Robust MPEG Watermarking in DWT Four Bands

E. Elbaşı

The Scientific and Technological Research Council of TURKEY
Tunus Caddesi No: 80 Ankara, Turkey
ersin.elbasi@tubitak.gov.tr

ABSTRACT
In this paper, we generalize an idea in a recent paper that embeds a binary pattern in the form of a binary image in the wavelet domain for images. Our generalization includes all four bands (LL, LH, HL and HH) in the DWT for MPEG video sequences. We tested the proposed algorithm against twelve attacks. Embedding the watermark in lower frequencies is robust to one group of attacks, and embedding the watermark in higher frequencies is robust to another group of attacks.

Keywords: non-blind video watermarking, DWT, visual watermark, MPEG, attacks.

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. 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.

Encryption and watermarking are two major tools that can be used to prevent unauthorized consumption and duplication. Both processes require secret keys to prevent unauthorized use of a particular technology by an adversary [1, 2, and 3]:

Encryption: Symmetric keys are commonly used to encrypt a multimedia element in transmission and storage. The decryption key should therefore be kept in secure and tamper-resistant devices.

Watermarking: A multimedia element is often watermarked with a key that determines the location of the watermark. The same key is used by the watermark detector or extractor.

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 [6, 7].

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 [5].

In a recent paper [9], two visual watermarks are embedded in the DWT domain through modification of both low and high frequency coefficients. Watermark data inserted into low frequencies is more robust to image distortions that have low pass characteristics like filtering, lossy compression, and geometric manipulations but less robust to changes of the histogram such as contrast/brightness adjustment, gamma correction, and cropping.

On the other hand, watermark data inserted into middle and high frequencies is typically less robust to low-pass filtering, lossy compression, and small geometric deformations of the image but extremely robust with respect to noise adding, and nonlinear deformations of the gray scale.

Criterion	Class	Brief description
Domain Type	Pixel	Pixels values are modified to embed the watermark.
	Transform	Transform coefficients are modified to embed the watermark. Recent popular transforms: Discrete Cosine Transform (DCT) Discrete Wavelet Transform (DWT) Discrete Fourier Transform (DFT)
Watermark Type	PRNS	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	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	The watermark and the secret key(s)
	Blind	Only the secret key(s)

Table 1. Classification of watermarking systems.

Since the advantages and disadvantages of low and middle-to-high frequency watermarks are complementary, embedding multiple watermarks in an image (namely, one in lower frequencies and the other in higher frequencies) would result in a scheme that is highly robust with respect to a large spectrum of image processing operations. After performing a two level decomposition of the cover image, the authors embed the first watermark in the LL2 band, and the second watermark in the HH2 band. The cover image tested in the paper is 128x128 “hetu.tif” while the visual watermarks are 32x32 binary patterns “CO” (which is embedded in the low frequency band), and “EP” (which is embedded in the high frequency band). In the experiments, the proposed scheme is tested against several attacks (JPEG compression, wiener filtering, Gaussian noise, scaling, cropping, histogram equalization, intensity adjustment, and gamma correction). According to the results, embedding in the LL2 band is more resistant to JPEG compression, wiener filtering, Gaussian noise, scaling, and cropping while embedding in the HH2 band is more resistant to histogram equalization, intensity adjustment, and gamma correction. Nevertheless, the implementation of the idea is seriously flawed. Without taking into consideration the difference in magnitudes of lower and higher DWT coefficients, the scheme is implemented with a scaling factor of 0.1 for both bands. This leads to highly visible degradation in all parts of the image, especially in low frequency areas such as the wall, causing two major detriments: (1) the commercial value of the image is reduced, and (2) a clue is provided to the hacker for unauthorized removal of the watermark [8].

In this paper, we will generalize the above image watermarking scheme by embedding the same visual watermark in all four bands using first level decompositions in MPEG video.

2. Algorithm

Most of the video watermarking techniques are based on either raw video or compressed e.g., (MPEG) video. A video file is a sequence of still images, but it may be compressed using different methods such as MPEG-1, MPEG-2 etc. MPEG

stands for “Moving Picture Experts Group”, which is developed in 1988. There are several MPEG standards; each compression standard was designed for a specific application. DWT based watermarking have some advantages over the other common methods:

• It has both spatial and frequency based localization.
• There is a both perceptual invisibility and robustness against to compression attacks.
• It is more robust against to adding noise, image processing techniques and median filtering.
• Resist to geometric transform.

Due to large amount of frames, similarity between frames and temporal attacks (frame dropping, frame averaging, frame swapping etc.), video watermarking process is more difficult than image watermarking. Current image watermarking methods are not adequate to solve these difficulties. We proposed a novel video watermarking algorithm based on the DWT in MPEG.

In two-dimensional separable dyadic DWT, each level of decomposition produces four bands of data, one corresponding to the low pass band (LL), and three other corresponding to horizontal (HL), vertical (LH), and diagonal (HH) high pass bands. The decomposed image shows a coarse approximation image in the lowest resolution lowpass band, and three detail images in higher bands. The low pass band can further be decomposed to obtain another level of decomposition [8]. This process is continued until the desired number of levels determined by the application is reached. The proposed MPEG watermarking algorithm is given below.

Watermark Embedding Procedure:

Input: Video sequence I and binary visual watermark W.
Process:
a. Split the video sequence into frames.
b. Convert the NxM RGB frame to YUV in I frames.
c. Compute the DWT of the luminance layer (Y) for each I frame.
d. Modify the DWT coefficients V_{ij} in the LL, LH, HL, and HH bands in all frames.
$V_{w,ij} = V_{i,j}^{k} + \alpha_k \cdot W_{i,j}$ where i =1,….,n ; j = 1,….,m
e. Apply inverse DWT to obtain the watermark cover frame I_w for each I frame.
Output: Watermarked cover video sequence.

Watermark Extraction Procedure:

Input: Watermarked (possibly attacked) MPEG compressed video.
Process:
a. Split the watermarked (possibly attacked) video into I, B and P frames.
b. Convert NxM RGB I frames to YUV.
c. Compute the DWT of the luminance layer (Y) for any I frames.
d. Extract the binary visual watermark from the LL, LH, HL and HH bands.
$W_{ij}^{*} = (V_{w,ij}^{*k} – V_{ij}^{k}) / \alpha_k$ where i = 1,….,n; j = 1,….,m
e. If $W_{ij}^{*} > T$, then $W_{ij}^{*} = 1$ else $W_{ij}^{*} = 0$, where T is the threshold between 0 and 1.
Output: Binary visual watermark.

3. Experimental Results

Since the magnitudes of DWT coefficients are larger in the lowest band at each level of decomposition, it is possible to use a larger scaling factor for watermark embedding. For the other 3 bands, the DWT coefficients are smaller, allowing a smaller scaling factor to be used. The resulting watermarked image does not have any degradation leading to a loss in its commercial value [4].

In the below experiments, we measured the visual quality of watermarked and attacked images using the Peak-Signal-To-Noise Ratio (PSNR) defined by PSNR = 20.log10.(255/RMSE), where RMSE is the Square Root of the Mean Squared Error (MSE) between the original and distorted images.

The visual quality of extracted visual watermarks is measured by the Similarity Ratio (SR) defined by SR = S/(S+D), where S denotes the number of matching pixel values in compared images, and D denotes the number of different pixel values in compared images.

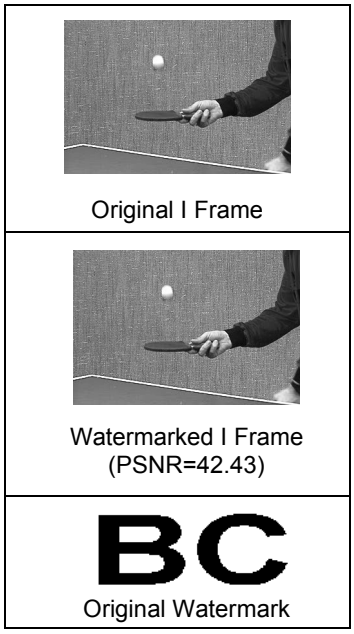

Figure 1. Original and watermarked I frames.

Figure 1 shows original I frame, watermarked frame and binary watermark.

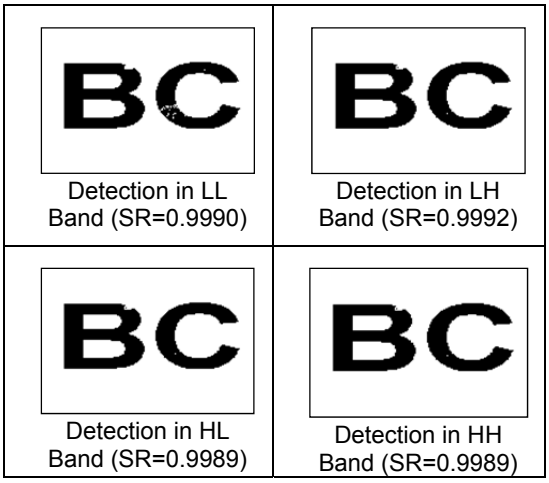

Figure 2. Watermarks extracted from LL, LH, HL and HH bands.

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, cropping, rewatermarking and collusion. Figure 3 shows I frames after common attacks.

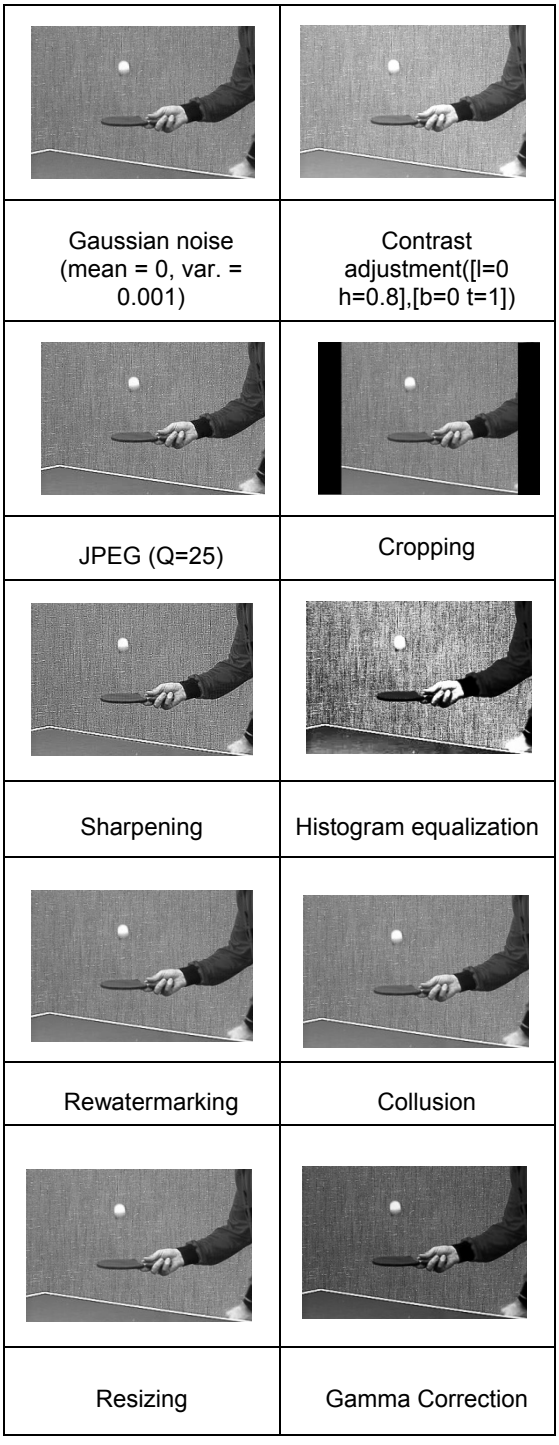

Figure 3. Attacks on MPEG video.

In Figures 4-8, we display the extraction responses for four bands in some of the common attacks.

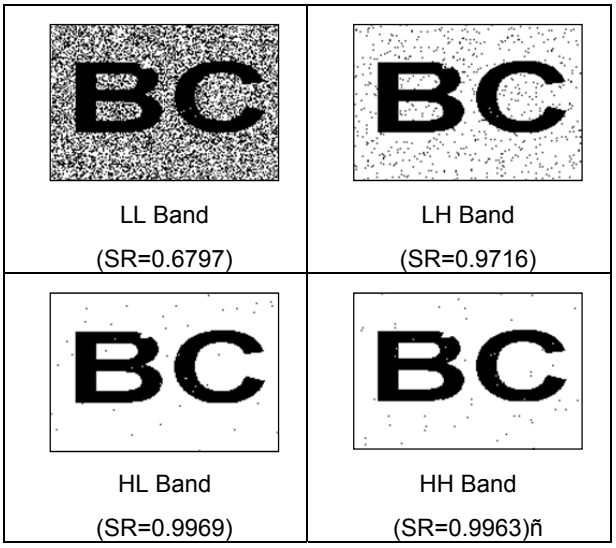

Figure 4. Extraction after Gaussian Noise.

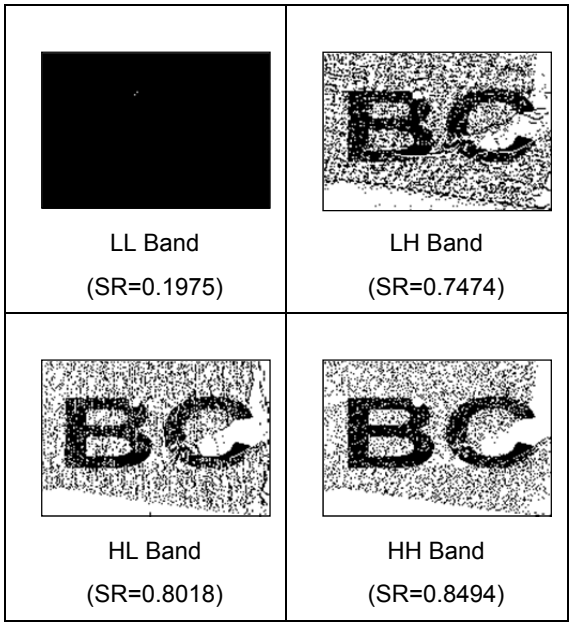

Figure 5. Extraction after Gaussian Noise.

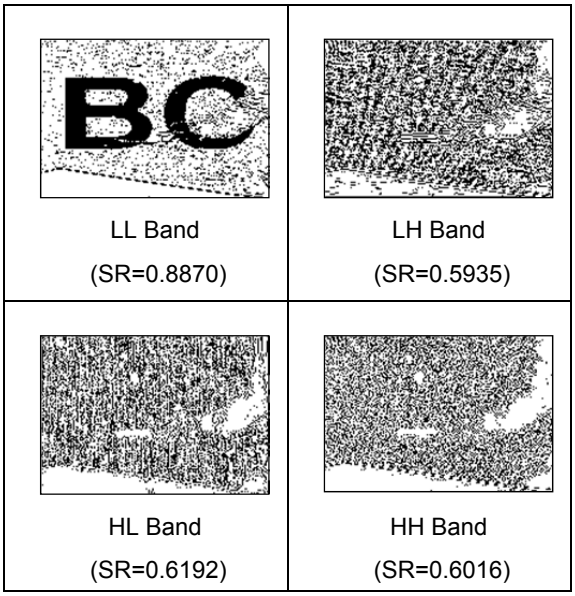

Figure 6. Extraction after Resizing.

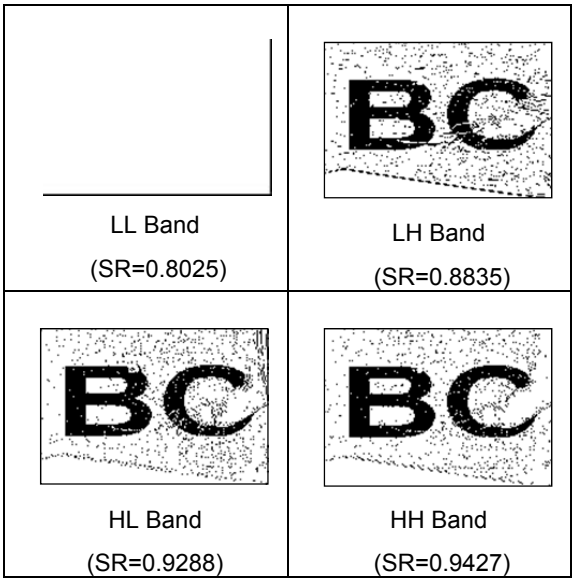

Figure 7. Extraction after Gamma Correction.

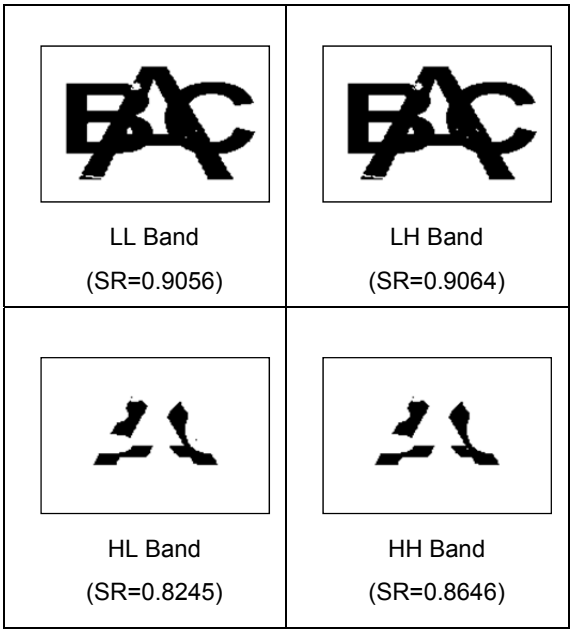

Figure 8. Extraction after collusion.

4. Conclusion

In a DWT-based semi-blind image watermarking, a watermark is embedded in three bands (HL, LH, and HH), 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 our research, we have extended the idea by embedding the same watermark in two bands (LL and HH) using different scaling factors for each band.

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 MPEG. 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 luminance layer of the YUV I frame. 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 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 T_2 in the LL and HH bands. In each band, if Z exceeds T, the watermark is present.

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 rewatermarking attack, there are two binary watermarks: BC and A. In all bands, the extractions are the union of the two binary images. For the collusion attack, the extractions appear to be the union of the two binary images in the lower bands. In the higher bands, the extractions look like the intersection of the two binary images.

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] 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.

[5] E. Elbasi and A. M. Eskicioglu, “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, January 15–19, 2006.

[6] 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.

[7] 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.

[8] Peining Tao, Ahmet M. Eskicioglu, "A Robust Multiple Watermarking Scheme in the Discrete Wavelet Transform Domain", Optics East 2004, Internet Multimedia Management Systems V Conference, Philadelphia, PA, October 25-28, 2004.

[9] R. Mehul and R. Priti, "Discrete Wavelet Transform Based Multiple Watermarking Scheme," Proceedings of IEEE Region 10 Technical Conference on Convergent Technologies for the Asia-Pacific, Bangalore, India, October 14-17, 2003.