

Speech Modulation for Image Watermarking

Mourad Talbi¹, Ben Fatima Sira²

¹Center of Researches and Technologies of Energy, Tunisia

²Engineering School of Tunis, Tunisia

Abstract

Embedding a hidden bits stream in a file is named Digital Watermarking. The file could be a text, an image, an audio, or a video. Actually, digital watermarking has many applications like broadcast monitoring, owner identification, proof of ownership etc... In this work we propose a new image watermarking approach using data modulation. This technique consists at first step in getting the first color in case of RGB image. Then, the Discrete Cosine Transform (DCT) is applied to this first color and the Watermark signal is inserted into the DCT coefficients. This Watermark signal is obtained after amplitude modulation of the original speech signal. After embedding the watermark signal, the DCT inverse is applied in order to obtain the watermarked asset. The novelty of this technique consists in embedding processed speech signal in an image. As previously mentioned, the speech processing is performed via amplitude modulation and for resolving the problem robustness against JPEG compression attack of the proposed technique, we have multiplied the original speech signal by a tuning factor α before performing its modulation. This factor permits to have a compromise between the perceptual quality of the reconstructed speech signal and that of the watermarked image.

1. Introduction

Embedding a hidden bits stream in a file is named Digital Watermarking. The file could be a text, an image, an audio, or a video. In nowadays, digital watermarking has many applications like broadcast monitoring, owner identification, proof of ownership, content authentication, transaction tracking, device control, file reconstruction and copy control [1]. In literature, the host file is named the “asset” and the bit stream is called the “message”.

The major specifications of a watermarking system are:

- Imperceptibility

- Robustness (Against intentional attacks or unintentional ones such as compression) and Capacity.

Importance of each depends on the application. As a matter of fact there exists a trade-off between these factors [2]. Although, watermarking in some literature includes visible imprints, in this paper we only mean the invisible embedding of the data. Author in [3], has showed how to use MATLAB for implementing image watermarking algorithms. These algorithms include the most famous ones which are widely used in current literature or more complex methods are based upon. These are generally classified into three classes [2]:

- Watermarking in Spatial Domain.
- Watermarking in Spectral Domain.
- Watermarking in Hybrid Domain.

The spatial domain watermarking techniques are simpler and are less robust against different geometric and non-geometric attacks [4]. The representative transform domain algorithms embed the watermark by modulating the magnitude of coefficients in a transform domain, such as DWT [5] and SVD [6], [7], [8] and [9]. Transform domain techniques can allow more robustness against many common attacks and more information embedding. Nevertheless the computational cost is higher than spatial-domain watermarking techniques.

DWT is very appropriate for identifying areas in the cover image where a watermark can be imperceptibly embedded due to its good properties of spatio-frequency localization. An important mathematical property of SVD is that slight variations of singular values don't have any influence on the visual perception of the host image, which motivates the watermark embedding procedure to achieve robustness and good transparency [10].

In the next section, we will present with details the new proposed image watermarking approach. In the third section are presented the used evaluation criteria. In the fourth section are presented the

simulation results and finally the conclusion is given in Section 5.

2. The proposed technique of image watermarking

In this work, we propose a new image watermarking approach using data modulation. This approach consists firstly in getting the first color in case of RGB image which is a 2D matrix. Then the Discrete Cosine Transform (DCT) is applied to this matrix and the watermark signal is inserted into the obtained DCT values. This watermark signal is obtained after amplitude modulation of the original speech signal. After embedding the watermark signal, the inverse of DCT is applied in order to obtain the watermarked asset. The extraction process is simply subtracting the original DCT coefficients from the watermarked image ones. After extracting the modulated signal, it is demodulated in order to recover the original signal. In Figure 1, is represented the flowchart of this technique:

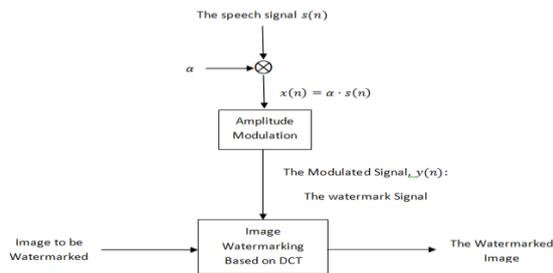


Figure 1. The flowchart of the proposed technique of image watermarking

As shown in this Figure 1, the watermark signal is the modulated signal $y(n)$. The latter is obtained from the amplitude modulation of the signal $x(n)$ which is obtained by multiplying the speech signal, $s(n)$ by a tuning parameter α . When there is no attack performed on the Watermarked Image, α is equals to 1 (see Figure 1).

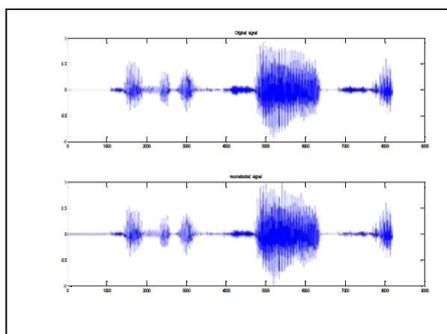


Figure 2. Example of speech extraction from Watermarked Image ($\alpha=1$). SNR=16.0922

Figures 2 and 3 illustrate an example of data embedding in an original image of Woman (Figure 3: (a)). This example is obtained in case of no attack performed on the watermarked image ($\alpha = 1$).

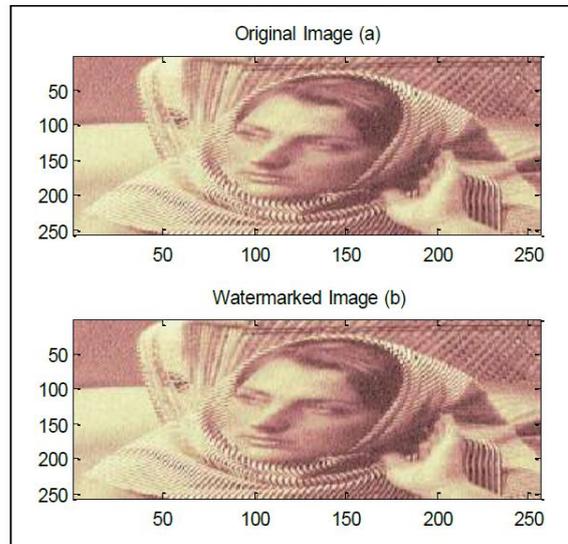


Figure 3. Example of Image watermarking using the proposed technique ($\alpha=1$) PSNR= 62.9315, SSIM= 0.9999

This example shows clearly a very good quality of the watermarked image and an acceptable quality of the reconstructed speech signal after extraction and this by referring to the values of the PSNR, the SSIM and the SNR.

In order to test the robustness of the proposed image watermarking system, a module of a JPEG compression attack is added to it as follow:

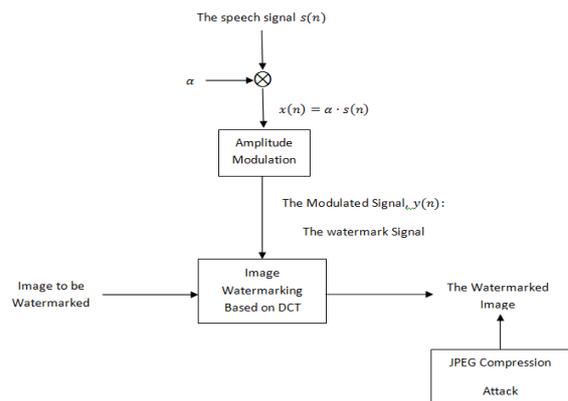


Figure 4. The flowchart of the proposed technique of image watermarking in case of JPEG compression attack

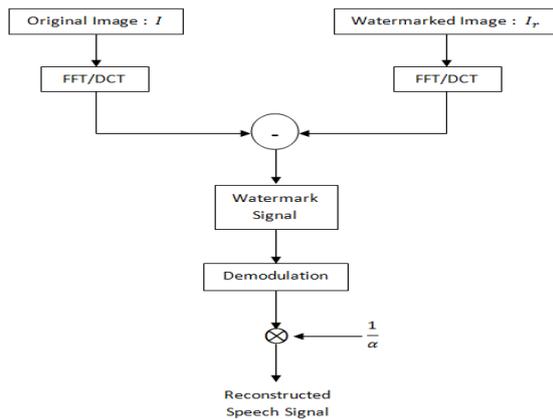


Figure 5. The flowchart of the watermark signal extraction

Figure 5 illustrates the system of watermark signal extraction. According to this Figure, the first step of this system consists in applying the DCT to both original and watermarked images.

In order to obtain the watermark signal, the second step consists in subtracting the DCT coefficients obtained from the watermarked image I_r from those obtained by applying the DCT to the original image I . The extracted watermark signal is then demodulated and the obtained signal is multiplied by $1/\alpha$ in order to have the reconstructed speech signal.

3. Discrete Cosine Transform (DCT)

Discrete Cosine Transform (DCT) transforms a signal from the spatial domain to the frequency domain. DCT is applied in many fields like data compression, pattern recognition and every field of image processing. DCT watermarking is more robust as compared to the spatial domain watermarking techniques. The main steps which used in DCT [6]:

1. Segment the image into non-overlapping blocks of 8×8
2. Apply forward DCT to each of these blocks
3. Apply some block selection criteria
4. Apply coefficient selection criteria
5. Embedded watermark by modifying the selected Co-efficient
6. Apply inverse DCT transform on each block

In DCT, for embedding the watermark information, we divide the image into different frequency bands. In Figure 6, F_L denotes the lowest frequency component of the block, while F_H denotes the higher frequency component and F_M denotes the middle frequency component which is chosen as the embedding region. The Discrete cosine transform achieves good robustness against various signal processing attacks because of the selection of perceptually significant frequency domain coefficients.

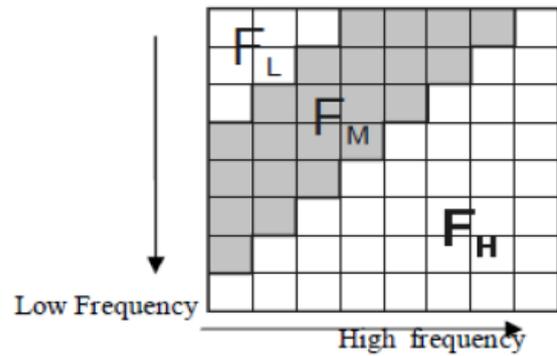


Figure 6. Discrete Cosine Transform Regions [12]

The DCT expression of a 1-D sequence, $f(n)$, of length N , is given as follow [6]:

$$c(u) = \alpha(u) \sum_{n=0}^{N-1} f(n) \cos \left[\frac{(2n+1)u\pi}{2N} \right] \quad (1)$$

For $u = 0, 1, 2, 3, \dots, N - 1$, the inverse of this transform, is defined as follow [6]:

$$f(n) = \sum_{u=0}^{N-1} \alpha(u) c(u) \cos \left[\frac{(2n+1)u\pi}{2N} \right] \quad (2)$$

For both (1) and (2), $\alpha(u)$ is expressed as follow:

$$\alpha(u) = \begin{cases} \sqrt{\frac{1}{N}} & \text{if } u = 0 \\ \sqrt{\frac{2}{N}} & \text{if } u \neq 0 \end{cases} \quad (3)$$

The 2-D DCT is an extension of 1-D DCT and is expressed as follow [6]:

$$c(u, v) = \alpha(u)\alpha(v) \sum_{n,m=0}^{N-1} f(n, m) \cos \left[\frac{(2n+1)u\pi}{2N} \right] \cos \left[\frac{(2m+1)v\pi}{2N} \right] \quad (4)$$

For $u, v = 0, 1, 2, 3, \dots, N - 1$ and $\alpha(u)$ and $\alpha(v)$ defined in expression (3), the inverse of 2D DCT, is expressed as follow:

$$f(n, m) = \sum_{u,v=0}^{N-1} \alpha(u)\alpha(v) c(u, v) \cos \left[\frac{(2n+1)u\pi}{2N} \right] \cos \left[\frac{(2m+1)v\pi}{2N} \right] \quad (5)$$

3.1. Advantages of DCT

The advantages of DCT are:

1. DCT is better than any of the spatial domain methods because this transform is robust against various kinds of attacks such as noising and filtering.
2. DCT is a real transform with better computational efficiency.
3. The DCT gives a better performance in the bit rate reduction.

4. The evaluation criteria

Different functions are used to test the performance of the watermarking through the examining tests on the resulted watermarked image.

4.1. Imperceptibility

The imperceptibility of the watermark is tested through the comparison between the watermarked image and the original one. Different tests are usually employed in this regard.

4.2. Mean Square Error (MSE)

The Mean Squared Error (MSE) is one of the earliest tests that were performed to test if two images are similar. It is expressed as follow:

$$MSE = \frac{1}{n} \sum_{i=1}^n (X_i - X_i^*)^2 \quad (6)$$

4.3. Pick Signal to Noise Ratio (PSNR)

Pick Signal to Noise Ratio (PSNR) is a better test since it takes the signal strength into consideration (not only the error). It is expressed as follow:

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right) \quad (7)$$

4.4. SSIM

The main problem about the previous two criteria is that they are not similar to what similarity means to human visual system (HVS). Structural Similarity (SSIM) is a function expressed in equation (8) and introduced by Wang et al. [11] for overcoming this problem to a great extent.

$$SSIM = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (8)$$

Where μ , σ and σ_{xy} are respectively the mean, variance, and covariance of the images, and c_1 , c_2 are the stabilizing constants.

4.5. Robustness

The robustness of a watermark technique can be evaluated by performing attacks on the watermarked image and evaluating the similarity of the extracted message to the original one.

5. Results and discussion

In this part, we will present the obtained results from the application of the proposed technique on a number of color images. Those results are in terms of MSE and PSNR between the original and the watermarked images and in term of SNR between the original and extracted watermarks.

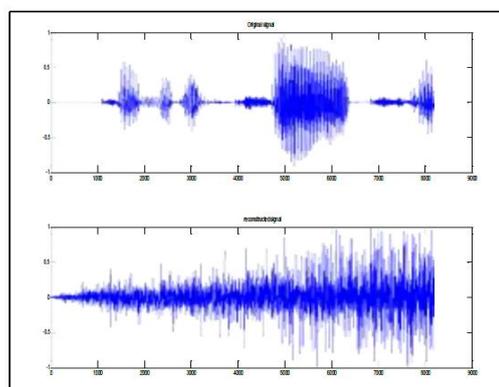


Figure 6. Example of speech signal extraction from Watermarked Image attacked by JPEG Compression in case of $\alpha = 1$

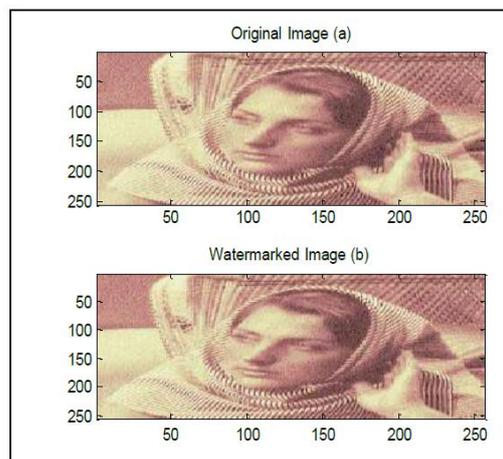


Figure 7. Example of Image watermarking using the proposed technique ($\alpha = 1$).

To solve the problem of non robustness of the proposed watermarking technique against JPEG compression attack, we have varying the value of the tuning parameter α in order to have a compromise between the perceptual qualities of the reconstructed

speech signal after extraction and the watermarked image.

Figures 8 and 9 illustrate an example of Image watermarking with $\alpha = 70$.

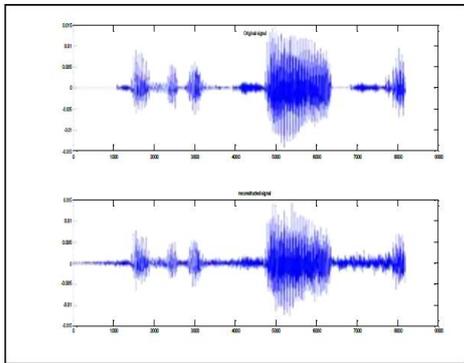


Figure 8. Example of speech signal extraction from Watermarked Image attacked by JPEG Compression in case of $\alpha = 70$. SNR=10.4900

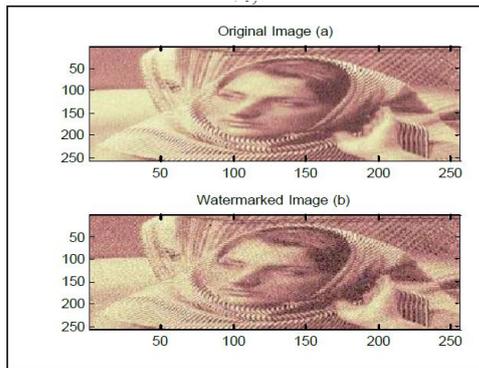


Figure 9. Example of Image watermarking using the proposed technique ($\alpha = 70$)

Figures 10 and 11 illustrate an example of Image watermarking with $\alpha = 80$.

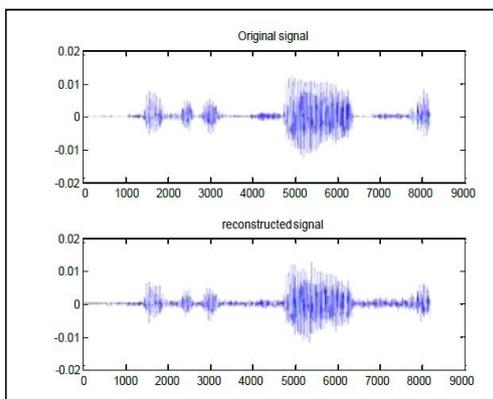


Figure 10. Example of speech signal extraction from Watermarked Image attacked by JPEG Compression in case of $\alpha = 80$. SNR=11.1452

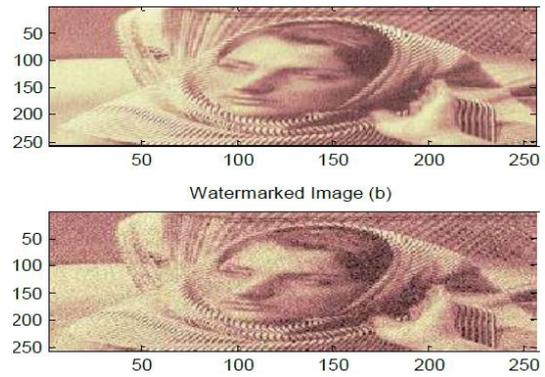


Figure 11. Example of Image watermarking using the proposed technique ($\alpha = 80$). PSNR = 24.819, SSIM = 0.7843

Figures 12 and 13 illustrate an example of Image watermarking with $\alpha = 100$.

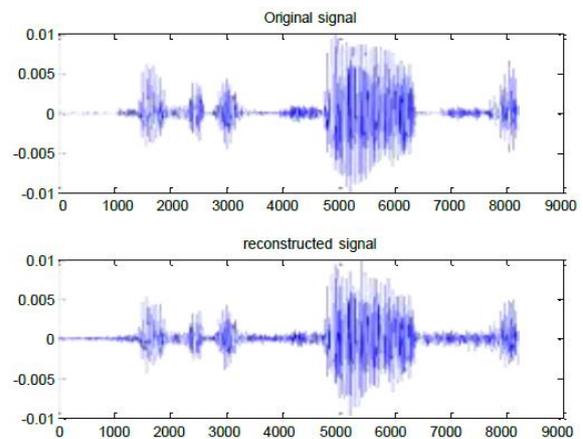


Figure 12. Example of speech signal extraction from Watermarked Image attacked by JPEG Compression in case of $\alpha = 100$. SNR=11.9827

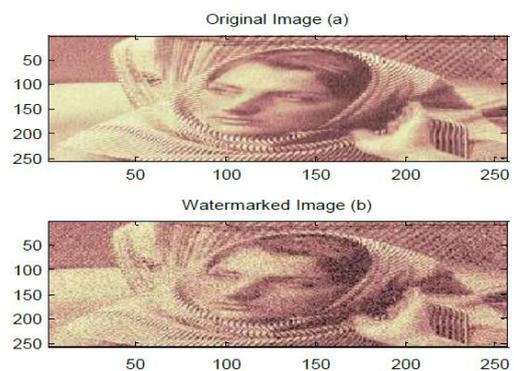


Figure 13. Example of Image watermarking using the proposed technique ($\alpha = 100$). PSNR=22.8809, SSIM=0.7113

According to these results, we remark that the proposed technique is efficient because the

watermark signal and the watermarked image are with good quality (according to PSNR, SSIM, SNR). Though, this proposed technique is not robust against jpeg compression attack ($\alpha = 1$) and the watermark is completely distorted (Figure 5). To solve this problem, we have multiplied the modulated speech signal by a tuning parameter α which permits to improve the watermark signal quality and recover information. In fact, these results show that when we increase the value of α , the quality of the speech signal to be embedded to the original image I , getting better and better. Whereas the quality of the watermarked image I_r is getting worse and worse. Therefore, we have to select the good values of α , that ensure the acceptable qualities of both the watermarked image and the watermark signal.

Table 1 list the results obtained from SNR, PSNR and SSIM computations and this for the proposed technique and the watermarking technique based on DCT and proposed in [3].

Table 1. Comparative study

The Watermarking Technique	SNR	SSIM	PSNR
The proposed technique applied in case of $\alpha = 1$ (no attack is performed)	15.7542	0.9999	62.8809
The proposed technique applied in case of $\alpha = 80$ (JPEG Compression attack)	11.1452	0.7843	24.8191
The proposed technique applied in case of $\alpha = 100$ (JPEG Compression attack)	11.9827	0.7113	22.8809
The image watermarking Technique based on DCT [3]	20.9629	0.9999	59.8783
The image watermarking Technique based on DCT [3] applied with JPEG compression attack	-3.6135	0.7916	31.6208

According to these results and when there is no attack performed on the watermarked image, the proposed technique permits to improve the perceptual quality of the watermarked image and this by referring to the watermarked image obtained when the technique based on DCT is applied [3].

This is based on the PSNR computation. Whereas, according to SNR computation, the extracted watermark (the speech signal) obtained from the proposed technique, is with worse quality when compared to the extracted watermark obtained from the image watermarking technique based on DCT [3] and this due to the amplitude modulation. These results also show that the proposed technique

outperforms the image watermarking technique proposed in [3] and this precisely when the JPEG compression attack is applied to the watermarked image. When using the tuning parameter α in case of applying the JPEG compression attack to the watermarked image, there is a compromise that should be insured in order to obtain an extracted watermark and a watermarked image with acceptable qualities.

6. Conclusion

In this paper we have proposed a new image watermarking technique using data modulation. This technique consists at first step in getting the first color in case of RGB image which is a two dimensional matrix. Then the Discrete Cosine Transform (DCT) is applied to that matrix and embedding the watermark signal into the DCT coefficients. This watermark signal is obtained after multiplying the speech signal (information to be embedded) by a tuning factor α and the obtained signal is then modulated using amplitude modulation. The latter is the watermark signal to be embedded in the original image.

After inserting the watermark signal into the host image, the inverse of DCT is applied in order to produce the watermarked asset. The extraction process is simply subtracting the original DCT coefficients from the watermarked image ones. After extracting the modulated signal, it is demodulated and multiplied by $1/\alpha$, in order to recover the original signal. The obtained results from the SSIM, the PSNR and SNR computations, show the performance of the proposed image watermarking technique.

As previously mentioned, the speech processing is performed via amplitude modulation and for resolving the problem robustness against JPEG compression attack of the proposed technique, we have multiplied the original speech signal by a tuning factor α before performing its modulation. This factor permits to have a compromise between the perceptual quality of the reconstructed speech signal and that of the watermarked image.

7. References

- [1] I.J. Cox, M.L. Miller, J.A. Bloom, J. Fridrich, and T. Kalker, "Digital Watermarking and Steganography," 2nd Edition, Morgan Kaufmann, ISBN-13: 978-0-12-372585-1, 2008.
- [2] Barni, M., & Bartolini, F., "Watermarking Systems Engineering," ISBN: 0-8247-4806-9 Marcel Dekker, Inc. 2004.
- [3] Pooya Monshizadeh Naini (2011). "Digital Watermarking Using MATLAB, Engineering Education and Research Using MATLAB," Dr.Ali Assi (Ed.), ISBN: 978-953-307-656-0, 2011, InTech, Available from: <http://>

www.intechopen.com/books/engineering-education-and-research-using-matlab/digital-watermarking-using-matlab.

[4] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Trans. Multimedia*, vol. 4, no. 1, pp. 121–128, Mar. 2002.

[5] Hassen Lazrag ; Med Saber Naceur Wavelet filters analysis for speckle reduction in intravascular ultrasound images *Sciences of Electronics, Technologies of Information and Telecommunications (SETIT)*, 2012 6th International Conference on 21-24 March 2012, Page(s):375 – 379.

[6] A. Nikolaidis and I. Pitas, "Asymptotically optimal detection for additive watermarking in the DCT and DWT domains," *IEEE Trans. Image Process*, vol. 12, no. 5, pp. 563–571, May 2003.

[7] J. R. Hernandez, M. Amado, F. Perez-Gonzalez, "DCT-domain watermarking techniques for still images: detector performance analysis and a new structure," *Image Processing, IEEE Transactions on* 9, pp. 55–68, Jan 2000.

[8] M. A. M. El-Bendary ; A. Haggag ; F. Shawki ; F. E. Abd-El-Samie, "Proposed approach for improving Bluetooth networks security through SVD audio watermarking," *Sciences of Electronics, Technologies of Information and Telecommunications (SETIT)*, 2012 6th International Conference on 21-24 March 2012.

[9] Adnan Al-smadi, "ARMA model parameters estimation using SVD," *Sciences of Electronics, Technologies of Information and Telecommunications (SETIT)*, 2012 6th International Conference on 21-24 March 2012, 2012, Page(s):814 – 816.

[10] Chih-Chin Lai, C.-C. Tsai, "Digital image watermarking using discrete wavelet transform and singular value decomposition," *IEEE Transactions on Instrumentation and Measurement*, vol. 59, No.11, pp. 3060-3063, Nov. 2010.

[11] Wang, Z.; Bovik, A. C.; Sheikh, H. R. & Simoncelli E. P. (2004). Image quality assessment: From error visibility to structural similarity. *IEEE Trans. Image Processing*, vol. 13, no. 4, pp. 600-612.

[12] Mohamed El Hajji. La sécurité d'images par le tatouage numérique dans le domaine d'ondelettes, thèse, 2012.