Combined Private and Public Watermarking in Wavelet Transform Domain

小波轉換域之秘密與公開混成數位浮水印

Der-Chyuan Lou (婁德權) Jiang-Lung Liu (劉江龍) Ming-Chang Chang (張明昌)

Department of Electrical Engineering
Chung Cheng Institute of Technology
National Defense University
Tahsi, Taoyuan 33509, Taiwan
e-mail: dclou@ccit.edu.tw

Abstract

In this paper, a wavelet-based digital watermarking algorithm is proposed. Unlike other watermark casting algorithms, which embedded either a random number of a sequence of bits or a visually recognizable pattern as a watermark into the original source at a time, we present an algorithm to embed two watermarks for the copyright protection improvement. In the proposed approach, an original image is decomposed into three levels using a discrete wavelet transform (DWT). The two watermarks, standing for the owner's signature and the customer's unique serial number, are embedded into and extracted from different middle-frequency subbands with private and public watermarking, respectively. The embedding and extraction procedures can be performed in parallel to reduce the processing time, especially in large-scale use of watermarks for the purpose of owner identification and transaction tracking simultaneously. Simulation results show that the embedded watermarks are imperceptible in the watermarked image and could be perfectly extracted under no attack. Moreover, the superior performance of the proposed technique is robust to various signal distortions.

Keywords: Digital watermarking, wavelet transform, copyright protection, image processing.

摘要

傳統的數位浮水印方法通常一次僅隱藏具視覺意義的圖騰或隨機位元序列，本文以小波轉換將影像切割成不同能量次頻帶，在不可見性的需求下，將分別代表原創作者的二值圖案與合法使用者之序號等兩種浮水印，以秘密與公開混成方式，同時隱藏在原始圖像中。本文方法在隱藏與萃取浮水印時均可平行處理，尤其在大量進行圖像浮水印操作具實用價值。實驗結果顯示，經過一般影像處理及幾何攻擊後，藏匿的浮水印仍可存活，證明本文方法在數位世代中深具潛力，可強化數位媒體著作權保護。

關鍵詞：數位浮水印，小波轉換，著作權保護，影像處理。

1. Introduction

The rapid development of the Internet and digital technology makes it easy and efficient to distribute multimedia data than before. However, because digital data, including audio, video, images, and documents, could be duplicated and modified without difficulty, there is an urgent need for copyright protection in the e-commerce era. Digital watermarking is a technology of embedding a hidden signal into digital contents to identify the legitimate owner, track unauthorized use, or detect intentional tampering of the original data. Digital watermarking plays an important role in these applications and draws universal attention both in academia and business over the last decade. The most important key requirements of watermarking schemes are imperceptibility and robustness. That is, the embedded watermark must be perceptually invisible and difficult to destroy without severe degradation in media fidelity [1].

According to the necessity of original media when extracting a watermark, watermarking systems can be classified into private and public ones (the latter is also referred to as blind or oblivious watermarking). Private algorithms need the original media and possibly distorted one during detection, which limits their usage since original media are difficult to obtain sometimes. On the other hand, public algorithms, requiring neither the original media nor the embedded watermark, have much wider applications such as broadcast monitoring, copy control, and transactional watermark (also known as fingerprinting) but remain the challenging problems. In general, the private algorithms are more robust than the public ones [2][7].

Wavelet-based methods become more prevalent in transform-domain watermarking community due to their excellent spatial localization and frequency spread characteristics. Moreover, increasing research results in the literature show that the wavelet-based techniques provide the superior robustness to various signal processing attacks and loosy compression. The proposed method focuses on digital watermarking for gray-level images using wavelet transform, which can be conveniently integrated in forthcoming compression standards, such as JPEG 2000 and MPEG 4. With the standardization process of JPEG 2000 and the shift from discrete cosine transform (DCT) to DWT method, watermarking schemes operating in the wavelet transform domain have become even more enthralling and pressing [3][4].

The proposed technique embeds two watermarks into different middle-frequency subbands to compromise between the transparency and the robustness requirements mentioned above, based upon the following two main reasons [5].

- Human visual system (HVS) is more sensitive to lower frequency noise.
- Higher frequency coefficients are susceptible to be suppressed by loosy compression.

Unlike traditional watermarking algorithms, which embedded either a random number of a sequence of bits or a visually recognizable pattern as a watermark into the original image at a time, the proposed algorithm embeds two binary watermarks all with values 0 or 1 for the copyright protection enhancement [6]. Specifically, one is a visually recognizable binary image; the other is a binary serial number (called w_1 and w_2 in the rest of this paper, respectively). The w_1 can be designed as the owner's seal, signature, or an organization's logo. The w_2 stands for buyer's unique information that could be identified as the legal recipient of the copy, and used to trace the source of illegally redistributed content. These are potentially useful both as a deterrent to infringement of copyright and a scientific aid to investigation.

The remaining paper is organized as follows. In Section 2, the details of the proposed watermarking algorithm are given. The experimental results of the proposed algorithm are shown in Section 3. Finally, the conclusions are drawn in Section 4.

2. THE PROPOSED METHOD

By using wavelet transform, a whole image is decomposed into four subbands, i.e., low frequency subband (LL), high-low frequency subband (HL), low-high frequency subband (LH), and high frequency subband (HH). The subband LL, which contains important information of an image, can be further transformed and divided into four subbands several times depended on the applications. The subbands labeled HL, LH, and HH represent edge details of horizontal, vertical, and diagonal directions, respectively. An illustration of three levels with ten subbands of wavelet structure is shown in Fig. 1.

Let X be the original gray-level image with size M ╳ M, w_1 be the binary-valued watermark image with size N ╳ N, and w_2 be the binary random sequence with length P. The algorithm of the proposed combined watermarking is presented below.

2.1 Embedding Procedure

The block diagram for embedding procedure is shown in Fig. 2. The original image X is decomposed into three levels with ten subbands of a wavelet structure Y. The embedding steps of w_1 and w_2 are performed as follows, respectively. Let $c_{LH3}(i,j)$, $c_{HL3}(i,j)$, $c'_{LH3}(i,j)$, and $c'_{HL3}(i,j)$ denote the original and watermarked coefficients of subbands LH3 and HL3, respectively.

2.1.1 Embedding steps of w_1

Step 1: Map the watermark w_1 content values 0 to –1, scramble its spatial relationship, and expand the size of w_1 to the same of LH3 subband. More precisely, each pixel in w_1 is expanded with size $\frac{M}{8N} \times \frac{M}{8N}$.

Step 2: Perform the watermark w_1 casting by using the spread spectrum technique defined as:

$$c'_{LH3}(i,j) = c_{LH3}(i,j) \times \left(1 + \alpha \times \omega_1(i,j)\right), \tag{1}$$

where α is a scaling factor.

2.1.2 Embedding Procedure of w_2

Step 1: Choose the watermark w_2 positions within HL3 subband randomly by a pre-determined key, key_0, in the pseudo-random number generating system. If the HL3 subband is of size $\frac{M}{8} \times \frac{M}{8}$, the position of each element in w_2 must be restricted to $\left[1,\ \frac{M}{8} - 2\right]$. This is due to the need of neighboring values during generating w_2 . Besides, to keep away from overlapping of w_2 allocation and alteration of coefficients, the modulated position is divided at least one pixel between each other and the chosen coefficients should not be selected as embedding position again in the remaining selection.

Step 2: Calculate mean value $m(i,j)$ of each chosen neighboring coefficients of $c_{HL3}(i,j)$.

$$m(i,j)=\left(\sum_{x=i\text{-}1}^{i+1}\sum_{y=j-1}^{j+1}\left(c_{HL3}(x,y)\right)-c_{HL3}(i,j)\right)\Big/8 . \tag{2}$$

Step 3: Modulate each chosen coefficient $c_{HL3}(i,j)$ to $c'_{HL3}(i,j)$, and generate a binary sequence $w_2(i,j)$ for detection procedure later.

$$c'_{HL3}(i,j)=c_{HL3}(i,j)\times\left(1+\beta\times t\right), \tag{3}$$

where β is a scaling factor and *t* is defined at the bottom of the page.

Finally, take the two-dimensional inverse DWT of the associated result to obtain the watermarked image.

2.2 Extraction Procedure

The block diagram for the extraction procedure is shown in Fig. 3. In this paper, w_1/w_2 can be extracted with/without original image. That is, both original image and the watermarked image are required in extracting w_1 , but only the latter is needed during extracting w_2 . Assume that both original image *X* and watermarked image *X’* are DWT transformed into ten subbands for three different levels, respectively. That is,

$$\begin{cases} Y=DWT(X), \\ Y'=DWT(X'). \end{cases} \tag{4}$$

The remaining extraction steps are depicted as follows.

2.2.1 Extraction steps of w_1

Step 1: Subtract the coefficients of the subband LH3 of *Y* from the coefficients of the subband LH3 of *Y’* to obtain the differences D_{LH3} .

$$D_{LH3}=Y'_{LH3}-Y_{LH3}. \tag{5}$$

Furthermore, for all $d_{LH3}(i,j)$ within D_{LH3} , if $c_{LH3}(i,j)<0$, then reverse the sign of $d_{LH3}(i,j)$.

Step 2: Sum the differences D_{LH3} to *S* for each $\frac{M}{8N}\times\frac{M}{8N}$ block, map each *S* to the binary-valued w'_{1p} by the following formula, and unscramble w'_{1p} to get the restored mark w'_1 .

$$t=\begin{cases} 1, & \text{if } c_{HL3}(i,j)\geq 0 \text{ and } c_{HL3}(i,j)\geq m(i,j)\Rightarrow w_2\left(i,j\right)=1 \\ -1, & \text{if } c_{HL3}(i,j)\geq 0 \text{ and } c_{HL3}(i,j)< m(i,j)\Rightarrow w_2\left(i,j\right)=0 \\ -1, & \text{if } c_{HL3}(i,j)< 0 \text{ and } c_{HL3}(i,j)\geq m(i,j)\Rightarrow w_2\left(i,j\right)=1 \\ 1, & \text{if } c_{HL3}(i,j)< 0 \text{ and } c_{HL3}(i,j)< m(i,j)\Rightarrow w_2\left(i,j\right)=0 \end{cases}$$

$$\begin{cases} w'_{1p} = 1, & \text{if } (S \geq 0), \\ w'_{1p} = 0, & \text{if } (S < 0). \end{cases} \tag{6}$$

2.2.2 Extraction steps of w_2

Step 1: locate the w_2 positions within subband HL3 of Y' using the same key, key_0, depicted in step 1 of embedding w_2.

Step 2: Calculate neighbors' mean value by equation (2), and restore w'_2 with the following rule.

```
if $c'_{HL3}(i, j) \geq m(i, j)$ then
    $w'_2(i, j) = 1$
else                                        (7)
    $w'_2(i, j) = 0$
end
```

3. EXPERIMENTAL RESULS

All the experiments described below use the discrete Haar wavelet transform to produce the frequency coefficients. The degradation of the watermarked image depends on the amount of embedding information and the embedding intensity. In the experiment, we use Lena as the original image, our institute's badge as a binary image watermark w_1, and the length of binary random sequence w_2 is 256. We choose α = 0.1 and β = 0.2 to balance the tradeoff between fidelity and robustness. Fig. 4 illustrates an example of the proposed method. Without any attacks, the embedded watermarks are perfectly extracted from the watermarked image.

The embedded watermarks not only should be perceptually invisible, but also must be robust to various attacks. To test and verify the robustness of our watermarking algorithm, the watermarked image is attacked by loosy compression, filtering, geometric distortions such as cropping and scaling. The robustness of the proposed watermarking algorithm is tested by the effects of distortion on the objective measurements described as follows.

- The peak-signal-to-ratio (PSNR) is given by

$$\text{PSNR} = 10\log_{10}\frac{255^2}{MSE} \ \text{(dB)}, \tag{8}$$

where *MSE* is the mean-square error between the original image and the watermarked one.

- Standard correlation coefficient (also referred to as correlation) is used to judge the similarity between the original watermarks and the extracted watermarks.. The correlation coefficient is defined as shown in (9) (at the bottom of the page), where *W* is the original watermark and *W'* is the extracted watermark. Their corresponding mean values are $\overline{W}$ and $\overline{W'}$, respectively. In this study, the criterion of correlation values can be divided into three levels, shown as follows.

Confidence level	Value
Low	Below 0.7
Middle	0.7 0.75
High	Above 0.75

$$\text{correlation} = \frac{\sum_i \sum_j \left(W(i,j) - \overline{W}\right)\left(W'(i,j) - \overline{W'}\right)}{\sqrt{\sum_i \sum_j \left(W(i,j) - \overline{W}\right)^2}\sqrt{\sum_i \sum_j \left(W'(i,j) - \overline{W'}\right)^2}}, \tag{9}$$

3.1 JPEG/JPEG 2000 Loosy Compression

JPEG and JPEG 2000 compression standards are used to examine the robustness of the watermark. When quality factor (QF) is low, it means the compression ratio is high with less image fidelity. We use JPEG and JPEG 2000 compression under different QF on the watermarked image, respectively. The extracted results are depicted in Table 1 and Table 2. From the simulation results, we can claim that the method performs best resistance to these two kinds of compression standards.

3.2 Filtering

In general, smoothing and sharpening operations are used to enhance the image quality. These operations are applied to evaluate the robustness of our algorithm. Table 3 shows the extracted results of applying these operations separately. As can be seen, the extracted watermarks are highly similar to the original. In general, the proposed method performs better in sharpening operations than in blurring ones under lower PSNR value.

3.3 Cropping

Usually, A pirate would try to remove the embedded watermark by cutting some uninteresting part of the watermarked image. For example, a quarter of the watermarked image is cropped, as shown in Fig. 5. Table 4 shows the relationship between the extracted results and the cropping ratio. Whether the missing portions are filled with zero values or original unwatermarked images, it is interesting to find out that the results are the same. Although the extracted w_1 is degraded linearly as the cropped ratio is increasing, the extracted rate of w_2 is still high.

3.4 Scaling

The watermarked image is scaled to its half size in both dimensions and then rescaled to its original size. Table 5 shows that the extracted result is still visually recognizable.

4. CONCLUSIONS

This paper has presented a novel algorithm for embedding two watermarks into the image with private and public watermarking at a time. This algorithm reduces noticeable artifacts by embedding the watermarks into different middle-frequency subbands of the wavelet transform. One benefit for the proposed algorithm is that we can embed/extract the two watermarks in parallel, especially in large-scale use of watermarks for copyright protection. Since the two watermarks, a visually distinguishable image and a binary random sequence, stand for the original owner’s signature and the buyer’s unique serial number, respectively. This algorithm can be used for the purpose of ownership identification and fingerprinting complementarily. Specifically, it would be useful to prove in court using public watermarking that a watermark is present without exhibiting the original image publicly. Furthermore, if necessary, we can enhance the authentication by private watermarking therein. Simulation results demonstrate that the proposed method has superior performances to common image operations and geometric distortions, and therefore satisfy the watermarking properties mentioned in the introduction section. With these advantages, this algorithm has potential for image copyright protection in digital world.

Future work will focus on incorporating the human visual model (HVS) and error correcting codes (ECC) to improve the robustness under some perceptual mask.

5. REFERENCES

[1] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

[2] I. J. Cox, and M. L. Miller, “The first 50 years of electronic watermarking,” *EURASIP Journal on Applied Signal Processing*, vol. 2002, no. 2, Feb. 2002, pp. 126–132.

[3] I. Hong, I. Kim, and S.-S. Han, “A blind watermarking technique using wavelet transform,” *Proceedings of the IEEE International Symposium on Industrial Electronics*, vol. 3, 2001, pp. 1946–1950.

[4] M.-S. Hsieh, D.-C. Tseng, and Y.-H. Huang, “Hiding digital watermarks using multiresolution wavelet transform**,”** *IEEE Transactions on Industrial Electronics*, vol. 48, no. 5, pp. 875-882, Oct. 2001.

[5] C.-T. Hsu and J.-L. Wu, “Hidden digital watermarks in images,” *IEEE Transactions on Image Processing*, vol. 8, no. 1, pp. 58 -68, Jan. 1999.

[6] H.-C. Huang, F.-H. Wang, and J.-S. Pan, “A VQ-based robust multi-watermarking algorithm,” *IEICE Transactions on Fundaments*, vol. E85-A, no. 7, pp. 1719-1726, July 2002.

[7] S.-J. Lee and S.-H. Jung, “A survey of watermarking techniques applied to multimedia,” *Proceedings of IEEE International Symposium on Industrial Electronics*, vol. 1, 2001, pp. 272–277.

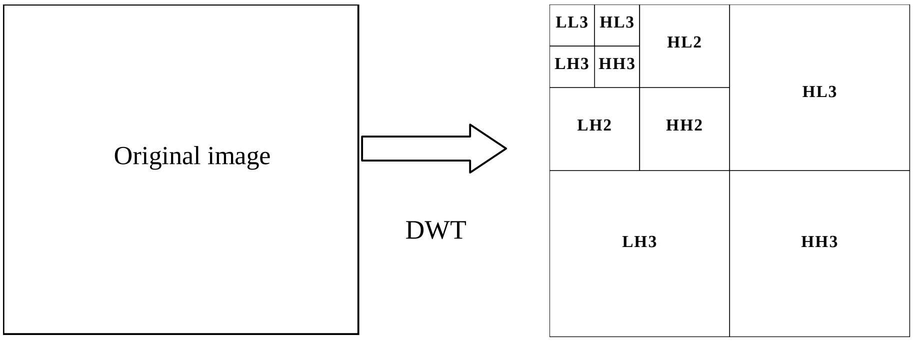


Fig. 1. Three-level DWT hierarchical decomposition of an image.

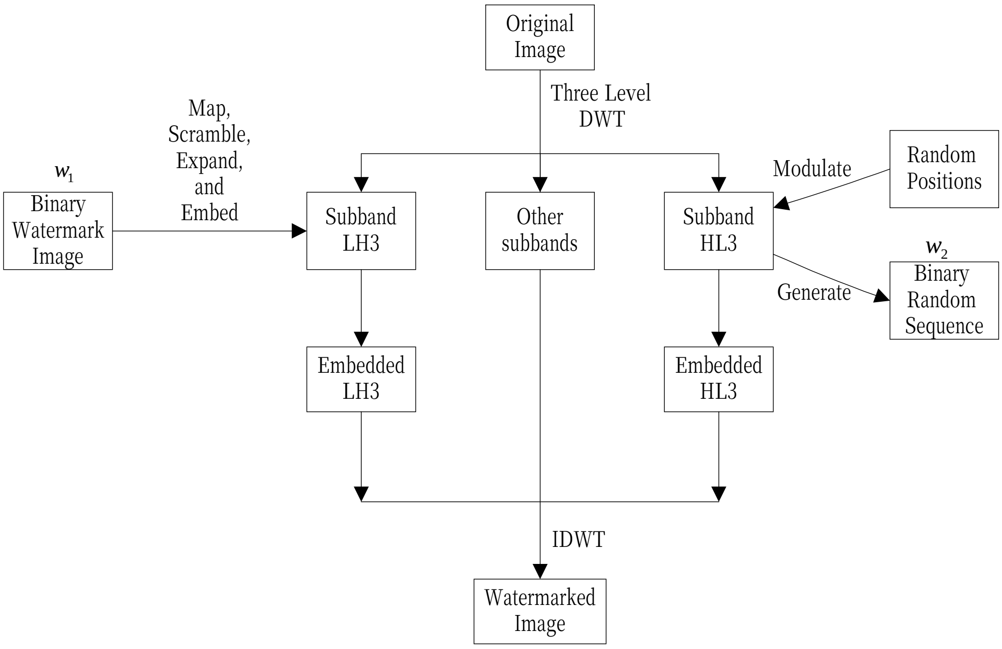


Fig. 2. The block diagram for embedding two watermarks.

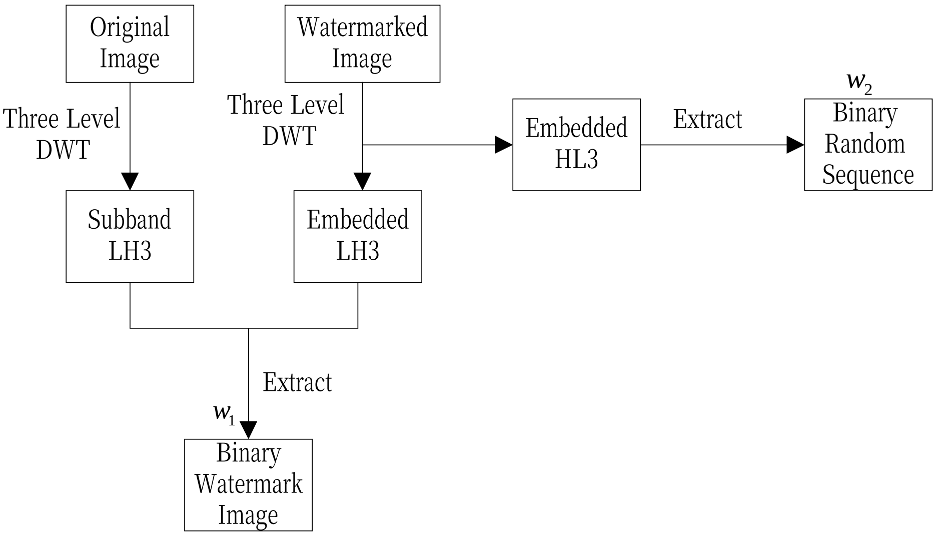
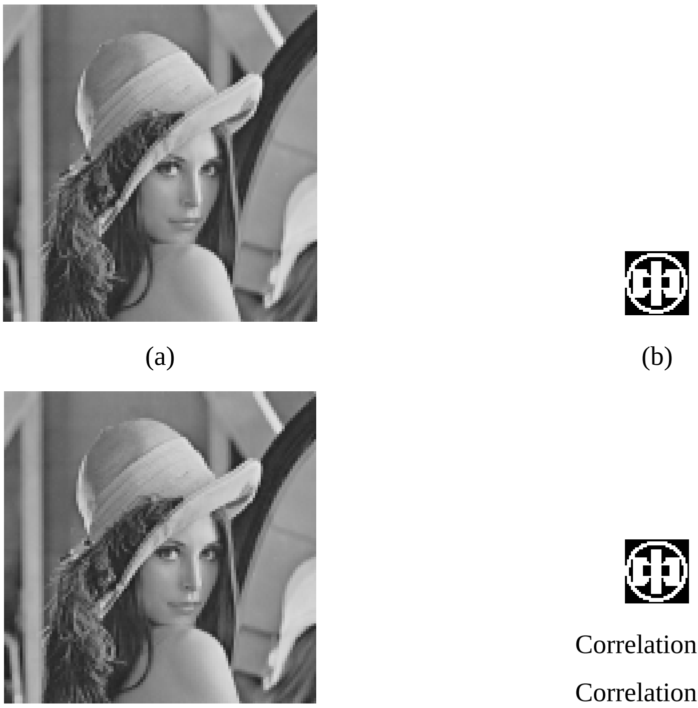


Fig. 3. The block diagram for extracting two watermarks.



(a) (b)

Correlation1=1

Correlation2=1

(c) (d)

Fig. 4. Example of the proposed watermarking approach. (a) Original gray level image Lena of size 512 by 512. (b) Watermark w_1 of size 32 by 32. (c) Image with embedded watermarks w_1 and w_2 (PSNR 46.55 dB). (d) The extracted watermarks with no attacks.

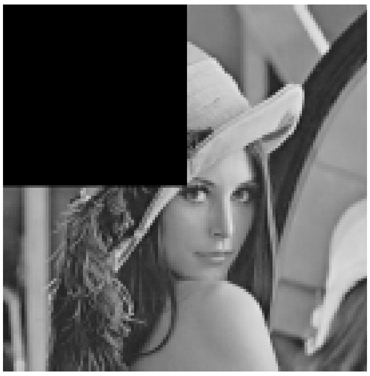


Fig. 5. Quarter of the embedded image is missing.

Table 1. Changes of measures and extracted watermarks under various JPEG quality factors.

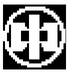
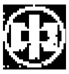
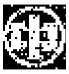
QF (%)	100	50	30
PSNR (dB)	42.66	35.03	33.7
Extracted watermarks			
Correlation1	1	0.9706	0.8650
Correlation2	1	0.8751	0.7513

Table 2. Changes of measures and extracted watermarks under various JPEG 2000 quality factors.

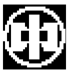
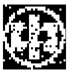
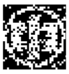
QF (%)	100	80	60
PSNR (dB)	44.65	37.65	37.05
Extracted watermarks			
Correlation1	1	0.8495	0.6865
Correlation2	0.9765	0.8437	0.7900

Table 3. Results of filtering.

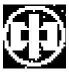
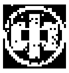
Image operations	Sharpen	Blur
PSNR (dB)	33.81	34.27
Extracted watermarks		
Correlation1	0.9768	0.8985
Correlation2	0.9844	0.9451

Table 4. Results of cropping.

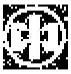
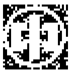
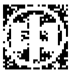
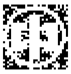
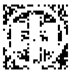
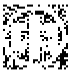
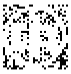
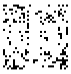
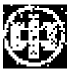
Remaining part	89.7%	79.8%	75.0%	69.7%	60.0%	50.0%	39.6%	29.5%	20.0%	9.9%
Extracted watermarks										
Correlation1	0.8723	0.8022	0.7439	0.7255	0.6280	0.5525	0.4745	0.4235	0.3533	0.2517
Correlation2	0.9922	1	1	1	0.9844	1	1	1	1	1

Table 5. Robustness to scaling attack.

PSNR	32.93
Extracted watermark	
Correlation1	0.8637
Correlation2	0.9611