Proceedings of the 5th WSEAS International Conference on Applications of Electrical Engineering, Prague, Czech Republic, March 12-14, 2006 (pp48-53)

Robustness Evaluation of Multiwavelet-Based Image Watermarking Techniques

PRAYOTH KUMSAWAT[1], KITTI ATTAKITMONGCOL[1] AND ARTHIT SRIKAEW[2]
[1]Signal and Image Processing Research Group, [2]Intelligent System Research Group
School of Electrical Engineering, Institute of Engineering
Suranaree University of Technology
111 University Avenue, Muang District, Nakhon Ratchasima, 30000
THAILAND

Abstract:- This paper presents the evaluation of robustness for image watermarking techniques in the multiwavelet transform domain. The first one is based on the concept of the watermarking technique that has been designed in the previous chapter and the second one is based on the code division multiple access (CDMA) technique. The embedding information is a visually recognizable pattern which can be extractable not just detectable to characterize the owner. Both techniques do not require the original image in the watermark extraction process. The normalized correlation and bit error rate are used to evaluate the robustness of the watermark and the evaluation process of robustness is performed on the watermarked images from both techniques under the same image quality. The attacks include JPEG compression, JPEG2000 compression, lowpass filtering and a series of selected attacks from StirMark benchmark.

Key-Words: - image watermarking, multiwavelet, multiwavelet tree, and code division multiple access

1 Introduction

With the rapid growth of Internet networks and the further development of multimedia technologies, the copyright protection of digital contents has been one of the most serious problems because digital copies can be made identical to the original. Consequently, intellectual property protection is a pressing concern for content owners who are exhibiting digital representation of the photographs, video clip and original artworks through the Internet.

Digital watermarking is one of the most popular approaches considered as a tool for providing the copyright protection of digital images. This technique is based on direct embedding of additional information data into the digital images. Ideally, there must be no perceptible difference between the watermarked and original images, and the watermark should be easily extractable, reliable and robust against image compression or any image manipulations [1]. According to the need of original data during watermark detection process, watermarking algorithms are classified into private algorithm and public or blind one. Private method needs the original signal during detection. In some cases, when the original data is not easy to obtain, or when we do not know which copy is the original one, it is necessary to used blind watermarking for resolving rightful ownership.

In previous research, Fridrich *et al.* [2] presented a methodology for comparing the robustness of spread spectrum image watermarking techniques in the discrete cosine transform domain. Furthermore, the authors describe a methodology for converting a detectable, one bit watermark into a readable watermark and vice versa. Kurugollu *et al.* [3] have compared four different wavelet transforms including scalar wavelet, multiwavelet, complex wavelet and wavelet packet transforms, for the use in fusion based watermarking applications. The main aim of the paper was to evaluate the performance of these transforms in term of the robustness of the watermarked images under certain imperceptibility. Wang *et al.* [4] proposed a wavelet-based blind watermarking scheme for the application of copyright protection. The wavelet coefficients of the host image are grouped into a predefined structure called supertree. Watermark bits are embedded by quantizing supertree and the resulting difference between quantized and unquantized trees will later be used for watermark extraction. In [5], Kumsawat *et al.* proposed a new approach for optimization in wavelet-based image watermarking using genetic algorithm (GA). The watermark insertion and watermark extraction are based on the CDMA technique and the watermark extraction process does not require the original image. Genetic Algorithm is applied to search for optimal strength of the watermark in order to improve quality of the watermarked image and robustness of the watermark.

In this paper, we focus our discussion on the comparison of robustness for multiwavelet based image watermarking using two different embedding techniques. First one is multiwavelet tree technique. This technique is a new watermarking algorithm based on discrete multiwavelet transform (DMT). The other one is based on CDMA technique from [5] without applying GA process. The experimental results have shown that the multiwavelet tree embedding technique yields more robust watermark than CDMA technique does.

2 Preliminaries

2.1 Multiwavelet Transform

Multiwavelet transform is a relatively new concept in the framework of wavelet transform and has some important differences. In particular, whereas wavelet has an associated one scaling function and wavelet function, multiwavelet has two or more scaling and wavelet functions. The most efficient way to perform multiwavelet transform is by using filter bank decomposition. The block diagram of a multiwavelet filter bank with prefilter $Q(z)$ and postfilter $P(z)$ is shown in Figure 1. Figure 2(a) show a four-level multiwavelet decomposition using the DGHM multiwavelet with optimal orthogonal prefilter [6].

2.2 Multiwavelet Tree

Multiwavelet coefficients have the property that the related coefficients in different scales are located at the same orientation and location in the multiwavelet hierarchical decomposition. With the exception of the highest frequency subbands, every coefficient at a given scale can be related to a set of coefficients at the next finer scale of similar orientation. The coefficient at the coarse scale is called the parent, and all coefficients corresponding to the same spatial location at the next finer scale of similar orientation are called children. For the multiwavelet hierarchical subband decomposition, the parent-child dependencies are shown in Fig. 2(b). For a given parent, the set of all coefficients at all finer scales of similar orientation corresponding to the same location are called descendants. A multiwavelet tree descending from a single coefficient in the subband HL_4 is shown in Figure 2(b).

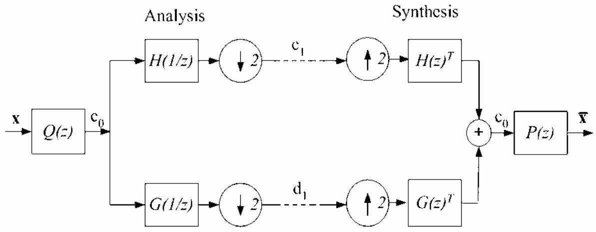
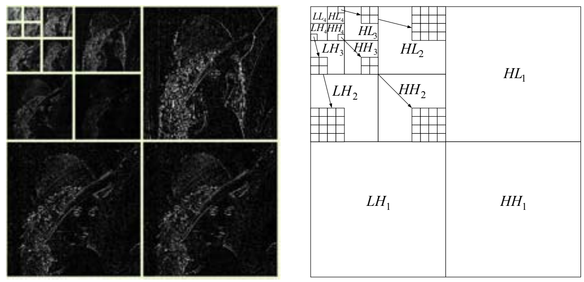
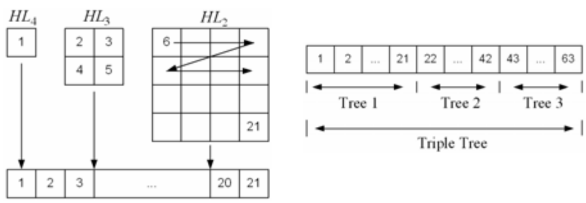


Fig. 1 Multiwavelet filter bank



(a) (b)

Fig. 2 (a) Four-level multiwavelet decomposition of Lena image having size of 512×512 pixels using DGHM multiwavelet and (b) the parent-child dependencies of multiwavelet tree.



(a) (b)

Fig. 3 (a) A group of multiwavelet coefficients in each tree and (b) the example of triple tree.

Except for highest-frequency subbands, we group the coefficients corresponding to the same spatial location together. Figure 3(a) shows an example of a group with one coefficient from HL_4, 4 coefficients from HL_3, and 16 coefficients from HL_2. The coefficients of the same group correspond to various frequency bands of the same spatial location and the same orientation. The total number of groups is equal to the sum of the number of coefficient in LH_4, HL_4 and HH_4, each of which has 32×32 coefficients. Thus, there are a total of $3 \times 32 \times 32 = 3072$ groups. We denote each group of multiwavelet tree by Tg_m, where $m = 1, 2, ..., 3072$.

3 Proposed Method

In this section, we first give a brief overview of the watermark embedding and watermark extracting in the DMT domain based on the concept of multiwavelet tree. We then describe the CDMA technique in multiwavelet-based image watermarking.

3.1 Multiwavelet Tree Watermarking Technique

3.1.1 Watermark Embedding Algorithm

This technique is a new watermarking algorithm in multiwavelet transform domain. The watermark embedding algorithm is as follows:

1. To increase security, perform a pseudo-random permutation in order to disperse the spatial relationship of the binary watermark pattern. Therefore, it would be difficult for a pirate to detect or remove the watermark. We use W and W^* to denote the original watermark image and the permuted watermark image, respectively. The relationship between W and W^* can be expressed as $W^*(i, j) = W(i', j')$, where (i', j') is permuted to the pixel position (i, j) in a secret order.

2. Transform the original image into four-level decomposition using the DMT. Then, create multiwavelet trees and rearrange them into 3072 groups.

3. Quantize each group by using JPEG quantization matrix [7] in order to gain the robustness to JPEG compression attack.

4. To increase watermarking security, order the groups Tg_m in a pseudorandom manner. The random numbers can be generated using the secret key. We further combine the coefficients of every three groups together to form "a triple tree: Tt_n", for $n = 1, 2, ..., 1024$. Each watermark bit is embedded into one triple tree. An example of a triple tree is shown in Figure 3(b).

5. For watermark embedding, we select N_w triple trees (Tt_k for $k = 1, 2, ..., N_w$, where N_w is the length of the watermark). Then, we modify the coefficients in each triple tree as follows:

$$Ttw_k = \begin{cases} Tt_k + Tt_k \bmod 2 - 1 & if\ W^*(i, j) = 1 \\ Tt_k - Tt_k \bmod 2 & otherwise \end{cases} \quad (1)$$

where Ttw_k is a triple tree that contains watermark information and "mod" is the modulo operator.

6. Perform inverse quantization in each group of all triple trees and pass the modified DMT coefficients through the inverse DMT to obtain the watermarked image. The watermark embedding process is shown in Figure 4.

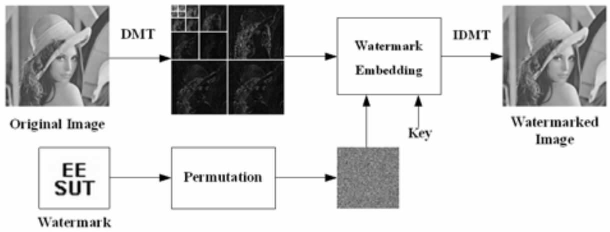


Fig. 4 Watermark embedding process

3.1.2 Watermark Extracting Algorithm

The watermark extracting algorithm is as follows:

1. Transform the watermarked image into four levels decomposition using the DMT. Then, create the multiwavelet trees and rearrange them into 3072 groups.

2. Apply JPEG quantization matrix to each group of multiwavelet tree. Then, order the groups in a pseudorandom manner using the secret key. We further combine every 3 groups to form a triple tree Tt_n, for $n = 1, 2, ..., 1024$.

3. To extract the embedded watermark, select N_w triple trees and count the *even* and *odd* number of the coefficients in triple tree based on $Tt_n \bmod 2$ computation. The embedded bits can now be recovered from a triple tree as follow:

$$\widetilde{W}^*(i,j) = \begin{cases} 1 & if \quad odd \geq even \\ 0 & otherwise \end{cases} \quad (2)$$

4. Inverse the permutation of $\widetilde{W}^*$ to obtain the extracted watermark $\widetilde{W}$. In our proposed method, the extracted watermark is a visually recognizable image. After extracting the watermark, we used normalized correlation coefficients to quantify the correlation between the original watermark and the extracted one. A normalized correlation between W and $\widetilde{W}$ is defined as [4]:

$$\rho(W, \widetilde{W}) = \frac{\sum_{k=1}^{N_w} w_k \widetilde{w}_k}{\sqrt{\sum_{k=1}^{N_w} w_k^2 \sum_k \widetilde{w}_k^2}} \quad (3)$$

where W and $\widetilde{W}$ denote an original watermark and extracted one, respectively.

For the application of copyright protection, a given watermark is detected if the correlation of the extracted watermark with the given watermark is above a pre-specified threshold. The watermark extraction process is shown in Figure 5.

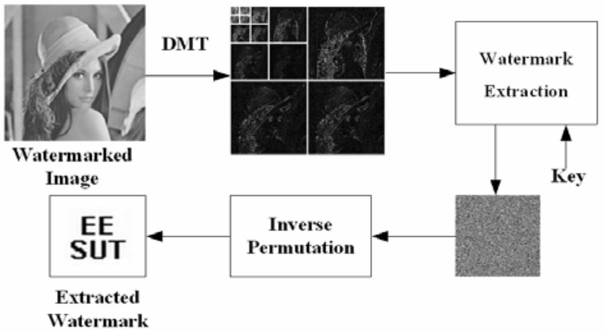


Fig. 5 Watermark extraction process

3.2 CDMA Watermarking Technique

In this paper, the CDMA watermarking technique is based on the proposed method in [5]. For a fair comparison, we do not apply any intelligent technique to this watermarking algorithm. Next, we give a brief overview of this technique (DMT-CDMA). A detailed discussion of this CDMA watermarking technique can be found in the given reference.

3.2.1 Watermark Embedding Algorithm

The image to be watermarked is first decomposed using DMT into two levels with DGHM multiwavelet filter. To increase security, the watermark is permuted into scrambled data before embedding. Then, we generate two-dimensional CDMA watermark from permuted watermark and pseudo-random noise pattern with the secret key and embed it directly in the selected middle bands which are $HL1, LH1, HL2$ and $LH2$. The selected DMT coefficients are modulated in the following way:

$$I_W(u,v) = \begin{cases} I(u,v) + \alpha \cdot W(u,v), & u,v \in HL1, LH1, HL2, LH2 \\ I(u,v), & u,v \in LL2, HH1, HH2 \end{cases} \quad (4)$$

where $I(u,v)$ is the DMT coefficient from selected subbands, $I_W(u,v)$ is coefficient of watermarked image, $W(u,v)$ and α denote CDMA watermark and the watermark strength, respectively. Finally, we pass the modified DMT coefficients through the inverse DMT to obtain the watermarked image. The watermark embedding process is similar to Figure 4.

3.2.2 Watermark Extracting Algorithm

The extraction process is the inverse procedure of the watermark insertion process. We first compute the multiwavelet coefficients of the suspected image. The permuted watermark bits are extracted by analyzing the coefficients and the correlation of pseudo-random sequence used in CDMA generation. Then, we perform inverse permutation of the permuted watermark to obtain the extracted watermark. This technique does not need the original image in watermark extraction. After extracting the watermark, we used normalized correlation in Equation (3) to quantify the correlation between the original watermark and the extracted one.

4 Experimental Results and Discussions

The experiment results are obtained by using a 256 gray-level "Lena" image of size 512×512 pixels and the binary logo "EE SUT" of size 32×32 pixels as a visually recognizable watermark. Figures 6(a) and 6(b) show the original image and the binary watermark image, respectively.

In order to compare robustness between the two techniques in a fair manner, the parameter for each scheme should be adjusted so that watermarked image of approximately the same imperceptibility are produced. In these experiments, the PSNR of watermarked image in each scheme was set to 37 dB and the watermarked versions of the Lena image from both techniques are not distinguishable from the original ones. According to the experimental results, the value of threshold was assigned to 0.4 in all following experiments.

(a) (b)

Fig. 6 (a) Original image, (b) watermark image.

The watermarked images are attacked using JPEG compression, JPEG2000 compression, lowpass filtering, and a series of selected attacks from StirMark benchmark [8]. Then, we perform the watermark extraction process and compute the normalized correlation coefficient and the bit error rate (BER). The bit error rate is calculated as the number of incorrectly decoded bits divided by the total number of embedded bits in the watermarked image.

The desirable property of an image watermarking algorithm is the robustness of watermark against lossy image compression. We first attack watermarked image by using JPEG and JPEG2000 compression. Table 1 shows the extracted logo from applying JPEG compression to watermarked images with quality factors 35% to 90%. For multiwavelet tree watermarking technique (DMT-Tree), it can be seen that the extracted logo is still visually recognizable, even for low quality factor as 35%. For watermark robustness against JPEG and JPEG2000 compression, the correlation coefficient and BER are shown in Figures 7(a), 7(b), 8(a) and 8(b), respectively. We can see that the DMT-Tree method gives more robust watermark than the DMT-CDMA method does.

Next, the robustness of the watermark is tested by using lowpass filtering. Figure 7(c) and Figure 8(c) show the normalized correlation coefficient and BER, respectively when the watermarked images are attacked by low-pass filtering. The results show that the DMT-Tree method yields more robust watermark than the DMT-CDMA method.

Finally, both watermarking systems are evaluated against a set of attacks in the StirMark benchmark system, including the noise-type attacks (median filtering, Gaussian filtering and Frequency Mode Laplacian Removal (FMLR)) and the geometric attacks (rotation with auto-scaling, flip and random geometric distortions). The simulation results using Lena image are given in Table 2. The results are similar to other images that were examined. From this table, we can also see that the watermarking algorithm using multiwavelet tree yields more robust watermark than the one using CDMA technique. Especially, it can survive to well known StirMark random bending attack.

5 Conclusions

In this paper, we have presented the robustness comparison of watermarking techniques in the multiwavelet transform domain. The first watermarking technique is based on the concept of multiwavelet tree and the second is based on the CDMA technique. The experimental results show that the multiwavelet tree watermarking technique produces robust watermark than the one using CDMA technique against all attacks which were included in this study such as JPEG compression, JPEG2000 compression, lowpass filtering and a series of selected attacks from StirMark benchmark.

Acknowledgements

The financial support from Suranaree University of Technology is greatly acknowledged.

References:

[1] F. Hartung and M. Kutter, " Multimedia watermarking techniques," *Proc. IEEE*, vol. 87, no. 7, pp. 1079-1107, July 1999.

[2] J. Fridrich and M. Goljan, "Comparing robustness of watermarking techniques," *Proc. of SPIE Vol. 3657 (Security and Watermarking of Multimedia Content)*, San Jose, Jan 25-27, 1999, pp. 214–225.

[3] F. Kurugollu, A. Bouridane, M. Roula and S. Boussakta, "Comparison of different wavelet transforms for fusion based watermarking applications," *Proc. of ICECS 2003*, vol. 3, pp. 1188 – 1191, 2003.

[4] Wang, S. -H. and Lin, Y. -P., "Wavelet tree quantization for copyright protection watermarking," *IEEE Trans. on Image Processing*, Vol. 13, No. 2, Feb. 2004.

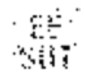
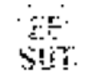
[5] P. Kumsawat, K. Attakitmongcol and A. Srikaew, " A new approach for optimization in wavelet-based image watermarking by using genetic algorithm**,"** *Proc. The 23rd IASTED International Multi-Conference Artificial Intelligence and Applications,* vol. 1, pp. 328-332, Feb. 2005.

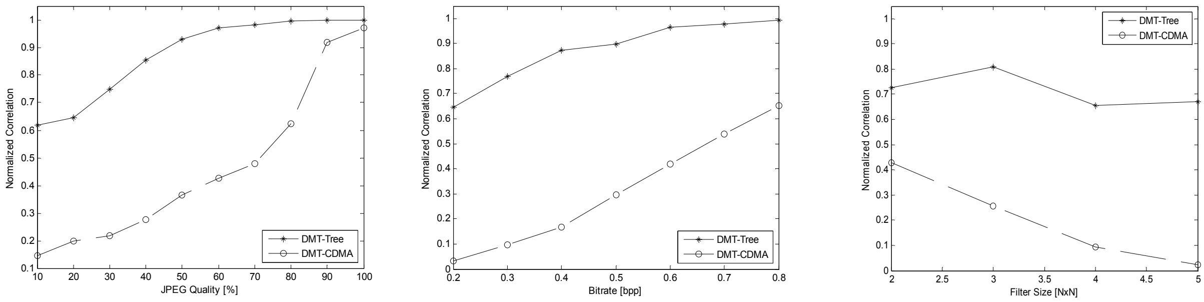
[6] K. Attakitmongcol, D. P. Hardin and D. M. Wilkes, "Multiwavelet prefilters II: Optimal orthogonal prefilters", *IEEE Trans. on Image Processing,* vol. 10, pp. 1476–1487, Oct. 2001.

[7] P. B. William, M. L. Joan, "JPEG still image data compression standard", Van Nostrand Reinhold, New York, 1993.

[8] M. Kutter and F. A. P. Pititcolas, "A fair benchmark for image watermarking systems," *Proc. SPIE: Security and Watermarking of Multimedia Content*, vol. 3657, pp. 219-239, Jan. 1999.

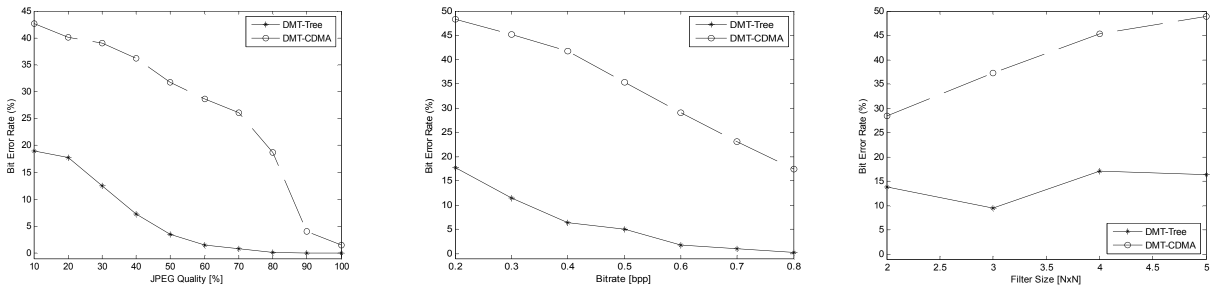
Table 1 Extracted logo of watermarked image after JPEG compression with various quality factors.

Technique	JPEG Quality factor (%)						
	35	40	50	60	70	80	90
DMT-Tree							
DMT-CDMA							



(a) (b) (c)

Fig. 7 Normalized correlation coefficient of the extracted watermark using (a) JPEG compression, (b) JPEG2000 compression and (c) lowpass filtering.



(a) (b) (c)

Fig. 8 Bit error rate of the extracted watermark using (a) JPEG compression, (b) JPEG2000 compression and (c) lowpass filtering.

Table 2 The normalized correlation coefficient and bit error rate from two different multiwavelet-based image watermarking techniques using Lena image

StirMark Functions	Normalized Correlation Coefficient		Bit Error Rate (%)	
	DMT-Tree	DMT-CDMA	DMT-Tree	DMT-CDMA
Median_filtering_2x2	0.6934	0.5039	15.33	24.80
Median_filtering_3x3	0.8047	0.7578	9.77	12.11
Median_filtering_4x4	0.6445	0.1387	17.77	43.07
Gaussian_filtering_3x3	0.8613	0.5234	6.93	23.83
FMLR	0.6328	0.4844	18.36	25.78
Flip	0.6211	0.0488	18.95	47.56
StirMark	0.6504	0.0020	17.48	49.90
rotation_scale_-1.0	0.6211	0.0098	18.95	49.51
rotation_scale_-0.5	0.6602	0.0059	16.99	49.71
rotation_scale_0.5	0.6543	0.0391	17.29	51.95
rotation_scale_1.0	0.6094	0.0156	19.53	50.78