

A Robust Image Watermarking Using Multiresolution Analysis of Wavelet

Chirawat Temi, Somsak Choomchuay, and Attasit Lasakul
 ReCCIT and Faculty of Engineering
 King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand
 E-mail: chirawat.temi@seagate.com, kchsomsa@kmitl.ac.th, and klattasi@kmitl.ac.th

Abstract: Embedding watermark in the wavelet becomes more attractive to most researchers as it could provide better performance. In this paper present a method of embedding binary visualized image into the host image by modifying coefficients of wavelet domain in LL bands with appropriate strength factor in order to compromise between acceptable imperceptibility level and attacks' resistance. Qualified Significant Wavelet Tree (QSWT) is used in both to select locations where watermark data are to be embedded, and to find locations of watermark in the extraction process. Results show that the proposed method successfully achieves robustness level of various attacks such as image processing, rotation attack etc.

Keywords: digital watermarking, data hiding, wavelet decomposition, qualified significant wavelet tree, multi-resolution analysis

I. INTRODUCTION

Digital contents in the form of text document, still image, motion picture, and music etc. are widely used in our normal life nowadays. With a rapid grown of internet users both at home and in working environment, it boots up transaction rates (file sharing, distribution or exchange). Trend goes up dramatically and continue growing everyday due to convenient and easy to access. It is, hence, copyright protection becomes more concerned to all content owners.

Although there are a number of methods available to protect misuse of the contents such as serial number entry, registration or encryption to validate the right owner/user but seem problem does not go a way. A number of users who violate copyright owner still exist and grow up. As a result, there is a need to continue a development of better scheme for copyright protection. Watermarking system (for still and moving pictures) is one of the promised methods that have been studied extensively in recent years.

In order to evaluate watermark system, the following requirements are generally considered in prior;

- **Readability:** A watermark should convey as much information as possible, statistically detectable, enough to identify ownership and copyright unambiguously.

- **Security:** Only authorized users gain access to the watermark data.
- **Imperceptibility:** The embedding process should not introduce any perceptible artifacts into original image and not degrade the perceive quality of image.
- **Robustness:** The watermark should be able to withstand various attacks while can be detected in the extraction process.

II. PRELIMINARIES

In this section, we review typical watermark system model and qualified significant wavelet tree concept as it is use to determine embedding locations in wavelet domain.

Fig. 1 shows typical watermark model for still image. Watermark W is embedded into image I with secrete key k , the watermarked image I_w later pass through distribution channel (typical communication channel, computer network, internet etc.), which are simulated under several kind of common attacks. The watermarked image after attack I_w^* , with the same secrete key, will then extracted in order to recover the original watermark data W' .

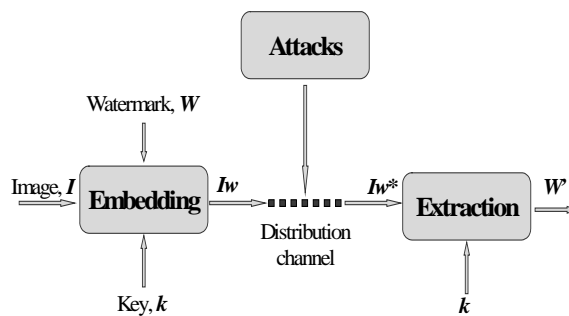


Fig. 1 Typical watermark system model

Our scheme is based on wavelet transform domain. As such, the host image is transformed to the desired resolution level whilst the watermark data are then embedded into it by modifying the coefficient values. Many researches have proposed Multiresolution Analysis (MRA) for embedding watermark data into image [3-6]. The challenges are how to select the coefficient of MRA and at which frequency band to be used under constrained

requirements. Derived from Embedded Zerotree Wavelet (EZW) [6], M.S. Hsieh, *et al.* [8] proposed a new method to select coefficients in MRA called “Qualified Significant Wavelet Tree (QSWT)”. The definition of QSWT is defined as following,

If a wavelet coefficient $x_n(i, j) \in D$ at the coarsest scale is a parent of $x_{n-1}(p, q)$, where D is a subband labeled LLn, HLn, LHn, HHn, satisfies $|x_n(i, j)| > T_1$ and $|x_{n-1}(p, q)| > T_2$, for a given threshold T_1, T_2 , then $x_n(i, j)$ and its children are call a QSWT.

III. PROPOSED METHOD

Embed watermark in low frequency band is most resistant to JPEG compression, blurring, adding Gaussian noise, rescaling, rotation, cropping, pixilation and sharpening while embedding in high frequency is most resistant to histogram equalization, intensity adjustment and gamma correction [10]. Although low frequency band has indicated its advantage to most common attack, because of its high energy any modification to its coefficient can be detected easily when compared to the high frequency band. Regarding a binary image watermark and with appropriate strength factor, an acceptable level of imperceptibly could be maintained. The uses of LL band for watermark embedding are also reported in [10]-[15].

In the embedding diagram shown in Fig. 2, we first decompose host image into three levels then find locations in LL bands by using QSWT algorithm. The coefficient at obtained locations will be sorted in descending order so that high coefficient location will be used in priority. Let L_2 and L_3 are the coefficients in LL band at level 2 and 3 respectively; the thresholds (T) are defined as followings,

$$T_3 = \frac{1}{n} \{ \bar{x}_{3rd} \mid x_1, x_2, x_3, \dots, x_i, \dots, x_n, x_i \in L_3 \}, \quad (1)$$

$$T_2 = \frac{1}{m} \{ \bar{x}_{2nd} \mid x_1, x_2, x_3, \dots, x_k, \dots, x_m, x_k \in L_2 \}. \quad (2)$$

Watermark image are permuted by Linear Feedback Shift Register (LFSR) [7] to enhance its security level, converted its bit value from $[0,1] \rightarrow [-1,1]$, and then sorted in ascending order.

At the selected locations, the watermark data are embedded by modifying coefficients of the LL band,

$$x'_3(i, j) = x_3(i, j) + \alpha w(k, l), \quad (3)$$

where α denotes a strength factor.

The watermarked image is then reconstructed by performing inverse wavelet transform (IDWT) to all subbands.

Shown in Fig. 3, the recovery process can be implemented easily by comparing the coefficient value of host and watermarked images. Both host and watermarked images are decomposed for 3 levels. QSWT is also used

location findings. The watermark pattern can be recovered by comparing coefficients at the same order of QSWT location of both images. Let I_{LL} and I'_{LL} are coefficients of LL band at QSWT location of host and watermarked image respectively, then watermark bit can be retrieved by

$$w'_b = \begin{cases} 1 & I'_{LL} > I_{LL} \\ 1 & otherwise \end{cases}. \quad (4)$$

Finally, the watermark bits are then reversely permuted to obtain the recovered watermark image.

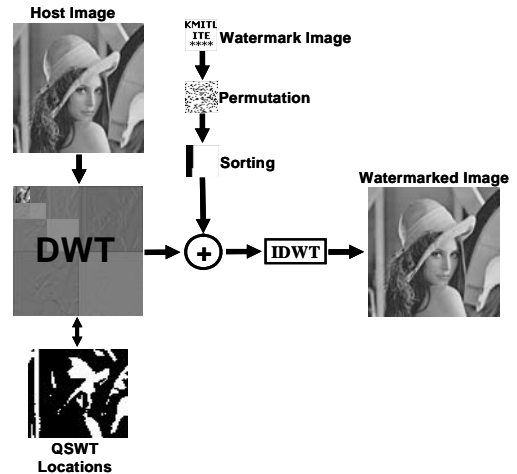


Fig. 2 Embedding diagram

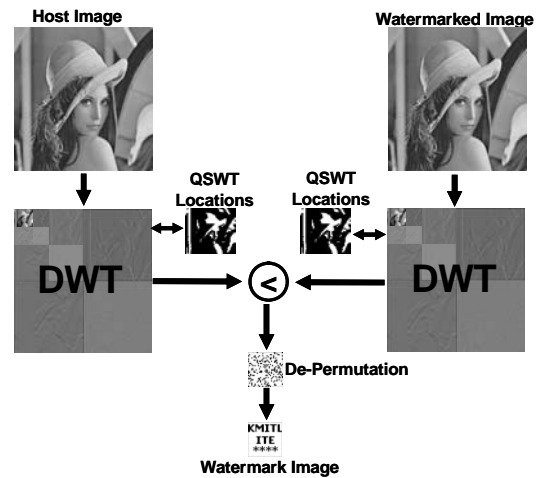


Fig. 3 Extraction diagram

IV. EXPERIMENTAL RESULTS

The experiments are performed on different gray scale host images such as Lena (Fig. 4a), Baboon, and Peppers. Watermark data is 32×32 binary image (Fig. 4b). We could obtain PSNR of 44.25 dB with no perceptibility problem on watermarked image when using α at 25 (Lena image).



Fig. 4 (a) Host image and (b) Watermark image

Peak Signal to Noise Ratio (PSNR) is used to measure quality of watermarked image while Normalized Cross Correlation (NC) is used to measure quality of watermark after recovery. PSNR and NC are defined as following,

$$PSNR = 10 \log \frac{255^2}{MSE}, \quad (5)$$

where MSE is defined as follow,

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

where M and N are size of images, $f(x,y)$ and $\hat{f}(x,y)$ are value at (x,y) location of host and watermarked image.

$$NC = \frac{\sum_i \sum_j p_{ij} p_{ij}^*}{\sum_i \sum_j (p_{ij})^2}, \quad (7)$$

where p_{ij} and p_{ij}^* are pixel value at i,j location of original watermark and recovered watermark pattern respectively.

Watermarked image is then subjected to different kind of attacks. Watermark pattern extraction is performed subsequently. Fig. 5a-5c demonstrate attacked images, QSWT locations, and extracted watermarks.



(a) JPEG Compressions (PSNR = 34.28, NC = 0.998)



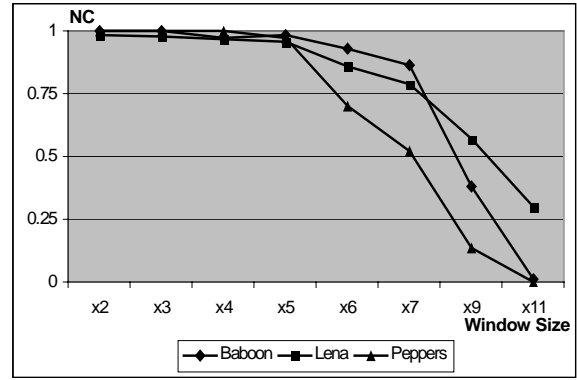
(b) Low pass filter at window size 7x7 (PSNR = 20.30, NC = 0.861)



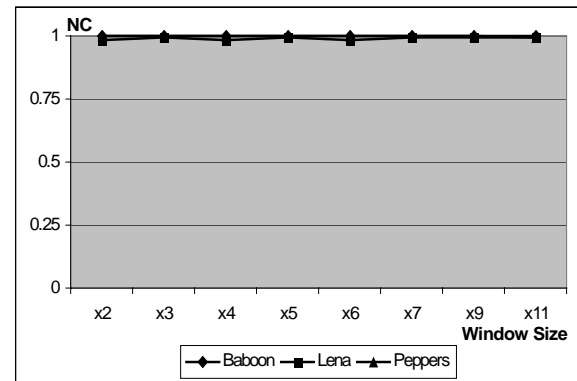
(c) White Noise (PSNR = 18.48, NC = 0.911)

Fig. 5a-c Watermarked image, QSWT location and extracted watermark

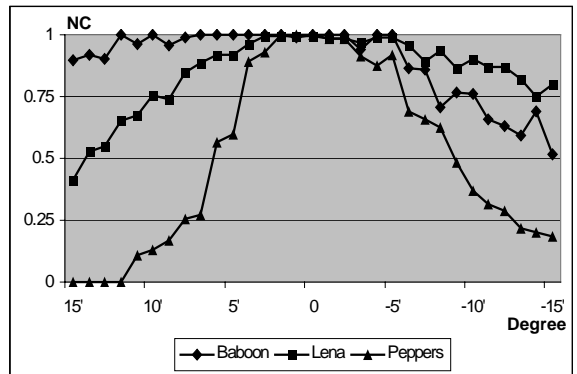
Fig. 6a-6f show the obtained NC values of different level of attacks of different host images.



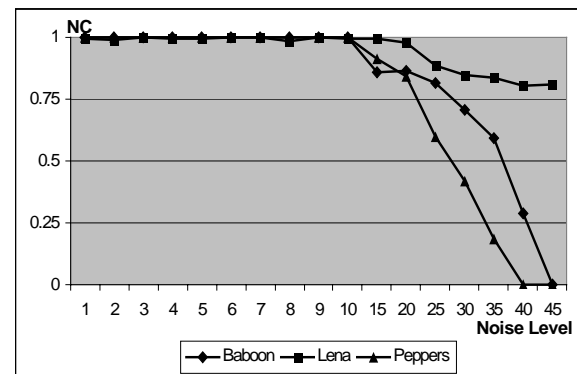
(a) Low Pass Filter



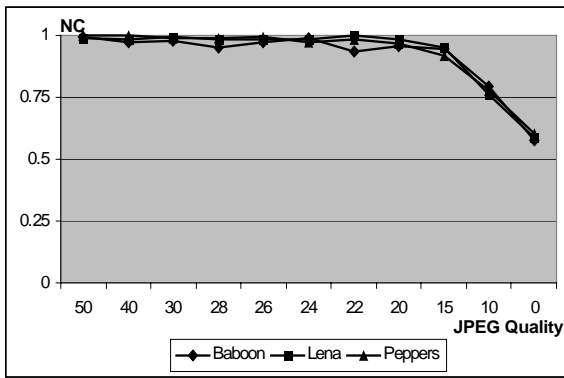
(b) Median Pass Filter



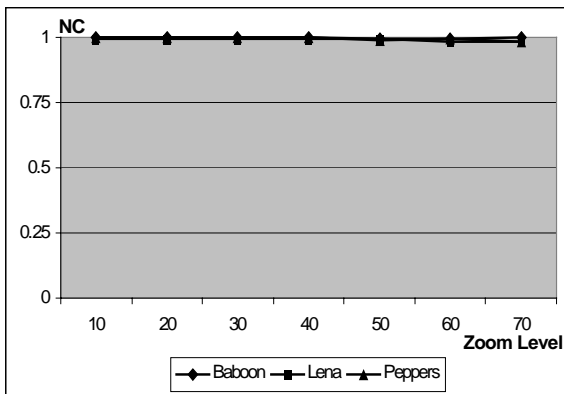
(c) Image Rotation



(d) Gaussian Noise



(e) JPEG Compression



(f) Image zooming

Fig. 6a-f Comparison of NC with different host images and attacks

V. CONCLUSIONS

The result shows that embed binary watermark pattern in LL band of wavelet decomposition with appropriate strength factor could achieve acceptable imperceptibly level. However, there is always a trade off between imperceptibly level and robustness of the system. The bigger strength factor value, the more robustness obtained, but worse in perceptible level. Although, PSNR is often a useful tool to measure perceptibly level, it is not always accurate to human eyes judgment. We, thus, need both of them to justify the appropriate strength factor.

We also found that obtained NC of extracted watermark depends on the host image as each image owns different frequency ranges. Since our scheme was to embed watermark in the low frequency band and used its coefficient to find embedding locations, the attack at this low frequency band is thus quite sensitive. The Peppers image has greatly impacted by low pass filtering and rotational attacks as these attacks effect low frequency band. Peppers image contains low frequency component more than others. Unlikely, the same image has shown similar NC values for all JPEG (compression), zooming, and median pass filter attacks.

Our proposed scheme has demonstrated that using LL band could achieve a desired robustness level without imperceptibly problem.

REFERENCES

- [1] R.G. van Schyndel, A.Z.Tirkel, N.R.A. Mee and C.F. Osborne, "A digital watermark," *IEEE Image Processing Conference*, Houston TX, USA, vol.2, pp. 86-90, Nov 1994.
- [2] I.J.Cox, J.Kilian, F.T.Leighton, and T.Shamoon, "Secure spread spectrum watermarking for multi-media," *IEEE Trans. on Image Processing*, vol.6, pp.1673-1687, Dec 1997.
- [3] Z.H. Wei, P. Qin, and YQ.Fu, "Percept digital watermark of image using wavelet transform," *IEEE Trans. on Consumer Electron*, vol.44, pp. 1267-1272, Nov. 1998.
- [4] H. Inoue, A. Miyazaki, A. Yamamoto, and T. Katsura, "A digital watermark based on the wavelet transform and its robustness on image compression," *IEEE International Conference on Image Processing*, vol. 2, pp. 391-395, 1998.
- [5] Y.S. Kim, O.H. Kwon, and R. H.Park, "Wavelet based watermarking method for digital images using Human Visual System," *Proc. IEEE International Symposium on ISCAS'99*, Orlando FL, USA, vol. 4, pp. 80-89, 1999.
- [6] J.M. Sapiro, "Embedded image coding using zerotrees of wavelet coefficients," *IEEE Trans. on Signal Processing*, vol. 41, pp. 3445-3462, Dec 1993.
- [7] C.H. Lee, Y.K. Lee, "An adaptive digital image watermarking technique for copyright protection," *IEEE Trans. on Consumer Electronics*, vol. 45, No.4, pp. 1005-1015, Nov 1999.
- [8] M.S. Hsieh, D.C. Tseng and Y.H. Huang, "Hiding Digital Watermarks Using Multiresolution Wavelet Transform," *IEEE Trans. on Industrial Electronics*, vol.48, no.5, pp. 875-882, Oct 2001.
- [9] C. Temi, A. Lasakul, K. Sripimanwat and S. Kondo, "Image Watermarking Using Multiresolution Analysis," *International Symposium on Nonlinear Theory and Its Application, NOLTA 2002*, Xi an, China, Oct 2002.
- [10] P. Tao and A.M. Eskicioglu, "A Robust multiple watermarking scheme in the Discrete Wavelet Transform domain," *Optics East 2004 Symposium, Internet Multimedia Management Systems Conference V*, Philadelphia PA, USA, Oct 2004.
- [11] Y. Wang, J.F. Doherty, and R.E. Van Dyck, "A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Image," *IEEE Trans. on Image Processing*, vol. 11, No. 2, pp. 77-88, Feb 2002.
- [12] S. Pereira, S. Voloshynovskiy and T. Pun, "Optimized Wavelet Domain Watermark Embedding Strategy using Linear Programming," *Proc. Of SPIE: Wavelet Applications VII*, vol. 4056, pp. 490-498, Apr 2000.
- [13] N.K. Abdulaziz and K.K. Pang, "Robust Data Hiding for Images," *International Conference on Communication Technologies (ICCT2000)*, Beijing, China, Aug 2000.
- [14] J.R. Kim and Y.S. Moon, "A Robust Wavelet-Based Digital Watermarking using Level-adaptive Thresholding," *IEEE Proc. of the 1999 International Conference on Image Processing (ICIP '99)*, Kobe, Japan, pp. 226-230, Oct 1999.
- [15] S. Joo, Y. Suh, J. Shin and H. Kikuchi, "A New Watermark Embedding into Wavelet DC Components," *ETRI Journal*, vol. 24, pp. 401-404, Oct 2002.