Two Bands Wavelet Based Robust Semi-Blind Image Watermarking

Ersin Elbasi

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 image watermarking paper embeds a PRN sequence as a watermark in three bands, excluding the low pass subband, using coefficients that are higher than a given threshold. During watermark detection, all the coefficients higher than another threshold are chosen for correlation with the original watermark. In this paper, we extend the idea to embed the same watermark in two bands (LL and HH). Our experiments show that for one group of attacks, the correlation with the real watermark is higher than the threshold in the LL band and for another group of attacks, the correlation with the real watermark is higher than the threshold in the HH band.

Keywords: semi-blind image watermarking, attacks, embedding algorithm, wavelet domain

İki Şeritli Dalgacık Dönüşümü Alanlarında Yarı-Kör Resim Damgalama

ÖZET

Güvenilir resim damgalama metodu görünmeyen damgaları gömme işlemidir.Böylelikle bazı saldırı ve resim işleme metodları ile damgayı silmek zorlaşır.Daha önce yapılmış DWT resim damgalama makalesinde PRN değerleri damga olarak kullanılıp LL şeridi dışında kalan 3 şeritte daha önceden belirlenen basamaktan büyük olan katsayılara gömülmüştür.Bu makalede ise bu fikri geliştirip aynı damga iki şeride gömüldü. Deneylerimiz gösterdi ki bir grup saldırı için, gerçek damgadaki korelasyon değeri LL bantı için belirlenen katsayıdan büyük, bir diğer grup saldırı için ise HH bantındaki katsayıdan büyük olmaktadır.

Anahtar Kelimeler: yarı-kör resim damgalama, saldırılar, gömme algoritması, dalgacık alanı

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.

Encryption is a procedure that renders the contents of a multimedia element unintelligible to unauthorized people. Watermarking embeds a digital signal in a multimedia element, which may contain information about the owner and the usage rights associated with the element. However, encryption is not an effective method because it does not provide permanent protection for the multimedia content after delivery.

Makale 02.07.2008 tarihinde gelmiş,19.09.2008 tarihinde yayınlanmak üzere kabul edilmiştir.

E. ELBASİ The Graduate Center, The City University of New York

365 Fifth Avenue, New York, NY 10016

e-posta : eelbasi@gc.cuny.edu

Digital Object Identifier 10.2339/2008.11.4. 329-337

A digital watermark is a pattern of bits inserted into a multimedia element such as a digital image, an audio or video file. The name comes from the barely visible text or graphics imprinted on stationery that identifies the manufacturer of the stationery. There are several proposed or actual watermarking applications : broadcast monitoring, owner identification, proof of ownership, transaction tracking, content authentication, copy control, and device control. 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. An embedded watermark should not introduce a significant degree of distortion in the cover image. The perceived degradation of the watermarked image should be imperceptible so as not to affect the viewing experience of the image. Robustness is the resistance of the watermark against normal A/V processes or intentional attacks such as addition of noise, filtering, lossy compression, resampling, scaling, rotation, cropping, and A-to-D and D-to-A conversions. Data capacity refers to the amount of data that can be embedded without affecting perceptual transparency.

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. The classification according to these criteria is listed in Table 1.

Criterion	Class	Brief description
Domain type	Pixel[6, 7, 8, 9, 19, 11]	Pixels values are modified to embed the watermark.
	Transform [12,13, 13, 15, 16]	Transform coefficients are modified to embed the watermark. Recent popular transforms are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT).
Watermark type	Pseudo random number (PRN) sequence (having a normal distribution with zero mean and unity variance) [12, 17, 18]	Allows the detector to statistically check the presence or absence of a watermark. A PRN sequence is generated by feeding the generator with a secret seed.
	Visual watermark [7, 19, 20, 21, 22, 23]	The watermark is actually reconstructed, and its visual quality is evaluated.
Information type	Non-blind	Both the original image and the secret key(s)
	Semi-blind [24, 25, 26, 27, 28]	The watermark and the secret key(s)
	Blind [29, 30, 31, 32]	Only the secret key(s)

2. RECENT WORKS

There are two major watermarking schemes in multimedia. The first is spatial domain watermarking, which basically embeds a visible logo or a PRN sequence directly to selected pixels in the host image. The second is transform domain watermarking such as DCT, DWT or DFT.

In a recent DCT-domain semi-blind image watermarking scheme [24], 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.

The watermark embedding and detection algorithms can be summarized as follows [24]:

Watermark embedding:

1. Compute the NxN DCT of an NxN gray scale image I.
2. Order the DCT coefficients in a zig-zag order as in the JPEG compression algorithm.
3. Skip the first L coefficients, and embed the watermark $X = \{x_1,x_2,\ldots,x_M\}$ to the next $L+M$ DCT coefficients $T = \{t_{L+i}\}$, $i = 1,2,\ldots,M$: $t'_{L+i} = t_{L+i} + \alpha|t_{L+i}|x_i$, $i = 1,2,\ldots,M$.
4. Replace $T = \{t_{L+i}\}$ with $T' = \{t'_{L+i}\}$, $i = 1,2,\ldots,M$ in the DCT domain.
5. Compute the inverse DCT to obtain the watermarked image I'.

Watermark detection:

1. Compute the DCT of the watermarked and possibly attacked image I^*.
2. Order the DCT coefficients in a zig-zag order.
3. Select the DCT coefficients from $(L+1)$st to $(L+M)$th to generate the vector $T^* = \{t^*_{L+1}, t^*_{L+2}, \ldots, t^*_{L+M}\}$.
4. Compute the sum $z = \frac{1}{M}\sum_{i=1}^{M} y_i t^*_{L+i}$, where y_i, $i = 1,2,\ldots,M$, represents either the real watermark $X = \{x_1,x_2,\ldots,x_M\}$ or a fake watermark $Y = \{y_1,y_2,\ldots,y_M\}$, and t_i^* represents the watermarked and possibly attacked DCT coefficients.
5. Choose a predefined threshold $T_z = \frac{\alpha}{3M}\sum_{i=1}^{M} | t_i^* |$.
6. If z exceeds T_z, the conclusion is the watermark is present.

In the paper, the following attacks have been used: JPEG compression, low pass filtering, median filtering, Gaussian noise, dithering, resizing to quarter of the original size, cropping, and adding multiple watermarks.

A DWT-based semi-blind image watermarking scheme follows a similar approach [25]. 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.

Although DWT or DCT based semi-blind watermarking (in high frequencies) schemes are robust against a number of attacks, they are not useful for some of the geometric attacks. Because of this reason we use two bands DWT based PRN embedding scheme in gray scale images.

3. METHODOLOGY

Discrete Wavelet Transform (DWT): The DWT separates the image into a lower resolution image (LL), and horizontal (HL), vertical (LH) and diagonal (HH) detail components. High resolution subbands are locate edge and texture patterns in an image. The magnitudes of DWT coefficients are larger in the lowest bands (LL) at each level of decomposition. 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 1 shows two levels of decomposition of Lena to be watermarked. The large coefficients in these bands normally indicate edges in the image. Two-dimensional DWT can be implemented using digital filters and downsamplers.

The proposed watermark embedding and detection algorithms can be summarized as follows:

Watermark embedding:

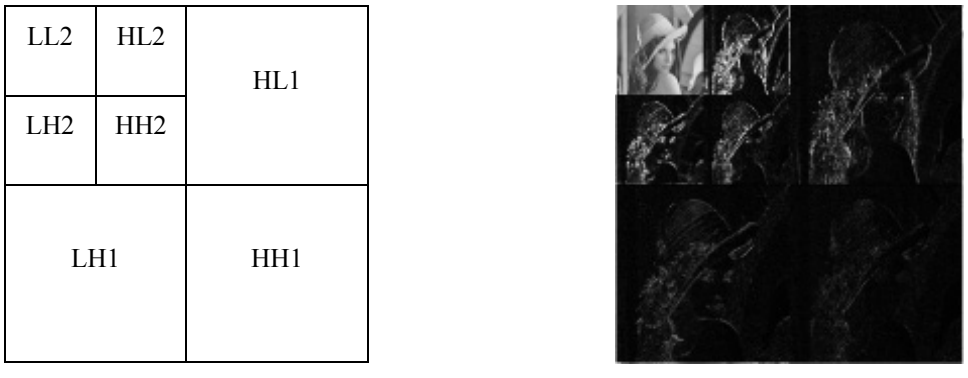
1. Compute the NxN DWT of an NxN gray scale image I.
2. Embed the watermark into the DWT coefficients > T_1: $T = \{t_i\}$, $t'_i = t_i + \alpha|t_i|x_i$, where i runs over all DWT coefficients > T_1 in LL and HH bands.
3. Replace $T = \{t_i\}$ with $T' = \{t'_i\}$ in the DWT domain.
4. Compute the inverse DWT to obtain the watermarked image I'.

Watermark detection:

1. Compute the DWT of the watermarked and possibly attacked image I^*.
2. Select all the DWT coefficients higher than T_2 in LL and HH bands.
3. 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..
4. Choose a predefined threshold $T_z = \frac{\alpha}{2M}\sum_{i=1} |t_i^*|$.
5. If z exceeds T_z, the conclusion is the watermark is present.

In the paper, the following attacks have been used: JPEG compression, median filtering, Gaussian noise, resizing to quarter of the original size, cropping, and etc.

In both of the above papers, the value of α is chosen as 0.2. In our extension to the DWT-based



(a) (b)

Figure 1. (a) Second level DWT decomposition, (b) Second level DWT decomposition of Lena

approach, we embed the same watermark in two bands (LL and HH) using different scaling factors for each band.

4. 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. There are 5 different gray scale image used with different sizes; Lena, Barbara and Cameraman experimental results are presented in the below.

The values of α and the threshold for each band are given in Table 2.

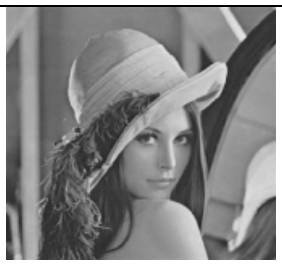
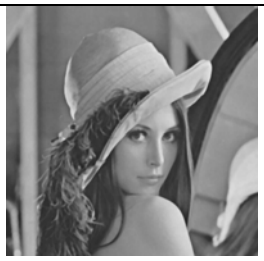
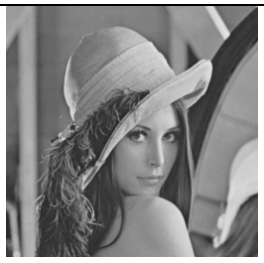
Table 2. Scaling factor α and threshold T

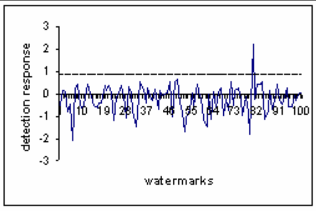
Parameters/ Bands	**LL**	**HH**
α	0.01	0.4
T_1	90	45
T_2	100	55

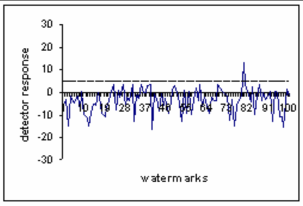
The 512x512 original test image, the watermarked image, and their difference are shown in Figure 2.

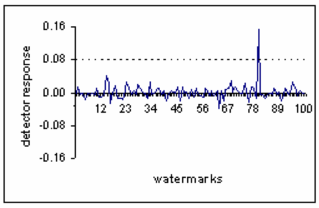
Same α and T parameters have been used in all experiments. Matlab was used for all attacks. The chosen attacks were JPEG compression, resizing, adding Gaussian noise, low pass filtering, rotation, histogram equalization, contrast adjustment, gamma correction, and cropping. The attacked images and the Matlab attack parameters are shown in Figure 3.

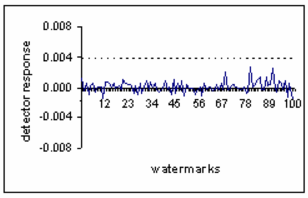
Figure 2. Embedding two watermarks into an image

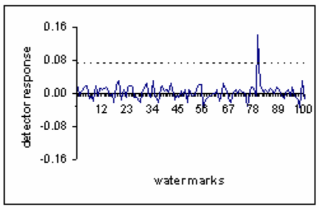
		
		
	^{0})	
		
		
	^{0})	
		

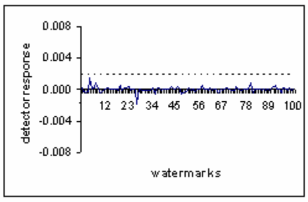

detection response
3
2
1
0
-1
-2
-3
watermarks

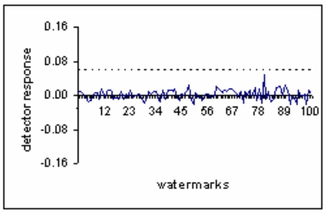

detector response
30
20
10
0
-10
-20
-30
watermarks

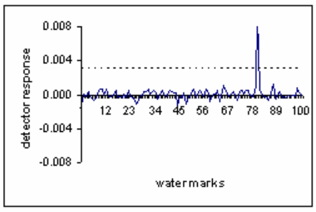

detector response
0.16
0.08
0.00
-0.08
-0.16
12 23 34 45 56 67 78 89 100
watermarks

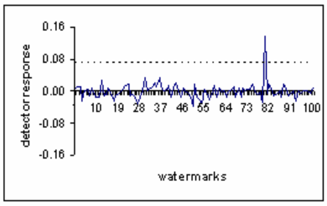

detector response
0.008
0.004
0.000
-0.004
-0.008
12 23 34 45 56 67 78 89 100
watermarks

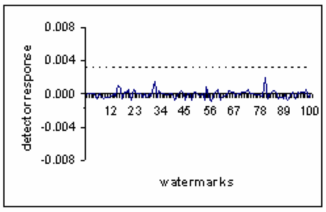

detector response
0.16
0.08
0.00
-0.08
-0.16
12 23 34 45 56 67 78 89 100
watermarks

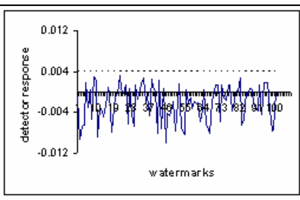

detector response
0.008
0.004
0.000
-0.004
-0.008
12 23 34 45 56 67 78 89 100
watermarks

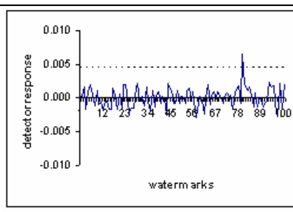

detector response
0.16
0.08
0.00
-0.08
-0.16
12 23 34 45 56 67 78 89 100
watermarks


detector response
0.008
0.004
0.000
-0.004
-0.008
12 23 34 45 56 67 78 89 100
watermarks


detector response
0.16
0.08
0.00
-0.08
-0.16
10 19 28 37 46 55 64 73 82 91 100
watermarks


detector response
0.008
0.004
0.000
-0.004
-0.008
12 23 34 45 56 67 78 89 100
watermarks

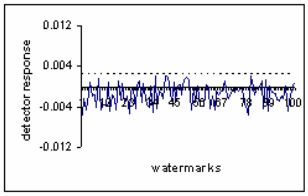

detector response
0.012
0.004
-0.004
-0.012
watermarks

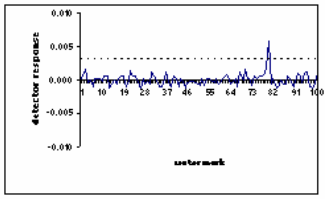

detector response
0.010
0.005
0.000
-0.005
-0.010
watermarks

In Figures 4-11, 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.

attack, the correlation with the real watermark is higher than the threshold in the HH band.

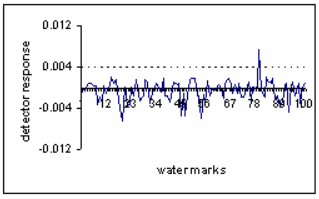
In future work, we will use this approach to watermark video sequences. We are planning to split

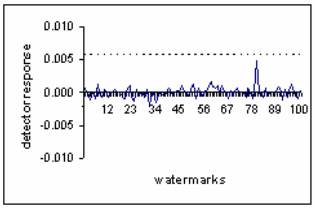




LL band (T=0.0024)	HH Band (0.00286)

Figure 10. Detector response for Cropping in Cameramen





LL band (T=0.00384)	HH Band (0.00571)

Figure 11. Detector response for Median Filtering in Cameramen

5. CONCLUSIONS

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.

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 to increase robustness.

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.

For the scaling and watermarking attacks, the correlation with the real watermark is higher than the threshold in the LL band, for the collusion attack, the correlation with the real watermark is higher than the threshold in the HH band, for the JPEG Compression + Gamma Correction and Gaussian Blur + Histogram Equalization attacks, the correlation with the real watermark is higher than the threshold in the LL band, and for the Gaussian Noise + Contrast Adjustment

MPEG video into I, B and P frames; then convert image from RGB format to YUV. Our expectation is embedding PRN sequence to luminance layer of the only I frames would be give similar results with the gray scale image watermarking scheme.

Acknowledgment

I would like to thank Prof. Dr. Ahmet M. Eskicioglu from Brooklyn College, CUNY for supervising me in this research work.

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

3. E. T. Lin, A. M. Eskicioglu, R. L. Lagendijk, and E. J. Delp, "Advances in Digital Video Content Protection," *Proceedings of the IEEE, Special Issue on Advances in Video Coding and Delivery*, 2004.

4. I. J. Cox, M. L. Miller, and J. A. Bloom, Digital Watermarking, *Morgan Kaufmann Publishers*, 2002.

5. Content Protection Status Report III, November 7, 2002, available at http://judiciary.senate.gov/special/mpaa110702.pdf.

6. R. G. Schyndel, A. Tirkel, and C. Osborne, "A Digital Watermark," *Proceedings of 1994 International*

Conference on Image Processing (ICIP 1994), Austin, Texas, November 13-16, 1994, pp. 86-90.

7. S. D. Lin and C.-F. Chen, "A Robust DCT-Based Watermarking for Copyright Protection," *IEEE Transactions on Consumer Electronics*, 46(3), August 2000, pp. 415-421.
8. W. Bender, D. Gruhl, and N. Morimoto, "Techniques for Data Hiding," *IBM Systems Journal*, Vol. 35, Nos. 3-4, 1996, pp. 313-336.
9. I. Pitas, "A Method for Signature Casting on Digital Images," *Proceedings of 1996 International Conference on Image Processing (ICIP 1996)*, Vol. 3, Lausanne, Switzerland, September 16-19, 1996, pp. 215-218
10. R. B. Wolfgang and E. J. Delp, "A Watermark for Digital Images," *Proceedings of 1996 International Conference on Image Processing (ICIP 1996)*, Vol. 3, Lausanne, Switzerland, September 16-19, 1996, pp. 219-222.
11. N. Nikolaidis and I. Pitas, "Robust Image Watermarking in the Spatial Domain," *Signal Processing*, 66(3), 1998, pp. 385-403.
12. I. J. Cox, J. Kilian, T. Leighton and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions on Image Processing*, 6(12), December 1997, pp. 1673-1687.
13. M. D. Swanson, B. Zhu, and A. H. Tewfik, "Transparent Robust Image Watermarking," *Proceedings of 1996 International Conference on Image Processing (ICIP 1996)*, Vol. 3, Lausanne, Switzerland, September 16-19, 1996, pp. 211-214.
14. J.J.K. Ó Ruanaidh, W.J. Dowling, and F.M. Boland, "Watermarking Digital Images for Copyright Protection," *IEE Proceedings on Vision, Signal and Image Processing*, 143(4), August 1996, pp. 250-256.
15. D. Kundur and D. Hatzinakos, "Digital Watermarking Using Multiresolution Wavelet Decomposition," *Proceedings of the 1998 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 1998)*, Vol. 5, Seattle, WA, May 12-15, 1998, pp. 2969-2972.
16. A. Lumini and D. Maio, "A Wavelet-Based Image Watermarking Scheme," *The International Conference on Information Technology: Coding and Computing (ITCC'00)*, Las Vegas, NV, March 27-29, 2000, pp. 122-127.
17. X.-G. Xia, C. G. Boncelet and G. R. Arce, "A Multiresolution Watermark for Digital Images," *Proceedings of the 1997 International Conference on Image Processing(ICIP 1997)*, Washington, DC, October 26-29, 1997.
18. 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.
19. J. J. Chae and B. S. Manjunath, "A Robust Embedded Data from Wavelet Coefficients," *Proceedings of the SPIE International Conference on Storage and Retrieval for Image and Video Databases VI*, Vol. 3312, San Jose, CA, January 28-30, 1998, pp. 308-317.
20. Y. Wang, J. F. Doherty and R. E. Van Dyck, "A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images," *IEEE Transactions on Image Processing*, 11(2), February 2002, pp. 77-88.
21. V. I. Gorodetski, L. J. Popyack, V. Samoilov and V. A. Skormin, "SVD-based Approach to Transparent Embedding Data into Digital Images," *International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security (MMM-ACNS 2001)*, St. Petersburg, Russia, May 21-23, 2001.
22. D. V. S. Chandra, "Digital Image Watermarking Using Singular Value Decomposition," *Proceedings of 45th IEEE Midwest Symposium on Circuits and Systems*, Tulsa, OK, August 2002, pp. 264-267.
23. R. Liu and T. Tan, "A SVD-Based Watermarking Scheme for Protecting Rightful Ownership," *IEEE Transactions on Multimedia*, 4(1), March 2002, pp.121-128.
24. A. Piva, M. Barni, F. Bartolini, V. Cappellini, "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, October 26-29, 1997.
25. 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.
26. V. Solachidis and I. Pitas, "Circularly Symmetric Watermark Embedding in 2-D DFT Domain," *Proceedings of the 1999 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 1999)*, Vol. 6, Phoenix, AZ, March 15-19, 1999, pp. 3469-3472.
27. V. Licks and R. Jordan, "On Digital Image Watermarking Robust to Geometric Transformations," *Proceedings of 2000 International Conference Image Processing (ICIP 2000)*, Vol. 3, Vancouver, BC, Canada, September 10-13, 2000, pp. 690-693.
28. C.-Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller, and Y. M. Lui, "Rotation, Scale, and Translation Resilient Watermarking for Images," *IEEE Transactions on Image Processing*, 10(5), May 2001, pp. 767-782.
29. R. Caldelli, M. Barni, F. Bartolini, A. Piva, "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, Vol. II, Vancouver, Canada, September 10-13, 2000, pp. 65-68.
30. S. Pereira and T. Pun, "Robust Template Matching for Affine Resistant Image Watermarks," *IEEE Transactions on Image Processing,* 9(6), June 2000, pp. 1123-1129.
31. G. C. Langelaar and R. L. Lagendijk, "Optimal Differential Energy Watermarking of DCT Encoded Images and Video," *IEEE Transactions on Image Processing*, 10(1), January 2001, pp. 148-158.
32. P. H. W. Wong, O. C. Au, and Y. M. Yeung, "A Novel Blind Multiple Watermarking Technique for Images,"

IEEE Transactions on Circuits and Systems for Video Technology: Special Issue on Authentication, Copyright Protection and Information Hiding, 13(8), August 2003, pp. 813-830.

33. Ersin Elbasi, Ahmet M. Eskicioglu, "A DWT-Based Robust Semi-Blind Image Watermarking Algorithm Using Two Bands", *IS&T/SPIE's 18th Annual Symposium on Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VIII Conference,* San Jose, CA, January 15–19, 2006