Wavelet Packet Based Digital Image Watermarking

A.Adhipathi Reddy, B.N.Chatterji
Department of Electronics and Electrical Communication Engg.
Indian Institute of Technology, Kharagpur – 721 302
{aar, bnc}@ece.iitkgp.ernet.in

Abstract

In this paper, a novel wavelet packet based watermarking scheme for copyright protection is presented. A key is used for wavelet bases selection, watermark generation and selection of blocks for embedding the watermark bits. Watermark is embedded by quantizing the mean of the wavelet coefficient block. A method for exploiting human visual system (HVS) characteristics in wavelet packet domain is presented. In our proposed method original image is not needed and only private key is required for extracting the watermark. Experimental results show that proposed method is robust to different types of attacks and is much superior to the other existing methods.

1. Introduction

With the increasing use of Internet and effortless copying, tampering and distribution of digital data, copyright protection for multimedia data has become an important issue. Digital watermarking emerged as a tool for protecting the multimedia data from copyright infringement. In digital watermarking an imperceptible signal "mark" is embedded into host image, which uniquely identifies the ownership. The main requirements of the watermarking are imperceptibility and robustness to intentional and unintentional attacks. An overview on watermarking techniques can be found in [7].

Watermarking methods can be broadly classified into two categories: spatial and transform domain methods. Transform domain method are more robust than spatial domain methods because when image is inverse transformed watermark is distributed irregularly over the image, making the attacker difficult to read or modify. Among the transform domain techniques wavelet based watermarking methods are gaining more popularity because of superior modeling of HVS. A detail survey on wavelet based watermarking methods can be found in [9]. Another important issue in watermarking is access to original image. In non-oblivious methods [1], original image is used for extracting the watermark but in oblivious methods it is not used. In many applications it is difficult to have access to original image, so it is desirable that the watermarks should be extracted without using original image.

Watermarking methods are also classified into two categories based on embedding mechanism [14]. In the first method, watermark bits are added directly to the host data by encoding or modulating. Example of this type of method is spread spectrum watermarking [5]. In the second method, single coefficients or group of coefficients are mapped to represent one bit of watermark information. These methods are free from host interference. Example of this type of watermarking is quantization based watermarking [14]. The main problem with additive watermarking techniques is that the signal-to-noise ratio is very small due to the host interference.

Many quantization based watermarking techniques have been proposed in literature [4], [6], [14], because of no interference of host data. In [6] a method to embed binary watermark bits in wavelet domain was given. In each level, coefficients of same spatial location from three detail subbands are sorted in ascending order and the middle coefficient is quantized to represent one watermark bit. In [4], watermark bits are embedded by quantizing the mean of a group of wavelet coefficients. More recently, in [12] a method for embedding the watermark by quantizing the wavelet tree was proposed. The wavelet coefficients are grouped into so-called super tree, and watermark bits are embedded by using two super trees.

Wavelet packets are successfully used for image compression [2],[10] to take advantages of better spatial frequency representation. Very few wavelet packet based watermarking methods have been proposed in literature. In [11] & [15] a key is used in selecting the watermarking portion and fining the wavelet packet transform for watermarking. The methods discussed above have not properly exploited HVS characteristics in embedding the watermark and hence these methods are not much robust against intentional and unintentional attacks.

To embed watermark more robustly by exploiting HVS characteristics, in this paper, a novel wavelet packet based watermarking method is presented. A method for exploiting HVS characteristics in wavelet packet domain is also presented. Watermark is embedded by quantizing the mean of wavelet coefficient block. A secrete key is used for wavelet bases selection, watermark generation and for selection of blocks for embedding the watermark. For extraction of the watermark only secret key is required and original image is not needed. Robustness of the proposed method is extensively tested with different types of attacks and results are compared with the existing methods. From the results it is be observed that proposed method is much better than the existing methods both interms of quality and robustness.

The rest of the paper is organized as follows. Exploitation of HVS characteristics is explained in section 2. In section 3 mean quantization, watermark embedding and extracting algorithms are explained. Experimental results and comparisons with existing methods are given in section 4. Finally, the concluding remarks are given in section 5.

2. HVS Characteristics

Number of factors affects the noise sensitivity of the human eye like luminance, frequency and texture. Human eye is less sensitive to areas of the image where brightness is high or low. As observed in [13], human eye is less sensitive to noise in high frequency bands and bands having orientation of 45 degrees. Sensitivity of human eye to noise in textured area is less and it is more near the edges. In [8], these observations are exploited for finding weight factors to quantize wavelet coefficients for image compression. With some modification, Barni et al. [3], used these weight factor in embedding the watermark. With some modifications we are proposing a method for exploiting HVS characteristics in wavelet packet domain.

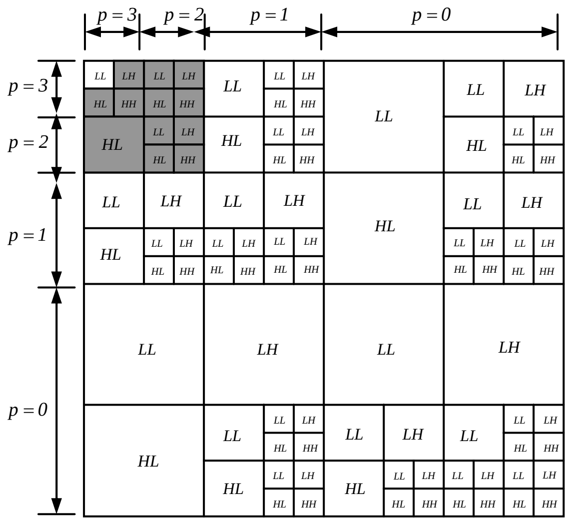

Figure 1. 4-level wavelet packet bases representation. Shaded bands are used for watermarking

The wavelet packet basis representation of a 4-level transformed image is shown in figure 1. Let us represent the subbands of image size $M \times N$ as S_m where $m = 1,2,3......N_m$ and N_m is the total number of subbands. Let θ_m be the orientation of the m^{th} subband where $\theta \in \{LL, LH, HL, HH\}$. l_m represents the level of m^{th} subband and p_m represents position as shown in figure 1. Let n_p be the total number of subbands in p^{th} position. For the sake of convenience let us represent the l^{th} level approximate band in pyramidal structure decomposition by G_l.

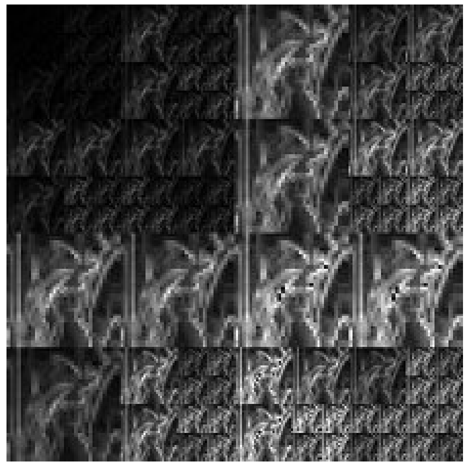

Figure 2. Visual mask calculated using method in [3]

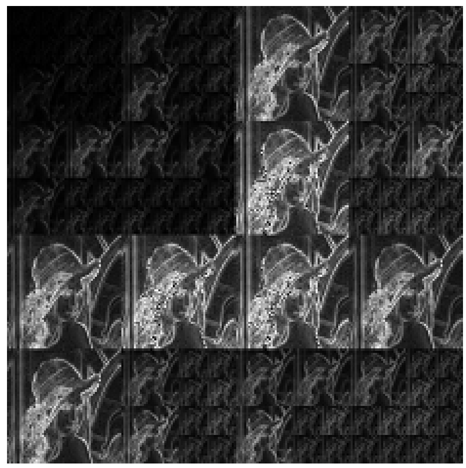

Figure 3. Visual mask calculated using proposed method

Based on the above observations of the sensitivity of human eye, weight factors for wavelet coefficients can be found by using three terms, namely, luminance L, frequency and orientation F, and texture activity T as given in equation (1) [3].

$$w_m(i,j) = F(l,\theta) L(l,i,j) T(l,p,i,j)^{0.2} \tag{1}$$

As per the results given in [8], first term in equation can be handled as follows

$$F(l,\theta) = \begin{cases} \sqrt{2} & \text{if } \theta = HH \\ 1 & \text{otherwise} \end{cases} * \begin{cases} 1.00, & \text{if } l = 0 \\ 0.32, & \text{if } l = 1 \\ 0.16, & \text{if } l = 2 \\ 0.10, & \text{if } l = 3 \end{cases} \tag{2}$$

As per the observations give by Barni et. al [3], human eye is less sensitive to noise in bright or dark background regions. They calculated the effect of luminance by considering the LL band of highest level as given below

$$L(l,i,j) = 1 + B'(l,i,j) \tag{3}$$

where

$$B'(l,i,j) = \begin{cases} 1 - B(l,i,j) & \text{if } B(l,i,j) < 0.5 \\ B(l,i,j) & \text{otherwise} \end{cases} \tag{4}$$

and

$$B(l,i,j) = \frac{1}{256} S_0\left(1+\left\lfloor \frac{i}{2^{3-l}} \right\rfloor, 1+\left\lfloor \frac{j}{2^{3-l}} \right\rfloor\right) \quad (5)$$

With the equation (5), the weight factors calculated in smooth regions are high as appeared in figure 2 with square blocks. This is because one coefficient in S_0 band corresponding to $2^{3-l} \times 2^{3-l}$ values in l^{th} level subband. To avoid this, we modified equation 5, so that it is calculated from same level LL band as given below

$$B(l,i,j) = \frac{1}{256} G_l(i,j) \quad (6)$$

Sensitivity to noise in texture areas can be found by finding the product of the local mean square value of the wavelet coefficients in all detail bands and local variance of the approximate band. These two terms are found in 2×2 neighborhood corresponding to the location (i,j). Mathematically, it can be represented as

$$T(l,p,i,j) = \sum_{k=p}^{3} \sum_{z=t_p}^{t_p+n_p} \frac{1}{16^{l_z-l}} \sum_{x=0}^{1} \sum_{y=0}^{1} S_z\left(x+\frac{i}{2^{l_z-l}}, y+\frac{j}{2^{l_z-l}}\right) * var\{(G_l(x+i,\ y+j))\}_{\substack{x=0,1\\ y=0,1}} \quad (7)$$

Here t_p be the number of first subband in p^{th} position. Figure 2 and 3 shows the visual mask calculated for the Lena image using the procedure in [3] and with our method. From these figures it is observed that in our method less weightege is given to smooth region compared to the method in [3].

3. Proposed Watermarking Method

In our proposed method discrete wavelet packets transform (DWPT) is used for embedding the binary watermark. Wavelet packets are used to gain the advantage of better frequency resolution representation. Another advantage of wavelet packet is that it also adds the security as the basis is selected using the secret key. Watermark is embedded in the middle frequency bands of the image as shown in figure 1 with shades. These frequency bands are used because watermark embedded in high frequency bands is less robust.

Block diagram for watermark embedding is shown in figure 4. A secrete key is used for wavelet basis selection, watermark generation and selection of blocks for watermarking. Watermark is embedded by quantizing the mean of a wavelet coefficients block. Mean quantization is used because quantizing mean of the block is more robust than quantizing a single coefficient [4]. This can be concluded from statistical principle, which states that for a given set of samples, the population mean has a smaller variance than that of a single sample. After embedding the watermark inverse discrete wavelet transform of the image is taken to get the watermarked image.

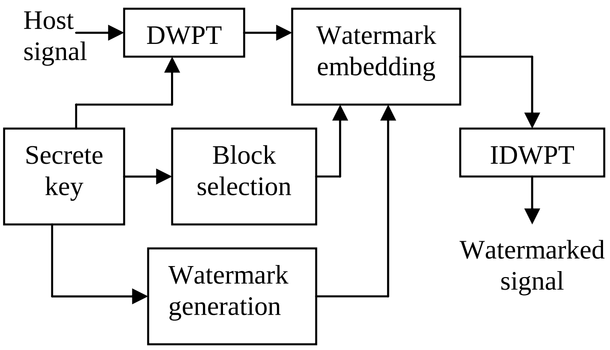

Figure 4. Block diagram of watermark embedding

Figure 5 shows the block diagram for watermark extraction. For watermark extraction only secrete key is required. Wavelet packet basis of doubtful image and watermarked blocks are found using secret key. After extracting the watermark, normalized correlation ρ between original and extracted watermark is calculated. Finally, ρ is compared with appropriate threshold T to find whether watermark is present or not.

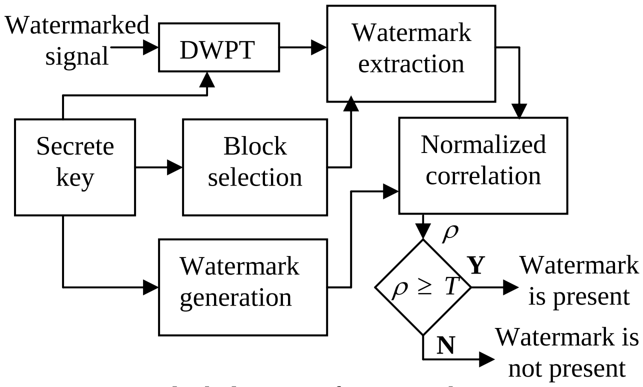

Figure 5. Block diagram of watermark extraction

3.1. Mean quantization

For quantizing the mean of the wavelet coefficients block, a quantization table is used which is available for both embedding and extracting. This quantization table is determined by considering the tradeoff between the watermarking strength and quality of watermarked image. For large value of quantization interval q, coefficients are quantized heavily, which increases watermarking strength but decreases the quality of the image.

Let $l \times m$ is size of the block chosen for embedding the watermark bit. $\bar{x}_n$ is the mean of the n^{th} block of wavelet coefficients $x(i,j)$ and is calculated as given in equation (8)

$$\bar{x}_n = \frac{1}{l \times m} \sum_{i=0}^{l-1} \sum_{j=0}^{m-1} x(i,j) \quad (8)$$

Quantization of mean value is illustrated in figure 6. Depending on watermark bit, mean value is quantized to nearest quantization interval. If the mean value is to be quantized from one qunatization interval to another interval then Δ_{min} and Δ_{max} are calculated. Δ_{min} is the minimum updating required so that the mean value will be within the required quantization interval. The maximum value of Δ_{min} is $q/2$. Therefore quantization interval q value is chosen such that $q/2$ should not give any perceptual degradation. Δ_{max} is the maximum updating that can be applied so that the mean will be mapped to middle of the required quantization interval. Based on the value of Δ_{min} and Δ_{max} each wavelet coefficient in the block are updated using equation (9).

$$x'(i,j) = x(i,j) + \Delta_{min} + w(i,j) * (\Delta_{max} - \Delta_{min}) \qquad (9)$$

where $x'(i,j)$ is updated wavelet coefficient and $w(i,j)$ is weight factor of the coefficient $x(i,j)$, which ranges between 0 and 1. If the mean value of the block is within the required quantization level then calculate Δ such that it will map the mean to the middle of the same quantization interval. Quantization of coefficients is done by equation (10).

$$x'(i,j) = x(i,j) + w(i,j) * \Delta \qquad (10)$$

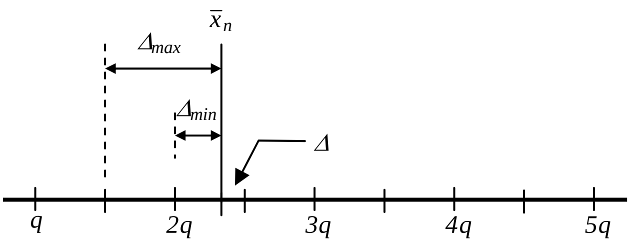

Figure 6. Illustration of quantization for watermarking

3.2. Watermark Embedding

Step 1: Generate binary watermark bits of ± 1 or randomize the owner signature using the secret key. Let us represent watermark bit with b_i where $i = 1 \ldots . N_b$, N_b is the length of the watermark.

Step 2: Decompose the host image using the key and DWPT into required number of levels.

Step 3: Choose the middle frequencies subbands and find the weight factor w of each coefficient in these subbands as explained in section 2.

For $i = 1 \ldots . N_b$ do step 4 and step 5.

Step 4: Find the wavelet coefficients block using secrete key and the mean using equation (8).

Step 5: Based on the watermark bit b_i and using quantization table quantize each coefficient in the block to desire value. If the mean is within the required quantization interval then calculate Δ and update coefficient using equation (10). Otherwise find Δ_{min} and Δ_{max}, and update each coefficient using equation (9).

Step 6: After embedding the watermark take IDWPT of the image to get the watermarked image.

3.3. Watermark Extraction

Step 1: Decompose the doubtful image using secrete key and DWPT and select the middle frequency bands.

For $i = 1 \ldots . N_b$ do step 2 and step 3

Step 2: Find the wavelet coefficient block using key and the mean using equation (8).

Step 3: Using quantization table determine the watermark bit b_i' by finding to which qunatization interval this mean belongs.

Step 4: After extracting all watermark bits find the normalized correlation between the given and extracted watermark sequence using equation (11).

$$\rho = \frac{\sum_{i=0}^{N_b-1} b_i \, b_i'}{\sqrt{\sum_{i=0}^{N_b-1} b_i^2} \sqrt{\sum_{i=0}^{N_b-1} b_i'^2}} \qquad (11)$$

After finding the normalized correlation ρ, it is compared with the appropriate threshold value T to decide whether watermark is present or not. If the ρ value is greater than or equal to T then watermark is present, otherwise watermark is not present.

4. Experimental Results

In order to verify the quality and robustness of the watermarked image of the proposed method, it is tested on different type of images. Here the results are presented for grayscale 8-bit Lena image of size 512×512 shown in figure 7. Daubechies 9/7 filter coefficients are used for DWPT of the image. Block size of 2×2 is used for embedding the watermark bit. The qunatization interval q equal to 2.5 is used for generating the quantization table. Binary watermark bits ($\pm$) of length 512 are used for embedding. For watermark length of 512, threshold value T is chosen to be 0.23 with a false positive probability of $P_{fp} = 1.03 \times 10^{-7}$. To evaluate the quality of the watermarked image we have used the peak signal-to-noise ratio (PSNR) as a measure. Even though it is not a good measure of quality of the image, it can be used as reference for measuring the invisibility. PSNR value of the watermarked Lena image shown in figure 8 is 48.23.

To test the robustness of the proposed algorithm watermarked Lena image is tested with different types of geometrical and non-geometrical attacks. Normalized correlation and detector responses with different types of attacks are given in tabular form. Detector response 'Y' indicates watermark is present and 'N' indicates watermark is not present. Table I shows the detector response after JPEG and SPIHT (Set Partition in Hierarchical Trees) compression of watermarked image.

Figure 7. Original Lena image of size 512×512

Figure 8. Watermarked Lena image

Table-I. Correlation ρ and detector responses (DR) with JPEG and SPIHT compression

	JPEG Compression (Q factor)			SPIHT Compression (bpp)		
	70	30	10	0.8	0.4	0.1
ρ	0.99	0.83	0.24	0.98	0.85	0.27
DR	Y	Y	Y	Y	Y	Y

To verify the robustness of the algorithm to common signal processing attacks, Lena image is tested for average, median and Gaussian filtering. Results are shown in table II for average and median filtering and for Gaussian filtering the results are given in table III. Detector responses after histogram equalization and image sharpening are given in table-III.

Table-II. Correlation ρ and detector responses (DR) at different filter size of average and median filters

Filter Dimension	Average Filtering		Median Filtering	
	ρ	DR	ρ	DR
3×3	0.91	Y	0.96	Y
5×5	0.64	Y	0.73	Y
7×7	0.46	Y	0.48	Y
9×9	0.24	Y	0.29	Y

Table-III. Correlation ρ and detector responses (DR) after Gaussian filtering Histogram equalization (HS), sharpening (IS) and warping (IW) attacks

	Gaussian filter (radius)			HE	IS	IW
	1	2	3			
ρ	0.87	0.52	0.31	0.36	0.65	0.38
DR	Y	Y	Y	Y	Y	Y

To show the robustness of proposed method to geometrical attack we verified with resizing, rotation and warping attacks. Table-IV shows detector responses with resizing and rotation attacks. For both resizing and rotation attacks, image is scaled to original size for watermark extraction. Positive angle represents clockwise rotation and negative angle represents anticlockwise rotation. Warped Lena image is shown in figure 9 and detector response is given in table-III. There are many attacks that can be tested for, but the results presented here give a good indication of the capabilities of the proposed method.

Table-IV. Correlation ρ and detector responses (DR) at different angle of rotation and resizing factor

	Resizing (scale factor)		Rotation in angle			
	2	3	0.25	0.5	-0.25	-0.5
ρ	0.69	0.51	0.52	0.26	0.49	0.24
DR	Y	Y	Y	Y	Y	Y

To show the superiority of the proposed method we compared our results with the method proposed in [12]. A detailed comparison of both the methods with robustness limit for different types of attacks is given in table-V. It can be observed from the PNSR that the quality of the image with our method is much better than the quality with the method in [12]. Robustness of our proposed method with different types of attacks is much better than the method in [12].

Figure 9. Warped watermarked Lena image

Table-V. Comparison of the proposed method with the method of [12]. Table shows robustness limit with different type of attacks

Attacks/PSNR	Ref [12]	Our Proposed Method
PSNR	38.2	48.3
Average Filter	3×3	9×9
Median Filter	3×3	9×9
Gaussian Filter	Radius 1	Radius 3
JPEG Compression	QF = 40	QF = 10
SPIHT Compression	bpp= 0.4	bpp= 0.1
Rotation	0.75^o	0.5^o

5. Conclusion

In this paper, a novel wavelet packet based watermarking method for copyright protection is presented. Wavelet packets are used to gain the advantage of better frequency resolution representation. A method for exploiting the HVS characteristics is also presented. Watermark is embedded by quantizing the mean of the wavelet coefficient block. Original image is not required for extracting the watermark. The proposed method is more secure as the security lies in secrete key, which is used for selecting the bases, watermark generation and selecting the watermark embedding blocks. Proposed method is tested with different type of geometric and non-geometric attacks. There are many attacks that can be tested for, but the results presented here give a good indication of the capabilities of the proposed method. Experimental results show that the proposed method is much better than the method in [12] both in terms of quality and robustness.

6. References

[1] A.Adhipathi Reddy, and B.N.Chatterji. Wavelet based Robust Logo Watermarking Scheme. *Proceedings of Int. Conf. on Advances in Pattern Recognition,* Kolkata, India, pp 359-363, Dec 2003.

[2] A.Adhipathi Reddy, and B.N.Chatterji. Texture Image Compression using Tree Structured Wavelet Transform. IETE Journal of Research,Vol.50, pages 63-67, Jan 2004.

[3] M.Barni, F.Bartolini and A. Piva. Improved Wavelet based Watermarking through Pixel-wise Masking. *IEEE Transaction on Image Processing,* vol.10, pp 783-791, May 2001.

[4] L.H.Chen and J.J.Lin. Mean Quantization based Image Watermarking. *Image and Vision Computing*, vol.21, pages 717-727, Aug 2003.

[5] I.J.Cox, J.Kilian, F.TLeighton and T.Shamoon. Secured Spread Spectrum Watermarking for Multimedia. *IEEE Tran. on Image Processing*, vol. 6, pp 1673-1687, Dec 1997.

[6] D.Kundur and D.Hatzinakos. Digital Watermarking using Multiresolution Wavelet Decomposition. *Pro. of the Int.. Conf.e on Acoustic, Speech and Signal Processing,* Seattle, W.A, pp 2969-2972, May 1998.

[7] G.C.Langelaar, I.Setyawan and R.I.Lagendijk. Watermarking Digital Image and Video Data. *IEEE Signal Processing Magazine*, pp 20- 46, Sep 2000.

[8] A.S.Lewis and G.Knowles. Image Compression using the 2-D Wavelet Transform. *IEEE Tran. on Image Processing,* vol. 1, pp. 244-250, Apr 1992.

[9] P.Meerwald and A.Uhl. A Survey of Wavelet-domain Watermarking Algorithms. *Proc. of SPIE,* CA ,USA, pp.505-516, Jan 2001.

[10] F.G.Meyer, A.Z.Averbuch, Stromberg. Fast Adaptive Wavelet Packet Image Compression. *IEEE Tran. on Image Processing*, Vol. 9, pp 792-800, May 2000.

[11] M.J.Tsai, K.Y.Yu and Y.Z.Chen. Wavelet Packet and Adaptive Spatial Transformation of Watermark for Digital Image Authentication. *IEEE Int. Conf. on Image Processing*, vol. 1. pp 450-453, Sep 2000.

[12] S.H.Wang and Y.P.Lin. Wavelet Tree Quantization for Copyright Protection Watermarking. *IEEE Tran. on Image Processing*, vol.13, pp 154-165, Feb 2004.

[13] A.B.Watson, G.Y.Yang, J.A.Solomon and J.Villasenor. Visibility of Wavelet Quantization Noise. *IEEE Tran. on Image Processing,* vol. 6, pp 1164-1175, Aug 1997.

[14] M.Wu. Joint Security and Robustness Enhancement for Quantization Based Data embedding. *IEEE Tran. on Circuit and System for Video Technology*, vol.13, pp 831-841, Aug 2003.

[15] J.L.Vehel and A.Manoury. Wavelet Packet based Digital Watermarking. Int. Conf. on Pattern Recognition, Barcelona, Spain**,** pp 413-416, Sep 2000.