VOL. 2, NO. 12, December 2011 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

A Watermarking of Medical Image: Method Based "LSB"

Mohamed Ali HAJJAJI
Laboratory EμE, Faculty of Sciences of Monastir, University of Monastir-Tunisia, LE2I Laboratory, Burgundy University, Dijon, France,
Mohamedali_hajjaji@etu.u-bourgogne.fr

Abdellatif MTIBAA
Laboratory EμE, Faculty of Sciences of Monastir, University of Monastir-Tunisia, National Engineering School of Monastir Tunisia.
abdellatif.mtibaa@enim.rnu.tn

El-bey BOURENNANE
LE2I Laboratory, Burgundy University, Dijon, France,
ebourenn@u-bourgogne.fr

ABSTRACT

In this paper, we present a new approach for watermarking of medical image that we are trying to adapt to telemedicine. This approach is intended to insert a set of data in a medical image. These data should be imperceptible and robust to various attacks. It's containing the signature of the original image, the data specific to the patient and his diagnostic. 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 LSB (least significant bits) of the image and tools borrowed from cryptography.

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

1. INTRODUCTION

Medical imaging is an important and vital aid in diagnostic and management decisions. In this regard, several different techniques and additional are used: Magnetic Resonance Imaging (MRI)Scanner, Computer Tomography (CT), Positron Emission of Tomography (PET), mammography, ultrasound, etc.

On the other hand, with the development of diseases, several diagnoses are insufficient, hence the need for cooperation of several colleagues in order to achieve a correct diagnostic, what is known in the field of health aid to medical diagnostic (telemedicine).

This continues to take an important place in various medical applications, but the main problem exist at the level of the exchange of data over the Internet, while maintaining their integrity and confidentiality against the appearance of considerable pirates.

In this 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.

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;
- Maintain confidentiality for patient and hospital data.

Indeed, this approach allows patients to insert data into a set of different types of images (IRM and Echographic). Obviously, all of the data included (Signature, Address, Patient Record, Hospital Signature, Medical diagnostic) should be hidden protected and correctly transmitted.

2. APPROACH PRESENTATION

As indicated in Figure 1, the message to insert consists essentially of:

- Patient information (First name, Age and Sex);
- Medical diagnostic.

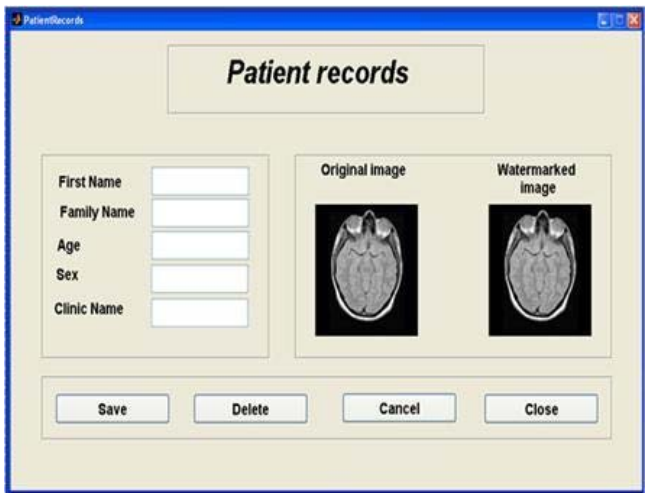

Figure 1: User interface for medical data introduction.

After that, the message is treated in two steps:

Step 1: Data Insertion:

In Figure 2, once information has been introduced by user, the step of data insertion in the medical image begins.

VOL. 2, NO. 12, December 2011 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

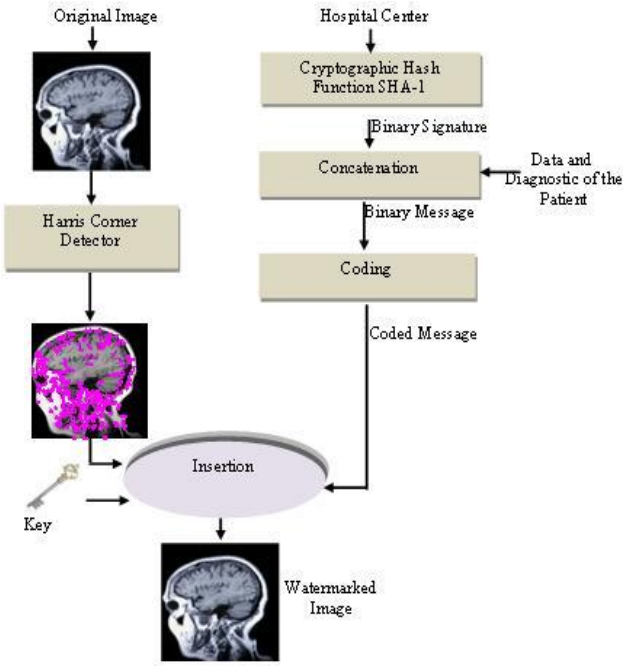

Figure 2: Data insertion.

First, using the SHA-1 (Secure Hash Algorithme), the binary signature of the hospital center is generated. This signature coded in 160 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 (ECC). In the proposed approach, the Turbo code is used in order to protect the message from alteration resulting on different attacks. For the original image, the pixels that carry the message to be inserted will be selected using tha Harris corner detector.

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.

Step 2: Data Detection:

As shown in Figure 3, 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 control the integrity the image.

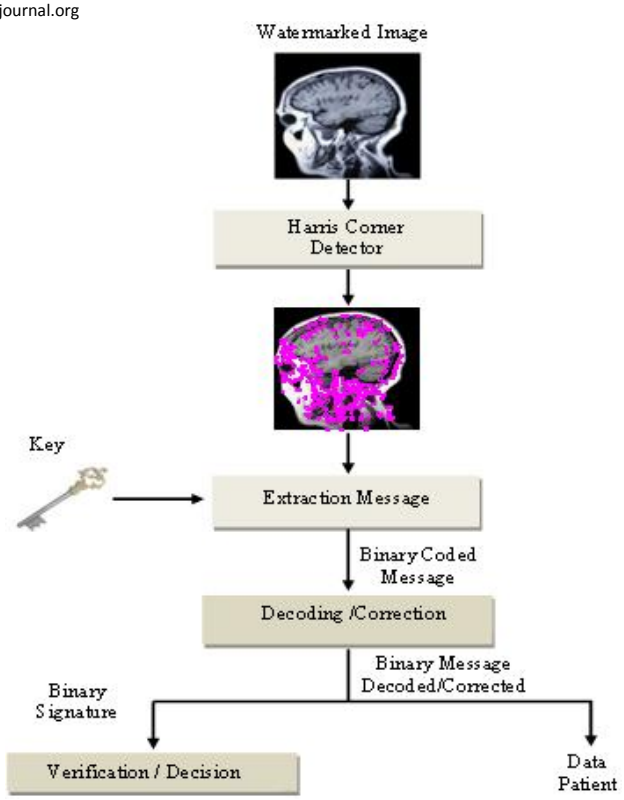

Figure 3: Data detection.

Harris Corner Detector: to detect differences pixels carry the message to be inserted.

The Error Correcting Code "Turbocode": to contribute to the data confidentiality, data verification and eventually error correction.

Cryptographic Hash Function SHA-1: to generate the hospital center signature and verify the integrity of the received medical image.

2.1 Harris Corner Detector

In [2] Bas and al. evaluate the performance of three commonly used detectors (Harris Corner Detector [3], The Achard-Rouquet detector [4] and The Suzan detector [5]) and conclude the Harris Corner Detector is the most robust.

If I(x,y) is the gray level intensity, the Harris corner detector refines the detection function [6] by using the following shape factor-based matrix M :

$$M(x,y) = \begin{bmatrix} A_{x,y} & C_{x,y} \\ C_{x,y} & B_{x,y} \end{bmatrix} = \begin{bmatrix} \left(\frac{\partial I(x,y)}{\partial x}\right)^2 & \left(\frac{\partial I(x,y)}{\partial x}\right)\left(\frac{\partial I(x,y)}{\partial y}\right) \\ \left(\frac{\partial I(x,y)}{\partial x}\right)\left(\frac{\partial I(x,y)}{\partial y}\right) & \left(\frac{\partial I(x,y)}{\partial y}\right)^2 \end{bmatrix} \quad (1)$$

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 $R(x,y)$:

$$R(x,y) = det\,(M(x,y) - K[trace(M(x,y))]^2 \quad (2)$$

$$R(x,y) = (A_{x,y}B_{x,y} - C_{x,y}^2) - K(A_{x,y} + B_{x,y})^2 \quad (3)$$

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

2.1.1 Medical image based adaptive Harris corner detector

The medical image content extraction algorithm uses the Harris corner detector to find important feature points (i.e., corner points) to reduce the synchronization errors in watermark detection. The principal contributions are :

- Apply some pre-processing techniques, if exist, to reduce the noise;
- Regulate the number of important feature points on the medical image.

The following steps detail the image content extraction procedure :

[1] Apply a Gaussian low-pass filter to original image I(x,y) to avoid corners due to image noise.

[2] Apply a rotationally symmetric(3*3) Gaussian low-pass filter with the standard deviation of 0.5 to three derivative images, namely,A(x,y),B(x,y) and C(x,y), to achieve additional resistance to possible image noise.

[3] Calculate R(x,y) within a circular window, which is at the image center and covers the largest area of the original image. The resulting function reduces the effect of image rotation attack.

[4] Apply a threshold T on R(x,y) for searching an important feature points based on the local maxima.

$$\{R(x,y) | R(x,y) > T \wedge R(x,y) \geq R(u,v,), \forall (u,v) \in V_{x,y}\} \quad (4)$$

Where T is a predefined threshold value. Empirically T is set to be 106, and $V_{x,y}$ represents a circular neighborhood centered at (x, y).

The circular neighborhood window is choosed to avoid the increasing detector anisotropy and to obtain a homogeneous distribution of feature points in the medical image.

It is important to determine the window size. If the window is too small, the distribution of feature points is concentrated on textured areas. If otherwise, the feature points become isolated.

Empirically, these feature points are obtained by using our proposed adaptive Harris corner detector with a 3*3 neighborhood window.

Figure 4 shows the different points detected by Harris corner detector applied on two types of medical images (Echographic and IRM).

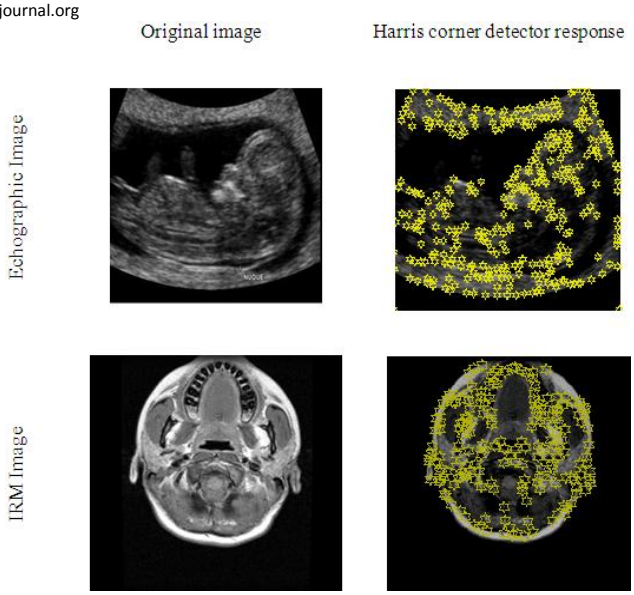

Figure 4: Example of interest points extracted by the Harris corner detector for images "Echographic" and "IRM".

2.2 Error Correcting Code "Turbocode"

The concept of turbo code, recently introduced, is approximated to the notion of concatenation Error Correcting Codes.

Indeed, a turbo code 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.

2.2.1 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".

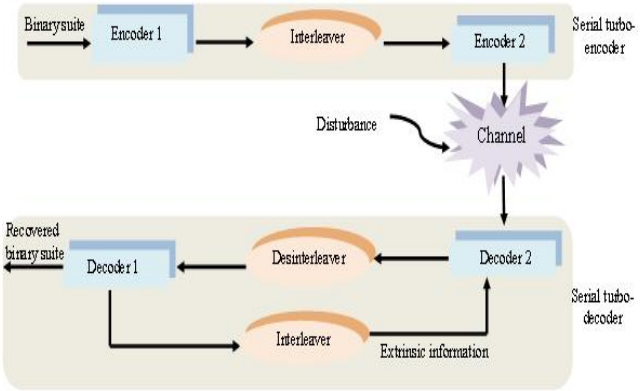

Figure 5: Serial Turbocode diagram.

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 [7].

2.2.2 Parallel "Turbocode"

A parallel turbocode is a simultaneous process consisting to use the two codes at the sometimes. Boumerdassi in [8] schematized a parallel turbo-encoder as follows:

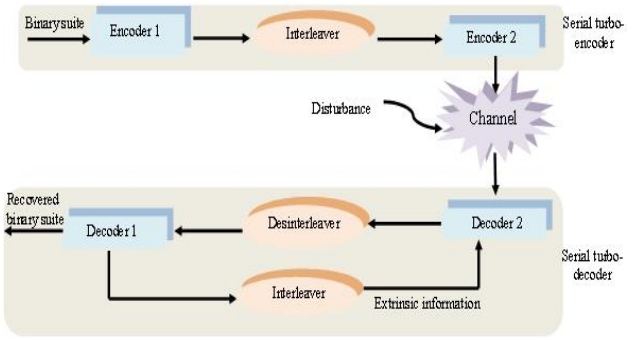

Figure 6: Parallel encoder diagram.

The three code words generated during encoding are obviously used in the decoding operation. Figure 7 shows the turbo-decoder architecture that should be adopted.

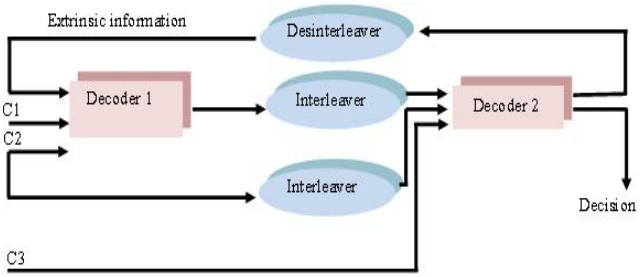

Figure 7: Parallel decoder diagram.

The block interleaver used toggles data during the transition between the convolutional codes used.
This treatment allows, by turning on an error bits divided into an error distributed throughout the sequence, that two symbols near the origin are as distant as possible from each other which can directly affect the minimum Hamming. Then we can estimate that the interleaver block is a required element in the diagram of a turbocode whose absence greatly affects its power.

2.3 Cryptographic Hash Function SHA-1

The SHA-1 is a cryptographic 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.

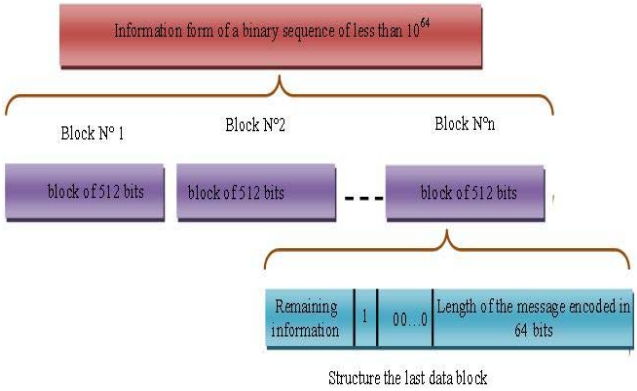

Figure 8: Decomposition of the message into blocks of 512 bits.

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 9 illustrate the different steps to find the hash of a block M(i).

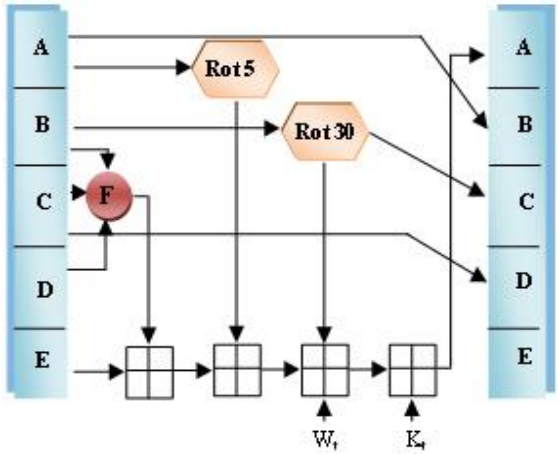

Figure 9: One iteration within the SHA-1 compression function.

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.

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 [9]:

- Innocent Attacks;
- Malicious attacks.

VOL. 2, NO. 12, December 2011 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

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, etc.

4. 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 [10]:

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 [11] [12]:

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.

4.2 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.

4.2.1 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 Peack Signal to Noise Ratio PSNR.
The SNR and the PSNR are respectively defined by the following formulas:

$$(\mathrm{SNR})_{\mathrm{dB}} = 10\log_{10}\left\{\left[\frac{\sum_{i,j} I^2(i,j)}{\sum_{i,j}[I(i,j) - I_w(i,j)]^2}\right]\right\} \quad (5)$$

$$(\mathrm{PSNR})_{\mathrm{dB}} = 10\log_{10}\left\{N * M\left[\frac{\max I^2(i,j)}{\sum_{i,j}[I(i,j) - I_w(i,j)]^2}\right]\right\} \quad (6)$$

4.2.2 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. [13] is defined by the following formulas:

$$(\mathrm{wPSNR})_{\mathrm{dB}} = 10\log_{10}\left\{\frac{M * N \max I^2(i,j)}{\sum_{i,j}\left[\frac{I(i,j) - I_w(i,j)}{1 + \mathrm{Var}_I(i,j)}\right]^2}\right\} \quad (7)$$

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

The proposed Watermarking Schema is divided into two steps:

5.1 Insertion step

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

- Using Harris corner detector, we look for points that can supported the data inserted.
- 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 [14]. 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 (Turbo code).
- With key, substituted the coded message into the N LSB location (with N = 2).
- Figure 10 summarizes the different steps of insertion diagram.

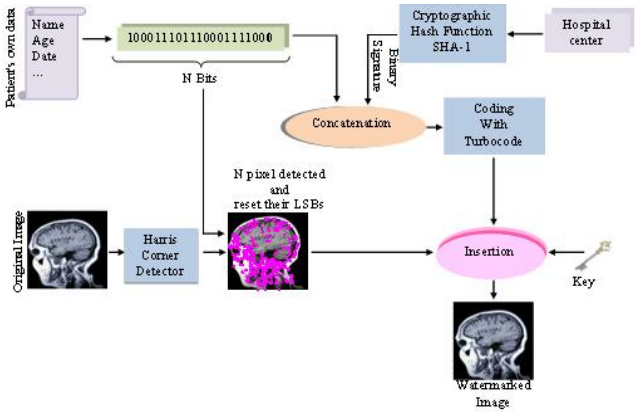

Figure 10: Watermarked insertion algorithm.

VOL. 2, NO. 12, December 2011 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

5.2 Detection step

The detection step is to extract patient 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 11 shows the different steps for detection, verification of integrity for medical image and control of authenticity for data patient.

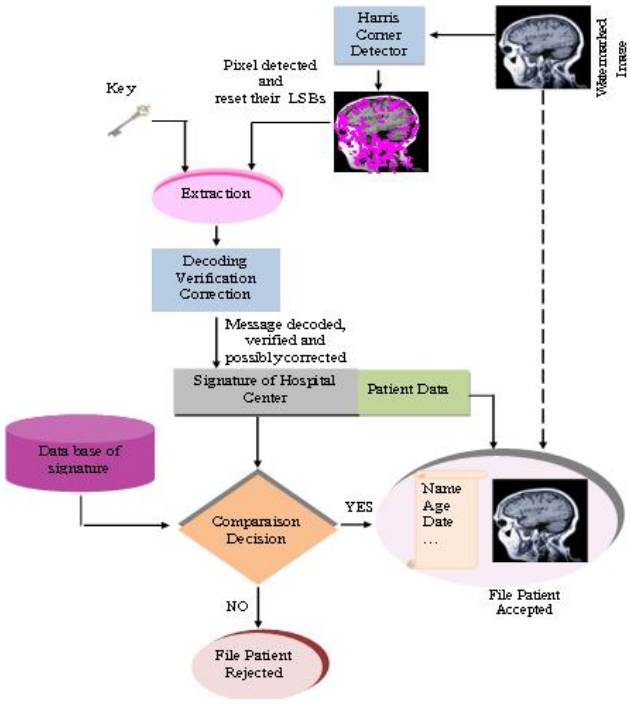

Figure 11: Watermarked extraction algorithm.

6. RESULTS

The proposed watermarking algorithm is applied to a database of 30 medical images (IRM and Echographic images). Table 2 shows the data will be inserted and these sizes before and after decoded with serial turbo code.

Table II:
Illustration of the different data to be inserted.

Information to be inserted	Number of bits before coded	Number of bits after coded with serial turbo code
First Name	80	1700
Family Name	160	
Age	24	
Sex	1	
signature of the original image	160	

This algorithm permits to detect the totality of the message inserted in the tested images. Then 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 (after applied the error correcting code). About it, we concluded that some alterations have been occurred.

Figure 12 and Figure 13 show the quality of IRM and Echographic watermarked image robustness of our watermarking schema against JPEG attacks with different rate compression.

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

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

Concerning the error correcting code (Figure 14), many tests show that we are able to correct the occurred errors when the tested images get compression image rate equal to 10%.

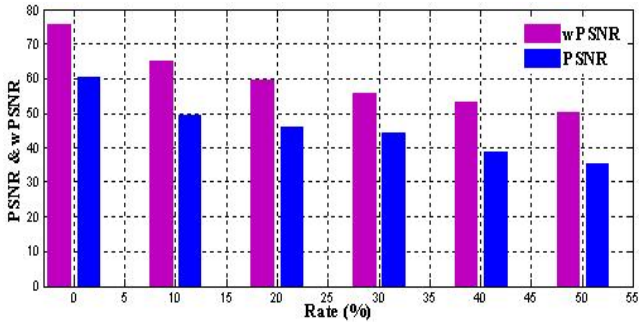

Figure 12: PSNR and wPSNR for Echographic image watermarked compressed.

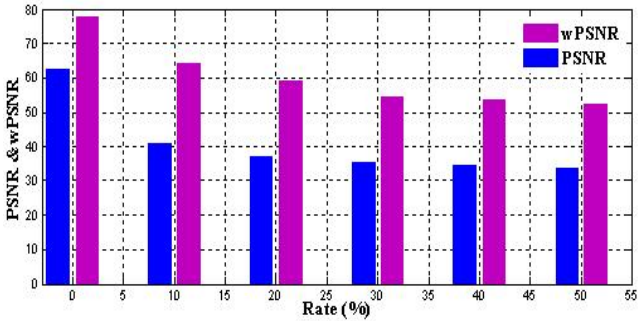

Figure 13: PSNR and wPSNR for IRM image watermarked compressed.

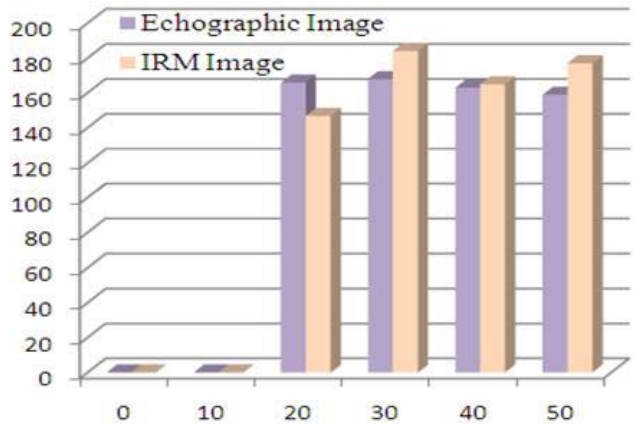

Figure 14: Remaining errors after correction for Echographic and IRM image.

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

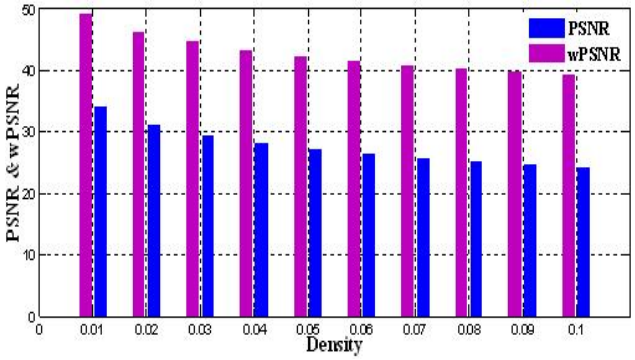

Figure 15: PSNR and wPSNR for Echographic images watermarked and attacked by an impultionnel noise.

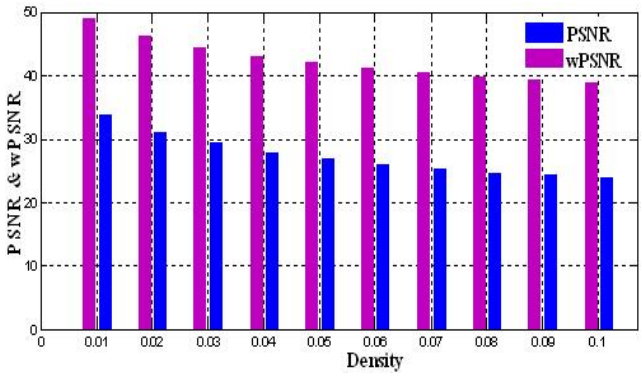

Figure 16: PSNR and wPSNR for IRM images watermarked and attacked by an impultionnel noise.

Figure 17 and figure 18 show the different errors produced during an attack implutionnel applied to IRM and Echographic images. It is noted that our method or watermarking managed to extract and correct any errors produced by this types of attack.

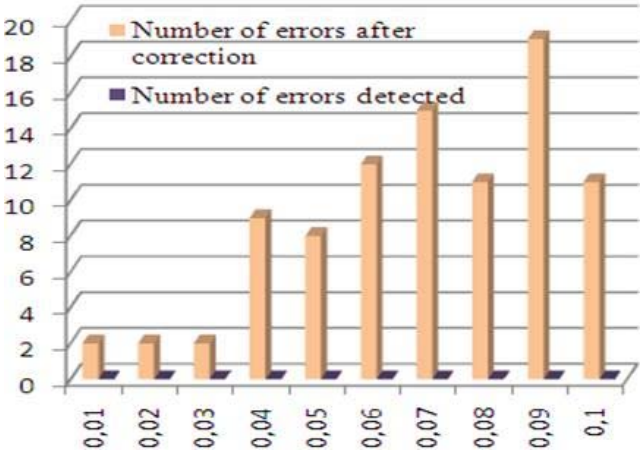

Figure 17: Illustration of the errors before and after correction for Echographic images.

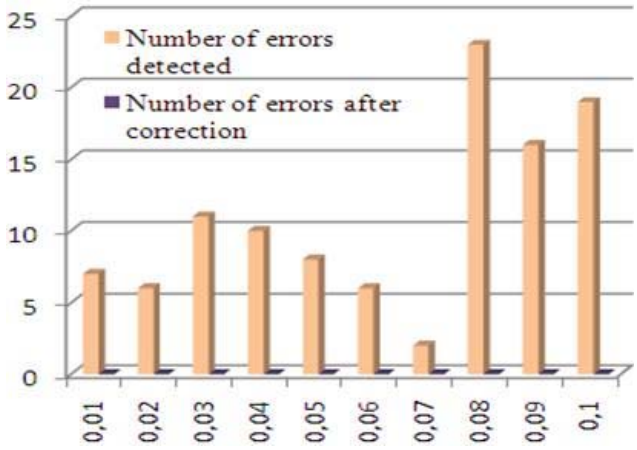

Figure 18: Illustration of the errors before and after correction for IRM images.

It should be noted that if applied a Gaussian noise, the proposed watermarking method cannot properly extract all the data substituted. In this case one loses 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 for contribute to the security of medical images shared on the Internet.

In this paper, we are interested in inserting a delicate 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, allowing you to insert the patient's own information while keeping a quality of the watermarked image.

REFERENCES

[1] Samia Boucherkha and Mohamed Benmohamed: A Lossless Watermarking Based Authentication System for Medical Images, World Academy of Science, Engineering and Technology 1 2005, 100-103.

[2] P. Bas, J.M. Chassery, B. Macq, Geometrically invariant watermarking using feature points, IEEE Trans. Image Process. 11 (9) (2002) 1014–1028.

[3] C. Harris, M. Stephen, A combined corner and edge detector, in: Proceedings of Fourth Alvey Vision Conference, Manchester, 1988, pp. 147–151.

[4] J. Devars, C. Achard-Rouquet, E. Bigorgne, Un detecteur de point carateristiques sur des images multispectrales extension vers un detecteur sub-pixellique, in: Proceedings of GRETSI'99, September 1999, pp. 627–630.

[5] S.M. Smith, J.M. Brady, SUSAN—a new approach to low level image processing, Int. J. Comput. Vis. 23 (1) (1997) 45–78.

[6] H. Moravec, Obstacle avoidance and navigation in the real world by a seen robot rover, Robotics Institute, Carnegie-Mellon Univ., Pittsburgh, PA, Tech. Rep. CMU-RI-TR-3, September 1980.

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

[8] Bouderbala Ahmed, "Implémentation d'un algorithme de tatouage vidéo robuste dans le domaine compressé", Master 2009.

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

[10] H. Mohamed Ali, "Tatouage des images médicales en vue d'intégrité et de confidentialité des données", Cinquième Workshop Amina, Tunisie 2010.

[11] A.Manoury, "Tatouage d'images numériques par paquets d'ondelettes", Ph.D., université de Nantes, 2001.

[12] "Méthode d'évaluation subjective de la qualité des images de télévision", Recommandation CCIR 500-4, Union internationale des Télécommunications (ITU), 1990.

[13] P.BAS, "Méthode de tatouage d'images fondé sur le contenu", Ph.D., INP Grenoble, 2000.

[14] Ondrej Mikle, "Practical Attacks on Digital Signatures Using SHA-1 Message Digest", Department of Software Engineering, Faculty of Mathematics and Physics, Charles University, Prague, Czech Republic, 2004.

BIOGRAPHYS

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 Microelectronic 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 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.