A Blind Image Watermarking Algorithm Based on Dual Tree Complex Wavelet Transform

S. Mabtoul , E. Ibn-Elhaj, D. Aboutajdine

***Abstract*—This paper presents a watermarking procedure for digital image in the Complex Wavelet Domain. First, a watermark image as copyright sign is preprocessed with a random location matrix. The original image is transformed in the complex wavelet domain by using DT-CWT, then, according to the characteristics of the image data, the preprocessed watermark image is adaptively spread spectrum and added into the host image DT-CWT coefficients. The proposed watermark algorithm needs two keys: a random location matrix ensures the security of watermarking procedure and spread spectrum watermark sequence guarantees its robustness. Simulation results demonstrate the robustness of our image watermarking procedure, especially under the typical attacks of geometric operations.**

I. INTRODUCTION

Multimedia watermarking technology has evolved very quickly during the last few years. A digital watermark is information that is imperceptibly and robustly embedded in the host data such that it cannot be removed [1, 2].

There are several watermarking algorithms transform the original image into critically sampled domain (The Discrete Real Wavelet Transform (DWT), the Discrete Cosine Transform (DCT) or the Discrete Fourier Transform (DFT)), and add a random sequence to the transformed image coefficients [3, 4].

In general, the DWT produces watermark images with the best visual quality due to the absence of blocking artifacts. However, it has two drawbacks:

--Lack of shift invariance, which means that small shifts in the input signal can cause major variations in the distribution of energy between DWT coefficients at different scales.

--Poor directional selectivity for diagonal features, because the wavelet filters are separable and real.

An important recent development in wavelet-related research is the design and implementation of 2-D multiscale transforms that represent edges more efficiently than does the DWT. Kingsbury's complex dual-tree wavelet transform (DT-CWT) is an outstanding example [5]. The DT-CWT is an overcomplete transform with limited redundancy (2m: 1 for m-dimensional signals). This transform has good directional selectivity and its subband responses are approximately shift-invariant. The 2-D DT-CWT has given superior results for image processing applications compared to the DWT [5, 6].

In the proposed scheme, we applied the Dual Tree Complex Wavelet Transform; the watermark image is preprocessed with a random matrix, adaptively spread spectrum [7] and added into the host image DT-CWT coefficients.

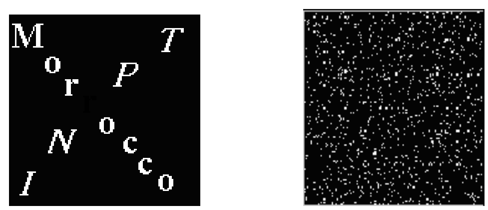
II. THE PROPOSED METHOD

A. *Watermark image disorder preprocessing*

The first step consists to change the watermark image W, which is a binary image {-1, 1}, into a pseudo random matrix W^d by using the following equation:

$$K: W \rightarrow W^d, \qquad W^d(K(i, j)) = W(i, j); \qquad i, j \in N \quad (1)$$

Where K present the first key in our watermark procedure, which is an exclusive key to recreate the watermark image. Figure 1 visualizes an example of watermark image disorder.



Original watermark image　　Disorder watermark image

Fig. 1. The original and disorder watermark image.

B. *Watermark embedding*

The original image is transformed in the complex wavelet domain by using DT-CWT [5]. The watermark image is changed into a pseudo random matrix W^d, then its adaptively spread spectrum W_k and add into low pass subband from final level. Figure 2 shows a block diagram of the proposed watermark embedding.

S. Mabtoul is with the GSCM, University Mohamed V, Rabat, Morocco (e-mail: mabtoul_samira@yahoo.fr).

E. Ibn-Elhaj is with the National Institute of Telecommunication (INPT), Rabat, Morocco (phone: (+212) 37 77 30 79 ; fax : (+212) 37 77 30 44 e-mail: ibnelhaj@inpt.ac.ma).

D. Aboutajdine is with the GSCM, University Mohamed V, Rabat, Morocco (e-mail: aboutaj@fsr.ac.ma).

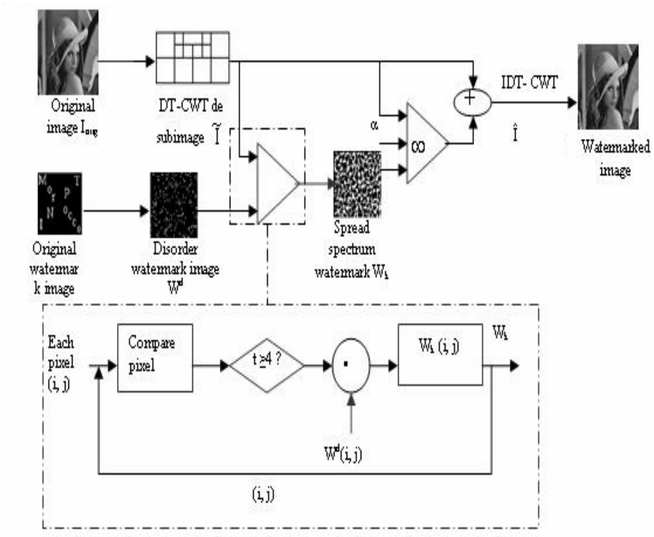


Fig. 2. Image embedding scheme

Image embedding algorithm

1) DT-CWT: perform a 2-level Dual Tree Complex Wavelet on original image I_{orig}. The DT-CWT coefficients are denoted by $\tilde{}$.

2) Generated the spread spectrum watermark W_k: for each pixel (i, j) of the low pass image from final level in $\tilde{}$, the value is compared with those of its eight neighbors, *t* denotes the total number which the value is larger than its neighbors, as described by the following formula:

$$W_k(i,j) = \begin{cases} 1 & \text{if } (t \geq 4 \text{ and } W^d(i,j) = 1) \\ & \quad (t < 4 \text{ and } W^d(i,j) = -1) \\ -1 & \text{else} \end{cases} \quad (2)$$

The spread spectrum watermark W_k present the second key of our image watermarking scheme.

3) Embedded watermark: the spread spectrum watermark sequence W_k is embedded by the following rule:

$$\hat{I}(i,j) = \tilde{I}(i,j) + \alpha . W_k(i,j) . \left|\tilde{I}(i,j)\right| \quad (3)$$

Where:

$\hat{I}$: are the watermarked DT-CWT coefficients.

$\tilde{I}$: are the original DT-CWT coefficients.

W_k: is the spread spectrum watermark image sequence.

α: is an intensity parameter of image watermark.

4) IDT-CWT: by the inverse DT-CWT, we obtain the watermarked image.

C. Watermark detection

Watermark detection is accomplished without referring to the original image and the original watermark image.

Figure 3 shows a watermark detection scheme.

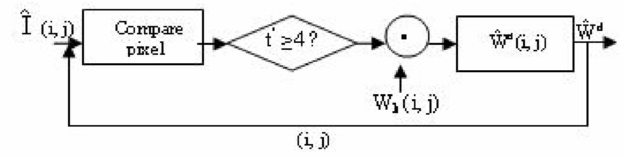


Fig. 3. Image detection scheme

Image detection algorithm

1) The DT-CWT is performed on watermarked image. $\hat{I}$ denote the DT-CWT coefficients.

2) Constructed Watermark image disorder $\hat{W}^d$ *:* for each embed watermark pixel in $\hat{I}$, its value is compared with those of its eight neighbors; *t'* denotes the total number which the value is larger than its neighbors. Disorder watermark image can be formed as:

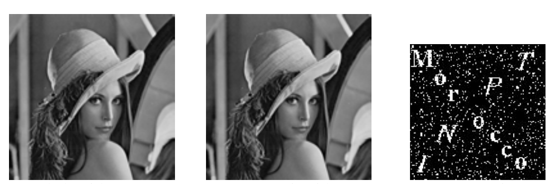
$$\hat{W}^d(i,j) = \begin{cases} 1 & \text{if } (t' \geq 4 \text{ and } W_k(i,j) = 1) \\ & \quad (t' < 4 \text{ and } W_k(i,j) = -1) \\ -1 & \text{else} \end{cases} \quad (4)$$

3) Reconstructed watermark image $\hat{W}$ *:* the reconstructed watermark image $\hat{W}$ is obtained by using the inverse transform of the preprocessing with the first key.

III. Results and Analysis

Our proposed scheme has been tested under various attacks. We chose to test this scheme under PSNR, median filter, JPEG compression, remove lines and scaling attacks introduced by Stirmark [8] and also rotation attack. We have performed the algorithm under Matlab 6.5 environment. In the experiments, we have tested tree test images ("Lena", "Barbara" and "Cameraman"), and there have the similar results. Here, we use "Lena" as an example and the watermark is a binary image with the size of 128x128 pixels.

Figure 4 presents the original image, the watermarked image and the reconstructed watermark image, in which the watermark intensity factor α equal 0.004. We see that the watermarked image is not distinguishable from the original image.



Original image (256x256 pixels) | Watermarked image (256x256 pixels) | Reconstructed watermark image (128x128pixels)

Fig. 4. Original and watermarked image and the reconstructed watermark image.

The robustness of watermarking is measured by the similarity of the detected watermark $\hat{W}$ and the original watermark W, which is defined as:

$$Sim(\hat{W},W)=\sum_i\sum_j(\hat{W}(i,j).W(i,j)) \Big/ \sum_i\sum_j(W(i,j)^2) \quad (5)$$

We tested this watermark approach with DWT transform; the results are gathered in figure 6.

In the first simulation, we tested the scheme's robustness under different PSNR situation. Figure 5.a show a typical result. Results show that we can still correctly detect the watermark under these types of PSNR attacks (figure 6.a). The results obtained with DT-CWT transform are better than the results obtained with DWT transform.

Median filter attack:

We tested the robustness against median filter. Figure 5.b has shown a typical result. The similarities of original watermark and reconstructed watermark are shown in figure 6.b. We noticed that we can still correctly detect the watermark with the algorithm used the DT-CWT transform. With the algorithm used the DWT transform, we can't detect the watermark if the filter factor is bigger than 7.

Scaling attack

We tested this scheme when the image undergone a scaling (see figure 5.c). The results are shown in figure 6.c. from the results obtained we notices that we can detect the watermark image if we used the DT-CWT or the DWT.

Remove line attack

The lines dropping, which are some lines are removed from the watermarked image. We tested this scheme against this type of attack (see figure 5.d). The experiment result is plotted in figure 6.d. The results show that we can reconstruct the watermark image correctly if we used the DT-CWT or the DWT.

JPEG compression attack

We have also tested the robustness against JPEG compression (see example in figure 5.e). The corresponding results are presented in figure 6.e. this scheme is robustness against this type of attack.

Rotation attack

We evaluated the robustness of this scheme against rotation attacks. Image rotation makes the coordinate axes changed. Without synchronization of orthogonal axes, we cannot reconstruct the image mark correctly Figure 5.f illustrates the effect of this transformation. The results are shown in figure 5.f. according to the results we notices that we can reconstruct correctly the watermark image if we used the DT-CWT.

IV. CONCLUSION

In this paper, we have proposed a novel scheme of image watermarking. This scheme applies the Dual Tree Complex Wavelet Transform; the watermark image is preprocessed with a random matrix, adaptively spread spectrum and added into the DT-CWT coefficients. The experimental results have confirmed that this new scheme has high fidelity and it's robust against JPEG compression, geometric attacks (scaling, remove line and rotation with small angle) and signal processing (PSNR, median filter) introduced in StirMark.

ACKNOWLEDGMENT

The authors would like to thank Dr. Nick Kingsbury for allowing use to use his DT-CWT algorithm, and for his valuable discussions.

REFERENCES

[1] F. P. Gonzalez & Juan R. Hernandez, " A tutorial on digital watermarking", In IEEE Annual Carnahan Conference on Security Technology, 1999.

[2] Ingemar J. Cox, Matt L. Miller, " The first 50 years of electronic watermarking", Journal of Applied Signal Processing, 2, 126-132, 2002.

[3] A. Piva, M. Barni, F. Bartolini, and V. Cappellini, "DCT-based watermark recovering without restoring to the uncorrupted original image," in Inter-national Conference on Image Processing, vol. III, pp. 520-523, 1997.

[4] D. Kundur and D. Hatzinakos, “A robust digital image watermarking method using wavelet-based fusion,” in *Proc. IEEE Int. Conf. Image Processing 1997 (ICIP 97)*, vol. 1, Santa Barbara, CA, Oct. 1997, pp. 544–547.

[5] N.G. Kingsbury, “Complex wavelets for shift invariant analysis and filtering of signals”, Applied Computational Harmonic Anal, vol. 10, no. 3, pp. 234-253, May 2001.

[6] T H Reeves and N G Kingsbury, “Overcomplete image coding using iterative projection-based noise shaping”, ICIP 02, Rochester, NY, Sept 2002.

[7] Z. Huai-yu, L. Ying and C. Wu: A blind spatial-temporal algorithm based on 3D wavelet for video watermarking. ICME 2004: 1727-1730.

[8] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Attacks on copyright marking systems,” in Lecture Notes in Computer Science: Information Hiding. Berlin, Germany: Springer, 1998, pp. 218–238.

Watermarked image with 40 % of PSNR quality | detected watermark image

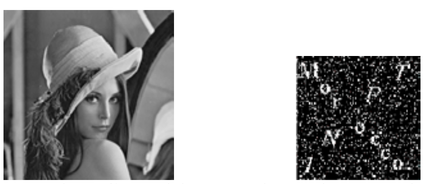
a. Test image under PSNR attack

Median filtered Watermarked image under factor 9 | detected watermark image

b. Test image under median filter attack

Scaled Watermarked image (ratio 50%) | detected watermark image

c. Test image under scaling attack



Removed 100 lines of the watermarked image | detected watermark image

d. Test image under remove lines attack

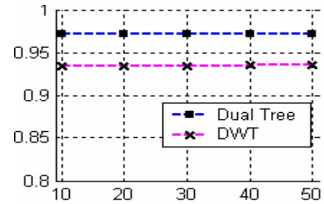
JPEG compressed Watermarked image of quality 35% | detected watermark image

e. Test image under JPEG compression attack

Rotated Watermarked image angle (10°) | Recovered image | detected watermarl image

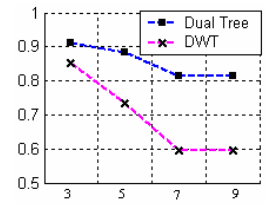
f. Test image under rotation attack

Fig. 5. The effect of attacks



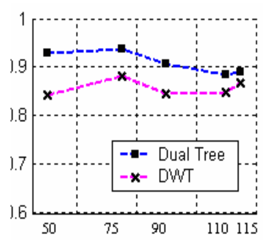
PSNR (db)

a. the effect of PSNR attack



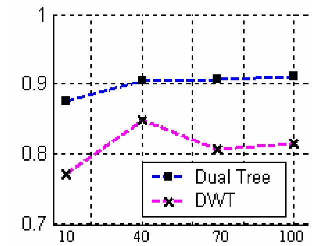
filter factor

b. the effect of median filter attack



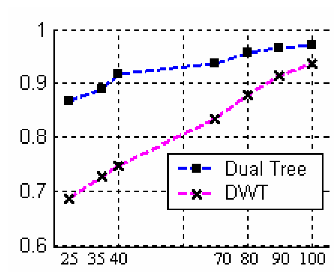
factor scaling (%)

c. the effect of scaling attack



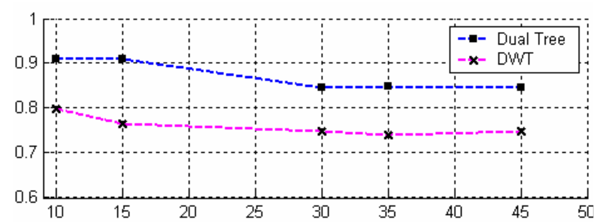
the number of line dropping

d. the effect of remove lines attack



the quality of image (%)

e. the effect of JPEG compression attack



angle (°)

f. the effect of rotation attack

Fig. 6. The experiment results of many attacks to the watermarking algorithm