PRN BASED WATERMARKING SCHEME FOR COLOR IMAGES

Ersin ELBAŞI[*] , Ahmet M. ESKİCİOĞLU[**]

ABSTRACT

Robust image watermarking is the process of embedding an invisible watermark in an image in order to make it very difficult to remove the watermark after intentional attacks and normal audio/visual processes. A recent DWT-based semi-blind image watermarking scheme leaves out the low pass band, and embeds the watermark in the other three bands into the coefficients that are higher than a given threshold T_1. During watermark detection, all the high pass coefficients above another threshold T_2 ($T_2 > T_1$) are used in correlation with the original watermark. In our extension to the DWT-based approach, we embed the same watermark in two bands (LL and HH) using different scaling factors for each band. 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 T2 in the LL and HH bands are selected. The next step is to compute the sum Z, where i runs over all DWT coefficients higher than a given threshold T2 in the 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.

Keywords: Semi-Blind Image Watermarking, Discrete Wavelet Transform, LL Band, HH Band, Attacks

PRN'a BAĞLI RENKLİ RESİM DAMGALAMA METODU

ÖZET

Dayanikli resim damgalama gorunmeyen damganin kasitli saldiri ve goruntu islemlerinden sonra damganin silinmesini oldukca zorlastiran resimlere gomulmesi islemidir. DWT ile yapilan yari-kor resim damgalama yontemi LL bantini disari atip, digger uc bandin daha onceden belirlenen basmaktan buyuk katsayilarina gomme yapilir. Damga Ortaya cikarma esnasinda ise, uc banttaki T2'den buyuk katsayilarin gercek damga ile korelasyonu hesaplanir. Bizim genisletilmis DWT algoritmamizda ayni damgayi LL ve HH bantlarina farkli katsayilar kullanarak gommekteyiz. Damga tespitinde ise damgalanmis RGB (ve saldirilmis olmasi mumkun) resim YUV resim modeline cevrilir. Luminance tabakasi DWT'ye cevrildikten sonra T2'den buyuk LL ve HH bantlari katsayilari secilir. Sonraki adimda ise toplam Z degeri hesaplanir bu katsayilar icin. Eger Z degeri T degerinden buyuk ise resim damgalanmis, aksi takdirde damgalanmamis demektir. Deney sonuclarimiz LL bantta gommek bir grup saldiriya karsi dayanikli olurken, HH banta gomme diger bir grup saldiriya karsi dayanikli olmaktadir.

Anahtar Kelimeler: Yarı- Kör Resim Damgalama, DWT, LL Bant, HH Bant, Saldırılar

[*] *The Graduate Center, The City University of New York 365 Fifth Avenue, New York, NY 10016 eelbasi@gc.cuny.edu*

[**] *Professors, Department of Computer and Information Science, Brooklyn College The City University of New York, 2900 Bedford Avenue, Brooklyn, NY 11210 eskicioglu@sci.brooklyn.cuny.edu*

1. INTRODUCTION

Content owners (e.g., movie studios and recording companies) have identified two major technologies for the protection of multimedia data: encryption and watermarking (Eskicioğlu and Delp, 2001). 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.

The most important properties of a watermarking system are robustness, invisibility, data capacity, and security. An embedded watermark should not introduce a significant degree of distortion in the cover multimedia element. Robustness is the resistance of the watermark against normal A/V processes or intentional attacks (Elbasi and Eskicioğlu, 2006). Data capacity refers to the amount of data that can be embedded without affecting perceptual transparency. The security of a watermark can be defined to be the ability to thwart hostile attacks such as unauthorized removal, unauthorized embedding, and unauthorized detection. There are basically two approaches to embed a watermark: spatial domain and transform domain (e.g., DCT, DFT, or DWT). In the spatial domain, the watermark is embedded by modifying the pixel values in the original image. Transform domain watermarking is similar to spatial domain watermarking; in this case, the coefficients are modified. Both methods have advantages and disadvantages: One disadvantage of spatial domain watermarking is that the cropping attack might remove the watermark.

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. Two-dimensional DWT can be implemented using digital filters and downsamplers. Each level of decomposition produces four bands of data denoted by LL, HL, LH, and HH. The LL subband can further be decomposed to obtain another level of decomposition. This process is continued until the desired number of levels determined by the application is reached (Dugad et al., 1998).

Another criteria in watermarking is the watermark type: Visual watermark and PRN sequence. The visual watermark is actually reconstructed, and its visual quality is evaluated. The PRN sequence allows the detector to statistically check the presence or absence of a watermark. A PRN sequence generated by feeding a linear or nonlinear generator with a secret key. However, embedding a meaningful watermark is essential in some applications. This watermark could be a binary image, stamp, logo or label.

2. EMBEDDING and DETECTION

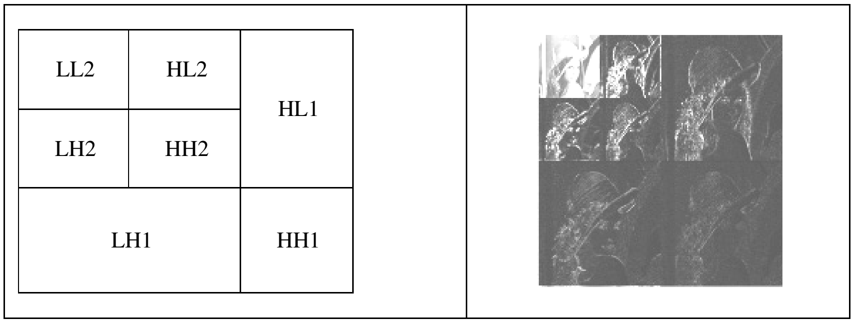
In a recent DCT-domain semi-blind image watermarking scheme (Piva et al., 1997) a pseudo-random number (PRN) sequence is embedded in a selected set of DCT coefficients. The watermark is consisted of a sequence of real numbers $X = \{x_1,x_2,\ldots,x_M\}$, where each value x_i is chosen independently according to $N(0,1)$. $N(\mu,\sigma^2)$ denotes a normal distribution with mean μ and variance σ^2.

In particular, after reordering all the DCT coefficients in a zig-zag scan, the watermark is embedded in the coefficients from the (L+1)st to the (M+L)th. The first L coefficients are skipped to achieve perceptual transparency.

A DWT-based semi-blind image watermarking scheme follows a similar approach (Dugad et al., 1998). Instead of using a selected set of DWT coefficients, the authors leave out the low pass band, and embed the watermark in the other three bands into the coefficients that are higher than a given threshold T_1. During watermark detection, all the high pass coefficients above another threshold T_2 ($T_2 \geq T_1$) are used in correlation with the original watermark.

In both of the above papers, the value of α is chosen as 0.2. In our extension to the DWT-based approach, we embed the same watermark in two bands (LL and HH) using different scaling factors for each band.

Two-dimensional DWT can be implemented using digital filters and downsamplers. Each level of decomposition produces four bands of data denoted by LL, HL, LH, and HH. The LL subband can further be decomposed to obtain another level of decomposition. This process is continued until the desired number of levels determined by the application is reached. Figure 2 shows two levels of decomposition luminance layer of Lena to be watermarked.



(a) (b)

Figure 1. (a) Second Level DWT Decomposition, (b) Second Level DWT Decomposition of Lena

Proposed watermark embedding and detection algorithms can be summarized as follows:

Watermark embedding procedure:

1. Convert the NxN RGB image to YUV.
2. Compute the DWT of the luminance layer.
3. Embed the same PRN sequence into the DWT coefficients higher than a given threshold T_1 in the LL and HH bands: $T = \{t_i\}$, $t'_i = t_i + \alpha|t_i|x_i$, where i runs over all DWT coefficients > T_1.
4. Replace $T = \{t_i\}$ with $T' = \{t'_i\}$ in the DWT domain.
5. Compute the inverse DWT to obtain the watermarked image I'.

Watermark detection procedure:

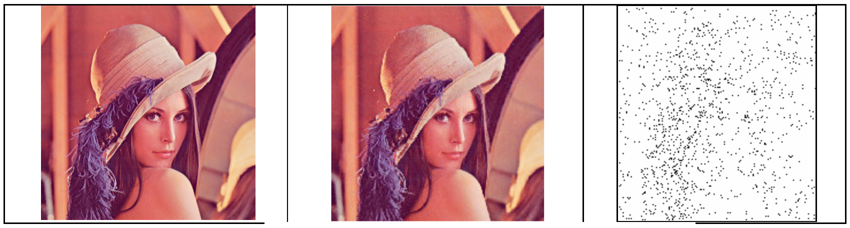
1. Convert the NxN watermarked (and possibly attacked) RGB image to YUV.
2. Compute the DWT of the luminance layer.
3. Select all the DWT coefficients higher than T_2 in LL and HH bands.
4. Compute the sum $z = \frac{1}{M}\sum_{i=1} y_i t_i^*$, where i runs over all DWT coefficients > T_2, y_i represents either the real watermark or a fake watermark, t_i^* represents the watermarked and possibly attacked DWT coefficients.
5. Choose a predefined threshold $T_z = \frac{\alpha}{2M}\sum_{i=1} | t_i^* |$.
6. In each band, if z exceeds T_z, the conclusion is that the watermark is present.

3. 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 first level decomposition using the Haar filter. The values of α and the threshold for each band are given in Table 1.

Table 1. Scaling Factor a and Threshold T

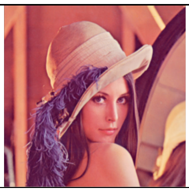
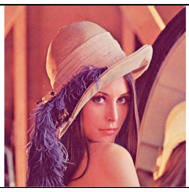
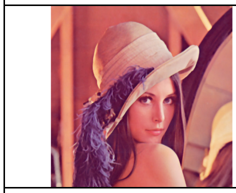
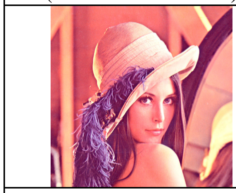
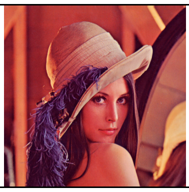
Parameters/Bands	LL	HH
α	0.4	3.5
T_1	15	45
T_2	25	55



Original Lena Watermarked Lena psnr = 46.26 The difference

Figure 2. 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.

		
JPEG compression psnr = 30.21 (Q=25)	Resizing psnr = 31.42 (512 → 256 → 512)	Gaussian noise psnr = 29.32 (mean = 0, variance = 0.001)
		
Low pass filtering psnr = 33.51 (window size=3x3)	Rotation (5^0) psnr = 13.81	Histogram equal. psnr = 17.71 (automatic)
		
Contrast adjustment psnr = 15.55 ([l=0 h=0.8],[b=0 t=1])	Gamma correction psnr = 19.77 (1.5)	Cropping on both sides psnr = 8.31

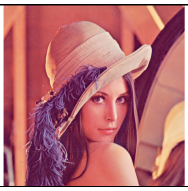
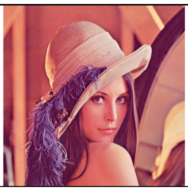
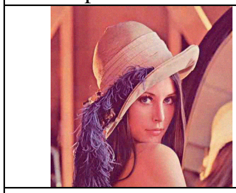
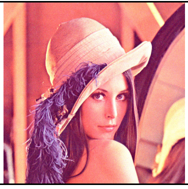
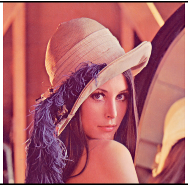
		
Scaling psnr=31.25	Collusion psnr=29.41	Rewatermarking psnr=33.62
		
Jpeg Comp.+gamma Corr. psnr=25.36	Gaussian Noise+Contrast adj. psnr=22.49	Multiple Watermarking psnr=31.08

Figure 3. Attacks on Watermarked Lena

In Figures 4-20 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.

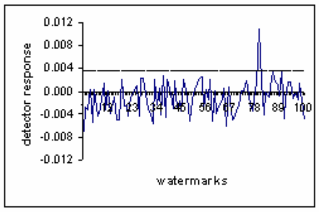
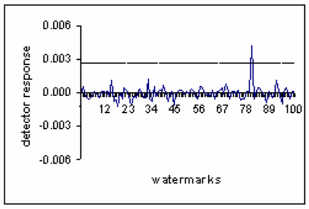
	
LL band (*T*=0.0035)	HH band (*T*=0.0027)

Figure 4. Detector Response for Unattacked Watermarked Lena

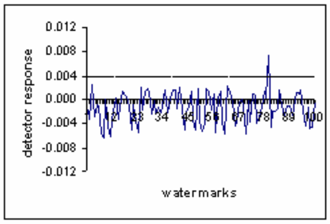
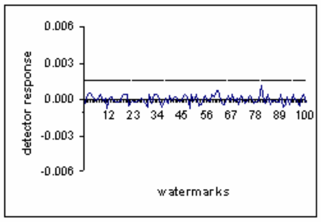
	
LL band (*T*=0.0037)	HH band (*T*=0.0015)

Figure 5. Detector Response for JPEG Compression: Q=25

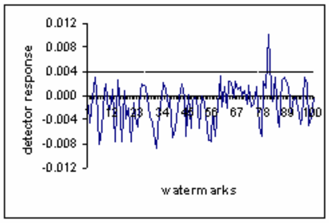
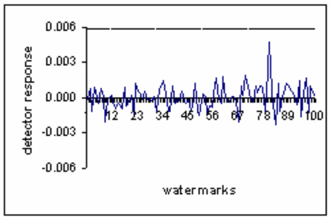
	
LL band (*T*=0.0040)	HH band (*T*=0.0059)

Figure 6. Detector Response for Gaussian Noise

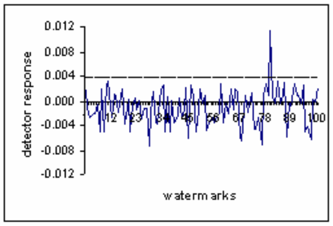
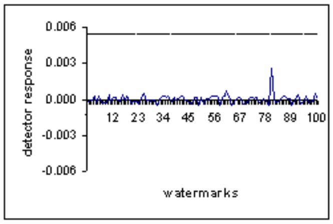
	
LL band (*T*=0.0054)	HH band (*T*=0.0037)

Figure 7. Detector Response for Resizing

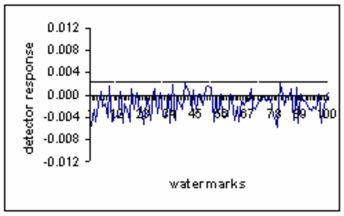
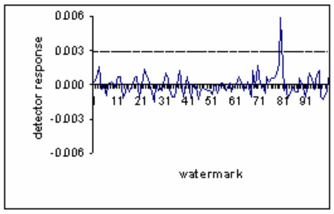
	
LL band (*T*=0.0024)	HH band (*T*=0.0028)

Figure 8. Detector Response for Cropping

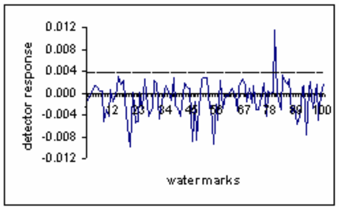
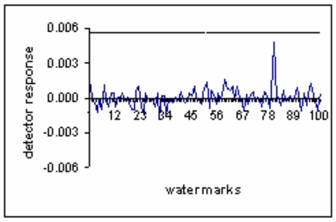
	
LL band (*T*=0.0038)	HH band (*T*=0.0057)

Figure 9. Detector Response for Low Pass Filtering

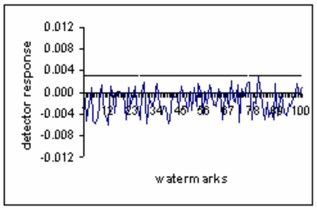
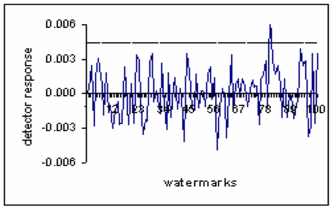
	
LL band (*T*=0.0033)	HH band (*T*=0.0044)

Figure 10. Detector Response for Histogram Equalization

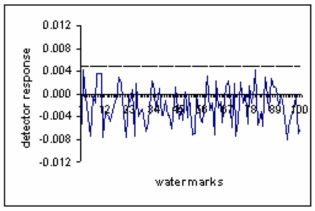
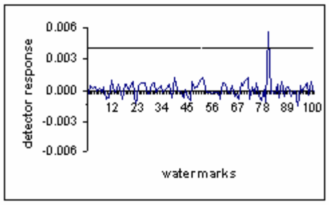
	
LL band (*T*=0.005)	HH band (*T*=0.004)

Figure 11. Detector Response for Contract Adjustment

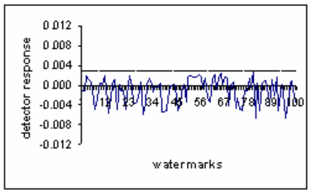
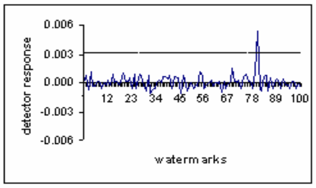
	
LL band (*T*=0.0029)	HH band (*T*=0.0031)

Figure 12. Detector Response for Gamma Correction

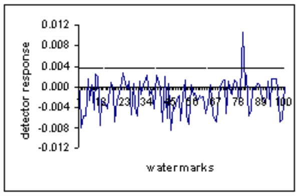
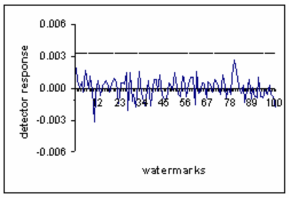
	
LL band (*T*=0.0031)	HH band (*T*=0.0029)

Figure 13. Detector Response for Rotation (5^0)

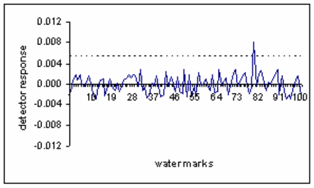
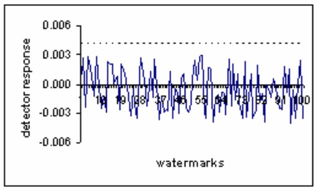
	
LL band (*T*=0.0031)	HH band (*T*=0.0029)

Figure 14. Detector Response for Scaling

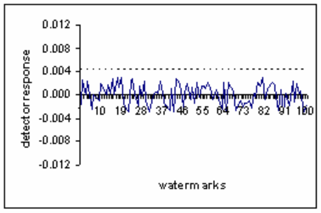
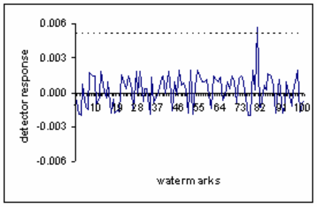
	
LL band (*T*=0.0031)	HH band (*T*=0.0029)

Figure 15. Detector Response for Collusion

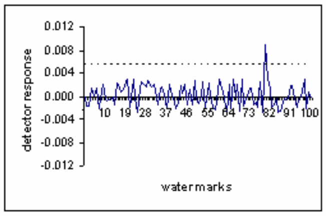
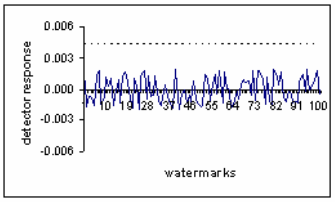
	
LL band (*T*=0.0031)	HH band (*T*=0.0029)

Figure 16. Detector Response for Rewatermarking

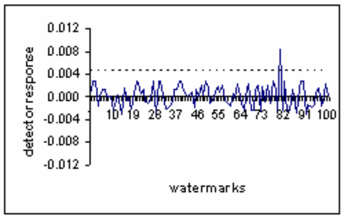
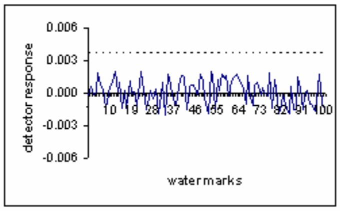
	
LL band (*T*=0.0031)	HH band (*T*=0.0029)

Figure 17. Detector Response for jpeg Compression Gamma Corr.

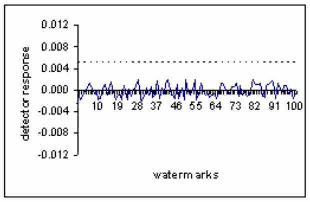
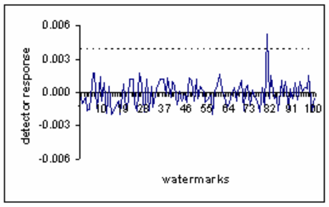
	
LL band (*T*=0.0031)	HH band (*T*=0.0029)

Figure 18. Detector Response for Gausian Noise + Contrast Adj.

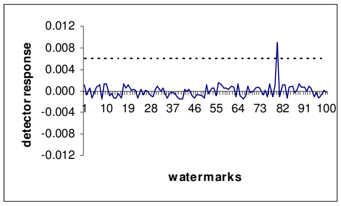
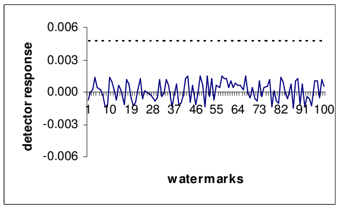
	
LL band (*T*=0.0031)	HH band (*T*=0.0029)

Figure 19. Detector Response for Gausian Noise + Histogram Equ.

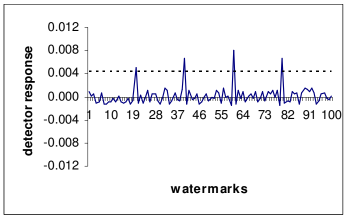
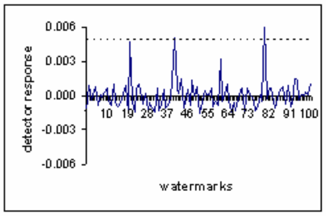
	
LL band (*T*=0.0031)	HH band (*T*=0.0029)

Figure 20. Detector Response for Multiple Watermarking

4. CONCLUSIONS

In this paper, we have extended the idea by embedding the same watermark in two bands (LL and HH) using different scaling factors and thresholds for each band in RGB color images.

In a DWT-based semi-blind image watermarking paper, a watermark is embedded in three bands, leaving out the low pass subband, using coefficients that are higher than a given threshold T_1. During watermark detection, all the high pass coefficients higher than another threshold T_2 ($T_2 \geq T_1$) are chosen for correlation with the original watermark.

Our experiments show that for one group of attacks (JPEG compression, resizing, adding Gaussian noise, 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 (histogram equalization, contrast adjustment, gamma correction, and cropping), the correlation with the real watermark is higher than the threshold in the HH band.

5. REFERENCES

Caldelli R., Barni M., Bartolini F. and Piva A., (2000), "Geometric-Invariant Robust Watermarking through Constellation Matching in the Frequency Domain", Proceedings of the 2000 International Conference on Image Processing (ICIP 2000), Vancouver, BC, Canada, September 10-13, 2000, Vancouver, Vol. II, 65-68.

Cox I. J., Kilian J., Leighton T. and Shamoon T., (1997), "Secure Spread Spectrum Watermarking for Multimedia", IEEE Transactions on Image Processing, 6 (12), 1673-1687.

Dugad R., Ratakonda K., and Ahuja N., (1998), “A New Wavelet-Based Scheme for Watermarking Images”, Proceedings of 1998 International Conference on Image Processing (ICIP 1998), Chicago, IL, Vol. 2, 419-423.

Elbasi E. and Eskicioglu A.M., (2006), “A DWT-based Robust Semi-blind Image Watermarking Algorithm Using Two Bands”, IS&T/SPIE’s 18th Symposium on Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VIII Conference, San Jose, CA.

Eskicioglu A.M. and Delp E.J., (2001), “Overview of Multimedia Content Protection in Consumer Electronics Devices”, Signal Processing: Image Communication, 16 (7), 681-699.

Eskicioglu A. M., Town J. and Delp E. J., (2003), “Security of Digital Entertainment Content from Creation to Consumption”, Signal Processing: Image Communication, Special Issue on Image Security, 18 (4), 237-262.

Langelaar G.C. and Lagendijk R.L., (2001), “Optimal Differential Energy Watermarking of DCT Encoded Images and Video”, IEEE Transactions on Image Processing, 10 (1), 148-158.

Lee C.H. and Lee Y.K., (1999), “An Adaptive Digital Image Watermarking Technique for Copyright Protection”, IEEE Transactions on Consumer Electronics, 45 (4), 1005-1015.

Lin C.Y., Wu M., Bloom J.A., Cox I. J., Miller M. L. and Lui Y. M., (2001), “Rotation, Scale, and Translation Resilient Watermarking for Images”, IEEE Transactions on Image Processing, 10 (5), 767-782.

Liu R. and Tan T., (2002), “A SVD-Based Watermarking Scheme for Protecting Rightful Ownership”, IEEE Transactions on Multimedia, 4 (1), 121-128.

Pereira S. and Pun T., (2000), “Robust Template Matching for Affine Resistant Image Watermarks”, IEEE Transactions on Image Processing, 9 (6), 1123-1129.

Piva A., Barni M., Bartolini F. and Cappellini V., (1997), “DCT-based Watermark Recovering without Resorting to the Uncorrupted Original Image”, Proceedings of the 1997 International Conference on Image Processing (ICIP ’97), Washington, DC, USA.

Zhu W., Xiong Z. and Zhang Y.Q., (1999), “Multiresolution Watermarking for Images and Video”, IEEE Transactions on Circuits and Systems for Video Technology, 9 (4), 545-550.