DIGITAL WATERMARKING IN WAVELET DOMAIN

D. Taskovski, S. Bogdanova, M. Bogdanov

University Sts. Cyril and Methodius, Faculty of Electrical Engineering
Karpos II b.b., P.O. Box 574, 91 000 Skopje, Macedonia
dtaskov@cerera.etf.ukim.edu.mk

ABSTRACT

In this paper we propose a wavelet transform based watermarking method. The wavelet coefficients of the watermark are embedded to the most significant coefficients at the low and high frequency bands of the discrete wavelet transform of an image. A multeresolution nature of wavelet transform can be exploit in the process of detection. Experimental results show that the proposed watermarking method results in almost invisible difference between the watermarked image and the original image. Moreover, proposed watermarking method is robust to DCT and wavelet based lossy image compression techniques, and some image processing operations like image resizing and cropping.

1. INTRODUCTION

The fast development of the Internet in the last decade has increased the company's opportunity for commercial presentation of their digital media products. Having the main interest in profit, the companies tend strongly to protect their ownership rights. Digital watermarking has been proposed as one way to accomplish this. The purpose of the watermark is to supply some additional information about the image without visibly modifying the image. In order to be maximum effective, the watermark should be invisible and robust to intentional or unintentional modification of the image. It should be robust against common image processing operations like filtering, requantization, resizing, cropping etc and common image compression techniques. It is common opinion that robustness against image distortion is better achieved if the watermark is placed in perceptually significant coefficients of the image [1]. This is argued by the fact that these coefficients do not change much after common image processing and compression operations. Also, if these coefficients are destroyed, the reconstructed image is different from the original image and the digital watermark become less meaningful. However, embedding the watermark in perceptually significant coefficients could alter the perceived visual quality of the image. This means that the two basic requirements for an effective watermarking scheme, robustness and invisibility conflict with each other.

A variety of watermarking techniques has been proposed in recent years. According to the way watermarking is embedded into the image, all techniques can be broadly classified in two categories: spatial domain and transform domain techniques. In spatial domain techniques, the values at the image pixels are directly modified based on the watermark that has to be embedded. The simplest way is to modify the last significant bits (LSB) of the image's pixel data. In transform domain techniques, first some invertible mathematical transform (DCT, DFT, wavelet) is applied to the image before embedding the watermark. Then, transform domain coefficients are modified by the watermark. The inverse transform is finally applied to obtain watermarked image. Probably the most famous transform domain technique proposed in [1] is based on the idea on spread spectrum communications. A set of randomly generated samples with Gaussian distribution is embedded into the perceptually most significant DCT coefficients of the image. This technique yields impressive results both in terms of image quality and robustness against various image processing operations.

The main motivation of our work is based on the idea proposed in [1]. Wavelet transform instead of DCT is applied to both, the watermark and the host image before the process of embedding. Then, wavelet coefficients of the watermark are added to the most significant coefficients of low and high frequency bands of the discrete wavelet transform of an image. With the appropriate choice of the embedding formulas and scaling parameters in different frequency bands invisibility and robustness of the watermark are insured.

In [1], as in most previous work, watermarking detection is based on classical detection theory. The original image is subtracted from the received image, and correlation between the signal difference and a specific watermark sequence is determined. The correlation value is compared to a predefined threshold to determine whether the received image contains the watermark in question. In our work, as in [2], visually recognizable pattern is used as watermark. Using visually recognizable pattern as watermark is more natural than using randomly generated sequences of bits and both, subjective judgment and objective measurement could be applied to determine whether suspected image is watermarked.

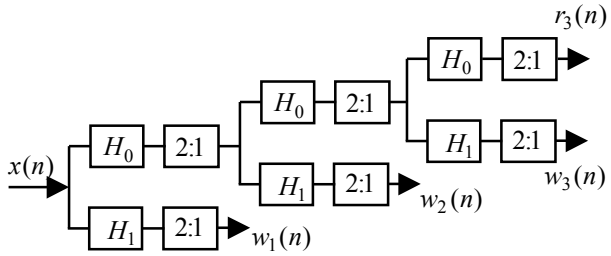


Figure 1. Two-channel dyadic wavelet transform

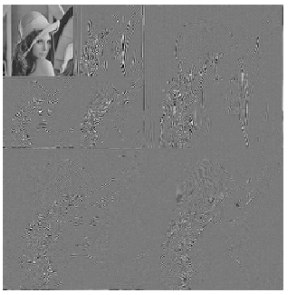


Figure 2. Wavelet decomposition of the image Lena

This paper is organized as follows. In Section 2 short review of discrete wavelet transform is given. The proposed watermarking method is described in Section 3. Experimental results are presented in Section 4 and Section 5 concludes the paper.

2. DISCRETE WAVELET TRANSFORM

A wavelet transform can be interpreted as decomposition into a set of frequency channels having the same bandwidth on a logarithmic scale [3]. The basic idea of the discrete wavelet transform is that of successive approximation, together with that of "added detail". At each stage, the input signal is decomposed into a coarse approximation signal (which can be considered as a lowpass version of the input) and an "added detail" signal (which can be considered as a highpass version).

One-dimensional discrete wavelet transforms (the separable 2-D case is a straightforward extension) can be described in terms of a filter bank as shown in Fig. 1. After K levels of decomposition, reference signal $r_K(n)$ with resolution reduced by factor 2^K with respect to the original signal, as well as the detail signals $w_K(n)$, $w_{K-1}(n)$, ... $w_1(n)$ are obtained. Each detail signal $w_i(n)$ contains precisely the information that, together with the reference signal $r_i(n)$, enables reconstruction of $r_{i-1}(n)$, which is the reference signal at the next higher resolution.

Figure 2 shows the tree levels wavelet decomposition of Lena image. The upper left block represents a smoothed approximation of the original image; its comes from three iterations of the lowpass with downsampling. The other subbands contain detail at various resolutions.

Transform-based image compression is one of most successful applications of the wavelet transform. The wavelet representation is wellmatched to psyhovisual models, and compression systems based on wavelet transform yield superior to other methods for given compression ratio. Extensive literature of wavelet theory can be found in the references of [4].

3. WATERMARKING IN WAVELET DOMAIN

Watermarking in the wavelet domain is composed of two parts: encoding and decoding. In the encoding part, the original image and the watermark are first decomposed using wavelet pyramid structure. Then, the wavelet coefficients W_W, of the low-resolution representation of the watermark W, are embedded in the largest wavelet coefficients I_W of the low-resolution representation of the original image I, in the following way:

$$I'_W = I_W\,(1+\alpha\, W_W) \qquad (1)$$

Spectrum analysis of the images reveals that most of the information in image is located in this low-resolution representation, which represents the smooth parts of the image. It is also known that human eyes are very sensitive to small changes in smooth part of the image. However, with the appropriate choice of the scaling parameter α, the invisibility of the watermark could be adjusted. Conversely, in case of possible attacks, the low-resolution representation of the watermark will still be preserved within the low-resolution representation of the image, which makes the watermark robust.

Other coefficients of the watermark are embedded in the higher frequency components of the image, which represent the edges and textures of the image. Using above equation either will produce watermarked image that is not robust to image operations that perform lowpass filtering (for small values of α) or will create visible defects in the images (for larger values of α). So in order to increase the robustness of the watermark, following equation is used:

$$I'_W = I_W + \beta\, W_W \qquad (2)$$

Since human eyes are not sensitive to small change in the edges and the textures of the image, invisibility of the watermark is kept. The watermarked image is obtained by applying inverse wavelet transform to the coefficients I'_W.

The watermarked image may then be subject to any number of distortions due to intentional or unintentional image processing operations. In the decoding process DWT of the suspected image $\bar{I}$ and of the original (unwatermarked) image is performed. Wavelet coefficients

of the low-resolution representation of the extracted watermark are obtained as:

$$\bar{W}_W = \frac{1}{\alpha}\left[\frac{\bar{I}_W}{I_W} - 1\right] \tag{3}$$

and wavelet coefficients in other frequency subbands as:

$$\bar{W}_W = \frac{1}{\beta}\left[\bar{I}_W - I_W\right] \tag{4}$$

With inverse wavelet transform of $\bar{W}_W$ the extracted watermark $\bar{W}$ is obtained. Since, we use visually recognizable pattern as watermark, extracted watermarks can be compared with original watermark subjectively. Beside subjectively judgment for the watermark fidelity, we have defined an objective measure of similarity between the original watermark and the extracted watermark in the following way:

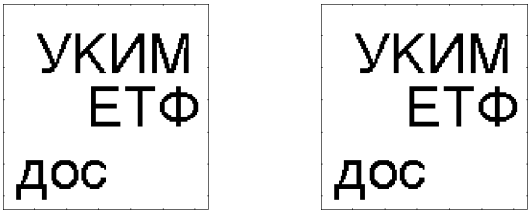
$$SIM = \frac{\sum_i \sum_j W(i,j)\,\bar{W}(i,j)}{\sum_i \sum_j [\,\bar{W}(i,j)]^2} \tag{5}$$

Also, these measures could be applied in wavelet domain to each frequency subband separately. This can benefit in the process of detection. For instance, applying any image processing operation to the watermarked image that performs lowpass filtering (compression, resizing), will result in lost of wavelet coefficients in higher frequency bands of the watermark. In this case, wavelet coefficients in lower frequency subbands could be used to determine whether suspected image contains watermarks.

4. EXPERIMENTAL RESULTS

In this section, some results are presented to demonstrate the invisibility and the robustness of the embedded watermark. The image Lena of size 256x256 is used as test image (Fig. 3(a)), and image pattern shown in Fig. 3(c) is used as watermark. The resolution of the watermark is half of the resolution of the Lena image. A two level wavelet transforms of the test image Lena and one level wavelet transform of the watermark is obtained using the Daubechies tap-6 and tap-2 filters, respectively. Choice of $\alpha = 0.03$ and $\beta = 25$ seems to give the best results in sense of robustness versus visibility. Watermarked Lena images obtained with proposed watermarking method is shown in Fig. 3(b). It can be seen that there is almost invisible difference between the watermarked and the original image, thus proving that the requirement of watermark invisibility is satisfied. In following, some geometric manipulations and compressions are applied to the watermarked image in order to test algorithm robustness.

(a) (b)



(c) (d)

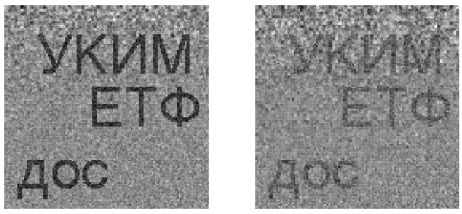
Figure 3. (a) The test Lena image, (b) the watermarked image, (c) the watermark, (d) extracted watermark ($SIM = 1$).

Robustness to DCT and DWT based compression schemes

Image compression can be considered as the most common signal processing operation performed on images. Resistance to this operation is good test for watermarking robustness. Since, DCT is base of current international standard for still image compression, JPEG, and since DWT is expected to be base of up-coming image compression standard JPEG2000, resistance to DCT and DWT based compression schemes is investigated in this experiment. Transform-based image coder [5] is used for this purpose. The compression ratios are chosen as 8 and 16, i.e. 1 and 0.5 bpp. Extracted watermarks are shown in Fig. 4 and Fig. 5, suggesting that the proposed watermarking method is robust to lossy compression. Increasing the compression ratio leads to visible distortion of the image and digital watermarking becomes less meaningful. Even then, watermark could be detected with the proposed watermarking algorithm, if subjective and objective measurements are applied to low-resolution representation of the extracted watermark.

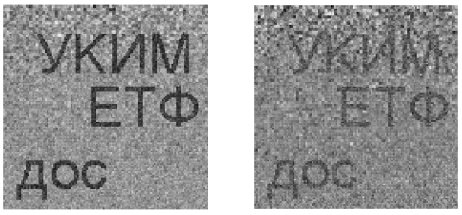
Robustness to Cropping

In this experiment the watermarked image is cropped to one-quarter of its original size, so that the center portion of the image is kept. In order to extract the watermark, the missing portion is replaced with the original unwatermarked image before the detection is carried out. Fig. 6(a) show extracted watermark of cropped image. Even thought 75% of the image is missing watermark still could be detected.



(a) (b)

Figure 4. Extracted watermarks of DCT compressed version of the watermarked image shown in Fig. 3(b): (a) with compression ratio 8:1 (*SIM* = 0.60), (b) with compression ratio 16:1 (*SIM* = 0.29)



(a) (b)

Figure 5. Extracted watermarks of wavelet compressed version of the watermarked image shown in Fig. 3(b): (a) with compression ratio 8:1 (*SIM* = 0.63), (b) with compression ratio 16:1 (*SIM* = 0.29)

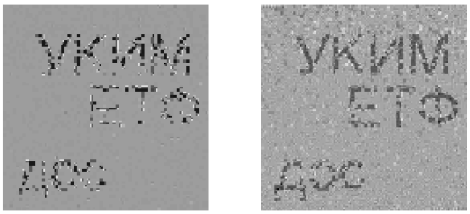
In the second implementation of this experiment watermarked image is compressed before cropping is applied. Extracted watermark of cropped version of DCT based compressed image with compression ratio 16:1 is shown in Fig. 6(b). Using some post-processing operations better results can be achieved.

Robustness to Resizing

In this experiment image is reduced to 75% of its original size. For this purpose MATLAB function "`imresize`" (`imresize(x,1-1/4,'nearest')`) is used. In this process fine detail are lost since subsampling of the image requires a lowpass spatial filtering operation. In order to recover the watermark, reduced image using the same function (`imresize(y,1+1/3,'bicubic')`) is rescaled back to the same size of the original image. Fig. 7 shows the extracted watermark.

5. CONCLUSION

In this paper, a wavelet-based watermarking method was proposed. As a digital watermark binary pattern was used. Wavelet transform was used to obtain multiresolution decomposition of the host image and of the watermark. The method of embedding the watermark is the same as



(a) (b)

Figure 6. (a) Extracted watermark of cropped version of the watermarked image (Fig. 3(b)). 75% of image is missing (*SIM* = 1). (b) Extracted watermark of the cropped version of the wavelet based compressed image with compressed ratio 8:1. 75% of image is missing (*SIM* = 0.72).

Figure 7. Extracted watermark of rescaled watermarked image shown in Fig. 3(b) where 25% reduction/ enlargement is done (*SIM* = 0.20)

spread spectrum watermarking method, and different embedding equations in different frequency bands were used. A multeresolution nature of wavelet transform can be exploit in the process of detection. Experimental results show that the proposed watermarking method results in almost invisible difference between the watermarked image and the original image. Moreover, proposed watermarking method is robust to DCT and DWT based lossy image compression schemes, and some geometric manipulations like image resizing and cropping.

6. REFERENCES

[1] I. Cox, J. Kilian, F.T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia, " *IEEE Trans. Image Processing* vol. 6, December 1997, pp. 1673-1689.

[2] C.-T. Hsu and J.-L. Wu, " Multiresolution watermarking for digital images, " *IEEE Trans. Circuits Syst. II,* vol. 45, August 1998, pp. 1097-1101.

[3] S. G. Mallat, "Multifrequency channel decomposition of images and wavelet models,'' *IEEE Trans. Acoust., Speech, Signal Processing,* vol. 37, December 1989, pp. 2091-2110

[4] G. Strang and T. Nguyen, *Wavelets and Filter Banks.* Wallesley, MA: Wellesley-Cambrige Press, 1996.

[5] Software for image compression: http://saigon.ece.wisc.edu/~waveweb/QMF.html