DWT Based Digital Watermarking Technique and its Robustness on Image Rotation, Scaling, JPEG compression, Cropping and Multiple Watermarking

S.M. Mohidul Islam, Rameswar Debnath, S.K. Alamgir Hossain

Department of CSE, Khulna University, Khulna, Bangladesh.
mohid_ku@yahoo.com, ramesward@gmail.com, hira82@gmail.com

ABSTRACT

We propose in this paper a Discrete Wavelet Transform (DWT) based digital image watermarking technique. For embedding process, we consider the watermark signal as a binary sequence which is embedded to the high (HL and HH) frequency band of the blue channel. For detecting process, the correlation between the high frequency band DWT coefficients of the watermarked image and the watermark signal is compared with the predefined threshold to determine whether the watermark is present or not. The experimental results show that the method is comparatively robust to several attacks such as rotation, scaling, JPEG compression, cropping, and multiple watermarking.

1. INTRODUCTION

The copyright of digital images in the internet can be easily violated by cropping and graphical modification. Some parts of an image such as the human face image can be cropped and applied to other images without permission. To protect the copyright, the digital image watermarking technique is applied. In watermarking the secret information called as watermark, is invisibly embedded into the host media. It is embedded permanently in an image and introduces invisible changes for the human vision that can be detected only by a computer program. The watermarks must be robust to distortions such as those caused by image processing algorithms. The watermark may become undetectable after intentional or unintentional image processing attacks. The watermark alterations should not decrease the image quality. A general watermarking framework for copyright protection has been presented in [1] and describes all these issues in detail.

Watermarking techniques can be categorized into two types (spatial or frequency domain) according to embedding processes. The advantages of embedding watermarks in the frequency domain over time domain is that the position of the watermark in time domain is sparsely spread, so that the intentional attempts to remove or destroy the watermark in time domain cannot be easily done. Due to some techniques in the frequency domain [2], [3] they required the original image. Among the methods which do not use the original image for watermark detection, Piva *et al.* [5] suggested adding the watermark to a larger number of DCT coefficients which need not be significant. A larger number of coefficients are here for a significant detector response as compared with the method in [2], since correlation is performed without subtracting out the original image.

In this paper, we propose an image watermarking technique based on DWT. In DWT the pixels when transformed are arranged from the most significant pixel to the least significant pixel i.e. DWT helps separate the image into parts (or spectral sub-bands) of differing importance. The features of our proposed technique are: (i) Add watermark to significant coefficients. (ii) Does not use the *original* image for watermark detection. (iii) Amount of watermark added is *adapted* to the image. (iv) Image sized watermark is not required (v) No explicit *visual masking* is required (This highly improves the detector response and becomes computationally *fast*).

In [8] the similar but DCT based technique is described and here we present the comparative performance of [8] and this proposed technique in section 3. In Section 2, the proposed DWT based technique is described and the conclusions are drawn in section 4.

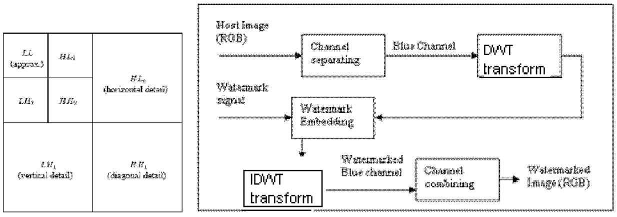
2. THE PROPOSED DWT BASED TECHNIQUE

The watermark is represented in binary form as $w'_{ij} \in \{0, 1\}$ for I, j = 1 to M where M is the number of bits in the message to be encoded. Here the value 0 represents black and 1 represents white value. The binary form of the message w' is then transformed to obtain the vector $w_{ij} \in \{1, -1\}$. The mapping 1→ -1 and 0 →1 is an extremely important step because it essentially enables us to replace the exclusive-OR operator used in finite field algebra with multiplication. One simple example where one can see this isomorphism at work is in considering the Hamming distance between two binary sequences which is the number of bits by which they differ. It is easy to show that this Hamming distance equals minus the correlation between the two sequences where the bits are replaced by ± 1 as described above.

Generally, the human visual system is least sensitive to the range of high frequency [4]. Among three channels of the RGB image, the blue channel has characteristic of the highest frequency range. Again, for high performance the blue channel is transformed into DWT domain and a watermark is embedded only from the high frequency band to the low frequency band of the blue channel of the host image. So the greater invisibility of the watermark in the watermarked image is achieved.

2.1 Embedding process

The binary watermark signal is first generated by pseudo random bit generator as described before. The proposed embedding method is shown in figure.1 (b). From the block diagram we see that, the three channels of RGB image are separated in channel separating stage and then only the blue channel is chosen to transform into DWT domain. However in case of grayscale image, it is transformed directly into DWT domain. Then the watermark is embedded from high frequency band to the low frequency band of that DWT domain and then it is transformed into inverse DWT domain. At this stage, for grayscale image we get the watermarked image but for RGB image we get the watermarked blue channel which is then combined to other two channels in channel combining stage to obtain the watermarked image.



(a) (b)

Figure 1: (a) Arrangement of frequency distribution after taking DWT and (b) block diagram of watermark embedding process

The relation of embedding process is given in (3) as used in [6].

$$F'_{i,j} = F_{i,j} + K|F_{i,j}|w_{i,j} \quad (3)$$

Where i and j ranges over all coefficients in the DWT domain $F_{i,j}$ and $F'_{i,j}$ denote the DWT coefficient of the blue channel of the original image and the watermarked image respectively, $w_{i,j}$ is the watermark signal and k is the scaling parameter which is described in section 3. In the case of multiple watermarking, the equation (3) is repeated as

$$F''_{i,j} = F'_{i,j} + K|F'_{i,j}|w'_{i,j} \quad 3(a_1)$$

$$F'''_{i,j} = F''_{i,j} + K|F''_{i,j}|w''_{i,j} \quad 3(a_2)$$

$$\vdots$$

$$F^{n}_{i,j} = F^{n-1}_{i,j} + K|F^{n-1}_{i,j}|w^{n-1}_{i,j} \quad 3(a_n)$$

Where the equations $3(a_1)$, $3(a_2)$ and $3(a_n)$ denote the watermarking in two times, three times and n times respectively. Exhaustive experiment is required to know the value of n of multiple watermarking. In the section 3.5 we have shown the result of watermarking in two times.

2.2 Detecting process

In the detection process, we require a watermarked image (NxN) and watermark signal (N_1xN_1, N_1<=N) and the detector detect whether the watermark is present or not in the watermarked image. At first apply DWT transform on the blue channel of the given watermarked image and determine the coefficients $F'_{i,j}$ (i, j = 1, 2 … N).

Now select N1xN1 coefficients from the high frequency part and compute the average T which we consider as a threshold.

$$T = \frac{1}{N_1^2} \sum_{i=N-N1}^{N} \sum_{j=N-N1}^{N} |F'_{i,j}| \quad (4)$$

Now determine the correlation C_0 between the selected DWT coefficients $F'_{i,j}$ and the provided watermark $w_{i,j}$ and compare C_0 with T.

$$C_0 = \frac{1}{N_1^2} \sum_{i=N-N1}^{N} \sum_{j=N-N1}^{N} F'_{i,j} w_{i,j} \quad (5)$$

If $C_0 > T$ then we can decide the provided watermark is detected , otherwise not. As $F'_{i,j}$ may be negative and $w_{i,j}$ has value in the range zero to one, so *T always greater than C_0.* As a result a scaling parameter is required. So the adjusted threshold is (6)

$$T = \frac{\alpha}{N_1^2} \sum_{i=N-N1}^{N} \sum_{j=N-N1}^{N} F'_{i,j} \quad (6)$$

The proposed detection process is shown in figure 2. From the block diagram we see that the watermarked image (For RGB image, the blue channel of watermarked image) is first transformed into DWT domain. Then from the selected coefficients, the threshold is calculated. In the mean time, from the selected coefficients and the provided watermark signal the correlation is calculated. The value of threshold and correlation is used to make the decision whether the watermark is detected or not.

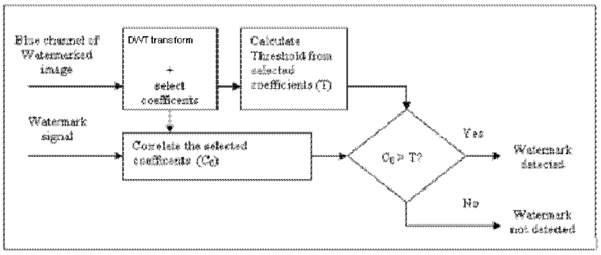

Blue channel of Watermarked image
DWT transform + select coefficents
Calculate Threshold from selected coefficients (T)
Watermark signal
Correlate the selected coefficents (C_0)
$C_0 > T$?
Yes
Watermark detected
No
Watermark not detected

Figure 2: Block diagram of watermark detection process

3. EXPERIMENTAL RESULTS

In this section, we illustrate and evaluate the performance of the proposed technique against rotation, scaling, cropping, JPEG compression and other attacks. We also show the comparative study with similar but DCT based technique [8]. Our proposed technique can be applied to both RGB and grayscale image. Here we present the experimental results using the standard image *"Lena"* (128×128 pixels, RGB) shown in Figure 3(b). Figure 3(a) shows a sample watermark signal (128×128 pixels, Black & White) and Figure 3(c) shows the corresponding watermarked image after embedding.

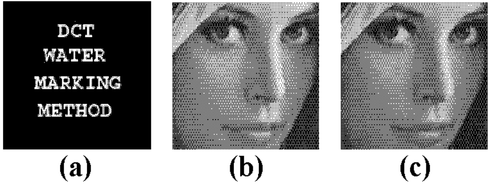


Figure 3: (a) Sample watermark signal (b) Host image (c) watermarked image

3.1 Determining the scaling parameter *K*

In the proposed method the scaling parameter (*K*) is an important factor. The larger the value of *K* the more the image quality is degraded. But small value of *K* degrades the detector response. So the value of *K* must be in a reasonable range for successful watermark detection. Table 1 shows the *Mean of luminance*, *Std. Deviation of luminance*, *Median of luminance* of original *Lena* image and the watermarked image for different values of *K*. Luminance is a measure of the amount of energy an observer perceives from a light source. High luminance can be detected to alteration by the human eyes less than at the lower luminance pixel. From the Table 1 we see that, the value for *K* = 0.1, the image quality remains in the acceptable range. For this reason for various experiments we use this value of *K*.

Table 1: Characteristics of original *Lena* and the watermarked image for different values of *K*

	Original *Lena*	**K = 0.1**	K= 0.2	K = 0.4
Mean of luminance	133.6	**133.39**	133.81	143.9
Std. Deviation of luminance	43.04	**43.02**	42.47	41.89
Median of luminance	137	**137**	136	147

3.2 Scaling, JPEG Compression, Cropping and Rotation attack

We perform several attacks (Scaling, JPEG compression, Cropping and Rotation) to the watermarked image using different scales listed in the column *Scale*, compression ratio listed in the column compression ratio, cropping attack listed in the column crop and rotating angle listed in the column angle of Table 2, 3, 4, 5 respectively.

Table 2: Scaling

Scale	Threshold (DCT)	Correlation (DCT)	Threshold (DWT)	Correlation (DWT)
0.5	0.4688	0.5812	0.2015	0.3545
0.6	0.4697	0.6910	0.2150	0.3930
0.7	0.4700	0.8312	0.2325	0.4125
0.8	0.4709	0.9065	0.2525	0.4155
1	0.4713	0.9194	0.2709	0.4172
1.1	0.5810	0.9291	0.2789	0.4212
1.2	0.6132	0.9361	0.2880	0.4310
1.3	0.8110	0.9390	0.3010	0.4425
1.4	**0.9900**	**0.9410**	0.3515	0.4410
1.5	**0.5720**	**0.9412**	0.4525	0.4525
1.6	**0.5900**	**0.9415**	**0.4629**	**0.4590**

From the table 2 we see that, the watermark is detected when the scale change is less than 1.6 whereas in DCT based method of [8] becomes inaccurate when the scale change(s) is 1.4.

Table 3: JPEG Compression

Compression ratio	Threshold (DCT)	Correlation (DCT)	Threshold (DWT)	Correlation (DWT)
No Compression	0.4713	0.9494	0.2709	0.4172
10%	0.4915	0.9242	0.2890	0.4172
20%	0.5110	0.9307	0.3010	0.4180
30%	0.5321	0.9599	0.3210	0.4195
40%	0.5731	0.9310	0.3550	0.4210
50%	0.6120	0.9488	0.3610	0.4250
60%	**0.7875**	**0.7845**	0.3815	0.4310
70%	**0.8214**	**0.7810**	0.4055	0.4330
80%	**0.8657**	**0.7521**	**0.4530**	**0.4450**

From the table 3 we see that the method performs well against JPEG up to compression ratio 70% this performance is better than the method in DCT based method of [8] in which it is 50%.

From the table 4 we see that, when the image is cropped by 32×32 the correlation value is less than threshold value, so the watermark cannot be detected. If the cropping is in a reasonable range, few of the image part is lost, so it can be detected by our proposed method, this cropping size is larger than in DCT based method of [8] in which it is 80 × 80.

Table 4: Cropping

Crop	Threshold (DCT)	Correlation (DCT)	Threshold (DWT)	Correlation (DWT)
128 × 128	0.4713	0.9494	0.2709	0.4172
120 × 120	0.4821	0.9043	0.2825	0.4185
100 × 100	0.4910	0.8627	0.3255	0.4190
80 × 80	**0.7825**	**0.7590**	0.3525	0.4270
64 × 64	**0.8150**	**0.7221**	0.3956	0.4299
32 × 32	**0.8351**	**0.7045**	**0.4525**	**0.4355**

Table 5: Rotation

Angle	Threshold (DCT)	Correlation (DCT)	Threshold (DWT)	Correlation (DWT)
350^0	**0.4990**	**0.4840**	**0.4419**	**0.4392**
360^0	0.4723	0.5761	0.3919	0.4282
370^0	0.4950	0.6730	0.3829	0.4252
375^0	0.4760	0.8455	0.3719	0.4182
0^0	0.4713	0.9494	0.2709	0.4172
5^0	0.4770	0.8415	0.3709	0.4192
10^0	0.4780	0.6710	0.3809	0.4242
20^0	0.4940	0.5741	0.3909	0.4292
30^0	**0.4980**	**0.4810**	**0.4409**	**0.4372**

From the table 5 we see that the method performs well when the rotated angle is up to 20^0. However, it becomes inaccurate when the rotated angle is greater than 360^0. In DCT based method of [8] it is 10^0 and 370^0 respectively.

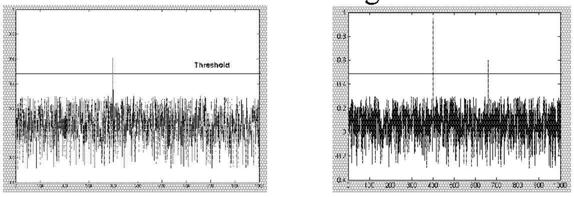
In all kinds of attack described above, our method also shows more robust result than [7].

3.4 Performance on random watermark test

We have performed our proposed watermarking system on different watermarks (shown in Figure 4(a)); here a watermarked image and 1000 watermark signal are used for watermark detection. Here one watermark signal is the same as the embedded watermark signal among the 1000 signals. In the figure 4(a), the X-axis represents 1000 randomly generated watermark signal with the embedded signal and the Y-axis shows the corresponding detector results. From Figure 4(a) we see that only watermark number 400 crosses the predetermine threshold value, which was the actual watermark that was embedded.

3.5 Performance on Multiple watermarks

Some applications require that more than one watermark is inserted in the image. To test the performance of our proposed technique, the original image was watermarked with two different watermarks. Figure 4(b) shows the detector response, which indicates the presence of all the two watermarks embedded in the image.



(a) (b)

Figure 4: Detector response (a) to 1000 randomly generated watermarks. Only watermark number 400 detected (b) on two different watermarks

We have performed the similar experiments discussed above to other test images and we obtained the similar results. From the experimental results, we can conclude that our method is robust to some attacks such as JPEG compression, Scaling and cropping compare to existing method [7][8].

4. CONCLUSIONS

This paper presents a digital image watermarking method based on DWT applied to the blue channel of the *RGB* image. The main goal of the proposed method is to improve the performance of the digital image watermarking process and to compare with the existing methods [7][8].

REFERENCES

[1] G. Voyatzis and I. Pitas, "Protecting digital-image copyrights: a framework," *IEEE Comput. Graph. Applicat.*, vol. 19, pp. 18–24, January/February 1999.

[2] I. J. Cox, J. Kilian, F.T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. on Image Processing,* Vol. 6, pp. 1673-1687, December 1997.

[3] H. Inoue, A. Miyazaki, A. Yamamoto and T. Katsura, "A digital watermarking based on the wavelet transform and its robustness on image compression and transformation," *IEICE Trans. Fundamentals,* Vol. E82-A, No.1. pp. 1-9, January 1999.

[4] R.C. Gonzalez and R.E. Woods, "Digital image processing," *Wesley*, pp. 21-25, 191-195, 1993.

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

[6] T. Tachibana, M. Fujiyoshi and H. Kiya, "An image quality guaranteed watermarking scheme with spreading spectrum of watermark,"*ISCIT*, Sapporo, Japan, 2004.

[7] S. Pereira, J.K. Ruanaidh and F. Deguillaume, "Template based recovery of Fourier-based watermarks using log-polar and log-log maps", *IEEE Int. Conf. on Multimedia computing an Systems*, Florence, Italy, June, 1999.

[8] *S.K. Alamgir Hossain, S.M. Mohidul Islam, Rameswar* Debnath, "Improved Performance DCT Based Digital Image Watermarking Technique", ICCIT, Dhaka, Bangladesh, 2006.