IMAGE WATERMARKING BASED ON WAVELET HARD THRESHOLDING

Mahmood Al-khassaweneh and Selin Aviyente

Department of Electrical and Computer Engineering,
Michigan State University, East Lansing, MI
e-mail:{alkhassa, aviyente}@egr.msu.edu

ABSTRACT

In this paper, we present a robust watermarking technique that uses the wavelet based hard thresholding concept for image denoising to determine the wavelet coefficients to be watermarked. A multi-bit watermark is embedded into the discrete wavelet coefficients of a still image. A corresponding blind watermark extraction algorithm is proposed. The proposed method is compared with other multiresolution watermarking methods. The simulation results show that the proposed method provides better performance under most attacks including JPEG compression.

1. INTRODUCTION

Image watermarking is the process of embedding a secret message, watermark, inside an image such that the visual perception of the watermarked image is unaltered and the watermark is invisible and robust to attacks. This secret watermark is used for copyright protection and ownership authentication. The two traditional approaches for image watermarking are the spatial and spectral domain techniques. In the spatial domain, the watermark is embedded in selected regions chosen based on the texture of the given image [1, 2]. While in the spectral domain, the watermark is embedded in the transform domain using methods such as DCT and DWT, in the mid-frequency range to ensure transparency and robustness of the watermark, simultaneously [3]. The DWT remains one of the most effective and easy to implement techniques in image watermarking. It has also been used in various image processing applications such as image denoising. The biggest issue in DWT-based image watermarking is how to choose the coefficients to embed the watermark. The most common approaches include modifying the largest DWT coefficients in all decomposition levels or quantizing certain DWT coefficients in different levels and scales. Other approaches mark the host image by setting modulo 2 difference between the largest and the smallest coefficients according to the watermark bit value [4, 5].

The effectiveness of DWT-based image denoising in separating the wavelet coefficients that belong to the noise and the signal motivates us to use it for watermarking. The threshold derived for separating the 'significant' and the 'insignificant' coefficients, i.e. signal and noise, will be used to determine the coefficients to be watermarked.

The paper is organized as follows. Section 2 gives a brief background on the use of DWT in watermarking and denoising. Section 3 describes the embedding stage of the watermarking algorithm while Section 4 derives the extraction algorithm. In Section 5, the performance of the algorithm under different attacks is demonstrated. A summary of the paper and some conclusions are given in Section 6.

2. BACKGROUND

In this paper, we use the DWT for embedding the watermark. The multiresolution wavelet transform of an image decomposes the image into bands of approximately equal bandwidth on a logarithmic scale. Similarly, the retina of the human eye splits the image into several components, each having a bandwidth of approximately one octave. Therefore, it is believed that the use of DWT for watermarking will produce an imperceptible watermark [4]. The use of the DWT domain for image watermarking and denoising have been studied in detail. The DWT splits the signal into high and low frequency parts. The high frequency part contains information about the edge components, while the low frequency part is split again into high and low frequency parts as in Fig 1. The high frequency components are usually used for watermarking since the human eye is less sensitive to changes in edges [6]. In watermarking, the main concern besides invisibility of the watermark is how to choose the coefficients to be watermarked such that they will survive the possible attacks that the transmitted image may go under. While for denoising, the concern is to get rid of the coefficients that do not carry important information, i.e noise. The proposed method uses the concept of image hard thresholding to determine which coefficients not to embed the watermark into. This involves finding the threshold for hard denoising and keeping all the coefficients under this threshold unmodified and choosing the coefficients just above the threshold to embed the watermark. This approach ensures simultaneously that the 'noise' or the 'insignificant' coefficients and the large coefficients which correspond to the 'visible' part of the image are not altered. This, in return, ensures imperceptibility and robustness of the proposed watermarking algorithm.

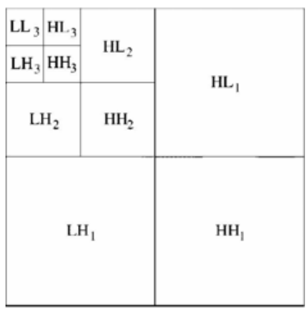

Figure 1: Three levels discrete wavelet decompositions.

3. WATERMARK EMBEDDING

In this paper, we assume that the original image I is of size $N \times N$ and the watermark, w, is a binary sequence of length R, which takes values from $\{1,-1\}$. The embedding algorithm can be summarized as follows:

1. Obtain the Lth level DWT of the original image to obtain the detail (horizontal HL_l, vertical LH_l and diagonal HH_l) images at each level $l = 1,2,...L$, plus the approximation at the Lth level. In this paper, L is set to 3.
2. For each orientation in level l , $s_l \in \{HL_l, LH_l, HH_l\}$, find all coefficients that satisfy: $C_{s_l}(n,m) > \hat{T}_B$, where l is the wavelet decomposition level, s is the orientation and $\hat{T}_B$ is the threshold for hard de-noising given by [7]:

$$\hat{T}_B = \frac{\hat{\sigma^2}}{\hat{\sigma_x^2}}, Y_{ij} \in \text{subband } HH_1, \tag{1}$$

where

$$\hat{\sigma^2} = \frac{Median(|Y_{ij}|)}{0.6745}, \tag{2}$$

$$\hat{\sigma_x} = \sqrt{max\left(\hat{\sigma_Y^2} - \hat{\sigma^2}, 0\right)}, \tag{3}$$

$$\hat{\sigma_Y^2} = \frac{1}{n^2}\sum_j^n = Y_{ij}^2 \tag{4}$$

This threshold is derived based on the generalized gaussian model for the wavelet coefficients and it minimizes the mean square error for hard thresholding.

3. Arrange the coefficients found in step 2 in descending order with respect to their absolute values.
4. Take the last R coefficients found in step 3 at each scale and proceed as follows:

$$C_{s_l}(n,m) = w_r \cdot \alpha \left|C_{s_l}(n,m)\right|, \quad r = 1,2,...R. \tag{5}$$

where α is a positive constant that controls the strength of the watermark embedding.

5. Save the locations of the modified coefficients as a key K. The key has value one if the coefficient is modified and zero if not.
6. Find the inverse DWT to obtain the watermarked image.

This method modifies some of the coefficients with values greater than $\hat{T}_B$ by scaling them with a constant α. Since the high coefficients which correspond to the 'visible' part of the image are not altered, the imperceptibility of the watermark is ensured even if the watermark is added in all levels.

4. WATERMARK DETECTION

For copyright protection applications, it is important to detect or extract the watermark even after the watermarked image is attacked. The extraction process can be summarized as follows:

1. Find the Lth level DWT of the received image $\hat{I}$.
2. Find the modified coefficients according to the given key K.
3. For each orientation s_l in every level l, estimate the value of the watermark bit according to the sign of the corresponding wavelet coefficient $\hat{C_{s_l}}(n,m)$:

$$\begin{aligned} &\text{if} \quad \hat{C_{s_l}}(n,m) > 0, \qquad \hat{w}_r = 1 \\ &\text{else} \quad \hat{w}_r = -1, \quad r = 1,2,...R. \end{aligned} \tag{6}$$

4. The most common bit value of the watermark among the different scales and levels is assigned to the estimated watermark.

The following correlation based detector is applied to determine the similarity between the extracted watermark, $\hat{w}$, and the actual one, w,

$$\langle w(n), \hat{w}(n)\rangle \underset{no\ watermark}{\overset{watermark}{\gtrless}} \eta. \tag{7}$$

The expected value of the maximum of this correlation is,

$$\eta_{max} = R. \tag{8}$$

Let,

$$z = \sum_n w(n)\hat{w}(n). \tag{9}$$

The threshold η is derived by applying the Neyman-Pearson criterion to this detection statistic, which corresponds to solving,

$$\overline{P_{FA}} = \int_\eta^{+\infty} f_z(z|H_0)\, dz, \tag{10}$$

where $f_z(z|H_0)$ is the pdf of z. The mean and the variance of z, since $w(n)\hat{w}(n)$ takes only two values -1 and 1 with equal probability, are given by,

$$\mu_z = 0. \tag{11}$$

$$\sigma_z^2 = R. \tag{12}$$

By applying the central limit theorem [8], the pdf of z can be assumed to be a normal distribution. Therefore, $\overline{P_{FA}}$ is given by,

$$\overline{P_{FA}} = Q\left(\frac{\eta}{\sqrt{R}}\right), \tag{13}$$

where $Q(y) = \frac{1}{\sqrt{2\pi}} \int_y^{+\infty} \exp\left(-\left(\frac{t^2}{2}\right)\right) dt$. For a given $\overline{P_{FA}}$, the threshold, normalized by its maximum value, can be written as,

$$\eta = \frac{Q^{-1}(\overline{P_{FA}})}{\sqrt{R}}. \tag{14}$$

The result in (14) shows that the choice of η should be dependent on the length of the watermark R. In particular, for $R = 128$ and $\overline{P_{FA}} = 0.01$, $\eta = 0.203$.

5. RESULTS

The watermark embedding algorithm proposed in this paper has been applied to the well-known Lena image of size 256×256. The watermark is a randomly generated sequence with values 1 and -1 of length 128 and is embedded into every resolution level using three level wavelet decomposition with haar filter and $\alpha = 6$ unless otherwise mentioned. The resultant watermarked image is similar to the original one with no visible differences with PSNR=$47.1dB$. The algorithm has been tested under different attacks. Table 1 shows the effect of the choice of α on the robustness of the proposed algorithm under additive white gaussian noise 'AWGN', JPEG compression, median filtering 'MF' and rotation. It is clear that increasing α improves the robustness of the algorithm. It is important to note that α should be chosen such that the imperceptibility of the watermark is maintained, so the choice of α is image dependent and for Lena image, it is found that $\alpha < 8$ will produce an invisible watermark and high PSNR. The PSNR ranges from $59.5dB$ for $\alpha = 1$ to $45.8dB$ for $\alpha = 7$.

Table 2 shows the effect of the watermark length R in the robustness of the proposed algorithm. The results are very close to each other for AWGN, JPEG and rotation attacks, while increasing R improves the robustness of the watermark under median filtering (MF).

Table 1: The correlation between the extracted and original watermarks under different types of attacks with different α values.

α	1	4	7
AWGN (PSNR=45db)	0.73	1	1
AWGN (PSNR=40db)	0.53	0.96	0.98
AWGN (PSNR=30db)	0.27	0.75	0.79
AWGN (PSNR=20db)	0.1	0.2	0.52
JPEG (Q=70%)	0.23	0.76	0.77
JPEG (Q=80%)	0.41	0.87	0.88
JPEG (Q=90%)	0.55	0.94	0.95
JPEG (Q=100%)	1	1	1
MF (1×1)	1	1	1
MF (3×3)	0.55	0.88	0.9
MF (5×5)	0.15	0.55	0.65
MF (7×7)	0.1	0.4	0.4
Rotation (1°)	0.85	1	1
Rotation (3°)	0.8	0.98	0.98
Rotation (5°)	0.8	0.97	0.97
Rotation (7°)	0.77	0.97	0.97

Table 2: The correlation between the extracted and original watermarks under different types of attacks for different watermarks with different lengths with $\alpha = 6$.

R	32	64	128
AWGN (PSNR=45)	1	1	1
AWGN (PSNR=40)	0.99	0.97	0.98
AWGN (PSNR=30)	0.7	0.75	0.74
AWGN (PSNR=20)	0.2	0.34	0.33
JPEG (Q=70%)	0.5	0.45	0.70
JPEG (Q=80%)	0.5	0.5	0.75
JPEG (Q=90%)	0.7	0.62	0.85
JPEG (Q=100%)	1	1	1
MF (1×1)	1	1	1
MF (3×3)	0.82	0.73	0.90
MF (5×5)	0.56	0.50	0.55
MF (7×7)	0.56	0.5	0.5
Rotation (1°)	1	1	1
Rotation (3°)	0.97	1	0.98
Rotation (5°)	0.98	0.97	0.97
Rotation (7°)	0.99	0.98	0.97

A comparison with another well-known DWT based algorithm introduced by Kundur and Hatzinakos has been performed [4]. The authors in [4] propose a DWT based watermarking algorithm based on quantizing certain DWT coefficients at each level. The same watermark has been used in both methods. The two methods were tested under attacks, AWGN, JPEG compression and median filtering (MF). Fig. 2 shows the correlation between the extracted watermark and the original one under different attacks for both methods. Although the performance under AWGN is very close, the proposed method performs better under JPEG compression and median filtering. One reason of this improvement is that the method in [4] modifies some of the DWT coefficients with small values (less than $\hat{T}_B$) which are not robust against attacks. Another reason is that the proposed method always chooses coefficients greater than $\hat{T}_B$ and embeds the watermark in a multiplicative way in all levels, which makes it more robust against attacks.

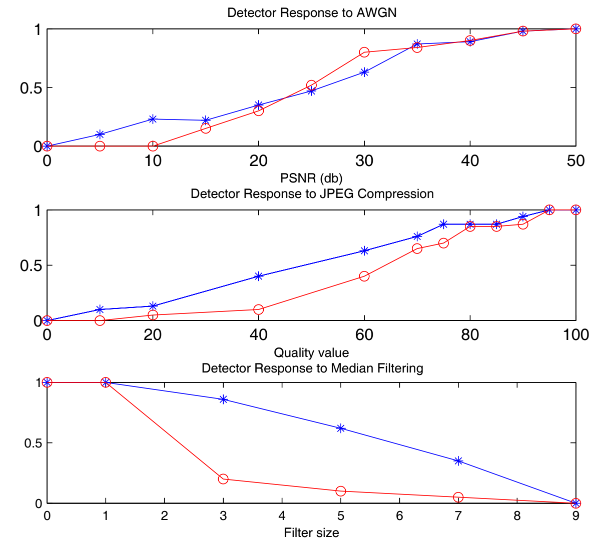

Figure 2: The comparison of the proposed method and the method in [4] under AWGN, JPEG compression and median filtering. The plots with '*' corresponds to the proposed algorithm.

6. CONCLUSIONS

In this paper, we have presented a new robust watermarking algorithm based on DWT. The algorithm uses the idea of hard de-noising for choosing the coefficients to be watermarked. The performance of the proposed blind detection algorithm is quantified by deriving the optimum threshold for a given false alarm rate. The proposed algorithm is shown to be transparent and highly robust under attacks. The proposed algorithm performs better than a previously introduced DWT based method. The effect of the choice of α and the watermark length were studied. Future work will focus on finding the optimal α and studying the possibility of applying soft thresholding in choosing the coefficients to be watermarked.

REFERENCES

[1] N. Nikolaidis and I. Pitas, “Robust image watermarking in the spatial domain,” *Signal Processing*, vol. 66, pp. 385–403, 1998.

[2] O. Bruyndonckx, J. J. Quisquater, and B. Macq, “Spatial method for copyright labeling of digital images,” in *Proc. IEEE Workshop on Nonlinear Signal and Image Processing*, June 1995, pp. 456–459.

[3] S. Pereira, S. Voloshynoskiy, and T. Pun, “Optimal transform domain watermark embedding via linear programming,” *Signal Processing*, vol. 81, no. 6, pp. 1251–1260, June 2001.

[4] D. Kundur and D. Hatzinakos, “Digital watermarking using multiresolution wavelet decomposition,” in *International Conference on Acoustic, Speech and Signal Processing (ICASP)*, Seattle, Washington, U.S.A., 1998, vol. 5, pp. 2969–2972.

[5] J. Ohnishi and K. Matsui, “Embedding a seal into a picture under orthogonal wavelet transform,” in *International Conference on Multimedia Computing and Systems*, 1996, pp. 514–521.

[6] X. G. Xia, C. G. Boncelet, and G. R. Arce, “A multiresolution watermark for digital images,” in *IEEE International Conference on Image Processing*, 1997, vol. 3, pp. 548–551.

[7] G. Chang, B. Yu, and M. Vetterli, “Adaptive wavelet thresholding for image denoising and compression,” *IEEE Trans. Image Processing*, vol. 9, pp. 1532–1546, Sept. 2000.

[8] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*, McGraw-Hill, New York, 1991.