Trends in Mathematics
Information Center for Mathematical Sciences
Volume 6, Number 1, June, 2003, Pages 63–69

A WATERMARKING SCHEME BASED ON LIFTING FILTERS

DAI-GYOUNG KIM AND JOO-YOEN LYU

ABSTRACT. Recently, digital multimedia contents can be easily accessed and modified by various digital technology. For protecting copyrights or intellectual properties of original data, digital watermarking technique has been attracted considerably. In this paper, we propose a robust watermarking scheme for digital images based on the lifting filters which provides a simple construction of second generation wavelets. The original image is transformed into wavelet domain by two sets of lifting filters; one is for usual wavelet filter, the other is for embedding watermarks whose locations are created randomly with secret key. We accomplish the Stirmark benchmark test(www.watermark.org) to demonstrate the robustness of our watermarking scheme to JPEG compression attacks, and others as well.

1. INTRODUCTION

There has recently been significant interest in digital watermarking. This is primarily motivated by a need to provide copyright protections to multimedia contents, such as audio, images, and video. Even if digital representations of multimedia contents have many advantages, an unlimited number of the perfect copies of the digital contents is a real threat to the copyright of content owners. The main goal of watermarking is to give a proof of ownership of original data by embedding copyright statements(cf. [2]). In addition, it has many applications in the area of information technology. For instance, one application is data monitoring or tracking, in which the user is interested in monitoring data transmission in order to control royalty payments, or simply track the distribution to localize the data from marketing and sales purposes(cf. [4]).

In many applications, the embedded information should be robust against manipulations or attacks that attempt to remove it. There are many reports for robust watermarking techniques(cf. [8]). In general, there two classes of invisible watermarking schemes depending on the embedding domain of watermarking: the spacial domain watermarking and frequency domain watermarking. The spatial domain watermarking is comparatively easy to implement but less robust than the frequency domain watermarking.

2000 *Mathematics Subject Classification.* 65D05, 65D15.

Key words and phrases. Copy protection, Data hiding, Digital watermarking, Wavelet transform.

This work was supported by the grant No. R01-2001-000-00350-0 from the Korea Science & Engineering Foundation.

One of the frequency domain watermarking schemes is based on the DCT(discrete cosine transform). For a robust watermarking in the frequency domain, the watermark is usually embedded in the lowest possible spacial frequencies. However, this approach is problematic since very low frequency modifications cause a perceptual distortion in the original image during watermarking process. Al-Mohimeed [1] has argued that wavelet transform is a good trade-off for this problem.

For robust watermarking, wavelet-based watermarking schemes are proposed by several authors (cf. [1],[3],[7]). Wang and Kuo [7] have suggested a multi-threshold wavelet coding scheme allowing significant coefficient searching. They assumed that those coefficients do not change much after several signal processing operations. If those coefficients lose their fidelity significantly, the reconstructed image could be perceptually different from the original one. In addition, the wavelet-based method is image dependent to be suitable for textured as well as smooth images, even if it selects a predefined set of coefficients (for instance, low-frequency coefficients).

In this paper, we propose a more robust watermarking scheme based on the lifting filters which provides a simple construction of second generation wavelets. The lifting scheme [6] has several advantages: for instant, (i) easy and flexible construction method of perfect reconstruction filters, (ii) in-place filter design. The proposed scheme turns the first to account so that the original image is transformed into wavelet domain by two sets of lifting filters; one is for usual wavelet filter, the others is for embedding watermarks whose locations are created randomly with secret key.

This paper is organized as follows. The lifting scheme is briefly reviewed in Section 2. The watermark embedding and detection algorithms based on multiresolution representation by lifting scheme are proposed in Section 3. Finally, a numerical simulation is accomplished to demonstrate the robustness of the proposed scheme to the JPEG compression attacks in Section 4.

2. Multiresolution Representation by Lifting Scheme

The wavelet transform develops an image into multiscale spatial-frequency decomposition. Figure 1 shows the decomposition of Lenna image with three scale levels. The lowest frequency band image is shown in the top-left conner(LL_3). At the same resolution level, the block HL_3 contains the high frequency band information in the horizontal direction and the low frequency band information in the vertical direction. Similarly, the block LH_3 contains the low frequency band information in the horizontal direction and the high frequency band information in the vertical direction.

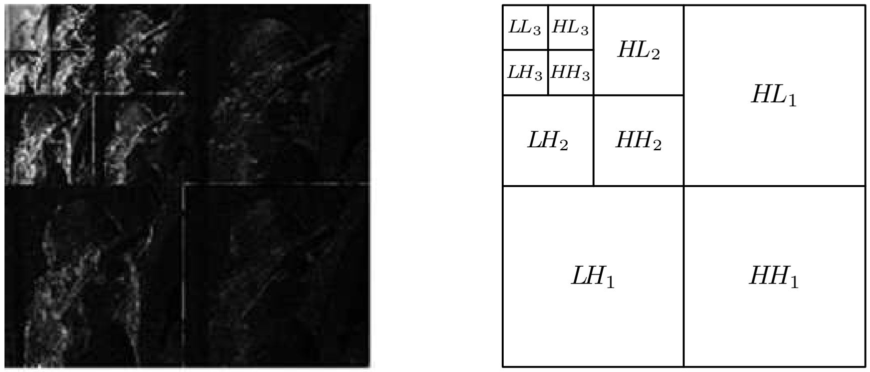

FIGURE 1. The wavelet decomposition of Lenna image with three scale levels.

One way to obtain the multi-scale information is to cascade two channel filter banks [5]. The lifting scheme [6] provides an efficient method for designing the FIR two channel filter banks, and has several advantages as well. In the present paper, we employ the advantage of easy and flexible construction for perfect reconstruction filters. Once we have an analysis filters bank via lifting scheme, then the inverse filter bank is just obtained by inverting the analysis processing.

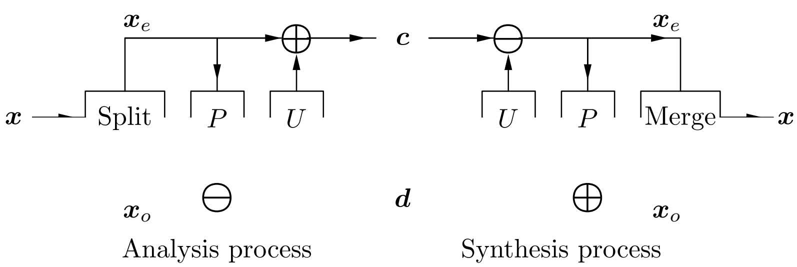

FIGURE 2. The diagram of analysis and synthesis processes by lifting scheme.

Let $\boldsymbol{x} = (x_n)_{n\in\mathbb{Z}}$ be a sequence of real numbers. The analysis processing by the lifting scheme is starting from splitting $\boldsymbol{x}$ into even and odd terms as $\boldsymbol{x}_e = (x_{2k})_{k\in\mathbb{Z}}$ and $\boldsymbol{x}_o = (x_{2k+1})_{k\in\mathbb{Z}}$. This splitting is referred as polyphase processing. For smooth signals the two phases are closely related, so that one can predict "odd" with "even". Let the difference be

$$\boldsymbol{d} = \boldsymbol{x}_o - P(\boldsymbol{x}_e) \tag{1}$$

where P is a predictor. Basic requirement for the predictor is the exactness up to polynomials with certain degree. The difference $\boldsymbol{d}$ is like an AC component, so that it is very small on a smooth region of a signal. U is an update operator on $\boldsymbol{x}_e$ with $\boldsymbol{d}$, that is,

$$\boldsymbol{c} = \boldsymbol{x}_e + U(\boldsymbol{d}) \tag{2}$$

By the update operator, the average of an original signal $\boldsymbol{x}$ is preserved. As a DC component, $\boldsymbol{c}$ is then an approximation of $\boldsymbol{x}$. Onthe other hand, the synthesis processing is obvious. For a given pair of $\boldsymbol{c}$ and $\boldsymbol{d}$, $\boldsymbol{x}$ is easily recovered by merging the results from inverting the analysis processing, that is,

$$\boldsymbol{x}_e = \boldsymbol{c} - U(\boldsymbol{d}); \quad \boldsymbol{x}_o = \boldsymbol{d} + P(\boldsymbol{x}_e); \quad \boldsymbol{x} = \boldsymbol{x}_e + \boldsymbol{x}_o \tag{3}$$

We notice that the predictor P has much freedom for choice, and it provides local transform, as well. In the present paper, we use the local property for embedding watermarking in predetermined regions.

3. Watermarking Algorithm with Lifting Scheme

For robust watermarking, most wavelet-based watermarking schemes may embed watermarks in the significant wavelet coefficients of a middle high frequency band. The coefficients have relatively high amplitude. In the present paper, we develop two sets of lifting filters; one is of usual wavelet filter and the other is of predetermined lifting filters to increase the amplitude of coefficients determined with a certain qualification. The qualified coefficients is selected by their locations created randomly with a secrete key(e.g., a seed number).

The watermark set $\{w_j\}$ is first generated by random number generation with positive numbers. For a given parameter ϵ, the watermarks are embedded in the qualified wavelet coefficients d_j of the host image as follow:

$$\frac{|d_j^w - d_j|}{d_j} = \delta_j w_j = \epsilon \tag{4}$$

where δ_j is the watermark strength parameter and d_j^w the watermarked coefficient. The embedding process is summarized as three steps.

- **Step1 :** Generating the position to be applied by lifting filters and decomposing the host image by two sets of lifting filters.
- **Step2 :** Determining the qualified coefficients.
- **Step3 :** Generating the flag and embedding watermarks.

In Step 1, the first candidate of watermark positions in the wavelet domain is generated by the pseudo random number generation with a seed number to be secrete key. Apply different lifting filters on that positions from the filters applied to other positions. In this case, we avoid overlapping of watermark positions and the supports of lifting filters. In Step 2, we choose the qualified(significant) coefficients by using the median of the absolute values of coefficients near the candidate of watermark position. Let $d_{i,j}$ be the coefficient at the candidate of watermark position and $m_{i,j}$ the median of the neighboring coefficient values such that

$$m_{i,j} = \text{median}(|d_{i-1,j-1}|, \cdots, |d_{i,j}|, \cdots, |d_{i+1,j+1}|) \tag{5}$$

If $|d_{i,j}| > m_{i,j}$, we classify the $d_{i,j}$ as a qualified coefficient. In Step 3, we generate the flags and embed watermarks in the qualified coefficients. With the qualified coefficients $d_{i,j}$ and predetermined watermark set $\{w_{i,j}\}$, we develop the watermarked coefficients $d^w_{i,j}$ as follow.

$$d^w_{i,j} = \begin{cases} d_{i,j}(1+\delta_{i,j}w_{i,j}), & \text{if} \quad d_{i,j} \geq m_{i,j} \\ d_{i,j}(1-\delta_{i,j}w_{i,j}), & \text{otherwise.} \end{cases} \tag{6}$$

We set the flag as $f_{i,j} = 1$ in the first case and $f_{i,j} = 0$ in the second case. The generated flag set is to be used in the process of watermark detection.

The extraction of watermarks is just inverse of embedding process. With the two secrete keys(the seed numbers), we recover the qualified watermark positions and the watermarks. Only the copyright holder knows the information of the keys for copyright assertion. For a possibly attacked image, we calculate the median of neighboring coefficients of a qualified watermark position as in Step 2 and generate the flags $\tilde{f}_{i,j}$ as in Step 3 above. To detect the watermarks, we compare the estimated flags $\tilde{f}_{i,j}$ and the original flags $f_{i,j}$

4. Numerical Experiments

We have tested the robustness of the proposed watermarking scheme against several attacks: JPEG compression, median filtering, and noise attacks. In order to obtain the objective benchmark, we employ the Stirmark(www.watermark.org) method. Throughout the experiments, the watermark strength parameter δ_j are determined by $\epsilon = 0.1$. The host image is the Lenna image that is an 8-bits gray image with 512×512 pixels. The watermark set is randomly generated by a seed number.

(a) (b)

Figure 3. (a) The original image(Lenna), (b) watermarked image with $\epsilon = 0.1$

The Stirmark JPEG compression attacks are accomplished with the quality factor varying from 1 to 100. The following table shows the robustness of the proposed watermarking scheme. The rates of detected flags are very consistent and high even in the case of the lowest quality(PSNR=24.9795dB).

JPEG quality	PSNR (dB)	Detected rate of flags
90	35.9517	100%
70	35.2260	100%
50	34.2450	100%
30	33.1503	100%
5	24.9795	98%

Table 1. Th detected rate of flags according to the JPEG quality of the attacked image for Stirmark benchmarking.

For the median attacks with 2×2, 3×3, and 4×4 median filterings, the proposed scheme detected full flags. However, in the case of the sharpening attacks, we lose relatively many of the flags.

5. Conclusion

In this paper, we have proposed a robust watermarking scheme based on the lifting filters. The original image is transformed into wavelet domain by two sets of lifting filters; one is for usual wavelet filter, the other is for embedding watermarks whose locations are created randomly with a secret key. Throughout the Stirmark benchmark test(www.watermark.org), we conclude that the proposed scheme is very robust against several attacks(JPEG, median filtering, and sharpening).

References

[1] M. Al-Mohimeed, "Wavelet-based digital watermarking" in *Proceedings of the SPIE, Security and Watermarking of Multimedia Contents III*, vol. 4314, pp. 418–423, Jan. 2001.

[2] M. Kutter and F. Hartung, "Introduction to watermarking techniques" in *Information Hiding*, S. Katzenbeisser and F. Petitcolas eds., Artech House Press, Boston, 2000, pp. 97–120.

[3] D. Kunder and D. Hatzinakos, "A robust digital image watermarking method using wavelet based fusion" in *Proceedings of the IEEE Int. Conference on Image Processing*, vol. 1, pp. 544–547, 1997.

[4] S. Lai and F. M. Buonaiuti, "Copyright on the Internet and Watermarking " in *Information Hiding*, S. Katzenbeisser and F. Petitcolas eds., Artech House Press, Boston, 2000, pp. 191–213.

[5] S. Mallat, *A wavelet Tour of Siganl Processing.* Academic Press, New York, 2nd ed., 1999.

[6] W. Sweldens, "The Lifting Scheme: A Construction of Second Generation Wavelets", *SIAM J. of Math. Analysis*, 29(2), pp. 511–546, Dec. 1997.

[7] H.-J. Wang, P.-C. Su, and C.-C. Kuo, "Wavelet-based Digital Image Watermarking", *J. of Optics Express*, vol. 3, no 12, pp. 491–496, Dec. 1998.

[8] P. W. Wong and E. J. Delp (eds.), "Security and Watermarking of Multimedia Contents III", *Proceedings of the SPIE*, vol. 4314, Jan. 2001.

Dai-Gyoung Kim : Department of Applied Mathematics, Hanyang University, Ansan, 425-791 Korea
E-mail address: dgkim@hanyang.ac.kr

Joo-Yoen Lyu : Department of Mathematics, Hanyang University, Seoul, 133-791 Korea
E-mail address: leina99@freechal.com