WPT versus WT for a Robust Watermarking Technique

Shereen Ghannam† Fatma E. Z. Abou-Chadi††,

Electronics and Communication Engineering Dept., Mansoura University, Egypt

Summary
This paper investigates the role of Wavelet Packet transform (WPT) versus the Wavelet Transform (WT) in providing a watermarking technique with higher performance in resisting common signal processing attacks. The same embedding strategy is used for both cases of WPT-based watermarking and WT-based watermarking. Experimental results show the superiority of the WPT-based watermarking in resisting the investigated attacks especially for the case of histogram equalization attack.

Key words:
Wavelet Packet Transform, Wavelet Transform, robust, watermarking.

1. Introduction

Digital watermark has been prevalently utilized as a possible solution for intellectual property rights protection [1]-[3]. Several spatial-domain and frequency-domain digital watermarking algorithms have been proposed. Among the proposed transform-domain watermarking approaches, DWT-based (Discrete Wavelet Transform) technique have gained interest as it performs an analysis similar to that of the human visual system (*HVS*) [4,5]. Wavelet packet coefficients which are computed with a filter bank algorithm that generalizes the DWT are also utilized in a number of watermarking techniques [6].

Placing watermark information into the perceptually significant portions of data guarantees robustness against large number of attacks like compression, filtering, and scaling while placing it into the perceptually insignificant portions guarantees robustness against attacks like gamma correction and histogram equalization [5].

The embedding strategy presented in this paper relies on inserting the watermark values into appropriate locations in two bands representing low and high frequency components in order to achieve both imperceptibility and robustness. The two bands chosen for embedding differ for the case of Wavelet Packet Transform from the case of Wavelet Transform.

This paper is organized as follows: Section 2 provides a quick review on WT and *WPT*. Section 3 explains the watermarking steps. Section 4 briefly explains the performance evaluation criteria. Section 5 presents the experimental results and Section 6 gives the concluding remarks.

2. Wavelet Transform versus Wavelet Packet Transform

Although both Wavelet transform and Wavelet Packet Transform decomposes image into several bands representing low and high frequency, they differ from each other in the number of resultant bands.

2.1 Wavelet Transform (*WT*)

In two-dimensional separable dyadic DWT, the first level of decomposition produces four parts of low, middle, and high frequencies (i.e. *LL*1, *HL*1, *LH*1, *HH*1 sub-bands). The *LL*1 band stands for the coarse one which represents the low frequency part where most energy focuses. The sub-bands labeled *HL*1, *LH*1, and *HH*1 represent the details of wavelet coefficients. To obtain the next coarser wavelet coefficients, the sub-band *LL*1 is further decomposed as shown in Fig.(1). This process can be repeated several times, which is determined by the requirement of user.

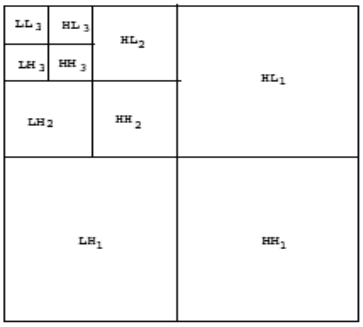


Fig.1 DWT Decomposition

2.2 Wavelet Packet Transform (*WPT*)

The wavelet packets transform is a generalization of the wavelet transform [7]. In the wavelet transform, only the low-pass filter is iterated. It is assumed that lower frequencies contain more important information than higher frequencies. This assumption is not true for many

Manuscript received January 5, 2009
Manuscript revised January 20, 2009

signals. The main difference between the wavelet packets transform and the wavelet transform is that, in the wavelet packets, the basic two-channel filter bank can be iterated either over the low-pass branch or the high-pass branch as shown in Fig. 2. This provides an arbitrary tree structure with each tree corresponding to a wavelet packet basis.
Wavelet packet bases are designed by dividing the frequency axis in intervals of varying sizes. These bases are thus particularly well adapted to decomposing signals that have different behavior in different frequency intervals.

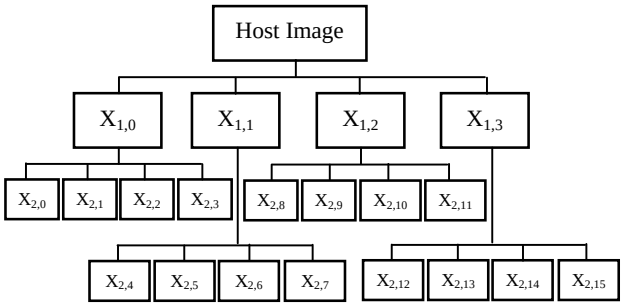


Fig. 2 The full quadtree of 2-level WPT

3. Watermarking Algorithm

The watermarking technique relies on embedding watermark into both low and high frequency components to achieve high robustness against all types of signal processing attacks but without introducing visual artifacts in the host image.

3.1 Watermark Embedding Procedure

Step1: Permute the watermark bits randomly using a secret seed in order to disperse the spatial relationship and to increase the invisibility based on the characteristics of images then map the values from {0,1} to {-1,1}.

Step2: Decompose the host image (x) into two levels using either *WPT or WT.*

Step3: The watermark is embedded into both low and high frequency components to achieve both invisibility and robustness.

- For the case of *WPT*, the nodes (2,0) and (2,12) are chosen for watermark embedding.
- For the case of *WT*, the LL_2 and HH_2 bands are chosen for embedding.

Step4: The selected coefficients for modification at the low frequency band are the first $m \times n$ coefficients after sorting them in ascending order while those at the high frequency band are the first $m \times n$ coefficients after sorting in descending order.

Step5: Modify the selected coefficients as follows:

$$f'_{lo}(i,j) = f_{lo}(i,j) + \alpha_1 w(i,j)\left|f_{lo}(i,j)\right| \quad (1)$$

where $\alpha_1 = \alpha / max(f_{lo})$

$$f'_{hi}(i,j) = f_{hi}(i,j) + \alpha_2 w(i,j)\left|f_{hi}(i,j)\right| \quad (2)$$

where $\alpha_2 = 2\alpha / max(f_{hi})$ and $\alpha = c.max(x)$

c is a user defined constant falls in [0.1,0.25]

Step6: Inverse Transform to obtain the watermarked image.

3.2 Watermark Extraction Procedure

In the proposed algorithm, the extraction of a watermark must refer to the original host image.

Step1: Decompose both of the host and watermarked images into the second level using either *WPT* or *WT.*

Step2: Extract the permuted values of the watermark from the selected coefficients at the two bands as follows:

$$w_1(i,j) = (f'_{lo}(i,j) - f_{lo}(i,j)) / \alpha_1 \left|f_{lo}(i,j)\right| \quad (3)$$

$$w_2(i,j) = (f'_{hi}(i,j) - f_{hi}(i,j)) / \alpha_2 \left|f_{hi}(i,j)\right| \quad (4)$$

Step3: Reverse permute the extracted logo values using the secret seed and map them back to the values {0,1}.

4. Performance Evaluation Metrics

To investigate the performance of the technique, it is essential to subjectively or objectively evaluate the quality of the image after the embedding process and evaluate the robustness of the extracted logos using appropriate metrics.

4.1 Perceptual Quality Evaluation Metrics

Objective image quality measures are based on image features, a functional of which, should correlate well with subjective judgement.

a. Error Sensitivity Based Metrics

A widely adopted assumption is that the loss of perceptual quality is directly related to the visibility of the error signal (watermark). The simplest implementation of this form is the *PSNR*, which quantifies the strength of the error signal.

- *Peak Signal to Noise Ratio (PSNR)*

It is a widely used fidelity measure. However, the correlation between it and the human judgement is not tight enough for most applications.

$$PSNR = 10 \log \left(\frac{L^2}{MSE} \right) \quad (5)$$

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} [y(i,j) - x(i,j)]^2 \quad (6)$$

where $L = 255$ is the dynamic range of the pixel values.

- *Weighted Peak Signal to Noise Ratio (wPSNR)*

wPSNR takes into account the local HVS sensitivity which is a measure criterion that holds account of the neighbors of the studied pixels [8].

$$wPSNR = 10 \log \left(\frac{L^2}{\| (y - x).NVF \|^2} \right) \quad (7)$$

where $$NVF = \frac{1}{(1 + \theta \, \sigma_x^2(i,j))} \quad (8)$$

$$\sigma_x^2(i,j) = \frac{1}{(2R+1)^2} \sum_{m=-R}^{R} \sum_{n=-R}^{R} (x(i+m, j+n) - \bar{x}(i,j))^2 \quad (9)$$

$$\theta = \frac{D}{\sigma_{x\,max}^2} \quad (10)$$

where σ^2_{xmax} is the maximum local variance of a given image over a window of size $(2R+1)\times(2R+1)$ and $D \in [50, 150]$ is a determined parameter.

b. Structural Similarity Based Metrics

Another category of image quality measures is based on the assumption that the human visual system is highly adapted to extract structural information from the viewing field [9]. The error sensitivity approach estimates perceived errors to quantify image degradations, while this approach considers image degradations as perceived structural information variation. The structural Similarity *(SSIM)* index can be calculated as a function of three components: luminance, contrast and structure.

$$SSIM(x,y) = [l(x,y)]^{\alpha} \cdot [c(x,y)]^{\beta} \cdot [s(x,y)]^{\gamma} \quad (11)$$

This results in a specific form of the SSIM index:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (12)$$

where $C_1 = (K_1 L)^2$, $K_1 << 1$ and $C_2 = (K_2 L)^2$, $K_2 << 1$.

For image quality assessment, it is useful to apply the SSIM index locally rather than globally. The local μ_x, σ_x and σ_{xy} are computed within a local square window, which moves pixel-by-pixel over the entire image. In practice one usually requires a single overall quality measure of the entire image.

$$MSSIM(X,Y) = \frac{1}{M} \sum_{j=1}^{M} SSIM(x_j, y_j) \quad (13)$$

4.2 Robustness Evaluation Metrics

Robustness is the ability of the watermark detector to extract the embedded watermark after different attacks. These attacks include common image processing operations such as filtering, compression, histogram equalization, intensity adjustment, gamma correction and geometric transformations like cropping and scaling. One of the most popular difference distortion measures is the Normalized Mean Squared Error (*NMSE*) metric which is defined as:

$$NMSE = \sum_{i,j} (y(i,j) - x(i,j))^2 / \sum_{i,j} x^2(i,j) \quad (14)$$

This metric is used to evaluate the distortion occurred in the extracted logo after attacks.

5. Experimental Results

A set of six 8-bit grayscale digital images, shown in Fig.3, were selected.

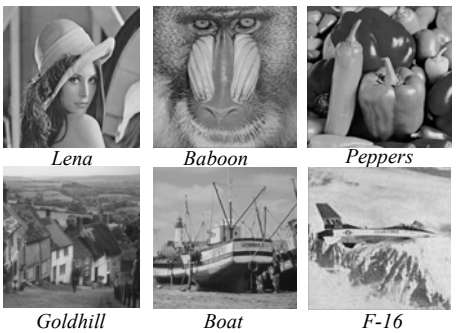


Fig.3 Image Database (size of 512×512 pixels)

The embedded watermark, shown in Fig.4, is a binary logo of size 32×32 pixels.

Fig.4 Embedded Watermark

5.1 Measuring Perceptual Quality

The PSNR, wPSNR and MSSIM values of each watermarked image are recorded in Table 1, Table 2 and Table 3 respectively.

Table 1 PSNR of watermarked images

	Lena	*Baboon*	*Peppers*	*Goldhill*	*Boat*	*F-16*
WPT-based	*41.1135*	*41.2084*	*41.1273*	*41.1728*	*41.1430*	*41.0333*
WT-based	*41.0143*	*41.0411*	*41.0432*	*41.1258*	*41.1108*	*41.0841*

Table 2 wPSNR of watermarked images

	Lena	*Baboon*	*Peppers*	*Goldhill*	*Boat*	*F-16*
WPT-based	*42.8968*	*47.8311*	*43.2061*	*43.0755*	*42.7345*	*44.0337*
WT-based	*43.2300*	*48.4609*	*43.3229*	*43.2545*	*43.1894*	*44.0140*

Table 3 MSSIM of watermarked images

	Lena	*Baboon*	*Peppers*	*Goldhill*	*Boat*	*F-16*
WPT-based	*0.9841*	*0.9960*	*0.9759*	*0.9838*	*0.9802*	*0.9899*
WT-based	*0.9859*	*0.9963*	*0.9809*	*0.9853*	*0.9817*	*0.9905*

The PSNR values of all the test images are adjusted at about 41 dB via choosing a suitable value of c from the range [0.1,0.25].

5.2 Measuring Robustness

Common signal processing attacks are applied to the watermarked images to measure and compare the robustness of the two techniques. The Normalized Mean Squared Error (*NMSE*) for the extracted logo after every attack is measured.

a. JPEG Compression Attack

JPEG is currently one of the most widely used compression algorithms and any watermarking system should be resilient to some degree of compression. JPEG compression with different quality factors are applied to the watermarked images resulted from the WPT-based and the WT-based watermarking techniques. The corresponding NMSE values are plotted against the quality factors in Fig.(5).

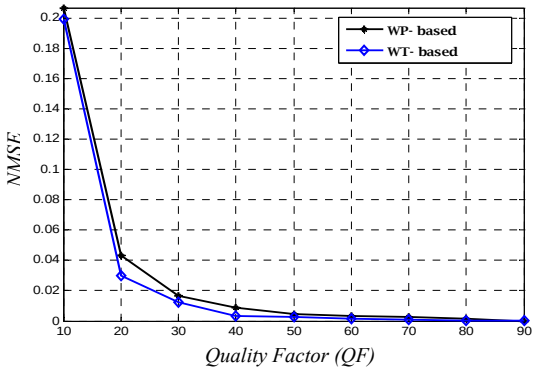


Fig.5 NMSE against Quality Factor of JPEG

b. JPEG2000 Compression attack

JPEG2000 is another kind of compression algorithms which uses wavelet instead of cosine transform. Fig.(6) shows the NMSE values of the extracted logos after applying JPEG2000 with different values of bit per pixel (*bpp*) on the watermarked images.

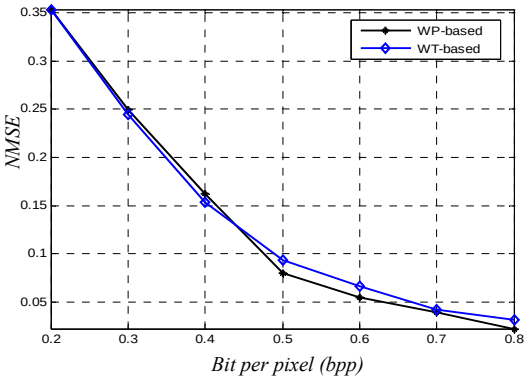


Fig. 6 NMSE against bit per pixel of JPEG2000

c. Median Filtering Attack

Median filtering is one of the most popular nonlinear enhancement techniques. The watermarked images are attacked by median filtering with different kernel (window) sizes. The corresponding NMSE values are plotted against the kernel size of the median filter in Fig.(7).

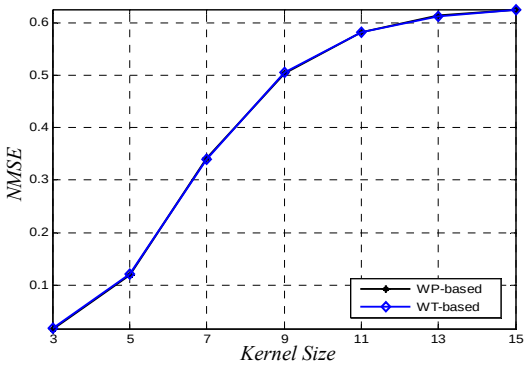


Fig.7 NMSE against kernel size of median filter

d. Wiener Filtering Attack

Wiener filter is another kind of enhancement techniques. Wiener filter is also applied to the watermarked images. Fig.(8) shows the NMSE values against different kernel sizes of wiener filter.

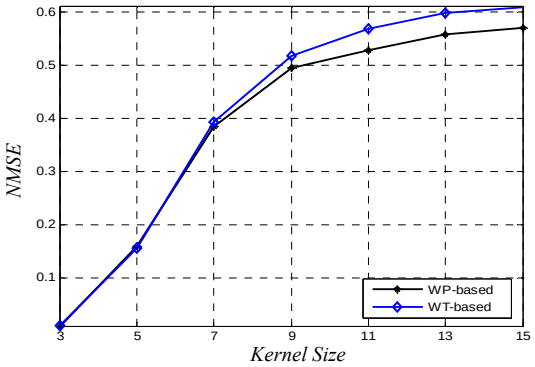


Fig.8 NMSE against kernel size of wiener filter

e. Cropping Attack

In Cropping, a smaller rectangular region of a larger image is extracted (cropped) and the remaining portions discarded. After applying cropping with different percentages, the NMSE values are measured and plotted against the percentage of discarded area in Fig.(9).

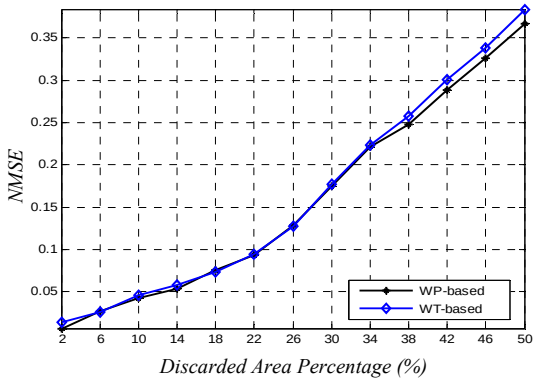


Fig.9 NMSE against percentage of discarded area

f. Resizing Attack

The watermarked images are scaled down in size by a factor of F and are resized to their original dimensions before watermark extraction. The NMSE values are plotted against different resizing factors in Fig.(10).

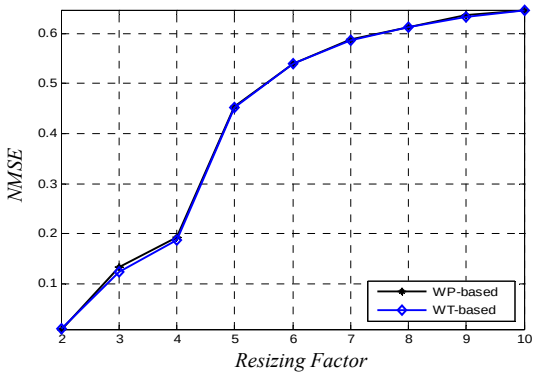


Fig.10 NMSE against resizing factor

g. Intensity Adjustment Attack

The intensity values between 0 and 0.8 in the watermarked images are mapped to values between 0 and 1and the NMSE values of the extracted logos are recorded in Table(4).

Table 4 NMSE of watermarked images after intensity adjustment

		Lena	*Baboon*	*Peppers*	*Goldhill*	*Boat*	*F-16*
WPT-based	*Lf*	*0.6228*	*0.6228*	*0.0048*	*0.6228*	*0.0000*	*0.6228*
	Hf	*0.0016*	*0.0000*	*0.0016*	*0.0032*	*0.0016*	*0.0127*
WT-based	*Lf*	*0.6228*	*0.6228*	*0.0000*	*0.6228*	*0.0000*	*0.6228*
	Hf	*0.0095*	*0.0000*	*0.0063*	*0.0000*	*0.0016*	*0.0681*

h. Gamma Correction Attack

If the function that used to map the intensity values in image into new ones is nonlinear, the operation is called gamma correction. Table(5) depicts the NMSE values of the extracted logos after applying gamma correction with factor 1.5 to the different watermarked images.

Table 5 NMSE of watermarked images after gamma correction

		Lena	*Baboon*	*Peppers*	*Goldhill*	*Boat*	*F-16*
WPT-based	*Lf*	*1.0000*	*1.0000*	*1.0000*	*1.0000*	*1.0000*	*1.0000*
	Hf	*0.0000*	*0.0000*	*0.0032*	*0.0000*	*0.0000*	*0.0000*
WT-based	*Lf*	*1.0000*	*1.0000*	*1.0000*	*1.0000*	*1.0000*	*1.0000*
	Hf	*0.0190*	*0.0048*	*0.1220*	*0.0032*	*0.0048*	*0.0016*

i. Histogram Equalization Attack

For each algorithm, the histogram of the watermarked images are equalized then the NMSE values of the extracted logos are measured and recorded in Table(6).

Table 6 NMSE of watermarked images after histogram equalization

		Lena	*Baboon*	*Peppers*	*Goldhill*	*Boat*	*F-16*
WPT-based	*Lf*	*1.0000*	*1.0000*	*0.0032*	*1.0000*	*1.0000*	*1.0000*
	Hf	*0.0063*	*0.0222*	*0.0000*	*0.0048*	*0.0063*	*0.0206*
WT-based	*Lf*	*1.0000*	*1.0000*	*0.0000*	*1.0000*	*1.0000*	*1.0000*
	Hf	*0.0650*	*0.5071*	*0.0365*	*0.0174*	*0.2282*	*0.2187*

6. Conclusion

This paper studies the role of the multiresolution analysis proposed by Wavelet Packet Transform in enhancing the performance of the presented watermarking strategy over the use of Wavelet Transform. Although the performance of the WT-based watermarking technique seems to be acceptable and very close to the performance of the WPT-based technique, some of the resultant NMSE values can be considered failure as in the case of histogram equalization on the watermarked baboon image. But the WPT-based watermarking technique succeeded in withstanding all the investigated signal processing attacks.

Working on the bands resulted from the decomposition performed by WPT represents the main reason for the superior performance of the WPT-based watermarking technique.

References

[1] F. Hartung, and M. Kutter, "Multimedia Watermarking Techniques", Proceedings of the IEEE, Special Issue on Identification and Protection of Multimedia Information 87, pp 1079-1107, July 1999.

[2] V. M. Potdar, S. Han, and E. Chang, "A Survey of Digital Image Watermarking Techniques", 3rd International Conference on Industrial Informatics, 2005.

[3] C. S. Lu, Multimedia Security: Steganography and Digital Watermarking for Protection of Intellectual Property, Idea Group Publishing, 2005.

[4] S. Joo, Y. Suh, J. Shin, and H. Kikuchi, "A New Robust Watermarking Embedding into Wavelet DC Components", ETRI Journal, vol. 24, no. 5, pp. 401-404, October 2002.

[5] 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.

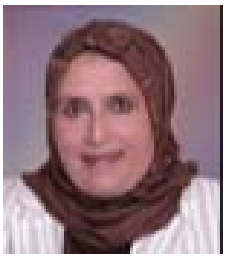
[6] P. Kumhom, S. On-rit, K. Chamnongthai, "Image Watermarking Based On Wavelet Packet Transform With Best Tree", ECTI Transactions on Electrical Engineeing, Electronics and Communications, vol. 2, No.1, February 2004.

[7] R. R. Coifman and M. V. Wickerhauser, "Entropy-Based Algorithms for Best Basis Selection", IEEE Transactions on Information Theory, vol. 38, No. 2, pp. 713-718, 1992.

[8] S. Voloshynovskiy, S. Pereira, A. Herrigel, N. Baumgartner, T. Pun, "A Stochastic Approach to Content Adaptive Digital Image Watermarking", Proceedings of the Third International Workshop on Information Hiding, pp.211-236, 1999.

[9] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error measurement to structural similarity" IEEE Transactions on Image Processing, vol. 13, No. 1, January 2004.

Shereen Ghannam received the B.S. in Electronics and Communications Engineering from Faculty of Engineering, Mansoura University, Egypt in 2004. She works as a demonstrator in Electronics and Communications Engineering Department, in Faculty of Engineering, Mansoura University since 2005. She is now preparing for M.S. degree in Electrical Engineering. Her interests include signal processing, image processing and information security.



Fatma El-Zahraa Abou-Chadi is currently a professor and head of department of Electronics and Communications Engineering Department, Faculty of Engineering, Mansoura University, Egypt. Her research interests focus on digital signal processing, image processing and biomedical engineering.