A Wavelet Transform based Watermarking for Digital Signatures

Sang-Heun Oh, Hee-Sup Lee, Keun-Young Lee
Department of Electrical and Computer Engineering, SungKyunKwan Univ
Kyunggi-Do Suwon Jangan-Gu Chunchun-Dong 440-746, Korea
Tel: +82-331-290-7193, Fax: +82-331-290-7180
E-mail: sam8080@mickey.skku.ac.kr

Abstract: This paper presents a new watermarking method based on wavelet transform. Embedding algorithm can define robust area by varying thresholds and gives a watermark image the priority of significance by analyzing spatial correlation of the watermark image. Detector can adjust thresholds to the distorted watermarked image. Also detector can extract the embedded data without an original image. A new measurement for detecting the correct watermark is suggested. Simulation results show that the embedded watermark is robust against various signal processing and compression attacks.

1. Introduction

With the recent growth of networked multimedia systems, techniques are needed to prevent the illegal copying, forgery and distribution of digital audio, images and video. It is also desirable to determine where and by how much the multimedia file has been changed from the original. One way to improve one's claim of ownership over an image, for instance, is to place a low-level signal directly into the image data. This signal, known as a digital watermark, uniquely identifies the owner and can be easily extracted from the image.

Current techniques describes in the literature for the watermarking of images can be grouped into two classes: spatial domain techniques [1][2] which embed the data by directly modifying the pixel values of the original image and frequency domain methods which embed the data by modulating the frequency domain coefficients. Frequency domain techniques can be divided further by which transform is used. DCT based embedding techniques [3][4] and wavelet transform based embedding techniques [5][6][7] are mostly researched. We propose a wavelet transform based watermarking methods which show greater robustness to common signal distortions. The fundamental advantage of our wavelet -techniques lie in the management of robustness during embedding watermark and distortion can be compensated during detecting watermark.

2. Proposed Watermark Method

In this section, we propose a watermark method using classified coefficients. The basic idea is the same as Inoue et. al. in [7] which shows good performance controlling the quality of image with two thresholds. While embedding a watermark, the wavelet coefficients lying between T1 and T2 are modified to one of thresholds according to a watermark bit. The distance of two thresholds can control trade off between the quality of the image and the robustness of the watermark. If the distance of two thresholds T1 and T2 become large, the quality of the image is degraded while the embedded watermark is robust to various attacks. There can be problem when the detector used the fixed thresholds T1, T2. Watermarked coefficients can be changed by attacks, so detector also needs to rebuild T1 and T2 dynamically.

The proposed embedding method saves $\Delta\alpha$, embedded position and watermark. $\Delta\alpha$ is proportion to the maximum coefficient of a subband and the robust area for the important part of the watermark can be defined by varying $\Delta\alpha$.

The proposed watermark extracting method rebuilds T1 by averaging coefficients in which the watermark "0"s are embedded and T2 by averaging coefficients in which the watermark "1"s are embedded. When all embedded watermarks are "0" or "1", one of two thresholds can't be estimated. In that case, the missed threshold can be estimated by using $\Delta\alpha$. When the correct watermark is used to estimate thresholds, the difference of T2 and T1 is larger than when incorrect watermark is used. From this fact, we find that the difference of thresholds can be used to measure uniqueness of the watermark from other watermarks.

The above embedding and detecting methods are for watermarks as random sequence or information data. In case of an image as a watermark, we segment the watermark image by using the correlation between pixels before embedding and compose it after extracting. During segmenting and composing a watermark image, we can extract significant bits to embed robust area of the original image. Also we can reduce bits to embed up to 20%.

This paper is organized as follows, In section 3, we propose the new watermark embedding method based on wavelet transform. In section 4, our new watermark extracting method is described. In section 5, watermarking method of images are suggested. In section 6, we implement some experiments in terms of several different image distortions, such as JPEG compression, rescaling, cropping, filtering and multiple watermarking.

3. Watermark Method for Information Data

3.1 Embedding Method

We describe the watermark embedding method using classified coefficients after wavelet decomposition. Watermarks are embedded by modifying classified wavelet coefficients at the coarsest scale, LH3, HL3 and HH3 except for the lowest frequency subband LL3. Two thresholds T1 and T2 are decided by $\Delta\alpha$ and Cmax's, the

This paper was supported by SamSung Research Fund. SungKyunKwan University, 1999

absolute maximum values of the coarser subbands LH3, HL3, HH3. The embedding algorithm is described as follows.

Stage1 Read watermark WM(k), k=1,2,........,N.

Stage2 Initiate α=1, Δα and get all Cmax's.

Stage3 T2=αCmax and T1=(α-Δα)Cmax and find the coefficients Ci(i=0,1,....,M), satisfying T1<|Ci|<T2.

Stage4 The watermark are embedded by modifying selected Ci
If W(k)=1 , then Ci=sign(Ci)×T2
If W(k)=0 , then Ci=sign(Ci)×T1

Stage5 If i< N×3 then α=(α-Δα) and set new Δα. go to stage 3.

Stage6 Save Δα and corresponding embedded position and W(k).

Information data is embedded three times because detector can vote for distorted data. It is well known that the modification of insignificant coefficients of small value can leads to perceptual degradation of the image. To avoid this, we suggest that Δα is decreasing as the coefficient value is closed to zero and coefficients which are classified by T1=0 are not modified. On the contrary, the large Δα near Cmax can make the robust area for the attacks.

3.2 Extracting Method

We propose a watermark detecting by using Δα, corresponding embedded position and the watermark W(k). After image processing or intentional attack, watermarked coefficients which have been mapped to one of thresholds are distorted, so detector needs to rebuild T2 and T1 for extracting watermark. After the wavelet decomposition of watermarked image, the method we propose is as follows,

Stage1 Read W(k), Δα and embedded position. Get Cmax's of each subband and set α=1.

Stage2 Using α and the embedded position read corresponding wavelet coefficients $\hat{Ci}$ (i =1,2..M).

Stage3 Read W(k),and set i=k,x=0,1,2,....,y=0,1,2,...
If W(i)="1" then $|\dot{Ci}| \in Cx$,
If W(i)="0" then $|\hat{Ci}| \in Cy$
T2=E[Cx]
T1=E[Cy]
If Cx=Ø then T2=αCmax.
If Cy=Ø then T1=(α-Δα)Cmax

Stage4 Extract watermark
If |Ci|<(T1+T2)/2, then $\dot{W}(i)$="0".
If |Ci|>(T1+T2)/2, then $\hat{W}(i)$="1".

Stage5 If i<N×3 then α=α-Δα read next Δα. go to stage3.

Stage6 Vote among extracted watermarks.

When the detector just need to select a correct watermark among other watermarks. We suggest the distance between T1 and T2 is a efficient measure to distinguish from other random sequences instead of using similarity measurement.

$D = \sum_{i=0}^{k} sign(T2_i - T1_i)(T2_i^2 - T1_i^2)$,k is the number of iteration from step5 to step3.
The experimental results are evaluated in section 6.

4. Watermark method for Binary Image

We introduce to embed a binary image as a watermark. Generally speaking, a watermark image need much more bits to represent than any other information data.(e.g. random sequence) and have higher spatial correlation. So we introduce the method to reduce bits for the watermark image and extracting significant components which are relative to HVS (Human Visual System). Significant components are given higher priority than other components. Also the more significant components are embedded at more robust coefficients to attack. Stages for extracting significant components of a binary image and embedding are as follows:

Stage1 Set X ,Y half of Row and Column size of the binary image.

Stage2 Divide watermark image to sub-blocks $X \times Y$ and search included bits, "0" or '1'
If all components of $X \times Y$ sub-block is '0',W(k)=0
If all components of $X \times Y$ sub-block is '1',W(k)=1

Stage3 If X and Y are not 1, X=X/ 2, Y=Y/2 go to step2.

Stage4 The same embedding stages in section 3.1.

During this procedure, ahead watermarks can have the information of larger spatial domain (e.g. X and Y =8 and W(k)="1" means all of corresponding 8×8 area are filled with "1" and can reduce bits 64:1). In section 3, we set Δα increasing, as coefficients are closed to Cmax, so we can say that significant bits are embedded in the robust area of the image. Extracting stages are:

Stage1 Read saved binary image and get W(k).

Stage2 Extract W'(k) after following steps in section 3.2 with W(k).

Stage3 Reconstructing the binary image with W'(k).

5. Experimental Implementation

In order to evaluate the proposed digital watermark, we applied to the 8bits/pixel 256×256 image "Lena" and "camman". We randomly generate 100 bits and use two 64×64 binary images as the watermarks. For the information data embedding, Δα=0.05 from α=0.05 to α=0.2, Δα=0.1 from α=0.2 to α=0.6, Δα=0.2 from α=0.6 to α=1.0 are applied. Table (1) shows decomposition results of watermark image.

Figure 1: Original Images "Lena" and "Camman" (256×256).

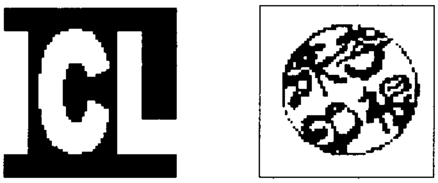

Figure 2: Original binary Watermark Images "ICL" and "stamp" (64×64).

Table 1. Decomposition of tested watermark image "ICL" and "Stamp"

Sub-block size	ICL	Stamp
32×32	0	0
16×16	0	0
8×8	24	22
4×4	72	43
2×2	234	256
1×1	472	976
Total bits	802	1297
Reduction ratio	5:1	3:1

6.1 Uniqueness of watermark

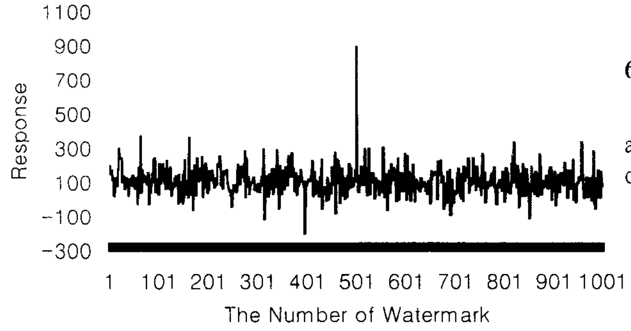

Figure 3: Watermark detector response to 1000randomly generated watermark. Only one watermark(500th) matches.

Figure (3) shows the response of the watermark detector to 1000 randomly generated watermarks. The 500th watermark is the only correct watermark. Figure (4) shows the response of the watermark detector after low pass filtering the watermarked image. Also we can recognize that the 500th watermark is the correct watermark.

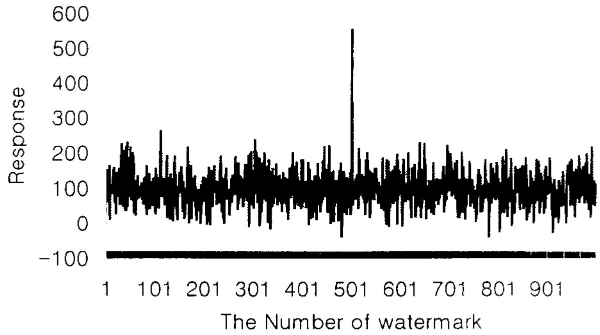

Figure 4: Watermark detector response after low pass filtering.

6.2 Robustness against JPEG compression

Figure (5) shows the rate of the detection error of the embedded data. The watermarked image are compressed with JPEG from quality Q=[100%] to [1%]. The error rate is zero when JPEG compression quality is over 30%.

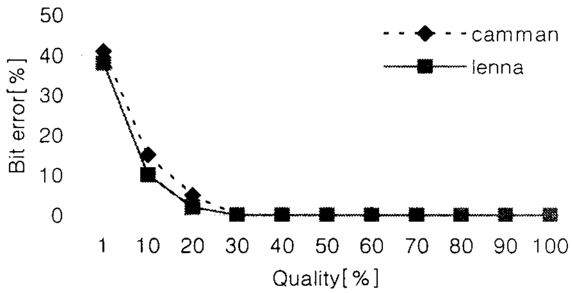

Figure 5: Compression with JPEG

6.3 Robustness against Image Scaling

Figure (6) shows extracted binary watermark image after the watermarked image was scaled to quarter of its original size and re-scaled to its original dimensions.

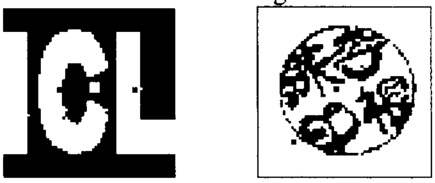

Figure 6: Extracted ICL(98.77%) image and Stamp(99.26%) image after re-scaling

4046 bits of total 4096 bits is correctly extracted for "ICL" watermark image and 4066 bits of 4096 bits for

"Stamp" watermark.

6.3 The Robustness against Image cropping

Figure (7a) shows a cropped version of the original image of figure (1). The missing part of the image is replaced with portions from the watermarked image, in which the "stamp" watermark image is embedded. In this case 88% of original stamp image can be extracted.

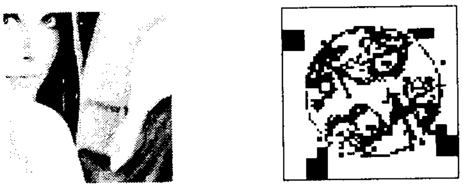

Figure 7(a): Cropped version 7(b): extracted "stamp"

6.4 The Robustness against Filtering

Figure (8) and Figure (9) show a low pass and high pass versions of "Lena" and "camman" respectively. The extracted images tell the suggested algorithm is robust to common filtering distortion. More than 98% of original watermark images are extracted.

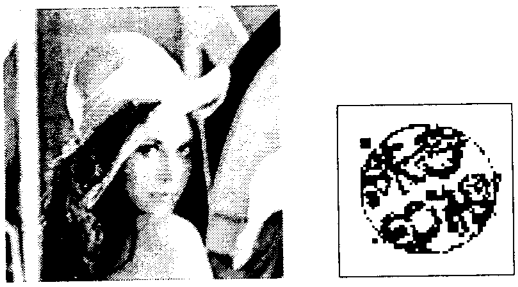

Figure 8: Low pass filtered version of watermarked image "Lena" and extracted watermark image "stamp".

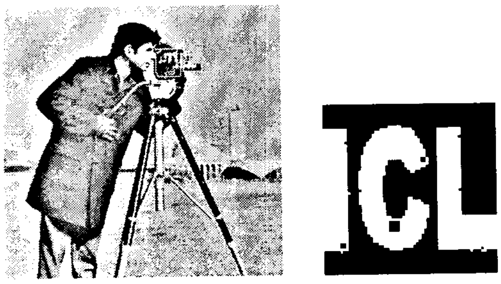

Figure9: High pass Filtered version of watermarked image "Camman" and extracted watermark image "ICL".

6.6 Robustness against Watermarking Watermarked images

While repeatedly embedding different watermark to an image the image degradation can occur, so this can be another form of attack. Figure (10) shows the response of detector to 1000 randomly generated watermarks. Three spikes indicate the presence of three watermarks.

7. Conclusions

We introduced a watermarking method which was based on wavelet transform. This method can adjust thresholds for distorted coefficients at a detector. As a result, it is robust to most common image processing. It doesn't need original image in order to detect the watermark. It was demonstrated that the proposed algorithm provided good robustness under various attacks and indicated a correct watermark among incorrect watermarks with distorted image.

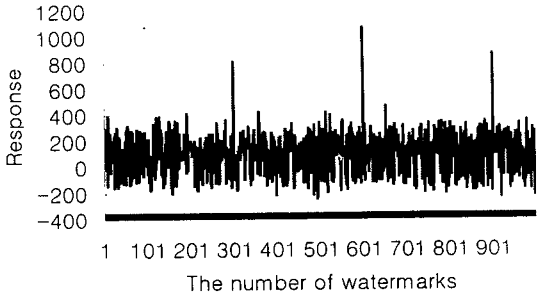

Figure 10: Watermark detector response to 1000 randomly generated watermarks after three successive watermarking operations.

References

[1] Mitchell D. Swanson, Mei Kobayashi, Ahmed H. Tewfik, "Multimedia Data_Embedding and watermarking Technologies", Proc. IEEE Trans. Image processing, Vol 86,pp1064-1087, June 1998.

[2] G. Voyatzis, I. Pitas, "Embedding Robust Watermarks by Chaotic Mixing", Proc. DSP'97, Satorini, Greece, Vol.2, pp.1121-1124, June 1997.

[3] I. J. Cox, J. Kilan, F. T. Leighton and T. Shannon, "Secure spread spectrum watermarking for multimedia", IEEE Trans. Image Processing. Vol 6. no. 12. pp. 1673-1687 1997.

[4] M. Barni, F. Bartolini, V. Cappellini, A. Lippi, A. Piva, "DWT-based technique for spatio-frequency masking of digital signatures", Proc. SPIE'99 California, USA, pp.31-39, January 1999.

[5] Xiang-Gen Xia, Charles G. Boncelet, Gonzalo R, Arce, "Wavelet transform based watermark for digital images", Proc. OCIS'98, Vol.3, pp.497-511, November 1998.

[6] Houng-Jyh Mike Wang, Po-Chi Su, C.-C. Jay Kuo, "Wavelet-based digital image watermarking", Proc. OCIS'98, Vol.3, pp.491-496, November 1998.

[7] H. Inoue, A. Miyajaki, A. Yamamoto, T. Katsura, "A Digital Watermark Technique Based on the wavelet Transform and Its Robustness on Image Compression and Transformation", Proc. IEICE. Trans. Funadamentals, Vol.E82-A, pp.2-10, January 1999.