A New Robust Watermark Embedding into Wavelet DC Components

Sanghyun Joo, Youngho Suh, Jaeho Shin, and Hisakazu Kikuchi

ABSTRACT— In this paper, we propose a non-blind watermarking method that embeds a pseudo-random sequence (watermarks) into wavelet DC components. The DC area is not suitable for embedding because of severe visual degradation. We overcome the degradation problem by embedding watermarks into visually insensitive locations. We compare our experimental results with respect to JPEG compression with Cox's popular correlation-based method. We also compare the robustness of our technique with other methods registered in CheckMark. This study reveals that the proposed method simultaneously provides good fidelity in quality as well as robustness against external attacks

I. INTRODUCTION

With rapid growth of multimedia technology, digital watermarking for multimedia has become one of the widely used copyright protection methods. Invisible watermarking requires a reasonable robustness against attacks such as JPEG compression, as well as little or no degradation in the subjective and objective image quality. Watermarking in the frequency domain is more robust than watermarking in the spatial domain [1], because the watermark information can be spread out to the entire image [2]. In the viewpoint of frequency, the high frequency area should be avoided for robustness while the low frequency area should be avoided for fidelity. Recent work has focused on developing methods for embedding watermarks in the middle frequency range, because this is known to provide a good trade-off between robustness and fidelity [2]-[4]. The DC area has been excluded from the consideration for watermark embedding, even though it can give the most robustness.

This paper demonstrates that the right technique can embed watermarks into the DC area while preserving good fidelity. Our embedding strategy is based on a wavelet transform. An image is decomposed into several sub-bands by a wavelet. To embed watermark bits $\{-1, +1\}$, a reference DC' is prepared by taking a low pass filtering to the original DC. The DC values are changed to values smaller or larger than the DC' values in accordance with the corresponding watermark bits. To reduce image degradation, the watermark bits are embedded into locations with small differences between the DC and DC'. As a result, watermarks can be strongly embedded with good fidelity.

II. WATERMARK EMBEDDING

The proposed watermarking is explained for a gray image. First, an original image in which the watermark is to be embedded is decomposed by a wavelet. In our embedding strategy, watermarks are embedded into wavelet DC components. The discrete wavelet transfrom (DWT) converts a signal into low (L) and high (H) frequency sub-bands. An image can be transformed by performing a DWT in both vertical and horizontal directions, resulting in one low frequency sub-band (LL) and three high frequency sub-bands (LH, HL, and HH). The same process is repeated on the LL sub-band to generate the next level of decomposition. For an n-level decomposition for an $M \times N$ image, the size of the DC area in which watermarks are to be embedded is $MN/2^{2n}$ (Fig. 1). Considering the length of the watermarks, robustness, fidelity, and so on, we determine the wavelet decomposition.

Manuscript received Mar. 5, 2002; revised July 6, 2002.

Sanghyun Joo (phone: +82 42 860 1631, e-mail: joos@etri.re.kr) and Youngho Suh (e-mail: syh@etri.re.kr) are with DRM Research Team, ETRI, Daejeon, Korea.

Jaeho Shin (e-mail: jhshin@dongguk.edu) is with Dongguk University, Seoul, Korea.

Hisakazu Kikuchi (e-mail: kikuchi@eng.niigata-u.ac.jp) is with Niigata University, Niigata, Japan.

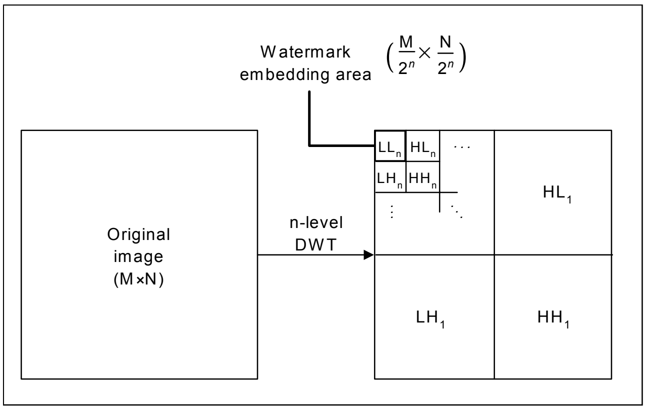


Fig. 1. n-level wavelet decomposition and its DC area to embed watermarks.

The determined LL_n can be seen as a reduced version of the original image. In our embedding strategy, a reference LL_n' is prepared. The original LL_n is further wavelet-transformed and then three high-frequency sub-bands (LH_{n+1}, HL_{n+1}, and HH_{n+1}, excluding LL_{n+1}) are initialized to zeros and inverse wavelet-transformed. We can then obtain another LL_n' from the process (Fig. 2). This newly prepared LL_n' is used for embedding as a reference sub-band. In addition, this process can be replaced with a low-pass filtering to the LL_n.

We use a binary watermark sequence, $w(i) \in \{-1, +1\}$, $1 \le i \le$ wm_length, generated by a seed. The LL_n values are replaced with $LL_n' \pm K \times w(i)$ (1), where K is a factor for controlling embedding intensity. Some change in LL_n is more visually sensitive than that in the other sub-bands. Thus, large changes in LL_n values cause a severe degradation in visual quality. To avoid this, the watermark bits should be embedded into the locations with small differences between LL_n and LL_n'. The location information is obtained by sorting $| LL_n - LL_n' |$ in magnitude (Fig. 2). This embedding process should be repeated, because the changes in LL_n values also cause some changes in its leading LL_n' values. As the embedding is repeated, the resulting peak signal-to-noise ratio is decreased but its reliability is increased. Figure 3 shows the relationship between the embedding iteration and its resulting PSNR.

```
for i = 1:wm_length
  if($w(i)$ == +1)
    if($LL_n(idx(i)) < LL_n'(idx(i)) + K$)
      $LL_n(idx(i)) = LL_n'(idx(i)) + K$
    end
  else if($w(i)$ == –1)
    if($LL_n(idx(i)) > LL_n'(idx(i)) - K$)
      $LL_n(idx(i)) = LL_n'(idx(i)) - K$
    end
  end
end                                                          (1)
```

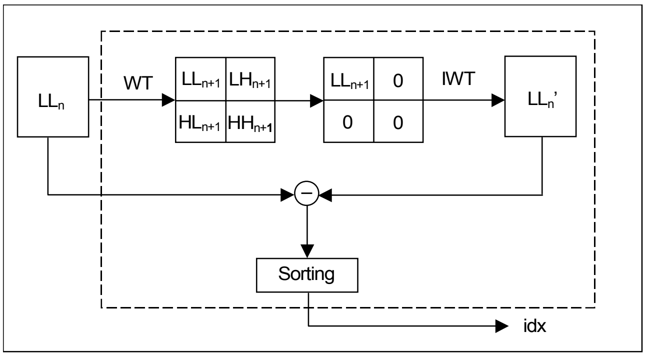


Fig. 2. Reference sub-band and location information for watermark embedding.

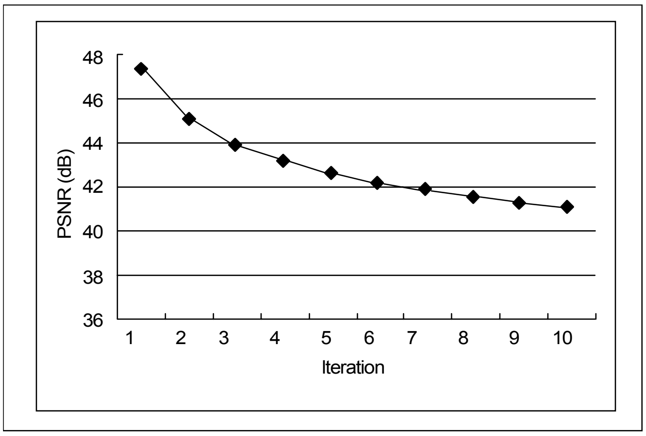


Fig. 3. Relationship between embedding iterations and the resulting PSNRs.

III. WATERMARK EXTRACTION

The original image is required in extracting watermarks. We classify such an extraction as non-blind watermarking. The same wavelet decomposition used in the embedding is applied to both the original and embedded images. The watermark-embedding locations are obtained from the original image. Since we obtain LL_n and LL_n' from the watermark embedded image, we can extract the watermarks by comparing the two values, LL_n and LL_n'. Then the extracted watermarks are compared with the original watermarks generated by the user key. In this comparison, we use the similarity measure given in (2), where · denotes the inner product.

$$\mathrm{Sim}(w, w^*) = \frac{w \cdot w^*}{\sqrt{w^* \cdot w^*}} \qquad (2)$$

IV. EXPERIMENTAL RESULTS

In our experiments, a pseudo-random binary sequence is used as a watermark. The sequence is generated from the seed number 500 and its length is 1000. The watermarks are embedded in the 512×512 gray-level Lena image. A three-level discrete wavelet transform is employed and thus the size of DC area to be embedded is 64×64.

Our method is compared with Cox's method [1], which is one of the most popular correlation-based watermarking techniques. To obtain similar fidelity after watermark embedding, we set K to 15 and the iteration to 10. The resulting PSNRs were 39.76 dB for Cox's and 40.69 dB for ours. For both methods, the original watermark was compared with the one extracted from the JPEG-compressed images. Figure 4 shows the detection values for JPEG images compressed with various quality factors. In this experiment, the JPEG quality factor was varied from 10% to 90%. Figure 5 shows the detection responses between the watermark sequence extracted from the JPEG-compressed image (20% quality factor) and the watermark sequences generated from seed numbers taken by 1 to 1000. Each peak value in the figure is matched with the similarity value corresponding to the same quality factor shown in Fig. 4.

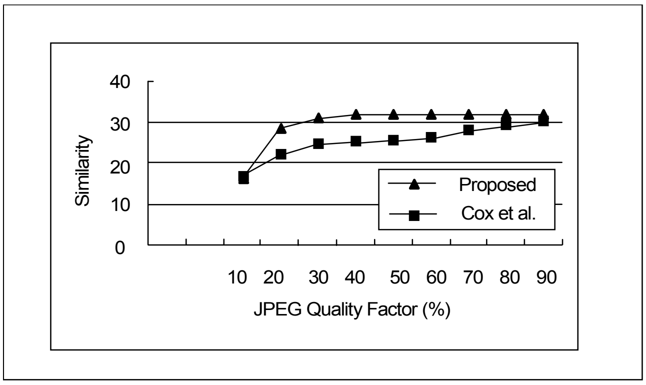
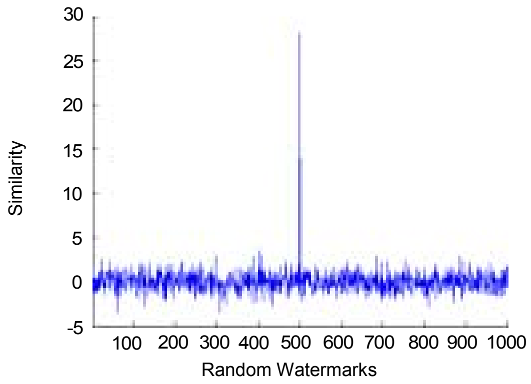
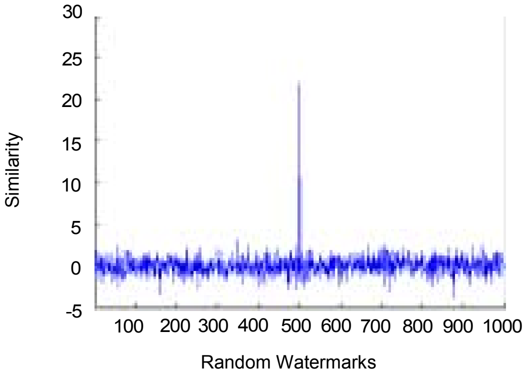


Fig. 4. Similarity comparison with various JPEG-compressed images.

As shown in the figures, the proposed method suffers much less from JPEG lossy compression than Cox's method. The proposed watermarking strategy is also very robust against non-geometric attacks such as filtering. The proposed method was also tested with respect to non-geometric attacks (the latest version 1.2) provided from CheckMark [5] and compared to those of other methods [2], [6], [7] registered to the CheckMark web site (Table 1). However, most correlation-based watermarking techniques, including the proposed one, suffer from geometric attacks such as rotation, scale, and translation. Some other researchers have tried to solve the problem by using templates [8]. Currently, we are working on further enhancing the robustness of our watermark embedding method using such a technique.



(a) The proposed method



(b) Cox's method

Fig. 5. Detection responses to JPEG image compressed with a qualtity factor of 20%.

Table 1. Detection comparisons to other techniques.

Methods, payload in bits	Non-geometric (5 images, 235 attacks)
Wang, 1	74%
Cox, 1 [2]	90%
Xia, 1 [5]	84%
Kim, 1 [6]	48%
Proposed, 1	93%

V. CONCLUSION

We proposed a robust watermark embedding method that is accomplished on the wavelet DC domain. To embed binary watermarks, we used a reference DC' obtained from the original DC. The watermarks were embedded by subtracting or adding K to DC'. Since the watermarks were embedded into the locations with small differences between DC and DC', we were able to strongly embed watermarks while preserving good fidelity. The experimental results show that the proposed embedding scheme is more robust against non-geometric attacks than other methods.

REFERENCES

[1] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, “Techniques for Data Hiding,” *IBM Systems Journal*, vol. 35, no. 3-4, 1996, IBM, USA, pp. 313-336.

[2] I.J. Cox, J. Killian, T. Leghton, and T. Shamoon, “Secure Spread Spectrum for Multimedia,” *IEEE Trans. on Image Processing*, vol. 6, no. 12, 1997, pp. 1673-1687.

[3] Jongwon Seok, Jinwoo Hong, and Jinwoong Kim, “A Novel Audio Watermarking Algorithm for Copyright Protection of Digital Audio,” *ETRI J.*, vol. 24, no. 3, June 2002, pp. 181-189.

[4] C.T. Hsu and J.L. Wu, “Hidden Digital Watermarks in Images,” *IEEE Trans. on Image Processing*, vol. 8, no. 1, 1999, pp. 58-68.

[5] CheckMark, http://watermarking.unige.ch/Checkmark/.

[6] X. Xia, C.G. Boncelet, and G.R. Arce, “A Multiresolution Watermark for Digital Images,” *Proc. of IEEE ICIP*, Santa Barbara, CA, USA, Oct. 1997, pp. 548-551.

[7] J.R. Kim and Y.S. Moon, “A Robust Wavelet-Based Digital Watermarking Using Level-Adaptive Thresholding,” *Proc. of IEEE ICIP*, vol. 2, Kobe, Japan, Oct. 1999, pp. 226-230.

[8] S. Pereira and T. Pun, “Robust Template Matching for Affine Resistant Image Watermarks,” *IEEE Trans. on Image Processing*, vol. 9, no. 6, pp. 1123-1129.