A Blind Chaos-Based Complex Wavelet-Domain Image Watermarking Technique

S. Mabtoul[1] *, E. Ibn-Elhaj*[2] *, D. Aboutajdine*[1]

[1] GSCM, University Mohamed V, Rabat, Morocco
[2] Institut National des Postes et Télécommunications (INPT), Rabat, Morocco.

Summary

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. In this scheme, we apply the DT-CWT transform only locally, we transform the subimage, which is extracted from the original image, in the complex wavelet domain by using DT-CWT, then, according to the characteristics of the subimage data, the preprocessed watermark image is adaptively spread spectrum and added into the host subimage DT-CWT coefficients. The proposed watermark algorithm needs three keys: a subimage, a random location matrix and spread spectrum watermark. The first and the second ones ensure the security of watermarking procedure and the third one guarantees its robustness. Simulation results demonstrate the robustness of our image watermarking procedure, especially under the typical attacks of geometric operations.

Key words:

Image watermarking, chaos, dual tree complex wavelet transform, spread spectrum.

Introduction

In recent years the phenomenal growth of data changes in the open networks and an extensive use of digital media. Consequently, security of multimedia data as well as the copyright protection becomes an important question [1, 2]. Digital watermarking technique has been identified as one of the possible solutions for copyright protection in the past two decades. It consists of hiding secret information in a robust and invisible manner into digital media, (e.g., image, audio and video). Many, digital watermarking algorithms has been proposed and applied with success in a wide variety of applications including copyright control (owner identification, proof of ownership, transaction tracking and copy control) broadcast monitoring and device control [3].

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 [4, 5, 6].

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 and Poor directional selectivity for diagonal features [7, 8]. 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 [7]. 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.

In the proposed scheme, we used the Dual tree Complex Wavelet Transform. It is well known that attacks on a local area in the image would cause serious effects to the complex wavelet coefficients used. In order to decrease the effects caused by local attacks, we apply, in our chaos-based complex wavelet domain watermarking framework, the Dual Tree Complex Wavelet Transform only locally, which means that DT-CWT is performed only in a local area in the image. We transform the subimage, which is extracted from the original image [9], in the complex wavelet transform domain by using DT-CWT, then, according to the characteristics of the subimage data, the preprocessed watermark image is adaptively spread spectrum [10] and add into the host subimage DT-CWT coefficients.

The paper is organized as follows. Firstly, we will present the different steps for the proposed scheme. Then, we will present the experimental results; and finely we will finish by a conclusion.

Manuscript received March 25, 2006.
Manuscript revised March 30 , 2006.

2. The Proposed Method

2.1 Watermark Image Disorder Preprocessing

This 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:

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

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.

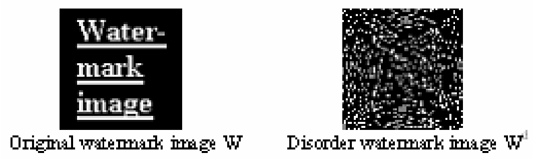


Fig. 1.The original and disorder watermark image.

2.2 Constructed Subimage

To construct the subimage we use the following process [9]:

1. We first split the original image I_{orig}, into many non-overlapping small blocks with 8x8 pixels in a scan-line order. With the image has 256x256 pixels, we will get 1024 small blocks.

2. We label the small blocks from number 1 to number 1024.

3. We generate a sequence S_i, which contains 1024 elements, by using the logistic map under a special initial value i_{seq}. The logistic map is one of the simplest chaotic maps, described by:

$$x_{k+1} = \mu x_k (1 - x_k) \qquad (2)$$

Where $0 \leq ì \leq 4$. When $3.5699456 \leq ì \leq 4$, the map is in the chaotic state [9].

4. We multiply each element of S_i by 1024 and then round it toward infinity. Therefore, we obtain a new sequence S_n, in the integer domain [1, 1024].

5. We select the forefront 256 different elements in the new sequence noted by S_1, and we choose the small blocks accordingly. Finally, we construct a subimage I_{sub} in a scanline order. Figure 2 visualizes this selection process.

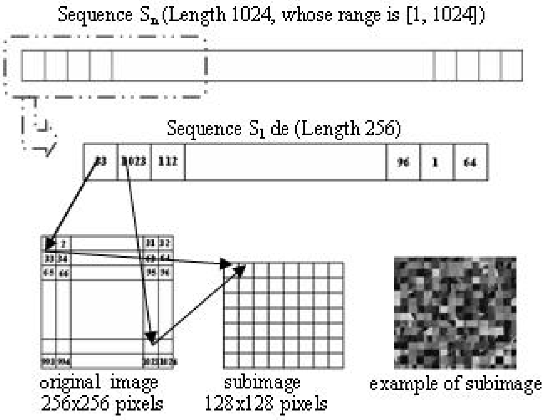


Fig. 2. Constructed subimage processing

2.3 Watermark Embedding

The subimage extracted from the original image is transformed in the complex wavelet domain by using DT-CWT [7]. The watermark image, which is changed into a pseudo random matrix W^d, is adaptively spread spectrum W_k and added into low pass subband coefficients [9, 10]. Figure 3 shows a block diagram of the proposed watermark embedding.

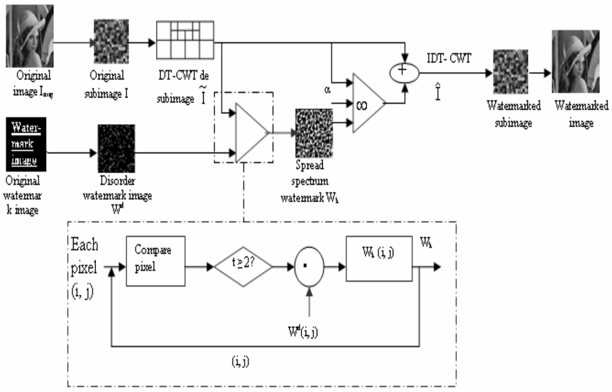


Fig. 3. Image embedding scheme

Image embedding algorithm:

1. Constructed subimage: the first, we extract the subimage from the original image which is to be watermarked (see sect. 2.2).

2. DT-CWT: perform a 2-level Dual Tree Complex Wavelet on original subimage I. the DT-CWT coefficients are denoted by $\tilde{I}$.

3. Generated the spread spectrum watermark W_k: for each pixel (i, j) of the low pass subband in $\tilde{I}$, the value is

compared with those of its eight neighbors, t denotes the total number which the value is larger than its neighbors. If the total number which the value is larger than its neighbors is bigger than 2 and $W^d(i, j)= 1$ or is lower than 2 and $W^d(i, j)= -1$, we puts $W_k(i, j) = 1$; otherwise, $W_k(i,j)= -1$, as described by the following formula:

$$W_k(i,j)=\begin{cases} 1 \quad if (t\geq 2 and W^d(i,j)=1) or \\ \qquad (t<2 and W^d(i,j)=-1) \\ -1 \quad else \end{cases} \tag{3}$$

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

4. Embedded watermark: spread spectrum watermark W_k is embedded by the following rule:

$$\hat{I}(i,j) = \tilde{I}(i,j) + \alpha . W_k(i,j) . \left|\tilde{I}(i,j)\right| \tag{4}$$

Where:

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

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

W_k: is the spread spectrum watermark.

α: is an intensity parameter of image watermark.

5. IDT-CWT: by the inverse DT-CWT, we obtain the watermarked subimage.

6. Finally, according to the label sequence S_1, we put every small block of the watermarked subimage into the original position of original image. Thus, we get the watermarked image.

2.4 Watermark Detection

Watermark detection is accomplished without referring to the original image and the original watermark image [9, 10]. Figure 4 shows a watermark detection scheme.

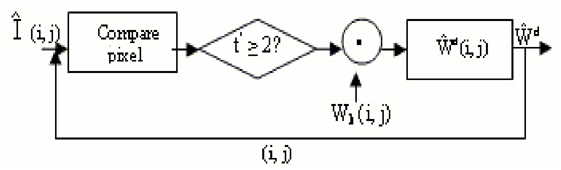


Fig. 4. Image detection scheme

Image detection algorithm:

1. The DT-CWT is performed on watermarked subimage, which extracted from the watermarked image. $\hat{I}$ denotes 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:

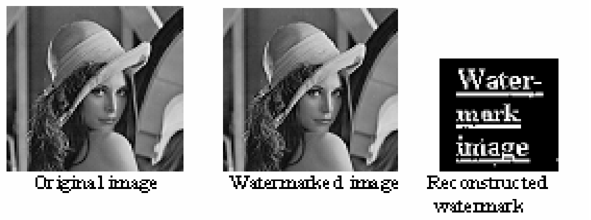
$$\hat{W}^d(i,j)=\begin{cases} 1 \quad if (t'\geq 2 and W_k (i,j)=1) or \\ \qquad (t'<2 and W_k (i,j)=-1) \\ -1 \quad else \end{cases} \tag{5}$$

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.

3 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, affine and scaling attacks introduced by Stirmark [11] 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 64x64 pixels.

Figure 5 presents the original image, the watermarked image and the detected watermark image, in which the watermark intensity factor á equals 0.004 and iseq equals 0.1564. We see that the watermarked image is not distinguishable from the original image.



Original image Watermarked image Reconstructed watermark

Fig. 5. Original and watermarked images and the reconstructed watermark

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

$$Sim(\hat{W},W)= \sum_i\sum_j(\hat{W}(i,j).W(i,j)) \Big/ \sum_i\sum_j(W(i,j)^2) \tag{6}$$

We chose to test this watermark approach with DWT transform and to compare the results. The results are gathered in figure 9.

Key attack:

The most attractive features of chaos in information hiding are its extreme sensitivity to initial conditions and the outspreading of orbits over the entire space. These special characteristics make chaotic maps excellent candidates for watermarking and encryption. All the sequences generated by the logistic map are very sensitive to initial conditions, in the sense that two logistic sequences generated from different initial conditions are uncorrelated statistically.

It is clear that the privacy key "K" and the initial conditions are fundamental to watermark detection; it is to say that the watermark image can be reconstructed correctly with the correct keys. A pirate has insufficient knowledge to reconstruct watermark image, and a watermark image with an error keys is shown in Figure 6.

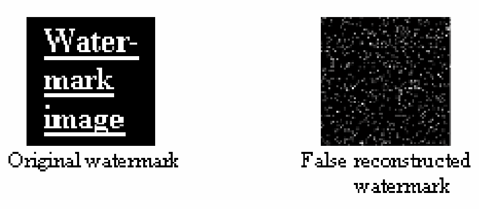


Fig. 6. The detected watermark with error key

Figure 7 show the result of similarity values obtained wherein we have 2000 different keys, and the correct key appears in position 1000. Only one (true) key gives high similarity value (0.9588), while the other 1999 keys have the similarity values distributes between 0.1294 and 0.1985.

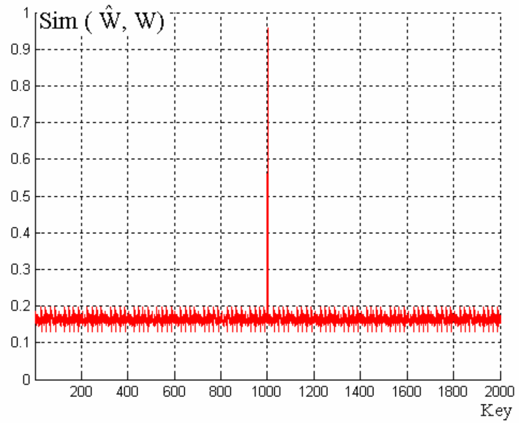


Fig. 7. Detector response for watermarked "Lena" image.

Noise attack:
We have tested the scheme's robustness under different PSNR situations. Figure 8.a show a typical result. The similarities of original watermark and reconstructed watermark are shown in Figure 9.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 8.b has shown a typical result. The similarities of original watermark and reconstructed watermark are shown in Figure 9.b. We noticed that we can still correctly detect the watermark with the algorithm used the DT-CWT transform.

JPEG compression attack:
We have also tested the robustness against JPEG compression (see example in Figure 8.c). The corresponding results are presented in Figure 9.c. this scheme is robustness against this type of attack.

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 8.d). The experiment result is plotted in Figure 9.d. The results show that we can reconstruct the watermark image correctly if we used the DT-CWT.

Affine attack:
We tested this scheme against affine attack (see Figure 8.e). The experiment result is plotted in Figure 9.e. The results show that we can reconstruct the watermark image correctly if we used the DT-CWT.

Scaling attack:
We tested this scheme when the image undergone a scaling (see Figure 8.f). The results are shown in Figure 9.f. From the results obtained, we notices that we can detect the watermark image if we used the DT-CWT or the DWT and The results obtained with DT-CWT transform are better than the results obtained with DWT transform.

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 8.g illustrates the effect of this transformation. The results are shown in Figure 9.g. According to the results we notice that we can reconstruct correctly the watermark image if we used the DT-CWT.

Conclusion

In this paper, we have proposed a novel scheme of image watermarking. This scheme applies the Dual Tree Complex Wavelet Transform only locally, based on the chaotic logistic map, the watermark image is preprocessed with a random matrix, adaptively spread spectrum and added into the DT-CWT domain. This algorithm has been tested on real image with various attacks. The experiments on simulations show that the proposed algorithm is robust to PSNR, median filter, JPEG compression, remove lines, affine, scaling and rotation attacks.

Acknowledgments

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] F. Hartung & M. Kutter, "Multimedia Watermarking Techniques", Proceedings of the IEEE, Vol. 87, No. 7, July 1999.

[4] Ersin Elbasi and Ahmet M. Eskicioglu "A DWT-Based Robust Semi-Blind Image Watermarking Algorithm Using Two Bands" IS&T/SPIE's 18th Annual Symposium on Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VIII Conference, San Jose, CA, January 15–19, 2006.

[5] G. Lo-varco and W. Puech. DCT-Based Data-Hiding for Securing ROI of Color Images. Proc. International Conference on Image Processing ICIP-2005, Genova, Italy, september 2005.

[6] Janusz Kusyk and Ahmet M. Eskicioglu. "A Semi-blind Logo Watermarking Scheme for Color Images by Comparison and Modification by Comparison and Modification of DFT Coefficients" Optics East 2005, Multimedia Systems and Applications VIII Conference, Boston, MA, October 23-26, 2005.

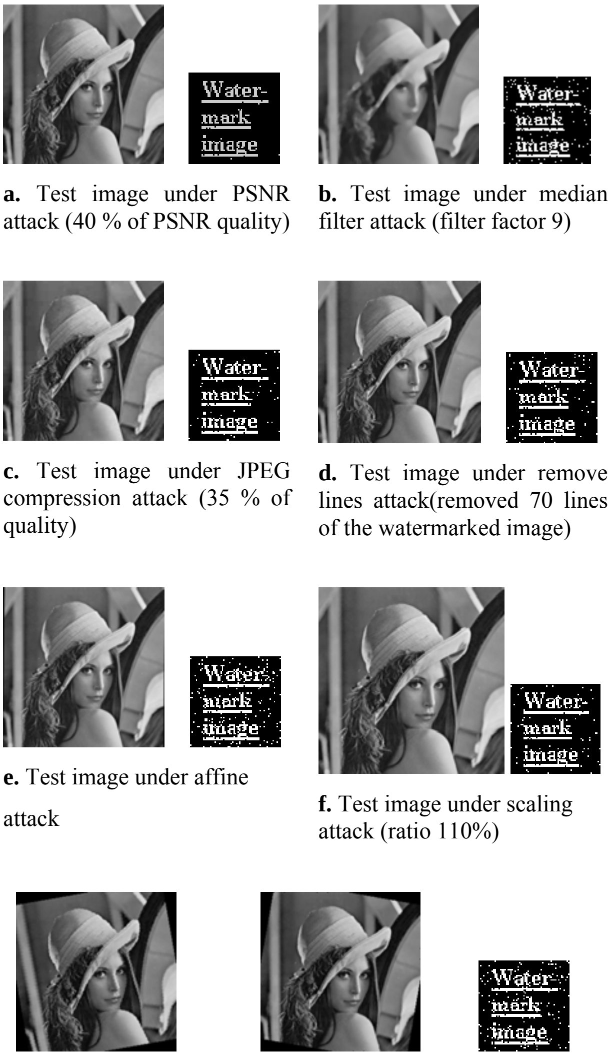
[7] N.G. Kingsbury, "Complex wavelets for shift invariant analysis and filtering of signals", Applied Computational Harmonic Anal, vol. 10, no. 3, pp. 234-253, May 2001.

[8] P.Loo and N G Kingsbury, "Watermarking using complex wavelets with resistance to geometric distortion", Proc. EUSIPCO 2000, Tampere, Finland, Sept 5-8, 2000.

[9] Z. Dawei, C. Guanrong and L. Wenbo, "A chaos-based robust wavelet-domain watermarking algorithm", Chaos, Solitons and Fractals, Vol. 22, pp. 47-54, Oct. 2004.

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

[11] Fabien A. P. Petitcolas, Martin Steinebach, Frédéric Raynal, Jana Dittmann, Caroline Fontaine, Nazim Fatès. A public automated web-based evaluation service for watermarking schemes: StirMark Benchmark. In Ping Wah Wong and Edward J. Delp, editors, proceedings of electronic imaging, security and watermarking of multimedia contents III, vol. 4314, San Jose, California, U.S.A., 20-26 January 2001. The Society for imaging science and technology (I.S.&T.) and the international Society for optical engineering (SPIE). ISSN 0277-786X.



a. Test image under PSNR attack (40 % of PSNR quality)

b. Test image under median filter attack (filter factor 9)

c. Test image under JPEG compression attack (35 % of quality)

d. Test image under remove lines attack(removed 70 lines of the watermarked image)

e. Test image under affine attack

f. Test image under scaling attack (ratio 110%)

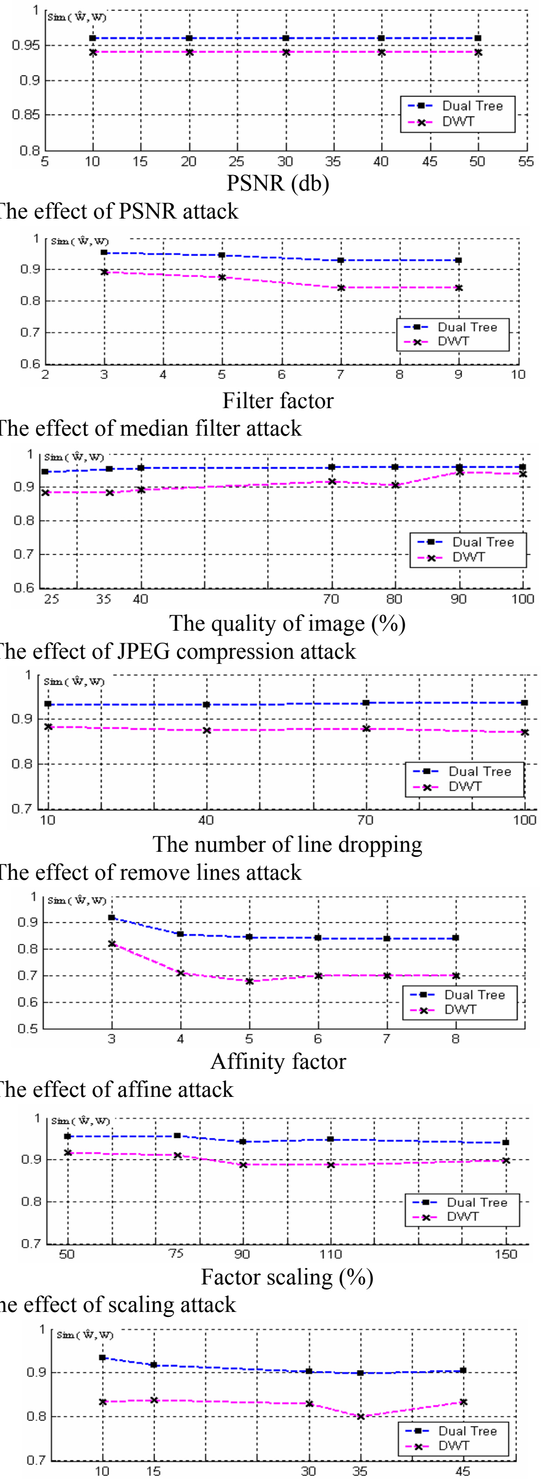
Rotated Watermarked image angle (10°)

Recovered image

detected watermark image

g. Test image under rotation attack

Fig. 8. The effect of attacks



a. The effect of PSNR attack

b. The effect of median filter attack

c. The effect of JPEG compression attack

d. The effect of remove lines attack

e. The effect of affine attack

f. The effect of scaling attack

g. The effect of rotation attack

Fig. 9. The experiment results of many attacks to the watermarking algorithm