”Last Signification Bits” Method for Watermarking of Medical Image

Mohamed Ali Hajjaji, Abdellatif Mtibaa, El-Bey Bourennane

"Last Signification Bits" Method for Watermarking of Medical Image

Mohamed Ali Hajjaji[1, 3], 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
abdellatif.mtibaa@enim.rnu.tn
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, Medical, 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 (IRM) 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 diagnosis (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.

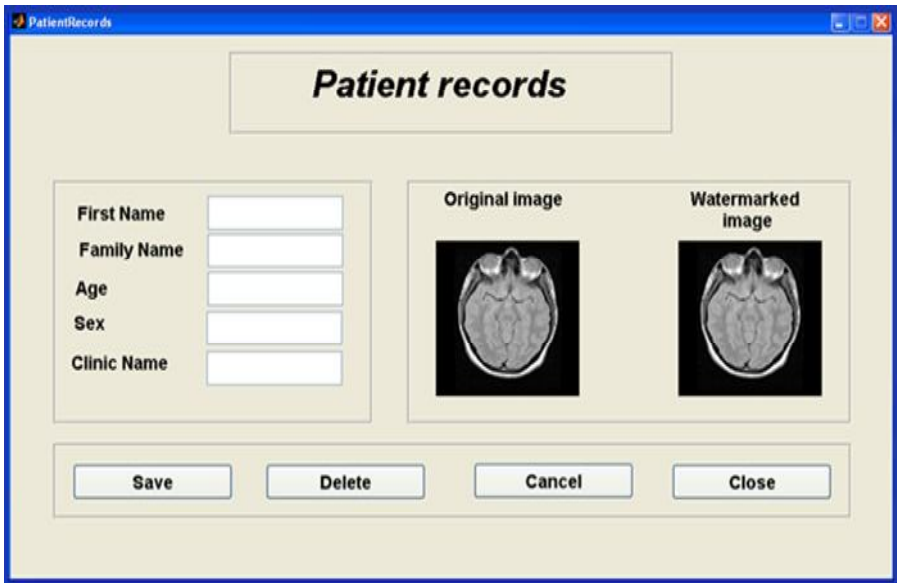

Fig. 1. User interface for medical data introduction.

After that, the message is treated in two steps:

Step 1: Data Insertion:

In Figure 1, once information has been introduced by user, the step of data insertion in the medical image begins.

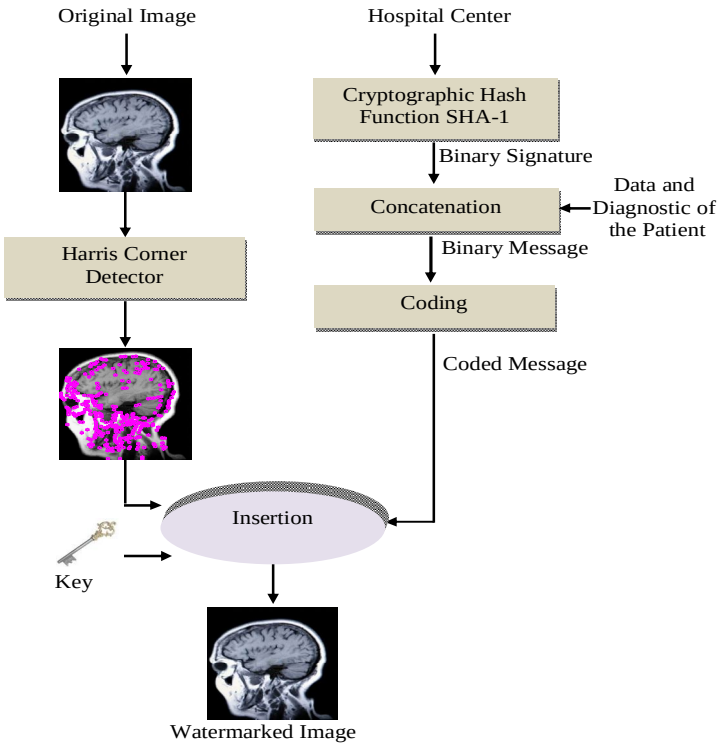

Fig. 2. Data insertion.

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 the Harris corner detector [2].
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 of the image.

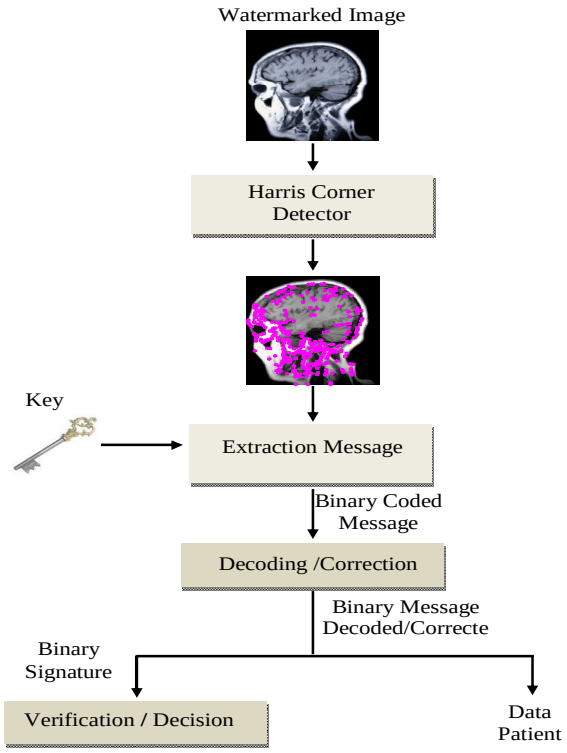

Fig. 3. Data detection.

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

- The Error Correcting Code "Turbo code" [3]: to contribute to the data confidentiality, data verification and eventually error correction.

- Cryptographic Hash Function SHA-1 [4]: to generate the hospital center signature and verify the integrity of the received medical image.

3. 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 [5].

3.1 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 [6] [7].

Table 1. 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.

3.2 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.

3.2.1 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:

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

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

3.2.2 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:

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

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.

4. Watermarking Schema Description

The proposed Watermarking Schema is divided into two steps:

4.1 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 [9]. 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 4 summarizes the different steps of insertion diagram.

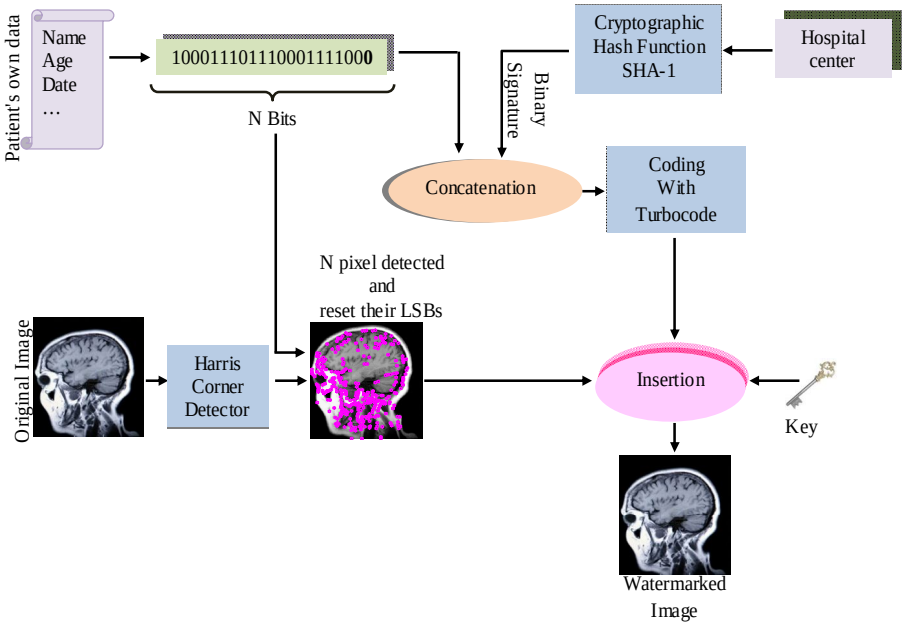

Fig. 4. Watermarked insertion algorithm.

4.2 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 5 show the different steps for detection, verification of integrity for medical image and control of authenticity for data patient.

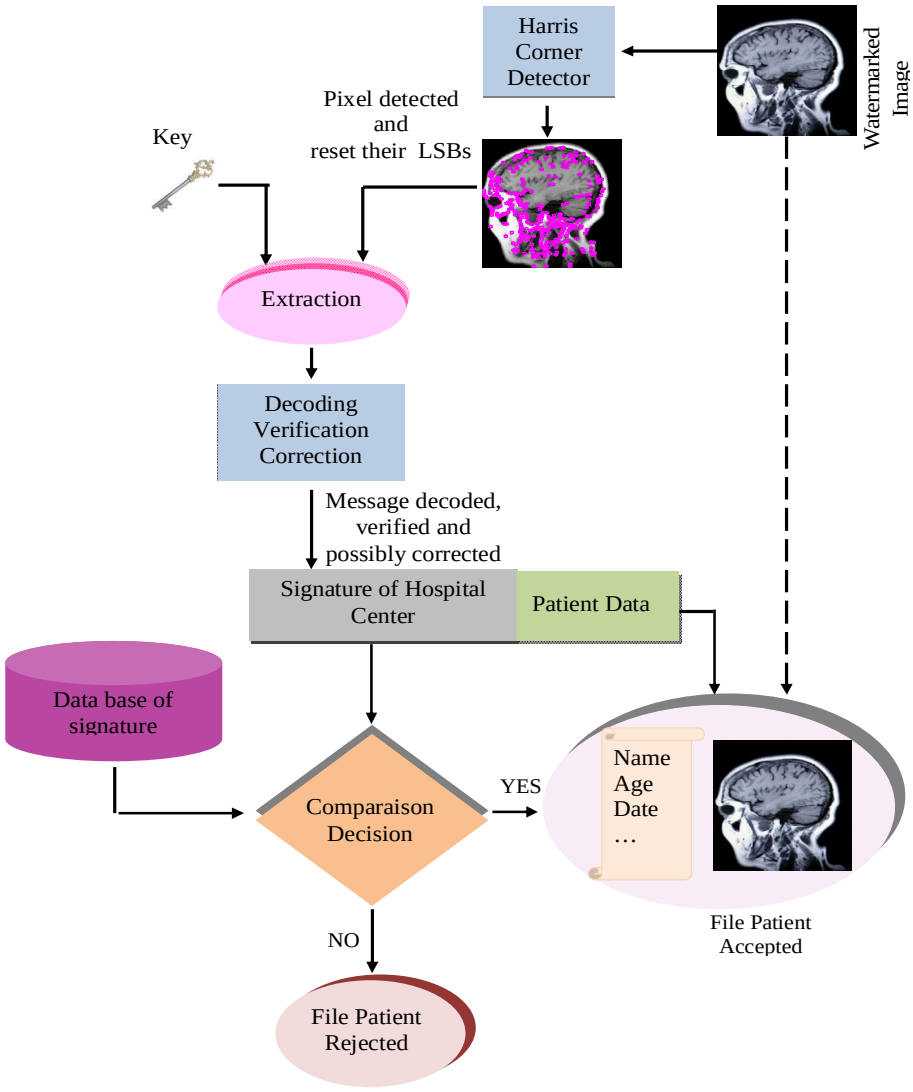

Fig. 5. Watermarked extraction algorithm.

5. Results

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

Table 2. Illustration of the different data to be inserted.

Information to be inserted	Number of bits before coded
First Name	80
Family Name	160
Age	24
Sex	1
signature of the original image	160

After that, these data will be coded with serial turbo code, his size is 1770 bits.
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 (after applied the error correcting code). About it, we concluded that some alterations have been occurred.
Figure 6 and Figure 7 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 8), many tests show that we are able to correct the occurred errors when the tested images get compression image rate equal to 10%.

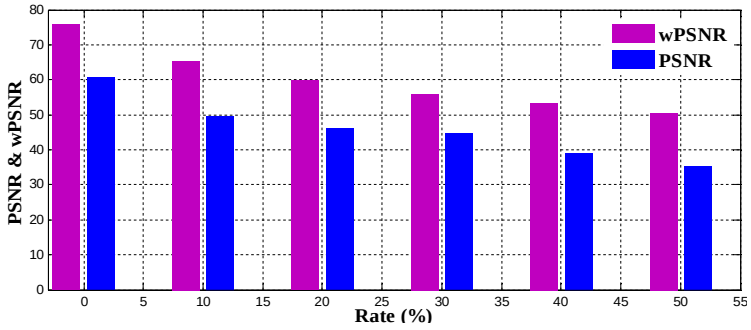

Fig. 6. PSNR and wPSNR for Echographic image watermarked compressed.

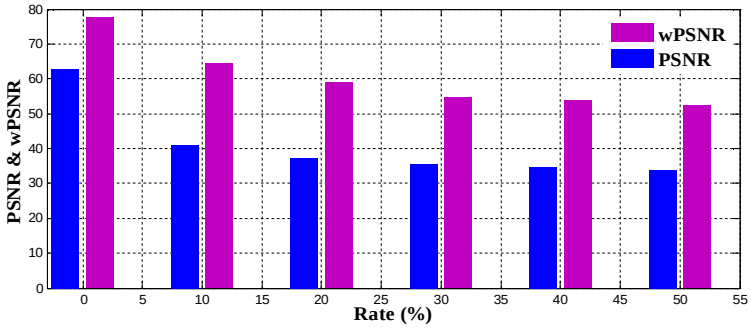

Fig. 7. PSNR and wPSNR for IRM image watermarked compressed.

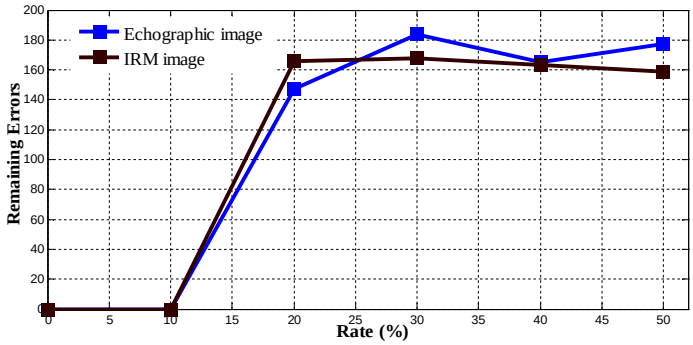

Fig. 8. Remaining errors after correction for Echographic and IRM image.

Fig.9 and Fig.10 show the quality (PSNR and wPSNR) of the IRM and Echographic images after applying an impultionnel noise attack.

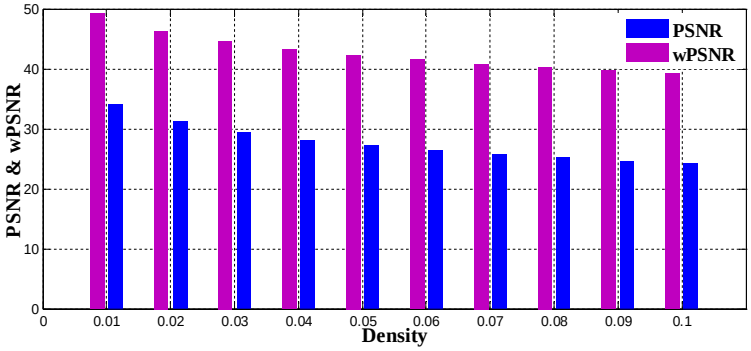

Fig. 9. PSNR and wPSNR for Echographic images watermarked and attacked by an impultionnel noise.

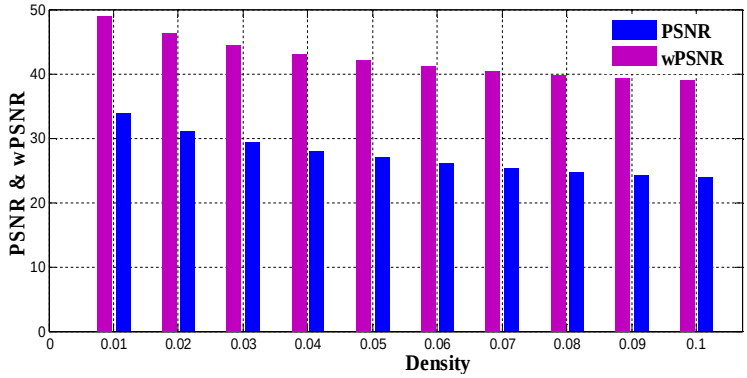

Fig. 10. PSNR and wPSNR for IRM images watermarked and attacked by an impultionnel noise.

Table 3 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 type of attack.

Table 3. IlluIllustration of the errors before and after correction for Echographic and IRM images.

	Density	**0.01**	**0.02**	**0.03**	**0.04**	**0.05**	**0.06**	**0.07**	**0.08**	**0.09**	**0.1**
Echographic Image	**Number of errors detected**	2	2	2	9	8	12	15	11	19	11
	Number of errors after correction	0	0	0	0	0	0	0	0	0	0
IRM Image	**Number of errors detected**	7	6	11	10	8	6	2	23	16	19
	Number of errors after correction	0	0	0	0	0	0	0	0	0	0

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.

6. 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. S. Boucherkha and M. Benmohamed "A Lossless Watermarking Based Authentication System for Medical Images", Engineering and Technology Journal (2005), 100-103. World Academy of Science.
2. Xiaojun Qi, Ji Qi "A robust content-based digital image watermarking scheme", signal processing (2007) 1264–1280, November 2006, Elsevier.
3. H. Jaber, "Conception architecturale haut débit et sûre de fonctionnement pour les codes correcteurs d'erreurs", Ph.D., Ecole doctorale IAEM – Lorraine, 2009, Lorraine - France.
4. "Secure hash standard", Federal Information Processing Standards Publication 180-2, 2002.
5. M.A. Hajjaji, R. Hajjaji, A. Mibaa and E. Bourennane, "Tatouage des images médicales en vue d'intégrité et de confidentialité des données", Cinquième Workshop Amina, Tunisie 2010.
6. A. Manoury, "Tatouage d'images numériques par paquets d'ondelettes", Ph.D., université de Nantes, 2001, Nante-France.
7. ITU, "Méthode Recommandation", Union internationale des Télécommunications CCIR 500-4, 1990.
8. P. Bas, "Méthode de tatouage d'images fondé sur le contenu", Ph.D., INP Grenoble, 2000, Grenoble-France.
9. 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.