A Novel CT Scan Images Watermarking Scheme in DWT Transform Coefficients

Muath AlShaikh[2], Lamri Laouamer[1, 2], Laurent Nana[2], Anca Pascu[2]
[1]Department of Management Information Systems, CBE,
Qassim University, P.O. Box 6633, Buraidah, 51452, KSA,
[2]Lab-STICC (UMR CNRS 6285), University of Western Brittany, Brest,
20 avenue Victor Le Gorgeu, BP 817 - CS 93837, 29238 Brest Cedex, France

ABSTRACT
Medical images transmitted through the communication networks needs more robust and reliable algorithms. In this paper, we propose a new medical image watermarking scheme of CT Scan images based on the wavelet transform. The main contribution in this paper lies in the extraction process that improves watermarking scheme robustness and efficiency against several scenarios of attacks. The obtained results are very encouraging, especially when the watermark is invisible. It became very helpful for authenticity and integrity of the DICOM images. Moreover, Our images present a high resistance against several dangerous attacks known in the image processing such as rotation and noise. This means that the proposed approach achieves a remarkable robustness.

Keywords:
Wavelets; Watermarking; Robustness; Attacks; Medical Images.

1.Introduction

The handling of numeric information in hospitals, especially in radiology systems, the storing and electronic transfer of medical images between hospital services, has become the central point of the information infrastructure of modern healthcare systems. The recent development of Information and Communication Technology (ICT) has strengthened the potential of tele-medicine, and more precisely of tele-consultation, tele-surgery and tele-diagnosis. The evolution in the ICT domain provides new solutions for storage, access and broadcasting of medical information, including medical images. Nevertheless, the use of ICT leads to new risks for the security of patient data, especially for personal data transmitted through the network and accessible via the internet. Given that all patient data are subject to medical secret, their confidentiality and their robustness should be ensured [1].

Watermarking is one of the best security solutions, it is subjected to cover the security shortcoming issues. Regarding medical image, watermarking method should be invisible, high imperceptible (transparency) with high fidelity. Where the physician diagnosis is based on those images, any slight modification will affect the treatments and the results. The general scenario of the digital watermarking methods is to hide data into a medical image, where the only authorized user can extract them and verify its integrity and authenticity [2].

Watermarking methods can be classified based on the embedding manner into spatial and frequency domains. The spatial domain provides less complexity, easy and fast embedding and extraction processes. Whereas, it presents a weakness in term of robustness against signal processing attacks. The most known techniques are the Least Significant Bit (LSB) [3] and the Local Binary Pattern (LBP) [4]. However, Frequency domain provides more robustness against different attacks. But presents a high complexity during the embedding and extraction phases. The most known techniques are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) [5], Discrete Fourier Transform (DFT) [6], Singular Value Decomposition (SVD) [7].

Indeed, the watermarking approaches in the frequency domain are more robust than approaches operating in the spatial domain. In this paper, we achieve our watermarking framework in the frequency domain which make it possible to ensure the image's authenticity and as a consequence the reliability. Whereas, our approach presents a high robustness and less complexity regarding the proposed algorithms in the literature.

We consider in particular the Digital Imaging and Communication In Medicine (DICOM) in our work. DICOM medical images have a special structure composed of two parts: the header and pixel data. The header contains the patient information like patient name, physician name and other information. For the pixel data, it consists of the image data to be displayed [8].

In the second section we present the wavelets decomposition principle. The third section deals with related works that address medical images authenticity and robustness. The fourth section is dedicated to the new watermarking approach we have proposed. In the fifth section, we present the test results in our algorithm. The paper ends by a conclusion and perspectives in the sixth section.

Manuscript received January 5, 2016
Manuscript revised January 20, 2016

1.1 Wavelet Decomposition Principle

Discrete Wavelet transform (DWT) is a mathematical model for decomposing a signal. It is valuable for handling of a non-fixed signals. The decomposition is based on a modest waves called wavelets. The one level wavelets decomposition principle for a given image is illustrated in figure1. In fact, this decomposition can have several levels called n-levels, multi-resolution domain. The result of this decomposition gives four sub-bands: Low-Low (LL), Low-High (LH), High-Low (HL) and High-High (HH). The LL sub-band contains the estimated original image while the other sub-bands contain the missing details. The LL sub-band output from any stage can be decomposed further [5].

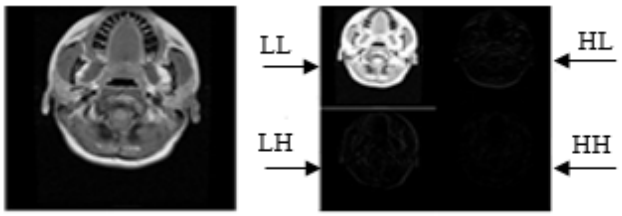

Figure. 1. 2D Medical image wavelet transform with one level decomposition.

The multi-resolution domain offers several advantages. The first advantage is that it defend for the used watermarking algorithms to be robust against JPEG 2000 compression. The second advantage is its power to choose the frequency set that is watermarked to control the most noticeable visual degradation in low and high frequencies. The embedding in the low frequency sub-band provides a high robustness, but the embedded watermark become visible which affects on the image quality. This means a degradation in the watermarked image [2]. While the embedding in the high frequency sub-band supports more visibility and low degradation, but less robustness [5]. This property is due to the impairment of the visual human contrast sensitivity at high frequencies [7].

2. Related Works

Among the existing wavelet based watermarking techniques addressing the authenticity and integrity of DICOM medical images, we can mention those based on the multiple watermark achievement [1], those based on different levels wavelet decomposition [5], those which perform watermarking on regions of interest (ROI) [9] or even combining ROI and non-region of interest (NROI) [10].

Other interesting works have been achieved in the image watermarking field. The authors in [11] applied image watermarking with multiple watermarking techniques based on Haar-DWT with four levels. Multiple watermarks are also used: the reference watermark, Tamper Assessment Factor (TAF), and physician's signature. When using the Haar wavelet technique the authenticity was satisfied against some kind of attacks, but for other attacks such as rotation and cropping, contrast, flip, blurring, sharpening, salt and pepper noise, and Gaussian noise, we note a remarkable lossless of the embedded data.

In [12] an algorithm of watermark embedding is proposed. It consists to divide the image into three wavelet transform by using a graph theory approach to find optimal places to embed the watermark key. The algorithm ensures a good invisibility and robustness, especially against LSB attacks and is reliable enough for tracing the intruder.

Authors in [13] proposed blind techniques using both DWT and DCT to improve the robustness and the invisibility of watermark. It is based on the regions of interests ROI. The embedding process consists to apply Arnold transform to the binary watermarking image, then decompose the image into one layer DWT, after that compute the DCT for the whole LL part to get featured vector. The lowest frequency in feature vector is chosen and one gets the sign sequence. The experimental result shows a good robustness against different attacks and high weakness when applying JPEG compression and Median Filter attacks.

In [14] the authors proposed an encryption and watermarking technique to improve the authenticity and the integrity of medical image. Firstly, the watermark phase is based on quantization index modulation (QIM) in the spatial domain. It is applied by embedding two messages as watermark (every message contains a code to verify the authenticity). Then, the encryption phase based on the symmetric technique Advanced Encryption Standard (AES) using Cipher Block Chaining (CBC) as mode of operation. It is applied to increase the integrity of medical image. The performance evaluation shows that the PSNR achieved the 60 dB and 105 dB for ultrasound and PET image. For the capacity issue, the size of the bits that was used for the watermark and encryption are enough and the capacity increases when the PSNR decreases.

We find also in [15] a proposed blind dual watermarking for binary image which is based on DWT and uses two watermark layers. The first layer watermarking consist to the original watermark signal. It is embedded in the lowest frequency sub-band of the wavelet domain. The second layer watermarking as well as a mapping between the two layer watermarks is built by combining the encryption technique with the invariant pixel distribution features extracted from the binary image. In comparison with usual single DWT techniques, the results obtained show a better robustness, especially in Gaussian noise, JPEG compression, and some geometric attacks, but present a less robustness against some attacks such as scaling and rotation.

Authors in [16] proposed a blind watermarking technique in the DWT domain, based on a chaotic mapping and a dynamic blocking. Arnod's Cat Map is used to produce the watermark key used in the LL (3) step of the DWT

transform. The key can therefore be produced in the extraction phase without the need of the original image or the transmitted information. The embedding of data was done in LH (3) and HL (3) by using the special dynamic blocking method and wavelet coefficient quantization. In the extraction process, they decompose the image, then decode the LL3 by chaotic map to get the key an extract the watermark. The experimental results show that the algorithm achieves a significant high security and robustness against several attacks such as JPEG compression, noise and median filter but not satisfy robustness against blurring attack.

The work presented in [17] showed a blind reversible watermark approach for medical images based on histogram shifting in wavelet domain. An integer wavelet transform is applied to map the integer host image components to integer wavelet coefficients. Finally, the watermark information is embedded into the high frequency sub-band of the transformed image. The PSNR of the extracted image exceeds the 53 dB in some non-geometrical attacks. The proposed algorithm doesn't take in consideration the case of geometric attacks.

The authors in [18] proposed a blind robust watermarking approach based on nonnegative matrix factorization (NMF) in DWT domain. The watermark is embedded into the "encoding" matrix, then the matrix is reconstructed. The experimental results show a robustness against JPEG compression, Gaussian low pass filtering and noise addition, but a weakness against geometrical distortions like rotation, cropping and resizing.

The author in [19] proposed a robust watermarking technique in the frequency domain. It is based on DWT three levels. The watermark embedded in the low frequency sub band using blending technique. In the embedding phase, three levels DWT transform are applied both to the original and the watermark image. Then, embedding the watermark image into the original image by using the linear interpolation (Equa. 1). Finally, inverse DWT (DWT-1) is applied to obtain the watermarked image. In the extraction phase, three levels DWT transform are applied to the watermarked image and original image. Then, they extract the watermark by using the linear interpolation (Equat.2)

$$iw_{mi} = k \times ll_3 + q \times w_{m3} \quad (1)$$

$$R_w = w_{mi} - k \times ll_3 \quad (2)$$

where $k, q \in [0,1]$, ll3 the 3-DWT original image, wm3 the 3-DWT watermark image, iwmi the watermarked image in the ll3, , Rw retrieved watermark. The quality of the watermarked image and the retrieved one is depending on the aspects k and q. The approach presents a high performance in case of no attacks, but after applying the attacks, especially the JPEG compression, adding noise and filtering attacks, the retrieved watermark image quality (PSNR) was around 22 dB which is qualified as a non robust algorithm.

Another blind watermarking approach was presented in [20], where the technique aimed to detect the tamper zones and robustness against signal processing attacks. The approach was based on DWT and cat map. The approximation discrete wavelet transformation coefficient of a block was embedded as a watermark in the detail coefficients of an another block. The experimental results show acceptable watermarked image after embedding. Moreover, after the attacks, the extracted watermark was robust against the compression and rotation attacks, where the PSNR was around 37 dB, but after the noise and filter attacks, the extracted watermark was distortion, where the PSNR was around 20 dB.

From the previous related works, we can conclude that the watermarking approaches in frequency domain still present some gaps against some scenarios of attacks, and also for the imperceptibility which remains a negotiate issue. Moreover, the computational complexity in watermark embedding/extraction has to be taken into account especially for a real time application.

3.Proposed Watermarking Algorithm

In our work, we apply one level DWT for both the used watermark and the original images. Then, we embed the watermark in the original image by using linear interpolation presented by our team in works [2, 21, 22, 23]. Linear interpolation provides an imperceptible of the watermark without degradation in the quality of the watermarked image.

Our technique considers two phases: embedding and extraction processes. In the embedding phase, one level DWT is applied to the watermark and also the original image. Then, we embed the watermark using linear interpolation. The inverse DWT (DWT-1) is applied to the DWT coefficients of the watermarked image in order to obtain a "readable" watermarked image. In the extraction phase, one level DWT is applied to the watermarked and watermark images. We achieve the embedding process using linear interpolation to get a new watermarked image. Then, the attacked watermarked image with the new watermarked image is an unmarked using linear interpolation. Finally, DWT-1 will be applied to the extracted attacked DWT watermark image to achieve a readable attacked watermark image.

3.1Watermark Embedding.

Figure 2 illustrates the watermark embedding process which is based on the level-1 wavelet decomposition. The watermark is embedded through a linear interpolation

$$i_w = (1 - t)w + ti \quad (3)$$

Where $t \in]0,1[$ and i, w and iw are respectively the original image, the watermark and the watermarked image. wDWT , iDWT and iwDWT are respectively the watermark, the original image and the watermarked image in wavelet decomposition.

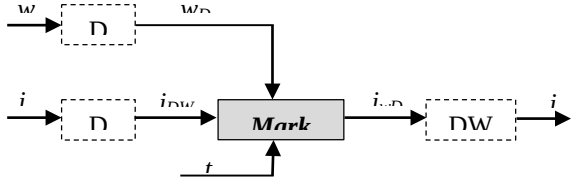

Figure 2. Watermark Embedding Process.

The main steps of the embedding process are as follows:

1. Divide the original image *i* and the watermark *w* into 8×8 blocks.
2. Apply the DWT (one level) to each block obtained in step one for the images *i* and *w*. The matrices of the DWT coefficients give as results the i_{DWT} and w_{DWT} matrices.
3. Mark w_{DWT} in i_{DWT} by the following equation:

$$i_{wDWT} = (1-t)w_{DWT} + t i_{DWT} \qquad (4)$$

where iwDWT are the watermarked matrices (visually this matrix is unreadable, so to make it readable we need to apply the step 4) and t is a given value $\in]0,1[$.

4. Apply the DWT inverse operation (DWT-1) to all the blocks in order to obtain the readable image iw

3.2 Watermark Extraction

The novelty and the contribution of this paper is in the extraction phase, which takes into account the watermarked image in the extraction process and not just the attacked watermarked image. Figure 3 shows the extraction scheme. We denote by "mark", the embedded watermark by linear interpolation, while "extraction" refers to the watermark inverse embedding:

$$w_a = \frac{1}{t} w_{iDWT} - \frac{1-t}{t} i_{wa} \qquad (5)$$

Where w_a, i_{wa} and w_{iDWT} are the extracted watermark, the attacked watermarked image and inverse DWT of watermark image, respectively. We resumed this process as follows:

1. Apply the DWT one level of each block of *w* and i_w to obtain w_{DWT} and i_{wDWT}.
2. Mark w_{DWT} in i_{wDWT} by using equation (6) to obtain w_{iDWT}.

$$w_{iDWT} = (1-t)i_{wDWT} + t w_{DWT} \qquad (6)$$

3. Apply the DWT one level of each block of the attacked watermarked image i_{wa} to obtain i_{waDWT} which is the DWT coefficient matrix of the attacked watermarked image.

4. Unmark i_{waDWT} , w_{iDWT} with the same *t* value used in the embedding process using the equation (7) to obtain w_{aDWT} .

$$w_{aDWT} = \frac{1}{t} w_{iDWT} - \frac{1-t}{t} i_{waDWT} \qquad (7)$$

5. Apply the DWT inverse for all the blocks on $\boldsymbol{w_{aDWT}}$ in order to obtain a readable and significant image wa .

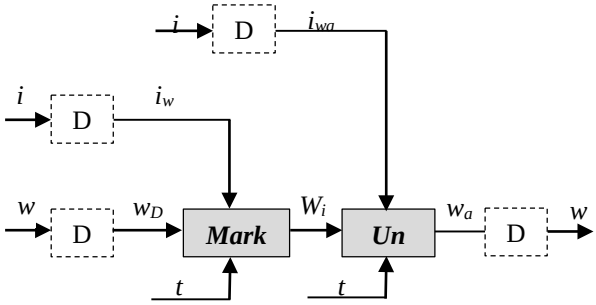

Figure 3. Watermark Extraction Process.

4.Experimental Results

We performed our tests on a gray CT scan medical image database that contains 250 images of size 256 × 256. The original images come from [24] while the watermark image contains the full name of one of this paper authors. The watermarking process has as the secret key, it varies exclusively between 0 and 1 in order to achieve a visible /invisible watermarking. Similarly, we tested our proposed watermarking algorithm against several kinds of attacks introduced in Stirmark Benchmark [2, 23] such as: median filtering, JPEG compression, rotation, adding noise and PSNR attacks. Through the obtained results we concluded that the invisible watermarking (where t close to 1) gives better results compared to the visible one (t = 0.2) and the semi-invisible one (t = 0.5) where the extracted watermarks are similar to the original one. As for the robustness of the proposed approach, we conducted tests in several cases (according to the values of t). Figure 4.A illustrates the head original image, watermark image and head watermarked images obtained after applying our algorithm with several values of the secret key t (0.2, 0.5 and 0.98) for a visible, semi-visible and invisible watermarking.

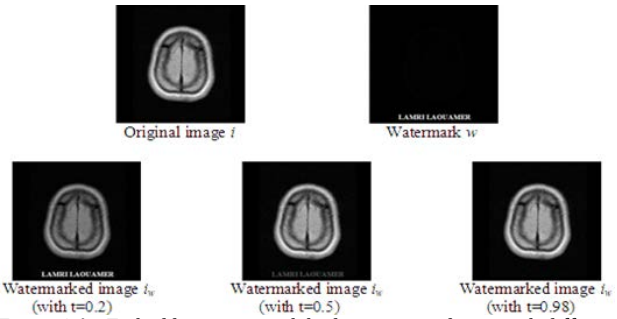

Figure 4.A. Embedding watermark by linear interpolation with different values of t (secret key).

In figure 4.B, the first level (a) shows the attacked watermarked images, the second level (b) shows the extracted attacked a watermark image and the third level (c) shows the differences between the original watermark image and the extracted attacked watermark in case of t=0.98.

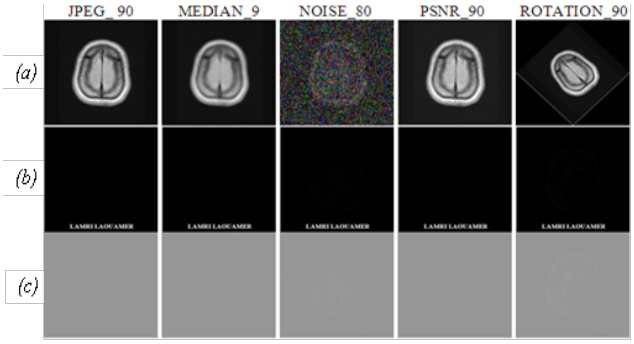

Figure 4.B. Watermark Extraction Results when t=0.98

In figure 4.C, the first level (a) shows the attacked watermarked images, the second level (b) shows the extracted attacked watermark image and the third level (c) shows the differences between original watermark image and extracted attacked watermark in case of t=0.5.

In figure 4.D, the first level (a) shows the attacked watermarked images, the second level (b) shows the extracted attacked watermark image and the third level (c) shows the differences between original watermark image and extracted attacked watermark in case of t=0.2.

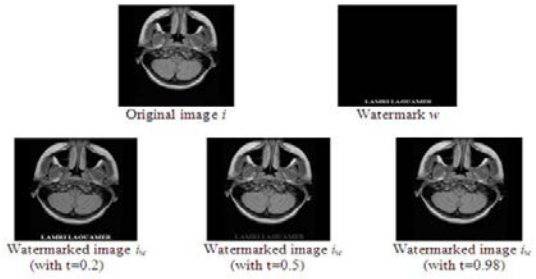

Figure 5.A. Embedding watermark by linear interpolation with different values of t (secret key).

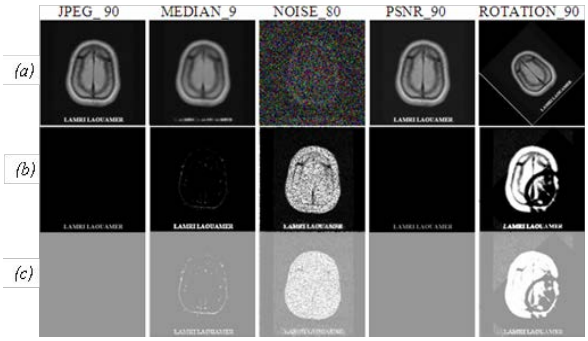

Figure 4.C. Watermark Extraction Results when t=0.5

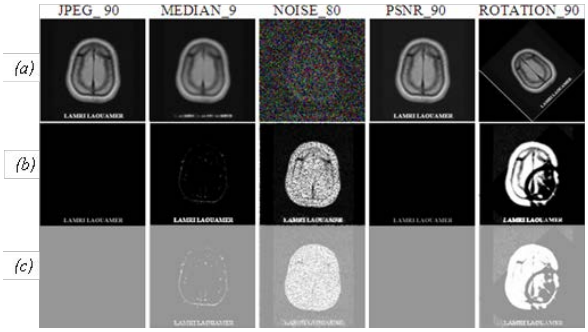

Figure 4.D. Watermark Extraction Results when t=0.2.

We have also made the same tests on other images following the same steps in the cases of visible, semi visible and invisible watermark by setting in each test the values of the key t. Figure 5.A, figure 5.B, figure 5.C and figure 5.D illustrate the results for used images sample such as: brain image, while figure 5.A, figure 5.B, figure 5.C and figure 5.D illustrate these results.

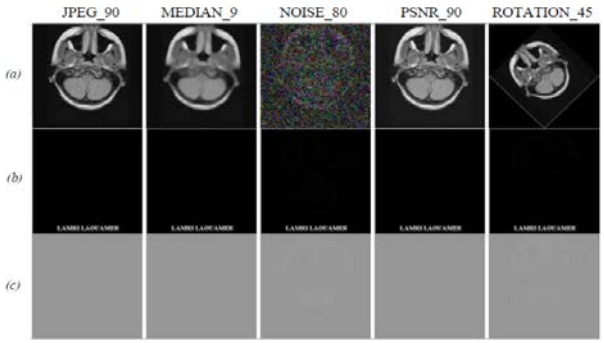

Figure 5.B. Watermark Extraction Results when t=0.98.

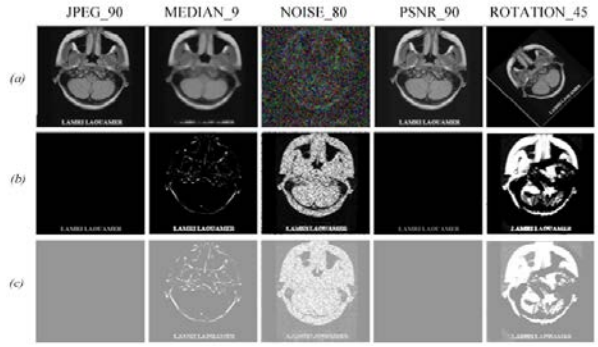

Figure 5.C. Watermark Extraction Results when t=0.5.

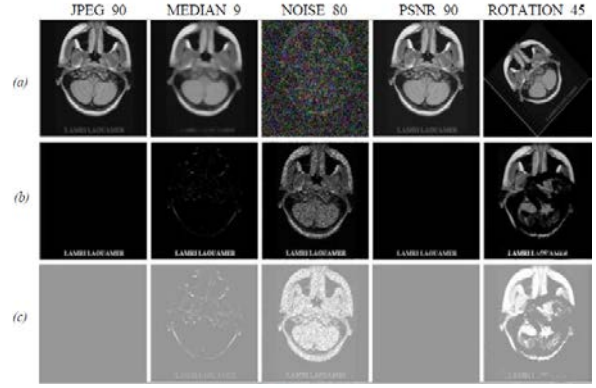

Figure 5.D. Watermark Extraction Results when t=0.2.

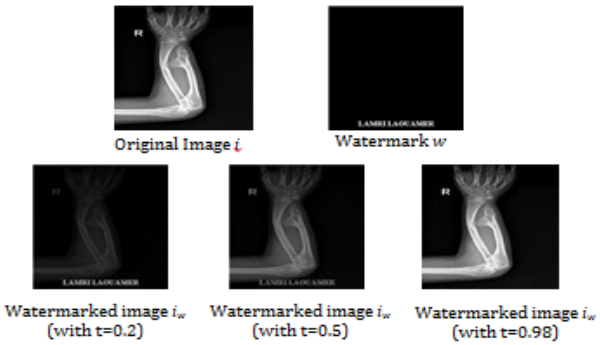

Figure 6.A. Embedding watermark by linear interpolation with different values of t (secret key).

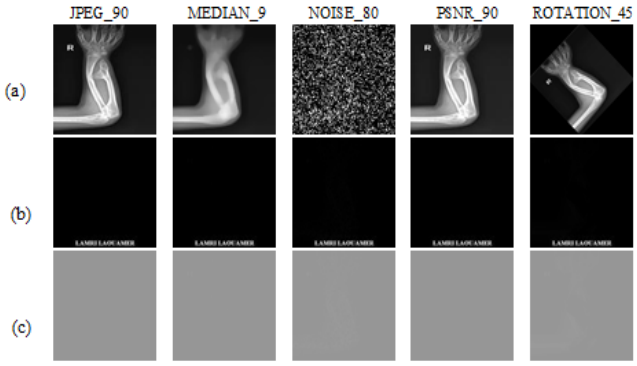

Figure 6.B. Watermark Extraction Results when t=0.98.

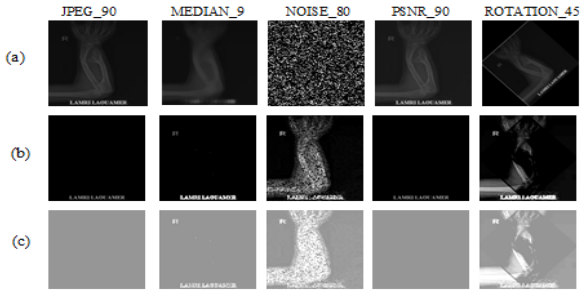

Figure 6.C. Watermark Extraction Results when t=0.5.

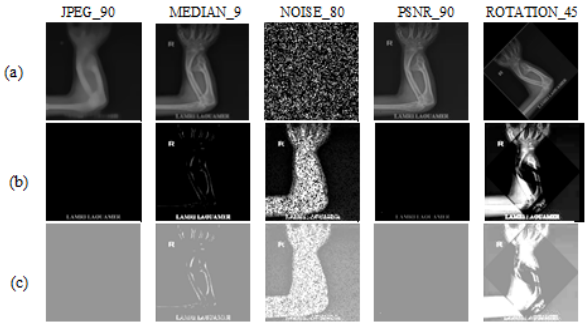

Figure 6.D. Watermark Extraction Results when t=0.2.

4.1. Robustness Measurements

To assess the robustness of the proposed approach in this paper, we introduce the latest techniques used in the literature. It consists to calculate the Peak Signal to Noise Ratio (PSNR), Structural Similarity Index SSIM [25] and Universal Quality Index (UQI) [26].

$$MSE(w, w_a) = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (w(i,j) - w_a(i,j))^2 \quad (8)$$

$$PSNR(w, w_a) = 10 \log_{10} \left(\frac{(2^P - 1)^2}{MSE} \right) \quad (9)$$

Where *w* and w_a are the original and extracted watermarks, respectively; P is the image depth; and *M* and *N* are the image size.

The values of PSNR against the applied multiple attacks show that its values exceeds 34dB (standard threshold) which means a low degradation between the original watermark and the extracted one.

$$SSIM(w, w_a) = \sum_{n,m} \frac{(2\mu_w \mu_{w_a} + c_1)(2\sigma_{ww_a} + c_2)}{(\mu_w^2 + \mu_{w_a}^2 + c_1)(\sigma_w^2 + \sigma_{w_a}^2 + c_2)} \quad (10)$$

Where *n* and *m* are the image size; μ_w and μ_{w_a} are the averages of *w* and w_a, respectively; σ_w^2 and μ_{w_a} are the variances of *w* and w_a, respectively; and σ_w^2 and $\sigma_{w_a}^2$ are the covariance of *w* and w_a, respectively.

$$UQI(w, w_a) = \frac{\sigma_{ww_a}}{\sigma_w \sigma_{w_a}} * \frac{2\, w` w_a`}{(w`)^2 + (w_a`)^2} * \frac{2\sigma_w \sigma_{w_a}}{\sigma_w^2 + \sigma_{w_a}^2} \quad (11)$$

Universal Index models comprises three different factors: correlation coefficient between w and wa with a value range of [-1,1]. The luminance distortion between w and wa with a range value of [0,1]. The contrast distortion to measure the similarity between w and wa with also a range value of [0,1].

For SSIM and UQI between the original watermark and the extracted one values, the dynamic range of SSIM and UQI is [-1,1], where is in the locality of 1 means a strong similarity between the original watermark and the extracted watermark images in case of all kinds of attacks. Table 1, figures 7.A and figure 7.B illustrate the PSNR, SSIM and UQI results after applying different attack scenarios.

Table 1. Robustness measurements after different attacks

Attacks	PSNR	SSIM	UQI
JPEG	69.1732	0.9997	0.9863
MEDIAN	51.1326	0.9986	0.9611
NOISE	41.1456	0.9794	0.9153
PSNR	65.8942	0.9999	0.9999
ROTATION	43.2264	0.9713	0.9237

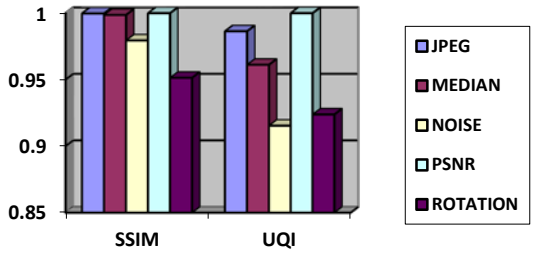

Figure 7.A. Robustness measures in case of SSIM and UQI

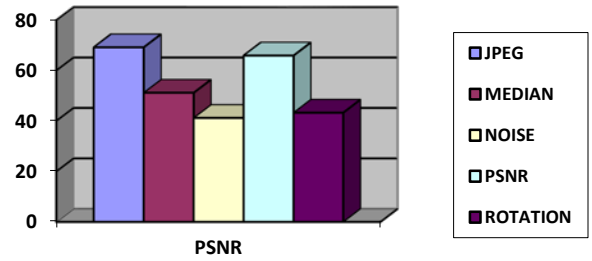

Figure 7.B. Robustness measure in case of PSNR.

4.2 Imperceptibility Measurements

Our approach aims to achieve a high imperceptibility regarding the watermark embedding . The degradation in the watermarked image after watermark embedding is very low. The optimal imperceptibility in our scheme when *t* is close to 1 (*t=0.98*). Moreover, we evaluate the imperceptibility for our approach by measuring the PSNR between the original image and the watermarked image. Table 2 shows the imperceptibility results of different values of *t*. While figure 8 shows the chart of these results.

Table 2. Imperceptibility measurement based on PSNR.

Image	PSNR		
	t=0.2	*t=0.5*	*t=0.98*
Head	39.2345	41.4658	56.3476
Brain	39.4574	40.6244	54.3487
Hand	38.5657	41.7065	55.5504

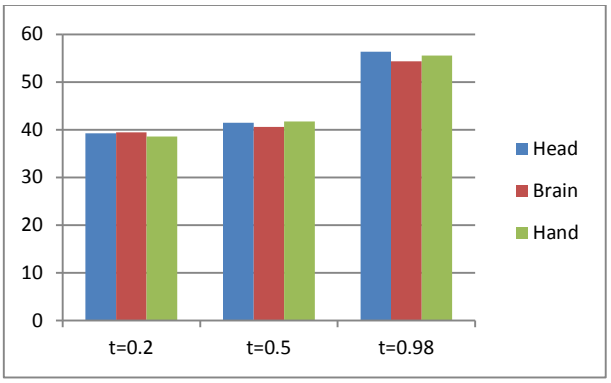

Figure 8. Imperceptibility results for different values of t

Based on the previous table and figure, our approach achieves a high imperceptibility when t=0.98. Moreover, the results indicate that the technique offers a high fidelity and imperceptibility, which means that our approach reserve the image quality after embedding, and there is no degradation effected to the watermarked image.

5.Comparative Study

In this section, we will compare the robustness of the proposed technique with the works in [19] and [20]. We provided the values of PSNR and SSIM of the extracted watermark. Those works have used the DWT technique, where the watermark image size in those works has the same size with the used watermark in our work.

Table 3. PSNR Comparative results

Attacks	[19]	[20]	Proposed technique
JPEG Compression	28.287	38.71	69.1732
Noise	20.272	25.74	41.1456
Median	27.497	14.22	51.1326
Rotation	43.596	36.68	43.2264

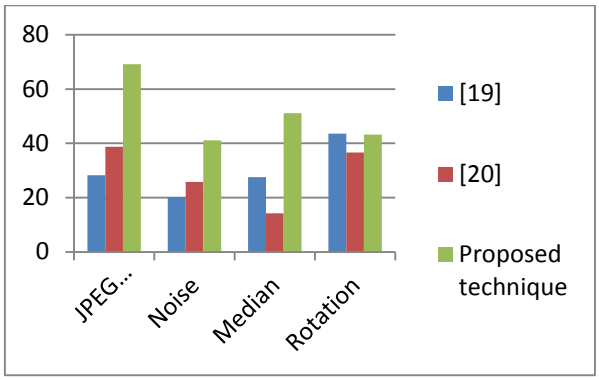

Figure 9. PSNR Comparative results with the works in [19] and [20]

Table 4. SSIM Comparative results

Attacks	[19]	[20]	Ours
JPEG Compression	0.9875	0.98	0.9997
Noise	0.9225	0.8	0.9794
Median	0.9852	0.6	0. 9986
Rotation	0.9999	0.97	0.9713

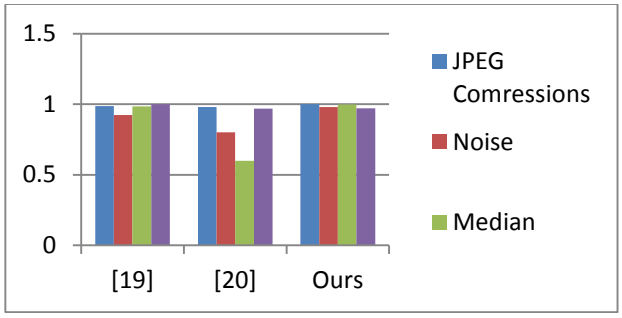

Figure 10. SSIM Comparative results with the works in [19] and [20]

We compared our results in term of robustness with those works in [19] and [20]. It is obvious from the table 3 and 4, and figures 9 and 10, that our results are better than those results in term of robustness by measuring the PSNR metric.

6.Conclusion

We proposed in this paper a new watermarking approach to ensure the CT scan medical image authentication and robustness, which is based on the wavelet transform. This approach is applicable to any kind of images, but more appropriate to the medical image because the high image quality and the less degradation. The embedding process is performed by a linear interpolation with an invisible way. Our tests were performed on a sample of 250 images. The results obtained are very encouraging, especially when the watermark is invisible (the watermarking key t close to 1). Similarly, we discuss about the robustness of our approach which consists to compare the original watermark and the extracted one after applying attacks. This aspect is achieved by applying the best known similarity measures between the original and the extracted watermarks as the PSNR, SSIM, UQI. The experimental results and the comparative study show that the proposed technique present more robustness against different kinds of attacks than some relevant works presented in [19] and [20].

References

[1] Woo, C. S., Du, J., & Pham, B. L. (2005). Multiple watermark method for privacy control and tamper detection in medical images..

[2] Laouamer, L., & Tayan, O. (2013). An enhanced SVD technique for authentication and protection of text-images using a case study on digital Quran content with sensitivity constraints. Life Science Journal, 10(2), 2591-2597.
[3] Jain, J., & Johari, P. (2014). Digital Image Watermarking Based on LSB for Gray Scale Image. IJCSNS International Journal of Computer Science and Network Security, 14(6), 108-112.
[4] Wenyin, Z., & Shih, F. Y. (2011). Semi-fragile spatial watermarking based on local binary pattern operators. Optics Communications, 284(16), 3904-3912.
[5] Sharma, P. Swami, S. , : Digital Image Watermarking Using 3 level Discrete Wavelet Transform, the 2013 Conference on Advances in Communication and Control Systems (CAC2S 2013), 2013.
[6] Hu, Y., & Li, J. (2015, April). A Robust Watermarking of Medical Image Based on 3D-DFT and Arnold Scrambling In Compressed Domain. In 2015 International Conference on Mechatronics, Electronic, Industrial and Control Engineering (MEIC-15). Atlantis Press.
[7] Laouamer, L., & Tayan, O. (2015). A Semi-Blind Robust DCT Watermarking Approach for Sensitive Text Images. Arabian Journal for Science and Engineering, 40(4), 1097-1109.
[8] Baisa, L. S. ,Mali, N.: ROI Based Embedded Watermarking of Medical Images for Secured Communication in Telemedicine, World Academy of Science, Engineering and Technology 68, 2012.
[9] Chih-Hung L., Ching-Yu Y., Chia-Wei C.,: Authentication and Protection for Medical Image, Proceedings of the Second International Conference, ICCCI 2010, Kaohsiung, Taiwan,pp 278-287, November 10-12, 2010.
[10] Baisa, L. S. ,Mali, N.: ROI Based Embedded Watermarking of Medical Images for Secured Communication in Telemedicine, World Academy of Science, Engineering and Technology 68, 2012.
[11] Kannammal, A. and Subha S.,: Authentication of DICOM Medical Images using Multiple fragile watermarking Techniques in Wavelet transform Domain, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6,pp 181-189, 2011.
[12] Fakhari, P., Vahedi, E., & Lucas, C, : Protecting patient privacy from unauthorized release of medical images using a bio-inspired wavelet-based watermarking approach, Digital Signal Processing, 21(3), 433-446, 2011.
[13] Li, J., Huang, M., Zhang, H., Dong, C., & Bai, Y, : The medical images watermarking using DWT and Arnold, 2012 IEEE International Conference In Computer Science and Automation Engineering, Vol1, pp 27-31, 2012.
[14] Bouslimi D., Gouenou C., Michel C., and Christian R., : A joint Encryption/Watermarking System for Verifying the Reliability of Medical Image, IEEE Transactions on Information Technology in Biomedicine , Vol 16, No. 5, pp 891-899, September 2012.
[15] Xia, W., Hongwei L., and Yizhu Z., :A dual binary image watermarking based on wavelet domain and pixel distribution features. Advances in Multimedia Modeling. Springer Berlin Heidelberg, 2010. 130-140.
[16] Keyvanpour, M., Bayat, F., : Blind image watermarking method based on chaotic key and dynamic coefficient quantization in the DWT domain , Mathematical and Computer Modelling, Volume 58, Issues 1–2, July 2013, Pages 56-67, ISSN 0895-7177.
[17] Golpira, H., and Habibollah D., : Reversible blind watermarking for medical images based on wavelet histogram shifting, Signal Processing and Information Technology (ISSPIT), 2009 IEEE International Symposium on. IEEE, 2009.
[18] Lu, W., Wei S., and Hongtao L.,: Robust watermarking based on DWT and nonnegative matrix factorization. Computers & Electrical Engineering 35.1 (2009): 183-188.
[19] Ahmad, A., Sinha, G. R., & Kashyap, N. (2014). 3-Level DWT Image Watermarking Against Frequency and Geometrical Attacks. International Journal of Computer Network and Information Security (IJCNIS), 6(12), 58.
[20] Benrhouma, O., Hermassi, H., & Belghith, S. (2015). Tamper detection and self-recovery scheme by DWT watermarking. Nonlinear Dynamics, 79(3), 1817-1833.
[21] Benhocine, A., Laouamer, L., Nana, L., Pascu, A. : New images watermarking scheme based on singular value decomposition. Journal of Information Hiding and Multimedia Signal Processing 4.1 (2013): 9-18.
[22] Benhocine, A., Laouamer, L., Nana, L., Pascu, A. : A new approach against color attacks of watermarked images. Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP'08 International Conference on. IEEE, 2008.
[23] Benhocine, A., Laouamer, L., Nana, L., Pascu, A. : Improving extraction of watermarks in color attacked watermarked images. Journal of Communication and Computer 6.5 (2009): 36-45.
[24] http://www.barre.nom.fr/medical/samples
[25] Hore, A., & Ziou, D. (2010, August). Image quality metrics: PSNR vs. SSIM. InPattern Recognition (ICPR), 2010 20th International Conference on (pp. 2366-2369). IEEE.
[26] Wang, Z., & Bovik, A. C. (2002). A universal image quality index. Signal Processing Letters, IEEE, 9(3), 81-84.

Author's Biography

Muath AlShaikh is an Ph.D. student in Computer Science since 2013, University of Bretagne Occidentale, France. He received his Master degree in computer science in 2010 from Utara University in Malaysia and his B.Sc in computer science in 2006 from AlBalqa Unversity, Jordan. He is affiliated to Lab-STICC / UMR CNRS 6283, SFIIS team of the University of Bretagne Occidentale, France. His research interests include image and video watermarking, cryptology, information security, image processing and computer vision.

Lamri Laouamer is an assistant professor at the department of Management Information Systems, College of Business and Economics at Qassim University, KSA. He is also an associate researcher in Laboratoire des Sciences et Techniques de l'Information, de la Communication et de la Connaissance (Lab-STICC), University of Bretagne Occidentale, Brest, France. He received his Ph.D. in 2012 in computer science, field of Information security from the University of Bretagne Occidentale, France. His M.Sc. in 2006 in computer science and applied mathematics from the University of Quebec at Trois Rivieres in Canada. His B.Sc. in 1999 in computer science from the University of Setif, Algeria. His research interests include multimedia watermarking, cryptology and information security. Dr. Lamri Laouamer is an associate editor of the journal of Telecommunication systems by Springer and Associate editor of the Journal of Innovation in Digital Ecosystems by Elsevier.

Laurent NANA is Professor in Computer Science at the Computer Science Department of the Faculty of Science of University of Brest in France. He is member of the Team « Security, Reliability, Integrity of Information and Systems » of the Laboratory of Sciences and Techniques of Information, Communication and Knowledge (Lab-STICC / UMR CNRS 6283). His research interests include security of electronic data exchange, software for crisis management, languages and software architectures for safe control of remote systems.

PASCU Anca Christine is professor at the University of Bretagne Occidentale in Brest, France. She received her PhD in Mathematics from the University of Bucarest, Romania in 1977 and PhD in Computer Science Applied to Humanities from the University of Paris-Sorbonne in 2001. She passed her HDR (Habilitation à Dirigée des Recherches) in Paris-Sorbonne with the Logic of Determination of Objects, a new non-classical logic applied to the language in 2006. Her research field is the logical models for the semantics of language and watermarking and cryptography as well.