Hidden Digital Watermarks in Images

Chiou-Ting Hsu and Ja-Ling Wu, *Senior Member, IEEE*

Abstract— In this paper, an image authentication technique by embedding digital "watermarks" into images is proposed. *Watermarking* is a technique for labeling digital pictures by hiding secret information into the images. Sophisticated watermark embedding is a potential method to discourage unauthorized copying or attest the origin of the images. In our approach, we embed the watermarks with visually recognizable patterns into the images by selectively modifying the middle-frequency parts of the image. Several variations of the proposed method will be addressed. The experimental results show that the proposed technique successfully survives image processing operations, image cropping, and the Joint Photographic Experts Group (JPEG) lossy compression.

Index Terms— Digital watermark, discrete cosine transform, JPEG compression, pseudorandom permutation.

I. INTRODUCTION

DUE TO THE rapid and extensive growth of electronic publishing industry, data can now be distributed much faster and easier. Unfortunately, engineers still see immense technical challenges in discouraging unauthorized copying and distributing of electronic documents [1]. Conventionally, a painting is signed by the artist to attest the copyright, an identity card is stamped by the steel seal to avoid forgery, and paper money is identified by the embossed portrait. Such kinds of handwritten signatures, seals, or watermarks have been used since ancient times as a way to identify the source or creator of a document or picture. However, in the digital world, digital technology for manipulating images has made it difficult to distinguish the visual truth. "Seeing is believing" will become an anachronism [2].

One potential solution for claiming the ownership is to use electronic stamps or so-called *watermarks*, which are embedded into the images, and have the following features:

- undeletable by hackers;
- perceptually invisible, i.e., the watermark should not render visible artifact;
- statistically undetectable;
- resistant to lossy data compression, e.g., the Joint Photographic Experts Group (JPEG) compression;
- resistant to image manipulation and processing operations, e.g., cut-and-paste, filtering, etc.

C.-T. Hsu is with the Communication and Multimedia Laboratory, Department of Computer Science and Information Engineering, National Taiwan University, Taipei, Taiwan, R.O.C. (e-mail: candy@cmlab.csie.ntu.edu.tw).

J.-L. Wu is with the Communication and Multimedia Laboratory, Department of Computer Science and Information Engineering, National Taiwan University, Taipei, Taiwan, R.O.C. (e-mail: wjl@cmlab.csie.ntu.edu.tw).

In the literature, several techniques have been developed for watermarking. In [3], three coding methods for hiding electronic marking in document were proposed. In [4]–[7], the watermarks are applied on the spatial domain. The major disadvantage of spatial domain watermarking is that a common picture cropping operation may eliminate the watermark. Other than spatial domain watermarking, frequency domain approaches have also been proposed. In [8], a copyright code and its random sequence of locations for embedding are produced, and then superimposed on the image based on a JPEG model. In [9], the spread spectrum communication technique is also used in multimedia watermarking.

In most of the previous works [8]–[10], the watermark is a symbol or an random number which comprises of a sequence of bits, and can only be "detected" by employing the "detection theory." That is, during the verification phase, the original image is subtracted from the image in question, and the similarity between the difference and the specific watermark is obtained. Therefore, an experimental threshold is chosen and compared to determine whether the image is watermarked. In this paper, we propose a technique for embedding digital watermarks with visually recognizable patterns into the images. Since, in daily life, one claim a document, a creative work, and so on, by signing one's signature, stamping a personal seal or an organization's logo, such kinds of visually recognizable patterns are more intuitive for representing one's identity than a sequence of random numbers is. More specifically, during the verification phase of our work, an "extracted" visual pattern in conjunction with the similarity measurement will be provided for verification.

First of all, the watermark is generated as a binary pattern, and then permuted to disperse the spatial relationship and to increase the invisibility based on the characteristics of images. Also, since human eyes are more sensitive to lower frequency noise, intuitively the watermark should be embedded into the higher frequency components to achieve better perceptual invisibility. However, since the energy of most natural images are concentrated on the lower frequency range, the information hidden in the higher frequency components might be discarded after quantization operation of lossy compression. Therefore, to invisibly embed the watermark that can survive the lossy data compression, a reasonable trade-off is to embed the watermark into the middle-frequency range of the image. In our scheme, watermarks are embedded by modifying the middle-frequency coefficients within each image block of the original image in considering the effect of quantization. The experimental results show that the proposed technique could survive several kinds of image processing and the JPEG lossy compression.

This paper is organized as follows. The embedding approach is described in Section II. Section III describes the watermark extraction method. In Section IV, the experimental results are shown. In Section V, several issues of the proposed method are discussed. The conclusion of this paper is stated in Section VI.

II. EMBEDDING METHODS

In our approach, a block DCT-based algorithm is developed to embed the image watermarking.

Let X be the original gray-level image of size $N_1 \times N_2$, and the digital watermark W be a binary image of size $M_1 \times M_2$. In the watermark, the marked pixels are valued as one's, and the others are zero's. Since only the middle-frequency range of the host image will be processed during the watermark embedding, the resolution of a watermark image W is assumed to be smaller than that of the original image X. For example, for each 8×8 image block, only $(64 \times \frac{M_1 \times M_2}{N_1 \times N_2})$ coefficients will be used for the watermark embedding. The ratio of $(M_1 \times M_2)$ and $(N_1 \times N_2)$ determines the amount of information to be embedded into the image. In general, for more robust and invisible embedding, the amount of information can be embedded should be reduced. On the other hand, in order to provide a visually recognizable watermark with nontrivial amount of information, instead of using an ID number with trivial amount of data, making the watermark embedding perceptually invisible is not a trivial problem.

The original image X and digital watermark W are represented as

$$X = \{x(i,j), 0 \le i < N_1, 0 \le j < N_2\} \tag{1}$$

where $x(i,j) \in \{0, \cdots, 2^L - 1\}$ is the intensity of pixel $x(i,j)$ and L is the number of bits used in each pixel.

$$W = \{w(i,j), 0 \le i < M_1, 0 \le j < M_2\} \tag{2}$$

where $w(i,j) \in \{0,1\}$.

In X, there are $\frac{N_1}{8} \times \frac{N_2}{8}$ image blocks with size 8×8. To obtain the same number $\frac{N_1}{8} \times \frac{N_2}{8}$ of blocks as the image X, the watermark W is decomposed into several blocks with size $(M_1 \times \frac{8}{N_1}) \times (M_2 \times \frac{8}{N_2})$. For example, if $M_1 = N_1/2$ and $M_2 = N_2/2$, the block size of the watermark block is 4×4, and if $M_1 = N_1/4$ and $M_2 = N_2/4$, the block size of the watermark block is 2×2. The extra columns and rows might be added to complete each image and watermark blocks.

A. Pseudorandom Permutation of the Watermark

In the approach, each watermark block is embedded into the middle-frequency range of each image block using block-transform instead of full-frame transform. Therefore, each watermark block will only be dispersed over its corresponding image block, instead of the entire spatial image. Obviously, without appropriate adjustment for the spatial relationship of the watermark, a common picture-cropping operation may eliminate the watermark.

To survive picture-cropping, a fast two-dimensional (2-D) pseudorandom number traversing method is used to permute the watermark to disperse its spatial relationship, i.e.,

$$W_p = \text{Permute}(W)$$
$$W_p = \{w_p(i,j)$$
$$= w(i',j'), 0 \le i, i' < M_1 \text{ and } 0 \le j, j' < M_2\} \tag{3}$$

where pixel (i', j') is permuted to pixel (i, j) in a pseudorandom order.

In our approach, the permutation is implemented as follows. First, number each pixel from zero to $(M_1 \times M_2)$. Second, generate each number in random order. Finally, generate the coordinate pairs by mapping the random sequence number into a 2-D sequence. For example, for a digital watermark of size 128×128, use a "linear feedback shift register" [11] to generate a random sequence from 1 to $16\,383$. Then, for each sequence element number M, compute $(M \text{ div } 128)$ and $(M \text{ mod } 128)$ as the permuted vertical and horizontal coordinates.

B. Block-Based Image-Dependent Permutation of the Watermark

In order to improve the perceptual invisibility, the characteristics of the original image should be considered, e.g., the modifications of high frequencies or high luminance regions are less perceptible. Such image-dependent properties can be used to shuffle the pseudorandom permuted watermark to fit the sensitivity of human eyes.

For each image block of size 8×8, the variances (which is used as a measure of invisibility under watermark embedding) are computed and sorted. For each watermark block of size, $(M_1 \times \frac{8}{N_1}) \times (M_2 \times \frac{8}{N_2})$, the amount of information (i.e., the number of signed pixels) are sorted also. Then, shuffle each watermark block into the spatial position according the corresponding sorting order of the image block, i.e., $W_b = \text{Permute}(W_p)$; in which

$$W_p = \left\{ w_p \left(k \times \left(M_1 \times \frac{8}{N_1} \right) + i, l \times \left(M_2 \times \frac{8}{N_2} \right) + j \right), \right.$$
$$0 \le k < \frac{N_1}{8}, 0 \le l < \frac{N_2}{8}, 0 \le i < \left(M_1 \times \frac{8}{N_1} \right),$$
$$\left. 0 \le j < \left(M_2 \times \frac{8}{N_2} \right) \right\} \tag{4}$$

and

$$W_b = \left\{ w_b \left(k \times \left(M_1 \times \frac{8}{N_1} \right) + i, l \times \left(M_2 \times \frac{8}{N_2} \right) + j \right) \right.$$
$$= w_p \left(k' \times \left(M_1 \times \frac{8}{N_1} \right) + i, l' \times \left(M_2 \times \frac{8}{N_2} \right) + j \right),$$
$$0 \le k, k' < \frac{N_1}{8}, 0 \le l, l' < \frac{N_2}{8}, 0 \le i < \left(M_1 \times \frac{8}{N_1} \right),$$
$$\left. 0 \le j < \left(M_2 \times \frac{8}{N_2} \right) \right\} \tag{5}$$

where block (k', l') is shuffled to block (k, l) by the block-based permutation. Fig. 1 shows an example of the sorting and the permutation.
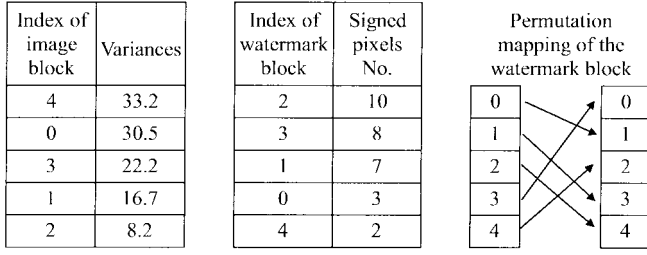
Index of image block	Variances
4	33.2
0	30.5
3	22.2
1	16.7
2	8.2

Index of watermark block	Signed pixels No.
2	10
3	8
1	7
0	3
4	2

Permutation mapping of the watermark block

0	0
1	1
2	2
3	3
4	4

Fig. 1. Example of block-based image-dependent permutation, where for each 8×8 image block, the variance is computed and sorted, and for each watermark block of size $(M_1 \times \frac{8}{N_1}) \times (M_2 \times \frac{8}{N_2})$, the amount of information (i.e., the number of signed pixels) is sorted also, and then each watermark block is shuffled into the spatial position according the corresponding sorting order of the image.

C. Block Transformation of the Image

Since the discrete cosine transform (DCT) used by JPEG [12] is performed on blocks of 8×8, the input image X is divided into blocks of 8×8, and each block is DCT transformed independently. That is,

$$Y = \text{FDCT}(X)$$

where FDCT denotes the operation of forward DCT.

D. Choice of Middle-Frequency Coefficients

The human eye is more sensitive to noise in lower frequency components than in higher frequency ones. However, the energy of most natural images are concentrated in the lower frequency range, and the information hidden in the higher frequency components might be discarded after quantization operation of lossy compression. In order to invisibly embed the watermark that can survive lossy data compressions, a reasonable trade-off is to embed the watermark into the middle-frequency range of the image. To this end, for each 8×8 image block, only $(64 \times \frac{M_1 \times M_2}{N_1 \times N_2})$ coefficients are selected out of the 64 DCT coefficients. Those selected coefficients are then mapped into a reduced image block of size $(M_1 \times \frac{8}{N_1}) \times (M_2 \times \frac{8}{N_2})$. That is, the middle-frequency coefficients selected from the image of size $(N_1 \times N_2)$ are collected to compose a reduced image of size $(M_1 \times M_2)$, which has the same resolution with the binary watermark.

$$Y_r = \text{Reduce}(Y)$$

where

$$Y = \left\{ y(k \times 8 + i, l \times 8 + j), 0 \leq k < \frac{N_1}{8} \right.$$
$$\left. 0 \leq l < \frac{N_2}{8}, 0 \leq i < 8, 0 \leq j < 8 \right\} \quad (6)$$

and

$$Y_r = \left\{ y_r\left(k \times \left(M_1 \times \frac{8}{N_1}\right) + i', l \times \left(M_2 \times \frac{8}{N_2}\right) + j'\right) \right.$$
$$0 \leq k < \frac{N_1}{8}, 0 \leq l < \frac{N_2}{8}, 0 \leq i' < \left(M_1 \times \frac{8}{N_1}\right)$$
$$\left. 0 \leq j' < \left(M_2 \times \frac{8}{N_2}\right) \right\}. \quad (7)$$

0	1	5	6	14	15	27	28
2	4	7	13	16	26	29	42
3	8	12	17	25	30	41	43
9	11	18	24	31	40	44	53
10	19	23	32	39	45	52	54
20	22	33	38	46	51	55	60
21	34	37	47	50	56	59	61
35	36	48	49	57	58	62	63

$\rightarrow$

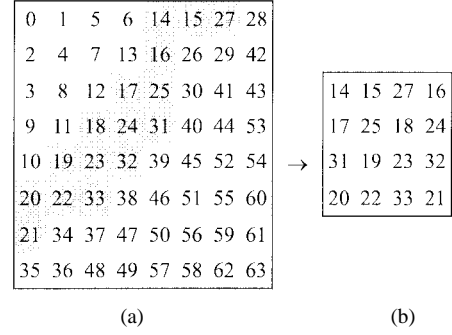| 14	15	27	16
17	25	18	24
31	19	23	32
20	22	33	21

(a)   (b)

Fig. 2. Example of defining the middle-frequency coefficients, in which the coefficients are picked up in zigzag-scan order and then reordered into block of 4×4. (a) Zigzag ordering of DCT coefficients and the middle frequency coefficients are shown in the shadow area. (b) Picked up coefficients are mapped into the 4×4 block.
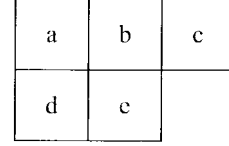
a	b	c
d	e	

Fig. 3. Residual mask, where each square includes a reduced image block of size $(M_1 \times \frac{8}{N_1}) \times (M_2 \times \frac{8}{N_2})$, and position e stands for the current reduced block.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

8	6	5	8	12	20	26	31
6	6	7	10	13	29	30	28
7	7	8	12	20	29	35	28
7	9	11	15	26	44	40	31
9	11	19	28	34	55	52	39
12	18	28	32	41	52	57	46
25	32	39	44	52	61	60	51
36	47	48	49	56	50	52	50

(a)   (b)

Fig. 4. Luminance quantization table. (a) Default JPEG quantization table. (b) JPEG quantization table used by Image Alchemy, Handmade Software Inc.

For example, if $M_1 = N_1/2$ and $M_2 = N_2/2$, only 16 DCT coefficients are processed during the watermark embedding, and the other 48 DCT coefficients are left unchanged. Fig. 2 exemplifies our definition of the middle-frequency coefficients, which are mapped into a reduced block of size 4×4.

E. Modification of the DCT Coefficients

Now, a permuted digital watermark and a reduced image (which contains only the middle-frequency components of the original image) both with size $(M_1 \times M_2)$ are obtained. For each watermark block of size $(M_1 \times \frac{8}{N_1}) \times (M_2 \times \frac{8}{N_2})$, the reduced image block of size $(M_1 \times \frac{8}{N_1}) \times (M_2 \times \frac{8}{N_2})$ at the corresponding spatial position will be modified adequately to embed the watermarked pixels.

In our opinion, embedding each watermarked pixel by modifying the polarity between the corresponding pixels in neighboring blocks is an effective approach to achieve the invisibility and survival for low compression ratio of JPEG. However, this method is not robust with respect to the compression attacks with higher compression ratio (≥ 6). At part (a), we will address the technical challenges. At part (b), an
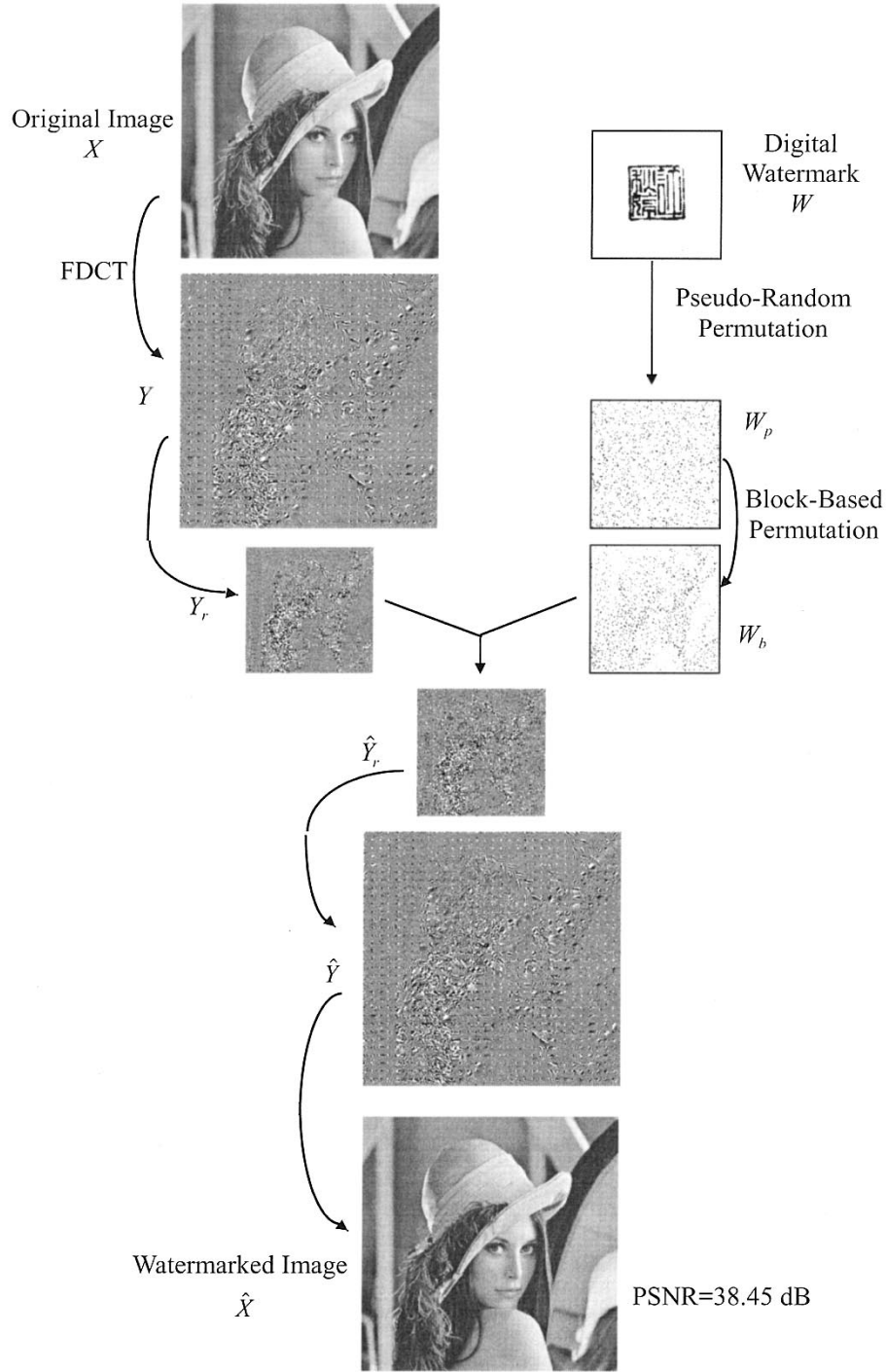
Fig. 5. Watermark embedding steps.

improved method that is resistant to higher compression ratio will be described.

1) Embedding into the Relationship Between Neighboring Blocks: A 2-D residual mask is used to compute the polarity of the chosen middle-frequency coefficients between neighboring blocks. For example, in Fig. 3, if $a = b = c = 0$, $d = -1$, $e = 1$, then the polarity is a binary pattern (zero or one) which represents the coefficients at the position of the current reduced-block is larger (polarity $= 1$) or less (polarity $= 0$) than the coefficient at the corresponding position of the previous reduced-block. That is,

$$P = \text{Polarity}(Y_r)$$
$$P = \left\{ p\left(k \times \left(M_1 \times \frac{8}{N_1}\right) + i, l \times \left(M_2 \times \frac{8}{N_2}\right) + j\right), \right.$$
$$0 \leq k < \frac{N_1}{8}, 0 \leq l < \frac{N_2}{8}, 0 \leq i < \left(M_1 \times \frac{8}{N_1}\right),$$
$$\left. 0 \leq j < \left(M_2 \times \frac{8}{N_2}\right) \right\} \tag{8}$$
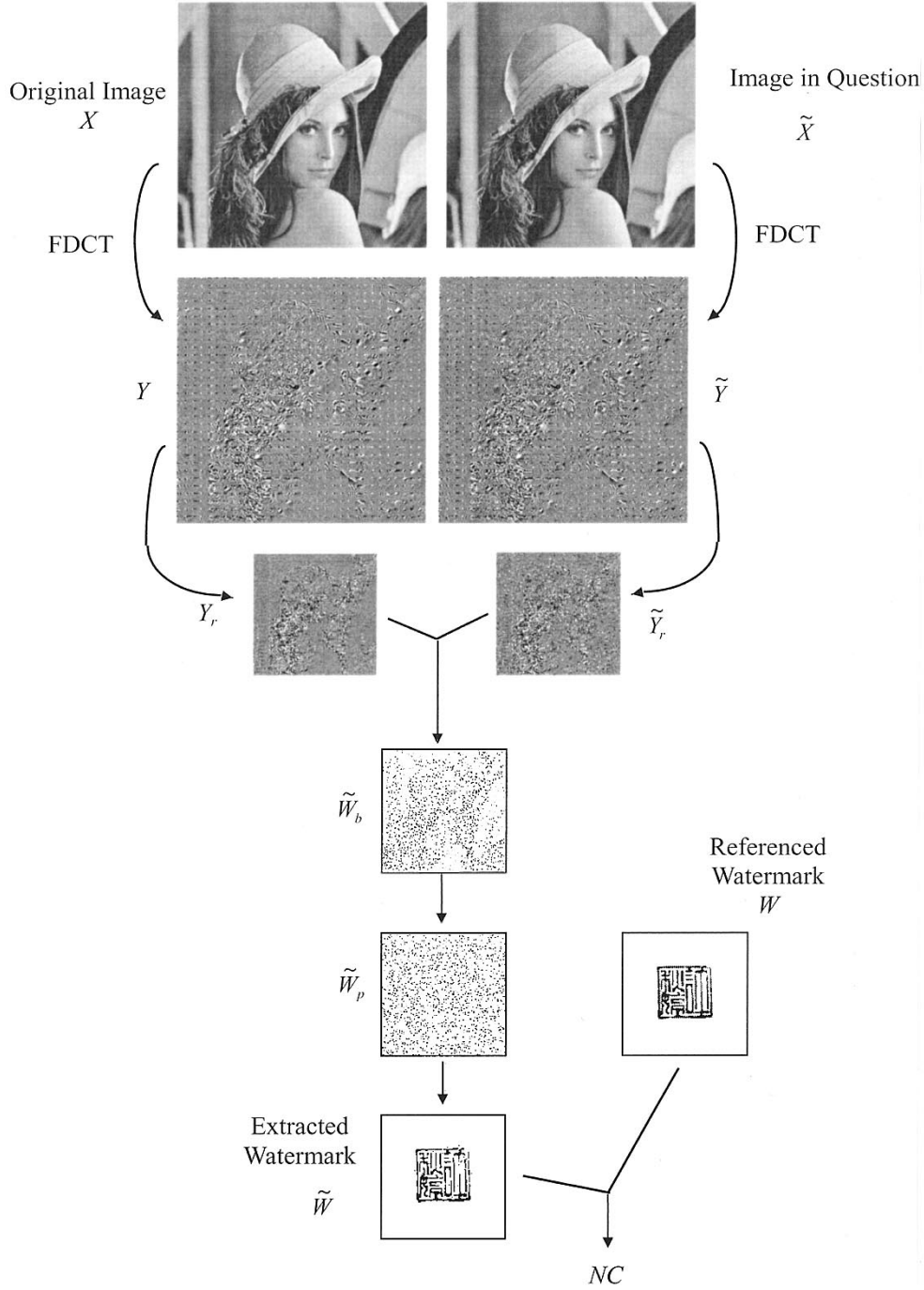
Fig. 6.   Watermark extracting steps.

where

$$p\left(k \times \left(M_1 \times \frac{8}{N_1}\right) + i, l \times \left(M_2 \times \frac{8}{N_2}\right) + j\right).$$

$$= \begin{cases} 1, & \text{if } y_r\left(k \times \left(M_1 \times \frac{8}{N_1}\right) + i, l \times \left(M_2 \times \frac{8}{N_2}\right) + j\right) \\ & \quad > y_r\left((k-1) \times \left(M_1 \times \frac{8}{N_1}\right) + i, (l-1)\right. \\ & \quad \left. \times \left(M_2 \times \frac{8}{N_2}\right) + j\right) \\ 0, & \text{otherwise.} \end{cases}$$

$$(9)$$

After the binary polarity pattern is obtained, for each marked pixel of the permuted watermark, modify the DCT coefficients according the residual mask to reverse the corresponding

polarity. That is,

$$\hat{P} = \text{XOR}(P, W_b)$$
$$\hat{P} = \{\hat{p}(i,j), 0 \le i < M_1 \text{ and } 0 \le j < M_2\} \qquad (10)$$

where

$$\hat{p}(i,j) = \begin{cases} 1 - p(i,j), & \text{if } w_b(i,j) = 1 \\ p(i,j), & \text{if } w_b(i,j) = 0 \end{cases} = p(i,j) \oplus w_b(i,j).$$

$$(11)$$

Then, construct $\hat{Y}_r$ from $\hat{P}$ such that the differences between $\hat{Y}_r$ and Y_r are minimized or smaller than a user specified

threshold;

$$\hat{Y}_r = \text{Expand}(\hat{P})$$
$$\text{s.t.} \sum_{i,j}(y_r(i,j) - \hat{y}_r(i,j))^2 < \text{threshold.} \quad (12)$$

Note that the "Expand" operation constructs $\hat{Y}_r$ based on polarity $\hat{P}$. For example, assign the initial coefficient $\hat{y}_r(i_0, j_0) = y_r(i_0, j_0)$, and add (or subtract) the coefficients of neighboring blocks according to the residual mask in order to match the corresponding polarity $\hat{p}(i_0, j_0)$. Then, proceed to successive coefficients by modifying only those who will not affect the polarities of the previous-processed coefficients.

In order to improve the invisibility, the polarity should be computed for absolute value of the coefficients so that the sign (plus and minus signs) of the coefficients are hopefully preserved to reduce the changes introduced by modification.

Besides, in order to survive the JPEG lossy compression, the quantization effect utilized in the JPEG codec must be considered. Fig. 4(a) shows the suggested luminance quantization table for JPEG standard, which usually cause perceptible artifacts when viewed on high-quality displays. Fig. 4(b) shows another quantization table used in most JPEG software. The values are almost half of the corresponding JPEG suggested quantization values. Based on a referenced quantization table, the polarity are computed from coefficients after quantization and then dequantization. Therefore, in case of quantization attack, the correct marked pixel should be extracted. That is, the polarity should be

$$p\left(k \times \left(M_1 \times \frac{8}{N_1}\right) + i, l \times \left(M_2 \times \frac{8}{N_2}\right) + j\right) =$$
$$\begin{cases} 1, & \text{if } \left\lfloor \frac{\left|y_r\left(k \times \left(M_1 \times \frac{8}{N_1}\right) + i, l \times \left(M_2 \times \frac{8}{N_2}\right) + j\right)\right|}{Q(i,j)} \right\rfloor Q(i,j) > \\ & \left\lfloor \frac{\left|y_r\left((k-1) \times \left(M_1 \times \frac{8}{N_1}\right) + i, (l-1) \times \left(M_2 \times \frac{8}{N_2}\right) + j\right)\right|}{Q(i,j)} \right\rfloor Q(i,j) \\ 0, & \text{otherwise} \end{cases}$$
$$(13)$$

where $Q(i,j)$ is the quantization value at the corresponding position (i,j).

However, since quantization tends to make many coefficients zero (especially those for higher spatial frequencies), if the modification of the coefficients is not large enough, most middle-frequency coefficients will also be truncated to zero after coarse quantization. Besides, in order to preserve the polarity to survive quantization according the specified residual mask, not only those middle-frequency coefficients in the current block have to be modified, but also all the neighboring blocks involved in the residual mask have be to modified with the same volume. Therefore, although survival for lossy compression, the watermarked image which are embedded with large modification will not be perceptually equivalent to the original image.

2) Embedding into the Relationship Within Each Block In order to overcome the technical challenges addressed above, while still hopefully not to propagate the modifications into the neighboring blocks (so as to improve the invisibility), the
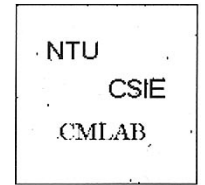

(a)
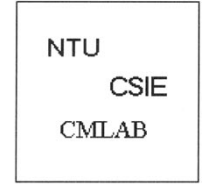
(b)

(c)

(d)

Fig. 7. Example of the proposed watermarking approach. (a) Test image Lena. (b) Watermark. (c) Watermarked image (with PSNR = 40.83 dB). (d) Extracted watermark (with $\text{NC} \cong 1$).

relatively more reliable DC coefficient (instead of the middle-frequency coefficients of neighboring blocks) is used as a reference value for each block. That is,

$$P = \text{Polarity}(Y_r)$$
$$P = \left\{ p\left(k \times \left(M_1 \times \frac{8}{N_1}\right) + i, l \times \left(M_2 \times \frac{8}{N_2}\right) + j\right), \right.$$
$$0 \le k < \frac{N_1}{8}, 0 \le l < \frac{N_2}{8}, 0 \le i < \left(M_1 \times \frac{8}{N_1}\right),$$
$$\left. 0 \le j < \left(M_2 \times \frac{8}{N_2}\right) \right\} \quad (14)$$

where

$$p\left(k \times \left(M_1 \times \frac{8}{N_1}\right) + i, l \times \left(M_2 \times \frac{8}{N_2}\right) + j\right)$$
$$= \begin{cases} 1, & \text{if } \left\lfloor \frac{\left|y_r\left(k \times \left(M_1 \times \frac{8}{N_1}\right) + i, l \times \left(M_2 \times \frac{8}{N_2}\right) + j\right)\right|}{Q(i,j)} \right\rfloor Q(i,j) \\ & > \left\lfloor \frac{|y(k \times 8, l \times 8)|}{\text{scale\_factor} \times Q(0,0)} \right\rfloor Q(0.0) \\ 0, & \text{otherwise.} \end{cases}$$
$$(15)$$

For each marked pixel, add (or subtract) the corresponding coefficient so that the modified coefficients $\hat{Y}_r$ will have the reverse polarity $\hat{P}$.

F. Inverse Block Transform

Finally, map the modified middle-frequency coefficients $\hat{Y}_r$ into Y to get $\hat{Y}$. Then, inverse DCT (IDCT) of the associated
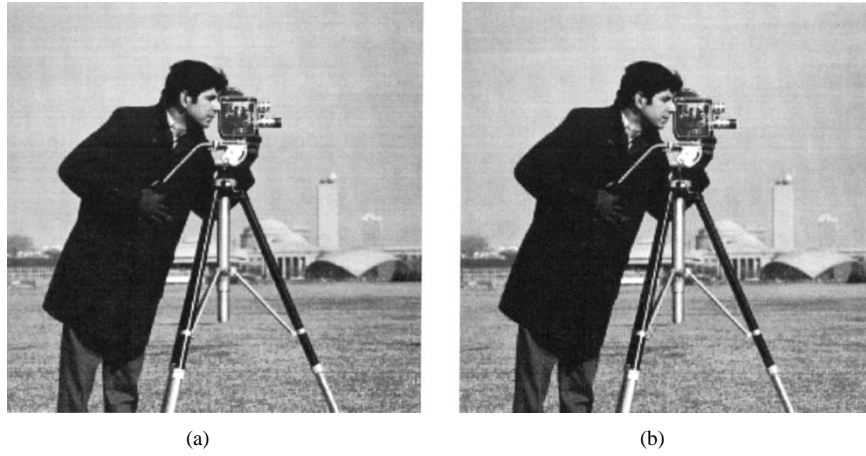
(a) (b)

Fig. 8. Another example of the proposed approach. (a) Cameraman test image. (b) Watermarked image (with PSNR = 39.29 dB).

result to obtained the embedded image.

$$\hat{X} = \mathrm{IDCT}(\hat{Y}).$$

Fig. 5 illustrates the steps of embedding the watermark, where Lena is used as the test image of size 256×256, and a seal with Chiou-Ting Hsu's Chinese name is used as a binary watermark of size 128×128.

III. WATERMARK EXTRACTING METHOD

The extraction of watermark requires the original image, the watermarked image, and either the watermark or the permutation mapping used in image-dependent permutation during the embedding steps. The extraction steps are described as follows.

A. Block Transformation

Both the original image X and the image in question $\tilde{X}$ are DCT transformed.

$$Y = \mathrm{FDCT}(X)$$
$$\tilde{Y} = \mathrm{FDCT}(\tilde{X}).$$

B. Generation of Polarity Patterns

Generate the reduced images which contain only the middle-frequency coefficients and then use these middle-frequency DCT coefficients to produce the polarity patterns. That is,

$$Y_r = \mathrm{Reduce}\ (Y)$$
$$\tilde{Y}_r = \mathrm{Reduce}\ (\tilde{Y})$$

and then

$$P = \mathrm{Polarity}\ (Y_r)$$
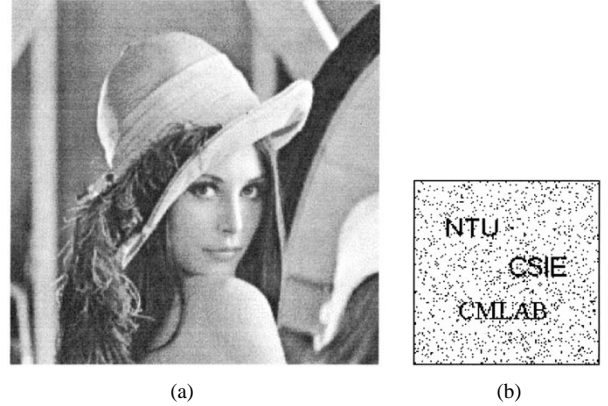$$\tilde{P} = \mathrm{Polarity}\ (\tilde{Y}_r).$$

(a) (b)

Fig. 9. (a) Blurred version of Fig. 7(c). (b) Extracted watermark with NC = 0.982.

C. Extract the Permuted Data

Perform exclusive-or (XOR) operation on these two polarity patterns to obtain a permuted binary data, i.e.,

$$\tilde{W}_b = \mathrm{XOR}(P, \tilde{P})$$

where

$$\tilde{w}_b(i,j) = p(i,j) \oplus \tilde{p}(i,j). \tag{16}$$

D. Reverse Block-Based Image-Dependent Permutation

The image-dependent permutation mapping could be obtained either by saving as a file during the embedding steps or recomputed from the original image and the watermark. Based on the mapping, reverse permute $\tilde{W}_b$ to get $\tilde{W}_p$.

E. Reverse Pseudorandom Permutation

Reverse-permute $\tilde{W}_p$ to get the watermark $\tilde{W}$

$$\tilde{w}(i,j) = \tilde{w}_p(i',j') \tag{17}$$

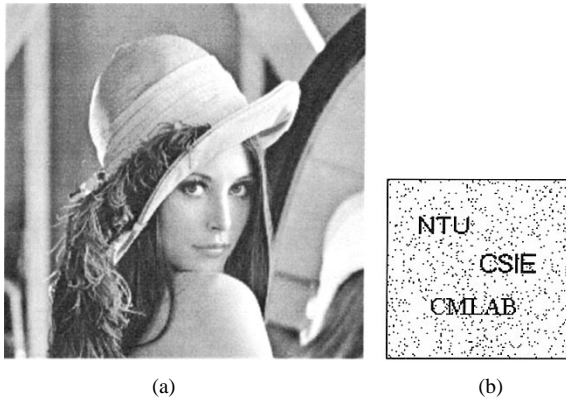where (i',j') is reverse-permuted to (i,j) according to the predefined pseudorandom order.

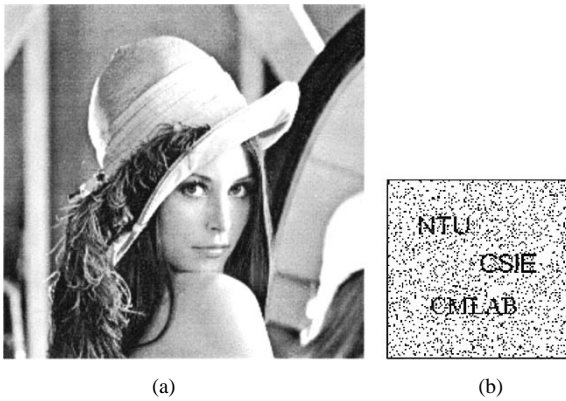Fig. 10. (a) Image enhanced version of Fig. 7(c) with slightly enhanced contrast. (b) Extracted watermark with $\mathrm{NC} = 0.9985$.

Fig. 11. (a) Image enhanced version of Fig. 7(c) with strongly enhanced contrast. (b) Extracted watermark with $\mathrm{NC} = 0.973$.

F. Similarity Measurement

In our scheme, the extracted watermark is a visually recognizable pattern. The viewer can compare the results with the referenced watermark subjectively. However, the subjective measurement is dependent on factors such as the expertise of the viewers, the experimental conditions, etc. Therefore, a quantitative measurement is needed to provide objective judgment of the extracting fidelity. We define the similarity measurement between the referenced watermark W and extracted watermark $\tilde{W}$ as

$$\text{Normalized Correlation (NC)} = \frac{\sum_i \sum_j W(i,j)\tilde{W}(i,j)}{\sum_i \sum_j [W(i,j)]^2} \tag{18}$$

which is the cross-correlation normalized by the reference watermark energy to give unity as the peak correlation.

Fig. 6 illustrates the procedures for extracting the watermarks.

IV. EXPERIMENTAL RESULTS

Fig. 7 shows an example of embedding and extracting results, where Lena is used as the test image again, and a pattern with "NTU CSIE CMLAB" is used as the watermark. Fig. 8 is another example, where the cameraman image is watermarked with Fig. 7(b).
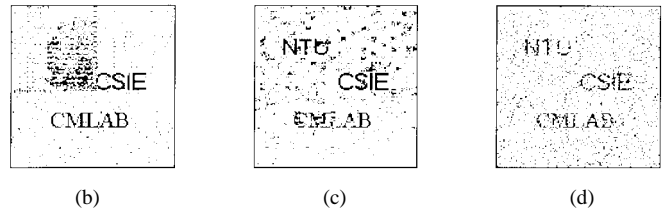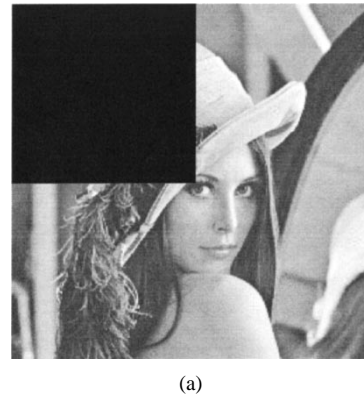

Fig. 12. (a) Quarter of an embedded image is discarded. And (b)–(d) are the extracted watermarks, where (b) is without pseudorandom permutation nor block-based image-dependent permutation ($\mathrm{NC} = 0.7922$), (c) is with only block-based permutation ($\mathrm{NC} = 0.9372$), and (d) is with both permutations ($\mathrm{NC} = 0.7623$).
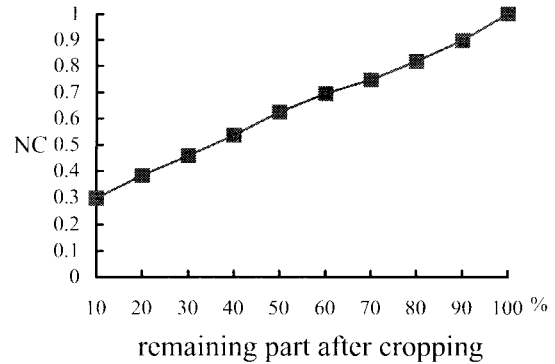

Fig. 13. Relationship between the cropping ratios and the NC values.

A. Image Processing Operation

Smoothing operations are used to diminish spurious effects which may be present in images from a poor transmission channel. Fig. 9 shows a blurred version of the watermarked image, and the extracted watermark, though interfered by noise is still recognizable.

The contrast of an image is usually adjusted to enhance the subjective quality. Figs. 10 and 11 show the results of applying slightly and strongly enhanced operations to a watermarked image accordingly. The extracted results are still highly similar to the original watermark.

B. Image Cropping Operation

During the image manipulation, the uninterested part of an image is usually cropped. As described in Section II-A, a pseudorandom permutation is performed to disperse the spatial relationship of the watermark. Therefore, it would be hard for
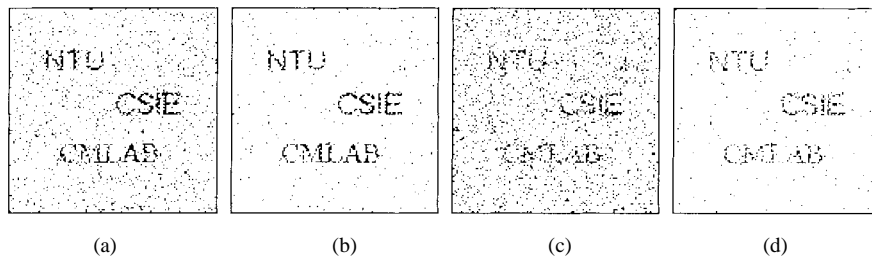
Fig. 14. Extracted watermarks of the cropped versions of Fig. 7(c). (a) A quarter of the image is cropped, and the missing portions is filled with zero values ($NC = 0.7623$). (b) A quarter of the image is cropped, and the missing portion is filled with unwatermarked image ($NC = 0.7339$). (c) Half of the image is cropped, and the missing portions is filled with zero values ($NC = 0.5964$). (d) Half of the image is cropped, and the missing portions is filled with unwatermarked image ($NC = 0.5276$).
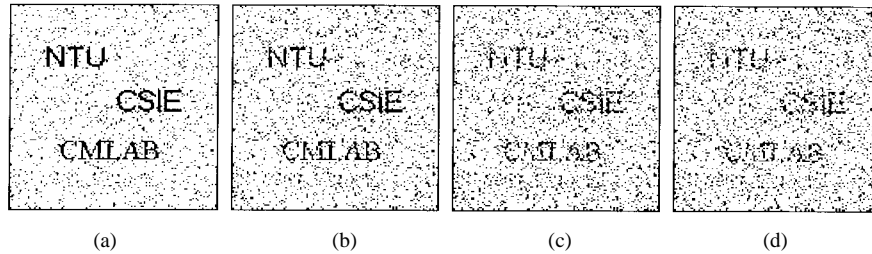

Fig. 15. Extracted watermarks of JPEG compressed version of Fig. 7(c), where (a) with compression ratio 5.92 and $NC = 0.99$, (b) with compression ratio 7.16 and $NC = 0.883$, (c) with compression ratio 8.46 and $NC = 0.726$, and (d) with compression ratio 9.05 and $NC = 0.661$.

TABLE I
CHANGES OF NC VALUES UNDER JPEG LOSSY COMPRESSION. AS THE COMPRESSION RATIO INCREASES FROM 3.49 TO 10.74, THE CORRESPONDING IMAGE QUALITY IS DROPPED FROM 33.78 dB TO 31.27 dB, AND THEREFORE, THE NC VALUES DECREASE FROM 0.999 TO 0.413, ACCORDINGLY.

	Digital watermarking under JPEG lossy compression										
Compression ratio	3.49	4.41	5.18	5.92	6.55	7.16	7.81	8.46	9.05	9.81	10.74
PSNR (dB)	33.78	35.52	34.74	33.84	33.15	32.56	32.07	31.75	31.47	31.41	31.27
NC	0.999	0.998	0.998	0.990	0.942	0.883	0.830	0.726	0.661	0.493	0.413

a "pirate" to detect or remove the watermark by cutting some part of the image. For example, in Fig. 12(a), a quarter of the watermarked image is discarded. If neither pseudorandom nor block-based image dependent permutation was applied during the embedding, the extracted watermark [as shown in Fig. 12(b)] will reveal the spatial information of the watermark embedding. However, once the permutation is introduced, the lost information will be distributed over the whole image, and the extracted error will also be distributed over the whole result. In such case, the results will be interfered with noises but will not reveal the spatial position of the watermark [as shown in Fig. 12(c) and (d)] Note that, since Fig. 12(c) is without using the pseudorandom permutation, the noises are less random then 12(d) does.

Fig. 13 shows the relationship between the similarity measurement NC and the cropping ratio. Since a pseudorandom permutation is applied, the effect of cropping operation to the NC of the extracted results is almost linear.

Fig. 14 shows the extracted results from various cropped image. Fig. 14(a) and (c) are extracted from cropped images where the missing portions are filled with zero values, and Fig. 14(b) and (d) are extracted from cropped images where the missing portions are filled with original unwatermarked images. As shown in the figure, filling with zero values in the missing portions distributes more noises over the entire results and influences the visual recognition.
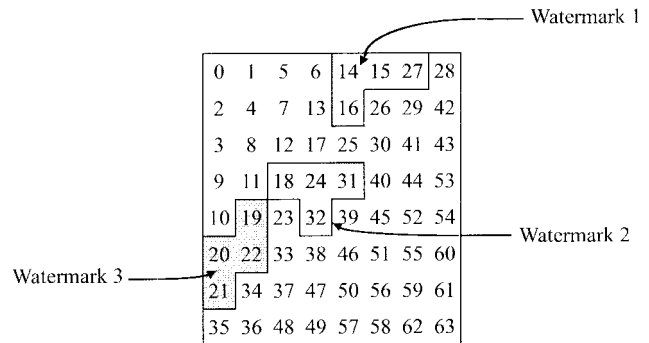

Fig. 16. If $M_1 = N_1/4$ and $M_2 = N_2/4$, then there are only four middle-frequency coefficients should be chosen for each watermark. These three watermarks would be embedded into one image with their individual user key, or identical watermark could be repeatedly embedded three times to improve the robustness.

C. JPEG Lossy Compression

Fig. 15 shows the extracted results from JPEG compressed version of the watermarked images with compression ratio 5.92, 7.16, 8.46, and 9.05. The quantization table in Fig. 4(a) is used as the referenced quantization values as described in Section II-E. Table I shows that as the compression ratio increases, the NC value decrease accordingly. Therefore, as the compression ratio are high enough to quantize DCT coefficients very coarsely, the watermark will be destroyed and
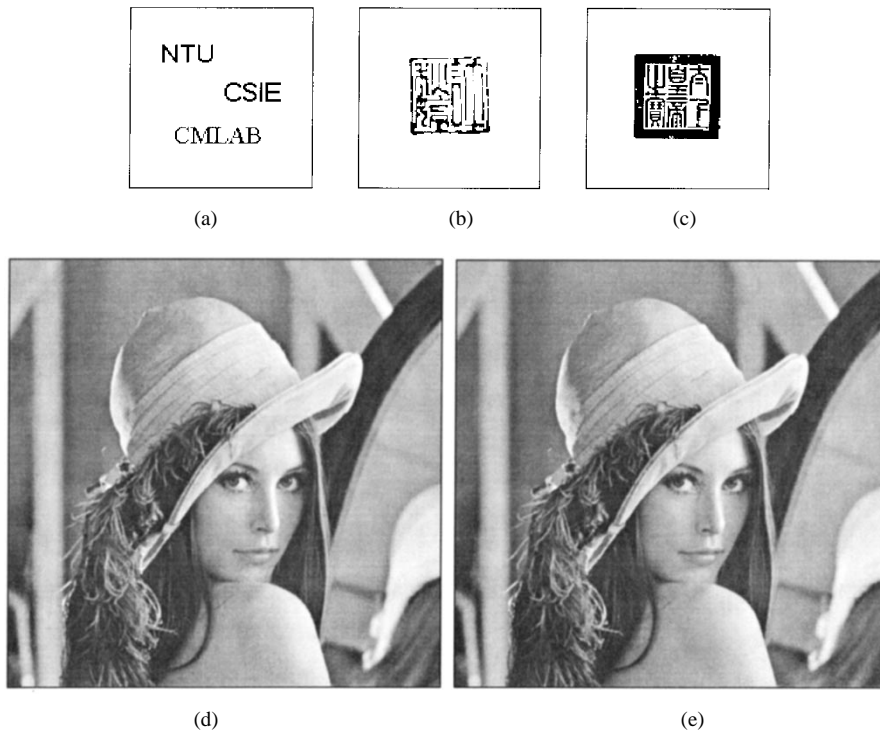
(a)   (b)   (c)

(d)   (e)

Fig. 17. Example of multiple watermarking using three watermarks with size 128×128 as shown in (a), (b), and (c) as watermarks 1–3 of Fig. 16 accordingly, where (d) is the host image with size of 512×512, and (e) is the multiple-watermarked image with PSNR = 39.48 dB.

become indiscernible. However, in this situation, the quality of the JPEG compressed image (without being watermarked) will be degraded severely so that the processes of digital watermarking become less meaningful.

V. DISCUSSION

A block DCT-based watermarking technique for images is proposed in this work. There are some issues are worthy of giving further discussion as follows.

A. Image Dependent Permutation

In Section II-B, a block-based image-dependent permutation according to the characteristics of both the image and watermark is used in our work. Although the watermark is embedded into the middle-frequency coefficients, for those blocks with little variances (i.e., the blocks containing low frequency contents), the modification of DCT coefficients will introduce visible artifacts. To reduce the artifacts, we sort the variances of image blocks and the amount of information within each watermark block, and then map the watermark blocks with more signed pixels into those image blocks with higher variances.

However, based on our simulation, no gain of objective quality (such as PSNR) can be obtained by using these kinds of permutations. However, better subjective quality, especially for those smoother parts of the image, could be obtained.

B. User Key

A "user key" is provided as a secret key that can be used to serve various embedding processes by using the

same embedding technology. Besides, a user key is treated as a parameter during the extracting steps. In the proposed embedding method, a "user key" should defines the following issues.

1) Seed of the pseudorandom number generator:
   The seed defines the initial position of an pseudorandom permutation, which could be any one between one and $(M_1 \times M_2)$.
2) Choice of middle-frequency coefficients:
   There are $(64 \times \frac{M_1 \times M_2}{N_1 \times N_2})$ middle-frequency coefficients should be picked out in all of 64 DCT coefficients for each block. In the user key, the coefficients to be processed should be specified.
3) Mapping of the chosen coefficients into a reduced block:
   Fig. 2(b) shows one way to map the chosen coefficients. Other kinds of mapping are also possible.

C. Size of Watermarks

With visually recognizable watermarks, there are nontrivial amount of information will be embedded into the original image. Obviously, once the ratio of $(N_1 \times N_2)$ and $(M_1 \times M_2)$ becomes larger, the number of DCT coefficients involved in the embedding will be smaller. In such case, the invisibility will be improved. In addition, multiple watermarking or repeatedly embedding identical watermarks to harden the robustness is also possible. For example, if $M_1 = N_1/4$ and $M_2 = N_2/4$, then there are only four middle-frequency coefficients should be chosen from 64 coefficients for the watermark. As shown in Fig. 16, three watermarks could be embedded into an image with different user key which chooses different coefficients from the image block. Fig. 17 shows an
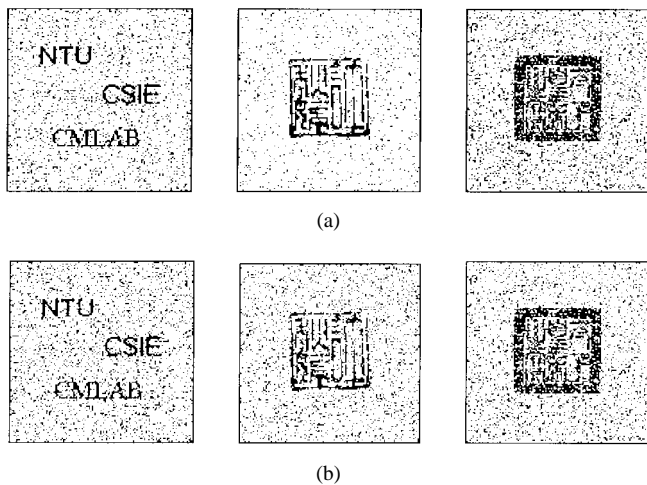
(a)

(b)

Fig. 18.   Extracted watermarks from JPEG compressed version of Fig. 17(e) with individual user keys, where (a) with compression ratio 5.58 and NC values are 0.996, 0.993 and 0.975 accordingly, and (b) with compression ratio 7.13 and NC values are 0.995, 0.983, and 0.892 accordingly.

example of multiple watermarked result from Fig. 16, and Fig. 18 shows the extracted results from JPEG compressed image of Fig. 17(e) with different user key.

VI. CONCLUSION

This paper has presented a technique for embedding digital watermark into the images. The embedding and extracting methods of the DCT-based approach have been described.

The experimental results show the proposed embedding technique can survive the cropping of an image, image enhancement and the JPEG lossy compression. By carefully defining the "user key," multiple watermarking and repeatedly embedding to harden the robustness are available. Our technique could also be applied to the multiresolution image structures with some modification about the choice of middle-frequency coefficients [13].

Other kinds of attacks, such as image resampling and image rotation, are still challenging to our current work, and have been chosen to be the major direction of our future work.

REFERENCES

[1] B. M. Macq and J. J. Quisquater, "Cryptology for digital TV broadcasting," *Proc. IEEE*, vol. 83, pp. 954–957, June 1995.
[2] W. J. Mitchell, "When is seeing believing?," *Sci. Amer.*, pp. 68–73, Feb. 1994.
[3] J. T. Brassil, S. Low, N. F. Maxemchuk, and L. O'Gorman, "Electronic marking and identification techniques to discourage document copying," *IEEE J. Select. Areas Commum.*, vol. 13, pp. 1495–1504, Oct. 1995.
[4] I. Pitas and T. H. Kaskalis, "Applying signatures on digital images," in *Proc. IEEE Nonlinear Signal and Image Processing*, June 1995, pp. 460–463.
[5] O. Bruyndonckx, J. J. Quisquater, and B. Macq, "Spatial method for copyright labeling of digital images," in *Proc. IEEE Nonlinear Signal and Image Processing*, June 1995, pp. 456–459.
[6] S. Walton, "Image authentication for a slippery new age," *Dr. Dobb's J.*, pp. 18–26, Apr. 1995.
[7] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for data hiding," *Proc. SPIE*, vol. 2420, p. 40, Feb. 1995.
[8] E. Koch and J. Zhao, "Toward robust and hidden image copyright labeling," in *Proc. IEEE Nonlinear Signal and Image Processing*, June 1995, pp. 452–455.
[9] I. J. Cox, J. Kilian, T. Leighton, and T. Shammoon, "Secure spread spectrum watermarking for multimedia," Tech. Rep. 95-10, NEC Res. Inst., Princeton, NJ, 1995.
[10] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Transparent robust image watermarking," in *Proc. ICIP'96*, pp. 211–214.
[11] B. Sklar, *Digital Communications.*   Englewood Cliffs, NJ: Prentice-Hall, 1988.
[12] W. B. Pennebaker and J. L. Mitchell, *JPEG: Still Image Data Compression Standard.*   New York: Van Nostrand Reinhold, pp. 34–38, 1993.
[13] C.-T Hsu and J.-L. Wu, "Multiresolution watermarking for digital images," *IEEE Trans. Circuits Syst. II*, vol. 45, pp. 1097–1101, Aug. 1998.
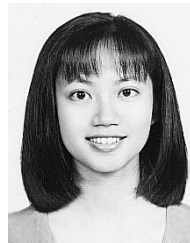
Chiou-Ting Hsu received the B.S. degree in computer and information science from National Chiao Tung University, Hsin-Chu, Taiwan, R.O.C., in 1991, and the Ph.D. degree in computer science and information engineering from National Taiwan University (NTU), Taipei, Taiwan, in 1997.

She is currently a Post-doctoral Researcher with the Communication and Multimedia Laboratory, Department of Computer Science and Information Engineering, NTU. Her research interests are in digital watermarking, multiresolution signal processing, and image/video coding.

Ja-Ling Wu (S'85–A'87–SM'98) was born in Taipei, Taiwan, on November 24, 1956. He received the B.S. degree in electronics engineering from Tam-Kang University, Tam-Shoei, Taiwan, R.O.C., in 1979, and the M.S. and Ph.D. degrees in electrical engineering from Tatung Institute of Technology, Taipei, in 1981 and 1986, respectively.

From August 1986 to July 1987, he was an Associate Professor in the Department of Electrical Engineering, Tatung Institute of Technology. He became an Associate Professor at the Department of Computer Science and Information Engineering, National Taiwan University, Taipei, in August 1987, and a Professor in August 1990. Since August 1996, he has been with National Chi-Nan University, Puli, Taiwan, as the Chairman of the Department of Information Engineering. He currently teaches courses in digital signal processing and multimedia data compression and conducts research in the areas of signal processing, image/video coding, and digital watermarking techniques. He has authored more than 150 technical papers in these areas.

Dr. Wu received the Outstanding Research Award of the National Science Council of the Republic of China from 1987 to 1994, the Outstanding Youth Medal of the Republic of China in 1989, the Award for 1993 R.O.C. Distinguished Information People of the Year, the Special Long-Term Award for Collaboratory Research, sponsored by the Acer Corporation in 1994, the Best Paper Award for the R.O.C. Association of Image Processing and Multimedia Applications in 1995, and the Long-Term Medal for Ten Distinguished Researchers in 1996.