FREQUENCY-DOMAIN WAVELET BASED MULTIRESOLUTION DIGITAL WATERMARKING

[1]Yüksel TOKUR
e-mail: tokur@gantep.edu.tr

[2]Ergun ERÇELEBİ
e-mail: ercelebi@gantep.edu.tr

[1]*Gaziantep University,MYO,* 27310, Gaziantep, Turkey
[2]*Gaziantep University, Electrical & Electronics Engineering,* 27310,Gaziantep, Turkey

Keywords: Digital Image Watermarking, Fast Fourier Transform, Discrete Wavelet Transform, White Noise

ABSTRACT

In this paper, we present a robust digital image watermarking technique. For robustness to geometric transformation, a watermark is embedded in the DFT domain with aid of geometric figures. Additionally, a second watermark is embedded in the DWT domain. The DCT coefficients are treated as wavelet transform coefficients. To robustness of the proposed method is tested by applying different types of attacks. The tests show good performances against common signal processing procedures such as noise addition, image compression, median filtering, as well as geometric transforms such as clipping and rotation.

I. INTRODUCTION

There has been tremendous growth in electronic commerce applications and online services recently but service provider fear unrestricted duplication and dissemination of copyrighted material. Publishers, artists, and photographers, however, may be unwilling to distribute pictures over the Internet due to a lack of security; images, music clips and digital video can be easily duplicated and distributed. In this study, we concentrate on the application of digital watermarking to images. Digital watermarking with an identification code makes it possible to identify the source, author, creator, owner, and distributor or authorized consumer of a document. For the digital media security such as copyright protection and authentication which creates a pressing need for digital media protection schemes.

In the literature for the watermarking of images can be grouped into two classes: spatial domain techniques [1,2] which embed the data by directly modifying the pixel values of the original image and transform domain methods [3,4] which embed the data by modulating the transform domain coefficients. Wavelet theory has emerged as an effect means of representing image signals in terms of a multiresolution structure [5]. Based on multiresolution representation [6-7], a signal is divided into a number of components, each corresponding to different frequency bands. Since each component has a better frequency and time localization, the multiresolution decomposed signal can be processed much more easily than its original representation. Multiresolution techniques are characterized by their successive approximation property. The multiresolution successive approximation not only enhances the resolution of an image, but also enhances the resolution of a watermark simultaneously [8].

The rest of the paper is organized as follows: Section 2 introduces the proposed method for digital watermarking. In Section 3 and 4 describes the embedding and detecting process as a function of the algorithm parameters. In Section 5, some experimental results are given and conclusions are provided in section 6.

II. PROPOSED WATERMARKING TECHNIQUES

The human eye is able to catch modifications to the lower frequencies since most of the energy of the image is put on low frequency components in the spectrum domain. Therefore, the watermark is usually inserted into the low frequency and middle frequency coefficients and the modifications will spread throughout the image. Low and middle frequency coefficients are less likely to be affected during common signal processing than high frequency coefficients. One of the main advantages of the WT is to describe more accurately aspects of human vision system (HVS) as compared to Fourier Transform (FT) and Discrete Cosine Transform (DCT). This advantage of the WT allows using higher energy watermarks in regions where the HVS is known to be less sensitive so that embedding watermarks in these regions provides to increase the robustness of the watermarking techniques.

In this work, a spread spectrum geometric watermark is embedded in the middle frequencies of DFT domain. Furthermore, a second watermark is embedded in the DWT domain since the DCT-based JPEG standard is widely used in image compression community. At frequency domain, the watermark is a geometric figure in which a hexagon lies inside a circle centered on the zero frequency term of an image's Fourier's magnitude spectrum. Furthermore, a second watermark is embedded in the DWT domain. Both watermarks can be detected without the use of original image.

III. WATERMARK EMBEDDING

The embedding procedure consists of two steps: the embedding in DFT and the embedding in DCT.

3.1 THE EMBEDDING OF WATERMARKING IN DFT DOMAIN

The watermark is a geometric figure, in which a hexagon lies inside a circle centered on the zero frequency term of an image's Fourier's magnitude spectrum. We attempt to encode a string of text using a hexagon lying inside a circle in the frequency domain. The watermark is inserted into the low frequency and middle frequency coefficients and the modifications will spread throughout the image. To create the data embedding process, a container image is selected and the input text message is converted to binary. In Fig. 1 (a) watermarking is applied to input of encoder, the output of encoder is a row vector of the binary representation of the text. For example; the watermarking of text 'image' is applied to input of the encoder, the output of encoder is a row vector of the binary representation of '001001001101000001000111000101'.

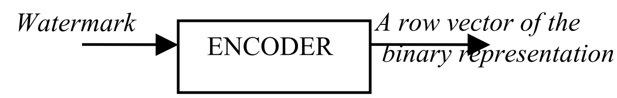

Fig. 1 The block diagram of the encoder

Fig. 2 illustrates a block diagram of the watermarking insertion process.

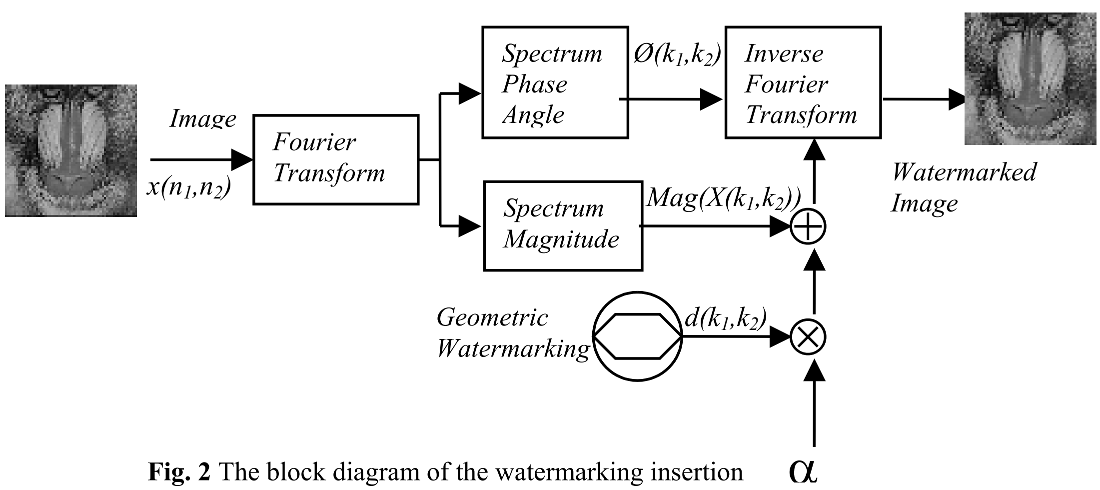

Fig. 2 The block diagram of the watermarking insertion techniques

3.2 THE EMBEDDING OF WATERMARKING IN DCT DOMAIN

The first step involves applying Lth level discrete wavelet decomposition on the image. The Haar wavelet basis is chosen due to its simplicity. The DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. We embed the watermark into the detail wavelet coefficients of the watermarked image at frequency domain with the use of a key. This key is randomly generated and d is used to select the exact locations in which to embed the watermark.

The watermarking based on WT uses the equation given below

$$I_{W_{u,v}} = \begin{cases} W_i + \alpha |W_i| x_i, & u,v \in HL, LH \\ W_i & u,v \in LL, HH \end{cases}$$

where W_i denotes the coefficient of the transformed image into wavelet domain, x_i the bit of the watermark to be embedded, and α a scaling factor. Fig. 3 illustrates the watermarking technique based on WT. The corresponding Lth level inverse wavelet transform from the composed image components is computed to form second watermarked image. The transformed image is shown in the Fig. 5 (c).

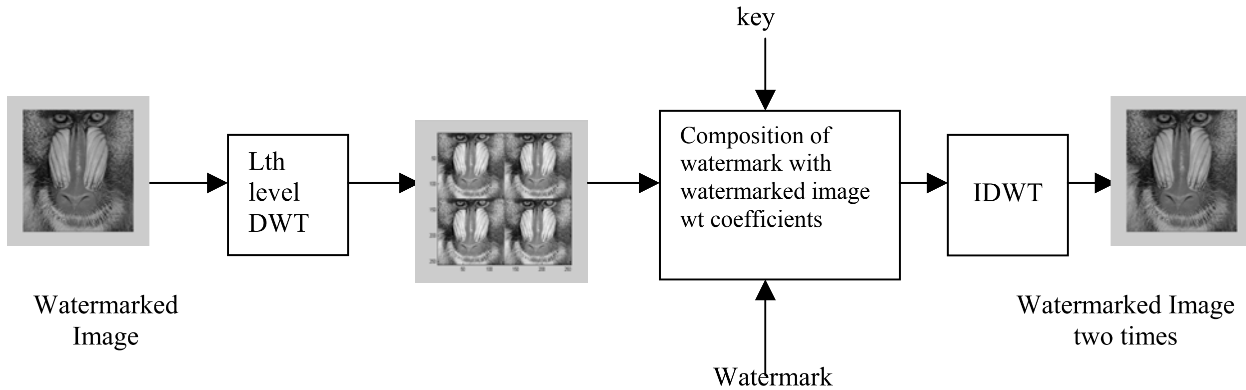

Fig.3 Embedding of a watermark in the wavelet domain

IV. WATERMARK DETECTION

The watermark detection is the reverse process of the watermark embedding process. It is also consists of two steps: extraction of watermarking in DFT and extraction of watermarking in DCT.

4.1 EXTRACTION OF WATERMARKING IN DFT

DFT domain detection doesn't need the original image. The key variables such as radius of circle and alpha values are needed to extract the text from the attacked image. The magnitude of the FFT is computed. The first key value, radius, tells the function where to look for the data. The second key value, alpha, is used as a threshold value in determining whether the pixel carries a logic value "1" or "0". The function encoder given in Fig. 1 performs the embedding process while decoder in Fig. 4 performing the extraction process.

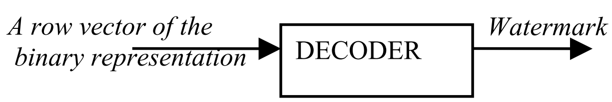

Fig. 4 The block diagram of the decoder

After the watermark extraction the bit error between the embedding watermark and the extracted watermark is computed.

4.2 EXTRACTION OF WATERMARKING IN DCT

The original image isn't needed for the watermark extraction either. The detection process requires knowledge of the watermark and the key. First step involves applying Lth level discrete wavelet decomposition on the image. We then make use of the key to find the location in which the watermark was embedded for each resolution level. After the watermark extraction the cross-correlation between the embedding watermark and the extracted watermark is computed.

V. EXPERIMENTAL RESULTS

The baboon (256x256 pixels) image is used as the container image. Fig. 5 (a) displays container image. Fig. 5 (b) plots watermarked image at DFT domain (psnr= 482.3894 dB). Fig. 5 (c) displays second watermarked image at DWT domain (psnr= 132.1404 dB). To form the watermarking at DFT domain, the 'GantepUniversity' text message is converted into binary using encoder (as shown in Fig. 1). The output of encoder, which is a row vector of the binary representation of the text, is used to obtain geometric watermarking image. Fig. 5 (d) displays addition of first watermark to container image in frequency domain. Fig. 5 (e) shows the second watermark image for DWT domain. Fig. 5 (f) illustrates recovered second watermark from image watermarked two times. We can see that the watermarked image looks almost the same as the original images and the watermarks are invisible.

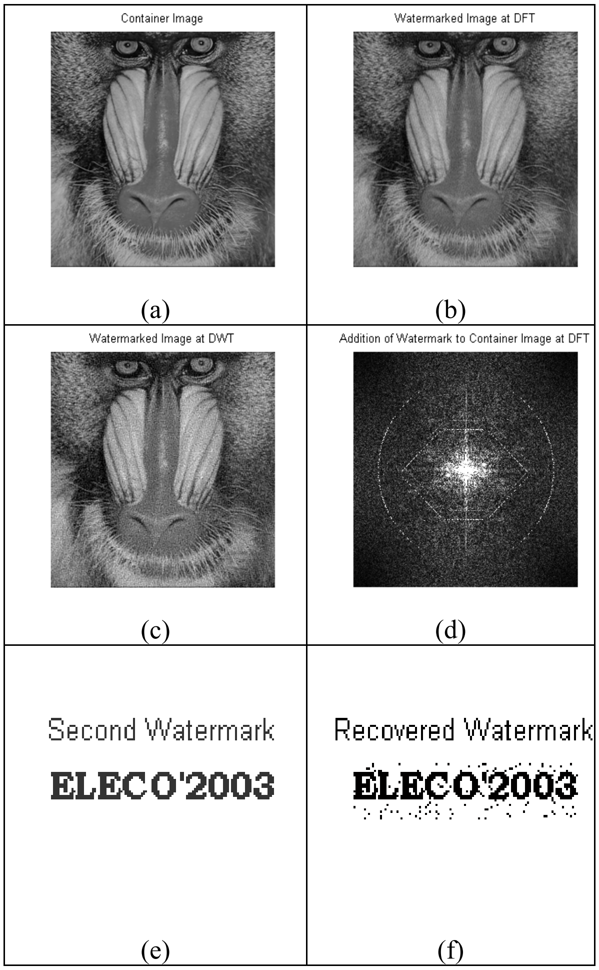

Fig. 5 (a) Container image (b) watermarked image at DFT domain (c) second watermarked image at DWT domain (d) addition of the first watermark to container image in frequency domain (e) the second watermark image which is embedded at DWT (f) recovered second watermark.

To test the robustness of the proposed algorithm to noise, we added noises to watermarked image at different PSNRs and extracted watermark data from corrupted watermarked image without loss of information. Fig. 6 (a) shows the corrupted watermark image by white Gaussian noise. Fig. 6 (b) plots the rotated watermarked image at psnr=15.7837dB. Fig. 6 (c) shows clipped watermarked image by the values of 100 rows by 100 columns. Fig. 6 (d) illustrates result of median filtering for watermarked image at psnr= 132.1404dB. After applying median filtering, the psnr value increased 135.970. Fig. 6 (e) shows the stirmarked image (banding=4.00). Fig. 6 (f) illustrates diffuse glow watermarked image (graininess=6, glow amount=10, clear amount=15).

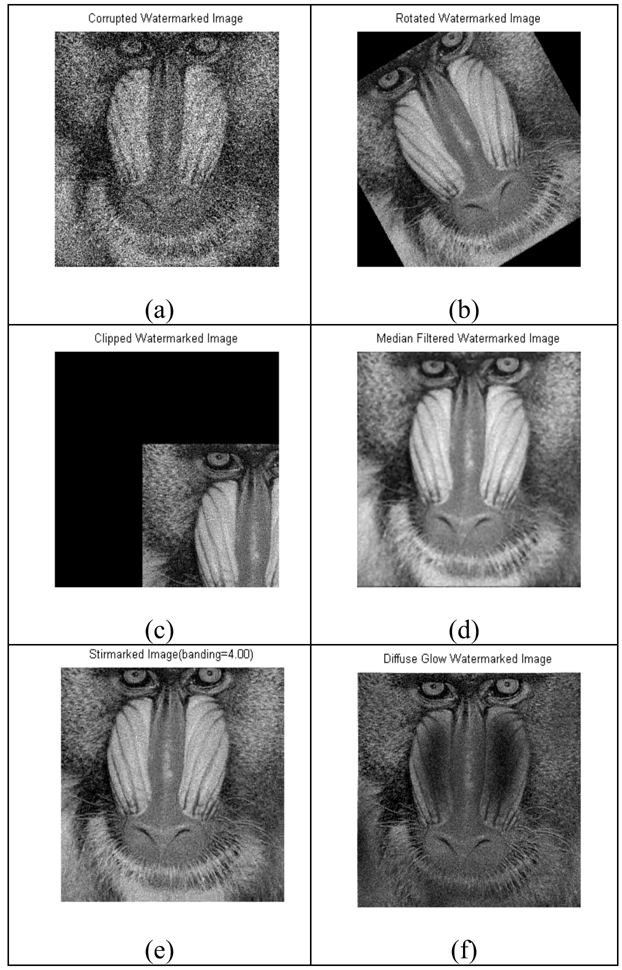

Fig. 6 (a) Corrupted watermarked image (b) rotated watermarked image (c) clipped watermarked image (d) median filtered watermarked image (e) stirmarked image (f) diffuse glow watermarked image

Noise values of white noise are adjusted in such a way that the noises at different psnr values are obtained. Table 1 tabulates bit error for different noise scale values. In Fig. 6 (a) displays corrupted watermarked image by white noise at psnr=15.7837 dB. Table 2 lists bit errors computed by applying different attacks. The attacks on watermarked image are shown in Fig. 6.

Table 1 Bit error for different scale values of the white noise

PSNR	Bit Error
132.1404	0.0%
121.0167	0.0%
98.4977	0.0%
57.4153	1.041%
33.8938	2.083%
22.1482	7.291%
15.7837	25%

Table 2 Bit error for different attacks

ATTACKS	Bit Error
Diffuse Glow	9.375%
Rotation	38.54%
Clipping	36.45%
Median Filtering	36.45%
Stirmark(banding=4.00)	37.50%

VI. CONCLUSIONS

In this work, we propose a new frequency-domain wavelet-based watermarking technique. A spread spectrum geometric watermark is embedded in the DFT domain. Furthermore, a second watermark is embedded in the DWT domain. The tests show good performances against common signal processing procedures such as noise addition, image compression, median filtering, diffuse glow as well as geometric transforms such as clipping and rotation. This method also tested with stirmark and watermark was detected with 37.50% bit error .The psnr of the output image is 32.7137dB. As shown in table 1, proposed algorithm was quite robust to noises. Further more bit error was computed with related to watermarked image in different attacks. Experimental results demonstrate that proposed technique was robust to signal processing techniques and geometric distortion.

REFERENCES

1. A. G. Bors and I. Pitas, "Image watermarking using DCT domain constraints," in Proc. IEEE Int. Conference on Image Processing, vol. 3, pp. 231–234, 1996.
2. R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in Proc. Int. Conference in Image Processing,vol. 2, pp. 86–90, 1994.
3. J. Ohnishi and K. Matsui, "Embedding a seal into a picture under orthogonal wavelet transform," in Proc. Int. Conference on Multimedia Computing and Systems, pp. 514–521, June 1996.
4. I. J. Cox, J. Killian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," Tech. Rep.95–10, NEC Research Institute, 1995.
5. I. Daubechies, *Ten Lectures on Wavelets*, Capital City Press, 1992.
6. A. N. Akansu and R. A. Haddad, *Multiresolution Signal Decomposition*, Academic Press, 1992
7. M. Vetterli and J. Kovacevic, *Wavelets and Subband Coding*, Prentice Hall, 1995.
8. C. T. Hsu and Ja-L. Wu,"Image Watermarking By Wavelet Decomposition",Academy of Information and Management Sciences Journal, Vol. 3, No. 1, pp. 70-86, 2000.
9. D. Kundur and D. Hatzinakos, "A robust digital image watermarking method using wavelet-based fusion," to appear in Proc. Int. Conference in Image Processing, 1997.
10. D. Kundur and D. Hatzinakos, "Digital Watermarking Based on Multiresolution Wavelet Data Fusion," Proc. IEEE, Special Issue on Intelligent Signal Processing, under review, 43 pages,1997.
11. J.J.K.O. Ruanaidh and T. Pun "Rotation, Scale and Translation Invariant Digital Image Watermarking", IEEE International Conference on Image Processing, pp. 536-539, Santa Barbara, October 1997.
12. Ioannis Pitas, Digital Image Processing Algorithms, Prentice Hall, 1993.