Medical Images Watermarking for Security in m-Health: Implementation on Smartphone Android OS

Mohamed Boussif[1], Noureddine Aloui[2] and Adnene Cherif[1]

[1] Sciences Faculty of Tunis, Laboratory of analysis and processing of electrical and energy Systems, University of Tunis El-Manar, El Manar, PB 2092, Tunisia

[2] Centre for Research on Microelectronics & Nanotechnology, Sousse Technology Park, Tunisia

Abstract

Medical data (imaging or report) are personnel information which are relative to the patient where this information is a medical secret. Therefore, in this paper, a new security system for medical imaging dedicated for m-Health is presented which is based on the high capacity robust/fragile blind watermarking of audio report in medical imaging. The audio signal is transformed with the decomposition by wavelet transform, then, we insert the normalized low coefficients of the transformed audio signal in spatial space of medical imaging to watermarked. After extraction, the imaging integrity is checked by analyzing the extracted audio. The imaging authentication is done by the robustness of watermarking against the different types of attack. The security of audio signal is done using an insertion key. The proposed algorithm is implemented on Smartphone android system, so, activities are built using XML script and Java for input speech of doctor, the insertion of this audio in medical imaging, and the extraction of an audio from a watermarked imaging. The objective of the paper is to concept a high capacity watermarking method which can store all audio report size. with an imperceptible watermark and an acceptable watermarked imaging quality and the system must be available in mobile Health system.

Keywords: *Security, Watermarking, Medical Imaging.*

1. Introduction

Like in human activities, embedded systems, such as Smartphone or tablet, tends to take an important place in the medicine field [1-2], where the exchange and storage of medical information, which were first developed around the computer, has invaded little by little the medical field, especially, the medical images which is therefore today undoubtedly one of the key elements for a medical approach in medicine, where the doctor seeks to bring together, in a virtual form, all relevant data to understand the pathology suffered by the patient, and choose the best approach therapeutic (medications, surgery, radiotherapy, etc.). Therefore, the medical imaging sharing is used in a wide variety of applications using PACS network (Picture Archiving and Communication System), which was introduced in the early 1980 to refer to computer systems of imaging communication and storage in the hospital, and was introduced Smartphone access in these last year's [3]. But, these systems require a security means for that medical secret of patients stay only accessible by the patient and her doctor. The medical imaging reliability is based on two terms: 1) The first is the integrity which is a proof that the information has not been altered or modified by non-authorized persons, several methods proposed in the literature for this security term as in [4] where the authors have proposed a watermarking system based on an image moment signature for tampering characterization i.e. integrity verification and in [5] where the authors have proposed image integrity scheme based on fixed point theory . 2) The second is the authentication which is a proof of the information origins and of its attachment to one patient, also, several methods proposed in the literature for this security term as in [6] where the authors have proposed a watermarked method based on watermark of medical imaging by patient data to enforce patient authentication and identification in radiology practices, and in [7] where the authors have proposed a novel robust data hiding scheme for image authentication. So, for securing a medical imaging in Reliability term two watermarking process are necessary, the first is robust as in [6-7] and the second is fragile as in [4-5]. But, the combination of the two-watermarking systems Leads to a large disturbance in level imaging, also, the second watermarking affect the first watermarking. So, in this work, we propose a single watermarking system for verifying the reliability (i.e. integrity and authentication) of a medical imaging.

In this paper, we propose an application for smartphone android which consist to hide the doctor's audio report in its medical imaging for the next security reasons: 1) The medical report must be hiding in its imaging, only the patient and his doctors have the access to the report. 2) The

medical imaging must be identified by this report i.e. authentication. 3) the medical imaging must be secured against modification i.e. integrity check. Therefore, watermarking the doctor's audio report in a medical imaging is motivated by several features. First, doctor's report contains a patient disease information, so, we hide this report in its medical imaging. Second, it is important to know the modification which are applied on the imaging, so, from the characteristics of audio signal (speech) as silence, we can detect the non-authorized modification applied on the medical imaging i.e. medical imaging integrity. Finally, also important to verify the attachment of attacked imaging by patient, so, we identify the medical imaging by the enhanced extracted audio using the information of patient as name which are recorded and watermarked by the doctor. The rest of this paper is organized as follows. In Section 2, we present the audio processing part which is divided in two sub part the audio processing before the insertion process and the audio processing after the extraction process. In Section 3, we detail the watermarking scheme which must be implemented on smartphone Android in Section 4. Section 5 is devoted to the experimental results and the security analyze. In Section 6 we discus and we compare our proposed with other paper. Concluding remarks are given in Section 7.

2. Audio Processing

In this section, we present the audio processing part which consist to: First, Transform in wavelet the audio signal before the watermarking process, and its transform reverse after the extraction process. Second, Denoisy the extracted audio from noise which is a low noise resulting of watermarking processes or attack. In the next of this section we detail each part i.e. wavelet transform and enhancement.

2.1 Wavelet decomposition and reconstruction

In this part, we prepare the audio signal to watermarking using the discrete wavelet decomposition. We effect a subjective test for determine the decomposition level N in different sampled frequency, therefore, its expression is given in equation (1). The discrete wavelet decomposition gives a multiscale representation of an input signal x(n), and is implemented by iterating the two channel of analysis filter bank given in equation (2) .Specifically, the wavelet decomposition of a signal is obtained by recursively applying the low/high pass frequency decomposition to the low pass output as illustrated in Fig. 1. The wavelet decomposition of the signal x is the collection of sub band of the signals, its inverse is obtained by iteratively applying the synthesis filter bank. The analysis filter bank decomposes the input signal $x(n)$ into two sub band signals, c(n) and d(n), where the signal c(n) represents the low frequency (or coarse) part of x(n), and the signal d(n) represents the high frequency (or detail) part of x(n), we denote the low pass filter by HD (analysis filter) and the high pass filter by GD (analysis filter). As shown in Fig. 1, the output of each filter is down-sampled by 2 to obtain the two sub band signals, c(n) and d(n) The number of iteration N is given by the next expression:

$$N = round\left[\frac{f_s}{10^3}\right] \quad (1)$$

Where fs, $round$, and N are the sampling frequency of audio signal, the function which allow conversion to nearest integer, and the wavelet decomposition level, respectively. The wavelet expression is given by the next expression:

$$C\_L[k] = \sum_n x[n].h_D[2k-n]\downarrow 2$$
$$C\_H[k] = \sum_n x[n].g_D[2k-n]\downarrow 2 \quad (2)$$

Where C_L[k] and C_H[k] are the outputs of the low-pass and high-pass filters, respectively, hD and gD are the coefficient of HD filter and the coefficient of GD filter, respectively. The synthesis filter bank combines the two sub band signals c(n) and d(n) to obtain a single signal y(n). The synthesis filter bank first up-samples each of the two sub band signals. The signals are then filtered using a low pass and a high pass filter. We denote the low pass filter by HR and the high pass filter by GR. The signals are then added together to obtain the signal y(n). If the four filters are designed so as to guarantee that the output signal y(n) equals the input signal x(n), then the filters are said to satisfy the perfect reconstruction condition.

$$R\_L[k] = \sum_n x[n].h_R[2k-n]\uparrow 2$$
$$R\_H[k] = \sum_n x[n].g_R[2k-n]\uparrow 2 \quad (3)$$

Where R_L[k] and R_H[k] are the outputs of the low-pass and high-pass filters, respectively, after up-sampling by 2. The choice of h and g depend of the wavelet.

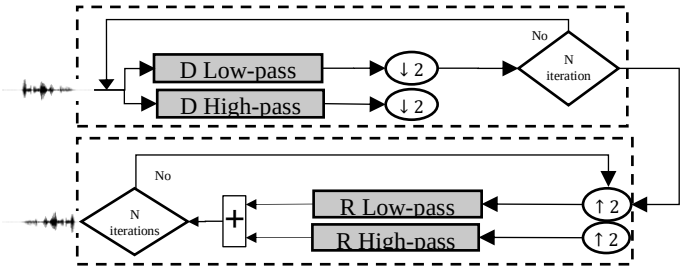


Fig. 1. The DWT/IDWT decomposition schema. The DWT process is before the watermarking and the IDWT process is after extraction process.

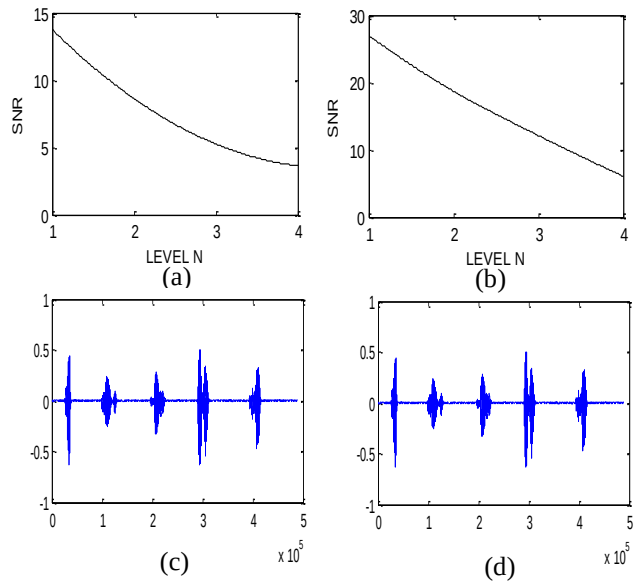


Fig. 2(a) SNR variation in function of wavelets Level decomposition for an audio sampled at 22050 Hz. (b) SNR in dB variation in function of wavelets Level decomposition for an audio sampled at 44100 Hz. (c) Original audio sampled at 44100 Hz. (d) Encoder/Decoder audio with N=4.

2.2 Extracted Audio Enhancement

For denoisy the decoded audio signal we use the denoising system proposed in paper [8] by STEVEN F. BOLL, which consist to eliminate the noise in the transformed domain FFT passing through the next step: In step 1, The input signal is windowed by Hanning window of length $round(0.31 \times f_s)$. In step 2, The windowed audio signal is transformed by the fast Fourier transform (FFT). In step 3, we compute the magnitude, we subtract the bias, finally, we rectify the half-wave and we reduce the noise residual. Then, we compute the speech activity detector. In step 4, we attenuate signal during non-speech activity i.e. thresholding. Finally, in step 5, we find the enhanced audio by the inverse transformation (IFFT).

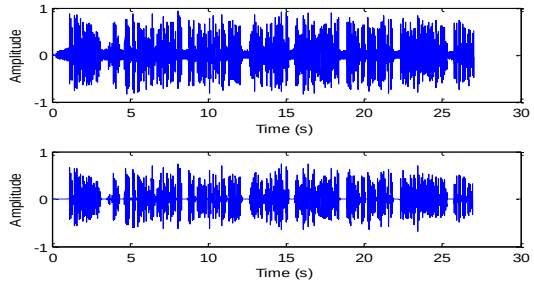


Fig. 3 STEVEN F. BOLL enhanced method: (a) original speech with noise. (b) enhanced speech.

3. Proposed Watermarking Scheme

In this section, we explicit the proposed watermarking system before detailing the mixing function. As shows in Fig. 5, the medical imaging to watermarked is divided in block of size b, for each block, we insert the i-th normalized low coefficient of the DWT decomposition of the all input audio in the average value of i-th block using the key θ which is the de-quantization of K_w key with $-\pi/2$ as minimum value and $\pi/8$ as quantization pas. The wavelet level N is given in equation (1). The mixed function which allow the insertion of a numerical value in another numerical value is given by the following expression:

$$w^f(I_i, w_i) = \begin{cases} k_i \dfrac{\pi}{f} - \dfrac{\theta}{f} + \text{acos}(w_i) & \text{if } k_i \, pair \\ k_i \dfrac{\pi}{f} - \dfrac{\theta}{f} - \text{acos}(w_i) & \text{if } k_i impair \end{cases}$$

$$k_i = r\left(f \times \frac{I_i - \theta}{\pi} \right) \quad (4)$$

Where the function r allows conversion to nearest integer. f and θ are the frequency and the dephasing, respectively. w^f is the mixing function. I_i and w_i are the pixel to watermarked and the watermark audio sample, respectively. k_i is an integer. For writing the mixing function as a single equation we replace + by $(-1)^{k_i}$ with its expression in equation (4):

$$w^f(I_i, w_i) = \frac{\pi}{f}\left[k_i - \frac{\theta}{\pi} \right] + (-1)^{k_i} \text{acos}(w_i) \quad (6)$$

Now, we replace k_i in equation (4) with its expression in equation (6) for find the final mixed function:

$$w^f = \frac{\pi}{f}\left[r\left(f \times \frac{I_i - \theta}{\pi} \right) - \frac{\theta}{\pi} + (-1)^{k_i} \frac{f}{\pi} \text{acos}(w_i) \right] \quad (7)$$

The reciprocal function of the mixing function which used for extracted the watermark from the image is given by the next equation:

$$w_{ex_i} = w^{-1^\theta}(I_i) = \cos(f \times I_i + \theta) \quad (8)$$

Where I_{w_i} and w_{ex_i} are the i-th watermarked pixel and the i-th extracted watermark, respectively. To note that I_i is a pixel for a block of sizes 1, and is the average value for a block of sizes b. For example, if I, w and φ are the original image, the watermark (Low coefficient of audio sample), and the key of insertion, respectively, where:

$I = \begin{pmatrix} 013 & 245 \\ 096 & 006 \end{pmatrix}$, $w = \begin{pmatrix} 0.13 & 0.01 \\ -0.56 & 0.21 \end{pmatrix}$, and $K_w = 194$.

For $b = 1$ and $f = 0.2$, we find the watermarked image I_w using the equation (7) as following:

$$I_w = W^{f,\theta}(I, w) = \begin{pmatrix} 005 & 241 \\ 103 & 005 \end{pmatrix}$$

To determine the extracted watermark w_{ex} must use the reciprocal function W^{-1} which is given in equation (8), we find the extracted watermark w_{ex} :

$$w_{ex} = \cos\left(f \times \begin{pmatrix} 005 & 241 \\ 103 & 005 \end{pmatrix} + \theta\right)$$

We replace f and θ with its value for find the extracted watermark which must be approach to w or $w_{ex} \approx$ w.

$$w_{ex} = \begin{pmatrix} 0.16 & -0.08 \\ -0.55 & 0.16 \end{pmatrix}$$

Now, we take $b = 2$ and we insert the same watermark with the same f and key in I:

$$I = \begin{bmatrix} 007 & 020 & 010 & 032 \\ 105 & 000 & 109 & 015 \\ 002 & 245 & 007 & 013 \\ 029 & 008 & 068 & 004 \end{bmatrix}$$

For $b = 2$ and $f = 0.2$, we find the watermarked image I_w using the equation (7) as following:

$$I_w = \begin{bmatrix} 011 & 024 & 005 & 028 \\ 108 & 003 & 105 & 011 \\ 003 & 246 & 006 & 012 \\ 030 & 008 & 068 & 004 \end{bmatrix}$$

To determine the extracted watermark w_{ex} we use the reciprocal function W^{-1} which is given in equation (8), we find the extracted watermark w_{ex} :

$$w_{ex} = \cos\left(f \times \begin{pmatrix} 36.5 & 37.25 \\ 71.75 & 22.5 \end{pmatrix} + \theta\right)$$

We replace f and θ with its value for find the extracted watermark which must be approach to w i.e. $w_{ex} \approx$ w.

$$w_{ex} = \begin{pmatrix} 0.14 & 0.00 \\ -0.57 & 0.19 \end{pmatrix}$$

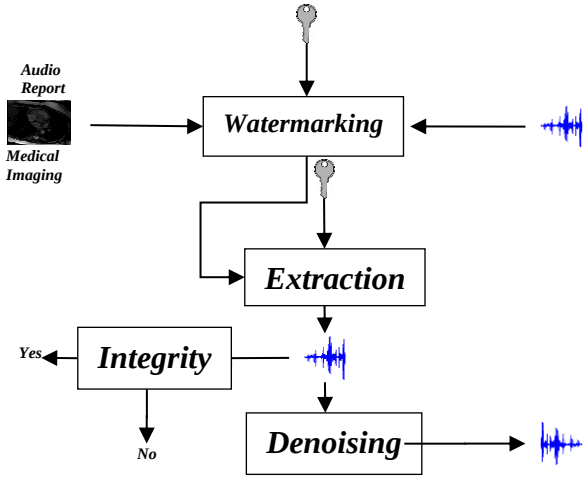


Fig. 4. Graphical illustration of the proposed watermarking system used in m-Health (Smartphone or Tablet).

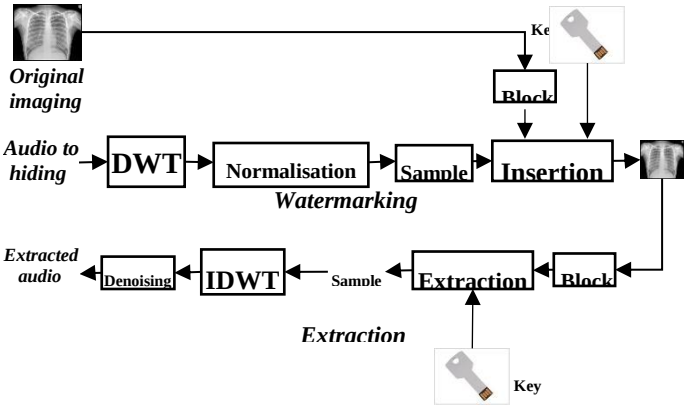


Fig. 5 Our proposed watermarking system. The DWT and IDWT process are illustrated in Fig. 2.

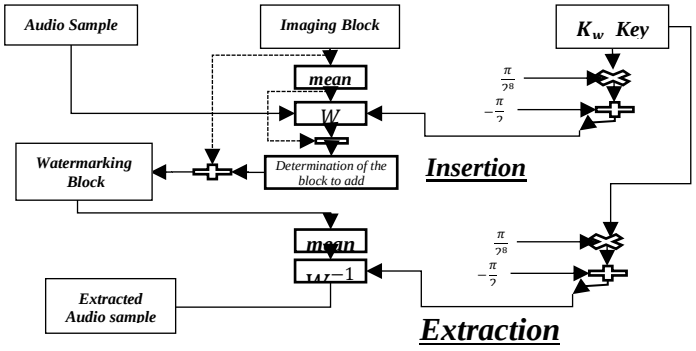
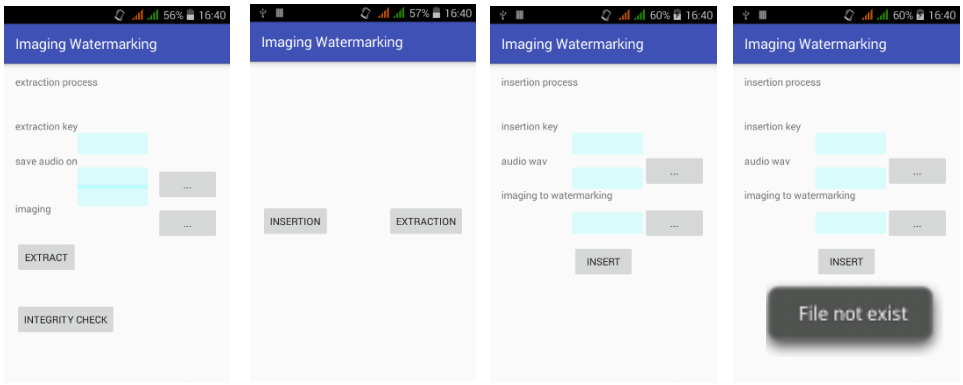


Fig. 6 The proposed insertion/extraction process. The function W is given in equation (7).

4. Implementation on Smartphone Android system

To implement the proposed schema on Smartphone android embedded system we must pass through the next three steps: In first step, we implement the algorithm in MATLAB@ tool for simulation and test. Then, in second step, after fixation of parameter and optimization of program, we convert the MATLAB function to JAVA package (this package named Watermarking), using application COMPILER of MATLAB, this package container a class with three methods: Insertion, Extraction and IntegrityCheck. In final step, we prepare the application Android (APK) using Android Studio tool. In this step, we prepare the next activity using the XML for graphic discerption and JAVA for event and processing: MainActivity, which is the home activity i.e. activity that starts when the user opens the application. In this activity,



Extraction_Activity ***Main_Activity*** ***Insertion_Activity*** ***Exception***

Fig. 7. Screen capture of the proposed application activity in Smartphone Android 4.4.4 System.

we define two buttons named B1 and B2. The event of B1 is to create the InsertionActivity and B2 to create the ExtractionActivity (the creation is done by the method OnCreate, the click event is done by the method OnClick and the added of listening is done by the method setOnClickListener). InsertionActivity, which is the activity of insertion as shower in Fig.7 this activity allows: 1) Read an imaging Dicom (.dcm file) using the class Dicom(we use the DicomDroid library). 2) Read a report audio (.wav file) using the package AudioStream. 3) Input a key for watermarking 4) Inset the audio in the imaging using the package Watermarking. 5) Save the watermarked imaging using the class Dicom (we use the DicomDroid library). ExtractionActivity, which allow extraction an audio report from a watermarked medical imaging. In this activity we must: 1) Read a watermarked medical imaging (.dcm file) using the class DICOM. 2) Input the key for extraction of audio report. 3) Extract the audio from the imaging using the package Watermarking. 4) Save the audio report using the package AudioStream. 5) After extraction of audio we can verify the integrity of the imaging.
The passage from an activity to another is done by the object Intent and the access to the XML description is done by the class R.

5. Experimental Results and Security Analyze

Experiments were conducted on four sets of medical images of different modality, sizes and depth: Magnetic Resonance imaging (modality MRA) of 240×320 pixels and 12-bit depth, Radio Fluoroscopy imaging (modality RF) of 512x512 pixels and 8-bit depth, Digital Radiography imaging (modality CT) of 512x512 pixels and 12-bit depth, Secondary Capture imaging (modality MR) of 560x1558 pixels and 12-bit depth. Some samples of our dataset are given in Fig. 8. We decided to use the peak signal to noise ratio (PSNR) in order to measure the distortion between an imaging I and its watermarked imaging I_{wdec}:

$$PSNR(I, I_{wdec}) = 10Log_{10}\left(\frac{\left[2^{dep}-1\right]^2}{MSE}\right)$$
$$MSE(I, I_{wdec}) = \frac{1}{L}\sum_{k=1}^{L}\left[I(k) - I_{wdec}(k)\right]^2 \quad (9)$$

where L corresponds to the number of pixels of the image I, and dep corresponds to its bit's depth. So, we decided to use the signal to noise ratio (SNR) to measure the distortion between an audio signal to watermarked S and its extracted audio signal S_{ex}:

$$SNR = \frac{\sigma^2(s)}{\sigma^2(s - s_{ex})} \quad (10)$$

Where σ the standard deviation defined as:

$$\sigma_x = \sqrt{E\left[x^2\right] - E[x]^2}$$
$$E[x] = \sum_{i=1}^{n} x_i p_i \quad (11)$$

For integrity check we use the histogram of extracted audio for create elements from audio which are sorted into 5 equally spaced bins between the minimum and maximum values of extracted audio, for example, if the minimum and maximum values equals to -1 and 1 respectively, then, $hist(-2)$ compute the number of sample in $[-1, -0.6[$, $hist(-1)$ compute the number of sample in $[-0.6, -0.2[$, $hist(0)$ compute the number of sample in $[-0.2, 0.2[$, $hist(1)$ compute the number of sample in $[0.2, 0.6[$, and $hist(2)$ compute the number of sample in $[0.6, 1]$. So, the imaging is not modified if:

$$\sum hist - hist(0) \leq \beta \times hist(0) \quad (12)$$

Where $hist$ and β are the histogram of extracted audio and a number between 0 and 1, respectively. As shown in Table 2, we find a best configuration for $\beta = 0.5$.

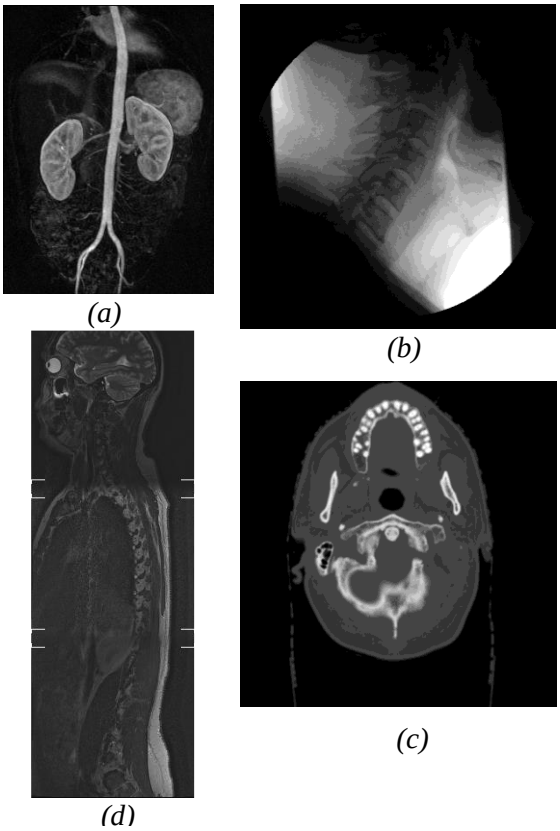


Fig. 8 Samples of our imagery test sets. (a) Modality MRA imaging. (b) Modality RF imaging. (c) Modality CT imaging. (d) Modality MR imaging.

6. Discussion and Comparison

In this section, before comparison with other methods and papers, we focus in result discussion where the experimental results and security analyze show that: In Fig 10, we can conclude that the watermark is imperceptible and the mean of watermarked imaging PSNR is equal to 60, as shown in Table 1, so, the quality of watermarked imaging is acceptable and can be used in medical imaging. The mean of extracted audio SNR is equal to 14, as shown in Table 1, So, the quality of extracted audio (watermark) is acceptable. The watermarking robust to attack such as compression, filtering, (see Fig 9 (a), (b) and (c)), also, as shown in Table 2 we can detect the unauthorized modification for the watermarked medical imaging. Fig 9 (d) shows that the execution time in MATLAB for an imaging of 512X512 full watermarking with audio equal to 10 second for insertion and 5 second for extraction, so, the proposed system posed a low complexity and can used in Smartphone.

As shown in Table 3, To further validate the proposed method, we compared our method with the discussed in: Fawad ur Rehman et al. [9] have proposed a robust audio watermarking in image based on the entropy using Wavelet Transform. (Published in 2009). Rabia Khan et al. [10] have proposed a robust audio watermarking in image based on the texture using Wavelet transform. Bouslehi Hamdi et al. [11] have proposed a new approach combining speech chaotic encryption with fragile image semi-blind watermarking for audio securing and intrusion detection in spatial domain. (Published in 2013). Mauro Barn et al. [12] have proposed a hiding method of signal in image (Published in 2001). Mourad Talbi et al. [13] have proposed a non-blind robust watermarking signal in image based on transformations LWT, FFT and DCT. (Published in 2015).

Table 2 Tamper detect (fragility) test of watermarked imaging with usual attacks for size block equal to 2, f=0.2 and $\beta = 0.5$, and different images.

Attack	∑hist -hist(0)	β×hist(0)	Integrity
Without	36075	41962	Yes
Compression (80%)	42223	38889	No
Filtering 2x2	87108	16446	No
Cropping (1/6)	75005	28343	No
Noise (0.005)	51287	44667	No
Contrast Adjustment	52399	43555	No

Table 1 SNR of extracted audio (watermark) and PSNR of the full watermarked medical imaging set for size block equal to 2 and f=0.2.

Images	a	b	c	d
PSNR of watermarked imaging	66.8575	53.6389	66.8783	66.8623
SNR of extracted audio	13.8883	13.2132	15.0818	14.4839

Table 3. Comparison of the proposed watermarking system with others proposed methods.

Papers	Availability in m-health	Fragility	Robustness	Capacity	Watermarked image PSNR	SNR of extracted audio
Fawad ur Rehman et al. [9]	No	No	Yes	-	39	+∞
Rabia Khan et al. [10]	No	No	Yes	-	30	+∞
Bouslehi Hamdi et al. [11]	No	No	Yes	0.03	-	26
Mauro Barn et al. [12]	No	No	Yes	-	-	-
Mourad Talbi et al. [13]	No	No	Yes	0.12	52	16
Proposed	Yes	Yes	Yes	0.25	60	14

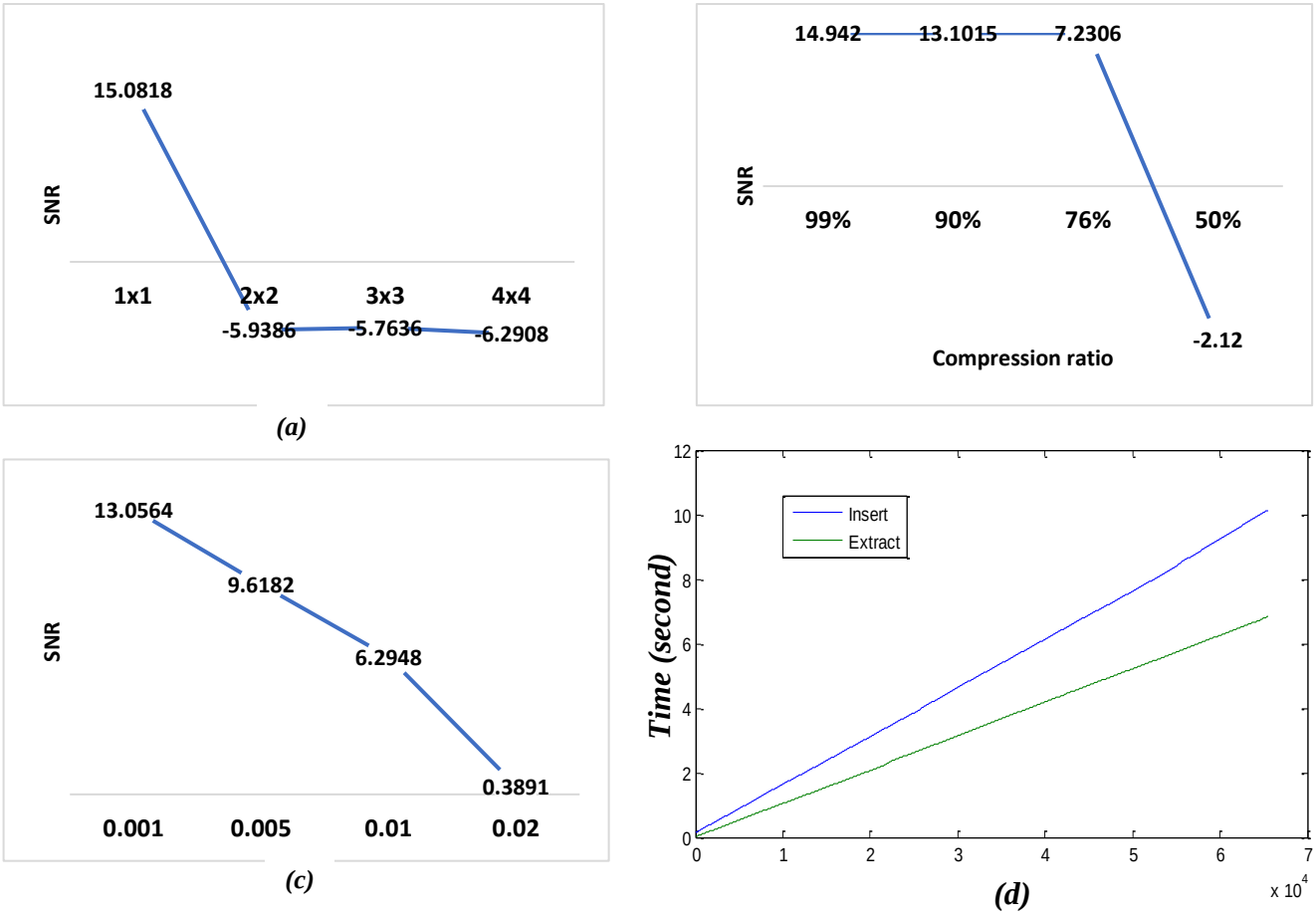


Fig. 9 Evolution of the proposed watermarking system for block size equal to 2 and the parameter ***f*** equal to 0.2. (a) robustness to average filtering. (b) robustness to Jpeg compression. (c) robustness to salt & pepper noise. (d) Time execution in Matlab@ of the insert and extract process.

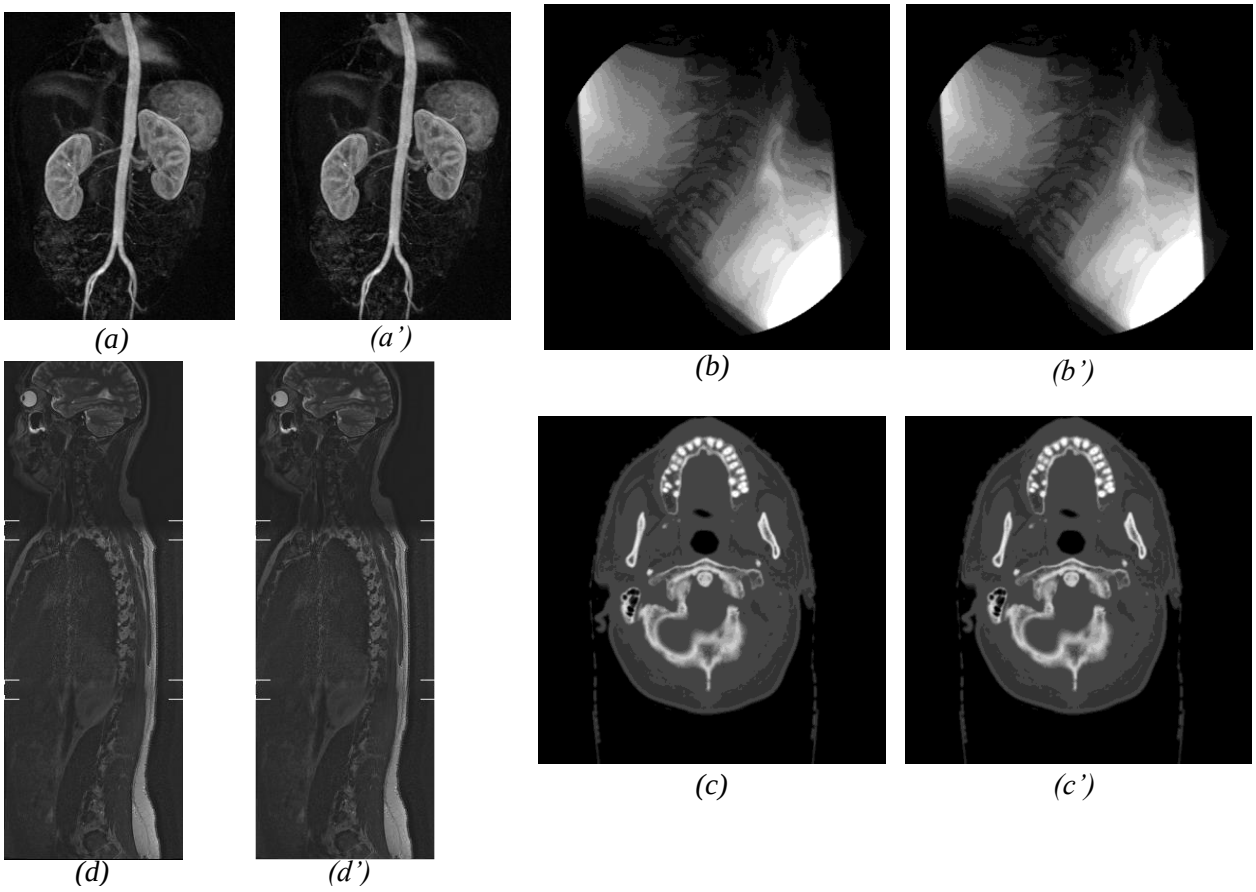


Fig. 10 (a), (b), (c) and (d) are the original images. (a'), (b'), (c') and (d') are the full watermarked images, respectively.

7. Conclusion

In this paper, we have proposed a security system for the reliability of medical images based on hiding of medical audio report of doctor in medical imaging, the experiment result show that the imaging quality is acceptable and the security analyze shows that the watermark robust to attacks as compression noise…, also, we have detected the non-authorized modification on the medical imaging as contrast adjustment, filtering. For availability in m-Health, we have implemented the system in Smartphone Android system using Android Studio tool.

Acknowledgment

We are grateful to the reviewers for their valuable comments that helped us to improve the quality of the paper.

References

[1] Bruno M. C. Silva, Joel J. P. C. Rodrigues, Ivo M. C. Lopes, Tiago M. F. Machado, and Liang Zhou," A Novel Cooperation Strategy for Mobile Health Applications," in IEEE JOURNAL on selected areas in communications/supplement, vol. 31, no. 9, pp.28-36 September 2013.

[2] K. N. Dias, D. Welfer, J. F. Kazienko and R. C. F da Silva," A Novel iOS m-Health Application to Assist the Hospital-Acquired Pneumonia Diagnosis and Treatment," in IEEE latin america transactions, vol. 14, no. 3, pp.1335-1342, march 2016.

[3] Constantinescu L, and Jinman Kim, SparkMed: A Framework for Dynamic Integration of Multimedia Medical Data into Distributed m-Health Systems, in IEEE Transactions on Information Technology in Biomedicine, 2011, pp. 40-52.

[4] G. Coatrieux, H. Huang, H.Z. Shu, L.M. Luo and Ch. Roux, "A Watermarking Based Medical Image Integrity Control System and an Image Moment Signature for Tampering Characterization," in IEEE transactions on information technology in biomedicine, pp.1-11, 2013.

[5] Xu Li, Xingming Sun and Quansheng Liu," Image Integrity Authentication Scheme Based on Fixed Point Theory," in IEEE transactions on image processing, vol. 24, no. 2, pp.632-645, 2015.
[6] Seenivasagam Vellaisamy and Velumani Ramesh," Inversion attack resilient zero-watermarking scheme," in IET Image Processing, Vol. 8, Iss. 12, pp. 718–727,2014.
[7] You-Hsiang Hsu, Yeni Anistyasari, Yi-Hui Chen and Kai-Lung Hua," A Novel Robust Data Hiding Scheme for Image Authentication for medical image authentication," Asia Pacific Conference on Multimedia and Broadcasting, Bali, 23-25 April 2015.
[8] STEVEN F. BOLL," Suppression of Acoustic Noise in Speech Using Spectral Subtraction", in IEEE Transactions on Signal Processing, 27(2), pp 113-120, 1979.
[9] Fawad ur Rehman, Rabia Khan, Naveed Iqbal and Fazal Ahmed," Entropy based Audio Watermarking in Image using Wavelet Transform," ISECS International Colloquium on Computing, Communication, Control, and Management, pp 478-481, 2009.
[10] Rabia Khan, Abdul Ghafoor and Naveed Iqbal Rao," A Blind Image Adaptive Watermarking Scheme for Audio using Wavelet Transform," in International Conference on Digital Image Processing, IEEE computer society, pp.67-71,2009.
[11] Bouslehi Hamdi, Seddik Hassene," A new Approach Combining Speech Chaotic Encryption with fragile Image Watermarking for audio securing and intrusion detection," in IEEE International Conference on Electrical Engineering and Software Applications (ICEESA), pp. 1-6,2013.
[12] Mauro Barn and Franco Bartolini," Watermark Embedding: Hiding a Signal Within a Cover Image," in IEEE Communicatioiis Magazine, pp. 102-108, 2001.
[13] Mourad Talbi, Siraa Ben Ftima, Adnen Cherif," Image Watermarking using Data Compression," in IEEE World Symposium on Computer Networks and Information Security (WSCNIS), pp.1-9, 2015.