A CASCADE DWT-DCT BASED DIGITAL WATERMARKING SCHEME

Serkan EMEK[1], Melih PAZARCI[2]

[1] YTÜ FBE Elektronik ve Haberleşme Müh., Yıldız, İstanbul, Phone: +90-212-326 0309, serkan.emek@digiturk.tv

[2] İTÜ Elektrik-Elektronik Fakültesi, Maslak, 34469 İstanbul, Phone: +90-212-285 3504, eepazarc@ieee.org,

ABSTRACT

Many watermark algorithms exist for the frequency domain using either the DCT or the DWT. In this paper, we propose a new watermark algorithm using the DWT prior to the DCT to provide better imperceptibility in harmony with the human visual system, and higher robustness against signal processing attacks. Experimental evaluations show that the technique performs well.

1. INTRODUCTION

There has been an explosion in the use and distribution of multimedia content because of the rapid development of information technologies for multimedia services. The success of the Internet, cost-effective and popular digital recording and storage devices, and the promise of higher bandwidth and quality of services for both wired and wireless networks have made it possible to easily create, replicate, transmit, and distribute digital content. Consequently, this has led to a strong demand for reliable and secure copyright protection techniques for multimedia data. Digital watermarking is a technique to embed generally invisible or inaudible data within multimedia content. Watermarked content contains copyright data. The hidden data for such purposes is called a watermark, and the content may be an image, audio or any other type of media in any of the available formats [1].

Each watermarking application has its own specific requirements, so there is no particular set of requirements to be met by all watermarking techniques, but some general principles are applicable in most cases.

- Imperceptibility: an embedded watermark is truly imperceptible if a user cannot distinguish the original from the watermarked version.
- Payload: the amount of information that can be stored in a watermark depends on the application. Generally 60 to 70 bits of information should be embedded in the host data, i.e., the image, the video frame or the audio fragment.
- Robustness: it should not be possible to remove or alter the watermark without sufficient degradation of the perceptual quality of the host data so as to render it unusable.
- Security: according to Kerckhoff's assumption, the security of the encryption techniques must lie in the choice of a key. This assumption is also valid for watermarking techniques.

Currently watermark techniques in the transform domain are more popular than those in the spatial domain. DCT based methods have been the most widely used among the transform domain methods. Furthermore wavelet based techniques have also been used for watermarking purposes. Embedding a watermark in the spatial domain scatters the information to be embedded making it hardly detectable. These techniques are advantageous in their resistance to cropping and translation, but they are weak to attacks like noise and compression. The most straightforward way to add a watermark to an image in the spatial domain is to add a pseudorandom noise pattern to the luminance values of its pixels. Several methods are based on this principle [3-5]. Block-based DCT is widely used for image and video compression. Using the DCT, an image is easily split up into pseudo frequency bands, and the watermark can be embedded in the significant middle band frequencies. The sensitivity of the human visual system (HVS) to the DCT based image processing errors has been extensively studied [6-9]. These results can be used for predicting and minimizing the visual impact of the distortion caused by watermarking. The robustness of a watermark can be improved by increasing the energy of the watermark. By exploiting the properties of the HVS, this energy can be increased locally so that the human eye will not notice it. From this point of view the discrete wavelet transform (DWT) is a very attractive transform because it can be used as a computationally efficient version of the frequency models for the HVS. Furthermore, DWT based image and video compression is included in image and video compression standards, such as JPEG2000 and MPEG4. Current methods apply the basic techniques to the high resolution DWT bands [10-13]. Compared to the spatial techniques, the frequency domain watermarking techniques are relatively robust to noise, image processing and compression.

In this work, we describe a DWT-DCT based digital watermarking technique. Rather than inserting the watermark to the DCT mid-frequency coefficients, we use a DWT beforehand to provide higher robustness and imperceptibility. The robustness is improved by the achieved ability to increase the energy of the watermark. The energy is increased locally by exploiting the properties of the HVS such that the human eye will not notice it. Furthermore imperceptibility is also improved due to the DWT.

2. WATERMARK EMBEDDING

The main purpose for inserting the watermark in the transform domain is the resulting dispersion of the watermark in the spatial domain, hence it becomes very difficult to remove the watermark from the image. We start the watermarking process by applying the DWT to the original image, and subsequently applying the DCT to the DWT sub-bands. This technique can be generalized by applying it to I-frames for MPEG-2 video streams. In our technique, we have combined the DCT with the DWT to provide the embedded watermark higher imperceptibility yet more energy. The watermark embedding in the DWT domain is implemented through the following steps.

1- By using the Daubechies bi-orthogonal wavelet filters, we apply a four level DWT to the input image S*(x,y)*, generating 12 subbands of high frequency (*Vi, Hi, Di i=1..4*) and one low frequency subband (*A4*), where *V*, *H*, and *D* denote the vertical, horizontal and diagonal high frequency subbands, respectively, and *A* is the low frequency approximation subband. A two level DWT subband decomposition is shown in Fig. 1. The watermark is embedded in the *V* or *H* subband of a selected level. *A* and *D* bands are not preferred due to perceptibility and robustness concerns, respectively.

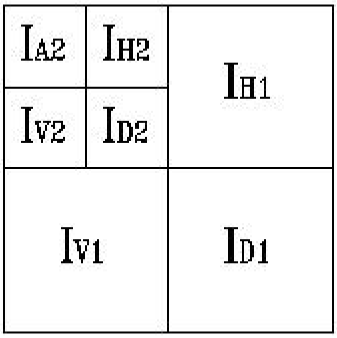


Fig. 1. DWT subband decomposition process for two levels

2- Prior to embedding the watermark in a subband, we apply the DCT to the particular subband in order to increase robustness against attacks like compression, cropping, rotating, etc.

$$I_{V,H}(k,l) = DCT\{J(u,v), J \in (V_n, H_n), 1 \le n \le 4\} \qquad (1)$$

3- A uniformly distributed zero-mean pseudorandom 2-D watermark, *W(u,v)*, is created using a seed value. The watermark values are in [-0.5, 0.5].

4- The 2-D watermark *W(u,v)* is embedded with a gain factor *K* in the *V* or *H* subband of the DWT of the input image after applying DCT to the particular DWT subband in 8x8 blocks. Furthermore, the watermark is not applied to all block DCT values, but is applied only to the mid-frequency DCT coefficients using a 2-D mask function *f( )* shown in Fig. 2.

$$I_{W(V,H)}(k,l) = I_{V,H}(k,l) + K.f(k,l)W(k,l) \qquad (2)$$

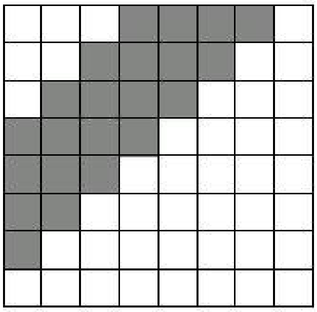


Fig. 2.DCT coefficient mask *f(k , l)* for watermark

5- To increase the efficiency of the watermark embedding, the process can be made image dependent by modulating the DWT coefficients of *V* or *H* bands as follows:

$$I_{W(V,H)}(k,l) = I_{V,H}(k,l)\left[1 + K.f(k,l)W(k,l)\right] \quad (3)$$

3. WATERMARK DETECTION

In our technique, the original input image is not needed at the watermark detector. The watermarked image, the gain factor, and the seed value for creating the watermark are sufficient for the detection. The detection is done on the DCT of the selected DWT subband in blocks using the same mask function. Fig.3 illustrates the watermark detection process:

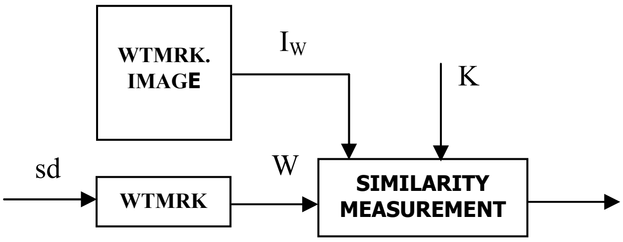


Fig. 3. Block diagram of the detection process (sd : seed)

We use two criteria for detection: A first criterion is similarity comparison result between *H* and *V* components for every 8x8 block. Second one is total average similarity measurement for every level. The watermark detection in the DWT domain is implemented through the following steps.

1. Similarity measurement is calculated between $I_{W(V,H)}(k,l)$ and $I_{W(V,H)}(k,l)*$, i.e., the product of the watermarked $I_{W(V,H)}(k,l)$ image and the watermark *W(k.l)*.

$$\begin{aligned}
&I_{W(V,H)}(k,l) = DCT\{J_W(u,v), J_W \in (V_n, H_n), 1 \le n \le 4\} \\
&I_{W(V,H)}(k,l)* = I_{W(V,H)}(k,l)\ \ W(k,l) \\
&E\left[I_{W(V,H)}\ I^*_{W(V,H)}\right] = E\left[\left(I_{V,H} + kI_{V,H}W\right)^2 W\right] \\
&sm_W = E\left[I_{V,H}{}^2 W\right] + 2K\,E\left[I_{V,H}{}^2 W^2\right] + K^2 E\left[I_{V,H}{}^2 W^3\right]
\end{aligned} \qquad (4)$$

using (3). A similarity measurement is calculated for each 8x8 DCT block of *V* and *H* subbands, as follows.

$$\begin{aligned}
&sm_V = E\left[I_{W(V)}(k,l)\ I^*_{W(V)}(k,l)\right], \\
&sm_H = E\left[I_{W(H)}(k,l)\ I^*_{W(H)}(k,l)\right] \\
&sm_V > sm_H \quad \rightarrow \quad cv = cv + 1, \\
&sm_H > sm_V \quad \rightarrow \quad ch = ch + 1
\end{aligned} \qquad (5)$$

2. If there is no watermark on the component (*K*=0), the similarity measurements become:

$$sm = E\left[I_{V,H}\ I^*_{V,H}\right] = E\left[I_{V,H}\ W\ I_{V,H}\right] = E\left[I_{V,H}{}^2 W\right] \qquad (6)$$

If we assume that the input data and the watermark are not correlated, and since the watermark has a zero mean value, (4) and (6) may be written as:

$$\begin{aligned}
&sm_W = 2K\,E\left[I_{V,H}{}^2 W^2\right] + K^2 E\left[I_{V,H}{}^2 W^3\right] \\
&sm = 0
\end{aligned} \qquad (7)$$

where $I_{V,H}(k,l)$ is computed by:

$$I_{V,H}(k,l) = I_{W(V,H)}(k,l) / \left[1 + KW(k,l)\right] \qquad (8)$$

The threshold values, *th*, are chosen between *sm* and sm_W

$$sm < th < sm_W . \qquad (9)$$

3. Average values of similarity measurements and thresholds of blocks for H and V components on a given level are calculated as:

$$\begin{aligned} &sm_{MH} = average(sm_H), \quad sm_{MV} = average(sm_V), \\ &th_{MH} = average(th_H), \quad th_{MV} = average(th_V). \end{aligned} \qquad (10)$$

where the averaging is over all 8x8 blocks.

4. For the detection decision, we use:

$$\begin{array}{l} sm_{MH} > th_{MH} \;\&\; sm_{MV} < th_{MV} \;\&\; ch > cv \rightarrow \; H \; watermarked \\ sm_{MV} > th_{MV} \;\&\; sm_{MH} < th_{MH} \;\&\; cv > ch \rightarrow \; V \; watermarked \\ sm_{MH} > th_{MH} \;\&\; sm_{MV} > th_{MV} \;\&\; ch \cong cv \rightarrow \; FalseDetection \\ sm_{MH} < th_{MH} \;\&\; sm_{MV} < th_{MV} \;\&\; ch \cong cv \rightarrow \; NoWatermark \end{array} \qquad (11)$$

This process is applied for every level, and the watermark embedding level is determined by the highest *ch/cv* ratio for the *H* component, and *cv/ch* ratio for the *V* component.

4. PERFORMANCE CRITERIA

In the evaluation of the performance of the watermarking scheme, we use the normalized mean square error *nMSE* between *I(u,v)*, *I_W(u,v)*, the original and watermarked images, respectively, and peak signal to noise ratio *PSNR*. The image pixels are assumed to be 8-bits to give a maximum pixel value of 255.

We have used the Stirmark 3.1 benchmark tools [14] for the evaluation of the robustness of the watermarking scheme. We have applied a multitude of available attacks using the Stirmark 3.1 benchmark and then attempted to detect the watermark:

5. EXPERIMENTAL RESULTS

The DCT-DWT based watermark technique has been applied to several images, including the 512x512 sizes of Baboon, Lenna, Boat, and Peppers which are well known in the literature. In these experiments, we have chosen a gain factor between 0.5 and 5, and used random seeds for creating the watermark matrices. Example watermarked images are shown in Figure 4; the embedded watermarks cause imperceptible distortion at levels that provide reliable detection. In Table 1, computed *nMSE* and *nPSNR* values for different DWT level and gain factors for Lenna are given.

Table 1. *nMSE* and *nPSNR* values for Lena

level	gain fac.	subband	seed	nMSE	nPSNR
1	3.0	H	654	6.06E-05	42.12
1	3.0	V	654	9.09E-05	40.41
2	2.0	H	654	4.11E-05	43.86
2	2.0	V	654	2.52E-05	46.01
3	1.0	H	654	7.75E-07	61.11
3	1.0	V	654	2.97E-05	45.27
4	1.0	H	654	2.82E-05	45.50
4	1.0	V	654	1.40E-04	38.54

In Table 2, the Stirmark benchmark tool results are shown. In the table, “1” shows that the watermark has been detected from the attacked image successfully, “0/1” indicates that watermark has been detected in some cases, and “0” shows that watermark has not been detected. We used the [1 2 1 ; 2 4 2 ; 1 2 1] filter for sharpening, 2x2, 3x3 and 4x4 sizes of median filtering, and 3x3 Gauss filter for attacking the watermarked image. After each filtering, the watermark is detected from the attacked image on every level and subband. We applied JPEG compression with quality factors: 20, 25, 30, 35, 40, 50, 60, 70, 80, 90, frequency mode Laplacian removal, and random geometric distortion. Our technique is also successful against these kinds of attack.

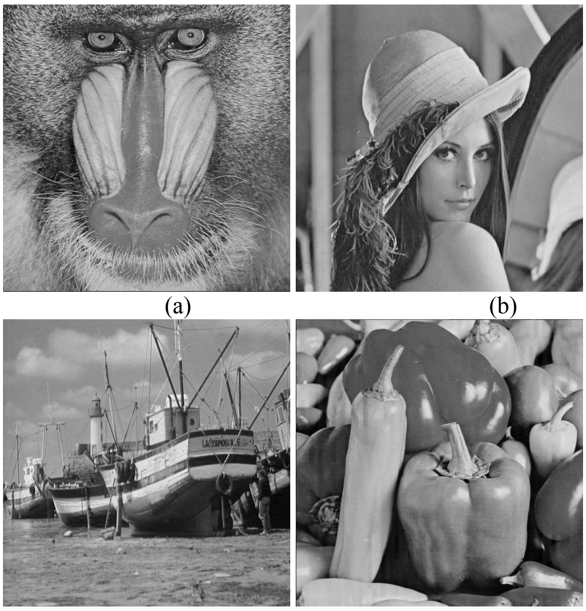
We have applied rotation with ±2º, ±1º, ±0.75º, ±0.5º, ±0.25º, 5º, 10º, 15º, 30º, 45º, 90º, rotation by a small angle and cropping, and rotation by a small angle followed by cropping and rescaling to keep the original size of the image. We have applied rotation with ±2º, ±1º, ±0.75º, ±0.5º, ±0.25º, 5º, 10º, 15º, 30º, 45º, 90º, rotation by a small angle and cropping, and rotation by a small angle followed by cropping and rescaling to keep the original size of the image. The DCT-DWT based technique is successful for 15º and less of rotation, and 5º and less of rotation and cropping, and rotation, cropping and rescaling. Fig. 5 shows the 15º rotated Baboon image; the watermark on this image is detected successfully. In some of the attacks that give a “0/1” result in Table 2, the value of the attacked image is arguable; when such an image is a frame of a video sequence, the image is no longer valuable in our opinion.

Table 2. Detection results for attacked watermarked images

Attack	Lenna	Baboon	Boat	Peppers
sharpening	1	1	1	1
Median filtering	1	1	1	1
Gauss filtering	1	1	1	1
JPEG compression	1	1	1	1
FLMR	1	1	1	1
random geometric distortion	1	1	1	1
rotation	1/0	1/0	1/0	1/0
rotation by a small angle and cropping	1/0	1/0	1/0	1/0
rotation by a small angle followed by cropping and rescaling to keep the original size of the image	1/0	1/0	1/0	1/0
scaling	1/0	1/0	1/0	1/0
symmetric and asymmetric line and column removal	1/0	1/0	1/0	1/0
symmetric and asymmetric shearing	1/0	1/0	1/0	1/0
general linear geometric transformation	1/0	1/0	1/0	1/0
centered cropping	0	0	0	0

We have applied rotation with ±2º, ±1º, ±0.75º, ±0.5º, ±0.25º, 5º, 10º, 15º, 30º, 45º, 90º, rotation by a small angle and cropping, and rotation by a small angle followed by cropping and rescaling to keep the original size of the image. The DCT-DWT based technique is successful for 15º and less of rotation, and 5º and less of rotation and cropping, and rotation, cropping and rescaling. Fig. 5 shows the 15º rotated Baboon image; the watermark on this image is detected successfully. In some of the attacks that give a "0/1" result in Table 2, the value of the attacked image is arguable; when such an image is a frame of a video sequence, the image is no longer valuable in our opinion. Similarly, when the watermarked image is scaled by factors of 0.5, 0.75, 0.9, 1.1, 1.5, 2, the technique is successful only for small changes in the attack factor (with respect to 1), but it has failed for larger deviations in the attack scale factor. It has also failed for centered cropping.

This technique may be extended to video sequences by applying to individual frames. A video version of this technique where the described procedure is applied to I-frames of MPEG-2 sequences has also been developed.



(a) (b)

(c) (d)

Fig. 4. Watermarked images (*seed* =654) (a) Baboon (*level*=1, *K*=1.70, *subband*=H, *nMSE*=8.81E-5, *nPSNR*=40.55 dB), (b) Lenna (*level*=2, *K*=2.0, *subband*=V, *nMSE*=2.52E-5, *nPSNR*=46.01 dB), (c) Boat (*level*=3, *K*=1.70, *subband*=H, *nMSE*=1.06E-4, *nPSNR*=39.76 dB), (d) Peppers (*level*=4, *K*=1.0, *subband*=V, *nMSE*=1.54E-4, *nPSNR*=38.14 dB)

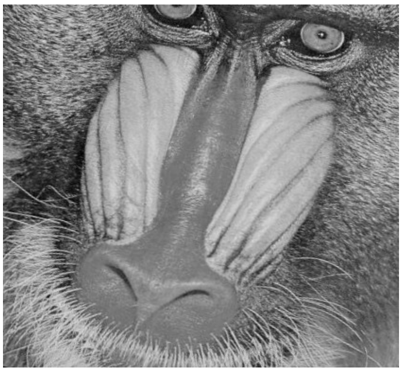


Fig. 5. 15º rotated watermarked Baboon.

6. CONCLUSION

The DWT/DCT combined technique provides better imperceptibility and higher robustness against attacks, at the cost of the DWT, compared to DCT or DWT only schemes. Performance has been verified through testing. The technique has also been extended to mpeg video sequences successfully; the video work will be described elsewhere.

7. REFERENCES

1. G.C. Langelaar, I. Setyawan, R.L. Lagendijk. "Watermarking Digital Image and Video Data", IEEE Signal Processing Magazine, Sept 2000, pp. 20-46.
2. C.J. Podilhuck, E.J. Delp. "Digital Watermarking: Algorithms and Applications" IEEE Signal Processing Magazine, July 2001, pp. 33-46.
3. M.D. Swanson, B. Zhu, and A. H. Tewhik, "Robust data hiding in images" in Proc. IEEE Digital signal processing Workshop, Loen, Norway, Sept. 1996, pp 37-40.
4. R.B Wolfrang, and E.J. Delp. "A Watermark for Digital Images" in Proc. Int. Conf. Image Processing, vol 3, Lausanne, Switzerland, Sept. 1996, pp. 219-222.
5. I. Pitas and T.H. Kaskalis, "Applying Signatures on Digital Images" in Proc. ICIP'96, IEEE Int. Conf. Image Processing vol.3,Lausanne, Switzerland, Sept. 1996, pp. 215-218.
6. I. Cox, J. Killian, T. Leighton, an T. Shamoon, "Secure Spread Spectrum Watermarking for Images, Audio and Video", in Proc. 1996 Int. conf. Image Processing vol.3 Lausanne, Switzerland, Sept 1996, pp. 243-246.
7. I. Cox, J. Killian, T. Leighton, an T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", IEEE Trans. Image Processing, vol.6, Dec1997, pp.1673 -1687.
8. A. Piva, M. Barni, F. Bartolini, and V. Capellini, "DCT based Watermark Recovering without Resorting to the Uncorrupted Original Image", in , IEEE Int. Conf. Image Processing, Santa Barbara, CA, Oct 1997, pp 520-527.
9. J.R.Hernandez, M. Amado, F.P.Gonzalez "DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure", IEEE Trans. on Image Processing, vol. 9, no:1, Jan 2000 pp 55-68.
10. X.G. Xia, C.G. Boncelet, and G.R. Aree, "A Multiresolution Watermark for Digital Images", in IEEE Int. Conf. Image Processing, Santa Barbara, CA, Oct. 1997, pp. 548-551.
11. C. T. Hsu and J.L. Wu, "Multiresolution Watermarking for Digital Images" IEEE Trans. CAS II: Analog and Digital signal Processing , vol. 45, no:8, 1998, pp. 1097-1101.
12. W. Zhu, Z. Xiong, and Y. Q. Zhang, "Multiresolution Watermarking for Images and Video: A Unified Approach", Proc. IEEE Int. Conf. on Im. Proc. vol. 1, 1997, pp. 448-465.
13. M. Ejima, A. Miyazaki, "A Wavelet-based Watermarking for Digital Images and Video", IEEE Proceedings. 2000, vol 3 , 2000, pp 678 -681.
14. M. Kutter, F.A. Petitcolas, "A fair benchmark for Image Watermarking Systems", 11th Annual Symposium on Electronic Imaging, IS&T/SPIE, pp 23-29, Jan 1999.