DCT-domain Watermarking Scheme Based on Majority Voting Criterion

Shen-Chuan Tai, Chuen-Ching Wang and Chong-Shou Yu
Institute of Electrical Engineering
National Cheng Kung University
Tainan, Taiwan, R.O.C
Email:sctai@mail.ncku.edu.tw

ABSTRACT

A robust watermarking strategy for copyright protection is proposed as a way that embeds multiple copyright information in a selected set of DCT coefficients. During watermark extraction, we introduce the majority voting scheme that can render more reliable watermark detection compared to some conventional image watermarking approaches. The proposed method can directly extract the embedded watermark from the watermarked image without using the original image, so it is feasible to implement it in a real time system. To further adaptively accommodate the characteristics of different images, the proposed algorithm uses an adaptive watermark strength factor (S) to strike a good balance between robustness and perceptual invisibility. Furthermore, the proposed algorithm can solve the problem inherent in traditional watermark systems: the security will degrade due to the publication of watermark algorithm. Experimental results demonstrate that the watermark is robust to most of the signal processing operations and geometric distortions. It can be found that detection capability, imperceptibility, and robustness of the watermarking technique can be guaranteed.

1. Introduction

The rapid development of digital information technology, combined with the simplicity of duplication and distribution of digital data across communication networks, has given rise to a real challenge of how to protect their electronic data for most content providers. Although cryptography is an effective tool against the illegal digital distribution problem, it is not only costly on computation and complexity but would also reduce the marketing possibilities for the service provider. One potential solution for claiming the ownership of these data is watermarking technique [1-14] that is a process of embedding information directly into the multimedia data by making small modification to them. The watermarks can be divided into either perceptually visible or invisible watermark. Visible watermarks can be used to discourage the illegal replication immediately. In most case, invisible watermark scheme is chosen to claim the ownership of still media data. For more information about visible watermarks, refer [2]. In this paper we focus on invisible watermark. In general, watermark schemes can be classified into two categories: spatial domain-based watermarking and frequency domain-based watermarking. A simple way of spatial domain-based watermarking scheme is that embeds some secret data into the least significant bits (LSB) of the image. However, this method is not robust to common image processing operation: the LSB will be easily altered and the secret data will be lost. Especially, the spatial domain watermark schemes are also unreliable to cropping attack. Watermark schemes based on frequency domain-based is more robust because all the secret data can spread the spectrum energy to everywhere of the media data and thus it is difficult to remove. However, the watermark can be extracted by comparing the watermarked image and original non-watermarked one in the ownership of verification process. Generally, a good watermark scheme must meet the following features:

- Robustness - The watermark system must be robust to common signal processing operations.
- Security - The watermark system must be able to resolve rightful ownership problem and survive known-algorithm attacks.
- Invisibility - The watermarked media data should retain its quality.

In this paper, we will concentrate on designing a digital watermarking scheme with a best tradeoff between perceptual invisibility and robustness to signal processing operation. To concern the requirement of security, the proposed watermark scheme is devised to extract the watermark bits without access to the original image. This will reduce the complexity of the watermarking system and avoid the original image to appear on anyone who wants to check the presence of the watermark.

The rest of the paper is organized as follows. The proposed algorithm is presented in section 2, and its simulation results are given in section 3. Finally, the conclusion and future research will be discussed in section 4.

2. The Proposed Watermark System

2.1 The Proposed Watermark Embedding

Referring Fig. 1, the algorithm of watermark embedding is first to transform the original image ***H*** into frequency domain by using full frame DCT. As the conventional JPEG process, the DCT coefficients are reordered into a zigzag scan. To achieve a good balance between robustness and invisibility, it is need for choosing a middle frequency band in order to embed the watermark information. In addition, to improve the security, the user key K_S in Fig. 1 is used for generating the pseudo random number to select which coefficients will be embedded the copyright information. Due to the secret key keeping in the owner, it is difficult for a hacker to remove or detect the watermark information in absence of K_S. Indeed, the security of a crypto-system resides in the secret key, but not resides in the cryptographic algorithm. On the other hand, the adaptive watermark strength factor *s*, obtained from the absolute mean value of coefficients in the middle band, is used to accommodate the image quality for different images. According to the *s*, a watermark bit can be embedded into the specific coefficient by the following rule.

1. If the embedded information bit is *"0"*, and the corresponding coefficient is *larger* than zero, then a random real number between -0.5*s* and -1.5*s* is generated to substitute the specific coefficient.

2. If the embedded information bit is *"1"*, and the corresponding coefficient is *smaller* than zero, then a random real number between 0.5*s* and 1.5*s* is generated to substitute the specific coefficient.

Finally, performing inverse DCT on the modified coefficients can generate the watermarked image H_W. After the embedding phase, for each information bit that is a zero, its corresponding coefficient is now a negative real number, and for each information bit that is a one, its corresponding coefficient is now a positive real number. This makes watermark detection quite easy, and also cannot be attacked by statistical analysis.

Assuming the original image ***H*** is size of $N1 \times N2$ and the *X* duplicate copyright information *W* is at length of *L* bits. Each bit of *W* is denoted as *W*(*l*), where $0 \leqq l < L$ and $W(l) = \{0, 1\}$. The user secret key is denoted as K_S. If we want to embed *the* copyright information into ***H***, then the algorithm of watermark embedding can be briefly expressed as follows.

<u>Step 1.</u> *Transform an $N1 \times N2$ image **H** to frequency domain by $N1 \times N2$ DCT; the DCT coefficients then are reordered into a zigzag scan* $C(n) = \{T_1, T_2, \cdots T_l, T_{l+1}, \cdots T_{l+m}, T_{l+m+1}, \cdots T_{N1\times N2}\}$ *, where $1 \leqq n < (N1 \times N2)$.*

<u>Step 2.</u> *Select a middle band* $M = \{T_{l+1}, T_{l+2}, \ldots T_{l+m}\}$ *and calculate adaptive watermark strength factor*

$$S = \frac{\sum_{k=l+1}^{l+m} |T_k|}{m},$$

<u>Step 3.</u> *Duplicate the watermark,* $W = \{w_1, w_2, \cdots w_L\}$, *into an X- copies version as follows.*

$$W' = \{\overbrace{w_1, w_1 \cdots w_1}^{X},\ \overbrace{w_2, w_2 \cdots w_2}^{X},\ \overbrace{\cdots, w_L, w_L \cdots w_L}^{X}\}$$

<u>Step 4.</u> *According to the seed of pseudo random number generator K_S, generate a random number list R(r); where $0 \leqq r < XL$ and $l+1 \leqq R(r) \leqq l+m$; $R(r) \neq R(q)$ for each $r \neq q$.*

<u>Step 5.</u> *For $0 \leqq r < XL$, embed W' into middle band M by modifying the specific coefficient value as the following rule:*

$$T'_{R(r)} = \begin{cases} +\alpha S, & \text{if } W'(r) = 1 \text{ and } T_{R(r)} < 0 \\ -\alpha S, & \text{if } W'(r) = 1 \text{ and } T_{R(r)} > 0 \\ T_{R(r)} & \text{otherwise} \end{cases}$$

where α is a random real number between 0.5~1.5.

<u>Step 6.</u> *Restore modified middle band to zigzag scan and form as* $C'(n) = \{T_1, T_2, \cdots T_l, T'_{l+1}, T'_{l+2} \cdots T'_{l+m}, T_{l+m+1}, \cdots T_{N1\times N2}\}$, *where $1 \leqq n < (N1 \times N2)$.*

<u>Step 7.</u> *Perform inverse DCT to form watermarked image H_W.*

2.2 Watermark Detection

The block-diagram of watermark detection shown in Fig. 2 is used to verify the ownership of a watermarked image. Because the watermark is embedded in the frequency domain, the full frame DCT is necessary to be performed first. A zigzag scan is performed to form a 1-D coefficient sequence. The owner's user key K_S is then used here to generate the coefficient selection list. Same as watermark embedding, the pseudo random number generator is used here to reproduce the same list. From the list, the addresses of coefficients that embedded with watermark could be found and the data can be extracted. The extracted coefficients will be converted into binary data: all positive coefficients will be converted into '1' and all negative ones will be converted into '0'. These converted data is so-called *extracted raw information.*

The extracted raw information, in fact, is from many copies of the secret information W during watermark embedding. Therefore, we propose the majority voting technique to recover the raw information into reconstructed *copyright information.*

Assuming the image $\boldsymbol{H_W}$ is at size $N1 \times N2$, and the secret key is $\boldsymbol{K_S}$. If the owner wants to verify the ownership of the image, the process of watermark extraction can be summarized as follows:

<u>Step 1.</u> *Transform an $N1 \times N2$ image $\boldsymbol{H_W}$ to frequency domain by $N1 \times N2$ DCT; the DCT coefficients then are reordered into a zigzag scan* $C'(n) = \{T_1, T_2, \cdots T_l, T'_{l+1}, T'_{l+2} \cdots T'_{l+m}, T_{l+m+1}, \cdots T_{N1\times N2}\}$, *where $1 \leqq n < (N1 \times N2)$.*

<u>Step 2.</u> *According to the seed of pseudo random number generator $\boldsymbol{K_S}$,generate a random number list $R\ (r)$;* *where $0 \leqq r < XL$ and $l+1 \leqq R\ (r) \leqq l+m$; $R\ (r) \neq R\ (q)$ for each $r \neq q$.*

<u>Step 3.</u> *Generate extracted raw information by the definition:*

$$W''(r) = \begin{cases} 1, & if \quad T'_{R(r)} > 0 \\ 0, & if \quad T'_{R(r)} < 0 \end{cases}; \qquad 0 \leqq r < XL.$$

<u>Step 4.</u> *Perform majority voting and obtain a result: $V(m) = W''(m \times X) + W''(m \times X+1) + \ldots + W''(m \times X+X-1)$, where $0 \leqq m < L$.*

<u>Step 5.</u> *Generate reconstructed copyright information* $\hat{W}(m)$;

$$\hat{W}(m) = \begin{cases} 1, & if\ V(m) > X/2 \\ 0, & if\ V(m) < X/2 \end{cases};$$

$0 \leqq m < L$

The proposed algorithm uses seven copies of secret information for majority voting. The more copies used for the majority voting the more error distortion will be corrected. The relationship between the amount of duplicated secret information copies and the error rate is shown in Fig. 3.

After some experiments, seven copies are chosen under the consideration of balance between error correction and coefficients amount. This is not always optimal, and the number of copies of copyright information is suggested an adjustable parameter of the proposed watermarking system.

3. Simulation Results

The proposed watermark system was simulated and applied on several gray level images for performance evaluation. All the tested gray level images $\boldsymbol{H}$ are at the resolution of 512 x512 with 8 bits per pixel. The length of user secret key and the copyright information are 64 bits and 256 bits respectively. Seven copies of copyright information, 1792 bits, are embedded into the host image for majority voting. The middle band was selected for embedding the copyright information from 27000th to 39060th coefficients after zigzag scan.

The quality of the watermarked image is evaluated by the peak signal-to-noise ratio (PSNR), which is defined as

$$PSNR = \log_{10}\left(\frac{255^2}{\frac{1}{m^2}\sum_{i=1}^{m}\sum_{j=1}^{m}(x_{ij}-x_{ij}')^2}\right) \quad \text{for an } m{\times}m \text{ image.}$$

Note that the X_{ij} and X_{ij}' denote the gray levels of pixel from original and watermarked image respectively.

The accuracy rate is defined as $(X_C/X_{TOTAL}) \times 100\%$, where X_C denotes the number of hit after being attacked and X_{TOTAL} denotes the total bits of copyright information.

The experiments of watermarked images are shown in Figs. 4, 5 and 6. It can be found that the proposed watermarking system retains the image quality after hiding the copyright information. Fig. 7 shows that the watermarked images are attacked by image cropping operation and JPEG compression. The result is shown in Table 1. The relationship between the JPEG compression ratio and watermark detection accuracy is shown in Fig. 8. Also, the relationship between the cropped size and watermark detection accuracy is shown in Fig. 9.

The watermarked images attacked by image rescaling operation are shown in Fig. 10. The example of images that attacked by sharpen filters, low-pass filters, and image-rotation are shown in Fig. 11.

The simulation results show that the multiple watermark strategy provides significant improvement on watermark robustness. Traditional watermark schemes lose their ability on certification when the watermarked images are compressed by JPEG with 10 or higher compression ratio, while the proposed algorithm can withstand the JPEG compression at CR=18. Furthermore, in this paper the watermarked images can preserve their high quality without noticeable noise.

4. Conclusion

In this paper, a highly robust watermark system is proposed. The necessary watermark requirements are considered and implemented, and the parameter of the proposed watermark system is chosen by experiments. The proposed watermark system can resist some image-processing operations, such as JPEG lossy compression, cropping, image re-sampling and image rotating.

The security problem about rightful ownership is also solved with the authorized copyright information. Due to using the secret key for embedding the copyright information, it is very difficult for a pirate to detect or remove the embedded information. The experimental results show that the proposed algorithm reaches 40dB or higher for nature images. The image quality is still good enough that the human eyes cannot sense the difference. With the achievements of robustness, security and invisibility, the proposed algorithm can meet all the requirements of the watermark system.

However, some attacks are still challenge to the proposed algorithm, such as StirMark [7], random rows/columns removal, print-scan and median filter. We will resolve these problems as our major direction in the future. Finally, the definition of middle band should be adjusted adaptively for different images and user's demand.

References

[1] Cox, I. J.; Kilian, J.; Leighton, F.T.; Shamoon, T., "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, Volume: 6 12, pp.1673-1687, Dec. 1997.

[2] G. W. Braudaway, K. A. Magerlein and F. Mintzer, "Protecting Publicly-available Images with a Visible Image Watermark," In *the Proc. of SPIE,* vol. 2659,1996, pp.126-133.

[3] George Voyatzis; Ioannis Pitas, "The use of watermarks in the Protection of Digital Multimedia Products," *Proceedings of the IEEE*, Vol.87, No.7, pp.1192-1207, July 1999.

[4] Wenjun Zeng; Bede Liu, "A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images," *IEEE Transactions on Image Processing*, Volume 8, 12, pp.1534-1548, Nov.1999

[5] Chiou-Ting Hsu and Ja-Ling Wu, "Hidden digital watermarks in images," *IEEE Transactions on Image Processing*, Volume: 8 1, pp. 58-68, Jan. 1999.

[6] Patrick Bas, Jean-Marc Chassery, "Using the fractal code to watermark images," *1998 International Conference on Image Processing*, Vol. 1, pp. 469-473, 1998.

[7] http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/

[8] M. Kutter, F. A. P. Petitcolas, "A fair benchmark for image watermarking systems," *Electronic Imaging '99,* Security and Watermarking of Multimedia Contents, Volume 3657, pp.1-14, Jan. 1999.

[9] Fabien A. P. Petitcolas, Ross J. Anderson, Markus G. Kuhn, "Attacks on copyright marking systems," in *David Aucsmith (Ed), Information Hiding, Second International Workshop*, IH'98, Portland, Oregon, U.S.A., April 15-17, 1998, Proceedings, LNCS 1525, Springer-Verlag, ISBN 3-540-65386-4, pp. 219-239.

[10] Fabien A. P. Petitcolas and Ross J. Anderson, "Evaluation of copyright marking systems," in *proceedings of IEEE Multimedia Systems (ICMCS'99)*, vol. 1, pp. 574-579, 7-11 June 1999, Florence, Italy.

[11] Juan R. Hernandez, Martin Amado and Fernando Perez-Gonzalez. "DCT-domain watermarking techniques for still images: detector performance analysis and a new structure," *IEEE Transactions on Image Processing*, Volume 9 1, pp. 55-68, January 2000.

[12] Neri Merhav, "On random coding error exponents of watermarking systems," *IEEE Transactions on Information theory*, Volume 46, No. 2, pp. 420-430, March 2000.

[13] Craver, S.; Memon, N.; Yeo, B.-L.; Yeung M.M., "Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks and implications," *IEEE Journal on Selected Areas in Communications*, Volume 16 4, pp. 573-586, May 1998.

[14] S. Craver, N. Memon, B. Yeo, and M. Yeung, "Can invisible watermarks resolve rightful ownerships?" in *Proc. IS&T/SPIE Electronic Imaging:Storage and Retrieval of Image and Video Databases*, Feb. 1997, Volume 3022, pp.310-321.

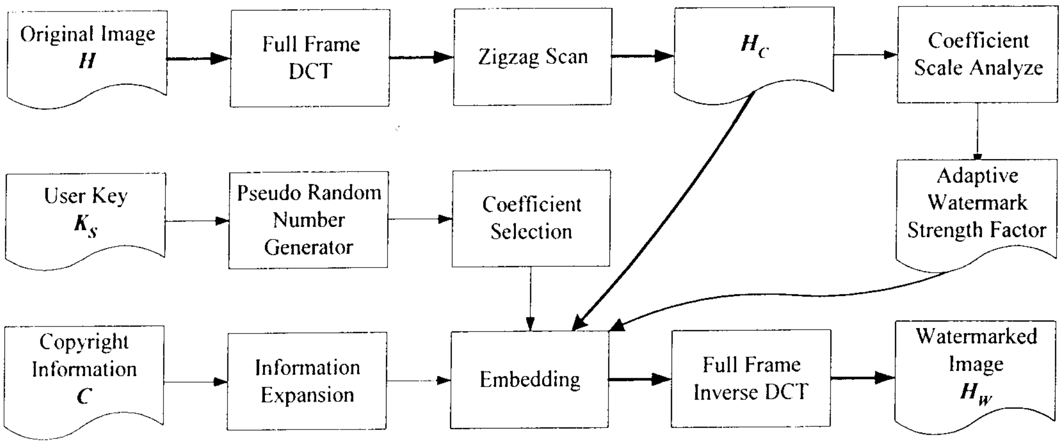


Fig. 1. The block-diagram of watermark embedding

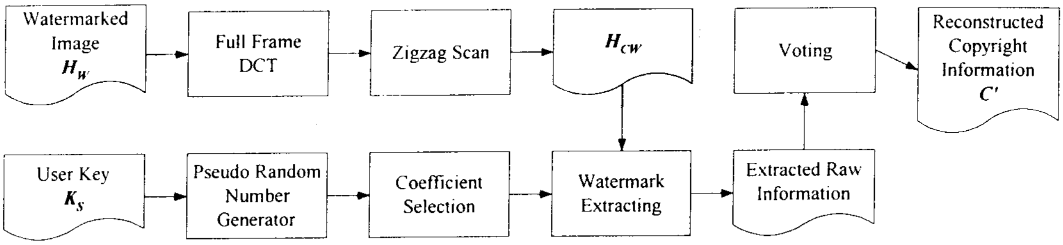


Fig. 2. The block-diagram of watermark detection

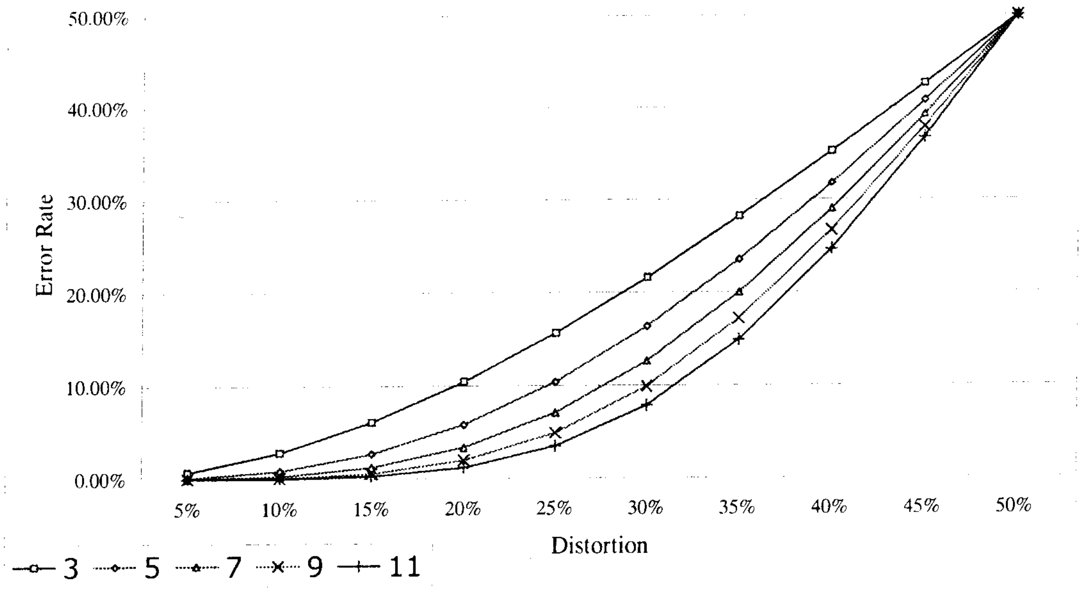


Fig.3. The relationship of distortion and error rate for different votes per information bit.

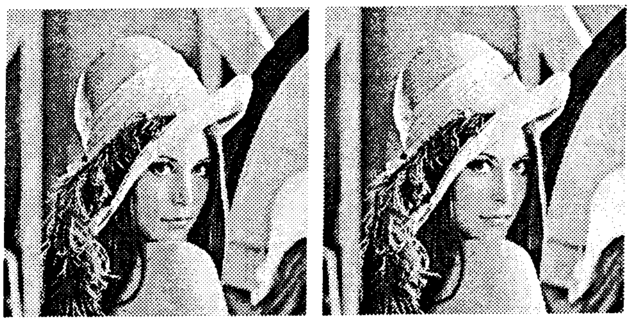


Fig. 4. Original and watermarked image 'Lena', SNR=42.1dB

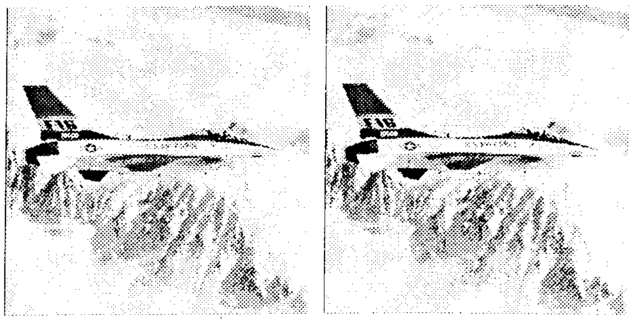


Fig. 5. Original and watermarked image 'F16', SNR=40.67dB

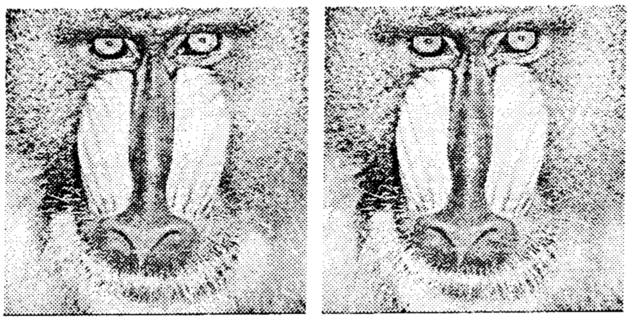
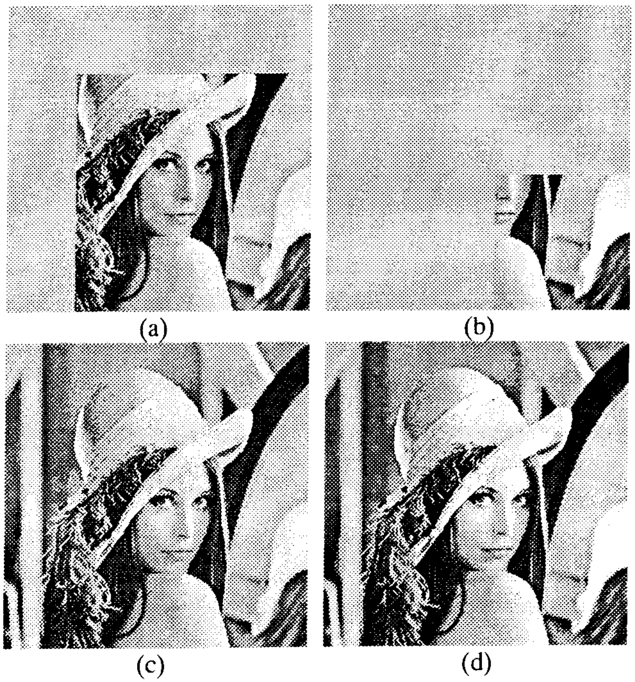


Fig. 6. Original and watermarked image 'Baboo', SNR=35.66dB



(a) (b)

(c) (d)

Fig. 7. Some attacked watermarked image samples:
(a) 40% cropped image;
(b) 80% cropped image;
(c) Watermarked image without attack;
(d) JPEG compressed at CR=18

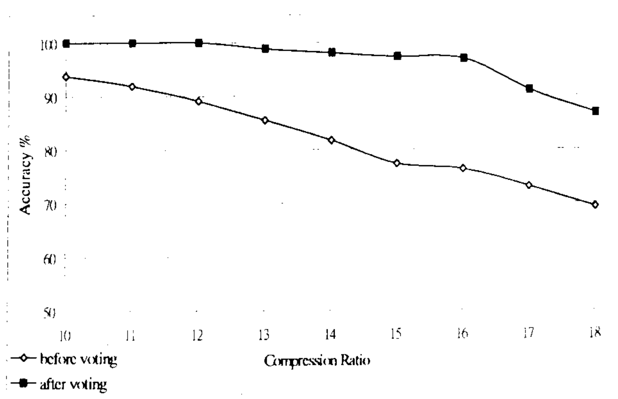


Fig. 8. The relationship between the compression ratio of the watermarked imageand the watermark detection accuracy.

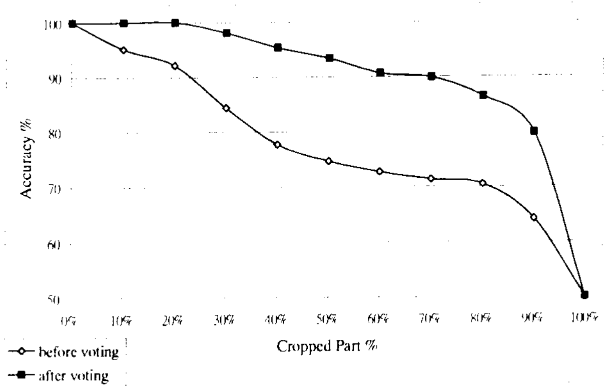


Fig. 9. The relationship between the size of cropped part of the watermarked image and watermark detection accuracy.

(a) (b)

Fig. 10. Resized watermarked images for detection test: (a)from 512x512 to 213x213, and (b) from 512x512 to 750x750

(a) (b)

(c) (d)

Fig. 11. Another example that several watermarked image for detection test:

(a) Rotated 3°clockwise

(b) Sharpened image by using PhotoShop sharpen filter

(c) 3x3 Low-pass masked, $\frac{1}{9}\begin{bmatrix}1 & 1 & 1\\ 1 & 1 & 1\\ 1 & 1 & 1\end{bmatrix}$

(d) 5x5 Low-pass masked, $\frac{1}{25}\begin{bmatrix}1 & 1 & 1 & 1 & 1\\ 1 & 1 & 1 & 1 & 1\\ 1 & 1 & 1 & 1 & 1\\ 1 & 1 & 1 & 1 & 1\\ 1 & 1 & 1 & 1 & 1\end{bmatrix}$

Table 1. The detection rate of copyright information of watermarked image 'Lena' after common image processing attacks.

Compress Ratio	8x8 JPEG quality factor	Accuracy % before voting	Accuracy % after voting
18	24	69.20	86.72
17	26	72.99	91.02
16	28	76.23	96.88
15	30	77.29	97.27
14	33	81.64	98.05
13	37	85.44	98.83
12	41	89.06	100
11	46	91.91	100
10	52	93.81	100
9	59	95.37	100

Cropped Part	Accuracy % before voting	Accuracy % after voting
10%	95.09	100
20%	92.13	100
30%	84.37	98.05
40%	77.68	95.31
50%	74.67	93.36
60%	72.71	90.62
70%	71.32	89.84
80%	70.42	86.33
90%	64.12	79.69
ALL	50.00	50.00

Table 2. Copyright information detecting result of watermarked image 'Lena' after some image processing operations.

Attack method	Necessary preprocess before watermark detection	Accuracy % before voting	Accuracy % after voting
Resized to 213x213	Restore image size	72.66	89.84
Resized to 750x750	Restore image size	99.16	100
Rotated 3°clockwise	Restore image orientation	94.81	100
Sharpened	(None)	98.66	100
3x3 Low-pass	(None)	99.16	100
5x5 Low-pass	(None)	61.77	73.83