QAM-DWT-SVD Based Watermarking Scheme for Medical Images

Habib Ayad* and Mohammed Khalil

Laboratory of Computer Sciences FST - Research Team: RTM, Hassan II University of Casablanca, B.P. 146 Mohammedia 20650 (Morocco)

Received 15 June 2017 | Accepted 30 November 2017 | Published 15 January 2018

unir
LA UNIVERSIDAD
EN INTERNET

Abstract

This paper presents a new semi-blind image watermarking system for medical applications. The new scheme utilizes Singular Value Decomposition (SVD) and Discrete Wavelet Transform (DWT) to embed a textual data into original medical images. In particular, text characters are encoded by a Quadrature Amplitude Modulation (QAM-16). In order to increase the security of the system and protect then the watermark from several attacks, the embedded data is submitted to Arnold Transform before inserting it into the host medical image. To evaluate the performances of the scheme, several medical images have been used in the experiments. Simulation results show that the proposed watermarking system ensures good imperceptibility and high robustness against several attacks.

Keywords

Watermarking, Medical Images, Information Security, Singular Value Decomposition, Discrete Wavelet Transforms, Quadrature Amplitude Modulation, Arnold Transform.

DOI: 10.9781/ijimai.2018.01.001

I. Introduction

With the widespread emergence of internet and computer applications, medical images can be shared between specialists and hospitals to determine suitable diagnostic procedures [6] and improve the understanding of a certain disease [9]. However, sharing medical images can lead data to be submitted to an act of tampering by unauthorized persons. As a result, a lot of worry has grown about the protection of authenticity, integrity and confidentiality of the content of medical images.

To avoid this kind of issues, image watermarking can be used as an effective and promising solution [4]. Image watermarking consists of hiding data into the original image without causing serious degradation of the perceptual quality [5]. In the inverse process, the watermark should be recovered from the watermarked image that can be disturbed by several attacks.

Image watermarking algorithms can be classified based on different views [19]. In terms of human perception, image watermarking can be grouped into visible and hidden methods. Visible watermarks such as logos are inserted into the corners of images for content or copyright protection. On the other side, hidden watermarks are imperceptible and are inserted on the unknown places in the host image. The similarity between the watermarked data and the original one should be high, in such a way that a simple user cannot make a difference. Image watermarking can also be categorized into fragile and robust, blind and non-blind.

In addition to above groupings, the digital image watermarking can be also classified into two groups according to the domain used for data embedding. The algorithms of the first group use the spatial domain for data embedding. In this case, the watermark is inserted by directly modifying the pixel values of the host image [12, 13]. In general, spatial methods are easy to implement but they are very fragile against attacks especially lossy compression. Moreover, the inserted data can be easily detected by computer programs since the watermark is embedded in the spatial domain of the image. The algorithms of the second group take advantage of transformation domains in which the watermark is embedded by modulating the coefficients in a transform domain such as discrete wavelet transform (DWT) [7], discrete cosine transform (DCT) [16], lifting wavelet transform (LWT) [8], integer wavelet transform (IWT) [2] and singular value decomposition (SVD) [3].

In general, transform domain methods are typically more robust to noise, attacks, common disturbances and compression compared to spatial transform algorithms. This is due to the fact that when image is inversely transformed, the watermark is distributed irregularly over the image. Furthermore, it is more difficult to detect the embedded data since the information contained in the watermark is distributed around the entire image. One of the limitations of transform methods is the capacity that is generally lower than that of spatial methods.

DWT based methods are among the most widely techniques used in image watermarking [19]. This is due to their good time-frequency features and directives that match well with the Human Visual System (HVS) [15]. Since the quality of medical images is very important for medical diagnosis, then the image quality must be preserved intact while the embedding capacity is increased [9].

The main goal of this paper is to propose an image watermarking scheme based on the discrete wavelet transform applied to a security context. We combine the DWT transform with SVD and QAM-16 to improve the performance of watermarking method. The main purpose of the proposed watermarking scheme is to increase the robustness without losing the imperceptibility of the embedded data.

* Corresponding author.

E-mail address: ayad.habib@gmail.com

The embedding process is carried out by inserting the watermark into the singular values of the DWT image. Specifically, the watermark is embedded by modifying the singular values of the DWT low frequency sub-band LL of the host image. The Arnold transform is used to increase the security of embedded data. At the extraction process, the operations are inversely done to extract the watermark from the watermarked image that can be disturbed by several distortions. The proposed scheme can be applied to several types of images especially medical ones that need higher quality for successful diagnosis.

The rest of the paper is organized as follows: in Section II, some useful and important preliminary ideas are discussed and then the proposed algorithm is introduced in Section III. Finally, simulation results are presented in Section IV followed by a discussion and conclusion in Section V.

II. Basic Concepts

In this work, Singular Value Decomposition (SVD), Discrete Wavelet Transform (DWT), Arnold Transform (AT) and Quadrature Amplitude Modulation (QAM) algorithms are used to design the proposed watermarking scheme. In the following subsections, a brief explanation of each algorithm is given. This section describes the overall basic concepts exploited in the proposed watermarking scheme.

- SVD is used to preserve significant amount of information of an image and makes the watermark more robust against attacks such as noise addition and scaling. The watermark can be then extracted effectively from the attacked watermarked image because of the special SVD properties.
- DWT transform is used to insert the watermark in imperceptible manner. The watermark bits are inserted in the significant coefficients sub-bands by considering the human visual system (HVS) characteristics.
- QAM technique is used to encode the character text before embedding it in the image.
- Arnold Transform is used to make the watermark more secure and protect the embedded data.

A. Singular Value Decomposition

Singular Value Decomposition (SVD) is an important technique of linear algebra that can be used to solve several mathematical problems. SVD is widely applied in many varieties of image processing applications such as image steganography, image watermarking, image compression and noise reduction [14].

From the perspective of linear algebra, a digital image can be viewed as a matrix composed of a number of non-negative scalars. The SVD of an image A with size $M \times N$ is represented mathematically as

$$A=USV^{T} \tag{1}$$

where U and V are the orthogonal matrices such that $UU^T = I_M$, $VV^T=I_N$ the columns of U are the orthonormal eigenvectors of AA^T, the columns of V are the orthonormal vectors of $A^T A$, and S is a diagonal matrix containing the square roots of the eigenvalues from U or V in descending order.

If r is the rank of the matrix A, then the elements of the diagonal matrix S satisfy the following relation:

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r \geq \lambda_{r+1} = \lambda_{r+1} = \cdots = \lambda_N = 0 \tag{2}$$

SVD has several interesting properties in image processing applications such as stability, proportionality, rotation and translation, etc. SVD can represent efficiently the intrinsic algebraic properties of an image. Indeed, the brightness of the image is specified by the singular values and corresponding pair of singular vectors reflect the geometry of the image.

The main goal of using SVD-based watermarking Techniques is to insert the data into the singular values by applying the SVD into whole or small blocks of the host image. Unlike the other watermarking methods, SVD can be utilized for non-square matrices because of its nonsymmetrical decomposition property. In general, SVD-based watermarking algorithms are robust against geometric attacks such as rotation, translation, noise addition and scaling. However, SVD still remains limited in comparison with transform domain methods. In order to increase the robustness, SVD can be combined with transform techniques such as DCT and DWT.

B. Discrete Wavelet Transform (DWT)

Discrete Wavelet Transform (DWT) is a multi-resolution mathematical tool that decomposes hierarchically an image and can be efficiently implemented using different digital filters. An image can be passed through high and low pass filters in order to be decomposed into several sub-bands with different resolutions. By applying DWT, the image is decomposed into four components namely LL, LH, HL and HH, corresponding to approximate, vertical, horizontal, and diagonal features respectively as illustrated in Fig. 1. The sub-band denoted by LL is approximately half of the original image. While LH and HL sub-bands contain the changes of edges or images along horizontal and vertical directions. Fig. 2 presents an example on 1-level DWT decomposition of Lena image that shows the four sub-bands LL, LH, HL an HH.

LL1	LH1
HL1	HH1

Fig. 1. The principle of 1-level DWT.

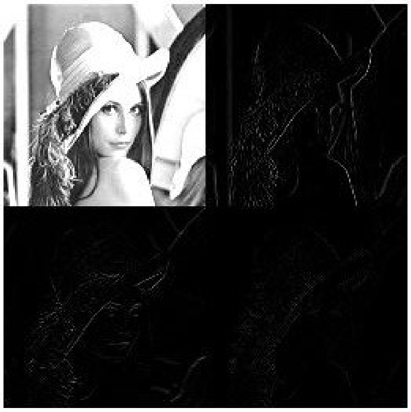


Fig. 2. 1-level DWT of Lena.

C. Arnold Transform (AT)

Arnold transform is a 2D chaotic map that is used to randomize a watermark matrix before embedding it into a cover image. Although there are many ways for scrambling, but in this paper, we will discuss only the Arnold transform [17] to increase the robustness and improve the security of the proposed watermarking scheme.

Arnold transform is an iterative process of moving the pixel position. Suppose that the original image is a $N \times N$ array and the coordinate of the pixel is $x, y \in \{0, 1, ..., N-1\}$. The generalized two dimension (2D)

Arnold transform is defined as:

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & k \\ l & kl+1 \end{bmatrix} \begin{bmatrix} x_{n-1} \\ y_{n-1} \end{bmatrix} mod\ N \quad (3)$$

where x_n and y_n are the transformed coordinates corresponding to x_{n-1} and y_{n-1} after n iterations respectively, k and l are positive integers, and N represents the width or height of the square image processed.

Arnold transform is a periodic process, so the original position of *(x; y)* coordinates gets back after T iterations. The factor T is called the transform period and depends on parameters $k;\ l$ and n. These parameters will be used as secret keys in this paper. To recover the original image, periodicity is required. If the scrambling has performed n iterations; then the original image can be obtained by performing $T - n$ iterations. Fig. 3 illustrates an example of Arnold Transform into an image with different iterations.

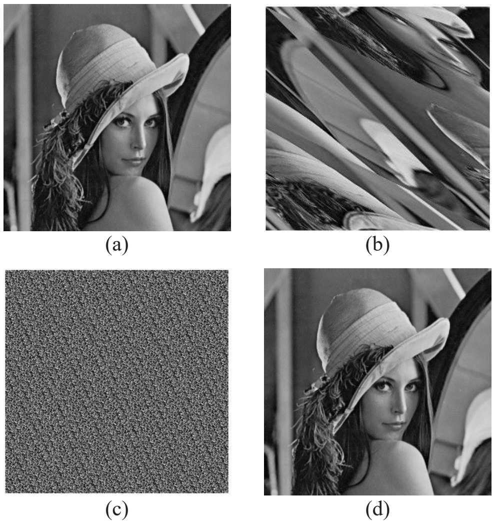


Fig. 3. Arnold transform with $k = l = 1$ (a) Lena 256 x 256. (b) AT with one iteration (c) AT with 10 iterations (d) AT with 192 iterations.

D. Quadrature Amplitude Modulation (QAM)

Quadrature Amplitude Modulation is a form of modulation that is a combination of phase modulation and amplitude modulation. A diversity of communication protocols implement quadrature amplitude modulation (QAM) such as digital video broadcast (DVB) and 802.11b wireless Ethernet (Wi-Fi).

For QAM-16, 4 bits are collected and mapped to one symbol from an alphabet with $2^4 = 16$ possibilities called constellations [11].

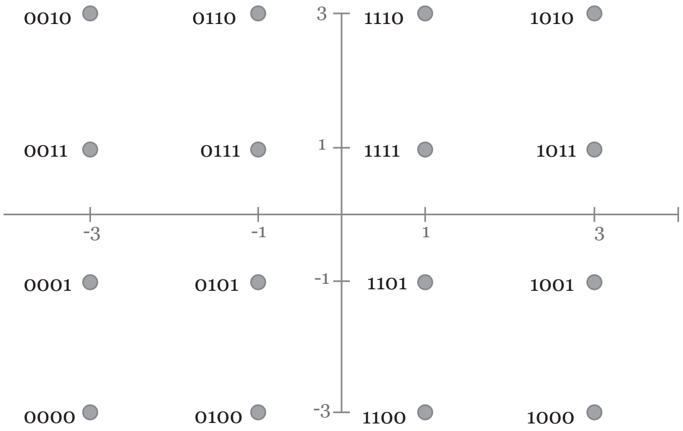


Fig. 4. Constellation diagram of QAM-16.

The symbols of QAM-16 alphabet are the complex numbers in the set $\{\pm3\pm3j, \pm3\pm j, \pm1\pm3j, \pm1\pm j\}$. The QAM-16 constellation is shown in Fig. 4. In this work, we use QAM-16 for encoding text characters to insert them into the host image.

Let z be a symbol in constellation QAM-16; $z = a + jb$ where $a, b \in \{-3, -1, 1, 3\}$ z can be also represented in the polar form as: $z = \rho e^{j\emptyset}$ where $\rho = \sqrt{a^2 + b^2}$ and $\emptyset = angle(z)$. Table I shows the correspondence between the binary codes and the complex symbols.

TABLE I. Correspondece Between Binary Codes and Complex Symbols

Binary code	Real part	Imaginary part	ρ	$\emptyset$ (degree)
0000	-3	-3	4.2426	-135
0001	-3	-1	3.1623	-161.5651
0010	-3	3	4.2426	135
0011	-3	1	3.1623	161.5651
0100	-1	-3	3.1623	-108.4349
0101	-1	-1	1.4142	-135
0110	-1	3	3.1623	108.4349
0111	-1	1	1.4142	135
1000	3	-3	4.2426	-45
1001	3	-1	3.1623	-18.4349
1010	3	3	4.2426	45
1011	3	1	3.1623	18.4349
1100	1	-3	3.1623	-71.5651
1101	1	-1	1.4142	-45
1110	1	3	3.1623	71.5651
1111	1	1	1.4142	45

Because the $\emptyset$ values will be used in a watermark matrix, the periodicity of sine and cosine functions can be used to change the negative values of $\emptyset$ by a positive values ($\emptyset + 360°$) as shown in Table II.

TABLE II. Correspondence Between Binary Codes and Complex Symbols with $\emptyset$>0

Binary code	Real part	Imaginary part	ρ	$\emptyset$ (degree)
0000	-3	-3	4.2426	225
0001	-3	-1	3.1623	198.4349
0010	-3	3	4.2426	135
0011	-3	1	3.1623	161.5651
0100	-1	-3	3.1623	251.5651
0101	-1	-1	1.4142	225
0110	-1	3	3.1623	108.4349
0111	-1	1	1.4142	135
1000	3	-3	4.2426	315
1001	3	-1	3.1623	341.5651
1010	3	3	4.2426	45
1011	3	1	3.1623	18.4349
1100	1	-3	3.1623	288.4349
1101	1	-1	1.4142	315
1110	1	3	3.1623	71.5651
1111	1	1	1.4142	45

TABLE III. Correspondece Between Bynary Codes and Complex Symbols Sorting According to ρ

Binary code	Real part	Imaginary part	ρ	$\emptyset$ (degree)
0000	-3	-3	4.2426	225
0010	-3	3	4.2426	135
1000	3	-3	4.2426	315
1010	3	3	4.2426	45
0001	-3	-1	3.1623	198.4349
0011	-3	1	3.1623	161.5651
0100	-1	-3	3.1623	251.5651
0110	-1	3	3.1623	108.4349
1001	3	-1	3.1623	341.5651
1011	3	1	3.1623	18.4349
1100	1	-3	3.1623	288.4349
1110	1	3	3.1623	71.5651
0101	-1	-1	1.4142	225
0111	-1	1	1.4142	135
1101	1	-1	1.4142	315
1111	1	1	1.4142	45

Table III is obtained by sorting Table II according to the ρ column. It is remarkable that the angles {315, 225, 135, 45} corresponding to magnitudes 4.2426 or 1.4142 as the rest of the angles correspond to the magnitude 3.1623. In this work, we use this correspondence to extract QAM-16 symbols. The symbols extraction decision is made in two stages: firstly the extraction of $\emptyset$ and secondly the extraction of ρ based on correspondence between ρ and $\emptyset$. For example, if the extraction of $\emptyset$ belongs to {341.5651; 251.5651; 288.4349; 198.4349; 161.5651; 108.4349; 71.5651; 18.4349} ρ is automatically equal to 3.1623 and if the extraction of $\emptyset$ belongs to {315; 225; 135; 45}. Finally, we make a decision of ρ on 4.2426 and 1.4142.

III. The Proposed Approach

The overall system of our proposed approach is illustrated in Fig. 5. First, we convert the electronic patient record (ERP) text into a watermark matrix using the QAM-16, then Arnold Transform is applied to the watermark matrix and the watermark is scrambled. The parameters of Arnold Transform are used as a key to increase the security of the watermark. The scrambled watermark matrix is embedded then into the host image. To recover the secret data, the scrambled watermark matrix is extracted from the watermarked image using the extraction procedure. Finally, the inverse Arnold Transform and QAM-16 procedure are successively applied to retrieve the original ERP data. The proposed algorithm consists of six main steps:

1. Conversion ERP text into a watermark matrix.
2. Scrambling the watermark matrix by Arnold Transform.
3. Embedding process.
4. Extraction process.
5. Inverse Arnold Transform.
6. Conversion watermark matrix to the original ERP.

A. Watermark Matrix

In this work, the watermark that is embedded in the original medical image is a matrix that is generated from the EPR. The characters of the EPR text are grouped into a matrix of size $2^m \times 2^m$. For example, an EPR of 1024 characters is represented in a matrix of size $2^5 \times 2^5$. Then, the ASCII code for each character i is converted to 8-bit binary code.

The QAM-16 is applied to the first 4 bits and the last 4 bits to obtain two pairs $(\rho_1^i, \emptyset_1^i)$ and $(\rho_2^i, \emptyset_2^i)$ which are grouped into a matrix of size 2 × 2 as shown in Fig. 6.

To ensure that the watermark matrix elements are between 0 and 1 we use $\frac{\rho}{10}$ rather than the magnitude ρ and $\frac{\emptyset}{10}$ rather than the angle $\emptyset$. After this process, the resulted watermark matrix is obtained by replacing each character by a 2 × 2 matrix that is composed by ρ and $\emptyset$ which gives a watermark matrix of size $2^{m+1} \times 2^{m+1}$.

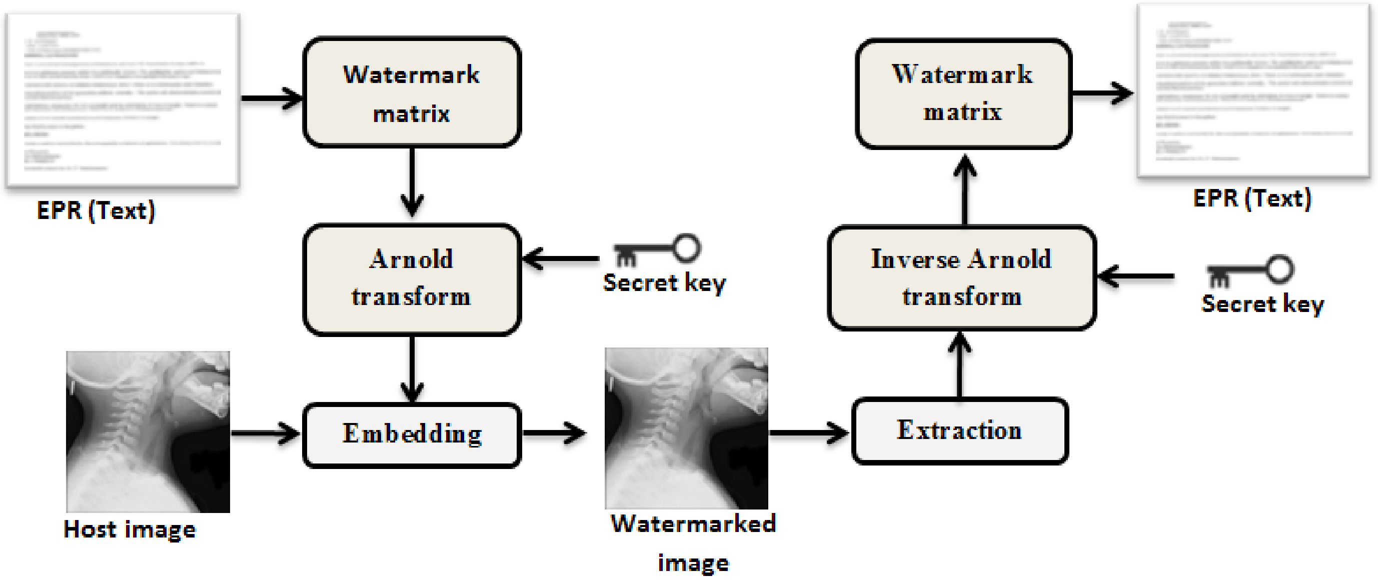


Fig. 5. The proposed watermarking scheme.

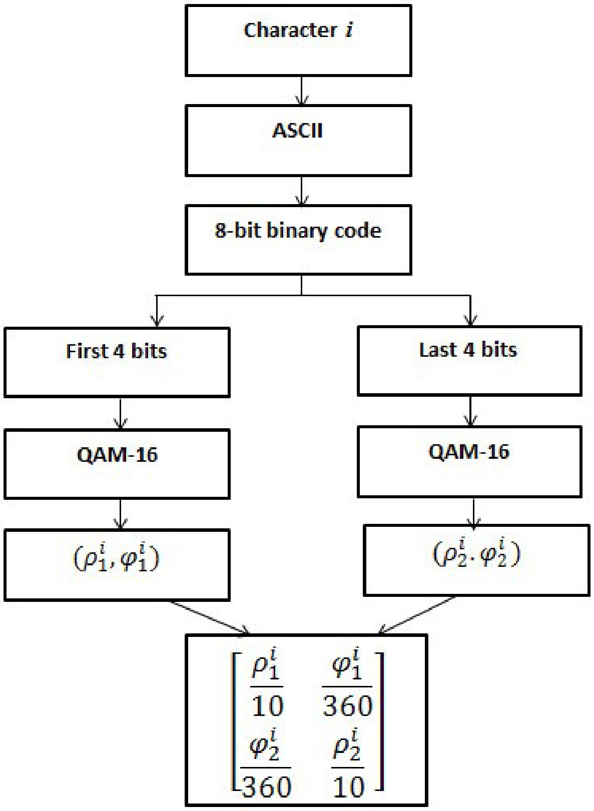

Character *i*
ASCII
8-bit binary code
First 4 bits
Last 4 bits
QAM-16
QAM-16
(ρ_1^i, φ_1^i)
$(\rho_2^i . \varphi_2^i)$
$\begin{bmatrix} \frac{\rho_1^i}{10} & \frac{\varphi_1^i}{360} \\ \frac{\varphi_2^i}{360} & \frac{\rho_2^i}{10} \end{bmatrix}$

Fig.6. The characters conversion process.

Example

Let *tex*=”Farabi2 hospital”, the size of *tex* is 16 characters that can be grouped into $2^2 \times 2^2$ matrix by replacing each character to its ASCII code. The resulted matrix is:

$$\begin{bmatrix} 70 & 98 & 104 & 105 \\ 97 & 105 & 111 & 116 \\ 114 & 58 & 115 & 97 \\ 97 & 32 & 112 & 108 \end{bmatrix}$$

By applying the process as shown in Fig. 6, we convert each ASCII code to a 2 × 2 matrix:

$$F \underbrace{\to}_{ASCII} 70 \underbrace{\to}_{Binary} \overbrace{0100}^{QAM-16} \underbrace{0110}_{QAM-16}$$

$$\Rightarrow \begin{bmatrix} \frac{\overbrace{3.1623}^{\rho_1^F}}{10} & \frac{\overbrace{251.5651}^{\phi_1^F}}{360} \\ \frac{\overbrace{108.4349}^{\phi_2^F}}{360} & \frac{\overbrace{3.1623}^{\rho_2^F}}{10} \end{bmatrix} \Rightarrow \begin{bmatrix} 0.3162 & 0.6988 \\ 0.3012 & 0.3162 \end{bmatrix}$$

Then, the resulted watermark $2^3 \times 2^3$ matrix is:

$$\begin{bmatrix} 0.3162 & 0.6988 & 0.3162 & 0.3012 & 0.3162 & 0.3012 & 0.3162 & 0.3012 \\ 0.3012 & 0.3162 & 0.3750 & 0.4243 & 0.8750 & 0.4243 & 0.9488 & 0.3162 \\ 0.3162 & 0.3012 & 0.3162 & 0.3012 & 0.3162 & 0.3012 & 0.1414 & 0.3750 \\ 0.5512 & 0.3162 & 0.9488 & 0.3162 & 0.1250 & 0.1414 & 0.6988 & 0.3162 \\ 0.1414 & 0.3750 & 0.3162 & 0.4488 & 0.1414 & 0.3750 & 0.3162 & 0.3012 \\ 0.3750 & 0.4243 & 0.3750 & 0.4243 & 0.4488 & 0.3162 & 0.5512 & 0.3162 \\ 0.3162 & 0.3012 & 0.4243 & 0.3750 & 0.1414 & 0.3750 & 0.3162 & 0.3012 \\ 0.5512 & 0.3162 & 0.6250 & 0.4243 & 0.6250 & 0.4243 & 0.8012 & 0.3162 \end{bmatrix}$$

B. Watermark Embedding Process

The proposed watermark embedding process is described as follows:

Input: Original Image I of size $2^J \times 2^J$, Watermark matrix of size $2^K \times 2^K$

Output: Watermarked Image I_W

1. DWT level $l = J - K$
2. Apply l-level DWT on the original image I to produce four sub-bands LL_l, LH_l, HL_l and HH_l ,
3. Perform SVD operation for low-pass sub-band LL_l

$$LL_l = U_L S_L V_L^T$$

4. Modify S_L, the singular values of the sub-band LL_l, by adding a watermark matrix, with the scaling factor α.

$$S_2 = S_L + \alpha W$$

5. Compute SVD of S_2

$$S_2 = U_2 S_3 V_2^T$$

6. Using S_3 to compute a modified low-pass sub-band LL'

$$LL' = U_L S_3 V_L^T$$

7. Compute the watermarked image I_W by applying the inverse DWT on LL' .LH_l, HL_l and HH_l.

C. Watermark Extraction Process

In general, the extraction process can be completed by reversing the steps of the embedding process. In watermark extraction, an eventually distorted watermark W can be extracted from the eventually distorted watermarked image I_W by effectively reversing the above watermark embedding steps. The process of watermark extraction can be described as follows:

Input: Watermarked Image I_W

Output: Watermark matrix

1. Apply l-levels DWT on the watermarked image to produce four sub-bands LL_w, LH_w, HL_w and HH_w
2. Compute SVD of low-pass sub-band LL_w

$$LL_w = U_w S_w V_w^T$$

3. Compute $\hat{S}$ using left and right singular vectors U_2 and V_2 in step 5 in watermark-embedding algorithm

$$\hat{S} = U_2 S_w V_2^T$$

4. Extract the watermark matrix $\widehat{W}$

$$\widehat{W} = \frac{\hat{S} - S_L}{\alpha}$$

IV. Experimental Results

To evaluate the performances of our proposed scheme, we have applied the embedding algorithm to a database of 100 grey scale medical images of four modalities: X-ray, Ultrasound, MRI and CT. All test images are 512 × 512 pixels. An example of these medical images is illustrated in Fig. 7.

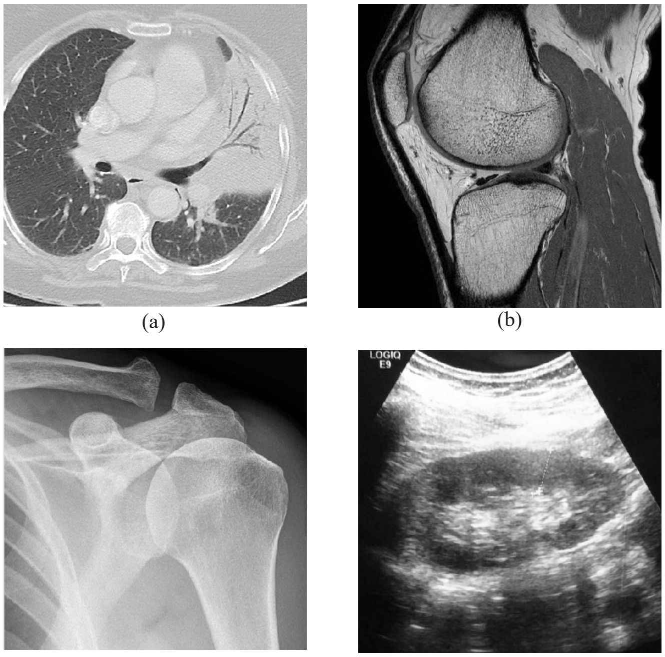

(a)
(b)
(c)
(d)

Fig. 7. (a) CT, (b) MRI, (c) X-Ray and (d) Ultrasound.

A. Quality Measures

Peak Signal to-Noise Ratio (PSNR) is one of the most commonly used measures of imperceptibility between an original image I of size M × N and a watermarked image I_W, which is computed by:

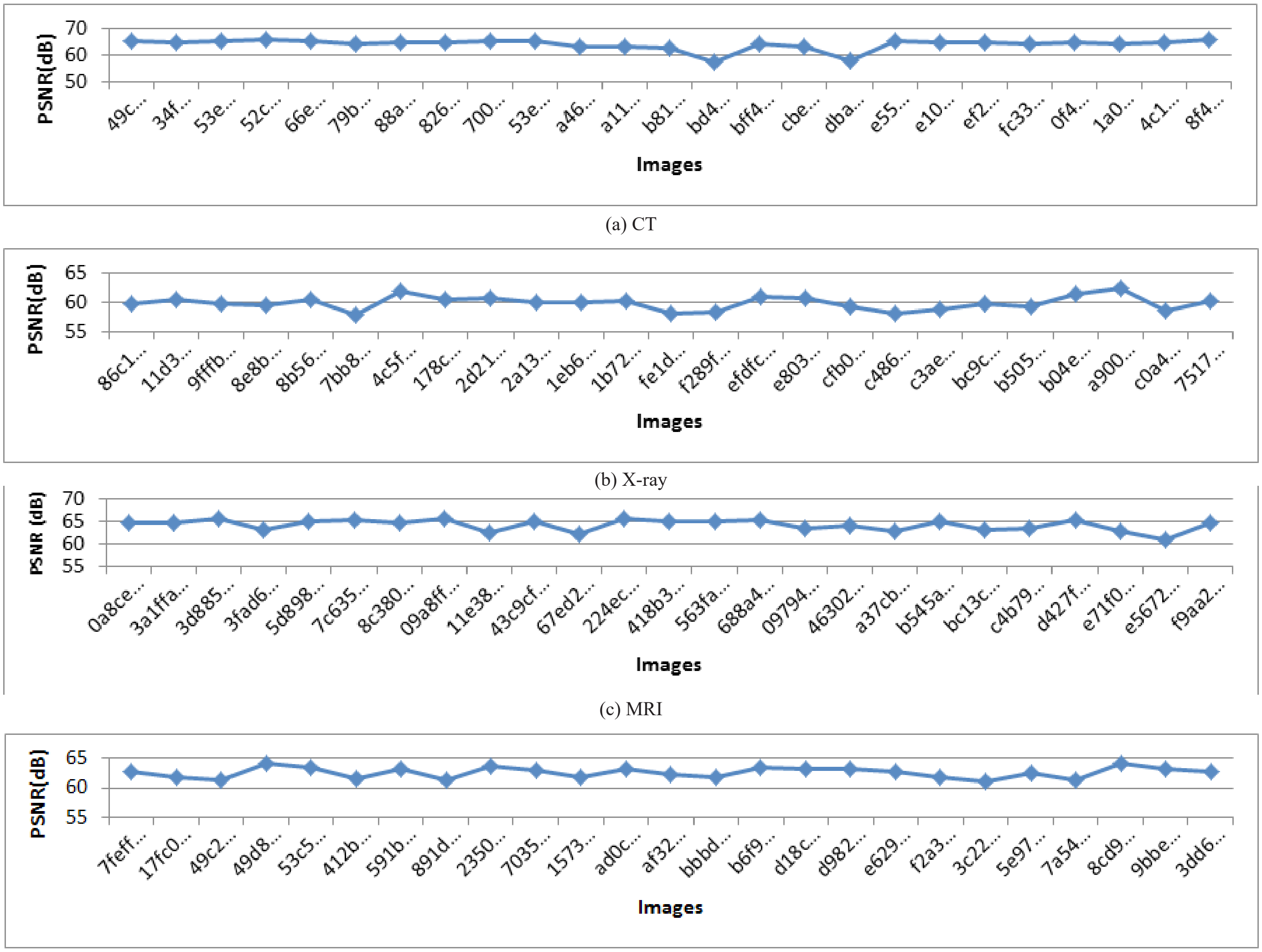
$$PSNR = 10\log\left(\frac{max(I(i,j)^2)}{MSE}\right) \tag{4}$$

$$MSE = \sum_{i=0}^{N-1}\sum_{j=0}^{M-1}\left(\frac{\left(I(i,j) - I_W(i,j)\right)^2}{NM}\right) \tag{5}$$

Structural Similarity Measure (SSIM) is another perceptual metric that quantifies the watermarked medical images quality. Image quality evaluation based on SSIM is based on the fact that the HVS is highly adapted to extract structural information from the viewing field. SSIM metric is ideal for testing of similarities in medical images because it focuses on local rather than global image similarity.

$$SSIM(A,B) = \frac{(2\mu_A\mu_B + c_1)(2\sigma_{AB} + c_2)}{(\mu_A^2 + \mu_B^2 + c_1)(\sigma_A^2 + \sigma_B^2 + c_2)} \tag{6}$$

where μ_A and μ_B are respectively the averages of A and B. σ_A^2 and σ_B^2 are respectively the variances of A and B. $c_1(c_1 = k_1L)^2)$ and



(a) CT

(b) X-ray

(c) MRI

(d) Ultrasound

Fig. 8. Curve of Peak Signal to Noise Ratio (PSNR) in dB for different medical images modalities (a) CT, (b) X-Ray, (c) MRI and (d) Ultrasound.

$c_2(c_2 = k_2L)^2)$ are two variables to stabilize the division with a weak denominator. L is also the dynamic range of the pixel-values. k_1 and k_2 have default values as *0.01* and *0.03*, respectively [18].

In order to compare the similarities between the original ERP text and the extracted ERP text, we define the character error rate in percentage (CER) as follows:

$$CER = \frac{NEC}{TC} \tag{7}$$

where:

- NEC: number of erroneous characters
- TC: total number of characters in a ERP text

B. Imperceptibility Medical Images

In this subsection, we investigate the imperceptibility of the watermark. The PSNR is used to measure the similarity between the original image and the watermarked image. When the PSNR value is higher than 30 dB, it will be difficult to find the difference between the original image and the watermarked image on human's eyes [10].

Fig. 8 (a)-(d) show the PSNR for different medical images modalities by embedding an ERP text of 2048 characters (2kb). The PSNR values reached for these 100 images are between 57.5306 dB and 66.0223 dB, which demonstrate that the proposed method achieves good imperceptibility.

C. Similarity for Different Embedded Data

Fig. 9 represents the PSNR values for different number of embedded characters from 128 (2^7) characters to 16384 (2^{14}) characters on four medical images CT, X-Ray, MRI and Ultrasound. We can notice that the value of PSNR decreases when number of embedded characters increases. On the other side, the PSNR values are greater than 45 dB, which mean that embedded data is undetectable according to the human visual perception.

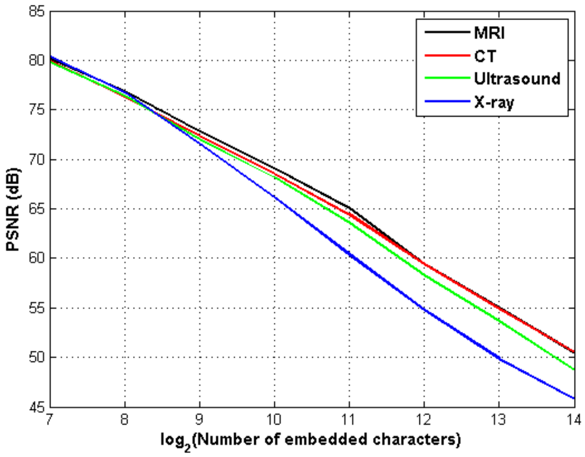


Fig. 9. PSNR values for different images and embedded data.

In Fig. 10, we evaluate the invisibility of embedded data with consideration to the properties of the human eye using Structural Similarity Metric Index (SSIM). For all images, SSIM is close to 1 (SSIM >0.999983) for embedded data less than 1024 characters (2^{10}). SSIM decreases when embedded data increases but remains greater than 0.998069 for maximal data embedding.

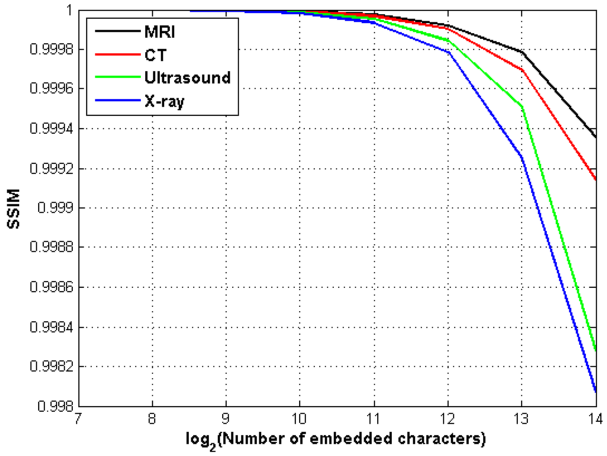


Fig. 10. SSIM values for different images and embedded data.

D. Comparison to Existing Scheme

To prove the effectiveness of the proposed scheme, our method is compared with another semi-blind scheme [1]. The watermarked image is attacked by applying salt & pepper noise and Gaussian noise in order to investigate the robustness.

In Table IV, we analyzed the variation of character error rate (CER) against varying density of Salt and Pepper for some images. For the proposed technique, we observe that the value of Character Error Rate (CER) is equal to zero for all density of Salt and Pepper noise, which means that the extraction of ERP text is done without any error and indicating the highly robust nature of our technique against Salt and Pepper noise. However, in the case of the Sleit's method, we observe that the Character Error Rate (CER) value increases as the density of noise increases, and that causes a deterioration of detection performance.

TABLE IV. Variation of CER on Different Values of Salt & Peppers Attack

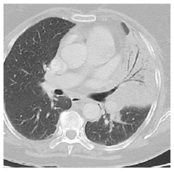
		Salt & Peppers noise density		
I_W	**Methods**	10^{-6}	10^{-5}	10^{-4}
	**Proposed**	0	0	0
	Sleit	0	0	4.6294
	Proposed	0	0	0
	Sleit	0	0	3.2109
	Proposed	0	0	0
	Sleit	2.8645	4.7582	32.5897
	Proposed	0	0	0
	Sleit	25.8245	32.5638	63.8453

TABLE V. Variation of CER on Different Values of Gaussian Attack

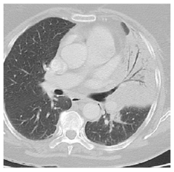
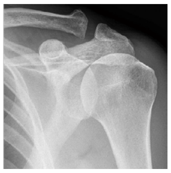
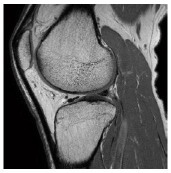
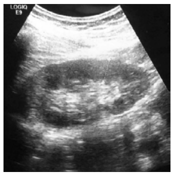
		Gaussian noise variance		
I_W	**Methods**	10^{-6}	10^{-5}	10^{-4}
	**Proposed**	0	0	0
	Sleit	0	0	5.7835
	**Proposed**	0	0	0
	Sleit	0	0	6.2578
	**Proposed**	0	0	0
	Sleit	6.1275	10.4852	27.8906
	**Proposed**	0	0	0
	Sleit	56.7582	61.2878	73.9245

Table V shows the robustness against Gaussian noise with different variances. We can observe that the CER value of Sleit's method is significantly higher than our method. It is also clearly that the CER value of the proposed method is equal to zero for all Gaussian noise values, which ensures an extraction without any error.

To further validate the robustness of the proposed scheme we compare it with the scheme presented in [1]. The considered disturbances are compression, low-pass filter (median filter) and speckle noise. From Table VI, it is obvious that our proposed system outperforms the algorithm introduced in [1] for all disturbances and for all test images. We notice also the compression deteriorates highly the watermark by using Sleit scheme [1] especially for MRI and CT images. Table VI indicates also that the robustness of our method against compression is much higher than the method in [1] and it guarantees the quality of the images with that mentioned behavior.

V. Conclusion

This paper presents a new watermarking scheme for medical images. The proposed scheme is based on a combination of DWT and SVD to embed the watermark in a transparent manner and extracted it with high fidelity. QAM-16 was also used to encode text characters and insert them into the host image. Overall, the proposed scheme demonstrates a good trade-off between of imperceptibility, robustness, and capacity as compared to state of the art methods. Our experimental results show the effectiveness of combination of wavelet algorithm with SVD technique as compared to non-hybrid SVD or DWT methods in terms of PSNR and SSIM.

In the future work, we will aim to overcome the limitation of the proposed semi-blind watermarking by extending it to the blind context. In particular, we will focus in reversible image watermarking by evaluating the performance with much more image types including not only medical image but also texture and biometric images.

References

[1] A. Sleit, R. Etoom, S. Abusharkh and Y. Khero. 2012. An enhanced semi-blind DWT-SVD-based watermarking technique for digital images. The Imaging Science Journal 60, 1 (2012).

[2] Muhammad Arsalan, Sana Ambreen Malik, and Asifullah Khan. 2012. Intelligent Reversible Watermarking in Integer Wavelet Domain for Medical Images. J. Syst. So‡w. 85, 4 (April 2012), 883–894. DOI:http://dx.doi.org/10.1016/j.jss.2011.11.005

[3] Veysel Aslantas. 2009. An optimal robust digital image watermarking based on SVD using differential evolution algorithm. Optics communications 282 (2009), 769–777.

[4] W. Bender, D. Gruhl, N. Morimoto, and Aiguo Lu. 1996. Techniques for Data Hiding. IBM Syst. J. 35, 3-4 (Sept. 1996), 313–336. DOI:http://dx.doi.org/10.1147/ sj.353.0313

[5] Ingemar J. Cox, Joe Kilian, Frank Œomson Leighton, and Talal Shamoon. 1997. Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Processing 6, 12 (1997), 1673–1687. DOI:http://dx.doi.org/10.1109/83.650120

[6] Sudeb Das and Malay Kumar Kundu. 2012. Effective Management of Medical Information (Trough A Novel Blind Watermarking Technique. J. Medical Systems 36, 5 (2012), 3339–3351. DOI:http://dx.doi.org/10.1007/s10916-012-9827-1

[7] Pegah Fakhari, Ehsan Vahedi, and Caro Lucas. 2011. Protecting patient privacy from unauthorized release of medical images using a bio-inspired wavelet-based watermarking approach. Digital Signal Processing 21, 3 (2011), 433–446. DOI:http://dx.doi.org/10.1016/j.dsp.2011.01.014

[8] K. Ghaderi, F. Akhlaghian, and P. Moradi. 2013. A new robust semi-blind digital image watermarking approach based on LWT-SVD and fractal images. 21st Iranian Conference on Electrical Engineering (ICEE) (2013), 1–5.

[9] Aggeliki Giakoumaki, Sotiris Pavlopoulos, and Dimitris Koutsouris. 2006. Multiple Image Watermarking Applied to Health Information Management. IEEE Trans. Information Technology in Biomedicine 10, 4 (2006), 722–732. DOI: http://dx.doi.org/10.1109/TITB.2006.875655

[10] J. Han and X. Zhao. 2015. An Adaptive Gray Scale Watermarking Method in Wavelet Domain. International Journal of Security and Its Applications 9, 10 (2015), 103–114.

[11] L Hanzo, S Xin Ng, WT Webb, and T Keller. 2004. .Quadrature amplitude modulation: From basics to adaptive trellis-coded, turbo-equalised and spacetime coded OFDM, CDMA and MC-CDMA systems. (2004).

TABLE VI. CER Results Under Various Attacks

Attack	Proposed scheme				**Sleit scheme**			
	X-ray	Ultrasound	MRI	CT	X-ray	Ultrasound	MRI	CT
Compression (Q=80%)	1.1254	1.6113	9.6845	8.2651	7.4852	11.2635	35.9475	31.4763
3 × 3 **Median filter**	0.4882	1.2695	1.1718	3.5644	5.8492	9.2383	8.3962	12.3549
Speckle noise	0.3662	0.4882	0.5859	0.7324	4.7482	15.2375	22.6534	8.4742

[12] P. S. Huang, C. S. Chiang, C. P. Chang, and T. M. Tu. 2005. Robust spatial watermarking technique for colour images via direct saturation adjustment. IEEE Proceedings - Vision, Image and Signal Processing 152, 5 (2005), 561–574.

[13] C. H. Lin, D. Y. Chan, H. Su, and W. S. Hsieh. 2006. Histogram-oriented watermarking algorithm: colour image watermarking scheme robust against geometric attacks and signal processing. IEE Proceedings - Vision, Image and Signal Processing 153, 4 (2006), 483–492.

[14] M. Moonen and B. De Moor. 1995. SVD and Signal Processing, III. Elsevier Science(1995).

[15] A. Adhipathi Reddy and Biswanath N. Chatterji. 2005. A new wavelet based logo-watermarking scheme. Pattern Recognition Letters 26, 7 (2005), 1019–1027. DOI:http://dx.doi.org/10.1016/j.patrec.2004.09.047

[16] ASLANTAS Veysel, OZER Saban, and OZTURK Serkan. 2009. Improving the performance of DCT-based fragile watermarking using intelligent optimization algorithms. Optics communications 282, 14 (2009), 2806–2817.

[17] L. Wu, W. Deng, J. Zhang, and D. He. 2009. Arnold transformation algorithm and anti-Arnold transformation algorithm. Proc. of 1st International Conference on Information Science and Engineering (2009), 1164–1167.

[18] R. Karakış, İ. Güler, İ. Çapraz and E. Bilir, A novel fuzzy logic-based image steganography method to ensure medical data security, Computers in Biology and Medicine, 67,(2015), 172–183.

[19] Mousavi SM, Naghsh A, Abu-Bakar SA. Watermarking techniques used in medical images: a survey. J Digit Imaging, 27(6), (2014), 714-29.

Habib Ayad

Habib Ayad is a Professor-Researcher in Computer Sciences at Hassan II University of Casablanca, Morocco; he received his PhD in Computer science from Cadi Ayyad University, Marrakech-Morocco in 2013. His research interests include digital image watermarking and content-based image retrieval.

Mohammed Khalil

Mohammed Khalil received his PhD in Computer Science from Department of Informatics, Faculty of Sciences and Techniques, Mohammedia, Morocco in 2014. He has published four journal papers, 12 communications in international conferences (including EUSIPCO, ICT, ICISP and ISCCSP) and five communications in national conferences. His research interests include digital image and audio watermarking.