

Protected transmission of medical images via LabVIEW using Watermarking technique

Nassiri Boujemaa¹, Latif Rachid², Toumanari Ahmed³, F. M. R. Maoulainine⁴

^{1,2,3}ESSI, National School of Applied Sciences, Ibnou Zohr University, Agadir, Morocco

⁴Team of child, health and development, CHU, Faculty of Medicine, Cadi Ayyad University, Marrakech, Morocco

¹nassi.bouj@gmail.com, ²latif_rachid@yahoo.fr, ³atoumanari@yahoo.fr, ⁴fadl2020@hotmail.com.ma

Abstract: Remote transmission of digital images is rapidly increasing computer networks, in particular telemedicine can transmit a very short time medical data, with the aim of improve the quality of life of the population, especially those people elderly, the disabled and those who need periodic medical. To ensure data transmission, we have developed two algorithms in the LabVIEW development environment. This platform is adopted for its speed of development and it includes a real-time module that provides the ability to easy data exchange between two or more remote systems. The LabVIEW application developed in this paper via the TCP/IP protocol ensures remote transmission of medical images between Client/Server architectures via the Internet. Computer networks are complex and attacks are possible. He poses a real problem for the security during transmission of images. Protection becomes important for many reasons such as confidentiality, authentication and integrity. Currently, the most suitable for the transfer of medical images lies in cryptography. However, once decrypted, the image is no longer protected and can be duplicated, copied, falsified and distributed easily. In this context, digital watermarking has quickly emerged as a new advanced technology to enhance the security of digital images. Indeed, the insertion of a watermark in a medical image can authenticate it and guarantee its integrity. The watermark must be generally hidden does not affect the quality of the medical image. The objective of this paper is to develop a watermarking algorithm to ensure an authentication service suitable for medical images to gray level fostering a fragility rather than robustness. Finally, we examine the watermarking technique used for the description of the results obtained in terms of imperceptibility and authenticity.

Keywords: Authenticity, ClientTCP/ServerTCP, Imperceptibility, LabVIEW, Watermarking, Wavelet transforms.

I. INTRODUCTION

The transmission of images between health professionals and healthcare organizations through computer networks has become possible thanks to the digital revolution. So today, when a doctor receives a patient he often requires the specialist advice before delivering his diagnosis. One possible solution is to transmit by a computer link, the images of the patient with the report of the specialist. In this paper, image transmission is ensured by the development environment LabVIEW (Laboratory Virtual Instrument Engineering Workbench). Transmission of medical information raises serious safety issues particularly against the demands of ethical and legal aspects specific to the medical domain. Several solutions exist to provide cryptography security services concerned with medical data (confidentiality, authentication, integrity ...) but only cryptography methods have become insufficient to cover all safety aspects of the processing and transfer scanned images and medical record [1]. Digital watermarking can advantageously complement cryptographic tools to protect medical images. In this paper we propose to combine two techniques; the first is devoted to the transmission of medical images by developing a development environment the two applications LabVIEW Client TCP and Server TCP, the second technique is digital watermarking to authenticate the medical image of the patient before making a diagnosis by the doctor. The choice of the tool used for the transmission of images is based on several criteria, namely:

- Facilitate real time visualization of medical data (signals, images and videos) [2].
- Control and remote diagnosis of patients.
- Easy exchanging of remote data and make decisions by specialists.

This paper is organized as follows. In section 2, we describe the various technology for data exchange based on Client/Server architecture via the LabVIEW software. In section 3, we illustrate two applications developed in LabVIEW and the results of their tests for the transmission of medical images via TCP/IP. In section 4, we highlight the need to secure medical images by introducing the watermarking technique. Following that is section 5 in which we including the steps of two important algorithms during watermarking process: the algorithm of insertion and extraction. Results and discussion are shown in section 6. The conclusion and future works are described in the last section.

II. TECHNOLOGIES FOR DATA EXCHANGE BASED ON A CLIENT/SERVER ARCHITECTURE

Since 1990, the exchange of data between different applications has been formalized with technology DDE (Dynamic Data Exchange) Microsoft, which sends data from one application to another [3]. Communication between two applications can be based on Client/Server architecture (Fig. 1). The LabVIEW environment provides essentially protocols for performing the data exchange. These protocols are:



- High Level (Data Socket, ActiveX, VIservers,...).
- Low level (TCP, UDP, Serial, Carte DAQ,...).

The data exchanged between Client/Server are secured by different levels of confidentiality. Using Data Socket technology is a very simple implementation, but it must nevertheless be limited to applications where the volume of data exchanged remains low. ActiveX technology allows going further with the ability to control one application from another, but it exists only in the Windows environment. It is possible in the LabVIEW environment to program these exchanges by returning to the protocols type communication network based on a protocol such as TCP (Transmission Control Protocol) or UDP (User Datagram Protocol). Preference is given to TCP for its simplicity, reliability and ability to receive entire data without transmission losses, plus it provides a secure service of package delivery.

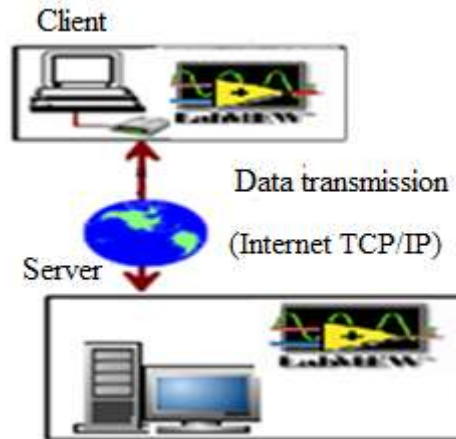


Figure 1. Configuring general Client/Server communication.

A. Client/Server architecture via TCP/IP

In this work, the application adopted uses TCP/IP protocol. It implements a server that sends data to the client on request. The progress of communication between two machines will be as follows:






- The server listens to a port, which we have arbitrarily chosen. The server is ready to answer a connection request.
- Once a client connects to this port, the server sends it a line of text in order to identify. The client then knows that the server is ready and he will be able to start a dialogue.
- The server, on its side, waits for orders from client. If it does not receive any orders for a certain time, it closes the connection and is once again waiting on the port.

On the LabVIEW platform, data exchange via the communication protocol is done thanks to the following basic functions: Open Connection TCP, TCP Listen, Read TCP, TCP Write and TCP Close Connexion. From these functions, we have developed Client/Server applications that are used to transfer local and remote medical images.

III. TRANSMISSION OF MEDICAL IMAGES VIA LABVIEW

For transmitting images via TCP/IP protocol using the LabVIEW graphical programming, it is necessary to add other functions to the functions referred to in paragraph above [4]. The Table 1 shows the different functions used in this work.

Table 1. Manipulation functions for the transmission of images.

Function	Name	Role
	Configure Grab	Acquisition
	IMAQ Create	Create a site in the temporary memory for an image
	IMAQ ReadFile	Read a file image
	IMAQ Open Camera	Configuration
	IMAQ Configure	Configuration



The algorithm for the transmission of images presented in fig. 2 and 3 can be subdivided into five main steps:

- Step 1: Configuration, setup and acquisition.
- Step 2: Connection request to the client side.
- Step 3: Open connection at the server side.
- Step 4: Data change.
- Step 5: Connection Closing.

The server application (fig. 2) developed allows to remotely transmitting medical images on the client application shown in fig. 3. The latter application of the demand side the opening of the connection to exchange and receive data transmitted by the server.

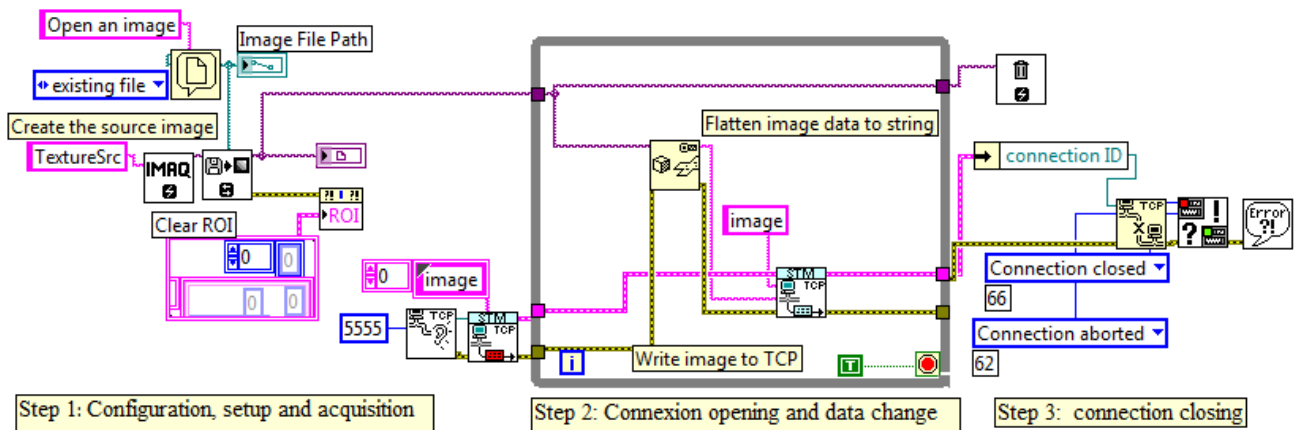


Figure 2. Application of image transmission server side

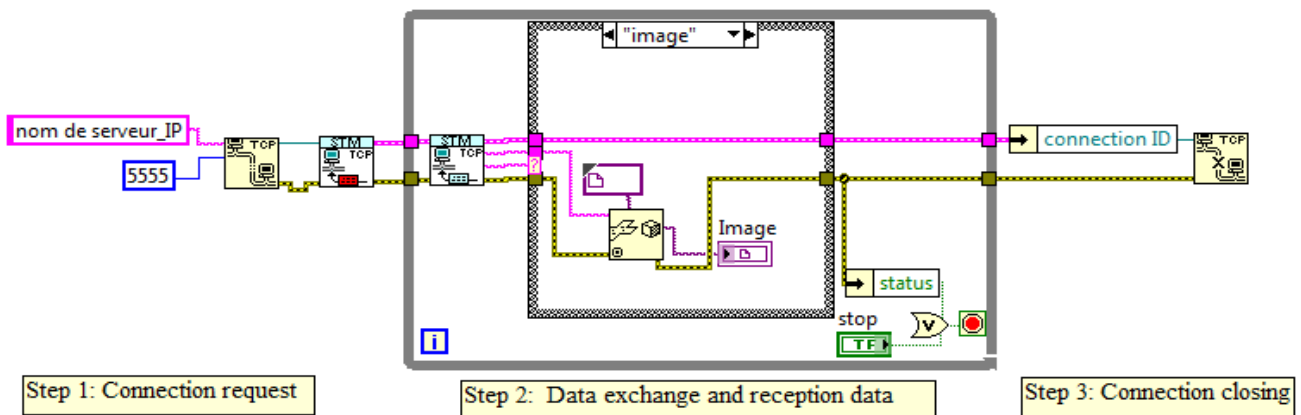


Figure 3. Application of image transmission client side.

The result of running these two applications is shows in fig. 4.

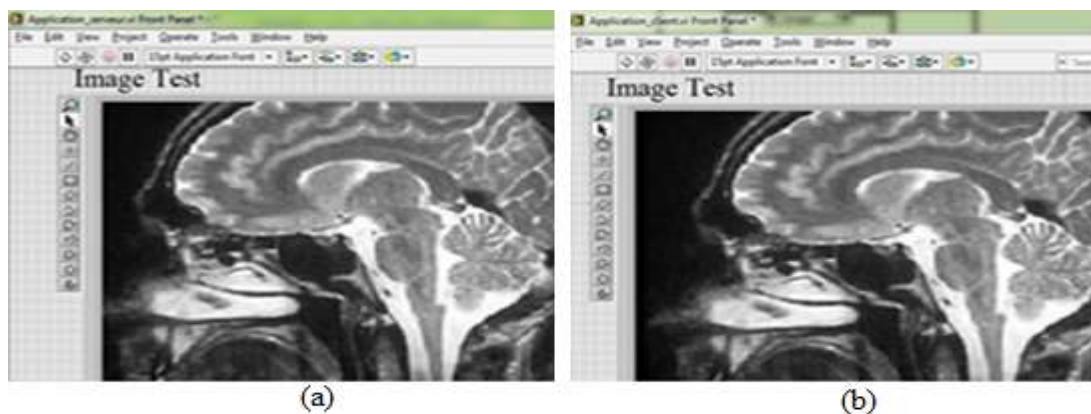


Figure 4 .Images transmitted (a) and received (b).

IV. PROTECTION OF MEDICAL IMAGES USING WATERMARKING TECHNIQUE

The transfer of medical images can be done with such a risk (attacks) and must therefore protect. Attacks can be treatments to either interfere or remove the watermark of image protection [5]. The most adapted protection for this type of communication lies in cryptography [6, 9]. However, once decrypted, the image is no longer protected and can be duplicated, copied, falsified and distributed easily. In this context, digital watermarking has quickly emerged as a new advanced technology to enhance the security of digital images. Digital Watermarking is inserted it into a digital document (image, video, audio) in a different kind of watermark to ensure a security service (copyright, authentication, integrity, etc.) [10, 12].

Watermarking techniques are divided in two categories: Spatial Domain Watermarking, and frequency domain watermarking, where the image is first transformed to frequency domain and then the low frequency components are modified to contain the watermark. Watermarking can be applied in frequency domain by applying transforms like Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Singular Value Decomposition (SVD) or Wavelet transform (DWT).

A. Watermarking process

It seems important to separate the different stages of a watermarking algorithm according to the following scheme fig.5:

- Initially, we start by formatting the watermark.
- Next, is the insertion phase, each domain has its specific (audio, image, video). The insertion is rarely done in spatial domain. We often work in a transformed domain with invariance properties facilitating the insertion of a robust and invisible watermark. In this paper, we will concentrate on the discrete wavelet transformation because the main advantage of wavelets over Fourier and DCT analysis is that they allow for both spatial and frequency resolution it has several strong characteristics in which they can be exploited to obtain a good watermarking algorithm.
- In the end come the extraction / detection phase.

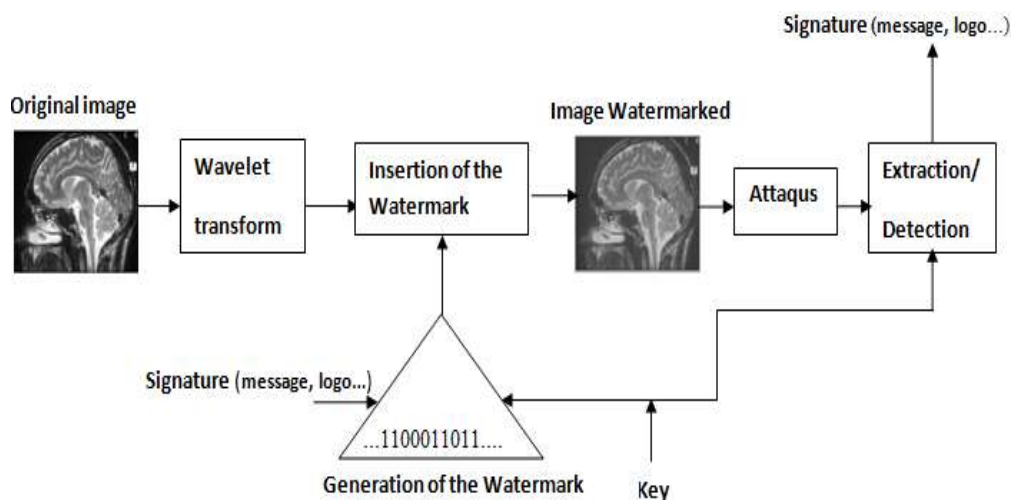


Figure 5. Complete scheme of watermarking method developed.

B. Discrete wavelet transform

Wavelet theory appeared in early 1990 [13]. It affects many areas of mathematics, particularly signal processing and image. The multi-resolution analysis provides a set of approximation signals and detail of a start signal [14]. We obtain a multiscale decomposition of the starting signal by separating each level of resolution at low frequencies (approximation A) and high frequencies (detail D) signal. The wavelet transform is one of the operations that provide a multi-resolution signals. The fig. 6 shows the result of a wavelet transform digital image. A first decomposition ($L = 1$) provides the thumbnail images $cj1$ with $j = \{h, v, d\}$ and BF1. The result of the second decomposition ($L = 2$), made from the thumbnail BF1 provides the thumbnail images $cj2$ with $j = \{h, v, d\}$ and BF2. Thumbnails BFL corresponds a rough representation of the image, while the thumbnail images cjL represent details of the vertical variations (cvL), horizontal (chL) and diagonal (cdL) of the image at different frequencies (according to the value of the scale of decomposition L, in practice $L=4$) [15].

The main advantage of discrete wavelet transform (DWT) is the discrete cosine transform (DCT) is applied in blocks, however, the DWT is applied to all image. In addition, this transformation is closer to the human visual system that DCT and it allows compression with a higher rate than DCT.

BF2	C_{h2}	C_{h1}
C_{v2}	C_{d2}	
C_{v1}		C_{d1}

Figure 6. Wavelet decomposition at level two image.



C. Principle of the proposed method.

Since the phases of insertion and extraction decide the characteristics of the other phases so they are most important. The algorithm uses the discrete wavelet transform to create a transformed domain, then, we exploit the characteristics of the domain and applying different techniques to implement the watermark.

C.1 Embedding process

The main steps of the embedding procedure developed are presented here:

1. Read the original image.
2. Resize the image.
3. Apply a wavelet decomposition on the image to the original scale L ($L=4$) to obtain the transformed image. In our decomposition, we have used 4 levels. This number was chosen to allow for good frequency resolution and to yield enough bands for embedding.
4. Add a mask psycho visual; to better ensure the invisibility of the watermark; psycho visual criteria are used to adjust the insertion force locally to the image. This allows us to maximize the mark embedding weights while minimizing the distortion introduced.
5. Prepare or generate watermark W ; the method used to prepare the watermark is the secret key identification that was generated by a generator of pseudo-random binary sequence.
6. Encrypt the watermark W with pseudo random binary vector P to produce W^* .
7. Specify the value of parameter robustness α ; this value determines the force of the watermark that will be inserted.
8. Embedded W^* in the host image.
9. Apply an inverse wavelet decomposition of the image transformed to the scale L ($L = 4$) to obtain the image.

C.2 Algorithm to extract the watermark

The extraction process has the following steps:

1. Perform wavelet transform on the possibly distorted watermarked image, using the same wavelet function.
2. Extract the watermark by the reverse process of embedding.
3. Decrypt the extracted watermark W^* using the same secret key as was used for embedding.
4. Compare the extracted watermark W^* with W . If both are same, received image is authentic, otherwise declare it as unauthentic.

During extraction, we need a key and a parameter α which are secret.

C.3 Watermark generation

In order to generate the watermarks, following steps are implemented:

1. Read the logo (ESSI)
2. Convert this gray intensity image into a binary image. We have used the following procedure to perform the above task:
 - 2.1. First resize the image to 25×25 pixels.
 - 2.2. Find mean value of gray scale image and call it threshold T .
 - 2.3. Based on this threshold value T , convert the grayscale image into binary by using the following formula:
 If $\text{logo}(m; n) > T$, make the pixel white
 Else make the pixel black. Now convert this binary image into vector and call it W such that.
3. A pseudo random binary vector P of the size same as W is generated by a secret key K . The following formula is used to get the ultimate watermark $W^* = W + P$.

The original image and signature to be inserted inside the image are shown in fig. 7.

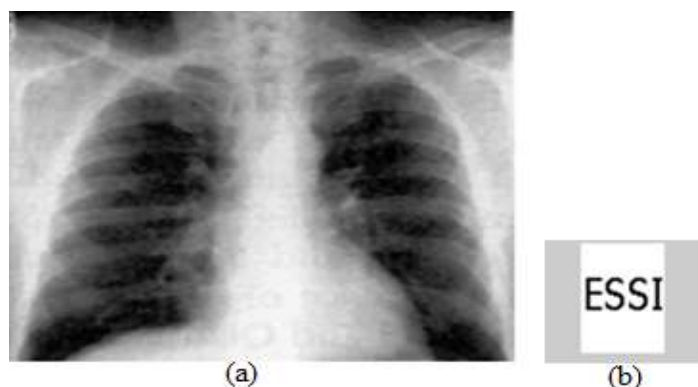


Figure 7. Original image (a), signature to insert inside the image (b).

We apply the algorithms written above; fig. 8 shows the watermarked image and the extracted signature.



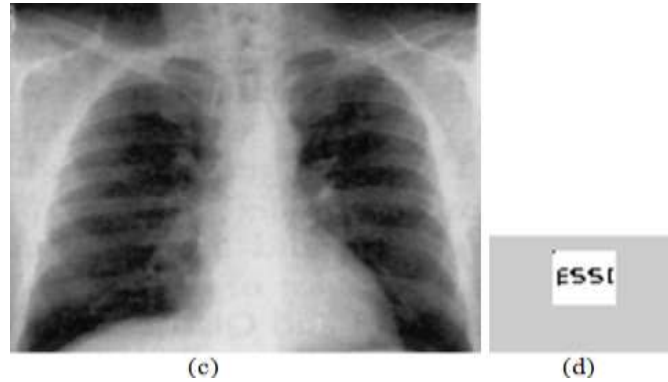


Figure 8. Marked image (c), extracted signature (d).

V. RESULTS AND DISCUSSION

In this section, we evaluate the performance of our method in terms of imperceptibility and robustness. The simulation results are separated into two parts: the first is devoted to testing the property of imperceptibility while the second is devoted to analyzing the robustness against some types of attacks.

A. Property of imperceptibility

To test the property of imperceptibility of our watermarking method, multiple images to grayscale 512×512 size are marked with the logo of our research team of size 25×25 . To assert the visual quality of our method, we use the MSE (Mean Square Error) and PSNR (Peak Signal Noise Ratio) respectively to estimate the degradation and distortion of marked images.

A.1 Mean Square Error

The MSE means the mean square error between the luminance of an image and the original marked image. The MSE evaluates degradation due to watermarking. It is defined by [16]:

$$MSE(I; I') = \frac{\sum_{i=1}^n \sum_{j=1}^m (I_{ij} - I'_{ij})^2}{mn} \quad (1)$$

I and I' are respectively the original image and watermarked image sizes $m \times n$ where I_{ij} and I'_{ij} are their components. This error is mainly due to the addition of the watermark.

A.2 Peak Signal Noise Ratio

The PSNR determines the imperceptibility of the signature. In other words, it evaluates the original image distortion caused by the watermarking and possibly other attacks. The PSNR after insertion of the watermark is given in decibels as [16-18]:

$$PSNR_{[dB]}(I; I') = 10 \log_{10} \left(\frac{N^2_{max}}{MSE(I; I')} \right) \quad (2)$$

For example for an image coded on 8 bits, $N_{max} = 255$

PSNR measures the fidelity between two images while the MSE measures the difference between two images [17-19]. Fig. 9 shows the impact of the proposed watermarking technique respectively in terms of visual aspect and variations of PSNR for the thoracic cage and brain.

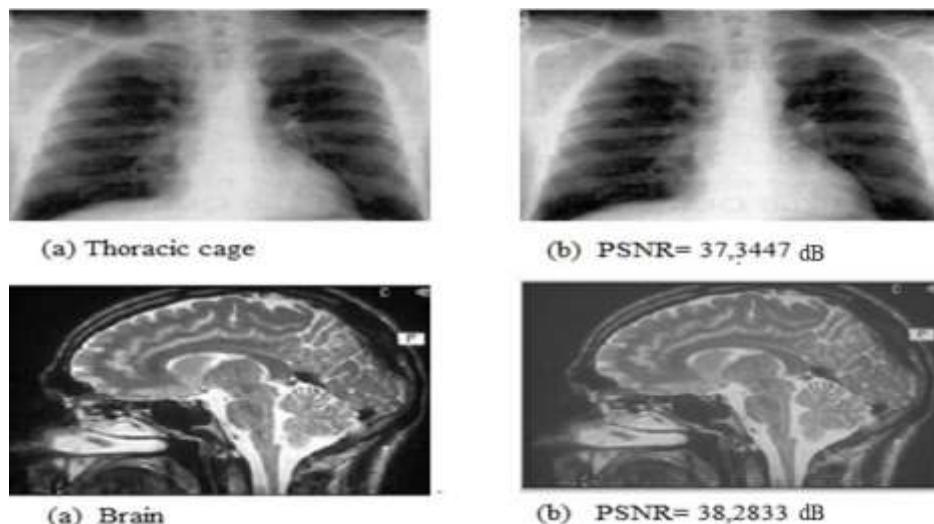


Figure 9. Original Images (a) and watermarked image (b).



To evaluate the method in terms of visual quality of the image gray scale, we conducted the comparison with another authentication Scheme .In the absence of evaluation standards for fragile watermarking systems; we need to compare our scheme with previously. For that reason, we have chosen commercially available watermarking software called Eikonamark [21].

From the comparison of the average PSNR value obtained with this software (38.42 dB) with the one obtained with our system (37.814 dB) [22].

B. Property of authenticity

Robustness tests have been developed primarily for two simple attacks: filtering and adding noise. In this section, the tests are conducted on the images to grayscale "Brain" and "thoracic cage" of size 512 × 512.

For the objective evaluation, BER (Bit Error Rate) measure is used to evaluate the technique for tamper detection.

The BER (expressed as a percentage) is defined as [20]:

$$BER = \frac{\text{number of erroneous bits}}{\text{total number of bits transmit}} \quad (3)$$

B.1 Filtering

Table 2 shows the BER of the signature obtained after extracting it from the watermarked image for different types of filters.

Table 2. BER comparison for different images.

Type of filter	Test images	
	Thoracic cage BER (%)	Brain BER (%)
Gaussian filter	58	43
mean filter	57	63
median filter	57	46
Vertical differentiating filter	56	55

From table 2, we can conclude that our method is almost fragile against certain types of filter selected.

B.2 Addition of noises

The table below shows some types of attacks with various values of noise density.

Table 3. BER comparison for different images.

Type of attack	Noise density	Test images	
		Thoracic cage BER (%)	Brain BER (%)
Multiplicative Uniform	0.1	7	3
	0.5	20	2
Multiplicative Gaussien	0.1	8	3
	0.5	27	3
Salt and pepper	0.09	63	61

According to the calculated values of BER, we can conclude that the robustness of the algorithm differs from one image to another. It can be observed that almost all the attacks were recognized by the proposed method. The logo used as watermark can easily detect the authenticity of the image when the image is tampered.

CONCLUSION

In the first part of this paper we have developed algorithms medical image transmission via LabVIEW between a TCP client and TCP server. The use of these algorithms can send an image via a local network and also via a wireless network, and more specifically the Internet. This application technique is intended to provide those most remote diagnostics competencies of the best experts as if they were on site.

To ensure the protection of medical images during transmission, we have developed in the second part of this paper the technique of watermarking images to grayscale. The basic idea is to insert a watermark in the low frequency part of the discrete wavelet transform of an image host. Then we try to diminish the value of parameter robustness alpha whose objective to have a fragile watermarking to verify that the medical image has not been modified or to ensure the authentication of the image. This new method is performance in terms of imperceptibility and maintains a high quality watermarked images from the calculated values of PSNR. We intend to improve the algorithm developed so that it is able to detect tampered regions (tampered capability of detected regions).

Finally, as part of the problem on watermarking, many techniques have been developed for medical images in grayscale. Then we propose to illustrate the extension of this technique to the image of watermarking color that represents the information support most frequently used.



REFERENCES

- [1]. W. Puech, J. Rodrigues and D. Morice, "Safe Transfert of Medical Images by Conjoined Coding: Selective Encryption by AES Using the Stream Cipher Mode OFB and JPEG Compression," *Treatment du signal*, volume 23- 6, 2006.
- [2]. D. Izbaim, A. Moudden, B. Faiz, and R. Latif, "Real time control of LabVIEW Olive Oil by the ultrasonic method", *The 9th Maghrebien Conference on Information Technology*, Agadir, Morocco 2006 December 7-9.
- [3]. C. Francis, and P. Michel, "LabVIEW and application programming". 2ème édition, p.271, 2009.
- [4]. R. Decout, "LabVIEW User Manual," 2011.
- [5]. B. Vassaux, P. Nguyen, S. Baudry and J.M. Chassery, "Scrambling technique for video object watermarking resisting to MPEG-4", In *International Symposium on VIPromCom Video Image Processing and Multimedia Communications*, 2000.
- [6]. D. Stinson, "Cryptography Theory and Practice", Thompson Publishing, AES. Announcing the Advanced Encryption Standard Federal Information Processing Standards Publication, 2001.
- [7]. J. Daemen and V. Rijmen, "AES Proposal: The Rijndael Block Cipher", Technical report, 2002.
- [8]. W. Diffie and M.E. Hellman, "New directions in cryptography", *IEEE Transactionson Information Theory*, 1976, vol. 26, n°6, p. 644-654.
- [9]. B. Schneier, "Applied Cryptography: Protocols, algorithms and source code in C", 1997.
- [10]. N. Jagadish, B. Subbanna, A. Rajendra and UC. Niranjana, "Simultaneous storage of medical images in the spatial and frequency domain: A comparative study", *BioMedical Engineering OnLine* 2004.
- [11]. J. Cox, M.L. Miller and J.A. Bloom, "Digital Watermarking", San Francisco, CA: Morgan Kaufman, 2002.
- [12]. R. Knopp and A. Robert, "Detection Theory and Digital Watermarking", *Proceedings of SPIE*, 3971:14-23, 2000.
- [13]. K.P. Soman and K.I. Ramachandran, "Insight into wavelets from theory to practice", Prentice-Hall of India, 2006.
- [14]. S. Mallat, "A wavelet tour of signal processing", the editions of the Polytechnic, 2000.
- [15]. A. Manoury, "Digital watermarking wavelet packet, Ph.D. thesis, University of Nantes", 2001.
- [16]. M.S. Chikhi, "Contribution to the authentication flexible digital images by digital techniques markings: application to medical images", *Doctoral thesis, University de Constantine Algérie*, 2008.
- [17]. M. Chaumont, "Digital Watermarking", 2008.
- [18]. Lu C. Shien, "Multimedia security: steganography and digital watermarking techniques for protection of intellectual property", *Institute of Information Science Academia Sinica, Taiwan*, 2005.
- [19]. F. Autrusseau, "Watermarking based on modeling the human visual system and the transformation Mojette", *Doctoral thesis, University of Nantes*, 2002.
- [20]. F. Zhang, X. Zhang and H. Zhang, "Digital image watermarking capacity and detection error rate". *Pattern Recognition Letters* 28, 1-10, 2007.
- [21]. F. Bartollini, A. Tefas, M. Barni and I. Pitas, "Image authentication techniques for surveillance applications", *Proc. IEEE* 89 (101403-1418), October 2001.
- [22]. H. Alexandre and Paqueta, "Wavelet packets-based digital watermarking for image verification and authentication", *Signal Processing* 83, 2117 - 2132, 2003.

