A Watermarking of Medical Image : New Approach Based On "Multi-Layer" Method

Mohamed Ali Hajjaji, Abdellatif Mtibaa, El-Bey Bourennane

A Watermarking of Medical Image : New Approach Based On "Multi-Layer" Method

Mohamed Ali Hajjaji[1], Abdellatif Mtibaa[2] and El-bey Bourennane[3]

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

[2] Electronics and Microelectronics Laboratory, Monastir University, Tunisia

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

Abstract

In order to contribute to security sharing and transmission of medical images, this paper propose a new approach for Watermarking image based on the techniques of Code Division Multiple Access (CDMA), Discrete Wavelet transform (DWT) and Error Correcting Code (ECC). The motivation of this approach is to improve the quantity of data integration with the conservation of the image visual quality. Therefore, this work permits to the user the capacity to correct the possible alterations if it exists. IRM and Echographic medical image are used to experiment this approach.

Keywords: *Error Correcting Code, Watermarking, Code Division Multiple Access, Discrete Wavelet transform, Medical image.*

1. Introduction

The revolution in technology and communication took place today affects various areas that lead to automate and facilitate the tasks of the working staff. Among the areas most affected, the the medical field that is usually named "telemedicine" is considered in this work.

The approach proposed in this work consists on designing a control and monitoring system in order to protect medical data shared between the hospitals. The idea is then to think about digital watermarking [1].

Indeed, this approach allows patients to insert data into a set of different types of images (IRM, Echography, Radiography…). Obviously, all of the data included (Signature, Address Patient Record, Hospital Signature, Medical Diagnostic) should be hidden, protected and correctly transmitted as the image is been shared between hosts.

2. Approach Presentation

First, information about the patient coordinates, medical center coordinates and eventually medical diagnostic are introduced. This information is organized, in data message, as shown in Fig.1.

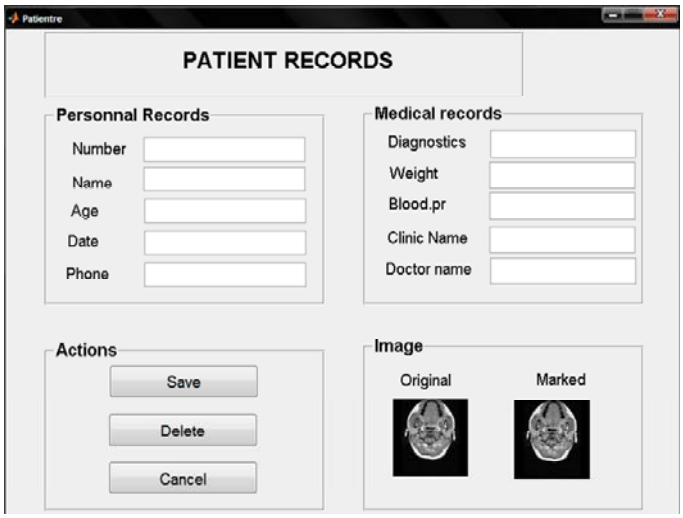

Fig. 1 User interface for medical data introduction.

Then, the message is treated in two steps:

Step 1: Data Insertion:

As shown in Fig.2, once information has been introduced by user, the step of data insertion in the medical image begins.

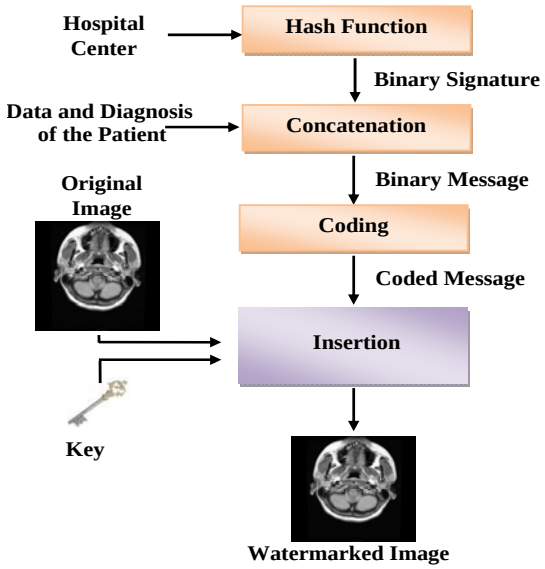

Fig. 2 Data insertion.

First, using the MD5 algorithm (Message Digest algorithm) [2], the binary signature of the hospital center is generated. This signature coded in 128 bits is concatenated with the full data of the patient and the medical diagnostic result to form a message to be inserted in the image.
This message is coded by the error correcting code. In the proposed approach, The BCH (Bose, Ray-Chaudhuri and Hocquenghem) [3] is used in order to protect the message from alteration resulting on different attack. At this step, the coded message, the key and the original image are done, the watermarking can be started.
In the reception, the watermarked image is obtained. This image may be altered as a result on different attacks. The next step on this approach consists in extracting the message from the watermarked image.

Step 2: Data Detection:

As shown in Fig.3, the detection is partitioned into 3 main parts:
Using the secret key, the message is extracted from the received image.
Then the BCH algorithm is used to verify the conformity of the obtained message and correct the possible alterations if they exist.
After that, the hospital center signature from the patient information is separated.
Finally, the signature is identified using a signatures database that leads to control the authenticity of the image.

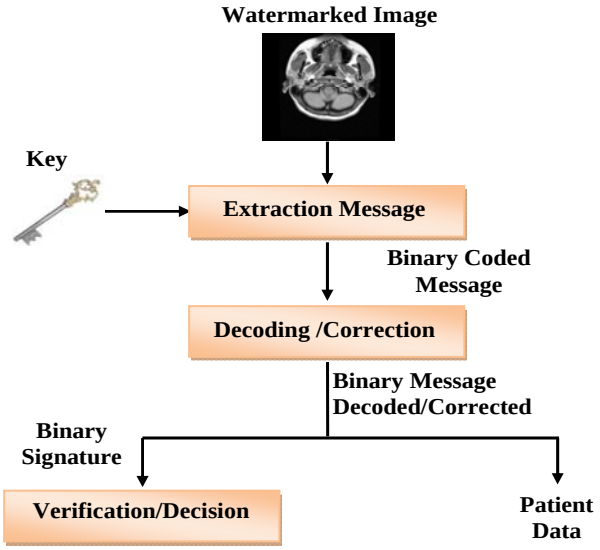

Fig. 3 Data detection.

CDMA Method [4]: to improve the rate of data integration.
The Error Correcting Corrector BCH: to contribute to the data confidentiality, data verification and eventually error correction.
The Wavelet Transform [5]: defines the domain where the insertion will be done.
The MD5 Method: to generate the hospital center signature and verify the authenticity of the received medical image.

2.1 CDMA Method

CDMA is a frequently used method in data transmission. This method consists in mixing different signal s in emission and detecting them in reception [6].
The CDMA uses the spectral dilatation of the signal which is transformed from a reduced spectral space signal to a noise-like signal with a large spectral band [7].
In this method, each bit equal to "1" is replaced by an M-sequence symbol, and each bit equal to "0" by a complimentary M-sequence symbols.
These sequence symbols should be chosen in respect to some mathematical proprieties.
In reception, a correlation between the received signal and a replication of the random code permits to generate the message bits by using the sign of the signal-values.
In respect to the compromise between the data integration rate and the quality of the watermarked image, many experiences are being and they prove that using 8 layers permit to give a good result.

2.2 Error Correcting Code

In order to contribute to robustness, performance and effectiveness of the data transmission, the patient's coded information should be secure and reliable.
The error correcting code is chose to deal with the problem of the alteration when receiving the signal. These alterations are due to different attacks when the signal is transmitted in the canal.
The error correcting code consists on adding to the signal supplementary bits as redundancy that permits to detect and eventually correct the signal errors.
In this approach, the BCH (Bose, Chaudhuri and Hocquenghem) is chose to work with which is a case of using a binary data in the Reed-solomon (RS) code.
A "RS" code (n ,k, d) leads to BCH code (n', k', d') with n' is the length of the coded word and it is equal to n. and k' is the initial code dimension and d' represents the minimal of the hamming distance that is superior to d [8].
It is necessary to note that the BCH code permits to correct a number of errors 't' between:

$$\frac{n'-k'}{m} \text{ and } \frac{n'}{2} \text{ with } n' = 2^m - 1 \quad (1)$$

2.2.1 Galois Field

For better understanding, a brief definition for Galois field is needed. For each integer q, we call a Galois field with defined arithmetic operators as a set of integers modulo q.
The BCH filed is defined with a binary data group:
GF(2) = {0,1}. This BCH field contains an "Or-exclusive" operator for addition and an 'And' operator for multiplication. In other hand, a superior order set is used: GF(q^m) with m is an odd number. This field has the same proprieties as the first even though; q is obtained by using a 'm' degree irreducible polynomial.

Propriety 1:

P(x) is an m degree irreducible polynomial. GF (QM) is a BCH field defined by P(x).
The polynomial p(x) does not contain roots in GF (q^m) field but it has a set of roots out of the field. We note "α" a root of this polynomial. The set of roots is:

$\{\alpha^0, \alpha^1, ..., \alpha^{q^m-2}\}$.

Propriety 2:

If α is a root for GF (q^m) then $\alpha^i \times \alpha^j = \alpha^{(i+j) \bmod (2^m-1)}$ is a root.

2.2.2 Coding [9]

In order to code a message in BCH field, a predefined polynomial which is named generator polynomial is used.
The code word is defined as a result of the Galois filed multiplication. The Galois field used is the field in which the root of the generator polynomial exits.

2.2.3 Decoding

The decoding step needs a set of algebraic operations such as: Given a p(x) polynomial that presents the received word.
The decoding step needs a set of algebraic operations such as: Given a p(x) polynomial that presents the received word.

Step 1:

Compute the syndrome: $S_1 = p(\alpha^1)$, $S_2 = p(\alpha^2)$, … $S_{2t} = p(\alpha^{2t})$ with 't' the number of errors that the code may correct.

Step 2:

If the syndrome is null, the received message is correct and without errors and the algorithm is ended otherwise, go to the step 3.

Step 3:

The number of errors that has taken place is calculated. It is noted δ. δ corresponds to the rank of the following matrix:

$$\begin{pmatrix} S_1 & \cdots & S_t \\ \vdots & \ddots & \vdots \\ S_t & \cdots & S_{2t-1} \end{pmatrix} \quad (2)$$

Step 4:

Depending on the number of errors, we solve the following system:

$$\begin{pmatrix} S_1 & \cdots & S_t \\ \vdots & \ddots & \vdots \\ S_t & \cdots & S_{2t-1} \end{pmatrix} \times \begin{pmatrix} \zeta_{\delta+1} \\ \vdots \\ \zeta_{2\delta} \end{pmatrix} = \begin{pmatrix} S_{\delta+1} \\ \vdots \\ S_{2\delta} \end{pmatrix} \quad (3)$$

Step 5:

Calculate the δ roots:
$\alpha^{-i_1}, ..., \alpha^{-i_\delta}$ corresponding to the polynomial M(x) defined as:

$$M(x) = \zeta^\delta \times X^\delta + \cdots + \zeta^1 \times X^1 \quad (4)$$

Step 6:

The errors take place in the positions $i_1,\ldots, i_\delta$, and these bits corresponding to the preceding positions would be reversed.

2.3 Multi-resolution Approach

As shown in Fig.4, the multi-resolution consists in presenting an image in several levels of resolution [10]. Given the original image I, and after N level decomposition, we will get two spaces:
The first named D-Space which corresponds to the details space (D_1, D_2, D_3 ...D_N) .This space is obtained by extracting the high frequencies from the initial image.
The second space named A-space is the approximation space (A_1, A_2, A_3 ... A_N), it represents the lows frequencies signals extracted from the original image I.
Each image from the N levels-image and belonging to one of the preceded spaces, corresponds to a defined\ frequency-band image level.

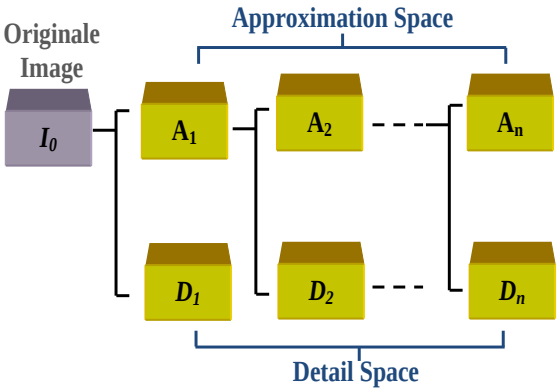

Fig. 4 Principe of multi-resolution approach.

2.3.1 Contribution of Wavelet 5/3

Wavelet 5/3 permits to work in the multi-resolution domain instead of the spatial domain [11]. They are based on the use of two types of filters, the first is a 5 order high-pass filter and the second is 3order low-pass filter.
Indeed, this type of wavelet requires a short computing time. These wavelets are reversible, conservative and frequently used in the JPEG2000 standard [12].
The equations of decomposition and reconstruction wavelet 5/3 are as follows:

Decomposition:

$$d[n] = d_0[n] - \left\lfloor \frac{1}{2}(s_0[n+1] + s_0[n]) \right\rfloor \quad (5)$$

$$s[n] = s_0[n] - \left\lfloor \frac{1}{4}(d[n] - d[n-1]) + \frac{1}{2} \right\rfloor \quad (6)$$

With: $S_0[n]=X[2n]$;
$d_0[n]=X[2n+1]$;
X: input signal.

Reconstruction:

The image reconstruction is based on the use of the application of the following two equations called twice GALL [12]:

$$d_0[n] = d[n] + \left\lfloor \frac{1}{2}(d[n] + d[n-1]) \right\rfloor \quad (7)$$

$$s_0[n] = s[n] + \left\lfloor \frac{1}{4}(d[n] + d[n-1]) + \frac{1}{2} \right\rfloor \quad (8)$$

3. 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 [12]:
• Innocent Attacks;
• Malicious attacks.

3.1 Innocent attacks

During the transmission phase, the image undergoes different treatments such as filtering, compression, geometric transformations. These treatments are classified as innocent attacks.

3.2 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 concern jittering, extra marking attack, and copying attack, mosaics attacks...

4. Evaluation of Watermarking Algorithm

Many criteria are used to evaluate the watermarking algorithm. 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 is evaluated with two types of measures [13]:

4.1 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 [14] [15]:

Table 1: Index of appreciation scale for image quality

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

Subjective measures are however costly, especially if you work with a large set of medical images.

4.2 Objective measures

Objective measures are based on the comparison between the original image and the received watermarked image. From these measures, we find the relative entropy, the mean squared error, the average absolute error, the Peak Signal to Noise Ratio (PSNR) and the weighted PSNR.

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:

$$(SNR)_{dB} = 10log_{10}\left\{\left[\frac{\sum_{i,j} I^2(i,j)}{\sum_{i,j}[I(i,j) - I_w(i,j)]^2}\right]\right\} \quad (9)$$

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

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 [16] is defined by the following formulas:

$$(wPSNR)_{dB} = 10log_{10}\left\{\frac{maxI^2(i,j)}{\sum_{i,j}\left[\frac{I(i,j) - I_w(i,j)}{1 + Var_I(i,j)}\right]^2}\right\} \quad (11)$$

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.

5. Watermarking Schema Description

Our Watermarking Schema is divided into two steps:

5.1 Insertion step

1. Compute the hospital signature center using 128-bit MD5 as a hash function.
2. Concatenate the signature that contains the patient-information and diagnostic data. These data will be transformed into binary message and encoded using the error correcting codes (BCH).
3. The standard JPEG2000 is the fifth level of decomposition, but in the insertion stage we stop at the second level of the decomposition in order to increase the insertion capacity. And then, we extract the 3 bands of details (horizontal, vertical and diagonal).
4. From a master key, we generate 24 different keys. They allow us to obtain 24 pseudo-random sequences (SPBA1, SBPA2... SBPA24).
5. The data to insert will be divided into 3 equal parts that correspond to the details bands (horizontal, vertical and diagonal). Each part will be divided into 8 blocks corresponding to the number of layers.
6. Each sub block is composed by adding (+SBPA) if we have "1" in the message and (-SBPA) if we have "0". Then, 8-square matrixes are obtained. These matrixes will be superposed to form the final watermark.

All of these steps are illustrated in the Fig.5.

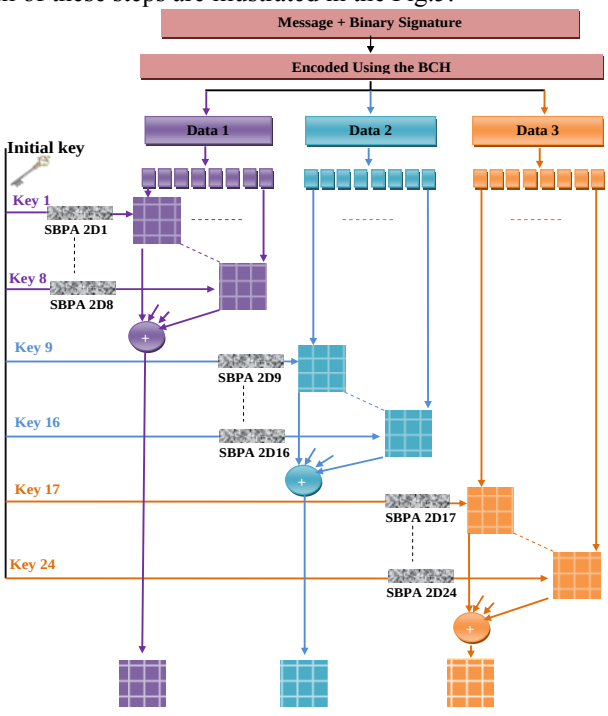

Fig. 5 Construction of all the marquees in a scheme to 8 layers.

Once the watermark message is constructed, the data obtained will be watermarked in the original image.
The watermarking process is done in 3 steps as shown in Fig.6:

1. The obtained matrixes will be multiplied by a visibility coefficient α.
2. Add each detail (vertical, horizontal, diagonal) to each resulting matrixes.
3. Reconstruct the watermarked image by applying the inverse wavelet-transform.

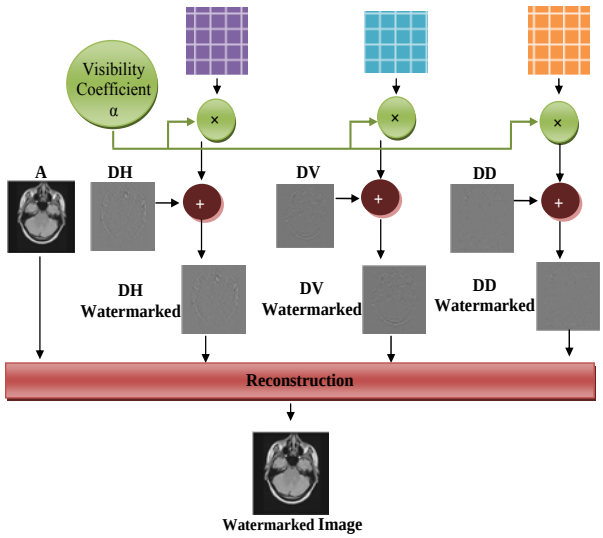

Fig. 6 Watermarked insertion algorithm.

5.2 Detection Step

In order to extract the image signature, use the inverse steps of the insertion phase is proposed.
With the principal key, a same-sized image matrix is generated.
This matrix is formed by a sequence of SBPA. Then, multiplication pixel by pixel is used between the SBPA matrix and the watermarked image as it is shown in the bellow Fig.7.
Finally, the message that is inserted in the watermarked image is extracted [17].

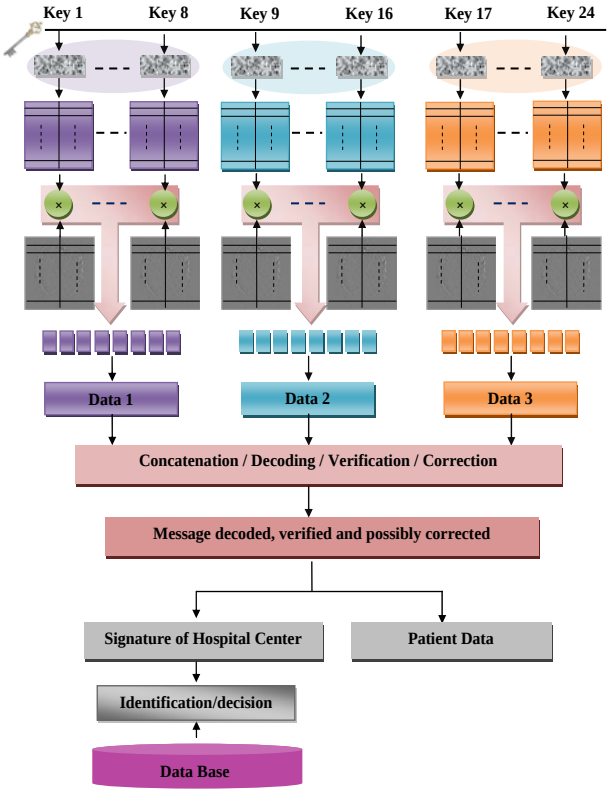

Fig. 7 Watermarked extraction algorithm.

6. Results

The watermarking algorithm with a different IRM and Echographic 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 alteration have been occurred
The Fig.8 and Fig.9 show measures of PSNR and wPSNR when the visibility coefficient α varies.

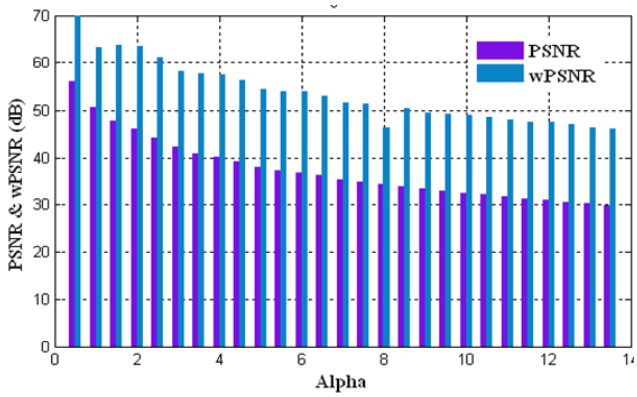

Fig. 8 PSNR and wPSNR for IRM image.

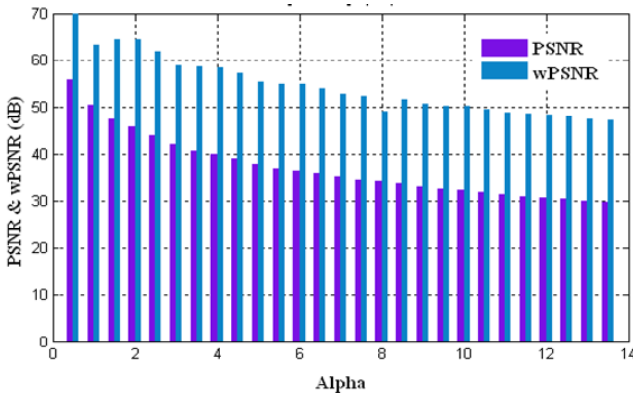

Fig. 9 PSNR and wPSNR for Echographic image.

Fig.10 and Fig.11 show the quality of IRM and Echographic watermarked image robustness of our watermarking schema against JPEG attacks with different rate compression. For rate compression equal to 90%, 80%, 70% and 60%, the watermark is successfully recovered (for the two types of medical images).
Concerning the error correcting code (Fig.12), many tests show that we are able to correct the occurred errors when the tested images get compression image rate inferior to 50%.

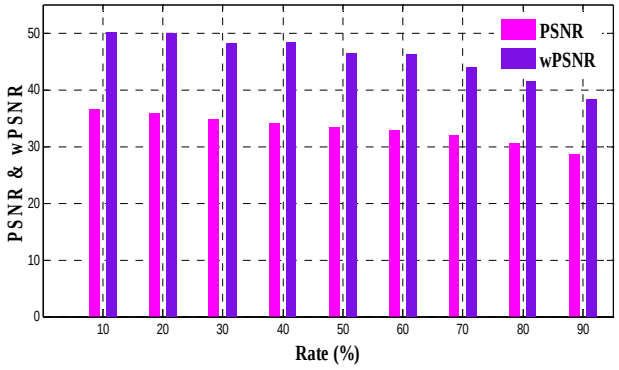

Fig. 10 PSNR and wPSNR for IRM image watermarked and compressed.

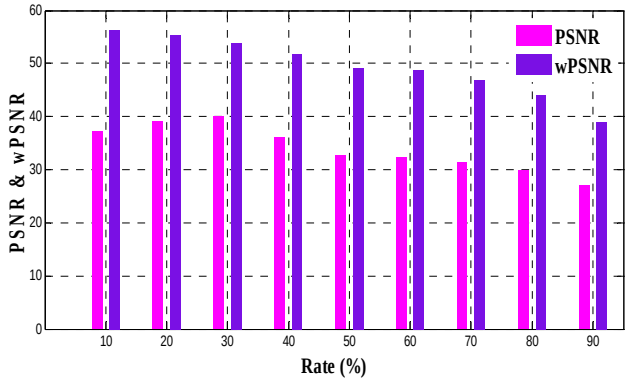

Fig. 11 PSNR and wPSNR for Echographic image watermarked compressed.

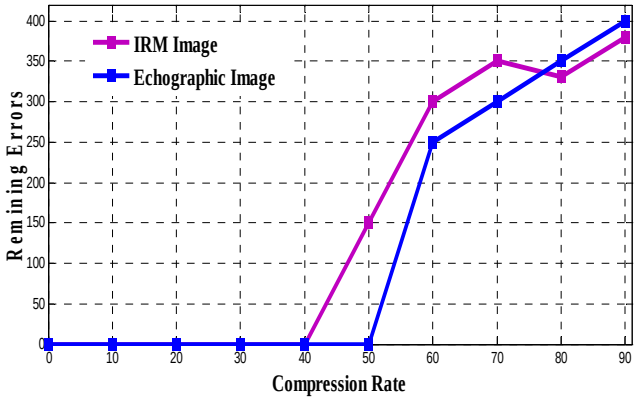

Fig. 12 Remaining errors after correction for Echographic and IRM image with α=5.

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

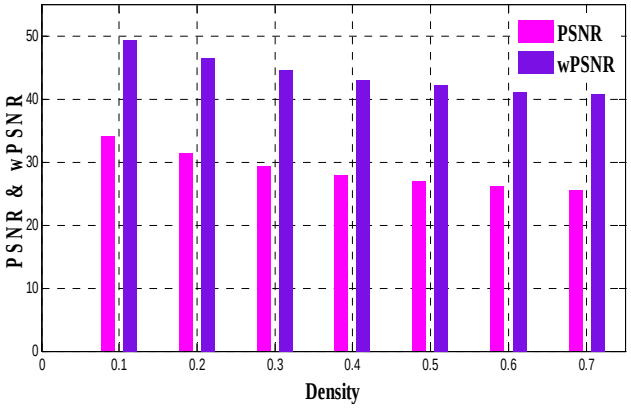

Fig. 13 PSNR and wPSNR for IRM images watermarked and attacked by an impultionnel noise.

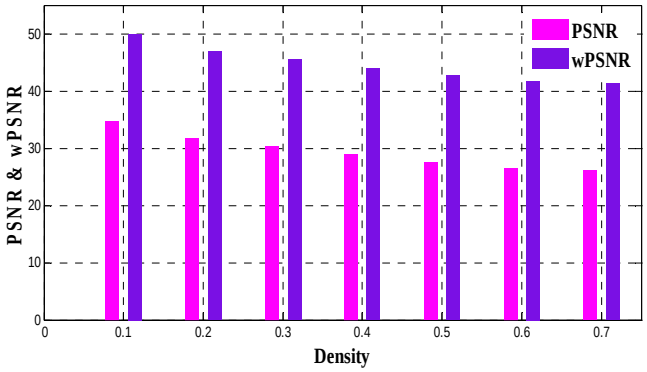

Fig. 14 PSNR and wPSNR for Echographic images watermarked and attacked by an impultionnel noise.

Concerning the robustness, many tests show that after adding an impultionnel noise attack, all inserted data are extracted, verified and corrected.
In what follows, Fig.15 and Fig.16 show the results, in term of visual quality (PSNR and wPSNR), for watermarked test images attacked by Gaussian noise with zero mean and different variances.

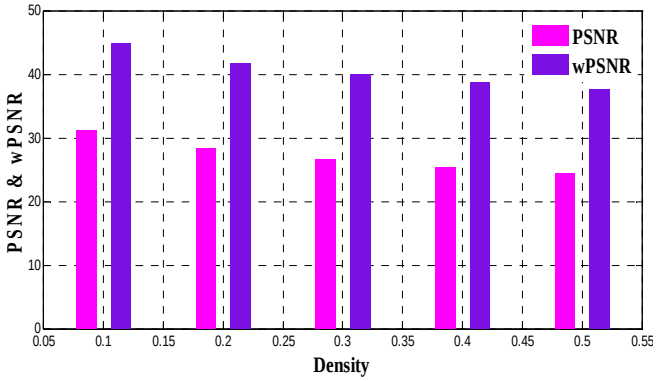

Fig. 15 PSNR and wPSNR for IRM images watermarked and attacked by a Gaussian noise.

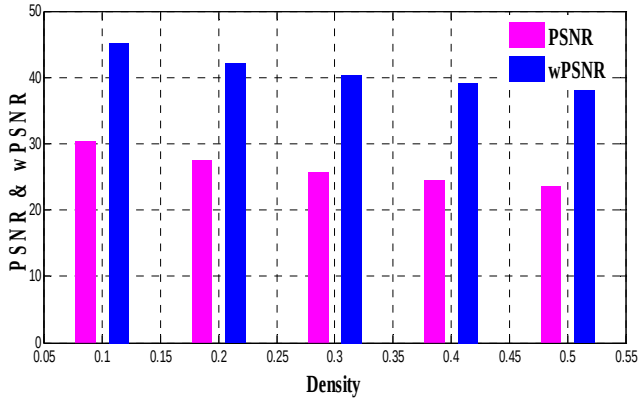

Fig. 16 PSNR and wPSNR for Echographic images watermarked and attacked by a Gaussian noise.

In the detection phase, and when extract and correct data, these obtained messages underwent alterations. Fig.17 shows the inefficiency of our method to face such attacks.

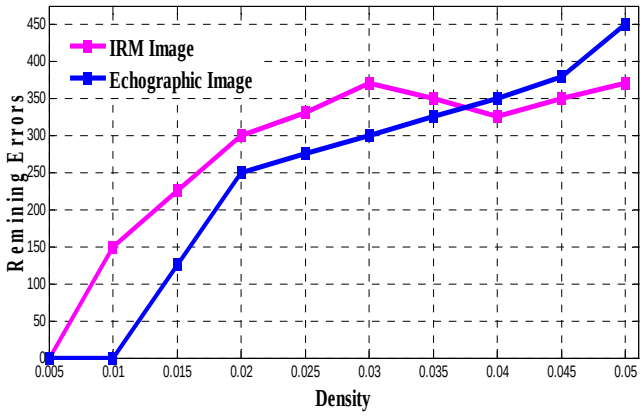

Fig. 17 Remaining errors after correction for Echographic and IRM image with α=5.

7. Conclusions

In this paper, which deals with medical image watermarking, we aimed using the "multi-layers" method. On the other hand, the hash function MD5 is used to improve the message integrity and the CDMA to increase the number of bits to insert. The authenticity and the robustness of the received image are verified against different attacks.
Despite using the correlation technique to extract data, we used the BCH 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 1536 bits using this new 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 2000 compression attack, and impultionnel and Gaussian noise attack.
Our method gives us a good result in the case of "copy/paste" attack, impultionnel noise attack and the JPEG 2000 compression when we are limited to 50% as a rate of compression.
On the other hand in the case of Gaussian noise attack the received message undergoes different alterations.
The major inconvenient of this method consist in the use of different layers, key, and this becomes binding with a large number of images.

References

[1] D.Fadoua, D.Florence, "Tatouage d'images par techniques multidirectionnelles et multi résolution", IRIS, Laboratoire Image Computing and Information Systems, 2004.
[2] Ondrej Mikle, "Practical Attacks on Digital Signatures Using MD5 Message Digest", Department of Software Engineering, Faculty of Mathematics and Physics, Charles University, Prague, Czech Republic, 2004.
[3] Abbas Z. Kouzani, Gulisong Nasireding, "Multilabel Classification by BCH Code and Random Forests", International Journal of Recent Trends in Engineering, 2009, Vol 2, pp. 113-116.
[4] Santi P. Maity, Malay K. Kundu, "A blind CDMA image watermarking scheme in wavelet domain", IEEE 2004.
[5] P. Valérie, "Transformée en Ondelettes Continue Directionnelle: applications en Imagerie Médicale", 2007, Vol.18
[6] Jack Raymond, David Saad, "Sparsely spread CDMA—a statistical: mechanics-based analysis", Journal of physics a: mathematical and theoretical, 2007.
[7] G. Philippe, "Accès Multiples par Répartition de Code : des Réseaux sans Fils aux Réseaux Optiques", 18ème colloque international optique hertzienne et diélectriques, 2005-Tunisie.
[8] C.S Stéphanie "Codage de canal pour les communications optiques", Université Paul Verlaine-Metz, 2009.
[9] H.Jaber, "Conception architecturale haut débit et sûre de fonctionnement pour les codes correcteurs d'erreurs", Ph.D., Ecole doctorale IAEM – Lorraine, 2009.
[10] M.D. Adams, "Reversible Integer to Integer Wavelet Transforms for image compression: Performance evaluation and Analysis", IEEE Trans. on Image Processing, Vol. 9, 2000.
[11] F.Imen, "Elaboration d'une nouvelle approche de tatouage fragile des images médicales", 3rd International Conférence : Sciences of Electronic, Technologies of Information and Telecommunications, 2005.
[12] T.Hanène, "Elaboration d'une nouvelle approche de tatouage pour l'indexation des images médicales", Ph.D., Université de Rennes 1, 2006.
[13] H. Mohamed Ali, "Tatouage des images médicales en vue d'intégrité et de confidentialité des données", Cinquième Workshop Amina, Tunisie 2010.
[14] A.Manoury, "Tatouage d'images numériques par paquets d'ondelettes", Ph.D., université de Nantes, 2001.
[15] "Méthode d'évaluation subjective de la qualité des images de télévision", Recommandation CCIR 500-4, Union internationale des Télécommunications (ITU), 1990.
[16] P.BAS, "Méthode de tatouage d'images fondé sur le contenu", Ph.D., INP Grenoble, 2000.
[17] Boris vasseau, "Codage et insertion des messages pour le tatouage des images", M.S, INP Grenoble, 2000.

Mohamed Ali Hajjaji received the degree in Electronics from Monastir University, Tunisia in 2007. In 2009 he received his M.S degree in Electronics and Micro-Electronics from Monastir University, Tunisia. He is currently preparing his PhD degree in the Electronics and image processing from the Le2i laboratory, from Burgundy University, France.

Abdellatif Mtibaa is currently Professor in Micro-Electronics and Hardware Design with Electrical Department at the National School of Engineering of Monastir and Head of Circuits Systems Reconfigurable-ENIM-Group at Electronic and microelectronic Laboratory. He holds a Diploma in Electrical Engineering in 1985 and received his PhD degree in Electrical Engineering in 2000. His current research interests include System on Programmable Chip, high level synthesis, rapid prototyping and reconfigurable architecture for real-time multimedia applications. Dr. Abdellatif Mtibaa has authored/co-authored over 100 papers in international journals and conferences. He served on the technical program committees for several international conferences. He also served as a co-organizer of several international conferences.

El-Bay Bourennane Received his degree in Telecommunications Engineering from Sétif University (Algérie) in 1990 and he received his DEA in Signal Processing Image and Parole from Grenoble school of Engineering and Phd training (INPG). He received his Ph.D. in image processing from Burgundy University (BU), France. He is currently a Professor in Bourgogne University.