An Adaptive Digital Image Watermarking Technique for Copyright Protection

Chang-Hsing Lee (**李建興**) and Yeuan-Kuen Lee* (**李遠坤**)
Department of Computer Science, Chinese Culture University
55 Hwa Kang Rd., Yang Ming Shan, Taipei, Taiwan 11114 (Email: chlee@ccu016.pccu.edu.tw)
*Department of Computer and Information Science, National Chiao Tung University
1001 Ta Hsush Rd., Hsinchu, Taiwan 30050 (Email: yklee@debut.cis.nctu.edu.tw)

Abstract

Digital watermarking technique is proposed for copyright protection or ownership identification of digital media, such as audio, image, video, or text. A digital signature or digital watermark is embedded in the host media. The digital watermark is hidden such that it is perceptually and statistically undetectable. This watermark can then be extracted from the host media and used to identify the owner of the media. In the application of copyright enforcement, the hidden watermark must still be recovered if the host media is compressed, processed, edited, or converted from digital to analog format and back. A digital image watermarking technique will be proposed in this paper. The proposed method uses the sensitivity of human eyes to adaptively embed a watermark in an image without affecting the perceptual quality of the underlying host image. In addition, the watermark will survive if some lossy image processing operations such as low-pass filtering and JPEG image compression are applied to the host image. Finally, we will combine the concept of cryptography and digital watermarking technique to implement a more secure digital watermarking system.

Keywords：copyright protection, digital watermarking, JPEG image compression

1. Introduction

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

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 to identify the author or distributor of the media.

Most of the watermarking algorithms use a serial number or 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) [14, 15]. Human eyes can then easily verify the extraction results. However, a large quantity of data must be embedded in a host media 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.

To be really effective for copyright enforcement, a digital watermarking technique must satisfy the following requirements:

A. *Perceptual transparency*
The watermark must be embedded without affecting the perceptual 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, human eyes should not perceive the existence of the watermark.

B. *Unambiguity*
The retrieval of a watermark should unambiguously identify the owner. In addition, the accuracy of owner identification should degrade gracefully under attacks.

C. *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 in the host media if some common signal processing operations are applied to the watermarked media. 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.

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

2. Previous Works

In this paper, we will concentrate on digital image watermarking techniques. The image watermarking algorithms can be classified into two categories: spatial-domain techniques (spatial watermarks) [1-8] and frequency-domain techniques (spectral watermarks) [9-18]. 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 [1]. 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 [2] 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 [3] approach to scramble the digital watermark before a watermark 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 [3, 5-7]. Darven and Scott proposed a fractal-based steganographic method to embed the watermark [8].

The frequency-domain techniques first transform an image into a set of frequency domain coefficients. The transformation may be DCT [10-11, 13-18], Fourier transform [12], or wavelet transform [9, 20], etc. The watermark is then embedded in the transformed coefficients of the image such that the watermark is less invisible and more robust to some image processing operations. Finally, the coefficients are inverse-transformed to form the watermarked image. The frequency sensitivity of the human visual system can be used to ensure that the watermark is invisible and more robust to any attacks [19, 20].

In this paper, we will propose an adaptive image watermarking technique that is robust to common image processing operations such as low-pass filtering and JPEG compression. 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 (e.g., an edge block), the intensities can be changed greatly without introducing any distortion to human eyes. On the other hand, if the contrast is small (e.g., a smooth block), the intensities can only be tuned slightly. In the following section, we will give a detailed description of the proposed method.

3. The proposed adaptive image watermarking algorithm

In this section, we will describe the proposed adaptive spatial-domain image watermarking technique. The

watermark used is a visually meaningful binary image rather than a randomly generated sequence of bits. Thus, human eyes can easily identify the extracted watermark. 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 more significant bits. This will introduce more distortion to the host image and conflicts with the invisible requirement. To meet both invisible and robust requirements, we will adaptively modify the intensities of some selected pixels as large as possible and this modification is not noticeable to human eyes. In addition, to prevent tampering or unauthorized access, the watermark is first permutated into scrambled data. The block diagram of the proposed watermarking system is depicted in Fig. 1. In the following subsections, we will first describe the embedding process and then the extraction process.

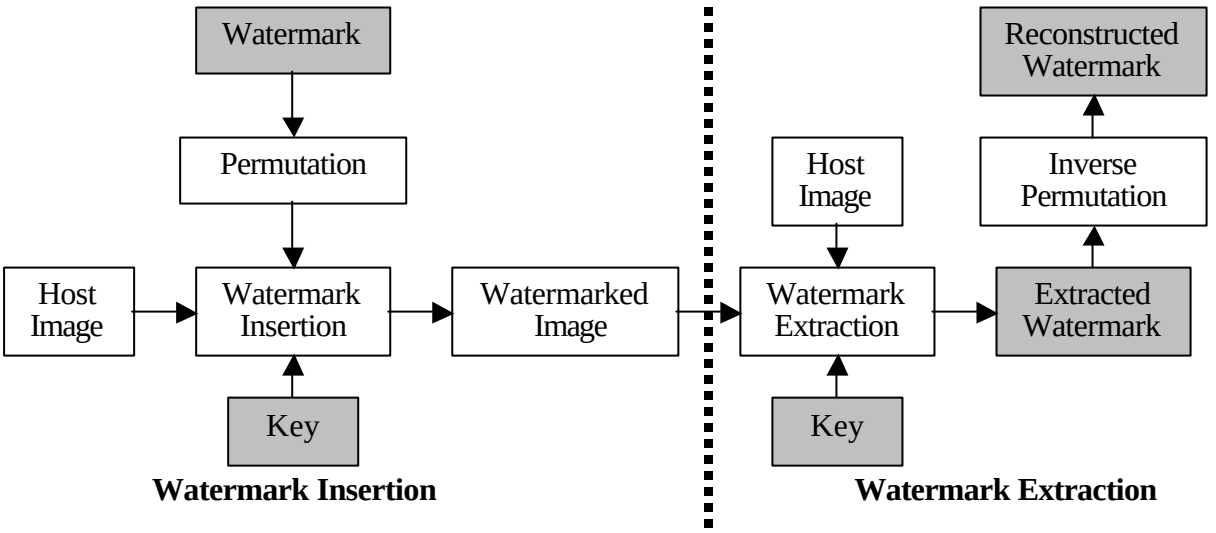

Fig. 1. Block diagram of the proposed watermarking system.

3.1 Watermark Embedding

In the proposed approach, the embedded watermark must be invisible to human eyes and robust to most image processing operations. To meet these requirements, a bit of binary pixel value (0 or 1) is embedded in a block of the host image. Before insertion, the host image is decomposed into N×N blocks. Depending on the contrast of a block, pixels in the block are adaptively modified to maximize robustness and guarantee invisibility. 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 the selected block, and g_{max}, g_{min}, and g_{mean} represent the maximal, minimal, and average intensities of the block, respectively. That is,

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

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

where b_{ij} represents the intensity of the (i, j)-th pixel in block **B**. Assume that the embedded pixel value b_w is 0 or 1. The embedding process modifies the intensities of pixels in the block **B** according to the following rules:

(1) $b_w = 1$:
$g' = g_{max}$ if $g > g_{mean}$,
$g' = g+\delta$ if $g \le g_{mean}$,

(2) $b_w = 0$:
$g' = g_{min}$ if $g < g_{mean}$,
$g' = g-\delta$ if $g \ge g_{mean}$,

where g' is the modified intensity and δ is a small value used to tune the intensities. The embedding of the watermark depends on the content of each block. If the block is of higher contrast, the intensities of pixels will be modified greatly. Otherwise, the intensities are tuned slightly. Thus the proposed algorithm can adaptively modify

the content of a block. Let blocks **B** and **B'** denote the original and watermarked 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**.

3.2 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 make reference to the original host image. First, we use the seed value, k, to generate 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 the following rule:

$b_w = 1$ if $S_w > S_o$,
$b_w = 0$ if $S_w \le S_o$.

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

4. Experimental Results

In the experiment, the size of the host image is 512×512 with 256 intensities. The watermark is a visually meaningful binary image of size 128×128. Figs. 2(a) and 2(b) show a 512×512 host image and a 128×128 binary watermark image, respectively. Fig. 2(c) shows the watermarked image that is derived by embedding the watermark image in the host image. From Figs. 2(a) and 2(c), we can not distinguish these two images since they look almost the same. Fig. 2(d) shows the reconstructed watermark, we can see that it is the same as Fig. 2(b). The similarity of these two images is quantitatively measured by the normalized cross correlation [14] 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 JPEG image compression, we first compress the watermarked image and then extract the watermark from the compressed image. Fig. 3 shows the compressed image with a compression ratio (*CR*) of 5.35 and the corresponding extracted watermark. The normalized cross correlation value *NC* is 97.24%. The low-pass filtered image and extracted watermark are shown in Fig. 4. From Figs. 3 and 4, we can see that the extracted watermarks can be used to identify the owner of the host image although some distortion exists due to lossy compression or low-pass filtering.

5. Conclusions

In this paper, we have proposed an adaptive image watermarking algorithm. The watermark adopted is a visually meaningful binary 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 block. Experimental results show that the proposed algorithm is robust to common image operations such as low-pass filtering and JPEG image compression.

Acknowledgement
This work was supported in part by the National Science Council of R.O.C. under Contract NSC87-2218-E-034-001.

(a)

(b)

(c)

(d)

Fig. 2 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 image.

(a)

(b)

Fig. 3 Result of applying JPEG to Fig. 2(c). (a) JPEG compressed image with CR=5.35. (b) Extracted watermark with *NC*=97.24%.

(a)

(b)

Fig. 4 Result of applying a low-pass filtering to Fig. 2(c). (a) Low-pass filtered image. (b) Extracted watermark with *NC*=89.22%.

References

[1] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "*A Digital watermark*", Proceedings of IEEE International Conference on Image Processing, Vol. 1, 1994, pp. 86-90.

[2] K. Matsui and K. Tanaka, "Video-Steganography: How to Embed a Signature in a Picture", in Proceedings of IMA Intellectual Property, Jan. 1994, Vol. 1, No. 1, pp. 187-206.

[3] I. Pitas, "*A method for signature casting on digital images*", Proceedings of IEEE International Conference on Image Processing, Vol. 3, 1996, pp. 215-218.

[4] G. Voyatzis and I. Pitas, "*Applications of toral automorphisms in image watermaking*", Proceedings of IEEE International Conference on Image Processing, Vol. 2, 1996, pp. 237-240.

[5] O. Bruyndonckx, J.-J. Quisquater, and B. Macq, "*Spatial method for copyright labeling of digital images*", Proceedings of IEEE Nonlinear Signal Processing Workshop, 1995, pp. 456-459.

[6] J. Smith and B. Comiskey, "Modulation and information hiding in images", in Proceedings of First International Workshop on Information Hiding, 1997, pp. 207-226.

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

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

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

[10] Marc Schneider and Shih-Fu Chang, "*A robust content based digital signature for image authentication*", Proceedings of IEEE International Conference on Image Processing, 1996, pp. 227-230.

[11] 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, Aug. 1996, pp. 250-256.

[12] J J K. O'Ruanaidh, W J. Dowling, and F M. Boland, "*Phase watermarking of digital images*", Proceedings of IEEE International Conference on Image Processing, Vol. 3, 1996, pp. 239-242.

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

[14] Chiou-Ting Hsu and Ja-Ling Wu, "*Hidden signatures in images*", in Proceedings of International Conference on Image Processing, 1996, pp. 223-226.

[15] Chiou-Ting Hsu, Ja-Ling Wu, "*DCT-based watermarking for video*", IEEE Transactions on Consumer Electronics, Vol. 44, No. 1, Feb 1998, pp. 206-216.

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

[17] Mitchell D. Swanson, Bin Zhu, and Ahmed H. Tewfik, "*Transparent robust image watermarking*", Proceedings of IEEE International Conference on Image Processing, Vol. 3, 1996, pp. 211-214.

[18] Adrian G. Bors and Ioannis Pitas, "*Image watermarking using DCT domain constraints*", Proceedings of IEEE International Conference on Image Processing, Vol. 3, 1996, pp. 231-234.

[19] J.-F. Delaigle, C. De Vleeschouwer and B. Macq, "*Psychovisual approach to digital picture watermarking*", Journal of Electronic Imaging, Vol. 7, No. 3, July 1998, pp. 628-640.

[20] Mitchell D. Swanson, Bin Zhu, Benson Chau, and Ahmed H. Tewfik, "*Multiresolution video watermarking using perceptual models and scene segmentation*", Proceedings of IEEE International Conference on Image Processing, Vol. 2 1997, pp. 558-561.