A Robust Digital Image Watermarking Scheme Based on DWT

Mohammad Reza Soheili
Department of Computer Engineering,
Faculty of Engineering,
Tarbiat Moallem University, Tehran, Iran
E-mail: soheili@tmu.ac.ir

Abstract

In this paper a wavelet-based logo watermarking scheme is presented. The logo watermark is embedded into all sub-blocks of the LLn sub-band of the transformed host image, using quantization technique. Extracted logos from all sub-blocks are merged to make the extracted watermark from distorted watermarked image. Knowing the quantization step-size, dimensions of logo and the level of wavelet transform, the watermark is extracted, without any need to have access to the original image.Robustness of the proposed algorithm was tested against the following attacks: JPEG2000 and old JPEG compression, adding salt and pepper noise, median filtering, rotating, cropping and scaling. The promising experimental results are reported and discussed.

Keywords: *Wavelet transform, watermarking, quantization technique.*

1. Introduction

Nowadays protecting the copyright of the digital media has become an important topic due to digital media can be copied and modified easily. Many watermarking techniques have been proposed to solve the copyright protection problem for multimedia images.

The spatial and transform domains are two common methods for image watermarking. Embedding the watermark into the transform-domain generally helps to increase the imperceptibility, security, and robustness. Therefore, at present, most of image watermarking methods are in the transform domain, where DFT [1], DCT [2], DWT [3] are three main transform methods used. In terms of the extracting scheme, watermarking algorithms are also divided into two groups: blind and non-blind watermarking. In a non-blind watermarking the original image is necessary for the watermark extraction whereas in a blind watermarking the original image is not needed for watermark extraction.

The paper is organized as follows. Section 2 explains the proposed algorithms for watermark embedding and extraction. Experimental results are presented in Section 3.

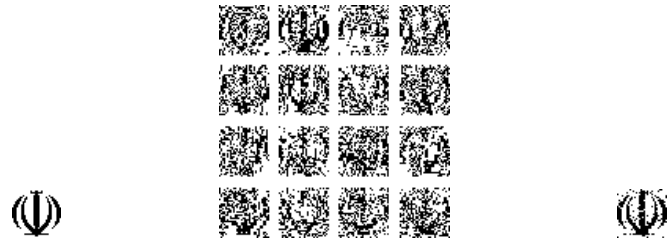
2. Proposed Watermarking Scheme

Nowadays, most watermarking algorithms use wavelet and quantization techniques; use of wavelet domain watermarking has the advantage of making the watermark robust against many of the distortions that change high frequency components of image such as compression and low-pass filtering, however it cannot resist the attacks such as

cropping that destroy a whole region of the watermarked image because each pixel of watermark is usually embedded only in one region of the host image.

Most of the wavelet based watermarking methods divide a wavelet sub-band to small sub-blocks and then embed each bit of logo watermark in one sub-block by quantizing the coefficients of that sub-band but for increasing robustness of our scheme against cropping attack, we proposed a method that embeds one logo in each sub-block. Therefore each bit of the logo watermark is stored in one coefficient of a sub-block to remain the capacity of watermarking fixed.

When a region of the watermarked image is destroyed; the whole watermark can be extracted using other regions of the watermarked image by merging extracted watermarks. Figure 1 shows result of merging logo watermarks that were extracted from a compressed (with JPEG2000 algorithm) watermarked image



(a) (b) (c)

Figure 1. (a) original watermark (b) extracted watermarks after compression (c) merged watermark

2.1. Watermark Embedding Algorithm

Suppose the host image I is a gray-level image with N by N pixels and logo watermark W is a binary image with M by M pixels.

$I = \{ I(i,j) \mid 1 \le i \le N , 1 \le j \le N , 0 \le I(i,j) \le 255 \}$
$W = \{ W(i,j) \mid 1 \le i \le M , 1 \le j \le M , W(i,j) \hat{I} \{0,1\} \}$

The watermark is embedded through the following steps:

Step 1: The host image is decomposed into *n* level using discrete wavelet transform. We select LL_n sub-band of the decomposed image for watermark embedding.

Step 2: The selected sub-band is divided into small sub-blocks B_k with the size of $M \times M$. Figure 2 shows the sub-blocks.

Step 3: The logo watermark is inserted to all of the sub-blocks by quantizing the coefficients of them according to the following formula:

$$q'_k(i,j) = \begin{cases} mQ & mQ < q_k(i,j) \le (m+0.5)Q \\ (m+1)Q & (m+0.5)Q < q_k(i,j) \le (m+1)Q \end{cases} \quad W(i,j) = 1$$

$$q'_k(i,j) = (m+0.5)Q \quad W(i,j) = 0$$

Where $q_k(i,j)$ is used to represent wavelet coefficients of B_k sub-block and $q_k'(i,j)$ is used to represent the same coefficients after quantization. $W(i,j)$ is the logo watermark, *m* is an integer and *Q* is the quantization step size.

Step 4: Finally with new coefficients values the host image is reconstructed to form the watermarked image.

The choice of *n* should be made based on an optimal compromise among robustness, invisibility and the attack. With a good choice, the watermark could be made more robust against image degrading. Selecting small *n* can cause to reduce robustness of

algorithm but will increase execution speed and decrease the degradation of watermarked image. Selecting large *n* can also cause to increase robustness of algorithm but will decrease the dimensions of LL_n region therefore cause to decrease number of sub-blocks(*K*).

It is obvious that there is a relation between *N*, *M* , *n* and *K*; in optimal case:

$N=M\times K\times 2^n$

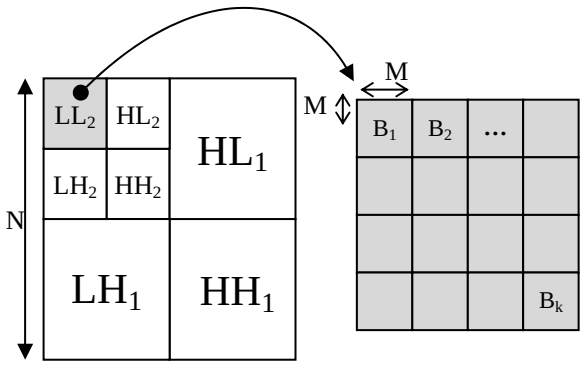


Figure 2. LL2 sub-band is divided into sub-blocks

2.2. Watermark Extraction Algorithm

Whereas most of methods for watermark extraction require the original image, the proposed method does not. For extracting watermark logo, size of host image, size of watermark image, quantization step size (Q), level of decomposition (n), number of sub-blocks (K) is needed.

The watermark is extracted through the following steps:

Step 1: The watermarked image is decomposed into level *n* using discrete wavelet transform. LL_n sub-band of the decomposed image is divided into sub-blocks B_k with the size of $M\times M$.

Step 2: Pixels of logo watermark W_k corresponded to each sub-block B_k are extracted with the following formula

$$W_k(i,j)=\begin{cases}1 & (m-0.25)Q\le q_k(i,j)\le(m+0.25)Q\\ 0 & (m+0.25)Q<q_k(i,j)<(m+0.75)Q\end{cases}$$

Where $q_k(i,j)$ is used to represent wavelet coefficients of sub-block B_k, *m* is a an integer and *Q* is the quantization step size.

Step 3: If no distortion was happened for watermarked image, all extracted logos W_k should be the same as the embedded logo. But if any distortion was happened for watermarked image, the extracted watermarks should be merged by voting to obtain the final result. Merging is done according to the following formulas [4]:

$$W(i,j)=\begin{cases}1 & E(i,j)\ge\frac{1}{2}K\\ 0 & E(i,j)<\frac{1}{2}K\end{cases}$$

$$E(i,j)=\sum_{k=1}^{K}W_k(i,j)$$

Where $W_k(i,j)$ is used to represent extracted watermark from sub-block B_k and $W(i,j)$ is used to represent the merged watermark. *K* is number of sub-blocks.

3. Exprimental Results

In the following experiments, two gray-level images with size of 512 by 512, "Airplane" and "Peppers" are the test images. The binary image "Allah" with size of 32 by 32 is used in our simulations as a watermark. Figure 3 shows the watermark. In the experiments Haar wavelet filter were used for discrete wavelet transform. The level of wavelet decomposition (n) and the number of sub-blocks (K) were also assumed to be 2 and 16 respectively.

Figure 3. The watermark used for embedding

The proposed watermarking algorithm is evaluated from the point of view of embedded watermark transparency and robustness; the result of each is shown in next two sections.

3.1. Image Quality

The PSNR (Peak Signal to Noise Ratio) is widely used to measure the difference between two images based on pixel differences. In the watermarking case, is used to evaluate the quality of the watermarked image. For a $N_1 \times N_2$ pixels image with pixels' luminance values ranging from zero (black) to L_{max} (white), the PSNR is defined as[5]:

$$PSNR = 10\log_{10}\frac{L_{\max} \times L_{\max}}{MSE}$$

Where MSE is mean square error defined as:

$$MSE = \frac{\sum_{i=1}^{N_1}\sum_{j=1}^{N_2}[I_o(i,j) - I_w(i,j)]^2}{N_1 \times N_2}$$

Where I_o and I_w are the respective luminance values of the original and watermarked images.

Selecting a good Q for this scheme is a very important because increasing Q can cause degradation of visual perception of watermarked image but increases it's robustness against most of attacks; therefore Q and PSNR are in inverse proportion.

But this measure is not very accurate and we can't select the correct Q value according to the PSNR value; the threshold of Q for degradation of watermarked image is different for every image and depends on its spatial frequency. Figure 4 shows original and watermarked images of "peppers" and "Airplane".

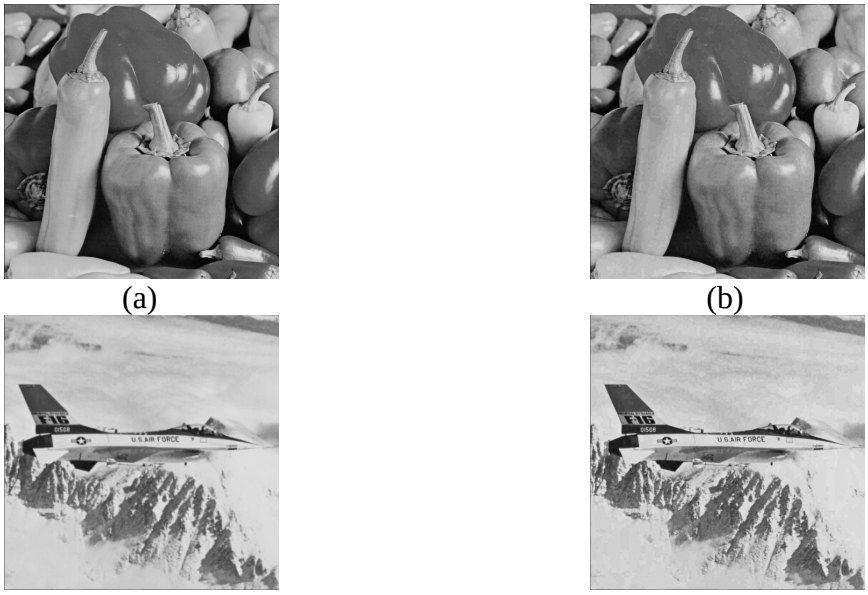


Figure 4. (a) The original "Peppers" image (b) Watermarked "Peppers" with Q=35 (c) The original "Airplane" image (d) Watermarked "Airplane" with Q=35

3.2. Robustness Against Image Processing

A set of distortions is applied to the watermarked image and the watermark is extracted from the distorted image. We used bit correct rate (BCR) to evaluate our proposed algorithm and it is calculated from the following equation [6]:

$$BCR = \frac{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2} \overline{W(i,j) \oplus W'(i,j)}}{M_1 \times M_2}$$

Where *W(i,j)* and *W'(i, j)* are respectively original and extracted watermarks with size of $M_1 \times M_2$ pixels.

The robustness of the proposed watermarking scheme is evaluated against several attacks including adding Salt&Pepper noise, rotation, scaling, cropping, filtering, JPEG and JPEG2000 compression. Table 1 shows PSNR and BCR values of the watermarked images under above distortions.

Table 1. PSNR (dB) of distorted watermarked images and BCR values of extracted watermarks under different distortions.

Host Image	**Pepper (Q=35)**		**Airplane (Q=35)**	
Attacks	PSNR	BCR	PSNR	BCR
Jpeg2000 (rate = 0.1 bpp)	36.03	0.99	37.96	0.99
Jpeg (Quality=20%)	32.30	0.91	32.43	0.93
Median Filter (window 7×7)	30.12	0.91	26.76	0.95
Salt&Pepper Noise(nd=0.05)	18.41	0.93	17.85	0.82
Image Resize (scale = ¼)	27.84	0.98	26.14	0.97
Image Rotation (deg = 0.5°)	23.31	0.86	22.23	0.91
Center Crop (40%)	9.33	0.98	7.19	0.98
Surrounding Crop (45%)	9.29	0.95	5.97	0.97

In general digital images are stored and transmitted after image compression. JPEG is more popular among image compression methods for still images. The watermarked images are compressed by JPEG2000 and JPEG compression with different compression ratios. Figure 5(a1) and (a2) show the compressed version of figure 4(a) respectively under JPEG2000(0.1 bpp) and JPEG(Quality=20%) compression. The corresponding extracted results are showed in figure 5 (b1) and (b2) with high BCR values (0.99) and (0.91).

We investigate the robustness by smoothing the watermarked image with median filter whose window size is 7×7 pixels. Figure 5(a3) shows the smoothed version of figure 4(a) under median filtering. The corresponding extracted result is showed in figure 5(b3) with high BCR value (0.91).

We evaluate the robustness by adding Salt&Pepper noise to the watermarked image. In this test density of additive noise was 0,05. Figure 5(a4) shows image of figure 4(a) after adding Salt&Pepper. Extracted watermark is showed in figure 5(b4) with high BCR value (0.93).

In figure 5(a5), Even though the wavelet transform is not rotational invariant, our proposed method can extract the watermark for small rotations. Extracted logo from 0.5° rotated watermarked image with BCR value of (0.86) is shown in Figure. 5(b5).

As we predicted, this watermarking method is very robust against image cropping; we extract 98% and 95% of watermark from the watermarked images that was cropped from center and surrounding with ratios of 40% and 45% respectively. Figure 5(a6) and (a7) show these cropped watermarked images and their corresponding extracted results are showed in figure 5(b6) and (b7).

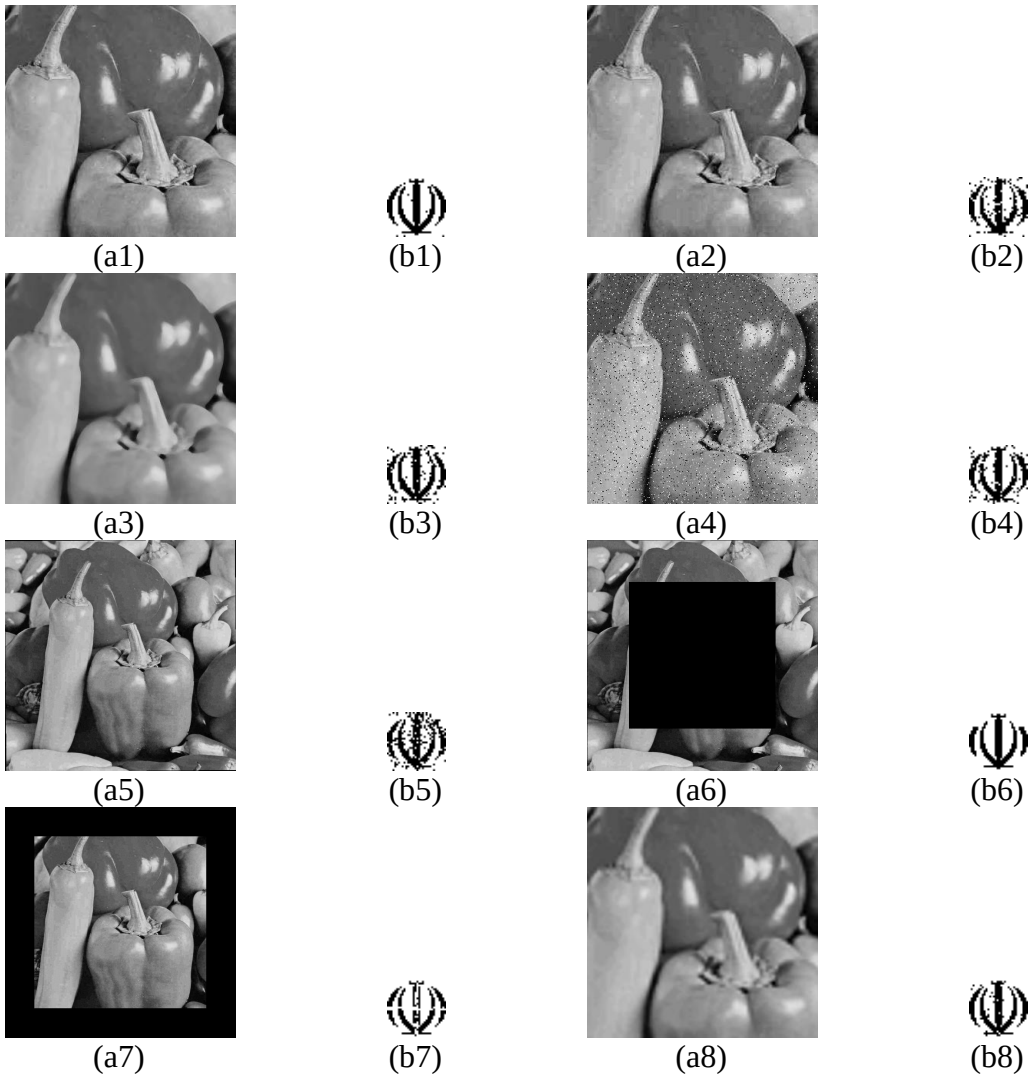


Figure 5. (a1), (a2), (a3), (a4), (a5), (a6), (a7) and (a8) watermarked image is degraded respectively through JPEG2000 compression, JPEG compression, median filtering, adding Salt&Pepper noise, rotating, center cropping, surrounding cropping and scaling. (b1), (b2), (b3), (b4), (b5), (b6), (b7) and (b8) The corresponding extracted watermarks.

Image resizing is also a common geometric transformation. The watermarked image is reduced to 25% of its original image size. Next, in order to detect the watermark, the reduced image is recovered to its original dimensions. Figure 5(a8) shows the reduced and recovered version of figure 4(a) and extracted watermark with high BCR value of (0.98) is shown in figure 5(b8).

The above simulations and analyses have all confirmed that the proposed scheme has high robustness against common geometric transformations, filtering, and compression. However, this scheme cannot well resist rotation and additive noise attacks. In some cases, we cannot detect the watermark correctly.

4. Conclusions

This paper has described a scheme for digital watermarking of still images based on discrete wavelet transform. In the proposed method, the embedded logo watermark can be extracted without access to the original image. It has been confirmed that the proposed watermarking method is able to extract the embedded logo watermark from the watermarked images that have degraded through compression, filtering, cropping and scaling. Although this algorithm is not robust against rotation, it can completely extract the watermark from watermarked images that lost about 35% of their areas by cropping attack.

References

[1] Wei W.; Aidong M.; Xiaobo C., "Robust Image Watermarking Scheme Based on Phase Features in DFT Domain and Generalized Radon Transformations", *2nd International Congress on Image and Signal Processing*, pp.1-5, Oct. 2009.

[2] Yigang Z.; Jia L., "Blind Watermarking Algorithm Based on DCT for Color Images," *2nd International Congress on Image and Signal Processing*, pp.1-3, Oct. 2009.

[3] Dazhi Z.; Boying W.; Jiebao S.; Heyan H., "A New Robust Watermarking Algorithm Based on DWT," *2nd International Congress on Image and Signal Processing*, pp.1-6, Oct. 2009.

[4] Soheili, M.R., "Redundant watermarking using wavelet packets", *IEEE/ACS Int. Conf. on Computer Systems and Applications*, pp.591-598, March 31 2008-April 4 2008.

[5] Ghannam, S.; Abou-Chadi, F.E.Z., "Enhancing performance of image watermarks using Wavelet Packet", *Int. Conf. on Computer Engineering & Systems*, pp.83-87, Nov. 2008.

[6] Tzu-Chao L., Chao-Ming L., "Wavelet-based copyright-protection scheme for digital images based on local features", *Journal of Information Sciences*, Volume 179, Issue 19, pp. 3349-3358, Sep. 2009.