

# A Semi-Blind Watermarking Scheme for Color Images Using a Tree Structure

Ersin Elbasi<sup>a</sup> and Ahmet M. Eskicioglu<sup>b</sup>

<sup>a</sup>The Graduate Center, The City University of New York  
365 Fifth Avenue, New York, NY 10016

<sup>b</sup>Department of Computer and Information Science, Brooklyn College  
The City University of New York, 2900 Bedford Avenue, Brooklyn, NY 11210  
eelbasi@gc.cuny.edu, eskicioglu@sci.brooklyn.cuny.edu

## ABSTRACT

In this paper, we use a tree structure to embed the watermark in DWT decomposition. In the watermark embedding algorithm, the RGB image is first converted to the YUV model. After computing the DWT of the luminance layer, the same PRN sequence is embedded into the DWT coefficients higher than a given threshold  $T_1$  in the LL2 and HH2 bands. The PRN sequence is then embedded into the children of the DWT coefficients in the LL2 and HH2 bands. In the final step, the inverse DWT is computed to obtain the watermarked image  $I$ . In the watermark detection algorithm, the watermarked RGB (and possibly attacked) image is converted to the YUV model. After computing the DWT of the luminance layer, all the DWT coefficients higher than a given threshold  $T_2$  in the LL2 and HH2 bands are selected. The next step is to compute the sum  $Z$ , where  $i$  runs over all DWT coefficients higher than a given threshold  $T_2$  in the LL2 and HH2 bands. This is repeated for the children of modified DWT coefficients in the previous step. In the final step, a predefined threshold  $T$  is chosen for LL and HH bands. In each band, if  $Z$  exceeds  $T$ , the watermark is present. Experimental results indicate that detection in the LL band is robust for one group of attacks, and detection in the HH band is robust for another group of attacks. In future work, we will use this approach to watermark video sequences.

Keywords: semi-blind image watermarking, tree structure, discrete wavelet transform, LL band, HH band.

## 1. INTRODUCTION

Multimedia can be defined to be the combination and integration of more than one media format (e.g., text, graphics, images, animation, audio and video) in a given application. Content owners (e.g., movie studios and recording companies) have identified two major technologies for the protection of multimedia data: encryption and watermarking [1,2,3].

A digital watermark is a pattern of bits inserted into a multimedia element such as a digital image, an audio or video file. In particular, watermarking appears to be useful in plugging the analog hole in consumer electronics devices. In applications such as owner identification, copy control, and device control, the most important properties of a watermarking system are robustness, invisibility, data capacity, and security.

In a classification of image watermarking schemes, several criteria can be used. Three of such criteria are the type of domain, the type of watermark, and the type of information needed in the detection or extraction process.

According to the domain type, we have pixel domain and transform domain watermarking schemes. In the pixel domain, the pixel values are modified to embed the watermark. In the transform domain, the transform coefficients are modified to embed the watermark.

According to the watermark type, we have pseudo-random number (PRN) sequence (having a normal distribution with zero mean and unity variance) and a visual watermark. The PRN sequence allows the detector to statistically check the presence or absence of a watermark, whereas the watermark is actually reconstructed, and its visual quality is evaluated.

According to the information type needed in the detection or extraction process, we have blind schemes, semi-blind schemes, and non-blind schemes. In the blind schemes, only the secret key(s) are needed. In the semi-blind schemes, the watermark and the secret key(s) are needed. In the non-blind schemes, both the original image and the secret key(s) are needed.

In [6], a blind watermarking technique for digital images is described. The authors use a technique to construct an image-dependent watermark in the discrete wavelet transform (DWT) domain and to insert the watermark in the most significant

coefficients of the image. The watermarked coefficients are determined by using the hierarchical tree structure induced by the DWT, similar in concept to embedded zerotree wavelet (EZW) compression. If the watermarked image is attacked or manipulated such that the set of significant coefficients is changed, the tree structure allows the correlation-based watermark detector to recover synchronization. Most of the proposed algorithms in transform domain watermarking are robust for one group of attacks [2,3,6]. In this paper, we proposed a novel technique which is robust against a larger group of attacks with detection both two bands in wavelet domain: LL and HH.

The proposed watermark embedding and detection algorithms are as follows:

#### Watermark embedding

1. The RGB image is converted to the YUV model.
2. Compute the DWT of the luminance layer.
3. Compute the two level DWT decomposition of the  $N \times N$  luminance layer.
4. Embed the same PRN sequence into the DWT coefficients higher than a given threshold  $T_1$  in the LL2 and HH2 bands:  
 $T = \{t_i\}$ ,  $t'_i = t_i + \alpha|t_i|x_i$ , where  $i$  runs over all DWT coefficients  $> T_1$ .
5. Embed the PRN sequence into the children of the DWT coefficients in Step 4.
6. Replace  $T = \{t_i\}$  with  $T' = \{t'_i\}$  in the DWT domain.
7. Compute the inverse DWT to obtain the watermarked image  $I'$ .

#### Watermark detection

1. The watermarked RGB (and possibly attacked) image is converted to the YUV model.
2. Compute the DWT of the luminance layer.
3. Select all the DWT coefficients higher than a given threshold  $T_2$  in the LL2 and HH2 bands.
4. Compute the sum  $Z = \frac{1}{M} \sum_{i=1}^M y_i t_i^*$ , where  $i$  runs over all DWT coefficients higher than a given threshold  $T_2$  in the LL2 and HH2 bands, and  $M$  is the length of the PRN sequence,  $\{y_i\}$  represents either the real watermark or a fake watermark,  $\{t_i^*\}$  represents the watermarked and possibly attacked DWT coefficients.
5. Compute the sum  $Z = \frac{1}{M} \sum_{i=1}^M y_i t_i^*$  for the children of modified DWT coefficients in Step 4.
6. Choose a predefined threshold  $T = \frac{\alpha}{2M} \sum_{i=1}^M |t_i^*|$  for LL and HH bands.
7. In each band, if  $Z$  exceeds  $T$ , the conclusion is that the watermark is present.

## 2. EXPERIMENTS

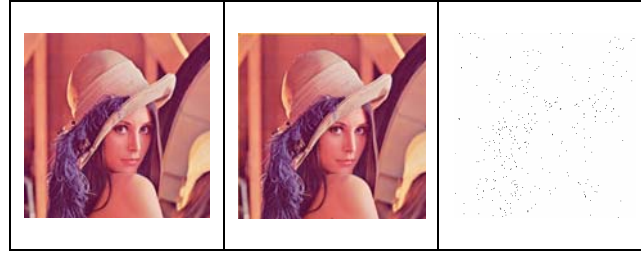
Several orthogonal wavelet filters such as the Haar filter or the Daubechies filters can be used to compute the DWT. In our experiments, we obtained the second level decomposition using the Haar filter.

The values of  $\alpha$  and the threshold for each band are given in *Table 1*.

*Table 1. Scaling factor  $\alpha$  and threshold  $T$*

Parameters/Bands	LL	HH
$\alpha$	0.5	3.6
$T_1$	10	40
$T_2$	20	50

In *Figure 1*, the original host image, the watermarked host image, and their difference are displayed.



(a) Original Lena (b) Watermarked Lena (c) Difference

Figure 1. Embedding two watermarks into an image

Matlab was used for all attacks. The chosen attacks were JPEG compression, resizing, adding Gaussian noise, low pass filtering, rotation, histogram equalization, contrast adjustment, gamma correction, and cropping.

In Figures 2 to 11, we display the detector responses for the real watermark, and 99 randomly generated watermarks. In each figure, the correlation with the real watermark is located at 80 on the  $x$ -axis, and the dotted line shows the value of the threshold.

### 3. CONCLUSION

We have presented a robust semi-blind color image watermarking scheme in DWT domain using tree structure.

Our experiments show that for one group of attacks (JPEG compression, adding Gaussian noise, resizing, low pass filtering, and rotation), the correlation with the real watermark is higher than the threshold in the LL band, and for another group of attacks (cropping, histogram equalization, contrast adjustment, and gamma correction), the correlation with the real watermark is higher than the threshold in the HH band. Watermark detection from both LL band and HH band is more robust against to all type of attacks than other algorithms.

In future work, we will use this approach to watermark video sequences such as akiyo, flower garden, and tennis.

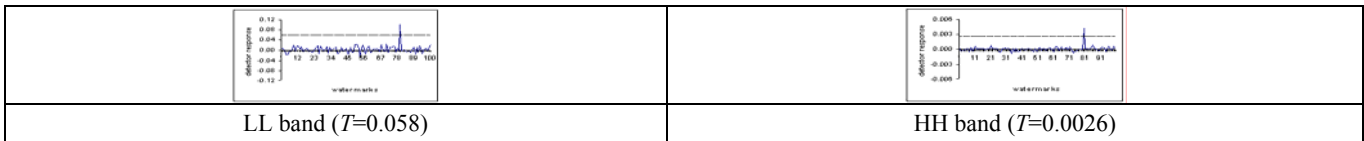


Figure 2. Detector response for unattacked watermarked Lena

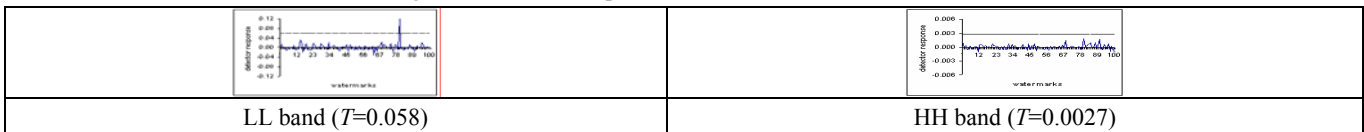


Figure 3. Detector response for JPEG compression: Q=25

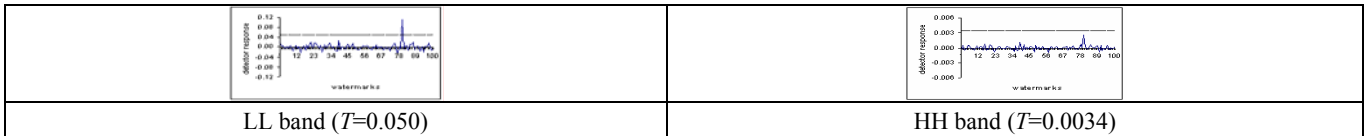


Figure 4. Detector response for Gaussian noise

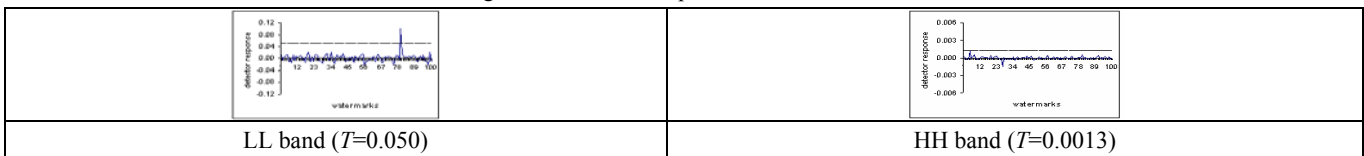


Figure 5. Detector response for resizing

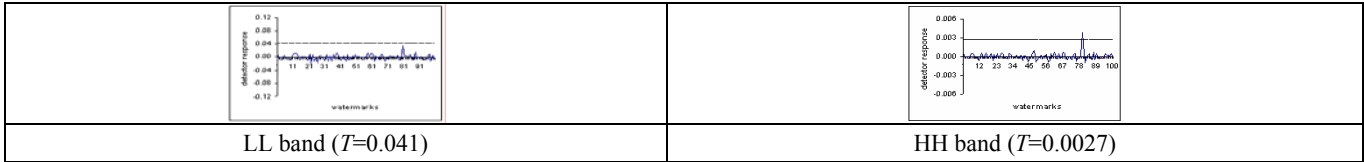


Figure 6. Detector response for cropping



Figure 7. Low pass filtering

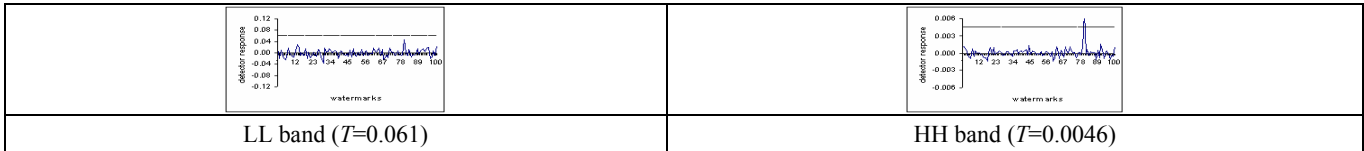


Figure 8. Detector response for histogram equalization

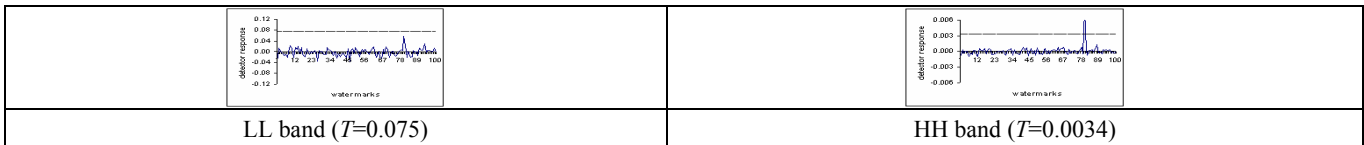


Figure 9. Detector response for contract adjustment

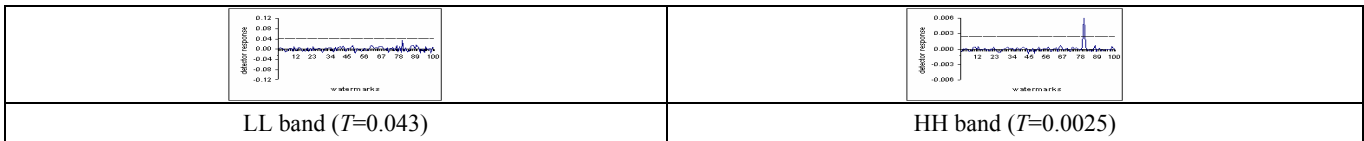


Figure 10. Detector response for gamma correction

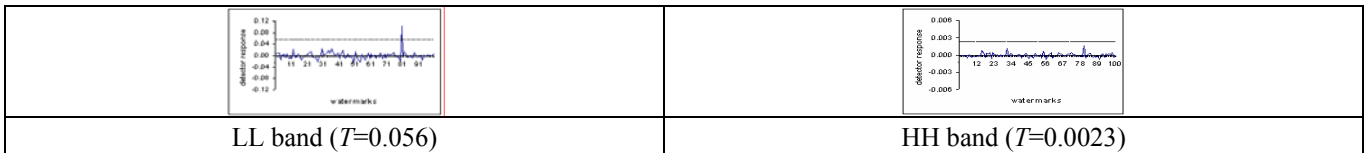


Figure 11. Rotation ( $5^0$ )

#### 4. REFERENCES

1. A. M. Eskicioglu and E. J. Delp, "Overview of Multimedia Content Protection in Consumer Electronics Devices," *Signal Processing: Image Communication*, 16(7), pp. 681-699, April 2001.
2. R. Dugad, K. Ratakonda, and N. Ahuja, "A New Wavelet-Based Scheme for Watermarking Images," *Proceedings of 1998 International Conference on Image Processing (ICIP 1998)*, Vol. 2, Chicago, IL, October 4-7, 1998, pp. 419-423.
3. I. J. Cox, J. Kilian, T. Leighton and T. Shamon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions on Image Processing*, 6(12), December 1997, pp. 1673-1687.
4. W. Zhu, Z. Xiong and Y.-Q. Zhang, "Multiresolution Watermarking for Images and Video," *IEEE Transactions on Circuits and Systems for Video Technology*, 9(4), June 1999, pp. 545-550. [3]
5. C.-H. Lee and Y.-K. Lee, "An Adaptive Digital Image Watermarking Technique for Copyright Protection," *IEEE Transactions on Consumer Electronics*, 45(4), November 1999, pp. 1005-1015.
6. O. G. Pla, E. T. Lin, E. J. Delp, "A Wavelet Watermarking Algorithm Based on a Tree Structure," *Proceedings of SPIE Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI*, Vol. 5306, pp. 725-736, San Jose, CA, January 18-22, 2004.