IMAGE WATERMARKING USING WAVELETS

P. Tay and J.P. Havlicek

School of Electrical and Computer Engineering
University of Oklahoma, Norman, OK USA
{ptay,joebob}@ou.edu

ABSTRACT

This paper proposes a novel image watermarking scheme. This technique uses a 2-D discrete wavelet transform to decompose an image into various frequency channels. A scaled image is used as the watermark and inserted into a mid-freqency wavelet channel. The watermark embedded image is produced by taking the inverse 2-D discrete wavelet tranform of the altered wavelet decomposition. The image size, the non-zero scaling factor, the channel in which the watermark is inserted, and the wavelet transform filters can be used as security keys for the extraction of the inserted watermark. The propose watermark extraction technique is independent of the original image. A compromise between visually perceptible artifacts and resiliency in preserving the watermark from attacks by JPEG compression, median filtering, and image cropping can be achieved by adjusting the scaling factor.

1. INTRODUCTION

Digital image watermarking techniques have been given considerable amount of attention in the recent literature [1–7]. Digital image watermarking is concerned with hiding information into a digital image. This information may be used for various applications such as authentication, copyright protection, proof of ownership, *etc.*

Some desirable properties of a watermarking techiques include the following:

- The inserted watermark should not introduce visible artifacts.
- The watermark should not be easily removable.
- The watermark should be resilient to lossy data compression such as JPEG.
- The watermark should be resilient to image processing technique such as median filtering.
- The watermark should be resilient to image cropping.
- The original image is not required in the watermark extraction.
- The watermark can only be extracted by privileged individuals who are given the security key.

Previously published watermarking techniques embed information in either the spacial domain and/or some transform domain. Spacial domain techniques embed the watermark by directly modifying pixels. Transform domain techniques require filtering the image into frequency channels then insert the watermark into one or more channels based on certain criteria. Spacial domain techniques generally require a lower computational cost than transform domain techniques, hence are generally easier to implement. A major concern of digital image watermarking is the trade-off between image degradation verses ease in removal of the inserted watermark via compression, filtering or cropping. Spacial domain techniques generally do not balance this trade-off well, hence transform techniques are preferred. This paper describes a algorithm that inserts a binary image watermark into a mid-frequency channel of a image's three level 2-D wavelet transform. The watermark embedding technique requires a non-zero scaling factor that accounts for the trade-off between image quality and resistance to various attacks to remove the watermark. This scaling factor and other parameters needed in the embedding scheme are used as a security key where extraction of the watermark is made possible only by the knowledge of this information. In addition the extraction technique does not require the original image to recover the watermark.

2. WATERMARK INSERTION

Let $\mathbf{I}$ be the original digital image of size $N_1 \times N_2$ and $\mathbf{W}$ be the three level 2-D wavelet transform of $\mathbf{I}$. Although the 2-D wavelet transform may be accomplished in a non-separable manner, the 2-D wavelet transform used in the experiment of this paper was performed in a separable manner. That is the 2-D transform is accomplished by performing a 1-D wavelet transform on each row of the image $\mathbf{I}$ then performing the exact same 1-D wavelet transform on the columns of $\mathbf{I}$. The details of the three-level 2-D wavelet transform can be found in [8]. Since it will be necessary to use the same wavelet transform for the watermark extraction, the filters used in this transformation can be determined by the owner of the image and used as part of the security key.

It is only required that the wavelet analysis and subsequent synthesis transform render an exact reconstruction system. We may choose any set of filters which are orthogonal, biorthogonal, or constitute a perfect reconstruction quadrature mirror filter bank.

A three level 2-D wavelet image decomposition $\mathbf{W}$ is composed of ten wavelet channels: **LL3**, **LH3**, **HL3**, **HH3**, **LH2**, **HL2**, **HH2**, **LH1**, **HL1**, and **HH1**. These channels correspond to sub-band frequencies of the image $\mathbf{I}$. The wavelet channels are illustrated in Fig. 1.

There are several factors used in determining which of the ten channels to insert the watermark. It is widely accepted that the energy of most natural images are concentrated on the lower frequencies [7]. Modifications to the coefficients to the low frequency **LL3** channel would cause severe and unacceptable image degradation to occur. In this scheme the watermark is never

0-7803-7523-8/02/$17.00 ©2002 IEEE

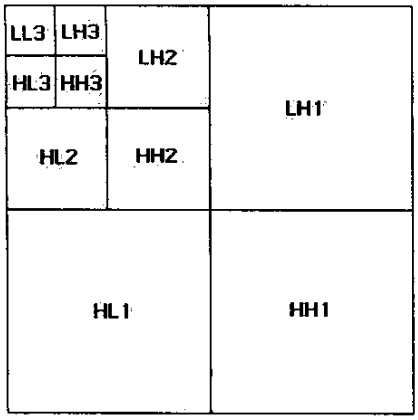

Fig. 1. The 10 channels of the three-level 2-D wavelet transform.

inserted into this channel. In order to provide resiliency to attacks by lossy compression and filtering operations which causes data losses in the high frequencies [6], the channels **LH2**, **HL2**, **HH2**, **LH1**, **HL1**, and **HH1** are not candidates for the watermark insertion. This leaves our choices to the three mid-frequency channels **LH2**, **HL2**, and **HH2**. Of these three channels the one which has the minimum ℓ_2-energy is chosen. In other words, let $\mathbf{C} \in \{\mathbf{LH2}, \mathbf{HL2}, \mathbf{HH2}\}$ be the channel in which the watermark is inserted, then

$$\|\mathbf{C}\|_2 = \min\{\|\mathbf{LH2}\|_2, \|\mathbf{HL2}\|_2, \|\mathbf{HH2}\|_2\}.$$

Let $\mathbf{M}$ be a image watermark we wish to embed into image $\mathbf{I}$ and $\mathcal{M} = g\mathbf{M}$ for some $g \in \mathbb{R} \setminus \{0\}$. The scale parameter g provides a trade-off between image degradation and resiliency to attacks which may remove the watermark. Choosing g with large absolute value renders more perciptible image artifacts and better resiliency to attacks. While g with small absolute values yields less perceptible artifacts and poor resistants to attacks. Denote the size of $\mathcal{M}$ as $N_3 \times N_4$. Since the size of wavelet channel $\mathbf{C}$ is approximately $\frac{N_1}{8} \times \frac{N_2}{8}$, it is required that $N_3 \leq \frac{N_1}{8}$ and $N_4 \leq \frac{N_2}{8}$. The watermark is inserted into channel $\mathbf{C}$ by the following equation

$$C(n,m) = \begin{cases} C(n,m) & \text{if } 0 \leq n < \frac{N_1}{8} - N_3 \\ & \text{and } 0 \leq m < \frac{N_2}{8} - N_4 \\ \mathcal{M}(n - \frac{N_1}{8} + N_3, m - \frac{N_2}{8} + N_4) & \text{otherwise} \end{cases}$$

where $0 \leq n \leq \frac{N_1}{8}$ and $0 \leq m \leq \frac{N_2}{8}$.

An inverse three level 2-D wavelet transform results in an image $\mathbf{J}$ which contains the embedded watermark. The original image size, the wavelet transform filters, the watermark scaling parameter g, and the channel $\mathbf{C}$ in which the watermark is inserted are components of the security key.

3. WATERMARK EXTRACTION

The watermark extraction requires that the original image size, the wavelet tranform filters, the scaling parameter g, and the wavelet channel in which the watermark is inserted are known. The same three level 2-D wavelet transform used in the embedding algorithm is performed on the watermark embedded image $\mathbf{J}$. The extracted watermark $\mathcal{N}$ is recovered from wavelet channel $\mathbf{C}$ by the following

$$\mathcal{N}(n,m) = g^{-1}C(n + \frac{N_1}{8} - N_3, m + \frac{N_2}{8} - N_4)$$

where $0 \leq n < N_3$ and $0 \leq m < N_4$.

4. EXPERIMENTAL RESULTS

Our experimentation was performed on the well-known *Lena* image, popularly used to test image processing applications. Fig. 2 shows the original unwatermarked *Lena* image. This version of *Lena* is 256 x 256 pixels with eight bit (256) gray scale levels.

Fig. 2. Original unwatermarked *Lena*

For the watermark image we use the 16 x 16 pixel binary image shown in Fig. 3. For display purposes the image is constrast stretched to eight bit gray scale and enlarged.

Fig. 3. The binary image used for the watermark.

Recall the only requirement of the wavelet transform is that the filters constitute a perfect reconstruction system. The examples in this paper use a length 20 Daubechies wavelet which has been shown to be a orthogonal system in [9].

4.1. Image Quality

In Fig. 4, the watermark in Fig. 3 is embedded in the the *Lena* image with scaling parameter $g = 1$. The checker board image artifact in the center of the image is obvious. When we allow the scaling parameter to be $g = 0.05$, the checkerboard image artifact is less evident. Image artifacts are present in the form of ripples on her shoulder, face, and hat. Nevertheless major features such as her face and feathers in her hat are distinguishible. The fine details of her face and feathers are easily seen. Clearly the image quality is improved. The watermark embedded image of *Lena* with scaling parameter $g = 0.05$ is shown in Fig. 5.

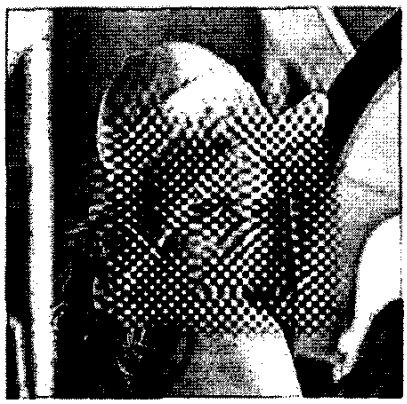

Fig. 4. Watermark embedded *Lena* with $g = 1$.

Fig. 5. Watermark embedded *Lena* with $g = 0.05$.

4.2. Security Key

It is at times advantageous for only the owner(s) of the security key to extract the watermark. In this subsection we will show the result of the extraction when the incorrect three-level 2-D wavelet transform is used to extract the watermark. Fig. 6 and Fig. 7 display the entire channel in which the watermark is embedded. Fig. 6 shows the channel in which the watermark is present and correctly extracted from the image in Fig. 5. The extraction process uses the length 20 Daubechies wavelet which is the same transform used in the embedding process. In Fig. 7, the length 18 Daubechies wavelet is used to extract the watermark from the image in Fig. 5. Our watermark image does not appear anywhere in the channel in which it was embedded. Thus correct detection for the watermark is not possible.

4.3. Resiliency to JPEG Compression

The image in Fig. 5 was compressed using a baseline JPEG coder. The JPEG quality parameter used in the compression was 20 which corresponds to approximately 14:1 compression ratio for this image. The decoded watermark was extracted and is shown in Fig. 8. Though the watermark image suffered some degradation,

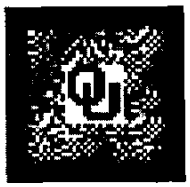

Fig. 6. Correct watermark extracted using a length 20 Daubechies wavelet.

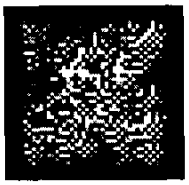

Fig. 7. Incorrect watermark extracted using a length 18 Daubechies wavelet.

the "OU" logo is still easily recognizable.

Fig. 8. Extracted watermark after JPEG compression of 14:1.

4.4. Resiliency to Median Filtering

It is important that the watermark be resilient to image processing techniques such as median filtering. We filtered the image in Fig. 5 with a median filter using a 3×3 mask. This process provided some smoothing of the finer details but preserved the major edges in the watermarked embedded image. The watermark image after 3×3 median filtering is shown in Fig. 9. We did not feel it important to test the resiliency of the watermark to median filtering with a larger mask than 3×3. Median filter with a mask larger than 3×3 caused significant removal of important image details.

Fig. 10 shows the extracted watermark removed from the 3×3 median filtered image in Fig. 9. Though some artifacts are introduced to the watermark image, the "OU" logo is clearly visible.

4.5. Resiliency to Image Cropping

In Fig. 11 the watermark embedded image of Fig. 5 is cropped to the center 128×128 pixel image. The cropped image is returned to its original size of 256×256 pixels by setting the pixels on the outside border to zero.

Fig. 12 is the extracted watermark from the cropped image. Even with the distortion on the left and bottom of the watermark image, the logo is easily recognize.

Fig. 9. Watermark *Lena* image with $g = 0.05$ and median filtered with 3×3 mask.

Fig. 10. Extracted watermark after 3×3 median filter.

5. CONCLUSION

We have presented a novel image watermarking technique. This technique inserts a scaled image into a mid-frequency channel of a three level 2-D wavelet transform. The watermark embedded image is produced by the applying the inverse three level 2-D wavelet transform to the altered wavelet decomposition. Multiplication by a non-zero scaling parameter g to the watermark image before inserting into the wavelet channnel allows us to adjust the image quality albeit resistance to attacks to remove the watermark.

The extraction of the watermark requires the correct security key, namely the image size $N_1 \times N_2$, the parameter g, the channel in which the watermark is inserted, and the filters used in the embedding process. If the security key is correct, the extraction process is straightforward.

Fig. 11. Cropped image of watermarked *Lena* with $g = 0.05$.

Fig. 12. Extracted watermark from cropped *Lena*.

Experimentation was performed on embedding a binary image watermark into the *Lena* image. Our results indicate that this watermark embedding technique is resilient to attacks by JPEG compression, 3×3 median filtering, and image cropping. In all cases the watermark was successfully recovered which supports the robustness of this image watermarking scheme.

6. REFERENCES

[1] Ming-Shing Hsieh, Din-Chang Tseng, and Yong-Huai Huang, "Hiding digital watermarks using multiresolution wavelet transform," *IEEE Trans. Industrial Elect.*, vol. 48, no. 5, pp. 875–882, Oct. 2001.

[2] Yiwei Wang, John F. Doherty, and Robert E. Van Dyck, "A wavelet-based watermarking algorithm for ownership verification of digital images," *IEEE Trans. Image Proc.*, vol. 11, no. 2, pp. 77–88, February 2000.

[3] C.-C. Chang, K.-F. Hwang, and M.-S. Hwang, "Robust authentication scheme for protecting copyrights of images and graphics," *IEEE Proceedings on Vision, Image, and Signal Proc.*, vol. 149, no. 1, pp. 43–50, February 2002.

[4] A. Lumini and D. Maio, "A wavelet-based image watermarking scheme," in *Proc. IEEE Int'l. Conf. Info. Tech.: Coding and Computing*, Las Vegas, NV, March 27-29 2000, pp. 122–127.

[5] Raymond B. Wolfgang and Edward J. Delp, "A watermark for digital images," in *Proc. IEEE Int'l. Conf. Image Proc.*, Lausanne, Switzerland, Sept. 16-19 1996, pp. 219–222.

[6] Ingemar J. Cox, Joe Kilian, F. Thomson Leighton, and Talal Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Proc.*, vol. 6, no. 12, pp. 1673–1687, December 1997.

[7] Chiou-Ting Hsu and Ja-Ling Wu, "Hidden digital watermarks in images," *IEEE Trans. Image Proc.*, vol. 8, no. 1, pp. 58–68, January 1999.

[8] S. G. Mallat, "A theory for multiresolution signal decomposition: the wavelet representation," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 11, no. 7, pp. 674–693, July 1989.

[9] I. Daubechies, "Orthonormal bases of compactly supported wavelets," *Commun. Pure Appl. Math.*, vol. 51, pp. 909–996, 1988.