Buletinul Ştiinţific al Universităţii "Politehnica" din Timişoara

Seria ELECTRONICĂ şi TELECOMUNICAŢII
TRANSACTIONS on ELECTRONICS and COMMUNICATIONS

Tom 49(63), Fascicola 2, 2004

A Wavelet-Based Watermarking for Still Images

Corina Nafornita[1]

Abstract – We present a robust watermarking method for still images, which uses the similarity of the discrete wavelet transform (DWT) and the human visual system (HVS). In order to make the mark imperceptible, the lowest frequencies are left unmodified, and the rest of the coefficients from the other sub-bands are spatially selected using an adaptive threshold. We test the robustness of the mark against different types of attacks, thus evaluating the robustness of the method proposed herein. We compare our performances with another frequency-based watermarking method.
Keywords: watermarking, copyright protection, discrete wavelet transform

I. INTRODUCTION

In the last decade we have been witnesses to an explosion in the use and distribution of digital multimedia data. PCs with Internet connections have made the distribution, both legal and illegal, of data and applications much easier and faster [1].
Since ancient times, there have been ways of establishing the identity of the owner of an object in case of dispute which range from simple inscribing the name of the owner on the object to embedding the owners seal in the object (like a tattoo on the head of slave) [2]. In the digital world, though, more sophisticated means are required to ensure the same, since copying and reproducing works of others has become extremely easy and the reproduced work generally spreads at the speed of light across the globe.
While encryption is a solution to protect the data transmitted from seller to buyer, watermarking has been proposed as a solution to ensure the copyright protection.
Digital watermarks can be used to identify the works as belonging to a company or individual. Watermarks encrypt the information as an imperceptible signal, which is added to the data in such a way that it is always retained [3].
Common types of multimedia data are image, video, audio data. Our paper concentrates on the watermarking for still images, although the same principles can be applied to both video and audio data.
To be effective in the protection of the ownership of intellectual property, the watermark should be [2, 4]:

1. *difficult/impossible to remove*, at least without visibly degrading the original image,
2. *robust* against image modifications that are common to typical image-processing applications (e.g. scaling, dithering, cropping, compression),
3. *imperceptible* to the human visual system (HVS),
4. *detectable with or without the original signal* - informed decoder and blind decoder, respectively,
5. *resistant against the ownership deadlock* – known as the IBM attack, appears whenever in the same data there are several watermarks claiming the same copyright. A solution is proposed by Craver et al in [5]: invertible and quasi-invertible watermarking schemes.

Current watermarking techniques for multimedia data developed in literature are spatial/time domain methods [14] and frequency domain methods [11-13]. Another possible classification is spread-spectrum (SS) techniques [6] and non-SS techniques, such as the QIM developed by Chen et al [7]. Our method embeds the watermark in the wavelet domain, and uses the characteristics of the human visual system by selecting the coefficients from each subband with a thresholding scheme.
The paper is organized as follows. Section II describes the proposed method. In Section III we present the simulation results and some attacks. Finally we give some concluding remarks.

II. PROPOSED METHOD

The discrete wavelet transform (DWT) decomposes the image into a high-high (HH), high-low (HL), and low-high (LH) subband for each resolution level, and a low-low (LL) subband for the coarsest resolution level. The LL band is also known as the approximation subimage because it contains most of the information from the image. The HL, LH, HH subbands are the detail subimages containing the horizontal, vertical and diagonal details. The details of the image such as edges and textures are confined into the HH, LH, and HL subbands of the DWT of the

[1] Politehnica University of Timisoara, Communications Dept.
Bd. V. Pârvan Nr. 2, 300223 Timişoara, e-mail corina@etc.utt.ro

image. We take into account the fact that the HVS is not sensitive to small changes in high frequencies of the image, but is rather sensitive to changes affecting the smooth parts of the image, that is, the coarsest resolution level of the image. Therefore, we place the mark into the wavelet domain, specifically, into the HH, LH, and HL subbands, selecting only part of these coefficients, leaving the LL subband unmodified.

A. *Insertion procedure*

Let X be the original gray-level image and the watermark W a pseudo random sequence, with binary values: $w(i) \in \{-1,1\}$ and length N_w. The basic steps for embedding the mark are:

(a) Wavelet decomposition of the original image by L levels to obtain a multiresolution decomposition:

$$Y = DWT(X)$$
$$= \{LL_L^x, HL_L^x, LH_L^x, HH_L^x, HL_{L-1}^x, ..., HH_1^x\}$$

(b) Compute threshold for each subband

Let the approximation coefficients be $c(m,n)$ and the detail coefficients from the resolution level j and sub band s be $d_{s,j}(m,n)$, where $s \in \{h,v,d\}$ and $j \in \{1,...,L\}$. The threshold is computed as follows

$$T_{s,j} = q_j \max_{m,n}\{d_{s,j}(m,n)\} \qquad (5)$$

where q_j is a level-dependant variable.

(c) Embed watermark

For each subband, if the detail coefficient is higher or equal to the above computed threshold, embed the watermark using

$$d_{s,j}^w(m,n) = d_{s,j}(m,n)\left[1 + \alpha\, w(m,n)\right], \quad (6)$$

where α is a parameter that controls the level of the watermark.

(d) Compute the IDWT from these new coefficients

We obtain the watermarked image X^w.

It is obvious that the higher the strength of the mark α and the lower the variables q_j are, the more robust yet visible the watermark will be.

B. *Extraction procedure*

The extraction process requires the original image, or at least some significant vector extracted from the DWT of the cover work, specifically, the detail coefficients with a value above the computed threshold.

To extract the mark from the watermarked possibly distorted work, $\hat{X}^w$, we make use of the wavelet coefficients $\hat{d}_{s,j}(m,n)$, that should contain a watermark bit:

$$\hat{w}(m,n) = \mathrm{sgn}\left(\frac{\hat{d}_{s,j}(m,n) - d_{s,j}(m,n)}{d_{s,j}(m,n)}\right), \quad (7)$$

A random guess is made for the watermark bit in the location (m,n) if $\hat{d}_{s,j}(m,n) = d_{s,j}(m,n)$ or if $d_{s,j}(m,n) = 0$.

If the mark has been embedded in different locations several times, the most common bit value is assigned for the recovered watermark bit.

We make use of the correlation coefficient to compare the original and the extracted mark:

$$c(w,\hat{w}) = \frac{\sum_{n=1}^{N_w} w(n)\hat{w}(n)}{\sqrt{\sum_{n=1}^{N_w} w^2(n)} \cdot \sqrt{\sum_{n=1}^{N_w} \hat{w}^2(n)}} \qquad (8)$$

where $c(w,\hat{w}) \in [-1,1]$. If the correlation coefficient is above a specified threshold, the watermark is positively detected in the image.

III. SIMULATION RESULTS

We performed simulations using several images Lena, Boat, Barbara, Peppers, all with size 256 x 256 (Fig. 1). The watermark was a binary pseudo-random sequence with $N_w = 256$. 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 strength of the watermark $\alpha = 0.1$, and the level-dependent variables $q_1 = 0.06$, $q_2 = 0.04$ and $q_3 = 0.02$.

We extract the watermark in two ways (Fig 1):

- from all levels, using a majority rule, (detector **NC1**)
- from the coarsest level only (since the lowest frequencies are not so affected by common signal distortions). (detector **NC2**)

We investigate the effect of common signal distortions (median filtering, JPEG compression, AWGN) on the correlation coefficient between the original and the recovered mark. We compare the performances of our method with the results obtained using the method proposed by Cox in [6]. The watermark used was bipolar and its length was for a better comparison, 256 bits. Also, the number of repetitions of the mark was the same in both cases.

The watermarked images using our method were not significantly distorted from the originals, whereas for the method presented by Cox et al the difference was clearly visible. The following table shows the values

of PSNR for each watermarked image, as a measure of the distortions introduced by the watermark:

	PSNR, proposed method	PSNR, Cox et al method
Lenna	45.39 dB	27.19 dB
Boat	44.35 dB	25.35 dB
Barbara	44.18 dB	26.44 dB
Peppers	45.55 dB	25.75 dB

We present for each image the detector response as a function of the filter size M, compression ratio and signal-to-noise ratio, in case of median filtering, JPEG compression and additive white noise, respectively. The detector response was computed as a mean value of 32 responses for 32 uncorrelated watermarks (Fig. 2-5).

The plots marked with the 'o' and '+' symbols are the results from the proposed method, with the detector NC1 and NC2 respectively, while the remaining plots are from the method proposed in [6].

Setting the threshold value in the detection process at 0.5 we have the followings.

Median filtering attack:

For all watermarked images, except Boat, the attack by median filtering with filter size larger than M=3 leads to a correlation smaller than 0.5. In fact, only the detector NC2 allows filtering with filter size M=3. For Boat watermarked image, not even the NC2 detector is successfully used in finding the mark.

JPEG compression:

For Lenna, the correlation is smaller than 0.5 at a compression rate of 16 (detector NC2 and Cox) and 10 (NC1), respectively.

For Boat and Barbara, the correlation is smaller than 0.5 at a compression rate of 13 for NC2, 10 for Cox and 7 for NC1.

For Peppers, the compression rate values for which the correlation is smaller than 0.5 is 15 (NC2, Cox) and 8 (NC1).

AWGN attack:

For Lenna and Peppers, the detector response in the Cox et al method is above 0.5 at a signal-to-noise ratio of 5 dB, having a considerably better performance than detector NC1 (12 dB) and NC2 (15 dB).

For Boat and Barbara, the detector values are approximately the same for each method: 3 dB (Cox), around 14 dB (NC2) and 7 dB (NC1).

IV. REMARKS

We proposed a robust wavelet-based watermarking method that embeds the mark in coefficients selected in such a manner that the visible impact on a human observer isn't very high. By embedding the watermark bits into the edges and textures of the image we make use of the human visual system. One can see that both methods, proposed in [6] and ours are image-dependant. Apparently, the Cox method is superior for AWGN attack, comparable with the NC2 detector in the case of JPEG compression, and inferior for median filtering. However if we take into account the fact visibility of the mark, an essential aspect of a watermarking system, it is possible that our methods, with the two proposed detectors (NC1 and NC2) to be considered comparable or better than the Cox method in the given situation.

Future work will concentrate into the study of coding the watermark bits for a better performance.

ACKNOWLEDGEMENT

This work was supported by a grant from the *Consiliul National al Cercetarii Stiintifice din Invatamantul Superior*, Romania, cod CNCSIS 47 TD.

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] A. Sequeira, D. Kundur, "Communications and Information Theory in Watermarking: A Survey", *Multimedia Systems and Applications IV*, A. G. Tescher, B. Vasudev, and V. M. Bove, eds., Proc. SPIE (vol. 4518), pp. 216-227, Denver, Colorado, August 2001.

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

[5] S. Craver, N. Memon, B. Yeo, M. Yeung, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications", *IEEE Journal On Selected Areas In Communications*, Vol. 16, No. 4, May 1998.

[6] I. Cox, J. Killian, T. Leighton, T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", *IEEE Transaction On Image Processing*, 6, 12, pp 1673-1687, 1997.

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

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

[12] C. Nafornita, A. Isar, "Digital Watermarking of Still Images using the Discrete Wavelet Transform", *Buletinul Ştiinţific al UPT*, Tom 48(62), Fascicola 1, 2003, pp. 73-78.

[13] C. Nafornita, M. Borda, A. Kane, "A Wavelet-Based Digital Watermarking using Subband-Adaptive Thresholding for Still Images", *microCAD 2004 International Scientific Conference*, University of Miskolc, 18-19 March 2004, pp.87-92.

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

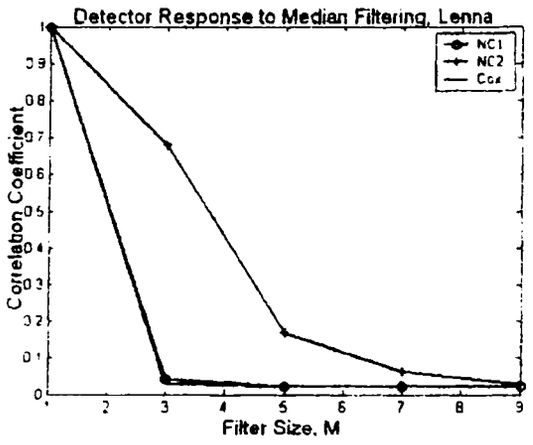
(a)

(b)

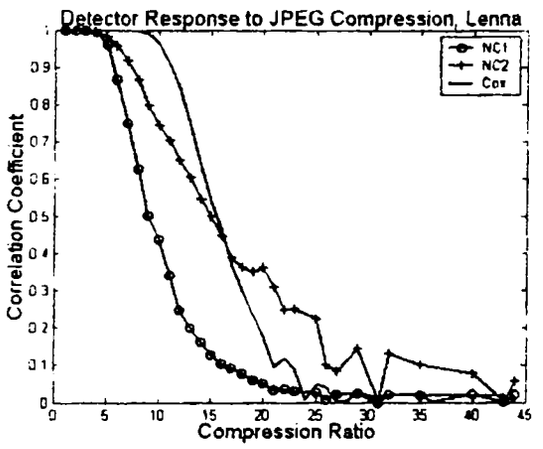
(c)

(d)

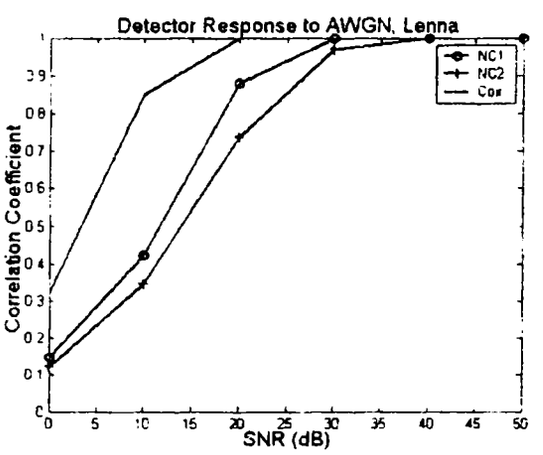
Fig. 1: Original images used for simulations: Lenna (a), Boat (b), Barbara (c) and Peppers (d).



(a)

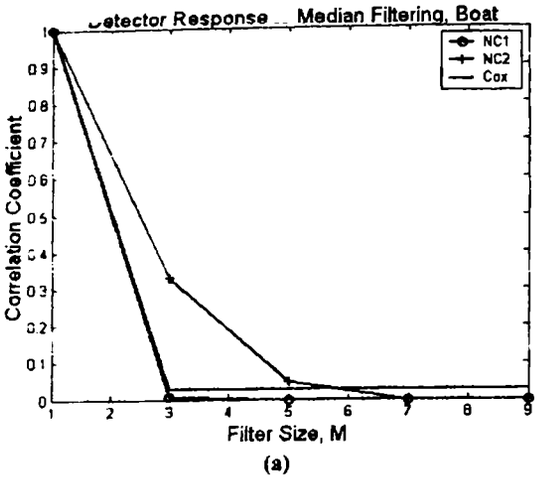


(b)

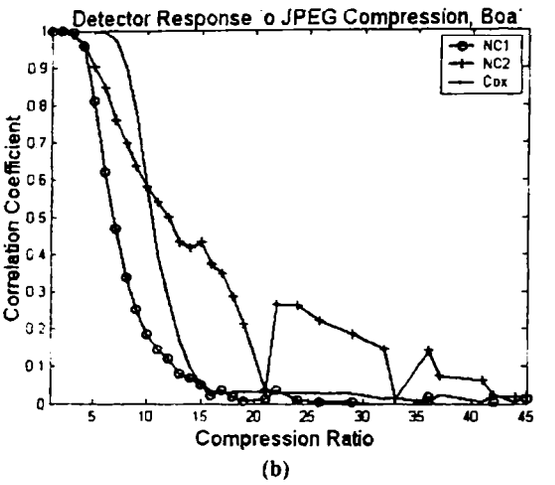


(c)

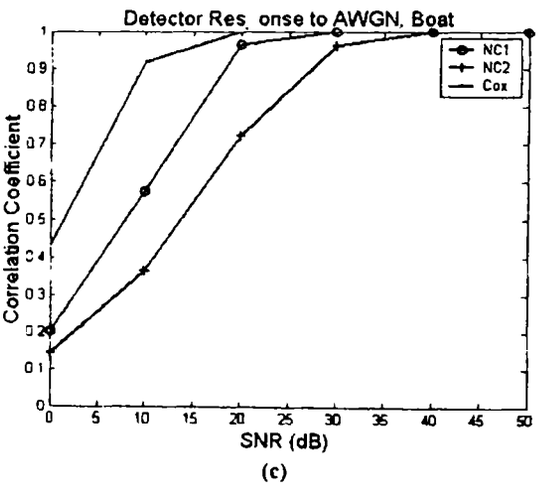
Fig. 2: Detector response to attacks against watermarked Lena: median filtering – (a), JPEG compression – (b), AWGN – (c) The plots marked with the 'o' and '+' symbols are the results from the proposed method, with the detector NC1 and NC2 respectively, while the remaining plots are from the method proposed in [6].



(a)

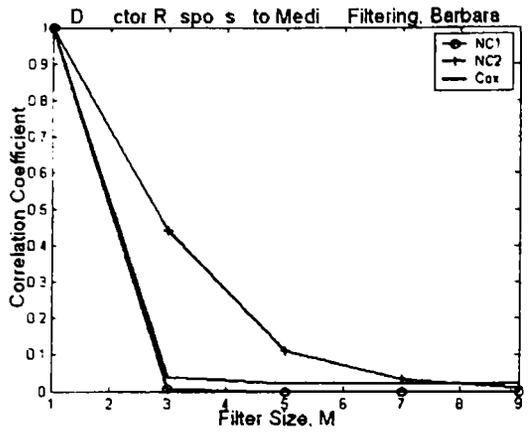


(b)

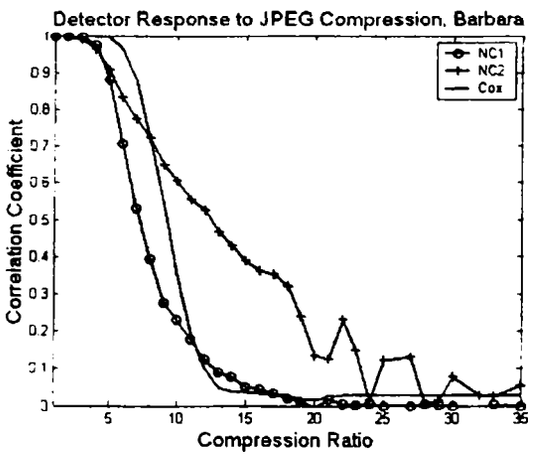


(c)

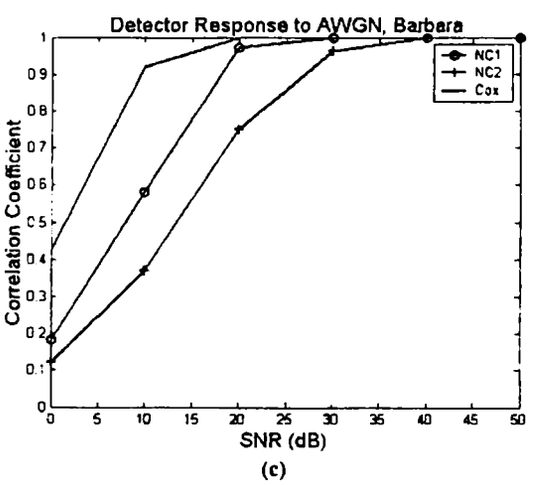
Fig. 3: Detector response to attacks against watermarked Boat (median filtering, JPEG compression, AWGN). The plots marked with the 'o' and '+' symbols are the results from the proposed method, with the detector NC1 and NC2 respectively, while the remaining plots are from the method proposed in [6].



(a)

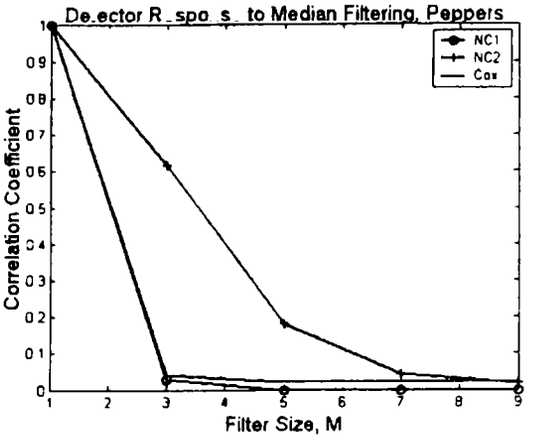


(b)

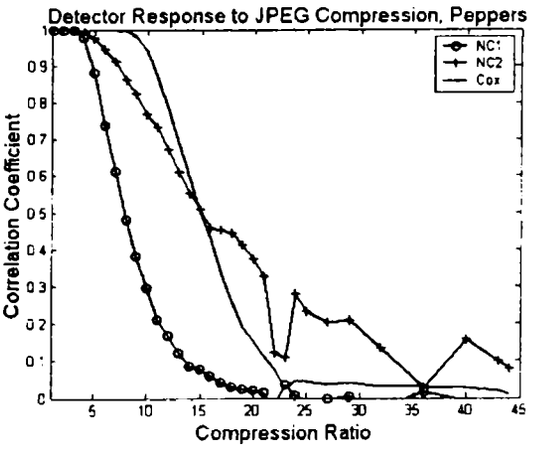


(c)

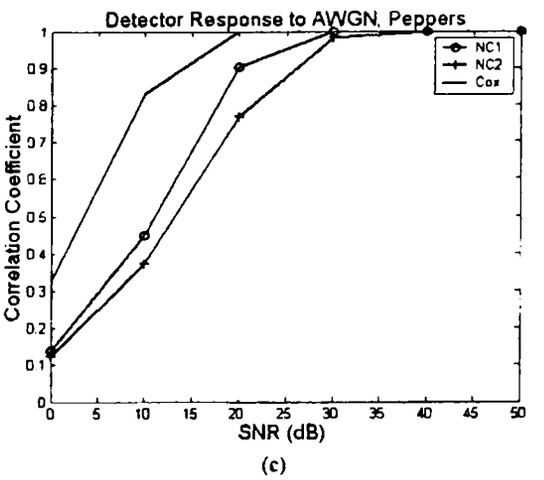
Fig 4: Detector response to attacks against watermarked Barbara: median filtering – (a), JPEG compression – (b), AWGN – (c). The plots marked with the 'o' and '+' symbols are the results from the proposed method, with the detector NC1 and NC2 respectively, while the remaining plots are from the method proposed in [6].



(a)



(b)



(c)

Fig 5: Detector response to attacks against watermarked Peppers: median filtering – (a), JPEG compression – (b), AWGN – (c). The plots marked with the 'o' and '+' symbols are the results from the proposed method, with the detector NC1 and NC2 respectively, while the remaining plots are from the method proposed in [6].