International Journal of Sciences and Techniques of Automatic control & computer engineering
IJ-STA, Volume 6, N° 1, June 2012, pp. 1764–1781.

Fragile Method for Watermarking of Medical Image: Method Based LSBs

Mohamed Ali HAJJAJI[1,3], Sondes AJILI[1],
Abdellatif MTIBAA[1,2], El-bey BOURENNANE[3]

[1]Electronics and Microelectronics Laboratory, University of Monastir, Tunisia.
[2]National Engineering School of Monastir, University of Monastir, Tunisia.
[3]LE2I Laboratory, Burgundy University, Dijon, France.

mohamedali_hajjaji@etu.u-bourgogne.fr, sondesinfo@gmail.com,
abdellatif.mtibaa@enim.rnu.tn, ebourenn@u-bourgogne.fr

Abstract

This paper presents a new fragile watermarking method applied to spatial domain of medical image. The proposed method uses the spatial domain of medical image; the pixels that carry the message to be inserted will be selected using Harris corner detector, and by secret key choose the locations where to embed the watermark. The purpose of the watermarking method is to check the integrity and preservation of the confidentiality of patient data in a network sharing. This approach is based on the use the LSBs (least significant bits) of the image and tools borrowed from cryptography.

Keywords. *Fragile Watermarking Method, LSBs, Confidentiality, Medical Image, Telemedicine.*

1 Introduction

The evolution of information technology and communication offer to the medical sector many opportunities to practice the medicine at distance in order to enhance the quality of life and increase the efficiency of medical services in particular in rural areas. This practice named "Telemedicine" can be applied through the Internet, using sites which offer access to patient's records and medical images. While these sites are protected by controlling access rights, security is never absolute.

At this point, the watermarking technique contributes to keep secret the identity of the patient and monitor the integrity of the medical image to deal with access and manipulation. Many methods have been proposed in the medical domain. Their shared concern is to preserve the quality of the watermarked image.

In fact the medical image, given its characteristics, must be manipulated with extreme caution because any degradation could result in an erroneous diagnostic.

In this context, we propose a watermarking method for medical images based on the least significant bits (LSBs) [1] , in order to check the integrity and confidentiality of medical information and maintain confidentiality for patient and

This paper was recommended for publication in revised form by the editor Staff.
Edition: CPU of Tunis, Tunisia, ISSN: 1737-7749

hospital data.
Indeed, this approach allows patients to insert data into a set of different types of images (IRM, Radiographic and Echographic). Obviously, all of the data included (Signature, Address, Patient Record, Hospital Signature) should be hidden, protected and correctly transmitted.
The paper is set up as follows:

- The following section shows the different criteria for evaluating a scheme of watermarking namely those known as subjective and objective measures.
- The fourth part is a presentation of tools and algorithms that will be used in our proposed method.
- The fifth part is a presentation of our proposed watermarking method.
- Our paper will end up in a conclusion on our proposed approach.

2 Evaluation of Watermarking Algorithm

For 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[2].

2.1 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[3][4][5].

Table 1: Index of appreciation scale for image quality.

N*ote*	*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.

2.2 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.

2.2.1 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:

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

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

2.2.2 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 [6] is defined by the following formulas:

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

With $var_{\mathrm{(i,j)}}$representing the local variance of pixel(i,j), $I_{\mathrm{(i,j)}}$ the intensity value for the pixel(i,j) from the original image and $I_{\mathrm{w(i,j)}}$ the intensity value for the pixel of the image in test. M and N are respectively the height and width of the image.

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 the attack that could be divided into two types [7] namely, innocent attacks and malicious attacks.

3.1 Innocent attacks

During the transmission phase, the image undergoes different treatments such as filtering, compression, geometric transformations. These treatments are considered 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 the signature of the watermarked image and this will lead to the loss of the coded data. Malicious attacks concern jittering, extra marking attack, and copying attack, mosaics attacks, etc.

4 Tools and Algorithms

4.1 Harris Corner Detector

The Harris corner detector was developed to allow reconstructions 2D/3D [8]. The corners are usually defined as the points where the gradient is high in different directions. This definition leads to detectors of corners based on the local derivatives (usually the first or second order) of the image.
To extract the interesting points in an image, it is recommended to calculate the matrix M for each pixel:

$$M(x,y) = \begin{bmatrix} A_{x,y} & C_{x,y} \\ C_{x,y} & B_{x,y} \end{bmatrix} = \begin{bmatrix} \left(\frac{\partial I(x,y)}{\partial x}\right)^2 & \left(\frac{\partial I(x,y)}{\partial x}\right)\left(\frac{\partial I(x,y)}{\partial y}\right) \\ \left(\frac{\partial I(x,y)}{\partial x}\right)\left(\frac{\partial I(x,y)}{\partial y}\right) & \left(\frac{\partial I(x,y)}{\partial y}\right)^2 \end{bmatrix} \tag{4}$$

where $\frac{\partial I(x,y)}{\partial x} \approx I\,(x,y)*[-1,0,1]$, $\frac{\partial I(x,y)}{\partial y} \approx I\,(x,y)*[-1,0,1]^T$, with $'*'$ denotes the convolution product.
The corner points are located at the positions with large corner response values, which are determined by the corner response function R(x,y) :

$$R(x,y) = \det\left(M(x,y)\right) - k\left[trace\left(M\left(x,y\right)\right)\right]^2 \tag{5}$$

Where K is a constant defined according to Harris, K=0.04.

$$If \begin{cases} R \succ 0 \Rightarrow Corner \\ R \prec 0 \Rightarrow Contour \\ R\ small \Rightarrow Flat\, region \end{cases}$$

Figure 1 shows the different points detected by Harris corner detector applied to two types of medical images (Echographic, Radiographic and IRM).

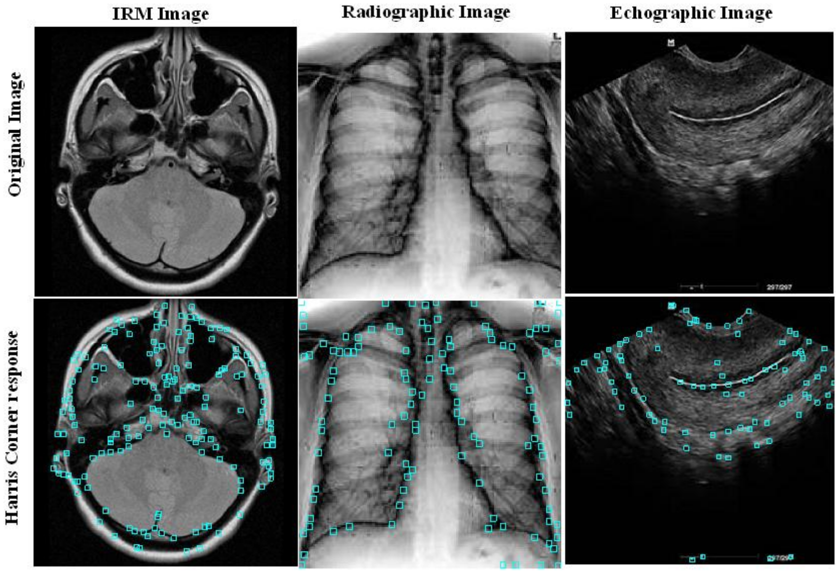

Figure 1: Example of interest points extracted by the Harris corner detector for images "Echographic", "Radiographic" and "IRM".

4.2 Error Correcting Code: Serial "Turbocode"

The concept of Turbocode, recently introduced, is approximated to the notion of concatenation many types of Error Correcting Codes. Indeed, a turbocode is to concatenate two or many error correcting codes 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 series. These codes are usually separated by an interleaver block. This architecture allows course to break the error packets whose origin is the within decoder in order to facilitate the work of the other decoder said "Exterior".

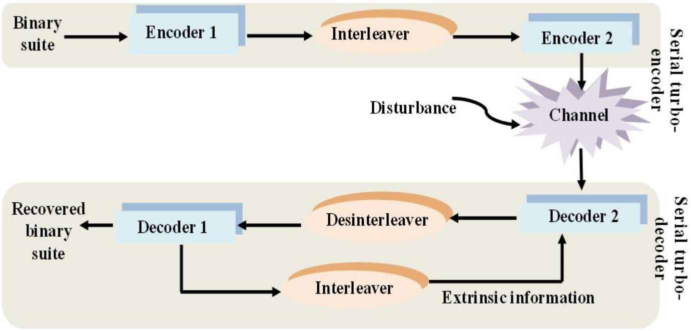

Figure 2: Serial "Turbocode" diagram.

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 [9].

4.3 SHA-1 Hash Function

The SHA-1 is a cryptographic [10] 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.

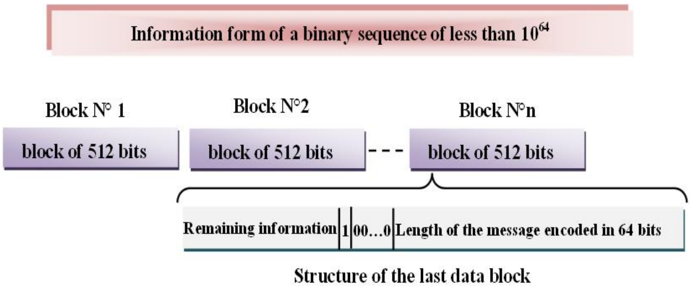
Information form of a binary sequence of less than 10^{64}
Block N° 1
Block N°2
Block N°n
block of 512 bits
block of 512 bits
block of 512 bits
Remaining information
1
00...0
Length of the message encoded in 64 bits
Structure of the last data block

Figure 3: 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 4 illustrate the different steps to find the hash of a block M(i).

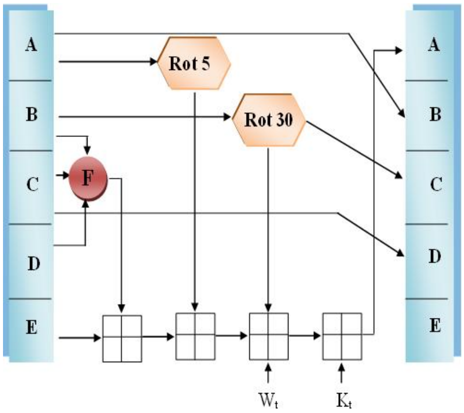

Figure 4: One iteration within the SHA-1 compression function.

With:

- Kt : constant used in the ieme 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.

5 Proposed Watermarking Schema

5.1 Presentation

Figures 5 illustrates the totality of message to insert. These data consist essentially in patient information, such as the first name, age and sex, and the medical diagnosis.

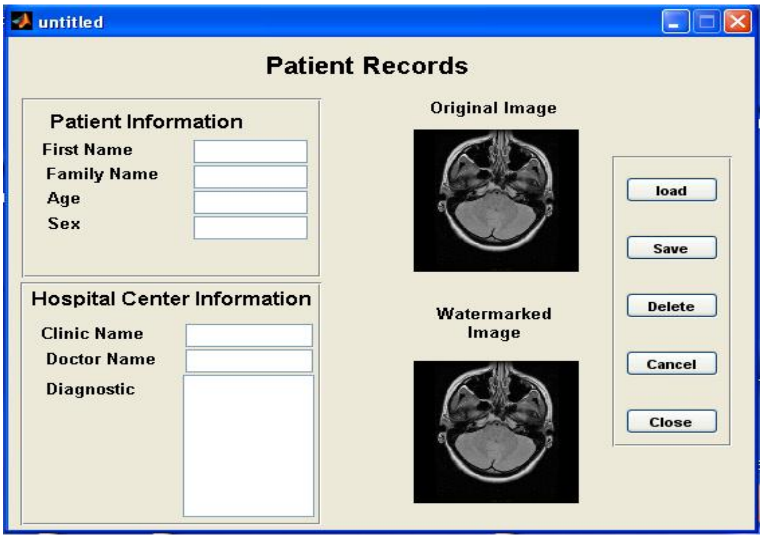

Figure 5: User interface for medical data introduction.

After that, the message is treated in two steps (insertion and detection).

5.1.1 Data Insertion:

In Figure 6, once information has been introduced by user, the step of data insertion in the medical image begins.

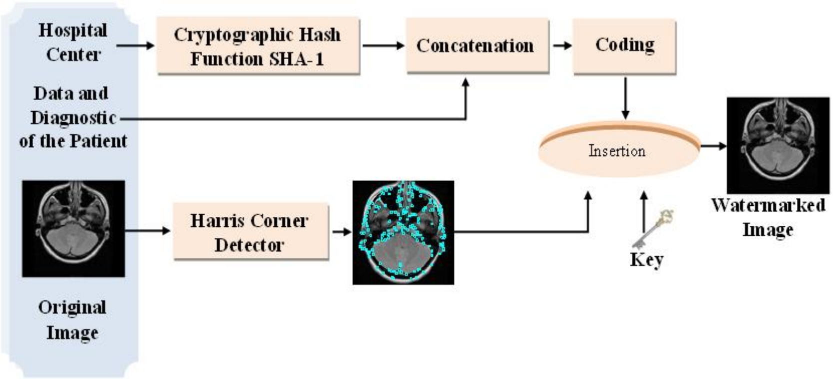

Figure 6: Data insertion.

Firstly, generate the signature of the hospital center (using Secure Hash Algorithm SHA-1) on 160 bits. After that, concatenate the digital signature with the full data of the patient to form the global message to be inserted in the image.

This message is coded by the error correcting code (ECC). In the proposed approach, The Turbo code is used in order to protect the message from alteration resulting in different attacks. For the original image, the pixels that carry the message to be inserted will be selected using the Harris corner detector [11].
At this step, the coded message, the key, pixels (carrying the message) selected are ready and the original image are done, the watermarking can be started.

5.1.2 Data Detection:

As shown in Figure 7, the detection is partitioned into 4 main parts:
Using the Harris corner detector, the pixels carrying the message, are extracted.
Then, using the secret key, the message is extracted from the pixels already selected.
Thirdly the Turbo code 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 the control of the integrity of the image.

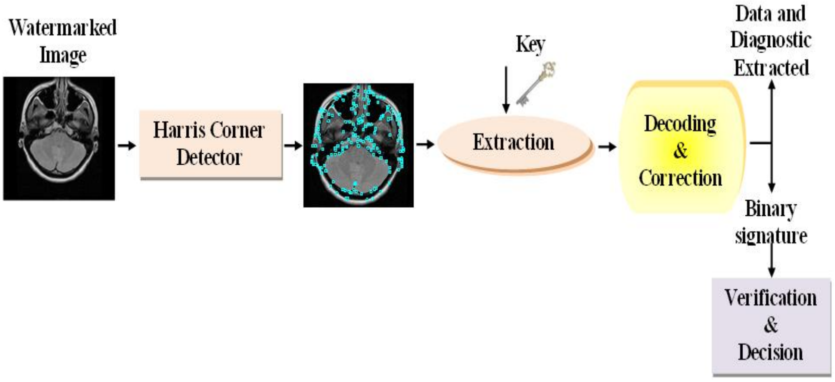

Figure 7: Data Detection.

5.2 Description

As are mentioned in the paragraph 5.1, the Proposed Watermarking Schema is divided into two steps:

5.2.1 Insertion step:

The inclusion of binary data in the image will undergo the following steps:

- Using Harris corner detector, we look for points that can support the inserted data.

- The number N (in our case N = 2) of LSBs sufficient for the integration of patient data and the binary signature of the hospital center, are calculated. This signature coded in 160 bits using SHA-1 [12]. Data size can be estimated (eg, the name is estimated at 15 characters, etc.), as well deducted after entering these information.
- Concatenate the signature of the hospital center with different data own the patient information. These data will be transformed into binary message and encoded using the error correcting codes (serial Turbocode).
- With key, substituted the coded message into the N LSB location (with N = 2).

Figure 8 summarizes the different steps of insertion diagram.

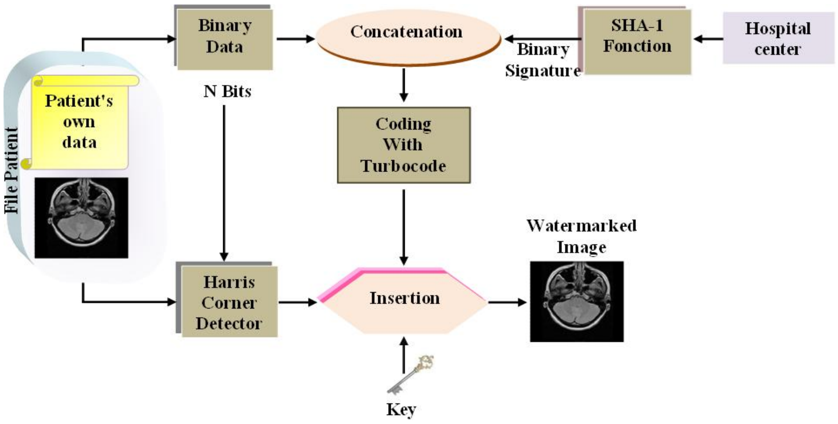

Figure 8: Watermarked insertion algorithm.

5.2.2 Detection step:

The detection step is to extract patient's data and the message digest (binary signature) of the hospital center, when the integrity is verified. The detection algorithm follows the steps in reverse insertion. Figure 9 shows the different steps of detection, verification of integrity for medical image and control of authenticity for data patient.

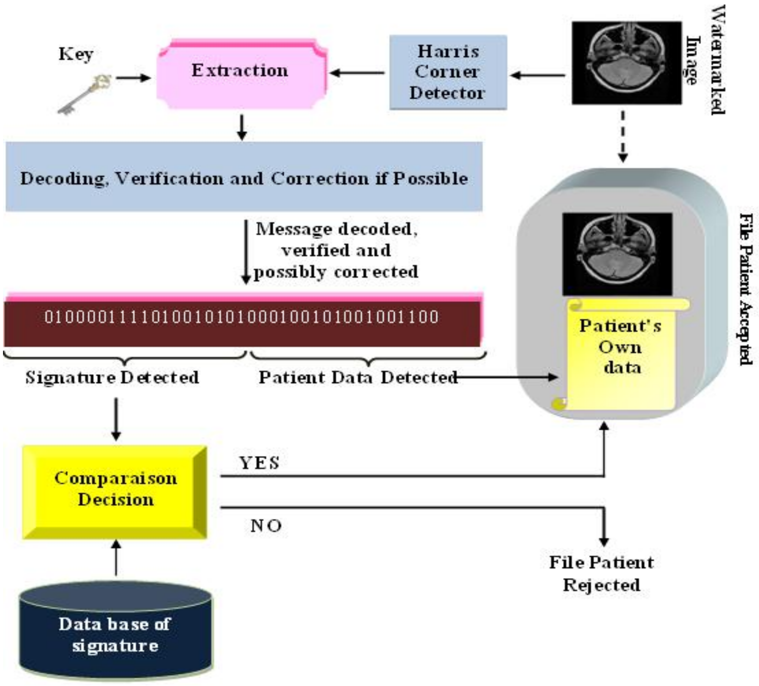

Figure 9: Watermarked extraction algorithm.

6 Results

The proposed watermarking algorithm is applied to a database of 30 medical images (IRM, Radiographic and Echographic).
Table 2 shows the data will be inserted and these sizes.

Table 2: Illustration of the different data to be inserted

I*nformationtobeinserte*	N*umberofbitsbeforecoded*	N*umberofbitsaftercodin*
First Name	80	1770
Family Name	160	
Age	24	
Sex	1	
signature of the original image	160	

When the tested watermarked image undergoes ”copy/past” attack, a message containing the patient’s data in addition to the hospital signature are extracted. But in some images the extracted signature are different from the initial one (after applying the error correcting code). We concluded that some alterations have been occurred.

Figure 10, 11 and 12 show the quality of IRM, Radiographic and Echographic watermarked image robustness of our watermarking schema against JPEG attacks with a different rate of compression.

It should be noted that for a compression ratio which ranges from 10% to 50%, the image does not lose its psychovisual aspect.

For rate compression equal to 10%, the watermark is successfully recovered (for the three types of medical images).

Concerning the error correcting code (Figure 13), many tests show that we are able to correct the occurred errors when the tested images get compression image rate equal to 10%.

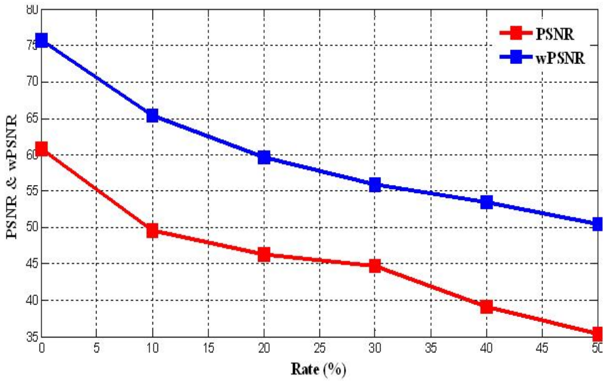

Figure 10: PSNR and wPSNR for Echographic image watermarked compressed.

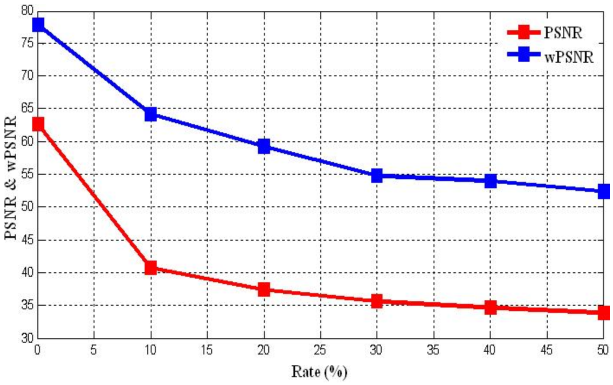

Figure 11: PSNR and wPSNR for IRM image watermarked compressed.

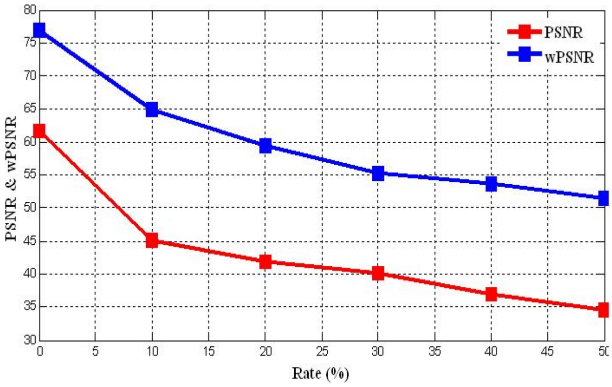

Figure 12: PSNR and wPSNR for Radiographic image watermarked compressed.

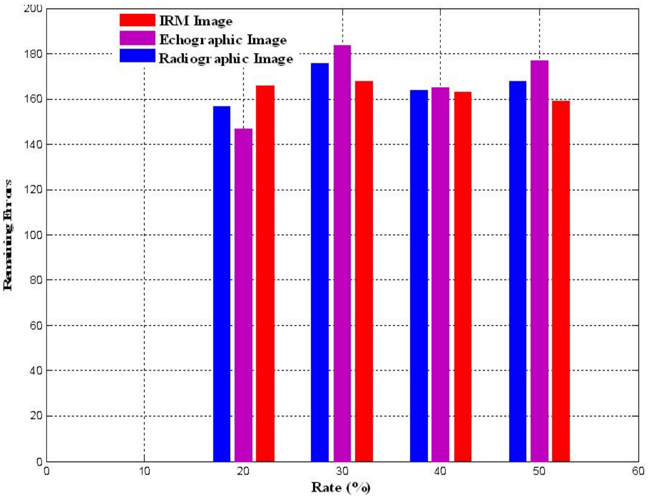

Figure 13: Remaining errors after correction for Echographic, IRM and Radiographic image.

Figure 14, 15 and 16 show the quality (PSNR and wPSNR) of the IRM, Radiographic and Echographic images after applying an impultionnel noise attack.

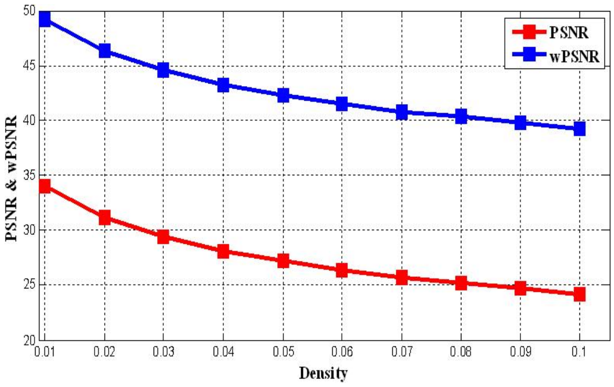

Figure 14: PSNR and wPSNR for Echographic images watermarked and attacked by an impultionnel noise.

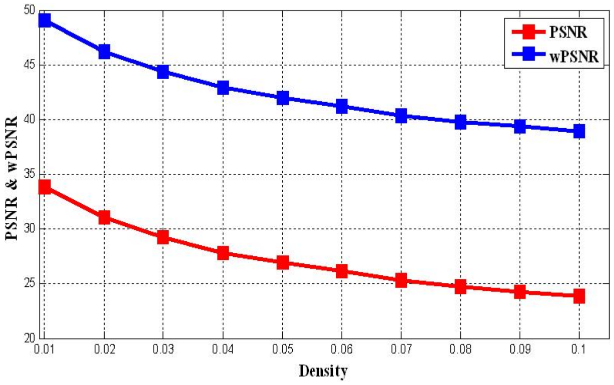

Figure 15: PSNR and wPSNR for IRM images watermarked and attacked by an impultionnel noise.

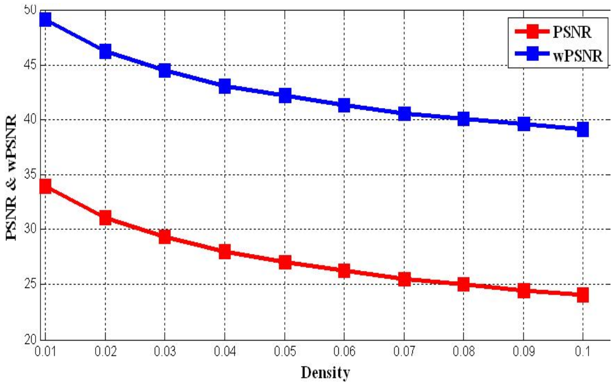

Figure 16: PSNR and wPSNR for Radiographic images watermarked and attacked by an impultionnel noise.

Table 3 shows the different errors produced during an attack implutionnel applied to IRM, Radiographic and Echographic images.
It is noted that our method or watermarking is managed to extract and correct errors produced by this type of attack.

Table 3: Illustration of the errors before and after correction of Echographic, Radiographic and IRM images

Image	Density	0.01	0.02	0.03	0.04	0.05	0.06	0.07	0.08	0.09	0.1
Echographic	errors detected	2	2	2	9	8	12	15	11	19	11
	errors after correction	0	0	0	0	0	0	0	0	0	0
IRM	errors detected	7	6	11	10	8	6	2	23	16	19
	errors after correction	0	0	0	0	0	0	0	0	0	0
Radiographic	errors detected	5	5	8	11	10	12	14	17	20	15
	errors after correction	0	0	0	0	0	0	0	0	0	0

It should be noted that if applied to a Gaussian noise, the proposed watermarking method cannot properly extract all the data substituted. In this case one risks losing information about its authenticity.

7 Conclusions

The watermarking of image is an application in the medical image, on particular in the telemedicine domain.Indeed, given the significance and growth experienced by the practice of telemedicine, the watermarking may be proposed to contribute to the security of medical images shared on the Internet.

In this paper, we are interested in inserting a fragile watermarking whose objectives are to verify the integrity of the medical image and preserve the confidentiality of patient data.

This method is perfectly suited to medical imaging because it benefits from the use of least significant bits (LSBs) of the image, and allows you to insert the patient's own information while keeping a quality of the watermarked image.

References

[1] S. Boucherkha and M. Benmohamed. "a lossless watermarking based authentication system for medical images". *, Engineering and Technology Journal*, (2005).

[2] Mohamed Ali Hajjaji Ridha Hajjaji, Abdellatif Mibaa and El bey Bourennane. "watermarking of medical images for integrity and confidentiality of data". In *Fifth Workshop Amina, Tunisia*, 2010.

[3] A. Manoury. *"Watermarking of digital images by wavelet packets"*. PhD thesis, University of Nante-France, 2001.

[4] International Telecommunication Union. *"Recommendation method" 1990.*

[5] Mohamed Ali Hajjaji Abdellatif Mtibaa and El bey Bourennane. "a watermarking of medical image-new approach based on multi-layer method". *International Journal of Computer Science Issues (IJCSI)*, Vol. 8, Issue 4:pp. 33–41, July 2011.

[6] P. Bas. *"Watermarking method based on image content"*. PhD thesis, INP Grenoble-France., 2000.

[7] T.Hanene. *"Development of a new approach to watermarking for indexing of medical images"*. PhD thesis, Universit de Renne-France, 2006.

[8] C. Harris and M. Stephen. "a combined corner and edge detector". In *Proceedings of Fourth Alvey Vision Conference, Manchester*, 1988.

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

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

[11] Xiaojun Qi and Ji Qi. "a robust content-based digital image watermarking scheme". *signal processing, Elsevier*, page 12641280, November 2006,.

[12] O. 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.