Watermark Extraction
by Magnifying Noise and Applying Global Minimum Decoder

Zhigeng Pan[a,b], Li Li[b], Mingmin Zhang[a], and David Zhang[c]
[a]*State Key Lab of CAD&CG, zhejiang University, Hangzhou, 310027*
[b]*Hangzhou Dianzi University,Hangzhou 310018, P.R.China*
[c]*Center for Multimedia Signal Processing and Department of Computing,Hong Kong Polytechnic University, Kowloon, Hong Kong*
(E-mail: lili@cad.zju.edu.cn)

Abstract

For the classical watermark embedment model $I = I + \alpha W$, the corresponding watermark detection has its limitation in its need of a fixed parameter for extracting watermarks. If the extraction parameter is too large, we cannot extract the watermark from the image that contains watermarks; if it is too small, the extracted watermarks may be blurred. This paper proposes a novel watermark extraction method. First, we treat the watermark information as noise for the watermarked image in its spatial domain. We then magnify the noise before detection. Next, we recover the watermark information by adjusting the extracted data from the frequency domain according to our global minimum method. Experimental results show that our watermark extraction method is more valid and accurate than the classical method. It can greatly reduce extraction errors.

1. Introduction

Using computer networks to transmit digital multimedia content is undoubtedly a feasible and economical way. However, transmitting information on computer networks is not secure at all – valuable data can be easily stolen during transmission. Hence, information security has become a critical issue in the digital world. As a result, many digital watermarking systems have been proposed for protecting a wide array of multimedia contents, such as text, image, graphics, video and audio, etc [1-4].

Research on the relationship between watermark embedment and the robustness of watermarking algorithms has obtained fruitful results [5-8].

There are also some research results on watermark detection when watermarks are pseudo random sequences [9-11].

It is interesting to note that there are relatively few papers that discuss about watermark extraction when watermarks are meaningful characters or images. Therefore, we present a novel watermark extraction method for a blind watermarking algorithm based on the frequency domain in this paper. First, we treat watermark information as noise for the watermarked image. We then magnify the noise before extracting the watermark. Next, an approximation of the original image is obtained by smoothing the watermarked image. A comparison between the watermarked image and the smoothed one is performed, where we obtained the watermark noise. The watermark noise is magnified before extracting. Then, we obtain the corresponding watermark information in the frequency domain and adjust them according to our principle of global minimum, which is related to watermark encoding. Finally, we present a new method to decide whether the watermark is true or false. Experimental results show that our watermark extraction is effective and accurate enough to decrease extraction errors.

2. Conventional watermark extraction

Generally, when watermarks are meaningful characters or images, watermark embedment can be classified into the following three models (except for the quantization method)

$$v_i^{'} = v_i + \alpha w_i, \alpha >> v_i \qquad (1)$$

Proceedings of the Third International Conference on Image and Graphics (ICIG'04)
0-7695-2244-0/04 $20.00 © 2004 **IEEE**

$$v_i^{'} = v_i(1+\alpha w_i) \quad (2)$$

$$v_i^{'} = v_i e^{\alpha w_i} \quad (3)$$

where v_i denotes the frequency domain of the original image, $v_i^{'}$ denotes the frequency domain of the watermarked image, w_i denotes watermark information after being encoded to consist of digital "*0*" and digital "*1*", and α denotes the strength parameter that is decided by the user. The corresponding watermark extraction is usually taken as in (4).

$$\begin{cases} w_i = 1, & v_i^{'} \geq \beta \\ w_i = 0, & otherwise. \end{cases} \quad (4)$$

where β denotes the extraction parameter that is usually the same to the strength parameter α.

However, it is difficult to find an extraction parameter that is suitable for any watermarked image since the watermarked image needs different extraction parameters to get a high quality recovered watermark image when it is attacked.

3. Our method in detail

3.1 Watermark extraction

In this paper, we smoothed the watermarked image A and get a new approximated image A^* by a de-noising method. Then, A minus A^* is considered as noise, where the watermark information is contained. Finally, we magnify the noise and add it to A^* and get a new image $\tilde{A}$, which is treated as the new watermarked image to be detected. The details will be discussed in following sections.

(a). Approximation by denoising the watermarked image

Suppose B is the corresponding frequency domain of the watermarked image A, we smooth some middle spectrum coefficients of B and obtained B^*. A^* is the corresponding spatial domain of B^*.

(b). Magnify the noise of watermark

We can get the new watermarked image $\tilde{A}$ by

$$\tilde{A} = A^* + (A - A^*) * \gamma \quad (8)$$

where γ is the magnifying weight.

3.2 Global minimum method for recovering watermarks

We propose a new method to extract the watermark without using an extraction parameter, thus avoiding the extraction parameter problem mentioned above. In this paper, watermarks are 64*64 binary images, the total number of 0 is *k* and the total number of 1 is (4,096-*k*). When the watermark information sequence *M* is extracted, find *k* minimum in the sequence *M* and turn them into *0*. Then, make others into *1* and get the recovered watermark information, where *k* can be regarded as one part of the key.

4. Algorithm design

Our blind digital watermarking algorithm is based on the FFT frequency domain. The original image is a color image with the size of 512*512. The watermark image is a binary image with the size of 64*64.

4.1 Embedding watermarks

Take the Fourier Transform of the RGB components of the original color image *I*, with a size of 512*512. Then, get the Fourier magnitude matrixes A_i and the angle matrix Z_i (i=1,2,3). If the size of the original color image is larger than 512*512, we only select one part of it with size of 512*512. The watermark image is binary and every pixel is *0* or *1*. We take every pixel of the watermark image and get a sequence of *0* and *1*. The sequence is divided into three groups and we can get B_i ($i = 1,2,3$). The total *0* in B_i is C_i ($i = 1,2,3$). C_i is regarded as the key. The following two steps describe the details of embedding the watermark image.

Step 1: Embed B_i into some fixed positions of A_i and get D_i ($i = 1,2,3$). The watermark embedment is taken as (9)

$$v_j^{'} = v_j + \alpha w_j, \alpha >> v_j \quad (9)$$

where $w_j \in B_i$, w_j =0 or 1, v_j is chosen data

from A_i ($i = 1,2,3$). The strength parameter $\alpha = 12000$.

Step2: Inverse the FFT transform to D_i (angle matrix is Z_i) and get $\tilde{A}_i$, which is the RGB components of the watermarked image. So, we get the watermarked image I_W^*.

4.2 Extracting watermarks

Step 1: Take the RGB components of the watermarked image I_W and get A_i, magnify the noise of A_i and get $\tilde{A}_i$ using the method mentioned in Section 2.1, where γ=30.

Step 2: Make the Fourier Transform of $\tilde{A}_i$ and get B_i ($i = 1,2,3$). Find watermark information from the corresponding positions of B_i and get the sequence E_i ($i = 1,2,3$). According to the key, turn the C_i minimum of E_i into digital "*0*" and turn others into digital "*1*" and get sequence F_i ($i = 1,2,3$).

Step 3: Let $F = \{F_i\}$ ($i = 1,2,3$). Turn F into 64*64 blocks and get the recovered watermark image $\tilde{W}$.

Step 4: Compute the correlation data r between the original watermark image *A* and the recovered watermark image *B*. If r is above 0.6, we can conclude that the watermark image and the recovered watermark image are basically coherent.

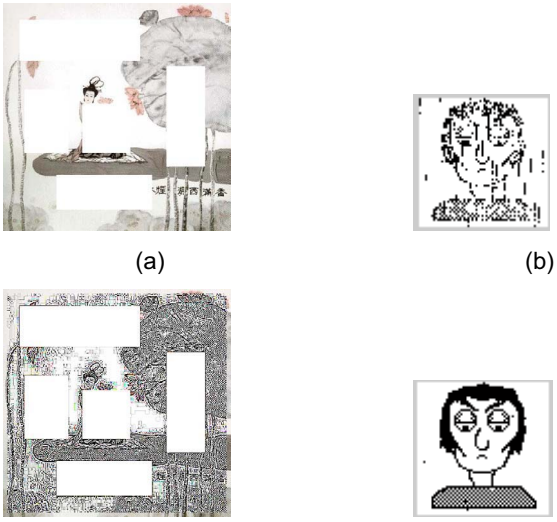
5. Experimental results

We have performed different attacks in our experiment. The attacks include cutting, erasing, adding noise, modifying color, modifying, translation, filtering and template attacks.

Fig.1 shows the original image and the watermark image. Figs. 2-3 show the comparative results obtained by general watermark extraction and our watermark extraction. It is obvious that our method can greatly reduce extraction errors. Table I gives some comparative parameters for the recovered watermark images using the two extraction methods. Two decision parameters are also given in Table 1, which gives comparative results for the recovered watermark images using the two extraction methods. R1 are the correlation data between the extracted watermark images that are obtained by the classical method and the original watermark image. R2 are the correlation data between the extracted watermark images that are obtained by our method and the original watermark image.. Experimental results prove that our watermark extraction can enhance the accuracy of extracting watermark.

(a) (b)

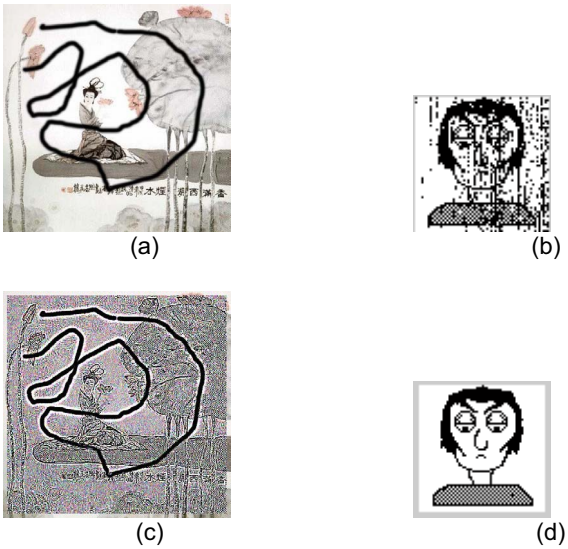
Fig.1. The testing images used in our experiments. (a) The original image; (b) The watermark image.



(a) (b)

(c) (d)

Fig. 2. Attacked I: cutting the watermarked image. (a) Watermarked image; (b) Result of classical method; (c) Magnify the noise; (d) Result of our method.



(a) (b) (c) (d)

Fig. 3. Attacked I: cutting the watermarked image. (a) Watermarked image; (b) Result of classical method; (c) Magnify the noise; (d) Result of our method.

Table1. Comparative results for the recovered watermark images using the two extraction methods

Attacks	PSNR	R1	R2
Attack 1 (cut)	23.3543	0.6381	0.8632
Attack II (erase)	17.7225	0.7957	0..9018
Attack III (translation)	16.5472	0.0732	0.5922
Attack IV (color modified)	14.9994	0.3054	0.7307
Attack V (jitter)	19.0204	0.5739	0.6739
Attack VI (uniform noise 5%)	37.3474	0.5965	0.5025
Attack VII (middle filter of window [3x3])	34.46773	0.0001	0.4462
Attack VIII (middle filter of window [5x5])	30.4940	0.0001	0.3889
Attack IX (template attack)	30.3332	0.1451	0.4651

Acknowledgement

This research is co-supported by Natinoa Natural Science Foundation and the Excellebt Young Teacher Program of MOE, PRC.

References

[1] J. Cox, J. Killian, F.T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia", *IEEE Trans. on Image Processing*, vol. 6, no. 12, 1997, pp. 1673-1687.

[2] L. Li, Z. Pan, S. Sun and X. Wu, "A private and lossless digital image watermarking system", *Second International Conference on Image and Graphics*, SPIE Publisher, 2002, pp. 365-370.

[3] L. Me and G.R. Arce, "A class of authentication digital watermarks for secure multimedia communication", *IEEE Transactions on Image Processing*, vol. 10, no. 11, 2001, pp. 1754 –1764.

[4] Y. Wang, J.F. Doherty, and R.E. Van Dyck, "A wavelet-based watermarking algorithm for ownership verification of digital images", *IEEE Transactions on Image Processing*, vol. 11, no. 2, 2002, pp. 77 –88.

[5] J.R. Hernandez, M. Amado, and F. Perez-Gonzalez, "DCT-domain watermarking techniques for still images: detector performance analysis and a new structure", *IEEE Transactions on Image Processing*, vol. 9, no. 1, 2000, pp. 55 –68.

[6] M. Tsai, K. Yu, and Y. Chen, "Joint wavelet and spatial transformation for digital watermarking", *IEEE Trans. on Consumer Electronics*, vol. 46, no. 11, 2000, pp. 241-245.

[7] J.J.K. O'Ruanaidh and T.Pun, "Rotation, translation and scale invariant sprectrum digital image watermarking", *Signal Processing, Special Issue on Copyright Protection and Control*, vol. 66, no. 3, 1998, pp. 303-317.

[8] C. Lin, M. Wu, J. A. Bloom, I. J.Cox, M. L. Miller, and Y. M.. Lui, "Rotation, scale, and translation resilient public watermarking for images", *IEEE Transactions on Image Processing*, vol. 10, no. 5, 2001, pp. 755-766.

[9] G. Depovere, T. Kalker, and J.P.M.G. Linnartz, "Improved watermark detection reliability using filtering before correlation", *Proceedings of the International Conference on Image Processing*, IEEE Signal Processing Society, Chicago, Illinois, USA, Oct. 1998, pp. 430-434.

[10] B. Chen, S. Cheng, and C. Sen, "A new algorithm for blind image watermark detection", *Chinese Journal of Computers*, vol. 24, no, 12, 2001, pp. 1179-1285.

[11] M. Barni, F. Bartolini, A. De Rosa and A. Piva, "A new decoder for the optimum recovery of non-additive watermarks", *IEEE Transactions on Image Processing*, vol. 10, no. 5, 2001, pp. 755-766.