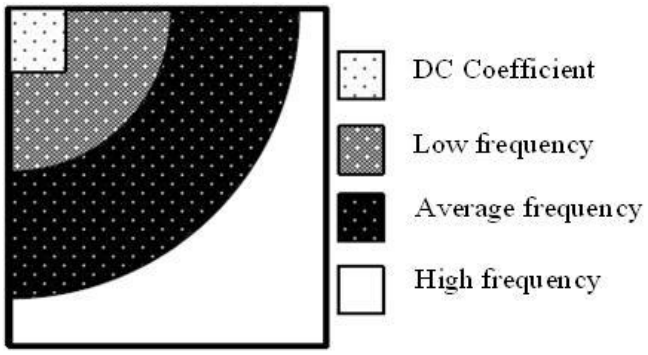

Fig. 5 Transformed into discrete cosine of a block 8*8

In the frequency domain, perceptually significant components generally correspond to low and mid-band frequencies. It is interesting to choose a mid-band frequency ensuring good compromise between the maximum resistance to attack and minimal degradation of image quality. Therefore, the mid-range is retained as a first selection.

VII. Watermarking Schema Description

Our Watermarking Schema is divided into two steps, insertion step and the detection step. For the insertion step, 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. These data will be 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, 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. Using a secret key is chosen by the

different frequencies to support the watermark. The procedure for inserting follows the formula;

$$Y'(i) = Y(i) + \alpha \times message(i) \quad (5)$$

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

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

VIII. RESULTS

The watermarking algorithm with a different IRM, Echographic, and Radiographic images is evaluated.

The message is formed with:

- Signature of hospital center;
- Patient information;
- Diagnostic information.

This algorithm permits to detect the totality of the message inserted in the tested images.

When the tested watermarked image undergoes "copy /past" attack, a message containing the patient's and diagnostic information data in addition to the hospital signature are extracted. But in some images the extracted signature are different from the initial one. About it, we concluded that some alterations have been occurred.

Figure 6, 7 and 8 show measures of PSNR and wPSNR when the visibility coefficient α varies.

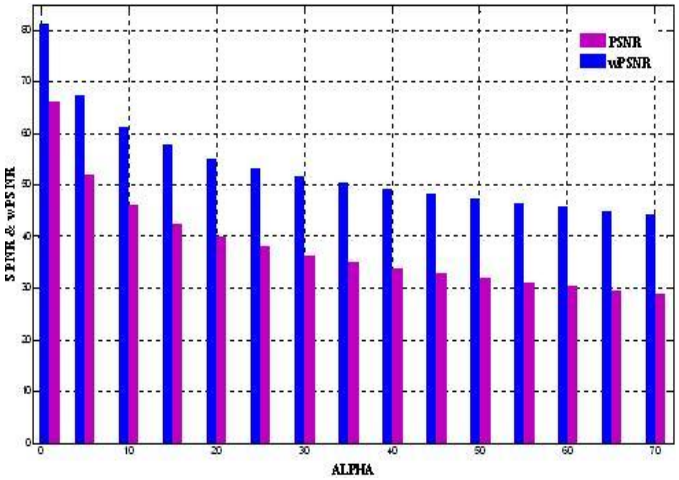

Fig. 6 PSNR and wPSNR for IRM image

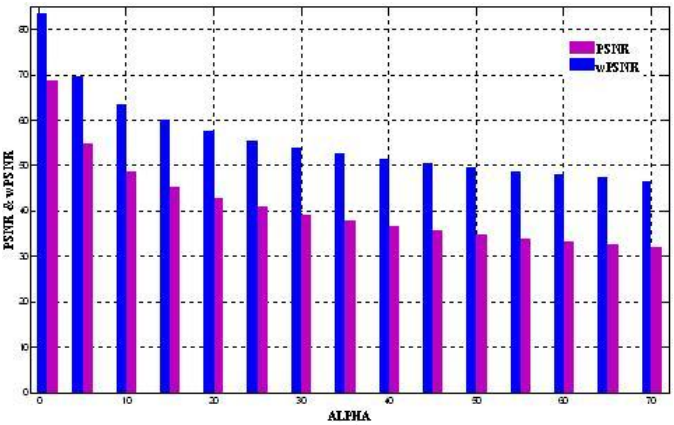

Fig. 7 PSNR and wPSNR for Echographic image

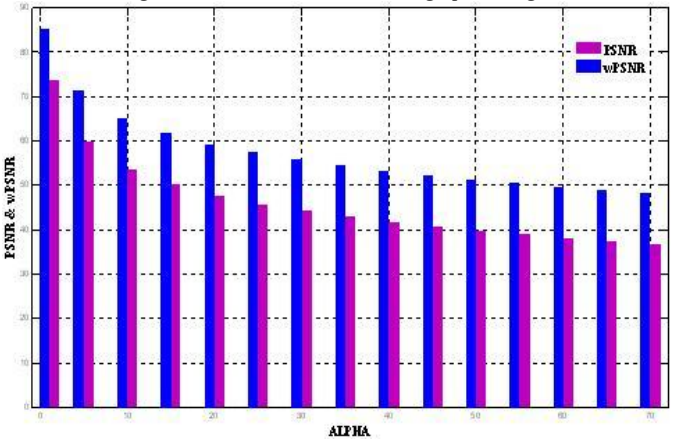

Fig. 8 PSNR and wPSNR for Radiographic image

Figure 9, 10 and 11 show the quality of IRM, Echographic and Radiographic watermarked image robustness of our watermarking schema against JPEG attacks with different rate compression.

Concerning the error correcting code (figure 12), many tests show that we are able to correct the occurred errors when the tested images get compression image rate inferior to 40% for image types IRM and Echographic and 50% for Radiographic image.

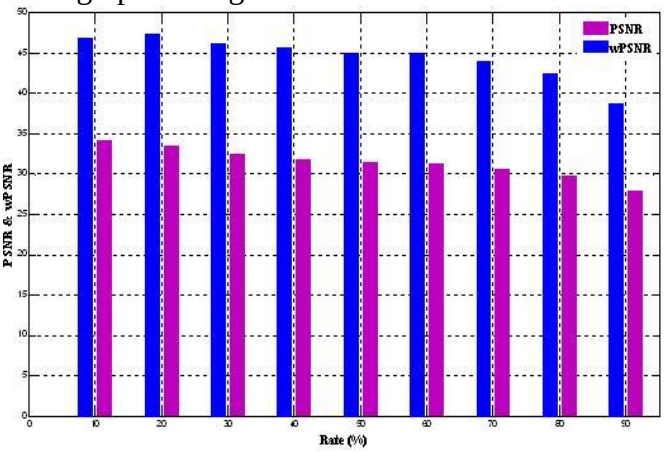

Fig. 9 PSNR and wPSNR for IRM image watermarked and compressed with α=20.

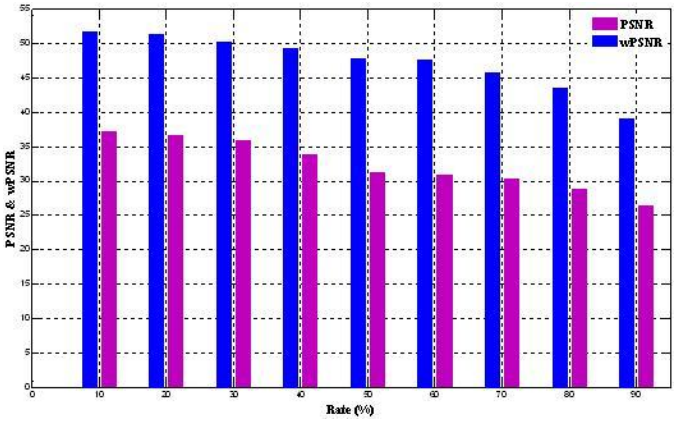

Fig. 10 PSNR and wPSNR for Echographic image watermarked and compressed with α=20

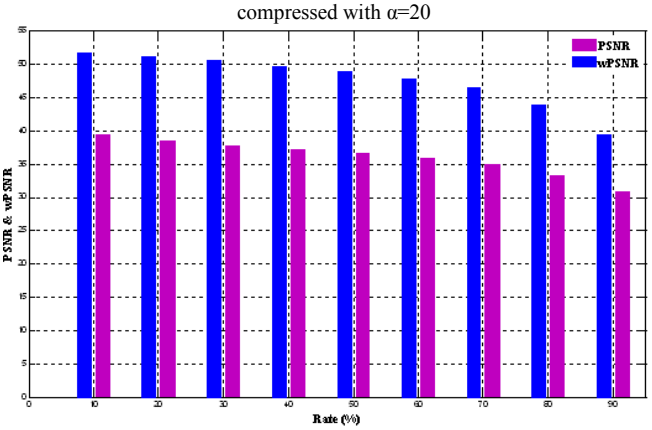

Fig. 11 PSNR and wPSNR for Radiographic image watermarked and compressed with α=20

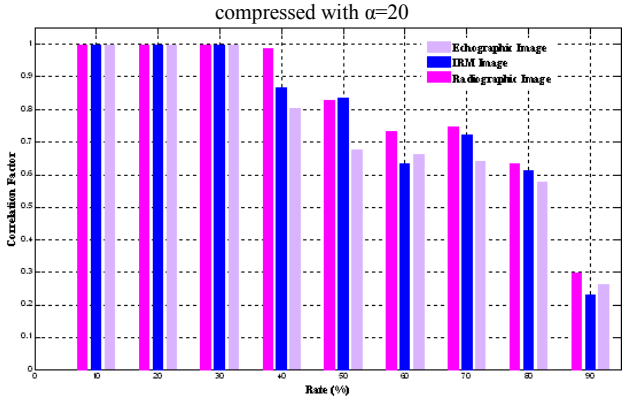

Fig. 12 Remaining errors after correction for IRM, Echographic and Radiographic image with α=20

Figure 13, 14 and 15 show the quality (PSNR and wPSNR) of the IRM,Echographic and Radiographic images after applying an impultionnel noise attack.

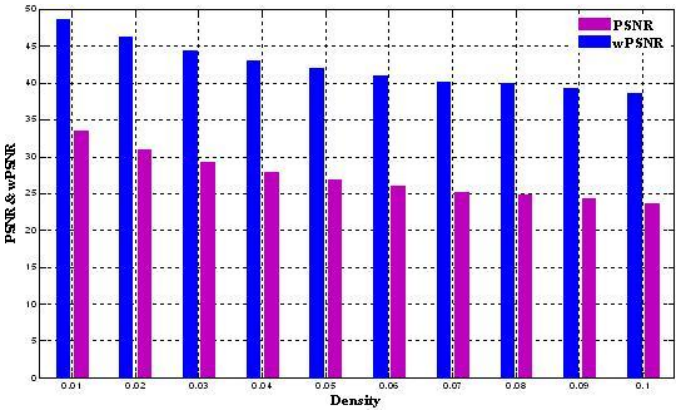

Fig. 13 PSNR and wPSNR for IRM images watermarked and attacked by an impultionnel noise with α=20

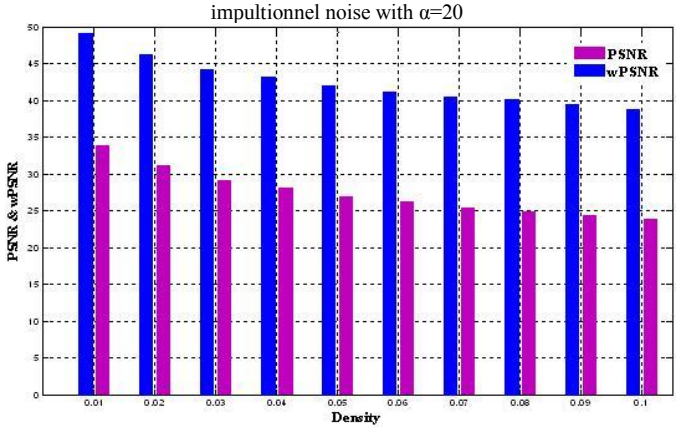

Fig. 14 PSNR and wPSNR for Echographic images watermarked and attacked by an impultionnel noise with α=20

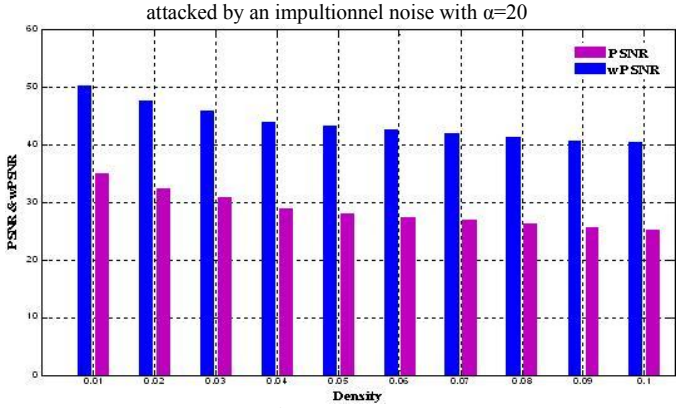

Fig. 15 PSNR and wPSNR for Radiographic images watermarked and attacked by an impultionnel noise with α=20

Concerning the robustness, many tests are shown after adding an impultionnel noise attack.

Figure 16 shows the correlation factor between the original and the extracted message.

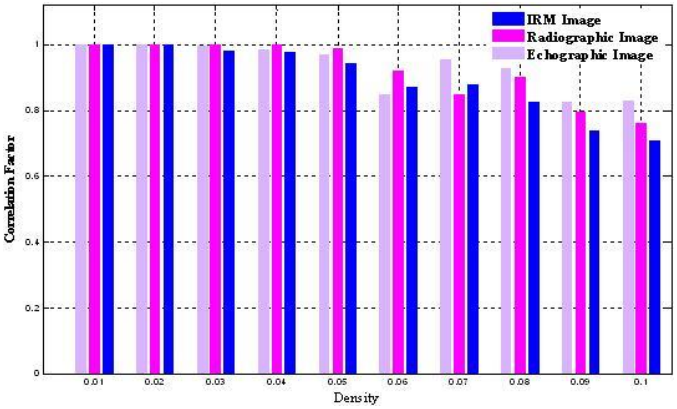

Fig. 16 Remaining errors after correction for IRM, Echographic and Radiographic image attacked by an impultionnel noise with α=20

IX. CONCLUSIONS

In this paper which deals with medical image watermarking, we aimed at using the DCT space 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 data extracted, we use the correlation technique to extract data, we used the serial turbocode 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 "copy/paste" attack, JPEG compression attack and impultionnel noise attack.

REFERENCES

[1] 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, University of Grenoble, 2004, France.

[2] M.A Hajjaji, A. Mtibaa, E. Bourennane , " A Watermarking of Medical Image: Method Based "LSB"", 714-721. Journal of Emerging Trends in Computing and Information Sciences, Volume 2, Issue 12. December 2011.

[3] D.Fadoua, D.Florence, "Tatouage d'images par techniques multidirectionnelles et multi résolution", IRIS, Laboratoire Image Computing and Information Systems, 2004 ,France.

[4] 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.

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

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

[7] 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.

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

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

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

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

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

[13] Stéphane Gastan, "Codage de canal pour les communications optiques ", Thesis, 2009.

[14] Sameh Oueslati and al., "A Fuzzy Watermarking Approach Based on the Human Visual System", 218-231, International Journal Of Image Processing (IJIP), Volume 4, Issue 3.