MULTIPLE EMBEDDING IN WAVELET SUBBANDS FOR ROBUST IMAGE WATERMARKING

Corina Nafornita[1] and Monica Borda[2]

[1]"Politehnica" University of Timisoara, Communications Dept.,
Bd. Parvan 2, 300223 Timisoara, ROMANIA, corina.nafornita@etc.utt.ro
[2]Technical University of Cluj-Napoca, Communications Dept.,
Cluj-Napoca, ROMANIA, Monica.Borda@com.utcluj.ro

ABSTRACT

We propose a robust watermarking method for still images that embeds the binary watermark into the detail subbands of the image wavelet transform. The perceptually significant coefficients are selected for each subband using a different threshold. For greater invisibility of the mark, the approximation subband is left unmodified. The watermark is embedded several times in each subband to achieve robustness. We test the performance against different types of attacks (lossy compression, AWGN, scaling, cropping, intensity adjustment and filtering) and compare it with a frequency-based watermarking method.

Keywords: multiple embedding, watermarking, copyright protection, discrete wavelet transform

1. INTRODUCTION

In the last decade there has been an enormous growth in the transmission of digital multimedia content over the Internet. Illegal copies of movies, music and images without quality loss have spread around the globe, leaving the copyright holders and the entertainment industry with serious financial losses. Protection of multimedia can be made through encryption and watermarking. Encryption makes the multimedia data unintelligible, therefore protecting it in transmission over insecure channels, while watermarking embeds into the host data in some invisible way a signal called watermark that is supposed to identify the owner [1]. Proposed or actual watermarking applications are broadcast monitoring, owner identification, proof of ownership, transaction tracking, content authentication, copy control, and device control. Important properties of an image watermarking system include perceptual transparency, robustness, and data hiding capacity [2]. The watermarking process should not degrade the image significantly. Robustness is the resistance of the mark against intentional or unintentional attacks like AWGN, filtering, lossy compression, scaling, cropping [2-3]. Data hiding capacity refers to the amount of information that can be embedded into the original cover work without causing serious distortions. There are several criteria that can be used to classify watermarking systems. Some of those are:

- The *selection of the locations* where the mark is embedded: using human visual models, or a randomly generated key,
- The *watermarking domain*: spatial domain [4], where the pixels are directly altered, or transform domain. Popular transforms are the Discrete Cosine Transform (DCT) [5], the Discrete Wavelet Transform (DWT) [6-11, 19], and the Discrete Fourier Transform (DFT) [12] although recent papers propose use of the Fourier-Mellin Transform [13], the Complex Wavelet Transform (CWT) [14], or Ridgelet Transform [15],
- *Encoding of payload*: using spread spectrum (SS) techniques [5] and/or error correction codes (ECC) [16, 17, 21],
- *Formation of the watermarked signal*: additive [5] or quantization-based [18, 19],
- The *watermark decoder*: blind (the cover work is not known at the decoder, only the secret key is used), semi-blind (using the watermarked data and the secret key) or non-blind (using the cover work and the secret key).

This paper is organized as follows. Section 2 presents some of the previous work. Section 3 describes the proposed non-blind watermarking system for images in the wavelet domain, for copyright protection purposes. Section 4 contains simulation results. Finally we draw some conclusions.

2. PREVIOUS WORK

Several papers deal with copyright protection for images. Most of these argue that the mark should be embedded in some transform domain selecting only perceptually significant coefficients (PSCs), because those are the most likely to survive compression [5-8].

Cox *et al* [5] embed a continuous watermark in the largest 1000 DCT coefficients of the original image, except the DC coefficient, thus spreading its energy on several bins of frequency. Detection is made using the similarity between the two watermarks.

Xia *et al* [6] insert several watermarks in the DWT domain in each detail image, except the approximation subband, suggesting that the detection could be done hierarchically, computing crosscorrelations of the water-

mark and the difference between the two images for each resolution level.

Other authors [7, 8] embed the watermark into perceptually significant coefficients for each subband of the DWT using statistical properties of the human visual system (HVS) and of the original image.

This paper proposes a technique that embeds the watermark into the wavelet domain, into perceptually significant coefficient using subband adaptive thresholding. The watermark is embedded repeatedly into the detail subbands, thus increasing the robustness of the method. At the detector, we compute an average of the extracted watermarks.

3. WATERMARKING IN THE DWT DOMAIN

In two-dimensional separable dyadic DWT, each level of decomposition produces four bands of data, one corresponding to the low pass band (LL), and three other corresponding to horizontal (HL), vertical (LH), and diagonal (HH) high pass bands. The decomposed image shows a coarse approximation image in the lowest resolution low pass band, and three detail images in higher bands. The low pass band can further be decomposed to obtain another level of decomposition. This process is continued until the desired number of levels determined by the application is reached. Figure 1 shows three levels of decomposition.

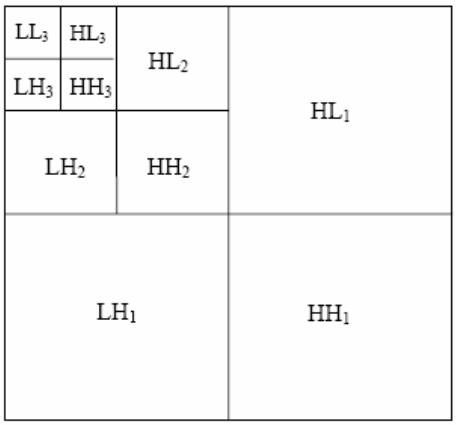

Figure 1: DWT decomposition with 3 levels.

Taking into account the fact that the HVS is not sensitive to small changes in high frequencies of the image, but rather sensitive to changes affecting the smooth parts of the image (the coarsest resolution level of the image), we embed the same watermark several times into the HH, HL and LH detail images, leaving the LL band unaffected.

3.1. Multiple embedding

Consider X the original gray-level image and the watermark W a pseudo random binary sequence, of length N_w with $w(i) \in \{-1,1\}$. The image is decomposed into L resolution levels using the DWT, thus obtaining for each resolution level "l" three detail subbands HH_l, HL_l, LH_l and one approximation subband (last level) LL_L. The current watermark bit w(i) is embedded if the wavelet coefficient $d_{s,l}(m,n)$ from the respective subband s (HH, HL, LH respectively) and level l, is higher than a threshold:

$$T_{s,l} = q_l \max_{m,n}\{d_{s,l}(m,n)\}, \qquad (1)$$

where $s \in \{HH, LH, HL\}$ and $l \in \{1,...,L\}$.

The value of the threshold is computed for every subband, depending on the wavelet coefficients from the subband and on a parameter q_l, different for each level. The watermarked coefficient is given by

$$d^w_{s,l}(m,n) = d_{s,l}(m,n)\left[1 + \alpha \cdot w(i)\right], \qquad (2)$$

where α is the embedding strength and w(i) is the watermark bit embedded at the location (m,n). The watermark is embedded repeatedly in each subband for a higher degree of robustness. The watermarked image X^w is computed with the IDWT from the new coefficients. It is obvious that the higher the strength of the mark α, and the lower the parameters q_l are, the more robust yet visible the watermark will be.

3.2. Detecting the watermark

The detection requires the original watermark and the original image, or some significant vector extracted from its wavelet transform, specifically in this case, the detail coefficients with a value above the computed threshold for each subband. The watermark bit $\hat{w}(i)$ is obtained from the wavelet coefficient $\hat{d}_{s,l}(m,n)$ of the possibly distorted image $\hat{X}^w$, and the original wavelet coefficient $d_{s,l}(m,n)$:

$$\hat{w}(i) = \operatorname{sgn}\left(\frac{\hat{d}_{s,l}(m,n) - d_{s,l}(m,n)}{d_{s,l}(m,n)}\right), \qquad (3)$$

A random guess is made for the watermark bit in the location (m,n) if the two coefficients are equal or if $d_{s,l}(m,n) = 0$. If the mark has been embedded in different locations several times, the most common bit value is assigned for the recovered watermark bit. The correlation coefficient compares the original and the extracted mark:

$$c\left(W,\hat{W}\right) = \frac{\sum_{i=1}^{N_w} w(i)\hat{w}(i)}{\sqrt{\sum_{i=1}^{N_w} w^2(i)} \cdot \sqrt{\sum_{i=1}^{N_w} \hat{w}^2(i)}} \qquad (4)$$

where $c\left(W,\hat{W}\right) \in [-1,1]$. If the correlation coefficient is above a specified threshold, the watermark is positively detected in the image. We consider that if the watermark length is large enough, setting the threshold

at 0.5 will not result in large probability of false negative.

4. SIMULATION RESULTS

We performed simulations using the test image Peppers, size 256 x 256 (Fig. 2), and a 256-bits watermark. The Daubechies 10pt wavelet was used to produce the wavelet coefficients. In all tests we used the following parameters: the number of resolution levels L = 3, the level-dependent parameters q_1=0.06, q_2=0.04, q_3=0.02. We varied the strength of the watermark α = 0.1, 0.2 and 0.3. The extraction of the mark is made from all levels, using a majority rule, (detector type I), and from the coarsest level only, since the lowest frequencies are not so affected by common signal distortions (detector type II).

We compare the method presented with the spread spectrum technique proposed by Cox et al in [5]. They embed a random noise-like sequence into the largest DCT coefficients of the original image, without affecting the DC component, thus spreading the mark in different bins of frequency:

$$v'(i) = v(i)(1 + \beta w(i)) \tag{5}$$

where v(i) is the DCT coefficient to be watermarked, w(i) is the watermark bit, β is the embedding strength and v'(i) is the watermarked coefficient. In the original paper, the watermark is a pseudo random sequence of type $\mathcal{N}(0,1)$ with the length of 1000 and the embedding strength is set at β = 0.1.

To make possible the comparison between our method and theirs, we embed the same binary watermark as in our case, and we use the same number of repetitions. The resulting images for Cox technique are visibly distorted from the original ones, having the peak signal-to-noise ratio (PSNR) around 25 dB, which is unacceptable. Setting the embedding strengths at β = 0.01, 0.02 and 0.03, the watermarked images with the Cox technique have comparable PSNR with those watermarked with our method. There are three cases to be considered separately: a) α = 0.1 and β = 0.01; b) α = 0.2 and β = 0.02; c) α = 0.3 and β = 0.03.

The original Peppers image and the watermarked images using both methods for the three different cases are shown in Figures 2, 3 and 4. Human observers cannot make a distinction between the original and the watermarked images. Also, Table 1 presents the values of the peak signal-to-noise ratio for each watermarked image (Peppers, Lena, Boat and Barbara) as a measure of the distortions introduced by the watermark:

$$PSNR = 10 \lg \left[\frac{M \cdot N \cdot 255^2}{\sum_{m,n} \left(X^w(m,n) - X(m,n) \right)^2} \right] \tag{6}$$

where M, N is the size of the image; X(m,n) and X^w(m,n) are the pixels' values for the original X and watermarked X^W images, respectively.

To prove the robustness of our method, we investigate the effect of common signal distortions on the correlation coefficient between the original and the recovered mark and compare the performances of our method with the results obtained using the method proposed by Cox in [5]. We performed several attacks against the watermarked images median filtering, JPEG compression, AWGN, JPEG2000 compression, resizing, scaling, intensity adjustment, cropping half of the image.

In Table 2, 3 and 4 we have the detector response for the two compared methods, when the watermarked Peppers image is attacked by lossy compression (JPEG and JPEG2000) with different compression rates; AWGN with the signal-to-noise ratio 11.4 dB, rescaling to half of the image, median filtering with filter size 3, intensity adjustment, cropping, resizing. From the correlation values we see that our method works better than Cox's method for each attack with some exceptions when the watermarks is undetectable in both cases (e.g. Table 2, α=0.1 and β=0.01 for intensity adjustment). In fact the results for the Cox method are much lower and fail to detect the watermark in most attacks (JPEG compression with compression rates higher than 10; cropping; scaling; median filtering; intensity adjustment; JPEG2000 compression with compression rates higher than 10).

Regarding our results, detector II yields in higher performances in the case of lossy compression, median filtering and scaling, whereas detector I has better results in the case of AWGN attack.

In the cropping attack, the two types of detector have the same results. In the case of intensity adjustment the watermark is positively detected by both detectors (I and II) only for the strength of α = 0.3.

The detector responses obtained for the images compressed with JPEG2000 are much higher than of those compressed with JPEG, thus proving the robustness of the watermark embedded in the DWT domain.

Generally speaking, the higher the embedding strength is, the better the performances are. However, since there is a tradeoff between robustness and invisibility, the strength should be restricted to a value of α=0.2.

5. CONCLUSION

We proposed a robust wavelet-based watermarking method that embeds the mark in coefficients selected in such a manner that the two images are practically indistinguishable by a human observer. By embedding the watermark bits into the edges and textures of the image we make use of the properties of the human visual system. One can see that by setting the watermark noise level at the same value, the performances obtained with our method works better than the method proposed in [5]. We have proposed two types of detectors. The positive detection of a watermark should be made after evaluation of both responses.

Future work should concentrate into better use of the HVS and statistical image properties as well as coding the watermark bits.

6. ACKNOWLEDGMENTS

The first author was supported by a grant from the National Council of Scientific Research and Education, (Consiliul National al Cercetarii Stiintifice din Invatamantul Superior), Romania, CNCSIS code 47 TD.
We would like to thank prof. A. Isar ("Politehnica" University of Timisoara) for the fruitful discussions that we had during the writing of this paper.

7. REFERENCES

[1] G. Voyatzis, I. Pitas, "Problems and Challenges in Multimedia Networking and Content Protection," *TICSP Series* No. 3, Editor Iaakko Astola, March 1999.

[2] I. Cox, M. Miller, J. Bloom, *Digital Watermarking*, Morgan Kaufmann Publishers, 2002.

[3] M. Borda, I. Nafornita, "Digital Watermarking – Principles and Applications," *Proc. Of Int. Conf. Communications* Bucharest, 2004, pp. 41-54.

[4] N. Nikolaidis, I. Pitas, "Robust Image Watermarking in the Spatial Domain," *Trans. Signal Processing*, Vol. 66, No. 3, pp. 385-403, 1998.

[5] I. Cox, J. Killian, T. Leighton, T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Trans. Image Processing*, Vol. 6, No. 12, pp. 1673-1687, 1997.

[6] X. Xia, C. G. Boncelet, and G. R. Arce, "Wavelet transform based watermark for digital images," *Optics Express*, Vol. 3, No. 12, 1998, pp. 497-505.

[7] J.R. Kim and Y.S. Moon, "A Robust Wavelet-Based Digital Watermarking Using Level-Adaptive Thresholding," *Proc. of IEEE ICIP*, Vol. 2, Kobe, Japan, Oct. 1999, pp. 226-230.

[8] B. S. Kim, K. K. Kwon, S. G. Kwon, K. N. Park, K. N. Park, K. I. Song, K. I. Lee, "A robust wavelet-based digital watermarking using statistical characteristic of image and human visual system," *Proc. of ITC-CSCC* 2002, vol 2. pp. 1019-1022.

[9] C. Nafornita, A. Isar, "Digital Watermarking of Still Images using the Discrete Wavelet Transform", *Scientific Bulletin of Politenica University of Timisoara*, tom 48(62), fascicola 1, 2003, pp. 73-78.

[10] C. Nafornita, M. Borda, A. Kane, "A Wavelet-Based Digital Watermarking using Subband Adaptive Thresholding for Still Images", *microCAD 2004*, Miskolc, Hungary, 18 – 19 March 2004, pp. 87 - 92.

[11] C. Nafornita, "A Wavelet-Based Watermarking for Still Images," *The Scientific Bulletin of Politenica University of Timisoara*, Electronics and Telecommunications, tom 49(63), fascicola 2, 2004, *Symposium of Electronics and Telecommunications ETc 2004*, 22 - 23 October 2004, Timisoara, pp. 126-131.

[12] M.Ramkumar, A.N. Akansu, A.A.Alatan, "A Robust Data Hiding Schemes for Images Using DFT," *IEEE International Conference on Image Processing*, II, pp 211-215, October 1999.

[13] C.Y. Lin, M. Wu, J. Bloom, I. Cox, M. Miller, Y.M Lui, "Rotation, scale and translation resilient watermarking for images," *IEEE Trans. Image Processing*, vol. 10, no. 5, May 2001.

[14] P. Loo and N. G. Kingsbury, "Watermarking using Complex Wavelets with Resistance to Geometric Distortion," *The 10th European Signal Processing Conference* (Eusipco 2000), 5-8 Sep. 2000, Tampere, Finland.

[15] P. Campisi, D. Kundur, A. Neri, "Robust Digital Watermarking in the Ridgelet Domain," *IEEE Signal Processing Letters*, Vol. 11, No. 10, October 2004, pp. 826-830.

[16] M. L. Miller, G. J. Doerr, I. J. Cox, "Dirty-Paper Trellis Codes for Watermarking," *IEEE Int. Conf. on Image Processing*, vol. 2, pp. 129-132, 2002.

[17] N. Abdulaziz, A. Glass, K. K. Pang, "Embedding data in images using turbo coding", *6th Int. Symposium on DSP for Communication Systems*, 28-31 Jan 2002, Univ. of Wollongong, Australia.

[18] B. Chen, G. W. Wornell, "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding", *IEEE Trans. Information Theory*, Vol. 47, No. 4, pp. 1423-1443, May 2001.

[19] D. Kundur, D. Hatzinakos, "Diversity and Attack Characterization for Improved Robust Watermarking," *IEEE Trans. Signal Processing*, Vol. 49, No. 10, 2003, pp. 2383-2396.

[20] F. A. Petitcolas, Matlab source code for Cox's algorithm, http://www.petitcolas.net/fabien/software/index.html

[21] A. Ambroze, G. Wade, C. Serdean, M. Tomlinson, Y. Stander, M. Borda, "Turbo code protection of video watermark channel", *IEE Proceedings Vision Image*, Signal Processing, Vol. 148, No. 1, Feb. 2001, pp. 54-58.

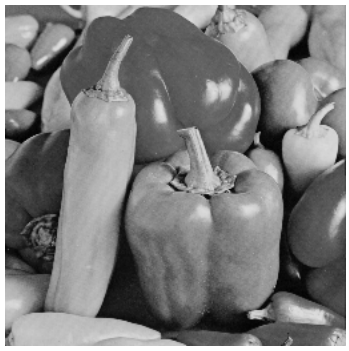

Figure 2: Original image

(a) α =0.1, PSNR=45.54 dB (b) α = 0.2, PSNR=40.28 dB (c) α = 0.3, PSNR=36.94 dB

Figure 3: Watermarked images using the proposed method, for different embedding strengths α, with the respective resulting PSNR as a measure of the distortion introduced by the watermark.

(a) β=0.01, PSNR=45.75 dB (b) β=0.02, PSNR = 39.73dB (c) β=0.03, PSNR = 36.21dB

Figure 4: Watermarked images using the SS method from [5], for different embedding strengths β, with the respective resulting PSNR as a measure of the distortion introduced by the watermark.

Table 1. Values of PSNR [dB] for watermarked images

Image \ Method	Proposed method			Cox's method		
	α=0.1	α=0.2	α=0.3	β=0.01	β=0.02	β=0.03
Peppers	45.54	40.28	36.94	45.75	39.73	36.21
Lena	45.39	40.12	36.77	47.19	41.17	37.65
Boat	44.35	38.86	35.45	45.35	39.33	35.81
Barbara	44.18	38.7	35.27	46.44	40.42	36.90

Table 2. Detector response for distorted watermarked images

Method / Attack	Proposed method, α=0.1		Cox's method, β=0.01
	Type I detector	Type II detector	
JPEG, Q=75 (CR=5.5)	0.78	0.98	0.59
JPEG, Q=50 (CR=8.3)	0.50	0.92	0.35
JPEG, Q=25 (CR=12.8)	0.16	0.65	0.04
JPEG, Q=20 (CR=15)	0.09	0.54	0
Crop, 1/2	0.30	0.34	0
AWGN, SNR=11.4dB	0.55	0.36	0.12
Scaling 256->128->256	0	0.14	0
Median filtering, 3	0.02	0.60	0
Intensity adjustment	0	0.03	0
JPEG2000, CR = 5	0.96	0.89	0.47
JPEG2000, CR = 10	0.20	0.66	0.14
JPEG2000, CR = 15	0.03	0.43	0.03
JPEG2000, CR = 20	0	0.32	0
JPEG2000, CR = 25	0	0.27	0

Table 3. Detector response for distorted watermarked images

Method / Attack	Proposed method, α=0.2		Cox's method, β=0.02
	Type I detector	Type II detector	
JPEG, Q = 75 (CR=5.5)	0.97	0.99	0.89
JPEG, Q = 50 (CR=8.3)	0.71	0.97	0.56
JPEG, Q = 25 (CR=12.8)	0.32	0.80	0.11
JPEG, Q = 20 (CR=15)	0.21	0.78	0.03
Crop, 1/2	0.42	0.40	0.007
AWGN, SNR=11.4dB	0.86	0.78	0.38
Scaling 256->128->256	0.08	0.52	0
Median filtering, size 3	0.13	0.82	0
Intensity adjustment	0	0.22	0
JPEG2000, CR = 5	0.99	0.98	0.85
JPEG2000, CR = 10	0.56	0.93	0.24
JPEG2000, CR = 15	0.24	0.78	0.04
JPEG2000, CR = 20	0	0.59	0.01
JPEG2000, CR = 25	0	0.51	0

Table 4. Detector response for distorted watermarked images

Method / Attack	Proposed method, α=0.3		Cox's method, β=0.03
	Type I detector	Type II detector	
JPEG, Q = 75 (CR=5.5)	0.99	1	0.99
JPEG, Q = 50 (CR=8.3)	0.85	1	0.67
JPEG, Q = 25 (CR=12.8)	0.40	0.89	0.18
JPEG, Q = 20 (CR=15)	0.25	0.89	0.09
Crop, 1/2	0.44	0.45	0
AWGN, SNR=11.4dB	0.89	0.78	0.39
Scaling 256->128->256	0.015	0.53	0
Median filtering, size 3	0.25	0.96	0
Intensity adjustment	1	0.95	0
JPEG2000, CR = 5	1	0.99	0.92
JPEG2000, CR = 10	0.67	0.97	0.34
JPEG2000, CR = 15	0.35	0.84	0.10
JPEG2000, CR = 20	0.12	0.71	0.01
JPEG2000, CR = 25	0.07	0.66	0