

Robust Image Watermarking Scheme Based on Wavelet Technique

Aree Ali Mohammed
College of Science, Computer Dept.
University of Sulaimani
Sulaimani, Iraq

aree.ali@univsul.net

Haval Mohammed Sidqi
Institute of Computer Science.
Technical Foundation
Sulaimani, Iraq

havalms@yahoo.com

Abstract

In this paper, an image watermarking scheme based on multi bands wavelet transformation method is proposed. At first, the proposed scheme is tested on the spatial domain (for both a non and semi blind techniques) in order to compare its results with a frequency domain. In the frequency domain, an adaptive scheme is designed and implemented based on the bands selection criteria to embed the watermark. These criteria depend on the number of wavelet passes. In this work three methods are developed to embed the watermark (one band (LL|HH|HL|LH), two bands (LL&HH | LL&HL | LL&LH | HL&LH | HL&HH | LH&HH) and three bands (LL&HL&LH | LL&HH&HL | LL&HH&LH | LH&HH&HL) selection. The analysis results indicate that the performance of the proposed watermarking scheme for the non-blind scheme is much better than semi-blind scheme in terms of similarity of extracted watermark, while the security of semi-blind is relatively high. The results show that in frequency domain when the watermark is added to the two bands (HL and LH) for No. of pass =3 led to good correlation between original and extracted watermark around (similarity = 99%), and leads to reconstructed images of good objective quality (PSNR=24 dB) after JPEG compression attack (QF=25). The disadvantage of the scheme is the involvement of a large number of wavelet bands in the embedding process.

Keywords: Multi-Bands Wavelet, Watermark, Semi Blind Watermark Detection, Robustness, Malicious Attacks.

1. INTRODUCTION

Digital watermarking is a method to hide some information that is integrated with a multimedia object [1]. The object may be any form of multimedia, such as image, audio, video, or text. Watermarking has many different applications [2], such as ownership evidence, fingerprinting, authentication and integrity verification, content labeling and protection, and usage control. The success of any watermarking scheme is determined by its performance against intentional and unintentional attacks [3,4]. Any watermarking technique has to be evaluated to judge its performance. Three factors, as given below, must be considered while evaluating an image watermarking algorithm.

1. Capacity, i.e. the amount of information that can be put into the watermark and recovered without errors;
2. Robustness, i.e. the resistance of the watermark to alterations of the original content such as compression, filtering or cropping;
3. Visibility, i.e. how easily the watermark can be discerned by the user.

Available techniques use different transform domains to embed the watermark inspired by information coding and image compression. The watermarking is performed in the cover (host) image through several domains such as discrete cosine transforms (DCT) [5], discrete wavelet

transforms (DWT) [6], and discrete Fourier transforms (DFT) [7]. The watermarking algorithm proposed in this work uses DWT ideas [8].

In this study a new digital image watermarking scheme is presented which is based on the float 9/7 Tap filter wavelet transform. Before performing wavelet transformation on the host image, some tests are taken in a spatial domain to make a comparison with a frequency domain. On the other hand, in a frequency domain the watermarking scheme is developed for non-blind and semi-blind techniques. In spatial domain, the watermark is directly embedded into the highly sorted pixel's value while in a frequency domain the host image is firstly decomposed by a multi-resolution wavelet transformation and then embedding watermark into either low or high frequencies based on some criteria [10-12].

The proposed scheme has a good robustness under some conventional attacks and geometrical attacks. Also it is robust against jpeg image compression. Figure (1) illustrates the general diagram of the proposed watermarking scheme applied on spatial and frequency domain respectively.

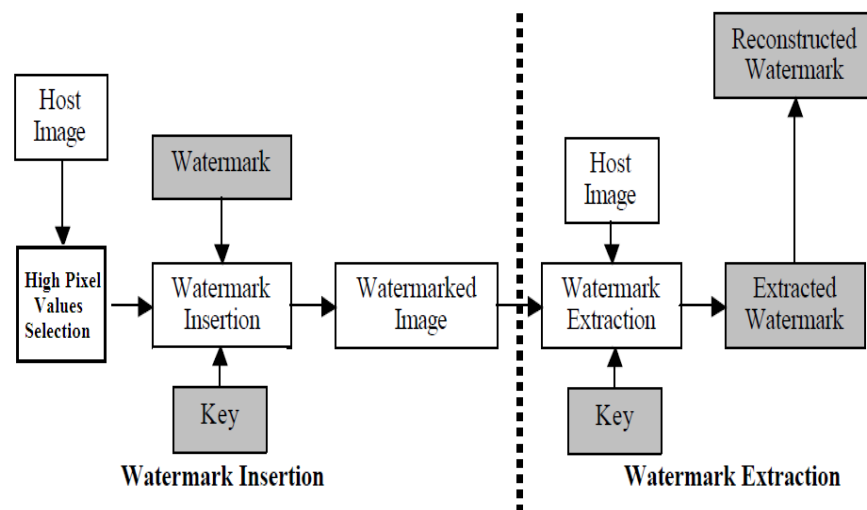


FIGURE 1: General diagram of the watermarking proposed scheme.

This paper will be organized as follows. Section 2 illustrates the proposed watermarking scheme in detail. Section 3 presents experiment results as well as some discussions. Conclusions are given in section 4.

2. PROPOSED WATERMARKING SCHEME

Digital watermarking algorithms are composed of three parts, namely, watermark embedding algorithm, watermark extraction algorithm and watermark detection algorithm. The following subsections describe the details of the proposed scheme.

2.1 Watermarks Type

The watermarks used in this work are divided into three types:

1. Gray or color image,
2. Logo and
3. Randomly generated sequence of bits

Figure (2) shows some watermark types used in image watermarking scheme.

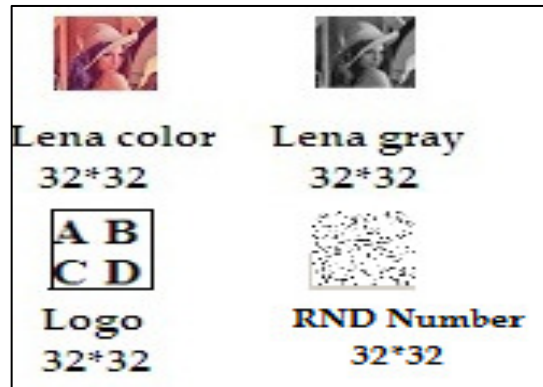


FIGURE 2: Watermarks type.

2.2 Watermarking Embedding Process

In the proposed approach, the embedded watermark must be invisible to human eyes and enough robust to some image processing operations. Before insertion, the host image color system (RGB) is converted to another color space (YCbCr) and then the histogram of the color values is calculated to find out the high pixel values in the host image. YCbCr is not an absolute color space; it is a way of encoding RGB information. The actual color displayed depends on the actual RGB colorants used to display the signal. Therefore a value expressed as YCbCr is only predictable if standard RGB colorants are used. Since the watermark is added to the luminance, the RGB color space of the image should be converted to YCbCr color space. The Y component is used later to embed the watermark.

In the embedding process the watermark is added not directly to the original pixel values of Y – Luminance component but to the selected pixel values based on histogram calculation of Y component. Figure (3) and (4) presents the flowchart of the embedding process in frequency domain for non and semi blind algorithm. The watermark used (random number, logo and gray or color image) is of size 32*32 pixels or 1024 bytes.

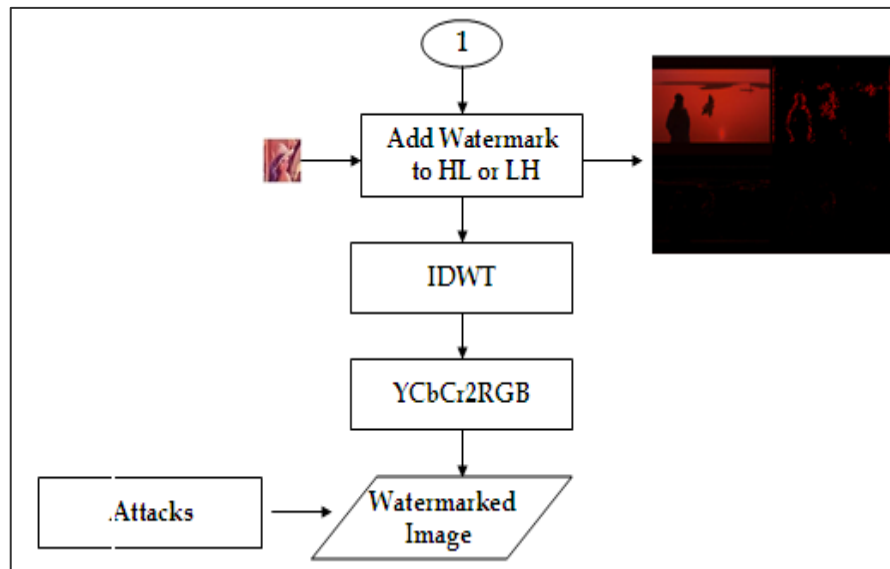
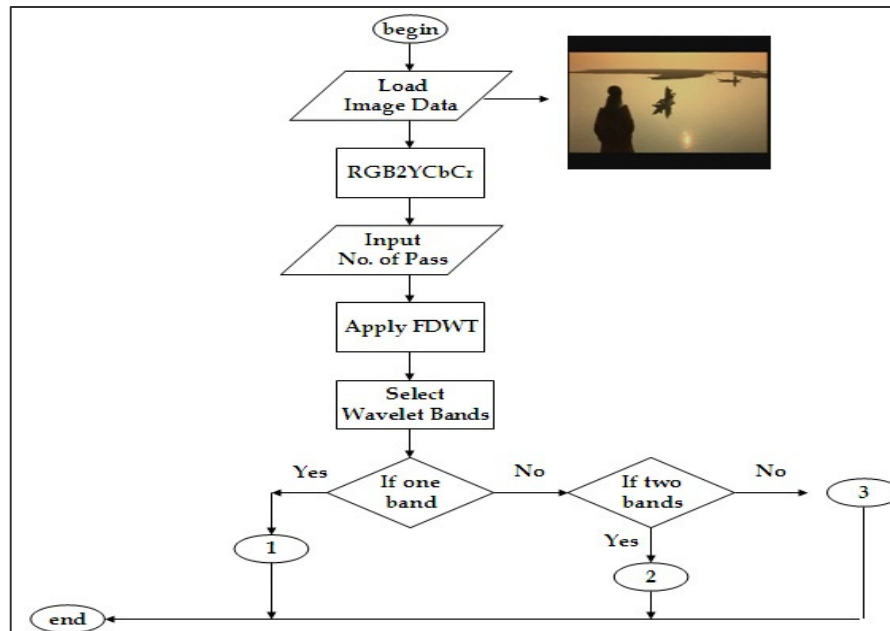
In the frequency domain the watermark is added not directly to the pixel values of the original image but the host image is first transformed into the frequency domain using float 9/7 Tap filter wavelet transform. The transformed image has now a low (approximation) and high (details) frequency regions. In any watermarking scheme developed in the literature, the most important step is the embedding process, which is hiding the information into the specific region of the host signal. In this work, the mid frequencies (HL, LH) depending on the number of pass are selected to embed the majority data of the watermark about (%80) and the rest of the data (%20) is added to the high frequencies (HH). As in the spatial domain the color space of the original image is converted from RGB to the YCbCr system. And then the Y (Luminance) channel which is adequate with a visual system is chosen to add the watermark data.

2.2.1 Non Blind Technique

In non-blind scheme watermark detection, both the original host information and watermark key are needed to estimate the embedded watermark data. The steps of this scheme are presented as follows (see figure 3):

1. Load original color image (RGB).
2. Convert RGB to YCbCr.
3. Apply forward wavelet transform (9/7 Tap Filter).
4. Select Y band to embed the watermark
 - a. Add to LL, HL, LH and HH separately
 - b. Add to (HL + LH) together
 - c. Add to (HL + LH) and some frequencies of HH
5. Store the position of the original image affected by the watermark.

6. Apply inverse wavelet transform.
7. Convert YCbCr to RGB.
8. Perform some malicious attacks on watermarked image (JPEG and JPEG2000 compression).
9. Find fidelity measure (PSNR) between original and watermarked image before and after attacks.
10. Extract watermark before and after attacks.
11. Determine similarity between embedded (original) and extracted watermark.



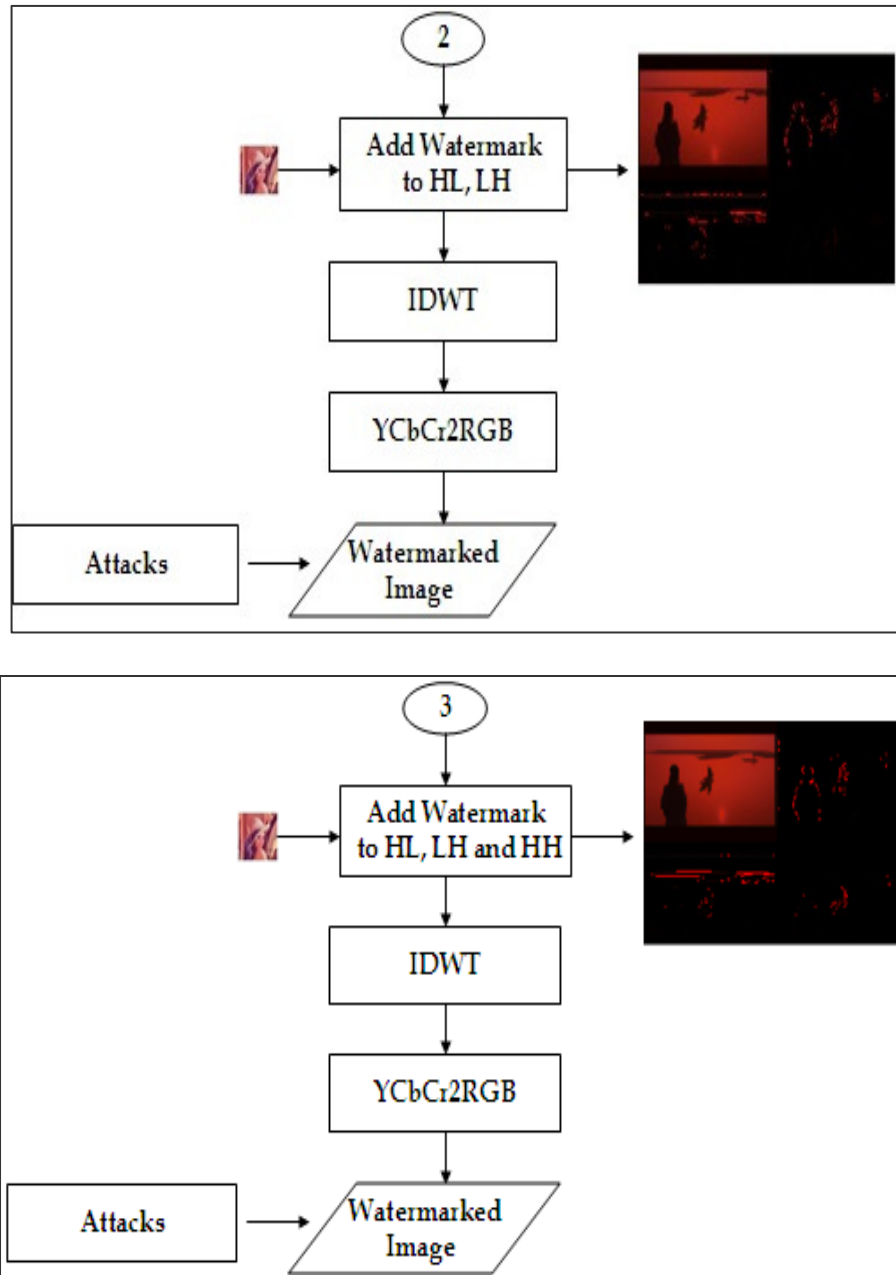


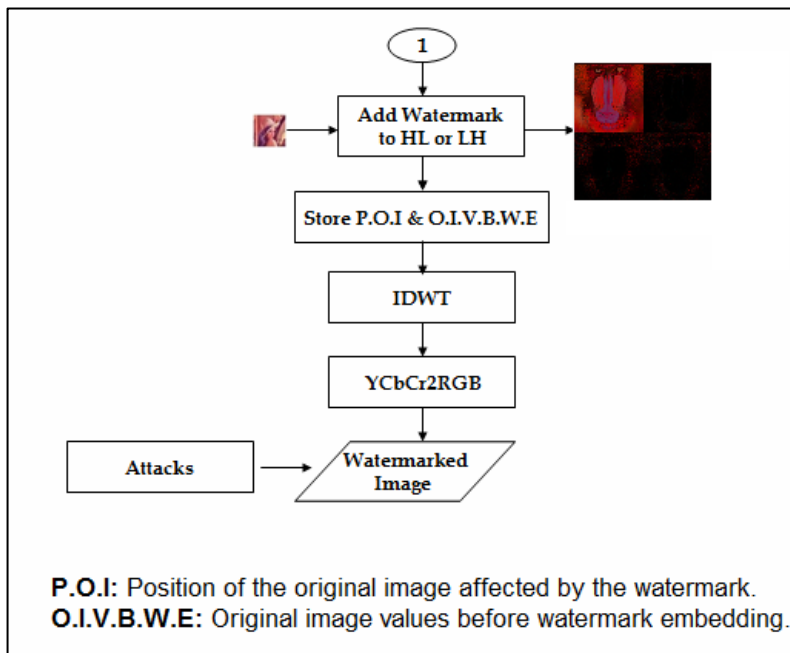
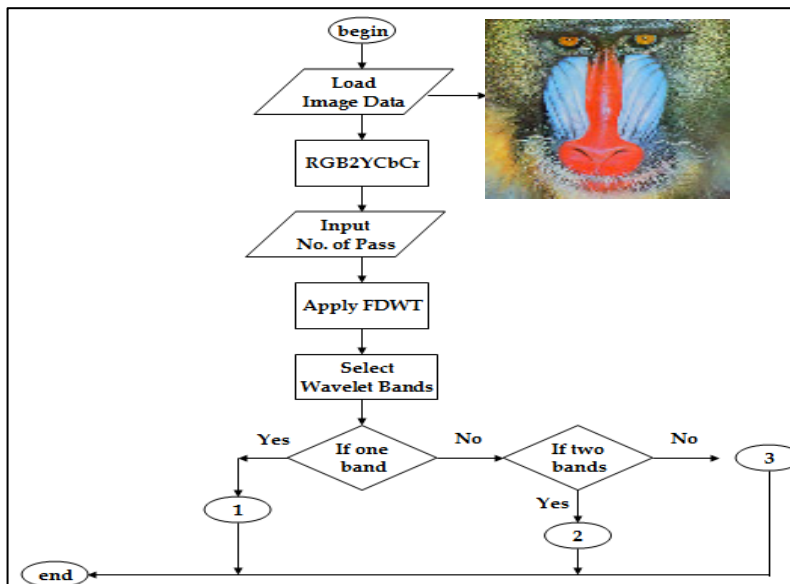
FIGURE 3: Non blind embedding process in frequency domain

2.2.2 Semi Blind Technique

In semi-blind watermark detection, both of the watermark key and watermark position in the original image that affected by the watermark are needed to estimate the embedded watermark data. The steps of this scheme are presented as follows (see figure 4):

1. Load original color image (RGB).
2. Convert RGB to YCbCr.
3. Apply forward wavelet transform (9/7 Tap Filter).
4. Select Y band to embed the watermark
 - a. Add to LL, HL, LH and HH separately

- b. Add to (HL + LH) together
- c. Add to (HL + LH) and some frequencies of HH
5. Store the position of the original image affected by the watermark and the original image values before watermark embedding.
6. Apply inverse wavelet transform.
7. Convert YCbCr to RGB.
8. Perform some malicious attacks on watermarked image (JPEG and JPEG2000 compression).
9. Find fidelity measure (PSNR) between the original and watermarked image before and after attacks.
10. Extract watermark before and after attacks.
11. Determine similarity between embedded (original) and extracted watermark.



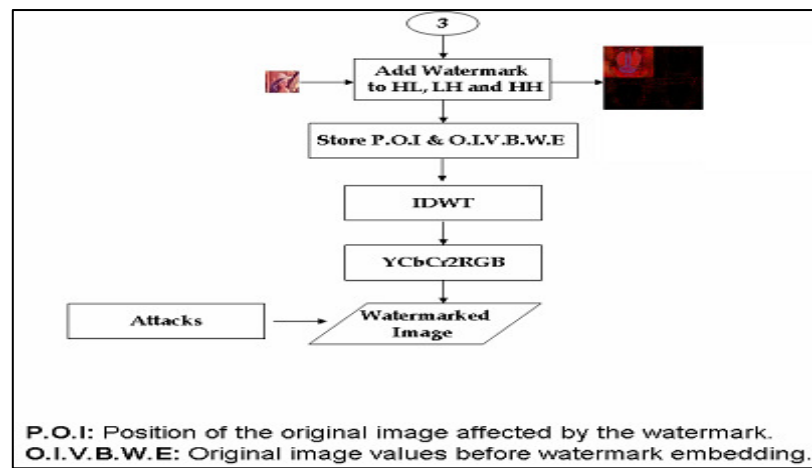
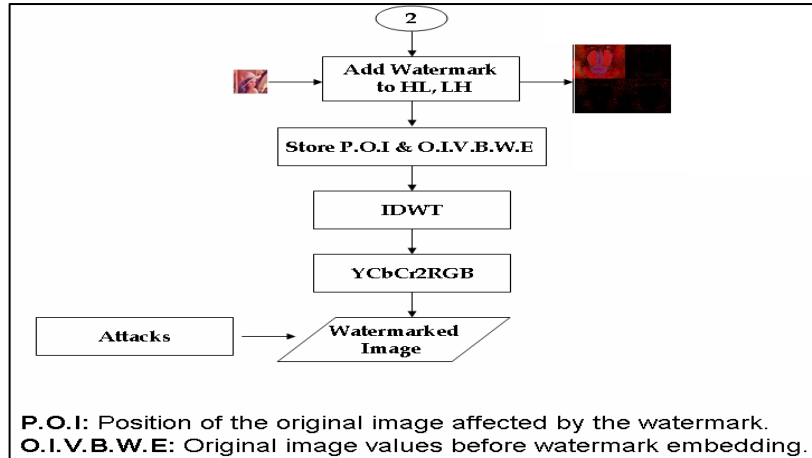


FIGURE 4: Semi blind embedding process in frequency domain

2.3 Watermarking Extracting Process

In figure (5) the flowchart of extraction process for the non-blind scheme is shown.

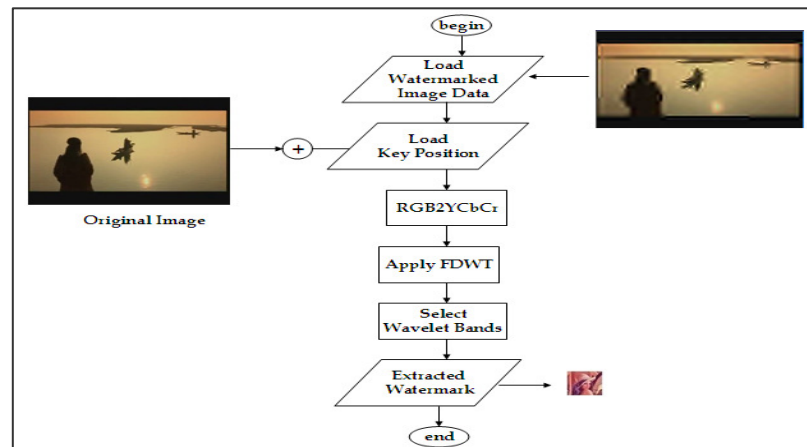


FIGURE 5: Non blind extraction process

In figure (6) the flowchart of extraction process for the semi-blind scheme is shown.

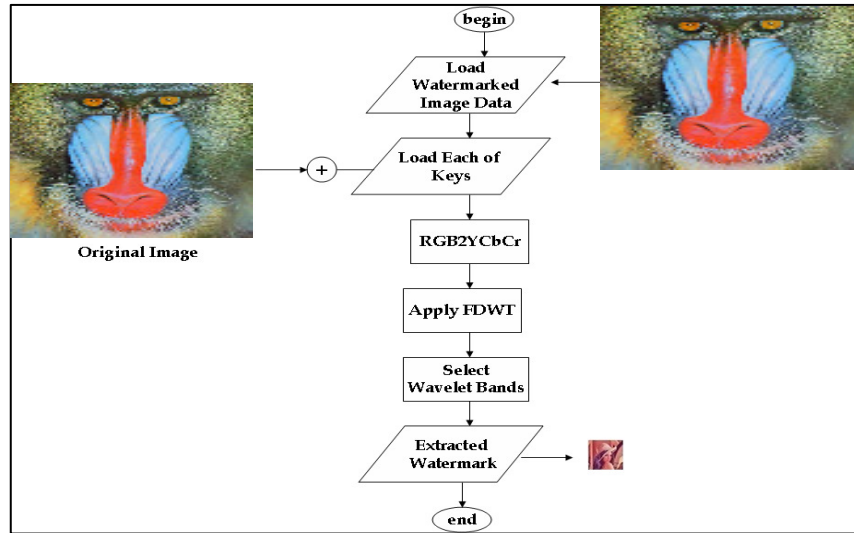


FIGURE 6: Semi blind extraction process

2.4 Watermarking Attacks

Working on attacks is to develop highly robust watermarking schemes and define better benchmarks. In this work, StirMark (benchmarking) program which is writing in C++ language is used to test the robustness of the image watermarking. The robustness tests (embedding, transformation, extraction) fall in (currently) three arbitrary categories:

- Signal processing: these tests typically apply transformation to the image but to not change its size (no resampling required);
- Geometric transformations: these require the use of resampling algorithm as they change the size of the picture.
- Special transforms: they basically include any other test not falling in the previous categories.

Figure (7) illustrates the attacks diagram on watermarked images in both spatial and frequency domain.

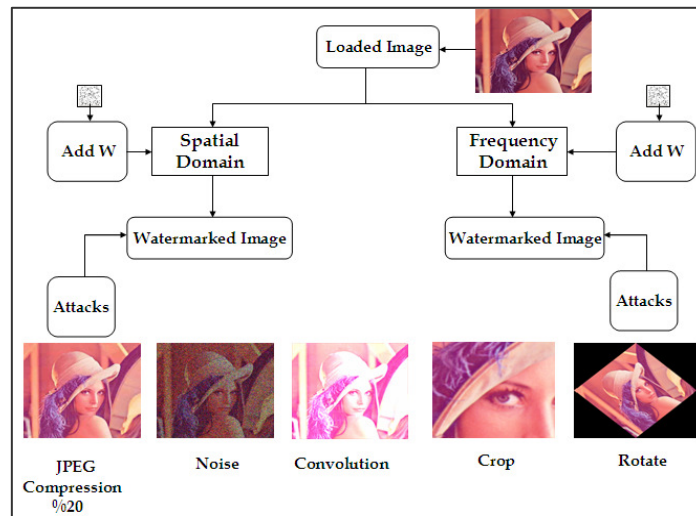


FIGURE 7: Watermarking Attacks type

3. EXPERIMENTS AND RESULTS

To show the efficiency of the proposed schemes in the frequency domain (non-blind and semi-blind), the schemes are tested with the optimal parameters (scaling factor =0.1, No. pass=3, No. band=2 (HL-LH)) on the gray Lena image (512 X 512) with a logo watermark (see Figure 8).



FIGURE 8: Left: original image, Mid: watermarked image, Right: watermark

Figures (9), (10) show the similarity values between numbers of pass under JPEG compression when the quality factor = 50 for (Non and Semi Blind) schemes respectively.

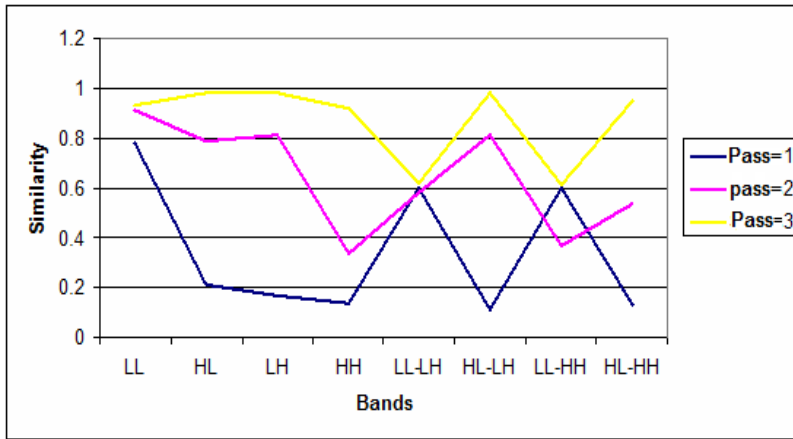


FIGURE 9: Similarity values between numbers of passes under JPEG compression (Non-Blind)

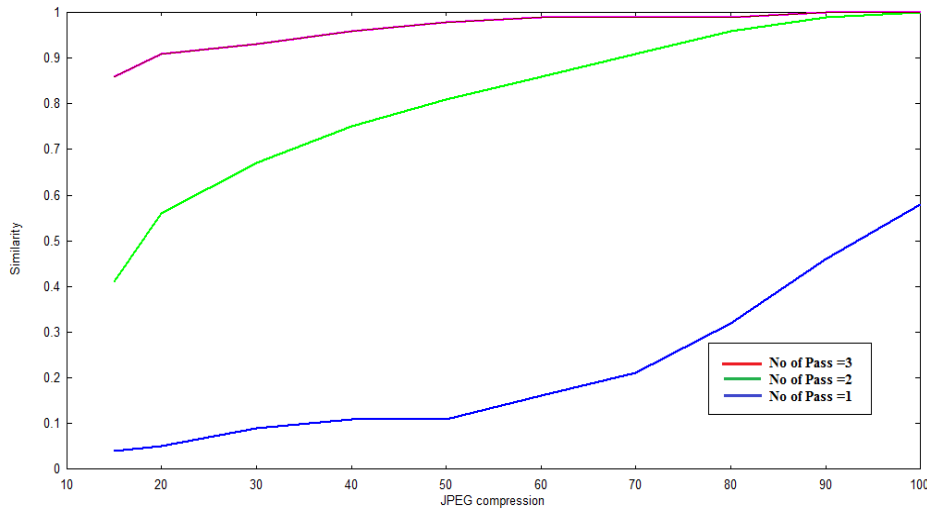


FIGURE 10: Similarity values between numbers of passes under JPEG compression (Semi-Blind)

Table (1) shows that even with low quality factor to 25, the proposed scheme can detect the existence of the watermark. Table (2) presents the comparison results between the current method and other recent publication, which is published in IEEE community [9]. The presented results below are obtained when the proposed scheme is tested for non-blind image watermarking. It also shows the imperceptibility (invisibility) of the watermarked image before the attack, for example the fidelity measure PSNR = 38 dB.






Quality Factor	80	70	50	40	25
Extracted Watermark					
Similarity	1	1	1	1	0.99

TABLE 1: Results against JPEG compression

Different attacks	Similarity		
	Lien[06]	Peng Liu[09]	Our scheme
JPEG (QF=25)	0.63	0.801	0.99
JPEG (QF=40)	0.79	0.828	1
JPEG (QF=50)	0.89	0.916	1
Median Filter 3*3	0.79	0.89	0.98

TABLE 2: Comparison of the proposed scheme with other schemes

4. CONCLUSIONS

The experimental results have shown that the proposed watermark in a frequency domain is invisible to human eyes and very robust to various attacks, such as image compression, image filtering, geometric transformations and noises. In frequency domain, the non-blind watermarking scheme is more robust than semi-blind scheme. For the same used parameters (No. of pass=3, No. of bands=2 HL, LH and scaling factor=0.1), the similarity between the original and the extracted watermark after median filter attack (WinSize=3*3) equals 96% and 92% respectively. The test results led to better performance when the watermark is embedded in the HL and LH bands with a three level of decomposition (i.e., No. of pass=3) in both non and semi-blind schemes.

Simulation results show that the number of wavelet pass affects the embedded watermark values. For the No. of pass=1, the PSNR of the extracted watermark after JPEG attack (CF=25) is equal to 4 dB but for three passes PSNR=24 dB.

Simulation results show that the selection of bands to embed the watermark is very important (in our case best bands are HL and LH). Optimal involved parameters give a new contribution results compared to the recent research publications (see Table 2).

5. REFERENCES

- [1] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques", Proceedings of the IEEE, vol. 87, no. 7, pp. 1079-1107, 1999.
- [2] BARNETT, R. 1999. Digital watermarking: Application, techniques, and challenges. IEE Electron. Comm. Engin. J., 173–183. BENDER, W., BUTERA, W., GRUHL, D., HWANG, R., PAIZ, F. J., AND POGREB, S. 2000. Applications for data hiding. IBM Syst. J. 39, 3 and 4, 547–568.
- [3] VOLOSHYNOVSKIY, S., PEREIRA, S., PUN, T., EGGERS, J., AND SU, J. 2001. Attacks on digital watermarks: Classification, estimation based attacks and benchmarks. IEEE Comm. Mag. 39, 9, 118–126.
- [4] P. Dong, G. Jovan, "Digital Watermarking Robust to Geometric Distortions" IEEE Transaction on Image Processing, vol. 14, no. 12, pp. 2140-2150, 2005.
- [5] J.R. Hernandez, M. Amado, and F. Perez- Gonzalez, "DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis And a New Structure," IEEE Trans. Image Processing, vol. 9, pp 55-68, Jan. 2000.
- [6] Chuanmu Li Haiming Song, 2009, A novel watermarking scheme for image authentication in DWT domain. IEEE on Security and Identification in Communication. pp. 160-162.
- [7] P. Premaratne, "A novel watermark embedding and detection scheme for images in DFT domain", Proceedings of IEE 7th International Conference on Image Processing & Applications, Vol.2, 1999, pp.780-783.
- [8] P. Meerwald, C. Koidl and A. Uhl, "Watermarking Method Based on Significant Difference of Wavelet Coefficient Quantization", IEEE Transaction on Multimedia, vol. 11, no. 5, pp. 1037-1041, 2009.
- [9] L. Peng and D. Zhizhong, "A blind image watermarking scheme based on wavelet tree quantization", IEEE 2nd International Symposium on Electronic Commerce and Security, ISBN: 978-0-7695-3643-9, 2009.
- [10] A. Hanaa, M. hadhoud, and A. Shaalan, "A Blind Spread Spectrum Wavelet Based Image Watermarking Algorithm" International Conference on Computer Engineering & Systems, pp. 251-256, 2009.
- [11] I. Cox, M. Miller, J. Bloom, J. Fridrich and T. Kalker, "Digital Watermarking and Steganography", (Second Edition), Morgan Kaufmann Publisher, ISBN-10: 0123725852, 2007.
- [12] Y. Zhang, "Digital Watermarking "Digital Watermarking Technology: A Review", International Conference on Future Computer and Communication, pp. 250-252, 2009.