The paper is intended for the Workshop on Cryptology and Information Security.

Title: A copyright protection technique by using hybrid domains

Abstract:

Nowadays, the digital image watermark techniques are still weak for resisting geometric distortions such as rotation, scaling and cropping.

In this paper, robustness against cropping is achieved by the proposed two concepts. Firstly, in spatial domain, the position block is decided by edges that could differentiate the importance on the human visual system. Secondly, the verification block is used to construct the oblivious watermarking system by taking advantage of wavelet transform properties. Meanwhile, some experimental results, including the analysis of importance in different digital images and of the resistance against attacks, are presented as well.

The first Author: Larry Huang(黃亮綜)

Affiliation: Department of Applied Mathematics, National Chung-Hsing University

Postal address: 250 Kuo-Kuang Rd. Taichung, Taiwan 402, R.O.C.

E-mail address: jim789@ms45.hinet.net

Phone/Fax: 886-0919-063-120/886-4-2313-1125

The second author: Jinn-Ke Jan(詹進科)

Affiliation: Department of Applied Mathematics, National Chung-Hsing University

Postal address: 250 Kuo-Kuang Rd. Taichung, Taiwan 402, R.O.C.

E-mail address: jkjan@amath.nchu.edu.tw

Phone/Fax: 886-4-2285-8200/886-4-2287-3028

The contact author: Larry Huang(黃亮綜)

Keywords: image, authentication, copyright, protection, watermark

A Copyright Protection Technique by Using Hybrid Domains

Larry Huang and Jinn-Ke Jan

Department of Applied Mathematics, National Chung-Hsing University,

250 Kuo-Kuang Rd. Taichung, Taiwan 402, Republic of China.

E-mail: jim@cc.ckit.edu.tw

ABSTRACT

Nowadays, the digital image watermark techniques are still weak for resisting geometric distortions such as rotation, scaling and cropping.

In this paper, robustness against cropping is achieved by the proposed two concepts. Firstly, in spatial domain, the position block is decided by edges that could differentiate the importance on the human visual system. Secondly, the verification block is used to construct the oblivious watermarking system by taking advantage of wavelet transform properties. Meanwhile, some experimental results, including the analysis of important areas in different digital images and of the resistance against attacks, are presented as well.

Keywords: image, authentication, copyright, protection, watermark

1. INTRODUCTION

Owing to the extensive growth of digital product, the convenience of duplicating has made the protection of intellectual property rights (IPRs) a big problem. Currently there are many researches of copyright protection going on such as digital image watermark. For many years, digital image watermarking technique has been outlined progressively **[1]**.

Digital image watermark techniques can be categorized on the basis of their distinct features. By considering the transparency the watermarked image has, they are divided to visible **[2]** and invisible **[3]**. On the other hand, they are called blind or oblivious **[4]** according if the extraction of the watermark is based on the original image or not. Moreover, they are classfied by the domains where the watermark is embedded such as spatial **[5]** and transform **[6, 7]** domain.

However, Digital image watermark techniques are still not perfect in practice. The continuing challenge has two parts **[8]**: one how to develop copyright applications that add value to media, and the other how to enhance the robustness against geometric and temporal distortions.

Cropping is one of the most important topics in geometric distortions. The recent research against geometric distortions is weakly resistant to cropping. For example, by the theory of integral transform invariants, the watermark can be resistant to translation, rotation and scaling but not to cropping **[9]**. **[10]** is another example. One effective method is using both patchwork and discrete cosine transformation **[11]**. However, because the method modifies only the portion of original image to embed watermark, the embeded part is likely to differ from the other in perceptual. For this reason, our proposed method chooses the concept of combination **[12]** to maintain the imperceptual property. This is also important to some applications **[13]**. Moreover, our proposed method automates the selection of combination position by human visual theory **[14]** .

In this paper, we begin with the introduction of our motivation and other related researches in Section 1. Then, Section 2 describes the copyright protection technique we propose in detail. Some experimental results, including the ability of the importance analysis and the robustness against attacks, are shown and discussed in Section 3. In Section 4, we make a summary and discussion some future work.

2. PROPOSED HYBRID DOMAIN WATERMARKING SCHEME

Our idea is to choose one important feature from the select range that could be adaptive. Then, we preserve the position block for locating and combine the verification block with the watermark to produce a secret key **[15]**. Meanwhile, the original image is analyzed by human visual theory to decide the important feature. When requiring verification, just the position block and the secret key are needed. Fig. 1 is one practical example of the *Lena* image.

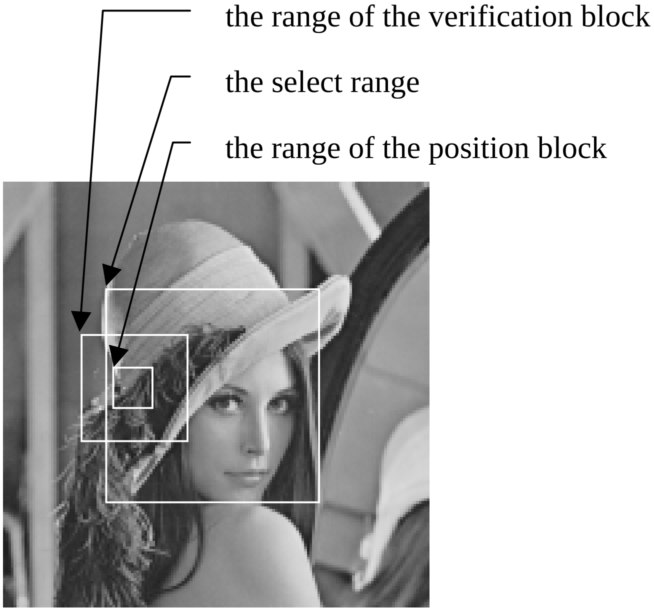

the range of the verification block
the select range
the range of the position block

Fig. 1. The *Lena* image and related ranges.

2.1. The Combination of Watermark and Original Image

This section describes how to combine the watermark with the important feature of the original image so that the watermark could survive after cropping attack.

The original image *O* is defined below.

$$O = \{o_{ij} \mid 0 \le o_{ij} \le 255, 0 \le i \le W_o, 0 \le j \le H_o\}, \qquad (2.1)$$

where W_o, H_o are the width, height of *O* respectively. After the process of Section 2.2 determines coordinate point *(x,y)* of *O* for combination, the corresponding B_p and B_v are defined as follows.

$$B_p = \{b_{ij} \mid b_{ij} \in O, (x - W_p) \le i \le (x + W_p), (y - H_p) \le j \le (y + H_p), W_p < \frac{W_o}{2}, H_p < \frac{H_o}{2}\}, \qquad (2.2)$$

$$B_v = \{b_{ij} \mid b_{ij} \in O, (x - W_v + 1) \le i \le (x + W_v), (y - H_v + 1) \le j \le (y + H_v), W_v < \frac{W_o}{2}, H_v < \frac{W_o}{2}\}, \tag{2.3}$$

where W_p, H_p, W_v, H_v are assigned according to the design of the system. In order to find the main energy of B_v, B_v is decomposed by repeating wavelet transform **[16, 17]** t times to obtain L. Next, we construct the most significant bit plane of L below.

$$P = \{p_{ij} \mid p_{ij} \in \{0,1\}, 0 \le i \le W_p, 0 \le j \le H_p, W_p = \frac{W_v}{2^t}, H_p = \frac{H_v}{2^t}\}, \tag{2.4}$$

where $p_{i,j} = \begin{cases} 0, & \text{if the most significant bit of the value in } L \text{ is } 0 \\ 1, & \text{if the most significant bit of the value in } L \text{ is } 1 \end{cases},$

W_p, H_p are the width, height of P respectively.

We express the value of the watermark W in binary notation. At the same time, the size of W should fit the size of L by duplication, repetition and shuffling **[18]**. That is,

$$W = \{w_{ij} \mid w_{ij} \in \{0,1\}, 0 \le i \le W_w, 0 \le j \le H_w, W_w = W_p, H_w = H_p\}, \tag{2.5}$$

where W_w, H_w are the width, height of W respectively. The secret key K is constructed by

$$K = P \oplus W, \tag{2.6}$$

here $\oplus$ is the exclusive-or operator. The B_p, K and W must be reserved in database for the verification of attacked images.

In a word, the importance of the original image is analyzed to decide the position block and the verification block. Then, the verification block and the watermark combine to produce a secret key. The complete steps are shown in Fig. 2.

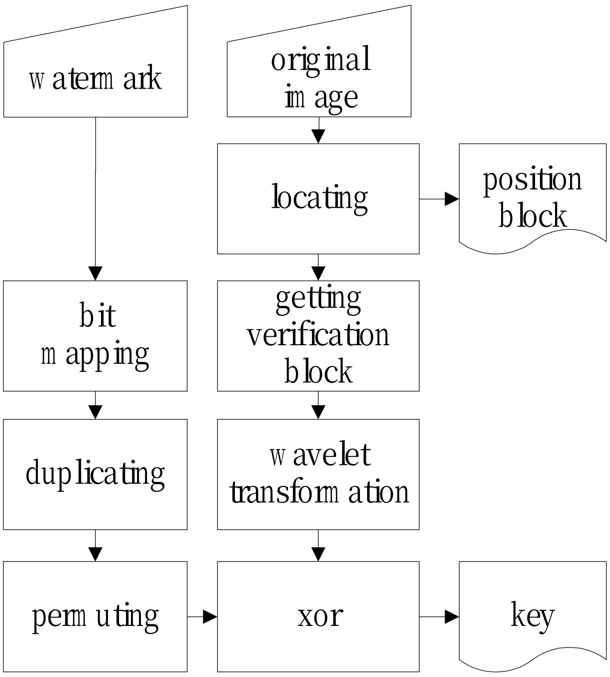


Fig. 2. Block diagram of the combination process.

2.2. The Analysis of Importance

In this section, we try to analyze the important features of *O* and choose one as the combination position. In general, the center of an image has more attraction than its corner. So we firstly reduce the select range toward the center of an image to determine coordinate point *(x,y)* from *O*. So, *O'* is defined as below.

$$O'=\{o'_{ij} \mid o'_{ij}\in O,(x_o-r*W_o)\le i\le(x_o+r*W_o),(y_o-r*H_o)\le j\le(y_o+r*H_o)\},\qquad(2.7)$$

where (x_o, y_o) is the center coordinate of *O*, *r (<0.5)* is concerned with the size of *O'*.

Then, we pick out one point (x_r, y_r) from *O'* at random and B_x is given by

$$B_x=\{b_{ij} \mid b_{ij}\in O',(x_r-s)\le i\le(x_r+s),(y_r-s)\le j\le(y_r+s)\},\qquad(2.8)$$

here *s* is concerned with the size of B_x. By using the Sobel edge dector by thresholding, we calculate *O'* and decide if B_x contains the edge. One point (x_r, y_r) is valid if its corresponding B_x contains the edge rather than smooth areas, textures or noises. However, we could change the definition of *O'* if the sum of all the valid points are very small in *O'*. Finally, we confirm the unique nature of B_p that corresponds to (x_r, y_r) to ensure finding the only one in *O*. If all is done well, we call the valid point (x_r, y_r) (x, y) specially.

Briefly, we choose one of the important features which depending on the edge of an image mainly. Moreover, the coordinate point *(x,y)* determines the combination position. All the steps are shown in Fig. 3.

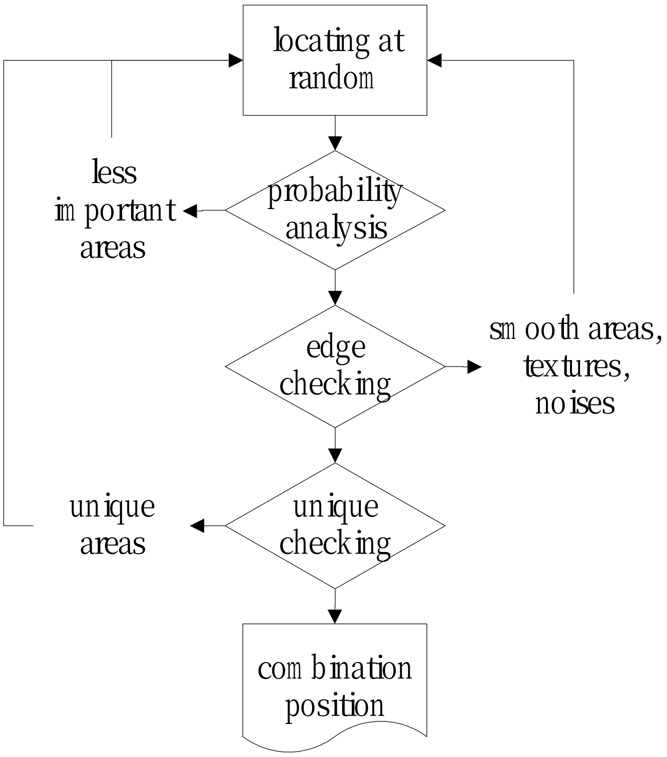


Fig. 3. Block diagram of the analysis process.

2.3. The Verification of Watermark

The verification of the watermark is similar to the process of Section 2.1. When we get a question image O_q, We locate B_p within O_q by template matching and calculate the corresponding point (x_q, y_q) by Equ. 2.2. Thus, we have

$$B_q = \{b_{ij} \mid b_{ij} \in O_q, (x_q - W_v) \le i \le (x_q + W_v), (y_q - H_v) \le j \le (y_q + H_v)\}. \qquad (2.9)$$

Next, B_q is decomposed by repeating wavelet transform t times and we also construct the most significant bit plane to obtain P_q. The extracted watermark W_q is obtained by

$$W_q = P_q \oplus K. \tag{2.10}$$

For comparing with W, W_q must be transformed into the previous expression of W by reverse-permuting and majority voting. All the steps are shown in Fig. 4.

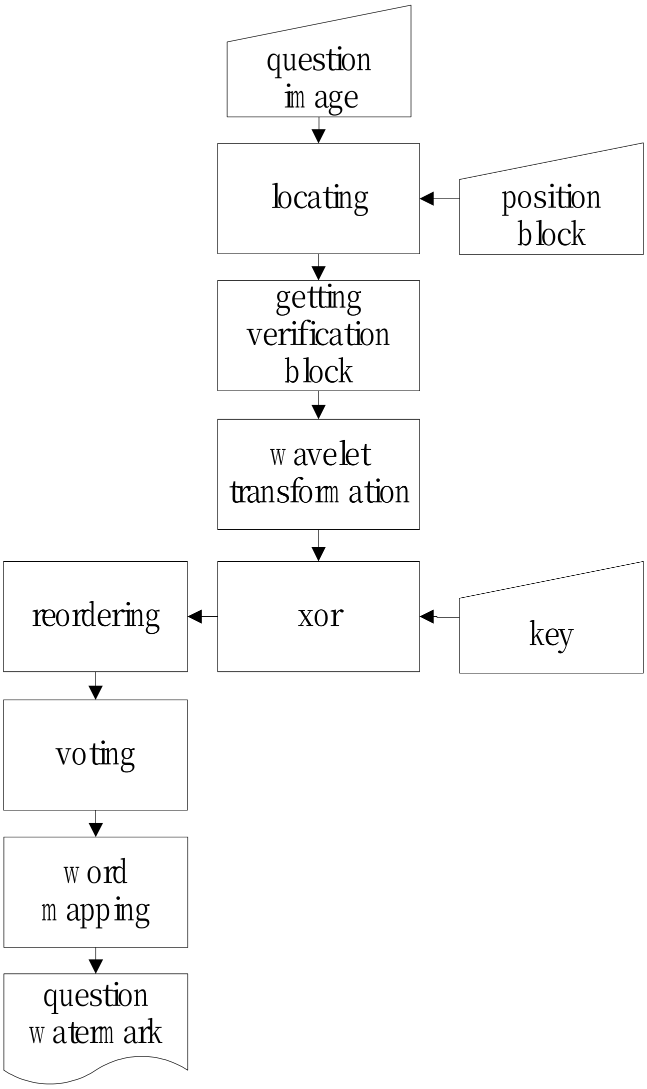


Fig. 4. Block diagram of the verification process.

3. EXPERIMENT RESULTS AND DISCUSSIONS

In order to evaluate the proposed method, we present the experiment results. We discuss the ability of the importance analysis in Section 3.1 and the robustness against different attacks in Section 3.2.

The methods that evaluate the quality between the attacked image and the original image are divided to two types: the subjective criteria and the objective criteria. For unperceivable variance, we adopt the latter and calculate the peak signal-to-noise ratio. The peak signal-to-noise ratio is defined below.

$$PSNR = 10 \times \log_{10}(\frac{255^2}{MSE}), \qquad (2.11)$$

where *MSE* is the mean square error between two images. The higher the value, the more similar two images are and vice versa. Generally speaking, while it is above 30db, we can't tell one from the other **[19]** by the naked eye. Besides, we use the false rate of the duplicates of every bit to evaluate the retrieved watermark.

3.1. The Ability of the Importance Analysis

To validate the ability of the importance analysis in the proposed method, we apply it to three images by individual. All three images are 256 gray-level images with the size of 480 by 720 pixels. We let W_p, H_p be 24 in Equ. (2.2), W_v, H_v be 64 in Equ. (2.3), r be 0.25 in Equ. (2.7) and s be 4 in Equ. (2.8).

Fig. 5(a) is the original *Sculpture* image and Fig. 5(b) presents the analysis of *Sculpture*, where *O'* is outlined and bright dots express the valid points of *O'*. The analysis process can find the edges of objects indeed and focus on the distinct foreground, which conforms to the human visual system.

We have the valid point statistics for three images shown in Table 1. The ratio of valid points to all is related with character of one image, but not with robustness. The more centralized the objects, the less the ratio.

In Fig. 6(a), the default threshold value of Sobel edge detector is applied to the *Dog* image. Observing the *Dog* image, the fuzzy edges reduce the ratio of valid points to all. Hence, some important features will be missed. To overcome this phenomenon, we use the concept of relative importance. If the ratio is below a threshold, we try to reduce the fixed threshold value of Sobel edge detector to raise the ratio. Fig. 6(b) shows the adjusted result.

Owing to the important features may be located around the center of one image like the *Church* image in Fig. 7. The selection of *O’* should be more adaptive. Fig. 7(a), 7(b) show the analysis inside *O’* and outside *O’* respectively. Here, Fig 7(b) has larger ratio than Fig. 7(a). It implies that more important features are outside and the selection of *O’* has to be adjusted.

3.2. The Robustness against Attacks

For comparing with other researches, we test the *Lena* image that is a 256 gray-level image with the size of 512 by 512 pixels. As mention in Section 2.1, we map the string “NCHU” to *W* and combine it with *P* to obtain *K*. Here, we continue using the parameter value in Section 3.1 and let *t* be 2 in Equ. (2.4). Finally, the *K* will be used to verify the these attacked images shown in Fig. 8.

To calculate *PSNR*, two images must be the same size. Accordingly, we align both the attacked image and the original image to the center and base the size of the attacted image. Besides, the false rate means the retrieved false duplicates for every bit. The bit will return correctly if the false rate falls below 50 percent.

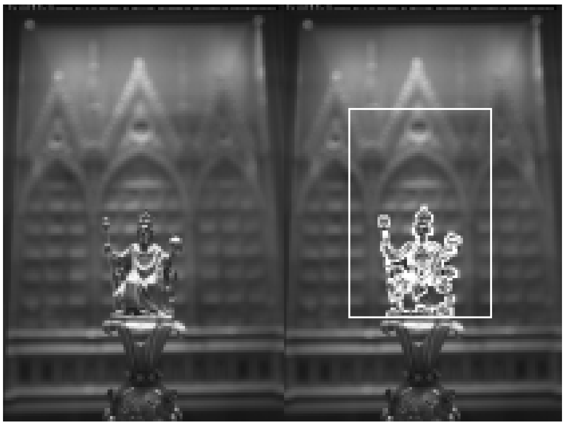
Especially, the *Lena* image is cropped to 256 by 256 pixels before these attacks are applied. That is to say, we apply double attacks on it. All the attacked image of Fig. 8 have be verified successfully.

Fig. 8(a) illustrates applying a 5 by 5 averaging filter to the cropped *Lena* image, in which the value of each element is 0.04. The aspect ratio of cropped rectangle don’t need to equal 1. Even the cropped shape could be irregular such as Fig. 8(b), which is cropped to a circle with a radius of 128 pixels. In the verification of watermark, the robustness mainly is based on the ability of locating B_p within O_q because locating B_p is previous to verify B_q. In Fig. 8(d), the JPEG compression is applied and the resulting compression ratio is 64KB/1.9KB, or 33.4:1. For the high compression ratio, the compressed image gives up too many alternating current (AC) coefficients so that the grid effect appears strongly.

4. CONCLUSIONS

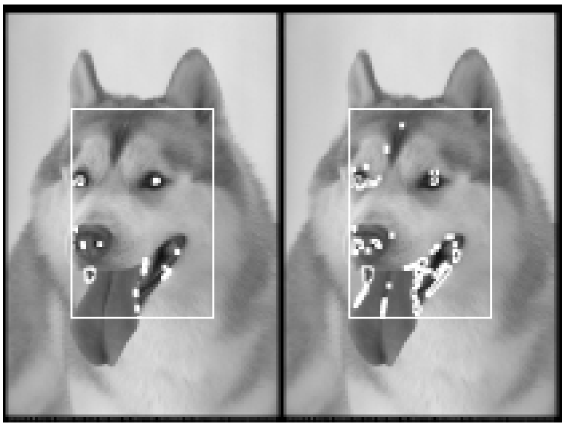
The human visual system is introduced into the proposed method to automate the complicated process of selecting combination position. Besides, it cleverly integrates the characters of spatial domain and discrete wavelet domain to construct the digital image authentication system against cropping; meanwhile, locating the block in spatial domain could reduce the cost of operations, and verifying the block in discrete wavelet domain could enhance the robustness of watermark. Experimental results show that the proposed method is quite robust against attacks like large scale cropping and irregular cropping; moreover, it could resist both the cropping attack and other image operations simultaneously.

In practice, it could be a kernel of the server that detects illegal use of the digital image. Hence, the server could search images all over the Internet and verify their copyright automatically. Especially, cropping attack is commonly used for image reproduction and distribution **[20]**. However, it is expected that the color image could be suitable for the method in the future.



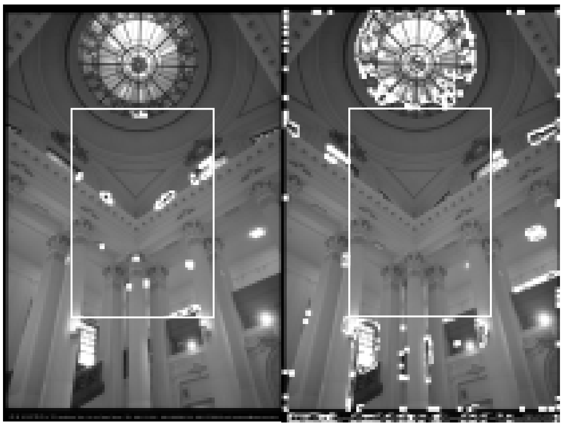
(a) (b)

Fig. 5. The analysis of a *Sculpture* image: (a) before; (b) after.



(a) (b)

Fig. 6. The analysis of a *Dog* image: (a) default; (b) adjusted.



(a) (b)

Fig. 7. The analysis of a *Church* image: (a) inside; (b) outside.

Table 1: Valid/invalid point statistics for Fig. 5, 6, 7.

Image Name	Valid Point	Ratio	Invalid Point	Ratio
	(pixels)	(%)	(pixels)	(%)
Sculpture	7002	8.10	79398	91.90
Dog	2161	2.50	84239	97.50
*Dog**	7085	8.20	79315	91.80
Church	3357	3.89	83043	96.11
*Church***	22816	8.80	236384	91.20

*Adjusted; **Outside

Table 2: The PSNR values and the false rate statistics for the corresponding images of Fig. 8.

Images of Fig. 8	PSNR	Mean of the False Rate	Stand Deviation of the False Rate
	(dB)	(%)	(%)
(a)	25.43	0.1484	0.884
(b)	25.63	0.1787	0.0568
(c)	29.08	0.1309	0.0511
(d)	25.51	0.1338	0.0484
(e)	16.06	0.1914	0.0501
(f)	15.91	0.1622	0.0501
(g)	15.49	0.1914	0.0571
(h)	15.67	0.1621	0.0541
(i)	22.11	0.1816	0.0558
(j)	17.50	0.0771	0.0476

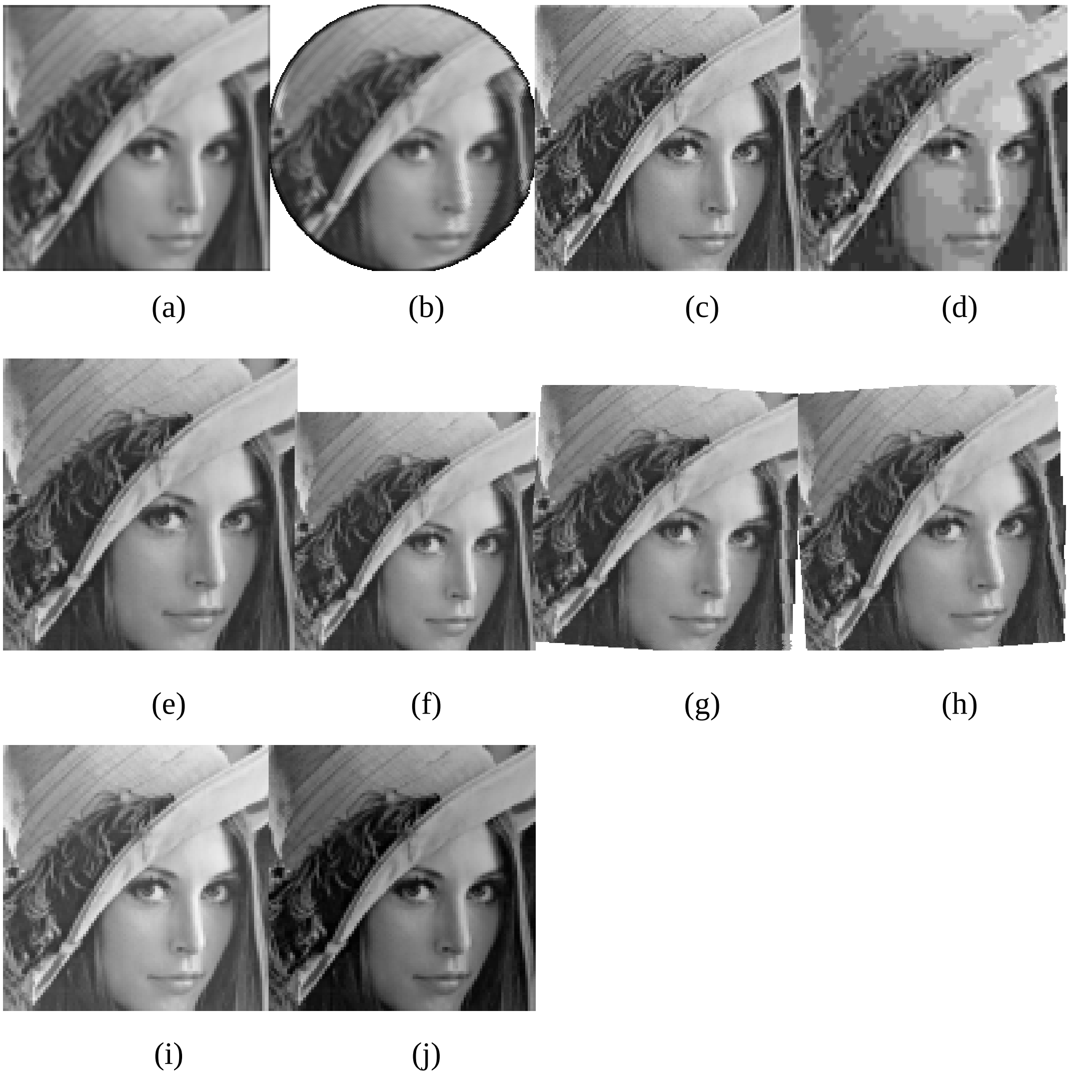


Fig. 8. Different attacked versions of the *Lena* image with cropping to 256 by 256 pixels: (a) blurring; (b) blurring but irregular cropping; (c) sharpening; (d) JPEG with compression ratio 33.4; (e) resizing to 282 by 282 pixels; (f) resizing to 230 by 230 pixels; (g) rotating by 4 degrees clockwise; (h) rotating by 4 degrees anti-clockwise; (i) brightening by 20 gray-levels; (j) darkening by 34 gray-levels.

REFERENCE

[1] N. Nikolaidis and I. Pitas, "Digital image watermarking: an overview", *IEEE International Conference on Multimedia Computing and Systems*, Vol. 1, pp 1-6, 1999.

[2] S. P. Mohanty, K. R. Ramakrishnan and M. S. Kankanhalli, "A DCT Domain Visible Watermarking Technique for Images", *IEEE International Conference on Multimedia and Expo*, Vol. 2, pp 1029-1032, 2000.

[3] M. Wu and B. Liu, "Watermarking for image authentication", *International Conference on Image Processing(ICIP)*, Vol. 2, pp 437-441, 1998.

[4] W. Zeng and B. Liu, "On Resolving Rightful Ownerships of Digital Images by Invisible", *International Conference on Image Processing*, Vol. 1, pp 552-555, 1997.

[5] M. Wu, E. Tang and B. Liu, "Data Hiding in Digital Binary Image", *IEEE International Conference on Multimedia and Expo*, Vol. 1, pp 393-396, 2000.

[6] I. J. Cox, J. Kilian, T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia", *IEEE Transactions on Image Processing*, Vol. 6, No. 12, pp 1673-1687, 1997.

[7] S. Suthaharan and S. Sathananthan, "Transform domain technique: robust watermarking for digital images", *IEEE SoutheastCon*, pp 407-412, 2000.

[8] I. J. Cox and M. L. Miller, "Electronic watermarking: the first 50 years", *IEEE Fourth Workshop on Multimedia Signal Processing*, pp 225-230, 2001.

[9] J. J. K. O'Ruanaidh and T. Pun, "Rotation, scale and translation invariant digital image watermarking", *International Conference on Image Processing*, Vol. 1, pp 536-539, 1997.

[10] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller and Y. M. Lui, "Rotation, scale, and translation resilient watermarking for images", *IEEE Transactions on Image Processing*, Vol. 10, No. 5, pp 767-782, 2001

[11] H. Kii, J. Onishi, S. Ozawa, “The digital watermarking method by using both patchwork and DCT”, *IEEE International Conference on Multimedia Computing and Systems*, Vol. 1, pp 895-899, 1999.

[12] C. C. Chang, K. F. Hwang and M. S. Hwang, “A block based digital watermarks for copy protection of images”, *Fifth Asia-Pacific Conference on Communications and Fourth Optoelectronics and Communications Conference*, Vol. 2, pp 977-980, 1999.

[13] I. J. Cox, M. L. Miller and J. A. Bloom, “Watermarking applications and their properties”, *International Conference on Information Technology: Coding and Computing*, pp 6-10, 2000.

[14] X. Ran, and N. Farvardin, “A perceptually motivated three-component image model-Part I: description of the model”, *IEEE Transactions on Image Processing*, Vol. 4, No. 4, pp 401-415, 1995.

[15] W. B. Lee and T. H. Chen, "A Robust Copyright Protection Scheme for Still Images", *Proceedings of 2000 International Computer Symposium Workshop*, 2000,

[16] C. T. Hsu and J. L. Wu, “Multiresolution Watermarking for Digital Images”, *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, Vol. 45, No. 8, pp 1097-1101, 1998.

[17] K. R. Castleman, *Digital Image Processing*, New Jersey: Prentice-Hall, 1996.

[18] M. Wu and B. Liu, “Digital Watermarking using shuffling”, *International Conference on Image Processing*, Vol. 1, pp 291-295, 1999.

[19] M. S. Hwang, C. C. Chang and K. F. Hwang, “A Watermarking Technique Based on One-way Hash Functions”, *IEEE Transactions on Consumer Electronics*, Vol. 45, No. 2, pp. 286-294, 1999.

[20] C. Y. Lin and S. F. Chang, “Distortion modeling and invariant extraction for digital image print-and-scan process”, *International Symposium. on Multimedia Information Processing (ISMIP 99)*, Taipei, Taiwan, 1999.