Image Watermarking Based on the Discrete Wavelet Transform Statistical Characteristics

Corina Nafornita, *Student Member, IEEE*, Alexandru Isar, *Member, IEEE* and Monica Borda, *Member, IEEE*

Abstract — **The current paper proposes a robust watermarking method for still images that embeds a binary watermark into the detail subbands of the image wavelet transform. The perceptually significant coefficients are selected for each subband using a different threshold. The threshold is computed based on the statistical analysis of the wavelet coefficients. For greater invisibility of the mark, the approximation subband is left unmodified. The watermark is embedded several times to achieve robustness. The method is tested against different types of attacks (lossy compression, AWGN, scaling, cropping, intensity adjustment, filtering and collusion attack). The proposed method was compared with a state-of-the-art watermarking method, highlighting its performances.**

Keywords — **copyright protection, discrete wavelet transform, statistical analysis, watermarking.**

I. Introduction

PROTECTION of multimedia transmitted over the Internet 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]. Important properties of an image watermarking system are [2]-[3]: perceptual transparency (the watermarking process should not degrade the image significantly), robustness (resistance of the mark against intentional or unintentional attacks like AWGN, filtering, lossy compression, scaling, cropping), and data hiding capacity (the amount of information that can be embedded into the original cover work without causing serious distortions).

Most of existing watermarking systems proposed in the literature can be classified depending on the watermarking domain, where the embedding takes place: spatial domain techniques [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], [13], and the Discrete Fourier Transform (DFT) [12].

In this paper, we present a watermarking technique in the DWT domain, for copyright protection purposes. The watermark is embedded several times into perceptually significant coefficients (PSCs) of the wavelet domain using statistical properties of the transformed image. An average of the extracted watermarks is computed at the detector. The detection is non-blind, thus increasing the probability of detecting the watermark.

Taking into account the fact that the human visual system (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), the embedding of the same watermark is made several times into the HH, HL and LH detail images, leaving the LL band unaffected.

II. Description of the proposed method

Several papers that deal with copyright protection for images 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 unintentional attacks (e.g. compression, [5]-[8]).

A. Embedding the watermark

Consider X the original gray-level image and the watermark W a pseudo random binary sequence, of length N_w with w(i) ∈ {-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 watermark is repeatedly embedded of M>1 times in the transformed image. Each repetition is denoted by W_r, with r=1,2,...,M. This can be viewed as a form of transmitting the watermark in different subchannels. It has been shown by Kundur et al. in [13] that diversity techniques can give very good results in detecting the watermark, considering the fact that many watermark attacks are more appropriately modeled as fading like.

Roughly speaking, the current watermark bit w_r(i) is embedded at the location (m,n) of subband s, level *l* if the absolute value of the wavelet coefficient $d_{s,l}$(m,n) is higher than a subband dependent threshold $T_{s,l}$. The watermarked coefficient is given by:

$$d^w_{s,l}(m,n) = d_{s,l}(m,n) + \alpha \cdot \left|d_{s,l}(m,n)\right| w_r(i) \quad (1)$$

$$\text{if } |d_{s,l}| > T_{s,l}$$

This paper was partially financed in the framework of a CNCSIS grant, TD/47/2004/33385.

C. Nafornita is with the Communications Dept., "Politehnica" University of Timisoara, Romania (e-mail: corina.nafornita@etc.utt.ro).

A. Isar is with the Communications Dept., "Politehnica" University of Timisoara, Romania (e-mail: alexandru.isar@etc.utt.ro).

M. Borda is with the Communications Dept., Technical University of Cluj-Napoca, Romania (e-mail: monica.borda@com.utcluj.ro).

where α is the embedding strength, r = 1,2,…,M and the threshold is:

$$T_{s,l} = m_{s,l}\sigma_{s,l} \tag{2}$$

The multipliers $m_{s,l}$ are selected on the basis of a statistical analysis of the DWT, [14]. The pdfs of the detail wavelet coefficients are heavy tailed. We have chosen the Laplace distribution, [15]:

$$f_{d_{s,l}}(y) = \frac{1}{2\sqrt{2}\sigma_{s,l}} \cdot e^{-\frac{|y|}{\sqrt{2}\sigma_{s,l}}} \tag{3}$$

The probability to select a detail wavelet coefficient with the absolute value higher than the threshold $T_{s,l}$ is given by:

$$P_{T_{s,l}} = P\left(\left|d_{s,l}\right| > T_{s,l}\right) = 2 \cdot e^{-\frac{T_{s,l}}{\sqrt{2}\sigma_{s,l}}} - 1 \tag{4}$$

Hence, the threshold values can be computed using the following relation

$$T_{s,l} = \sqrt{2} \cdot \sigma_{s,l} \cdot \ln\left(\frac{2}{P_{T_{s,l}} + 1}\right) \tag{5}$$

Choosing the value $P_{Ts,l} = 0.5$ and taking into account the relation, [14]:

$$\sigma_{s,l}^2 = 2^{2l-2} \cdot \sigma_{s,1}^2$$

the threshold values become:

$$T_{s,l} = 0.2 \cdot 2^l \cdot \sigma_{s,1} \tag{6}$$

So, a half of the detail wavelet coefficients, $d_{s,l}$, in a certain subband (s,l) are higher in absolute value than the thresholds $T_{s,l}$. In fact, because the proposed method requires the insertion of the same watermark (having a length of N_w) many times, more room in each subband must be necessary (especially for large values of l). This is the reason why we conceived an adaptive threshold selection method, initialized with the values in (6). At each iteration the threshold values are decreased:

$$\begin{aligned} T_{s,l}(0) &= T_{s,l} \\ T_{s,l}(p) &= T_{s,l}(p-1) - 0.25 \end{aligned} \tag{7}$$

and the insertion of an integer number of watermark repetitions (at least one) is verified. When this condition is satisfied for the first time, the iteration cycle is stopped. The watermarked image X_w is computed with the IDWT from the new coefficients. The higher the strength of the watermark α, and the higher the parameters $m_{s,l}$ are, the more robust yet visible the watermark will be.

B. 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 an absolute value above the computed threshold for each subband. The watermark bit $\hat{w}_r(i)$ 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):

$$\hat{w}_r(i) = \operatorname{sgn}\left(\frac{\hat{d}_{s,l}(m,n) - d_{s,l}(m,n)}{\alpha \cdot \left|d_{s,l}(m,n)\right|}\right) \tag{8}$$

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. Extraction of the watermark is made using the majority rule: the most common bit value is assigned for the recovered watermark bit, [11]. This is done from all levels (detector type I) or from level 3 (detector type II), since the lowest frequencies are not so affected by compression. The correlation coefficient compares the original and the extracted mark:

$$c\left(W,\hat{W}\right) = \frac{\sum_{i=1}^{N_w} w(i)\hat{w}(i)}{\sqrt{\sum_{i=1}^{N_w} w^2(i)} \cdot \sqrt{\sum_{i=1}^{N_w} \hat{w}^2(i)}} \tag{9}$$

where ŵ(i) is the watermark bit estimate. If the correlation coefficient is above a specified threshold, the watermark is positively detected in the image.

The embedding and extraction procedure are shown in Fig. 1 and 2.

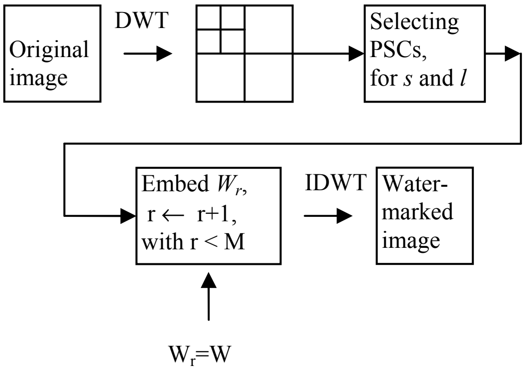

Fig. 1.Embedding part of the watermarking system.

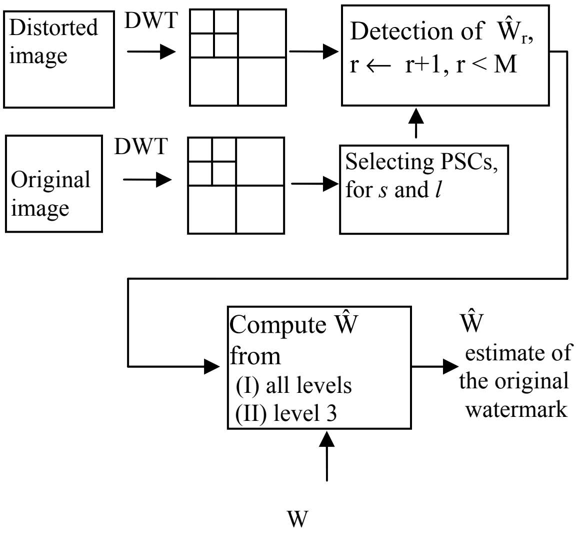
Distorted image
DWT
Detection of $\hat{W}_r$, r ← r+1, r < M
Original image
DWT
Selecting PSCs, for s and l
Compute $\hat{W}$ from
(I) all levels
(II) level 3
$\hat{W}$
estimate of the original watermark
W

Fig. 2.Detection part of the watermarking system.

III. Simulation results

We performed simulations using the test image Peppers, size 256 x 256, 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, and the strength of the watermark α = 0.1. Specifically, we affected 2816 coefficients from a total of 65536 (including the LL subband). The repetition number of the original watermark was for this image M=11. Human observers cannot make a distinction between the original and the watermarked image. The distortion introduced by the watermark can be measured with the peak signal-to-noise ratio PSNR, in this case is 44.95 dB.

To prove the robustness of the method, we investigate the effect of common signal distortions on the correlation coefficient between the original and the recovered mark and compare the new performances with the results obtained using the method 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:

$$v'(i) = v(i)(1 + \beta w(i))$$

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. The resulting image for Cox technique is visibly distorted from the original one, having the peak signal-to-noise ratio (PSNR) around 25 dB, which is unacceptable. Setting the embedding strength at β=0.01, the watermarked image with the Cox technique has a comparable PSNR with the watermarked image with our method.

In Table 1 we have the detector response for the two methods, when the watermarked Peppers image is attacked by lossy compression (JPEG, quality factor 75, 50, 25, 20 and JPEG2000, compression rate 5, 10 and 15); AWGN with the SNR = 11.4 dB, rescaling to half of the image, median filtering, filter size 3 and 5, intensity adjustment, cropping. From the correlation values we see that our method works better than Cox's method for each attack.

We can clearly see that detector II yields in higher performances in the case of lossy compression, median filtering, scaling and intensity adjustment, whereas detector I has better results in the case of AWGN attack, cropping and JPEG2000.

In Table 2 we have the detector response for the collusion attack: when four watermarked images are averaged. It is obvious that all four watermarks are still detectable.

Fig. 3(a)-(c) shows the original and watermarked images, using the proposed method, and the image difference between them (the watermark in the spatial domain).

Fig. 3(d) shows the key that indicates the selected coefficients for each subband. Obviously, the selected coefficients that will contain a watermark are indeed edges and textures in the original image.

Table 1: Comparison between the proposed method and Cox et al. method.

Attack vs. detector response	**Proposed method**		**Cox et al. method**
	Detector I	Detector II	
JPEG, Q=75	0.9688	1	0.8984
JPEG, Q=50	0.8281	0.9531	0.7031
JPEG, Q=25	0.4219	0.7813	0.4531
JPEG, Q=20	0.3281	0.6797	0.3047
Median filtering, 3*3	0.2891	0.7500	0.4375
Median filtering, 5*5	0.0234	0.2344	0.1563
Resizing, 256->128->256	0.0703	0.2422	0.0469
AWGN, SNR = 11.4 dB	0.6484	0.6094	0.2734
Cropping ½	0.4219	0.3906	-0.0156
Intensity adjustment	0.0234	0.0859	0.0547
JPEG 2000, CR=15	0.5859	0.6563	0.4844
JPEG 2000, CR=10	0.9766	0.8984	0.6484
JPEG 2000, CR=5	1	0.9922	0.8750

Table 2: Results for collusion attack, averaging four watermarked images

Detection type vs. detector response	**Original watermark**			
	W_1	**W_2**	**W_3**	**W_4**
Type I	0.37	0.34	0.39	0.40
Type II	0.38	0.36	0.39	0.36

IV. Conclusions

We proposed a robust wavelet-based watermarking method that embeds the mark in a transparent manner using statistical analysis of the 2D DWT. By embedding the watermark bits into the *edges and textures* of the image we make use of the statistical properties of the DWT and of the human visual system (HVS). One can see that by setting the watermark noise level at the same value (PSNR), the performances obtained with our method are better than those obtained with the method 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 properties as well as coding the watermark bits.

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

[14] A. Isar, S. Moga, X. Lurton, “A Statistical Analysis of the 2D Discrete Wavelet Transform,” Proc. of the International Conference *AMSDA 2005*, May 17-20, 2005, Brest, France, pp. 1275-1281.

[15] L. Sendur, I. W. Selesnick, “Bivariate Shrinkage Functions for Wavelet-Based Denoising Exploiting Interscale Dependency,” *IEEE Trans. on Signal Processing*, vol. 50, no.11, November 2002, pp. 2744-2756.

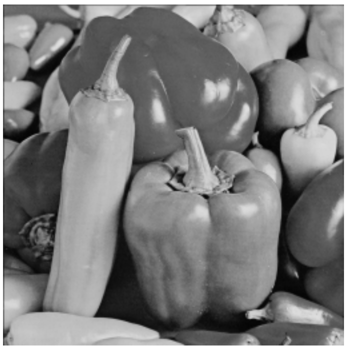
Fig.3(a) Original image Peppers

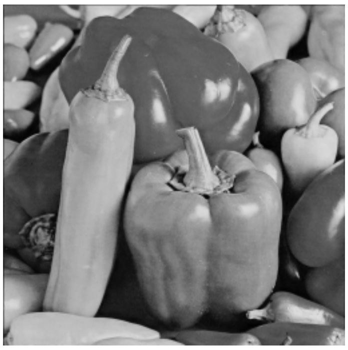
Fig.3(b) Watermarked image, PSNR=44.95 dB

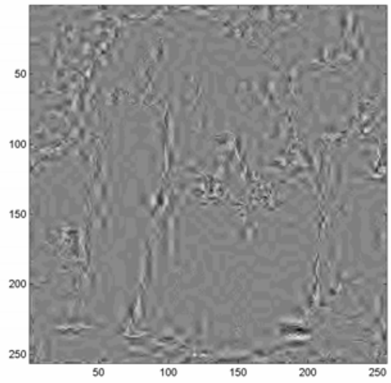

Fig.3(c): Difference image between the two images

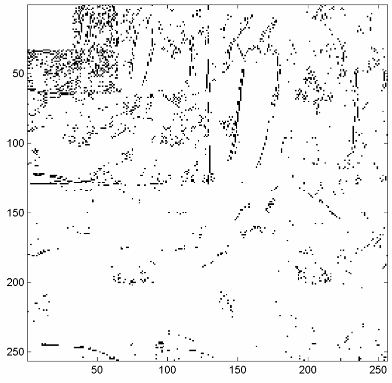

Fig.3(d): Watermarking key that indicates the selected coefficients for each subband.