AN ADAPTIVE DIGITAL IMAGE WATERMARKING TECHNIQUE FOR COPYRIGHT PROTECTION

Chang-Hsing Lee[1] and Yeuan-Kuen Lee[2]

Department of Computer Science, Chinese Culture University[1]
55 Hwa Kang Rd., Yang Ming Shan, Taipei, Taiwan 11114

Department of Computer and Information Science[2]
National Chiao Tung University
1001 Ta Hsush Rd., Hsinchu, Taiwan 30050

Abstract- An adaptive digital image watermarking technique is proposed in this paper. The proposed method exploits the sensitivity of human eyes to adaptively embed a visually recognizable watermark in an image without affecting the perceptual quality of the underlying host image. In addition, the watermark will still be present if some lossy image processing operations such as low-pass filtering, median filtering, resampling, requantization, and lossy JPEG image compression are applied to the watermarked image. Experimental results show the effectiveness of the proposed watermarking method.

Index Terms- copyright protection, digital watermarking, JPEG compression

I. INTRODUCTION

The rapid evolution of the Internet makes easier the transmission of digital multimedia content such as text, audio, image, and video. Digital media can be accessed or distributed through the network. As a result, replications of digital media are simple with no loss of fidelity, that is, the copy of a digital medium is identical to the original one. Through the network, an unlimited number of identical copies of digital media can be illegally produced, this is a serious threat to the intellectual property rights of the media owner. Therefore, to protect and enforce intellectual property rights of the media owner is an important issue in the digital world.

To protect digital media, traditional encryption algorithms such as DES or RSA are widely adopted [1, 2]. In these encryption algorithms, the digital media is encrypted into scrambled data using a predetermined encryption key (private key or public key). The encryption algorithms hide the meaning of the original media. An opponent who accesses the encrypted data does not know what the original message is. Only the holder who knows the correct decryption key can decrypt the encrypted data and recover the original media. However, the decrypted media, which is identical to the original one, may be illegally distributed or copied. The digital watermarking technique provides a good way to solve this issue. A digital watermark can be used to claim the ownership of the digital media and protect the intellectual property rights of the media creator or owner.

The digital watermarking technique embeds a digital signature or digital watermark, which asserts the ownership or intellectual property rights of the media creator or owner, in the digital media such as text, audio, image, and video. The watermark can then be extracted from the watermarked media and is used to identify the author or distributor of the media. The principle of digital watermarking is the robust and secret embedding of copyright information in a digital medium. To be really effective for copyright enforcement, a digital watermarking technique must satisfy the following requirements:

(1) *Perceptual transparency*

The embedded watermark must be perceptually invisible or inaudible to maintain the quality of the host media under typical perceptual conditions. That is, human observers cannot distinguish the original host media from the watermarked media. As a result, the existence of the watermark is hidden to human observers.

(2) *Unambiguity*

The retrieval of a watermark should unambiguously identify the owner. In addition,

* This research was supported in part by the National Science Council of R. O. C. under contract NSC87-2218-E-034-001.
Contributed Paper

Manuscript received April 5, 1999

the accuracy of owner identification should degrade gracefully under attacks.

(3) *Robustness*

As a watermark is used to identify the owner of digital media, removal of the embedded watermark should be difficult for an attacker or any unauthorized user. In practice, any watermark can be removed if sufficient knowledge about the process of watermark insertion is known. However, if only partial information is available, attempting to remove or destroy the watermark should produce a remarkable degradation in media quality before the watermark is lost. In general, lossy signal processing operations that damage the watermarked media may also damage the watermark. Therefore, the watermark must still be present if the watermarked media are processed by some common signal processing operations. These operations include resampling, requantization, lossy compression (e.g., JPEG, MPEG, wavelet compression), linear filtering (e.g., low-pass and high-pass filtering), nonlinear filtering (e.g., median filtering), geometric distortions (e.g., scaling, translation, rotation, and cropping), as well as digital-to-analog and analog-to-digital conversion. In general, the robustness often conflicts with transparency requirement. To be robust, a watermark should be embedded in perceptually significant regions of the host media. On the other hand, to be transparent to human observers, a watermark should be embedded in perceptually insignificant regions of the host media. Therefore, to propose a transparent and robust watermarking scheme is an impediment to many researchers.

(4) *Tamper-resistance*

The embedded watermark must be resistant to tampering through collusion by comparing multiple copies of the media embedded with different watermarks.

A transparent and robust digital image watermarking approach is proposed in this paper. The embedded watermark is invisible to human eyes and is robust if the watermarked image is processed by some lossy image processing operations, such as low-pass filtering, median filtering, resampling, requantization and JPEG image compression. In the next section, we will give a survey of existing watermarking methods. The proposed digital image watermarking approach is described in Section 3. In Section 4, we present the experimental results and show the robustness of the proposed approach. Finally, a brief conclusion and discussion is presented in Section 5.

II. PREVIOUS WORKS

In this section, we will give a review on digital image watermarking techniques. A detailed review on multimedia data embedding and watermarking techniques can also be found in [3, 4]. The digital image watermarking techniques can be classified into two categories: spatial-domain techniques (spatial watermarks) [5-14] and frequency-domain techniques (spectral watermarks) [15-26]. The spatial-domain techniques directly modify the intensities or color values of some selected pixels while the frequency-domain techniques modify the values of some transformed coefficients.

The simplest spatial-domain image watermarking technique is to embed a watermark in the least significant bits (LSBs) of some randomly selected pixels [3-5]. The watermark is actually invisible to human eyes. However, the watermark can be easily destroyed if the watermarked image is low-pass filtered or JPEG compressed. To increase the security of the watermark, Matsui and Tanaka [6] proposed a method that uses a secret key to select the locations where a watermark is embedded, e.g., the use of a pseudo-random number generator to determine the sequence of locations on the image plane. Voyatzis and Pitas used a toral automorphism [7] approach to scramble the digital watermark before it is inserted into an image. To increase the robustness of the watermark, many approaches have been proposed to modify some properties of selected pixels or blocks [8-14]. Wolfgang *et al.* reshaped an m-sequence into two-dimensional watermark blocks, which are added and detected on a block-by-block basis [8]. Pitas proposed a method that shifts some pixel values for data embedding [9, 10]. In his method, a digital watermark S is a specific binary pattern of size $N \times M$ where the number of 1's equals the number of 0's.

Depending on the binary pattern of *S*, the gray scale image *I* is split into two subsets, *A* and *B*, of equal size $P=N\times M/2$. The intensities of pixels in subset *A* are added by a quantity *k* while the intensities of pixels in subset *B* are not altered. Bryundonckx *et al.* proposed a block-based spatial watermarking method that modifies the average luminance value of a block [11, 12]. An image is first decomposed into a set of $n\times n$ blocks. A key is used to determine the embedding blocks or locations. Each block is classified into one of the three types of contrast: hard, progressive, and noise contrast. The pixels in a block are assigned to one of two zones, zone 1 and zone 2. Each zone is further divided into two categories: *A* and *B*. The division is based on a grid determined by the coder. Embedding of a bit *b* is performed based on the following embedding rule:

$$\begin{aligned} \text{if } b=0: \quad & {m_{1B}}^{*} - {m_{1A}}^{*} = L \\ & {m_{2B}}^{*} - {m_{2A}}^{*} = L \\ \text{if b=1:} \quad & {m_{1A}}^{*} - {m_{1B}}^{*} = L \\ & {m_{2A}}^{*} - {m_{2B}}^{*} = L, \end{aligned}$$

where ${m_{1B}}^{*}$, ${m_{1A}}^{*}$, ${m_{2B}}^{*}$, and ${m_{2A}}^{*}$ are the average luminance values after embedding a bit *b* and *L* is the embedding level. Kutter *et al.* proposed an amplitude modulation approach for color images watermarking [13]. The locations, where the watermark is embedded, are determined by using a secret key. The watermark bits are embedded in the blue channel since the human visual system (HVS) is relatively less sensitive to this color information. A single bit *s* is embedded in a pseudo-randomly selected pixel at location (*i*, *j*) by modifying the blue channel *B* by a fraction of the luminance *L* as:

$$B_{i,j} \leftarrow B_{i,j} + q(2s-1)L_{i,j},$$

where *q* is a constant value used to determine the strength of the signature and is selected to optimize robustness and invisibility. Darven and Scott proposed a fractal-based steganographic method to embed binary messages [14]. Fractal analysis is first used to identify similar blocks. The set of similar blocks is then divided into two categories. To embed a "0" bit, the blocks in the first category are used. On the contrary, to embed a "1" bit, the blocks in the second category are used.

The frequency-domain techniques first transform an image into the frequency domain coefficients. The transformation may be Fourier transform [15], DCT [16-23], or wavelet transform [24-26], etc. The watermark is then embedded in the transformed coefficients according to the perceptual significance of the transform coefficients. Therefore, the watermark is irregularly distributed over the entire image. Finally, the coefficients are inverse-transformed to form the watermarked image, which is identical to the original image. As a result, the watermark is invisible for an enemy to decode or to read and is more robust to some image processing operations. O'Ruanaidh *et al.* [15] embedded the watermark in the phase information in the discrete Fourier transform domain since the phase distortion is more sensitive to human visual system than the magnitude distortions. Therefore, it is more robust to tampering when compared to magnitude modulation. Cox *et al.* [17] proposed a secure spread spectrum watermarking method for embedding a watermark in the DCT domain. In the algorithm, the watermark is inserted in the perceptual significant portion of the image in order to provide greater robustness. The watermark *W* is a sequence of normally distributed, zero-mean and unit-variance random numbers. That is, $W = (w_1, w_2, \ldots, w_n)$, where each w_i is chosen according to $N(0, 1)$. A DCT is first performed on the entire image and the coefficients with the largest magnitudes are identified as the perceptually significant portion of the image. Then, the watermark is inserted into these selected coefficients by setting each frequency coefficient C_i as:

$$C_i \leftarrow C_i\,(1 + w_i\alpha_i),$$

where α_i is a scalar factor. Finally, the inverse DCT of the watermarked coefficients will form a transparently watermarked image. Both the original and watermarked images are needed to extract the embedded watermark. A similarity measure is then used to compare the extracted watermark with the original one to test whether a watermark is present in the image. The results show that the technique is effective in terms of transparency and robustness. A block-based DCT watermarking approach was proposed by Hsu and Wu [18-20]. The watermark is a visually recognizable pattern such as an image of a seal with Chinese characters. An image is first divided into blocks and DCT is performed on each block. The watermark is then embedded by selectively modifying the middle-frequency DCT coefficients. Since the embedded watermark is an image, human eyes can easily identify the extracted watermark. They claim that the watermarked image is robust to general image operations and lossy JPEG compression. Tang and Aoki [21] also proposed a block-based middle-band embedding algorithm, which is similar to [18-20]. A differential pulse code modulation is used to permute a watermark image. Similar to some methods [16, 22, 23], their approach expolits the characteristics of human visual system in the embedding process. The aim is to insert more embedding bits where they are most robust to attack and are least noticeable.

Ohnishi and Matsui embedded a watermark in the Harr wavelet transform domain [24]. To embed the watermark, one is added or subtracted from some selected transform coefficients. Xia *et al.* introduced a multiresolution watermarking method for digital images based on digital wavelet transform [25]. In the method, a watermark $W(m, n)$ is a Gaussian noise with zero-mean and unit-variance. The watermark is inserted into the large coefficients at the high and middle frequency bands of an image according to the following equation:

$$\boldsymbol{I}^{w}_{l,f}(m, n) = \boldsymbol{I}_{l,f}(m, n) + \alpha\, [\boldsymbol{I}_{l,f}(m, n)]\; W(m, n),$$

where $\boldsymbol{I}_{l,f}(m, n)$ and $\boldsymbol{I}^{w}_{l,f}(m, n)$ refer to the original and watermarked wavelet coefficients at position (m, n) in resolution level l and frequency orientation f, and α is a constant that is maximized under the transparency constraints. Kunder and Hatzinakos used multiresolution fusion techniques and incorporated a model of the human visual system to embed a watermark [26].

In general, a spatial-domain watermarking method has larger capacity than that of a frequency-domain method. That is, more data can be embedded in the spatial domain than in the frequency domain. However, data embedded in the frequency domain is more robust to common image processing operations. Therefore, there is a trade-off between the capacity and robustness. Most of the watermarking algorithms use a serial number, a set of normally distributed random numbers, a Gaussian distribution, or an author ID as a watermark. In these algorithms, a quantitative measure is required to verify the extraction results. Usually a similarity, q, between the original watermark and extracted watermark is computed. The value of q is then tested against a threshold T. If $q > T$, it is assumed that the image is watermarked, otherwise the image has no watermark. However, the determination of the threshold value T produces ambiguity. A small value of T will accept the existence of a watermark although there is none. On the other hand, a large value of T will reject the existence of a watermark although there is one. Therefore, how to decide a proper threshold value becomes a serious problem. A better solution is to use a visually meaningful watermark (e.g., a small image) [18-20]. Human eyes can then easily verify the extraction results. However, a large quantity of data must be embedded in the host image if a visually meaningful watermark is adopted. Thus the embedding algorithm must adapt its insertion strategy to accommodate a large quantity of data in the host image.

As described above, to provide larger capacity for watermark insertion, a spatial-domain watermarking method is preferable. In fact, embedding a watermark in the least significant bits of a pixel is less sensitive to human eyes. However, the watermark will be destroyed if some common image operations such as low-pass filtering are applied to the watermarked image. Therefore, to make the embedded watermark more resistant to any attack, the watermark must be embedded in the most significant bits. However, this will introduce more distortion to the host image and conflicts with the invisible requirement. To meet both invisibility and robustness, we will propose a method that adaptively modifies the intensities of some selected pixels as much as possible and this modification is not noticeable to human eyes.

In next section, we will describe an adaptive image watermarking approach. The proposed approach utilizes the sensitivity of the human visual system to adaptively modify the intensities of some pixels in a block. The modification of pixel intensities depends on the content of a block. If the contrast of the block is large, the intensities can be changed greatly without introducing any distortion. On the other hand, if the contrast is small, the intensities can only be changed slightly.

III. THE PROPOSED APPROACH

In this section, we will describe the proposed adaptive image watermarking technique. The watermark used is a visually recognizable binary image rather than a randomly generated sequence of bits. Thus, human eyes can easily identify the extracted watermark. The proposed technique adaptively modifies the intensities of some selected pixels as much as possible and the modification is not noticeable to human eyes. In addition, to prevent tampering or unauthorized access, the watermark is first permuted into scrambled data. The block diagram of the proposed watermarking system is depicted in Fig. 1. In the following subsections, we will first give the permutation algorithm, and then describe the watermark embedding and extraction processes.

A. Watermark Permutation Algorithm

To prevent the watermark from tampering or unauthorized access by attackers, the watermark image is first permuted to be scrambled data before insertion. The watermark permutation strategy is the same as that proposed in [20]. A two-dimensional pseudo-random number traversing method is used to permute the watermark. Let $\mathbf{W}$ and $\mathbf{W}_p$ be the original and permuted watermark image, that is,

$$\mathbf{W}_p = \{w_p(i,j)=w(i',j') \mid 0 \le i,i' < M \text{ and } 0 \le j,j' < N\},$$

where pixel at (i',j') is mapped to pixel at (i,j) in a pseudo-random order, M and N are the height and width of the watermark image, respectively. The permutation algorithm is implemented as follows:

Step 1: Number each pixel from 0 to ($M \times N$-1) in a raster scan order of the image.

Step 2: Generate a sequence of ($M \times N$) random numbers between 0 and ($M \times N$-1) using linear feedback shift register [28]. Each pixel p is then mapped to a random value q.

Step 3: Replace the pixel value of p with q.

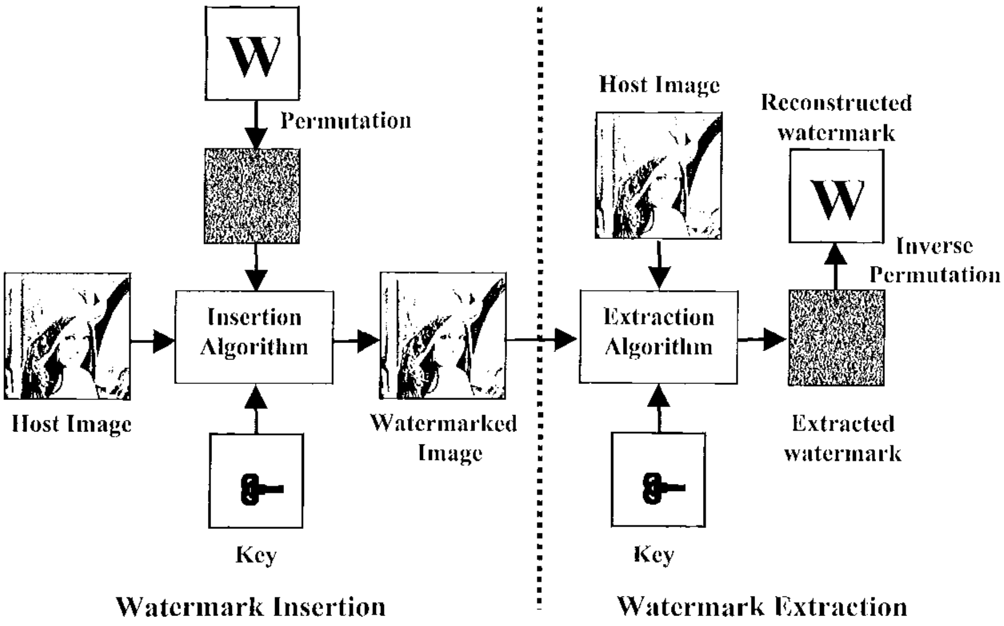


Fig. 1 A block diagram of the proposed watermarking system.

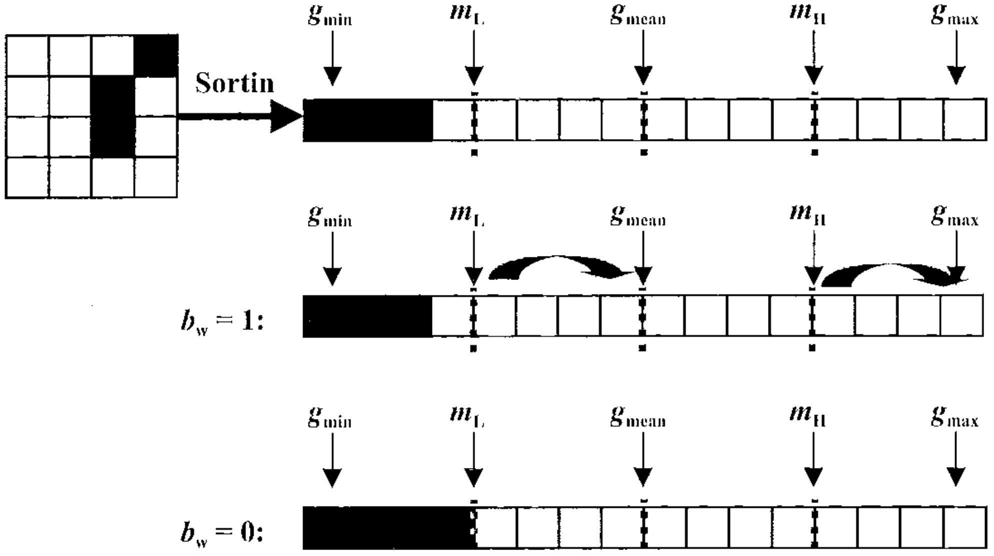


Fig. 2 An illustration of the rules for pixel intensity.

B. Watermark Embedding

After the binary watermark image is permuted, the scrambled data sequence is then inserted into the host image. The embedded watermark must be invisible to human eyes and robust to most image processing operations. To meet these requirements, a bit of pixel value (0 or 1) is embedded in a block of the host image. Depending on the contrast of the block, pixels in this block are adaptively modified to maximize robustness and guarantee invisibility. Before insertion, the host image is first decomposed into blocks of size $n \times n$. The position or block for embedding is selected by a pseudo-random number generator using a seed value k. The value of k is similar to the secret key of a secure DES system. Let **B** be a selected block, the watermark insertion method is described as follows:

Step 1: Sort the pixels in block **B** in an ascending order of pixel intensities.

Step 2: Compute the average intensity g_{mean}, maximal intensity $g_{\max}$, and minimal intensity $g_{\min}$ of the block. That is,

$$g_{\text{mean}} = \frac{1}{n^2}\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} b_{ij},$$

$$g_{\max} = \max\,(b_{ij},\ 0 \le i, j < n), \text{ and}$$

$$g_{\min} = \min\,(b_{ij},\ 0 \le i, j < n),$$

where b_{ij} represents the intensity of the (i, j)-th pixel in block **B**.

Step 3: Classify every pixel in **B** into one of the following categories by using g_{mean}:

$$b_{ij} \subset \boldsymbol{Z}_H \quad \text{if } b_{ij} > g_{\text{mean}}$$

$$b_{ij} \in \boldsymbol{Z}_L \quad \text{if } b_{ij} \le g_{\text{mean}},$$

where $\boldsymbol{Z}_H$ and $\boldsymbol{Z}_L$ represent high-intensity category and low-intensity category, respectively.

Step 4: Compute the mean values, m_H and m_L, of these two categories.

Step 5: Define the contrast value of block **B** as

$$C_B = \max(C_{\min},\ \alpha(g_{\max} - g_{\min})),$$

Where α is a constant, and $C_{\min}$ is a constant value which determines the minimal value a pixel should be modified.

Step 6: Assuming that the embedded value b_w is 0 or 1. Modify the pixel values in block **B** according to the following rules:

if $b_w = 1$:

$$\begin{array}{ll} g' = g_{\max} & \text{if } g > m_H, \\ g' = g_{\text{mean}} & \text{if } m_L \le g < g_{\text{mean}}, \\ g' = g + \delta & \text{otherwise}, \end{array}$$

if $b_w = 0$:

$$\begin{array}{ll} g' = g_{\min} & \text{if } g < m_L, \\ g' = g_{\text{mean}} & \text{if } g_{\text{mean}} \le g < m_H, \\ g' = g - \delta & \text{otherwise}, \end{array}$$

where g' is the modified intensity and δ is a randomly generated value between 0 and C_B. Fig. 2 depicts the modification of pixel intensities according to the rules described above.

The embedding of the watermark bit depends on the content of each block. If the block is of larger contrast, the intensities of pixels will be changed greatly. Otherwise, the intensities are tuned slightly. In the extreme case, if a smooth block, where all the pixels have the same pixel intensity, is chosen for data embedding, the pixel intensities will be tuned by a small randomly generated value. This modification can avoid the blocking artifact since the pixel intensities are added or subtracted by some randomly generated values instead of a constant value. Thus the pixel intensities can be adaptively modified depending on the contrast of a block. Let block **B** and **B′** denote the original and modified blocks, respectively. The sum of pixel intensities of **B′** will be larger than that of **B** if the inserted watermark pixel value b_w is 1. On the contrary, if the inserted watermark pixel value b_w is 0, the sum of pixel intensities of **B′** will be smaller than that of **B**.

C. Watermark Extraction

The extraction of a watermark is similar to the embedding process while in a reverse order. In the proposed algorithm, the extraction of a watermark must refer to the original host image. First, we use the seed value, k, to get a sequence of positions or blocks where the watermark is embedded. For each selected position, let **B** and **B′** represent the corresponding blocks of the original host image and watermarked image, respectively. Compute the sum of pixel intensities, S_o and S_w, of **B** and **B′**. The retrieved watermark bit value b_w is determined by comparing S_o and S_w:

$$b_w = 1 \quad \text{if } S_w > S_o,$$
$$b_w = 0 \quad \text{otherwise.}$$

The extracted watermark bit values, b_w's, are then inversely permuted to get the reconstructed watermark.

IV. EXPERIMENTAL RESULTS

In the experiments, the host image is of size 512×512 with 256 gray levels. The watermark is a visually recognizable binary image of size 128×128. Figs. 3(a) and 3(b) show a 512×512 host image and a 128×128 binary watermark image, respectively. Fig. 3(c) shows the watermarked image that is derived by embedding the watermark in the host image. From Figs. 3(a) and 3(c), we can see that these two images look almost the same. Fig. 3(d) shows the reconstructed watermark, we can see that it is the same as Fig. 3(b). The similarity between these two images is quantitatively measured by the normalized cross correlation [18] defined as:

$$NC = \frac{\sum_i \sum_j W_{ij} W'_{ij}}{\sum_i \sum_j [W_{ij}]^2},$$

where W_{ij} and W'_{ij} represent the pixel values at location (i, j) in the original and extracted watermark images, respectively.

To show the robustness of the proposed algorithm under common image processing operations, we have processed the watermarked image using the following operations: linear low-pass filtering, median filtering, resampling, requantization, and lossy JPEG compression. Fig. 4(a) shows the result of applying a linear low-pass filtering to the watermarked image. The filter is a neighborhood averaging operation with a mask of size 3×3. Fig. 4(b) shows the extracted watermark from Fig. 4(a). The normalized cross correlation value NC between the extracted watermark and original one is 0.9658. Fig. 5(a) shows the result of applying a 3×3 neighborhood median filtering to the watermarked image. The extracted watermark is shown in Fig. 5(b). The normalized cross correlation value NC is 0.8879. From Figs. 4(b) and 5(b), we can easily verify the existence of the watermark although there is some distortion in the extracted watermark.

Fig. 6(a) shows the result of applying resampling operation to the watermarked image. The watermarked is first scaled to be 1/4 of its original size by using a 2×2 subsampling operation. Then the subsampled image is interpolated to the size of the original one. Fig. 6(b) shows the extracted watermark from Fig. 6(a). The normalized cross correlation value NC is 0.9891. Fig. 7(a) shows the result of applying requantization operation to the watermarked image. The watermarked image with 256 gray levels is requantized to be of 32 gray levels. The extracted watermark from this 32-level image is shown in Fig. 7(b). The normalized cross correlation value is 0.9475. From Figs. 6(b) and 7(b), we can see that the extracted watermark is almost the same as the original one. Thus, the proposed method is very robust to image resampling and requantization.

To show the robustness of the proposed algorithm under lossy JPEG compression, we first compress the watermarked image and then extract the watermark from the compressed image. Fig. 8(a) shows the compressed image with a compression ratio (*CR*) of 7.27. The extracted watermark is shown in Fig. 8(b). The normalized cross correlation value *NC* is 0.9929. Fig. 8(c) shows the compressed image with a compression ratio (*CR*) of 14.39. The extracted watermark is shown in Fig. 8(d). The normalized cross correlation value *NC* is 0.9103. Fig. 9 compares the normalized cross correlation values for different JPEG compression ratios. From this figure, we can see that the normalized cross correlation values range from 0.9103 for a high JPEG compression ratio to 0.9998 for a low image compression ratio.

From the above experimental results, we can see that the extracted watermarks can be easily used to identify the owner of the host image since it is a visually recognizable binary image. In addition, the proposed algorithm is robust to common image processing operations such as low-pass filtering, median filtering, resampling, requantization, and lossy JPEG compression.

V. CONCLUSIONS

In this paper, we have proposed an adaptive watermarking algorithm for images. The watermark adopted in this paper is a visually meaningful image such that human eyes can easily judge the extraction result. To embed a watermark in the host image, the proposed approach utilizes the sensitivity of human visual system to adaptively modify the contents of a set of blocks. The pixel intensities in a block are changed adaptively depending on the contrast of the block. The modification of pixel intensities depends on the content of a block. If the contrast of the block is large (e.g., an edge block), the intensities can be changed greatly without introducing any distortion. On the other hand, if the contrast is small (e.g., a smooth block), the intensities can only be tuned slightly. Experimental results show that the proposed algorithm is robust to common image processing operations such as low-pass filtering, median filtering, resampling, requantization, and lossy JPEG compression.

REFERENCES

[1] B. Schneier, *Applied Cryptography*, 2nd Edition, John Wiley & Sons, 1996

[2] D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press, 1995.

[3] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data-embedding and watermarking technologies", *Proceedings of the IEEE*, Vol. 86, No. 6, pp. 1064-1087, June 1998,

[4] W. Bender, D. Gruhi, N. Morimoto, and A. Lu, "Techniques for data hiding", *IBM Systems Journal*, Vol. 35, Nos. 3&4, pp. 313-335, 1996.

[5] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark", in *Proceedings of ICIP'94*, Vol. 1, pp. 86-90, 1994.

[6] K. Matsui and K. Tanaka, “Video-steganography: how to embed a signature in a picture”, in *Proceedings of IMA Intellectual Property*, Vol. 1, No. 1, pp. 187-206, Jan. 1994.

[7] G. Voyatzis and I. Pitas, "Applications of toral automorphisms in image watermarking", in *Proceedings of ICIP'96*, Vol. 2, pp. 237-240, 1996.

[8] R. B. Wolfgang and E. J. Delp, "A watermark for digital images", in *Proceedings of ICIP'96*, Vol. 3, pp. 219-222, 1996.

[9] I. Pitas, "A method for signature casting on digital images", in *Proceedings of ICIP'96*, Vol. 3, pp. 215-218, 1996.

[10] I. Pitas, "A method for watermark casting on digital images", *IEEE Transaction on Circuits and Systems for Video Technology*, Vol. 8, No. 6, pp. 775-780, Oct. 1998.

[11] O. Bruyndonckx, J. J. Quisquater, and B.

Macq, "Spatial method for copyright labeling of digital images", in *Proceedings of IEEE Nonlinear Signal Processing Workshop*, pp. 456-459, 1995.

[12] V. Darmstaedter, J.-F. Delaigle, J. J. Quisquater, and B. Macq, "Low cost spatial watermarking", *Computer and Graphics*, Vol. 22, No. 4, pp. 417-424, 1998.

[13] M. Kutter, F. Jordan and F. Bossen, "Digital watermarking of color images using amplitude modulation", *Journal of Electronic Imaging*, Vol. 7, No. 2, pp. 326-332, April 1998.

[14] P. Davern and M. Scott, "Fractal based image steganography", in *Proceedings of First International Workshop on Information Hiding*, pp. 279-294, 1997.

[15] J J K. O'Ruanaidh, W J. Dowling, and F M. Boland, "Phase watermarking of digital images", *in Proceedings of ICIP'96*, Vol. 3, pp. 239-242, 1996.

[16] J J K. O'Ruanaidh, W J. Dowling, and F M. Boland, "Watermaking digital images for copyright protection", *IEE Proceedings: Vision, Image & Signal Processing*, Vol. 143, No. 4, pp. 250-256, Aug. 1996.

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

[18] C.-T. Hsu and J.-L. Wu, "Hidden signatures in images", in *Proceedings ICIP'96*, pp. 223-226, 1996.

[19] C.-T. Hsu and J.-L. Wu, "DCT-based watermarking for video", *IEEE Transactions on Consumer Electronics*, Vol. 44, No. 1, pp. 206-216, Feb. 1998.

[20] C.-T. Hsu and J.-L. Wu, "Hidden digital watermarks in images", *IEEE Transactions on Image Processing*, Vol. 8, No. 1, pp. 58-68, 1999.

[21] W. Tang and Y. Aoki, "A DCT-based coding of images in watermarking", in *Proceedings of the International Conference on Information, Communications and Signal Processing*, Vol. 1, pp. 510-512, 1997.

[22] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Transparent robust image watermarking", in *Proceedings of ICIP'96*, Vol. 3, pp. 211-214, 1996.

[23] C. Podilchuk and W. Zeng, "Digital image watermarking using visual models", in *Proceedings of SPIE/IS&T Electronic Imaging'97: Human Vision and Electronic Imaging*, Vol. 3022, pp. 310-321, Feb. 1997.

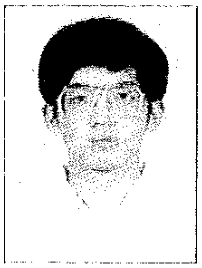
[24] J. Ohnishi and K. Matsui, "Embedding a seal into a picture under orthogonal wavelet transform", in *Proceedings of Multimedia*, pp. 514-521, 1996.

[25] X.-G. Xia, C. G. Boncelet, and G. R. Arce, "A multiresolution watermark for digital images", in *Proceedings of ICIP'97*, Vol. 3, pp. 548-551, 1997.

[26] D. Kundur and D. Hatzinakos, "A robust digital image watermarking method using wavelet-based fusion", in *Proceedings of ICIP'97*, Vol. 1, pp. 544-547, 1997.

[27] T. A. Wilson, S. K. Rogers, and L. R. Myers, "Perceptual based hyperspectral image fusion using multiresolution analysis", *Optical Engineering*, Vol. 34, No. 11, pp. 3154-3164, Nov. 1995.

[28] B. Sklar, *Digital Communications: Fundamentals and Applications*, Prentice-Hall, 1988.



Chang-Hsing Lee was born on July 24, 1968 in Tainan, Taiwan, Republic of China. He received the B.S. and Ph.D. degrees in Computer and Information Science from National Chiao Tung University in 1991 and 1995, respectively. He was a second lieutenant during his compulsory military service in the Chung Cheng Institute of Technology from 1995 to 1997. Since 1997 he has been an Assistant Professor in the Department of Computer Science, Chinese Culture University, Taipei, Taiwan. His main research interests include image processing, multimedia data compression, neural networks and digital watermarking.

Yeuan-Kuen Lee received both the B.S. and M.S. degrees in Computer and Information Science from National Chiao Tung University, in 1989 and 1991, respectively. From September 1993 to July 1995 he worked as a lecture in the Tamsui Oxford University College, Taipei. He is currently a Ph.D. student in the Department of Computer and Information Science at National Chiao Tung University. His research interests include image processing, image cryptography, and data hiding.

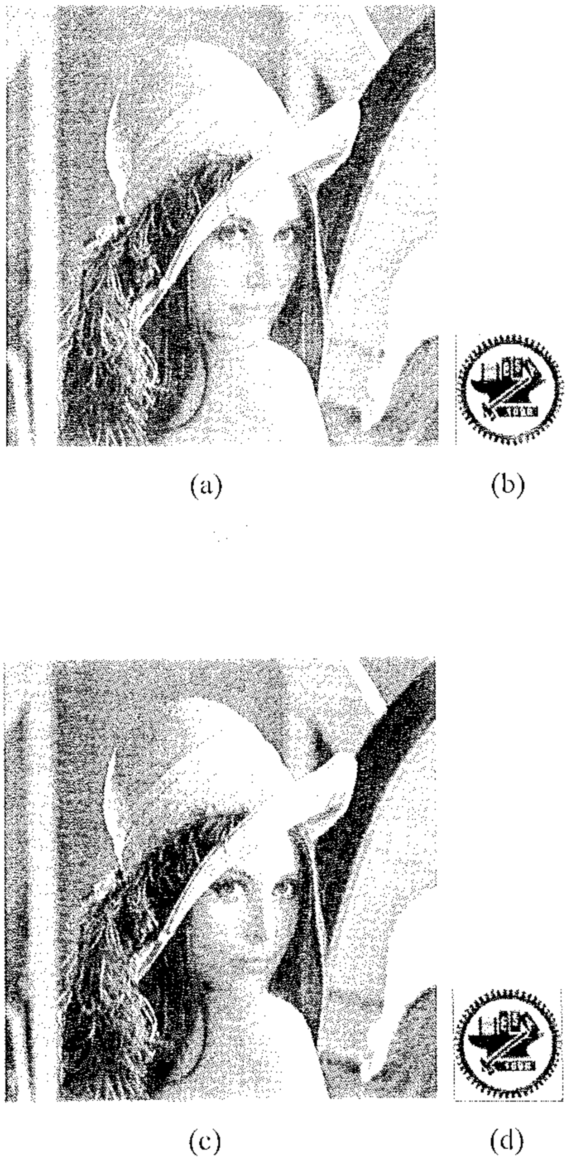


Fig. 3 An example to illustrate the proposed method. (a) Host image of size 512×512. (b) Binary watermark image of size 128×128. (c) Watermarked image. (d) Extracted binary watermark.

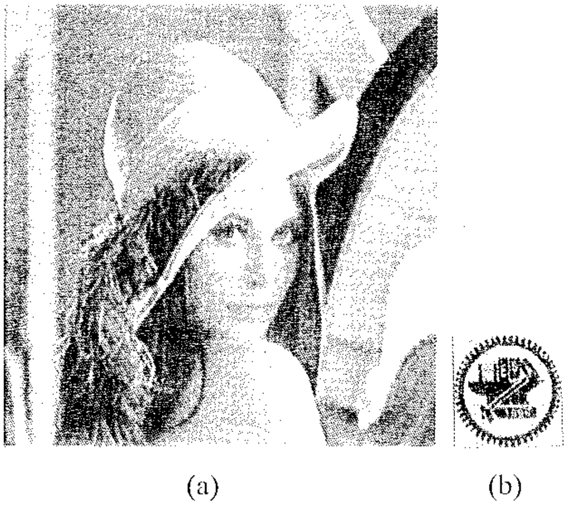


Fig. 4 Result of low-pass filtering. (a) Low-pass filtered image. (b) Extracted watermark with NC=0.9658.

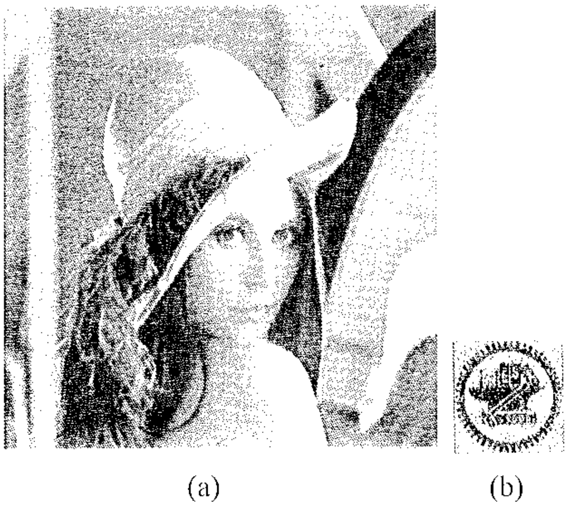


Fig. 5 Result of median filtering. (a) Median filtered image. (b) Extracted watermark with NC=0.8879.

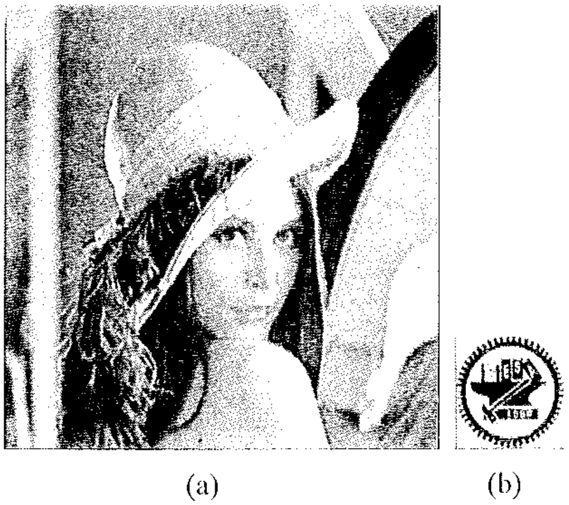


Fig. 6 Result of resampling. (a) Resampled image. (b) Extracted watermark with *NC*=0.9891.

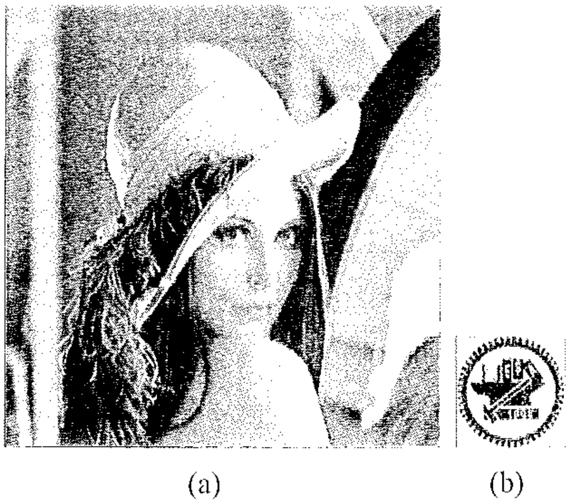


Fig. 7 Result of requantization. (a) Requantized image. (b) Extracted watermark with *NC*=0.9475.

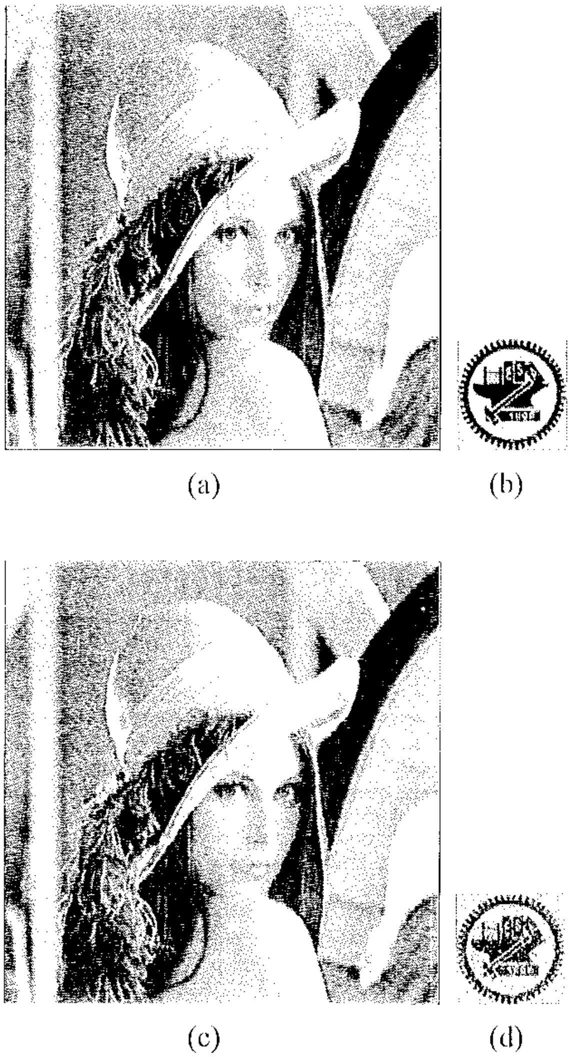


Fig. 8 Results of JPEG compression. (a) JPEG compressed image with CR=7.27. (b) Extracted watermark with *NC*=0.9929. (c) JPEG compressed image with CR=14.39. (d) Extracted watermark with *NC*=0.9103.

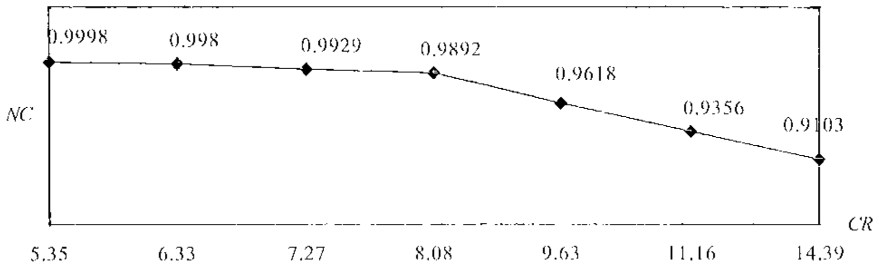


Fig. 9 A comparison of normalized cross correlation values for variant JPEG compression