Robust watermarking of color images based on the Discrete Wavelet Transform

Ovidiu COSMA
Department of Mathematics and Computer Science
North University Center
Baia Mare, Roumania
e-mail: ovidiu.cosma@yahoo.com

***Abstract*—This article presents a method of semi-blind watermarking based on the discrete wavelet transform, that uses the chrominance components of the image for watermark embedding. The watermark is resistant to usual image processing operations such as compression, noise addition, cropping, histogram adjustment and filtering.**

Keywords—watermarking;discrete wavelet transform

I. INTRODUCTION

Watermarking is a technique of embedding secret data within an image, in such a way that their subsequent detection is possible. Depending on robustness, the watermarking techniques are divided into 3 categories: fragile, semi-fragile and robust. Fragile watermarks are destroyed by the tiniest changes to the image data, performed by operations such as compression, noise addition, filtering and geometric distortions. The applications of these techniques are authentication and integrity checking. Semi-fragile watermarks can withstand some of these changes, such as compression and noise. Robust techniques are designed to withstand strong image processing operations. Removing the watermark would require in this case significant changes to the image data that would induce unacceptable distortions. The applications of robust watermarking are copy control and monitoring.

Depending on the detection mode, there are three types of watermarks: non-blind, semi-blind and blind. For detection of a non-blind watermark both the original image and watermark are required. For semi-blind watermark detection, only the watermark is needed and in the case of a blind watermark nothing else is required besides the image that contains the watermark.

The watermark embedding process can be performed in the spatial domain, or in a transform domain. Spatial domain watermarking requires either modification of some pixels, or changing other features of the image in such a way that the watermark remains invisible. Transform domain watermarking places the secret data in the transform coefficients, making it more robust and hard to detect. Some of the most common transforms used in digital image watermarking are the discrete cosine transform (DCT) and the discrete wavelet transform (DWT).

II. DISCRETE COSINE TRANSFORM WATERMARKING

A robust watermark embedding method that is based on DCT is presented in [1]. The image is divided into blocks for which the DCT is calculated and the watermark is placed into a set of the coefficients selected so that the induced distortions may not be visible. Since the watermark is placed in a multitude of harmonics, this method was called spread spectrum watermarking. The watermark is represented by a set of real numbers randomly generated with a normal distribution and mean 0. The variants expressed by (1), (2) and (3) are proposed in [1] for watermark embedding, where v_i are the transform coefficients, x_i are the watermark elements and $\propto$ is a constant.

$$v_i' = v_i + \propto x_i \tag{1}$$

$$v_i' = v_i(1 + \propto x_i) \tag{2}$$

$$v_i' = v_i(e^{\propto x_i}) \tag{3}$$

The first variant is considered unsuitable for situations where the x_i coefficients vary widely, as in the case of DCT, because small changes to large coefficients could be lost, and significant changes applied to small coefficients could cause noticeable distortions. The results presented in [1] correspond to the embedding variant in (2), with constant $\propto = 0.1$ and watermarks of 1000 elements.

The watermark checking is performed in a non - blind manner that contains the following two steps:

1. Extraction of the watermark X^* based on relation (2), using the original and the watermarked image data.
2. Estimation of the similarity between the original watermark X and the extracted one X^* using relation (4).

$$sim(X, X^*) = \frac{X^* \cdot X}{\sqrt{X^* \cdot X^*}} \tag{4}$$

III. DISCRETE WAVELET TRANSFORM

The DWT decomposes an image into a number of sub-bands in which the elements represent the details of the image at a certain scale [2]. The first sub-band contains the details of the image at the largest scale and the last one contains the finest details of the image. The last sub-band contains the largest number of coefficients, thus providing enough space to place hidden data. This area is the ideal location to put a fragile watermark since the fine details are altered by the smallest changes to the image, such as for example compression, adding noise or smoothing. The first sub-bands are suitable in the case of robust watermarks. They, however, have a smaller number of coefficients and their alteration can produce distortions much more noticeable to the naked eye.

IV. COLOR SPACES

The color of each pixel on the computer screen is synthesized using three separate stimuli of red, green and blue colors, with appropriate dosed intensities. Every nuance on the computer screen corresponds to a point in a three-dimensional space, with the axes red green and blue. This color space is called Red Green Blue (RGB) [4]. The luminance chrominance color spaces are more advantageous for digital image processing because the light intensity is separated from color. They are all three-dimensional color spaces in which one of the axes (Y) is the luminance and the other two contain the color information [5]. These color spaces have the advantage of enabling the speculation of the human eye characteristics, which has a much better sensitivity to light than color. Therefore the two chrominance components are the perfect place to hide secret data because the afferent distortions will be more difficult to spot with the naked eye than those induced by the change of the luminance component.

The most popular luminance chrominance color spaces are YIQ, YUV and YCbCr [5]. The luminance (Y) component has been deduced experimentally and is identical for all these color spaces. For converting an RGB image into a luminance chrominance color space the linear transform specified in (5) is applied.

$$\begin{bmatrix} Y \\ C_1 \\ C_2 \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ cr_1 & cg_1 & cb_1 \\ cr_2 & cg_2 & cb_2 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} = A \begin{bmatrix} R \\ G \\ B \end{bmatrix} \quad (5)$$

The sum of the coefficients on the first line of the transformation matrix is 1, and the sums of the coefficients on lines 2 and 3 are 0. Thus if R = G = B, $C_1 = C_2 = 0$ and Y = R = G = B, so the image has no colors.

The inverse transformation is based on (6). Due to the properties of the transformation matrix A, the elements of the first column in A^{-1} are all equal to 1. Thus if $C_1 = C_2 = 0$, R = G = B = Y.

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = A^{-1} \begin{bmatrix} Y \\ C_1 \\ C_2 \end{bmatrix} \quad (6)$$

When using the two chrominance components as secret data container, the watermarking operation is closely related to the color space. The watermark cannot be extracted if the color space used in the insertion process is unknown. To make it more difficult for third parties to detect the watermark, the insertion process can use an original color space, different from the well-known ones. The transformation matrix shown in (7) was used for the experiments presented in this article [3].

$$A = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.2 & -0.6 & 0.8 \\ -1.1 & 1.1 & 0 \end{bmatrix} \quad (7)$$

V. RELATED WORK

A watermarking scheme that is robust to a wide range of attacks is presented in [8]. The proposed method is based on DWT and Singular Value Decomposition (SVD). After image decomposition with DWT, the SVD is applied to the subbands and the watermark is embedded by modifying the singular values. The given results show that the method is resistant to a wide variety of attacks. A blind watermarking scheme that is robust against compression, histogram and spectrum spreading, noise addition and rotation is presented in [9]. The watermark is inserted by adding edges in the HH subband of the host image. A non-blind watermarking method that uses the LL subband of images is presented in [10]. To avoid image degradation, only the visually insensitive locations are used for storing the watermark. The technique of adding and extracting the watermark resembles the one proposed in [1], but using DWT coefficients for storing the watermark leads to better performance. A method for inserting a watermark in the image subbands corresponding to different scales is presented in [11]. The watermark is inserted using a secret key that is required in the watermark extraction process. The method is tested on color and grey-scale images and is robust to some image processing operations. A non-blind watermarking technique based on multiresolution fusion that uses a model of the Human Visual System (HVS) is presented in [12]. The authors show that the proposed method is robust against the usual image tampering techniques.

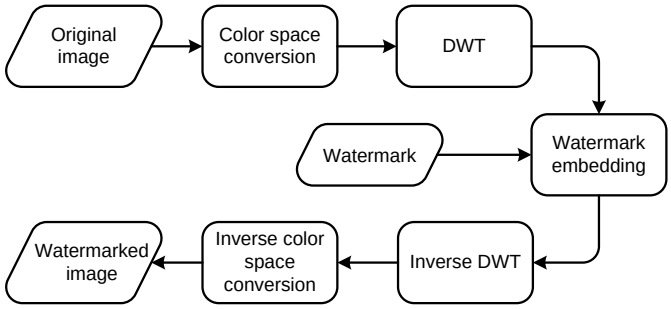
VI. WATERMARK EMBEDDING

The watermark embedding process is shown in Fig. 1. The color space conversion block converts the original RGB image into a luminance chrominance color space. The next block performs the DWT. For the experiments in this article the Villasenor 18/10 biorthogonal filter was used [6]. The Watermark embedding block acts on the two chrominance components, leaving the luminance component unchanged.

The wavelet transform has the property of energy invariance. The changes performed on the transform coefficients are proportionally reflected in the reconstructed image and are not related to the size or position of those coefficients [2]. In the case of using DCT, a method for selecting the coefficients that are suitable for watermarking is required [1]. Because of the wavelet transform properties, this

operation is not necessary, all coefficients in a sub-band or in multiple sub-bands can be used for watermarking.

Fig. 1. Watermark embedding



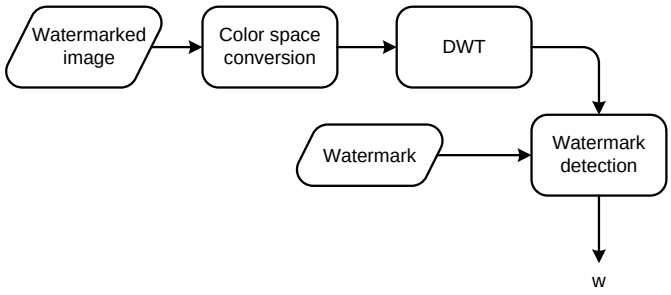
The proposed variant uses relation (1) for inserting the watermark in the fifth sub-band coefficients of the chrominance components. This sub-band was chosen because it has a sufficient number of coefficients (16x16x3 = 768) [7] and corresponds to average frequencies that will confer robustness to the watermark. The components of this sub-band are not affected to a large extent by the usual image processing operations that strongly affect the fine details of the image. If both of the chrominance components are used, then 1536 coefficients are available. The watermark is a set of randomly generated real numbers with 0 mean and normal distribution.

The $\propto$ constant in (1) was chosen so that the watermark will be strong enough to withstand the possible transformations of the image, but it does not create visible distortions. Distortions become visible at around $\propto = 80$. A watermark intensity constant $\propto = 50$ corresponds to invisible distortions.

VII. Watermark Detection

The watermark detection process is presented in Fig.2. It is a semi-blind operation, so only the watermark coefficients are need, and not the entire original image.

Fig. 2. Watermark detection



The detection of the watermark is based on relation (8), where v_i^* are the DWT coefficients of the watermarked image, and x_i are the elements of the watermark. The result $w(X, V^*)$ is the trust level corresponding to the presence of the watermark X in the image V^*.

$$w(X, V^*) = \sum_{i=1}^{n} v_i^* x_i \quad (8)$$

VIII. Experimental Results

Since the watermark is embedded in the chrominance components, images with varied content of colors were used in the evaluation process. The image shown in Fig. 3 was marked with 100 randomly generated watermarks, of intensity $\propto = 50$. The trust levels w obtained in the detection process are shown in Fig. 4. The average of the trust level w always stood very close to the watermark intensity expressed by constant $\propto$.

Fig. 5 shows the results for the detection of a watermark that was previously embedded in the image, and 100 other randomly generated watermarks. The embedded watermark was correctly detected, with $w \approx \alpha$, and for all the other watermarks the trust level was situated below the threshold of 15.

The next experiment demonstrates the strength of the method in the case of JPEG image compression. Fig 6 shows the watermarked image after compression with JPEG at a compression ratio of 77. The size of the compressed image is only 10kB. Fig. 7 shows the calculated trust level for the existing watermark and another 100 randomly generated ones. Only for existing watermark the trust level stood well above the threshold of 15, and still close to the watermark intensity $\propto = 50$.

For the next experiment, random noise was added over the watermarked image, resulting in a distorted image with the peak signal-to-noise ratio (PSNR) of 11.14. The noisy image is presented in Fig. 8. The results of the watermark detection process are presented in Fig. 9. The correct watermark was easily detected but for the random ones the computed trust levels were greater than in previous cases. To avoid false detections, the threshold was raised to 30.

Fig. 3. Test image

Fig. 4. Positive detection of random watermarks.

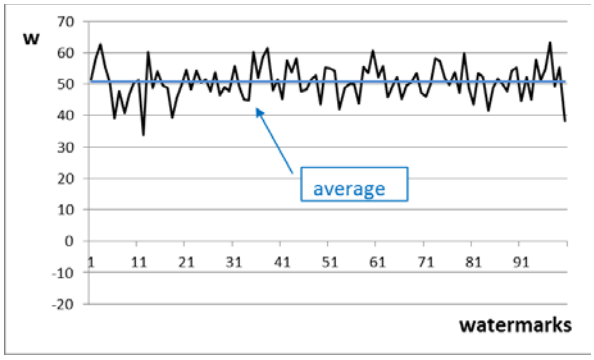


Fig. 5. Negative detection of random watermarks.

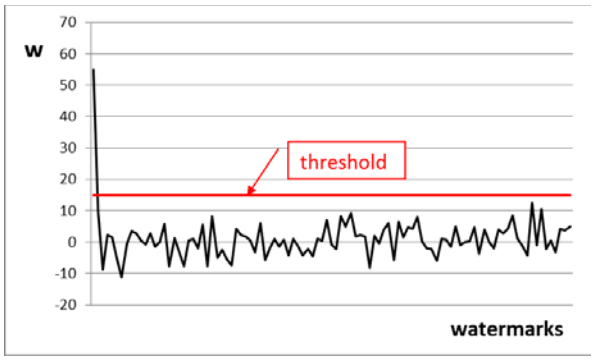


Fig. 6. JPEG compression of watermarked image.

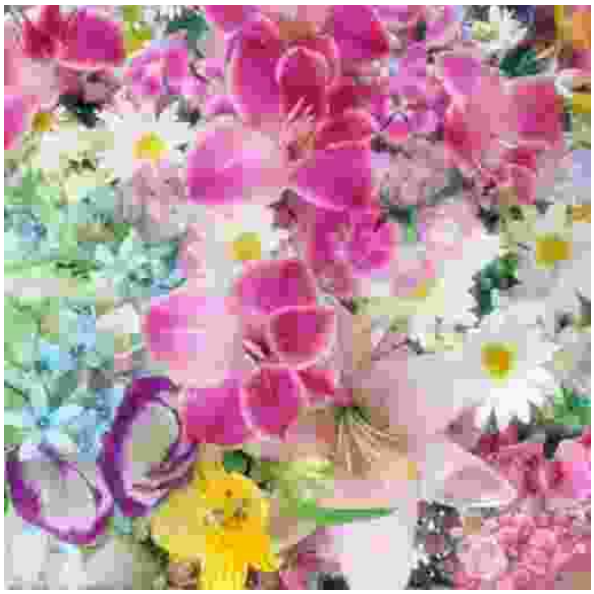


Fig. 7. Watermark detection after JPEG compression.

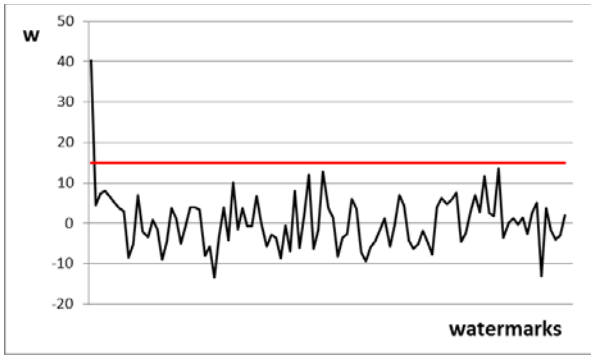
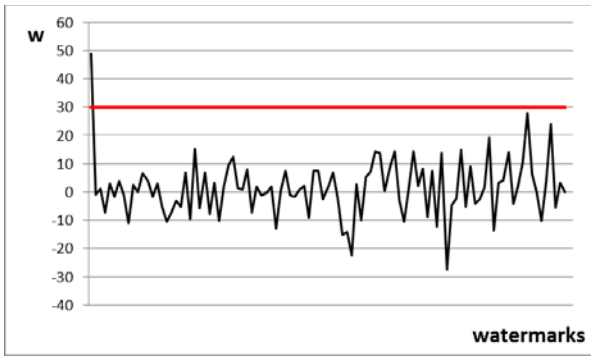


Fig. 8. Watermarked image with added noise.

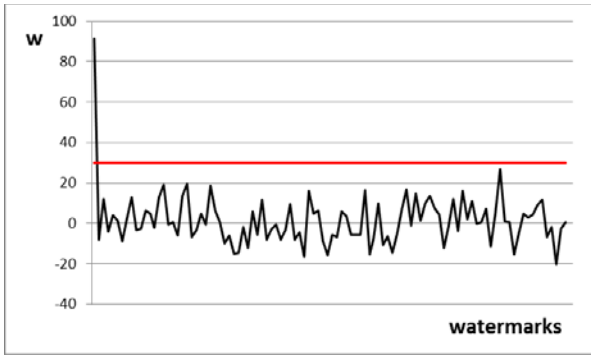
Fig. 9. Watermark detection after noise addition.



In the next experiment, the three components (RGB) of the watermarked image have undergone a histogram normalization process. The resulting image is shown in Fig. 10. and the results of the watermark detection are shown in Fig. 11. In this case the correct watermark was detected with ease. All the trust levels computed for the random watermarks were under 15.

Fig. 10. Watermarked image after histogram normalization.

Fig. 11. Watermark detection after histogram normalization.



In the next experiment the watermarked image was cropped so that 30% of the data was lost. The resulting image is presented in Fig. 12. Fig. 13 presents the results of the watermark detection process, based on the cropped image. The trust level for the correct watermark decreased to about half, but for all other watermarks it stood below the threshold of 15.

Fig. 14 and 15 show the watermark detection results after the watermarked image has been processed with two common image filters: the 3 x 3 box filter and the median filter. As well as in the other situations there were no problems in detecting the correct watermark, but in order to avoid false detections, the threshold was raised to 30, as an increase in the trust level calculated for some of the random watermarks has been observed.

Fig. 12. Watermarked image after cropping.

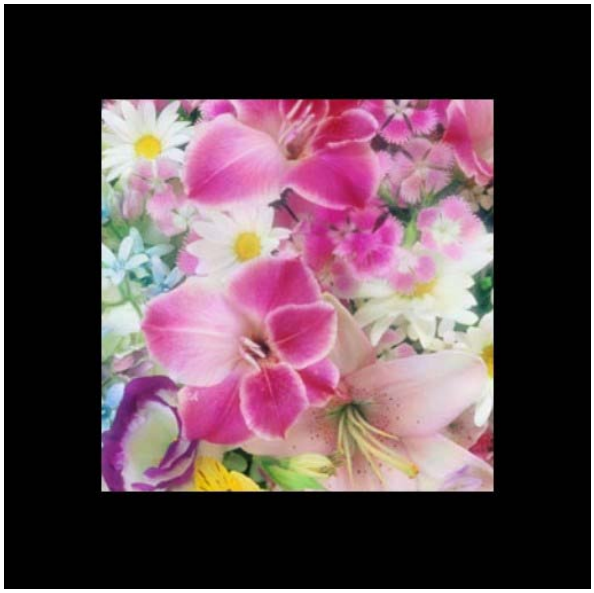


Fig. 13. Watermark detection after cropping.

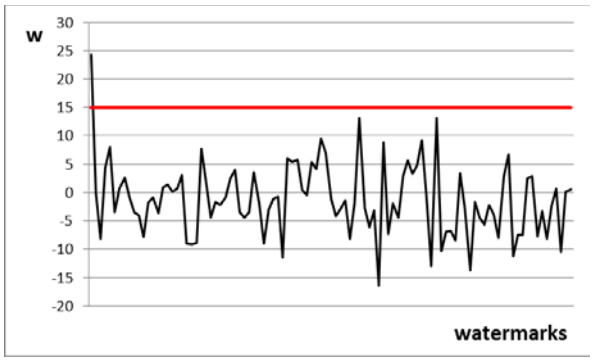


Fig. 14. Watermark detection after applying the box filter.

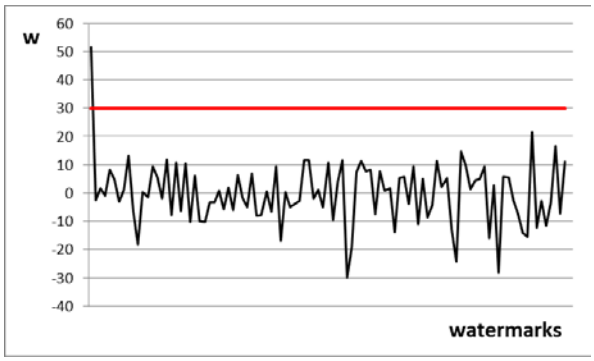
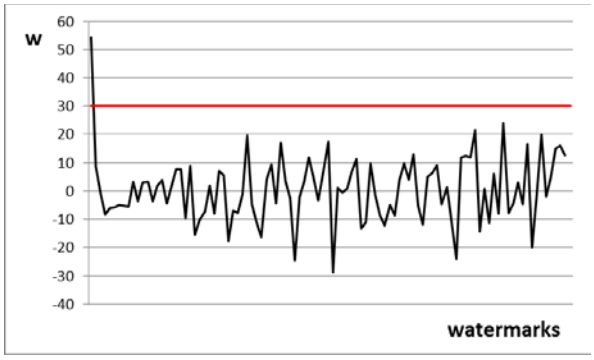


Fig. 15. Watermark detection after applying the median filter.



IX. CONCLUSIONS

Using the chrominance components as container allows placing a relatively strong watermark in the middle frequency spectral components, without noticeable effect on the image. Due to the properties of the wavelet transform, there is no need to carefully select the coefficients to be used in the embedding process. All the coefficients in a given subband, or in several subbands can be used. In the proposed method the watermark uniformly covers the entire image without using the fine details. Due to these properties, the watermark is robust; it can withstand the usual image processing operations. One of the features that distinguish the proposed method from most of the other robust DWT based methods is that it is semi-blind. The original image is not required to verify the presence of the watermark.

REFERENCES

[1] Ingemar J. Cox, Joe Kilian, F. Thomson Leighton, and Talal Shamoon, "Secure spread spectrum watermarking for multimedia", IEEE Transactions on Image Processing, vol. 6, no. 12, December 1997, pp.1673-1687.

[2] Eric J. Stollnitz, Tony D. DeRose, and David H. Salesin, "Wavelets for computer graphics", part 1, IEEE Computer Graphics and Applications, vol.15(3), May 1995, pp.76-84.

[3] Ovidiu Cosma, "The deduction and evaluation of a new colour space for image compression", Carpathian Journal of Mathematics, vol. 19, no.1, 2003, pp. 35-40.

[4] Charles Poynton, "A Guided Tour of Color Space", SMPTE Advanced Television and Electronic Imaging Conf. 1995

[5] Adrian Ford, AlanRoberts, "Colour SpaceConversions", http://www.poynton.com/PDFs/coloureq.pdf, August 1998

[6] Signal and Image Processing Group, University of Bath, "The Bath Wavelet Warehouse" , http://dmsun4.bath.ac.uk

[7] Ovidiu Cosma, "Image processing based on the Wavelet Transform", Carpathian Journal of Mathematics, vol. 20, No.2, 2004, pp.155 - 159.

[8] Emir Ganic, Ahmet M. Eskicioglu, "Robust DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies", MM & SEC 2004, September 20-21, Magdeburg, Germany

[9] Henri Bruno Razafindradina, Attoumani Mohamed Karim, "Blind and robust images watermarking based on wavelet and edge insertion", International Journal on Cryptography and Information Security (IJCIS), Vol.3, No. 3, September 2013, pp 23-30.

[10] Sanghyun Joo, Youngho Suh, Jaeho Shin, and Hisakazu Kikuchi, "A New Robust Watermark Embedding into Wavelet DC Components," ETRI Journal, vol. 24, no. 5, Oct. 2002, pp. 401-404.

[11] Yasuhiko Dote, Muhammad Shafique Shaikh, "A Robust Watermarking Method for Copyright Protection of Digital Images using Wavelet Transformation" Trans. of the Institute of Electrical Engineering of Japan, vol. 122, No.2, Jan. 2003.

[12] Deepa Kundur, Dimitrios Hatzinakos, "A Robust Digital Image Watermarking Method using Wavelet-Based Fusion", Proceedings of International Conference on Image Processing, Santa Barbara, CA 1997, Vol.1, pp. 544 - 547