A BTC-BASED WATERMARKING SCHEME FOR DIGITAL IMAGES

Shu-Fen TU and Ching-Sheng HSU

Abstract: This article presents a novel watermarking scheme for digital images based on Block Truncation Coding (BTC). Unlike other watermarking schemes, the proposed method does not alter the original image during the process of watermark casting. Instead, an ownership share is constructed as a key to reveal the watermark without resorting to the original image. Moreover, it is possible to register multiple watermarks for a single host image in the proposed scheme. During watermark casting, the feature of the host image, which is extracted by means of BTC, is combined with the watermark to generate an ownership share. When revealing the watermark, the author can address his/her ownership share to extract the watermark. Even though the host image has been attacked, the extracted watermark is still perceivable. Altogether, the method has many other applications besides copyright protection. For example, it can be used to cover the transmission of confidential images. The experimental results of this study show the robustness of the novel scheme against several common attacks.

Keywords: Copyright Protection Scheme, Block Truncation Coding, Intellectual Property Right, Watermarking.

The development of Internet promotes communication of digital multimedia, such as image, audio, and video. All digital data possess several common features that can be used to harm the intellectual property right. For example, they are easy to falsify, to counterfeit, to snoop, and to duplicate. Nowadays, many techniques have been developed to protect the intellectual property right for digital images. Digital watermarking, a kind of such technique, is designed to insert a meaningful signature, called a watermark, directly into a digital host image to register the ownership. Then, the watermark can be extracted when the ownership of the image needs to be identified. The watermark in the watermarked image can be either visible[1] or invisible.[2,3,4,5] This article focuses on the invisible watermarks. Generally, the watermark should meet certain requirements, such as:

- Imperceptibility to human eyes,

- Robustness to common image processing operations and malicious attacks,
- Unambiguousness to ownership and copyright identification,
- Security and keys against unauthorized parties, and
- Capacity for embedding maximum information.[6,7,8,9]

Some of these requirements may conflict with each other and thereby introduce many technical challenges. For example, imperceptibility and capacity may conflict with robustness. Therefore, a reasonable compromise is required to achieve better performance for the intended applications. Current watermarking methods can be grouped into two categories. One is the spatial-domain approach,[10,11,12] and the other is the transform-domain approach.[13,14,15,16] Most related techniques have to alter the original image to embed watermark. Therefore, if multiple watermarks need to be registered for a single digital image, it is impossible for such methods to embed a subsequent watermark without destroying the former ones. In addition, when the ownership of the image needs to be identified, some of the methods require the aid of the original image to extract the watermark.

Recently, Chang, Hsiao, and Yeh[17] utilized visual cryptography and discrete cosine transformation (DCT) to design a copyright protection scheme that allows registering multiple ownerships. In essence, their model comprises ownership share construction and watermark revelation phases. During the ownership share construction phase, the DC coefficients of the different DCT blocks are extracted from the host image to form a master share, then an ownership share obtained by combining the master share and the watermark is constructed as a key to reveal the watermark without resorting to the original image. Since their method does not actually embed the watermark into the image, the host image will not be altered. However, their method requires the size of the watermark to be much smaller than that of the host image. For example, if the size of the original image is $M_1 \times M_2$, then the size of watermarks in their method should be at most $M_1/12 \times M_2/12$ for four colors, $M_1/20 \times M_2/20$ for 13 colors, and $M_1/92 \times M_2/92$ for gray-level and 256 colors.[18] Besides, a transformation of the image from the spatial domain to the frequency domain has to be performed so that the master share can be extracted.

In this article, a digital watermarking scheme without resorting to the host image is proposed. The authors apply Block Truncation Coding (BTC) to transform a gray-level host image into a binary image, which preserves the features of the host image. Then, the binary image is combined with the watermark to construct the ownership share with the aid of the XOR operation. During the watermark casting process, a pseudo-random key is used to permute the host image to enhance the robustness of the proposed scheme. When the rightful ownership needs to be identified, the authors

again transform the image to be identified to a binary one and then combine it with the ownership share to reveal the watermark.

In summary, the new method has several advantages. First, there is no need to alter the original image; hence, the image quality will not be degraded and the risk of deliberately detecting or erasing the watermark from the host image can be avoided. Second, the proposed method can identify the ownership without resorting to the original image. Third, multiple watermarks are allowed to be registered for a single image without causing any damage to other hidden watermarks. Fourth, the method can achieve the requirement of robustness for digital watermarking due to the fact that the features of the image can not be easily changed by many attacks. Fifth, the security of the scheme is ensured by the ownership share kept by a trusted third party and the secret key held secretly by the copyright owner. Altogether, the new method has many other applications than copyright protection. For example, it can be applied to protect the transmission of confidential images.

The rest of the article is organized as follows. The next section presents a brief description of Block Truncation Coding (BTC). Then, the authors demonstrate how to utilize BTC in the method to construct a copyright protection scheme with a binary watermark. Experimental results, which prove the robustness of the proposed method, are given after that. And finally, discussion and conclusions are presented in the last section.

Block Truncation Coding

Block truncation coding is a lossy compression technique for gray-level images proposed by Delp and Mitchell.[19] The image is divided into blocks of m pixels and each block is processed separately. The mean value (μ) and the standard deviation (σ) are calculated for each block and the first two sample moments are preserved in the compression. The original block is encoded into a bit plane (B), where pixels with values less than the mean value are set to '0', and those with values greater than or equal to the mean value are set to '1'. The block is decompressed according to the triple (μ, σ, B). The bit '0' of B is set to a, and the bit '1' of B is set to b, where a and b are computed according to Equations (1a) and (1b), and q stands for the number of bits '1' in B.

$$a = \mu - \sigma \cdot \sqrt{\frac{q}{m-q}} \tag{1a}$$

$$b = \mu + \sigma \cdot \sqrt{\frac{m-q}{q}} \tag{1b}$$

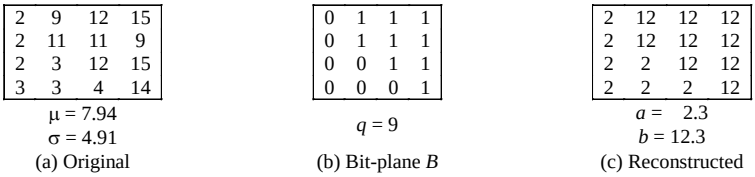


Figure 1: An Example of BTC by (μ , σ , B).

Figure 1 is an example taken from the article of Fränti, Nevalatinen, and Kaukoranta.[20] Figure 1(a) is an original block of 16 pixels, and the mean value μ and standard deviation σ of the block are 7.94 and 4.91, respectively. The block is encoded into a bit plane B with nine bits '1' as shown in Figure 1(b). The block can be reconstructed according to triple (μ , σ , B) and Equations (1a) and (1b). Although the compression ratio (i.e. a bit rate) is not low enough, this coding method gives good reconstructed image since it preserves local characteristics of blocks of the image important to the human observer. Besides, the process of compression and decompression is very simple and fast.

In this article, the authors utilize BTC to construct the master share of the original image; therefore, the master share can preserve the features of the original image. Together, the master share and the watermark are used to construct the ownership share. Even though the original image is attacked, the features of the image can not be changed much. Since the ownership share is generated according to the features of the original image, the authors can enhance the robustness of their scheme. Readers interested in BTC can refer to the work of Delp and Mitchell[21] and Fränti, Nevalatinen, and Kaukoranta[22] for further reading.

The Proposed Scheme

This section demonstrates how to cast a binary watermark into a gray-level host image and how to detect the watermark from a gray-level test image to identify the ownership. The whole process in the proposed scheme can be partitioned into two phases: one is the watermark casting phase; the other is the watermark detection phase. In the watermark casting phase, the host image is divided into equal-sized blocks of 3×3 pixels. Then, BTC is used to extract the features of each block. Finally, the ownership share is constructed according to the features of the host image and the pixels of the watermark. In the watermark detection phase, the test image and the ownership share are divided into equal-sized blocks of 3×3 pixels. Then, each block of the test image is transformed into a bit plane. Finally, the pixels of the watermark are set according to the bit planes of the test image and the corresponding block of the ownership share. Since the ownership share is the key to identify the ownership of the image, the copy-

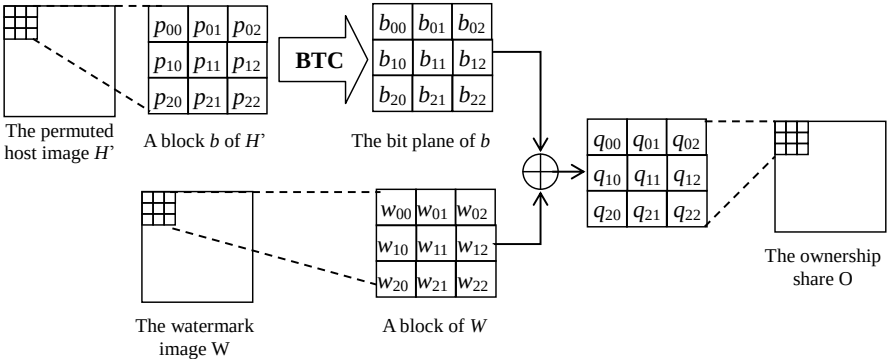


Figure 2: Illustration of Watermark Casting.

right owner has to send it to a trusted third-party for further authentication. Combined with BTC, the proposed scheme is shown to be robust for detecting the watermark. Note that the host image has to be permuted by a pseudo random number generator before BTC is applied to it.

Watermark Casting

Presume that a binary watermark W of $N \times M$ pixels is cast into a gray-level host image H of $N \times M$ pixels. First, H has to be permuted by a pseudo-random number generator seeded by a key k to enhance the robustness of the scheme. Then the permuted host image H' is divided into blocks of 3×3 pixels, each of which corresponds to a pixel of W. Each block of H' is transformed into a bit plane according to the mean value μ of the pixels in the block; that is, pixels with values greater than or equal to μ are set to '1' (i.e. black), and those with values less than μ are set to '0' (i.e. white). Meanwhile, the corresponding pixel of W is divided into blocks of 3×3 pixels as well. The two bit planes are used to create the corresponding 3×3 block of the ownership share O through XOR logic. Figure 2 depicts the whole process of watermark casting, and the algorithm of watermark casting is shown below.

Algorithm *Watermark Casting*

Input: A gray-level watermark image W of $N \times M$ pixels
A gray-level host image H of $N \times M$ pixels
A seed k of the pseudo random number generator

Output: An ownership share O of $N \times M$ pixels

Step 1. Permute H by pseudo-random numbers seeded by k. Denote the permuted image as H'.

Step 2. Divide H' into equal-sized blocks of 3×3 pixels to derive a set of blocks $\{H'_{ij}\}$, where $i = 0 \sim (N/3-1)$ and $j = 0 \sim (M/3-1)$. Each pixel of H'_{ij} is denoted as p_{mn}^{ij}, where $m = 0..2$ and $n = 0..2$, and p_{00}^{ij} is located at $(3i, 3j)$ of H'.

Step 3. For each block H'_{ij}, calculate the mean value μ_{ij} of the pixels. Set p_{mn}^{ij} to '1' if its value is greater than or equal to μ_{ij}; otherwise, set it to '0'. Hence, H' is transformed into a binary image containing $(N/3) \times (M/3)$ bit planes $\{B_{ij}\}$ of 3×3 pixels b_{mn}^{ij}, where $i = 0..(N/3-1)$, $j = 0..(M/3-1)$, $m = 0..2$ and $n = 0..2$.

Step 4. Divide W into equal-sized blocks of 3×3 pixels to derive a set of blocks $\{W_{ij}\}$, where $i = 0..(N/3-1)$ and $j = 0..(M/3-1)$. Each pixel of W_{ij} is denoted as w_{mn}^{ij}, where $m = 0..2$ and $n = 0..2$, and w_{00}^{ij} is located at $(3i, 3j)$ of W.

Step 5. Generate the pixel q_{uv} of O through XOR logic; i.e. $q_{uv} = b_{mn}^{ij} \oplus w_{mn}^{ij}$, where $u = 3i + m$, $v = 3j + m$, $i = 0..(N/3-1)$, $j = 0..(M/3-1)$, $m = 0..2$ and $n = 0..2$.

Step 6. Perform Step 5 repeatedly until all pixels of O are generated.

Figure 3 is an example of watermark casting. Suppose that Figure 3(a) is a 3×3 block of H' and the corresponding bit plane of W is shown in Figure 3(c). The mean value μ of the pixels in b is 69.33; therefore, pixels with values greater than or equal to 69.33 are set to '1'; otherwise, they are set to '0' as shown in Figure 3(b). Figure 3(d) is the corresponding block of the ownership share, where each pixel is the XOR result of the corresponding pixels of the two bit planes. After completing watermark casting, the copyright owner has to send the ownership share to a trusted third-party for authentication. In addition, the key to permute the host image has to be kept by the owner.

55	120	70
25	36	6
18	94	200

(a) A block *b* of H' μ = 69.33

0	1	1
0	0	0
0	1	1

(b) The bit plane of (a)

1	1	1
1	1	1
0	0	0

(c) The corresponding bit plane of *W*

1	0	0
1	1	1
0	1	1

(d) The XOR result of (b) and (c)

Figure 3: An Example of Watermark Casting.

Watermark Detection

If a gray-level image G is suspected to be a piracy copy, the owner can resolve the dispute about the ownership by detecting the existence of a watermark. First, the test image G is permuted by a pseudo-random number generator seeded by the same key k. Then, both the permuted image G' and the ownership share O are divided into blocks of 3×3 pixels. Each block of G' is transformed into a bit plane by means of BTC. Then the owner has to address his/her authenticated ownership share O. Note that G has to be permuted with the same pseudo-random key before starting the process of master share construction. Let G' denote the permuted image. With G' and O we can reveal the watermark W', which may be different from the original one W. The process of watermark revelation is described as follows.

Algorithm *Watermark Detection*

Input: A gray-level test image G of $N \times M$ pixels
An ownership share O of $N \times M$ pixels
A seed k of the pseudo random number generator

Output: A watermark W' of $N \times M$ pixels

Step 1. Permute G by pseudo-random numbers seeded by k. Denote the permuted image as G'.

Step 2. Divide G' into equal-sized blocks of 3×3 pixels to derive a set of blocks $\{G'_{ij}\}$, where $i = 0..(N/3-1)$ and $j = 0..(M/3-1)$. Each pixel of G'_{ij} is denoted as p^{ij}_{mn}, where $m = 0..2$ and $n = 0..2$, and p^{ij}_{00} is located at $(3i, 3j)$ of G'.

Step 3. For each block G'_{ij}, calculate the mean value μ_{ij} of the pixels. Set p^{ij}_{mn} to '1' if its value is greater than or equal to μ_{ij}; otherwise, set it to '0'. Hence G' is transformed into a binary image containing $(N/3) \times (M/3)$ bit planes $\{B_{ij}\}$ of 3×3 pixels b^{ij}_{mn}, where $i = 0..(N/3-1)$, $j = 0..(M/3-1)$, $m = 0..2$ and $n = 0..2$.

Step 4. Divide O into equal-sized blocks of 3×3 pixels to derive a set of blocks $\{O_{ij}\}$, where $i = 0..(N/3-1)$ and $j = 0..(M/3-1)$. Each pixel of O_{ij} is denoted as q^{ij}_{mn}, where $m = 0..2$ and $n = 0..2$, and q^{ij}_{00} is located at $(3i, 3j)$ of O.

Step 5. Generate pixels w_{uv} of W through performing XOR logic on b^{ij}_{mn} and q^{ij}_{mn};

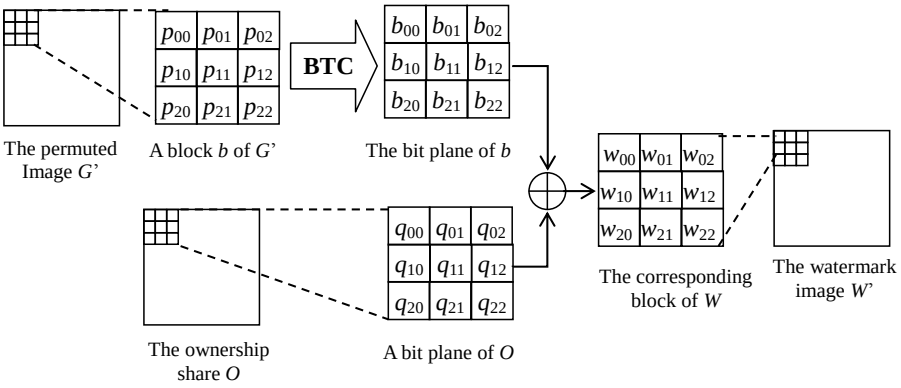


Figure 4: Illustration of Watermark Revelation.

i.e. $w_{uv} = b_{mn}^{ij} \oplus q_{mn}^{ij}$, where $u = 3i + m$, $v = 3j + m$, $i = 0..(N/3-1)$, $j = 0..(M/3-1)$, $m = 0..2$ and $n = 0..2$.

Step 6. Perform Step 5 repeatedly until all pixels of W are generated.

Figure 4 illustrates the process of watermark revelation. The permuted gray-level image G' is divided into equal-sized blocks of 3×3 pixels. We take a block b from G' and transform it into a bit plane by means of the BTC method. Next, we take a corresponding bit plane from O and perform the XOR operation on the two bit planes. Finally, the corresponding block of W' can be generated. The remaining blocks of W' are generated by analogy. Figure 5 is an example of watermark revelation. Figure 5(a) is a block b of G' with mean value μ =50.67. Performing XOR logic on the bit plane of b (Figure 5(b)) and the corresponding bit plane of O (Figure 5(c)), we can get the corresponding block of W' as shown in Figure 5(d).

92	15	100
66	84	10
3	26	60

(a) A block *b* of G'
μ = 50.67

1	0	1
1	1	0
0	0	1

(b) The bit plane of (a)

0	1	1
1	0	0
0	0	0

(c) The corresponding bit plane of *O*

1	1	0
0	1	0
0	0	1

(d) The XOR result of (b) and (c)

Figure 5: An Example of Watermark Revelation.

Experimental Results

In this section, we use Figure 6(a) as an experiment to demonstrate the robustness of the proposed scheme against several common attacks, including blurred (Figure 6(b)), brighten (Figure 6(c)), JPEG lossy compressed (Figure 6(d)), cropped (Figure 6(e)),

darken (Figure 6(f)), distorted (Figure 6(g)), noised (Figure 6(h)), rescaled (Figure 6(i)), and sharpen (Figure 6(j)). Two common similarity measurements are introduced to evaluate the proposed watermarking scheme. One is the peak signal-to-noise ratio (PSNR) used to evaluate the similarity of two gray-level images and the other is the normalized correlation (NC) used to measure the similarity between two bi-level images. The first measurement, signal-to-noise ratio, is defined as follows:

$$PSNR = 10 \times \log \frac{255^2}{MSE} \tag{2}$$

where

$$MSE = \frac{1}{M_1 \times M_2} \sum_{i=1}^{M_1} \sum_{j=1}^{M_2} (c_{i,j} - c'_{i,j})^2 \tag{3}$$

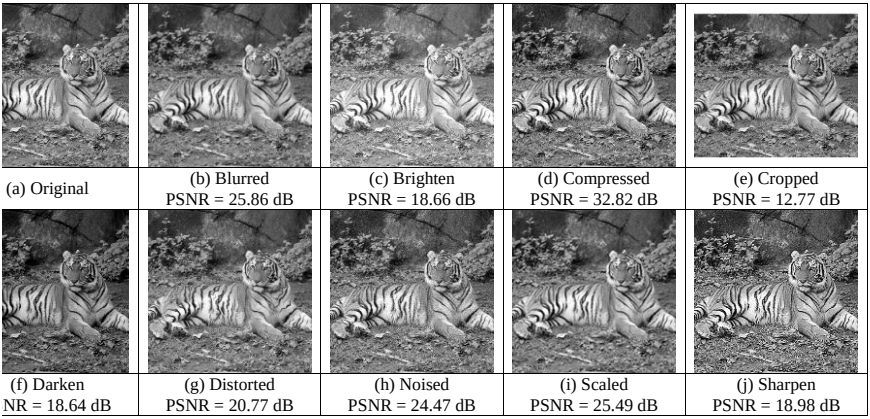
$c_{i,j}$ denotes a pixel color of the original host image, $c'_{i,j}$ denotes a pixel color of the attacked image, and $M_1 \times M_2$ is the image size. The second measurement, normalized correlation, is defined as follows:

$$NC = \frac{\sum_{i=1}^{N_1} \sum_{j=1}^{N_2} \overline{w_{i,j} \oplus w'_{i,j}}}{N_1 \times N_2} \times 100\% \tag{4}$$

where $w_{i,j}$ denotes a pixel color of the original watermark W, $w'_{i,j}$ denotes a pixel color of the revealed watermark W', and $N_1 \times N_2$ is the image size.[23]

The size of the host image is 384×384 pixels, and that of the watermark is 192×192 pixels. Therefore, only half of the host image is needed to construct the ownership share. We use the PSNR as a measurement to express how severe the host image is attacked. The smaller the PSNR is, the more dissimilar the attacked image is. Usually, '30' is a tolerable bottom line. Observing Figure 6, we can see that most PSNR values are less than '30', which means that the host image comes under severe attacks.

Figure 7(a) is the original watermark, and Figures 7(b)-7(j) are extracted watermarks from Figures 6(b)-6(j). These extracted watermarks are compared to the original watermark with the measurement NC. The larger the NC is, the more similar the extracted watermark is. Usually, '80%' is a tolerable bottom line. We can see from Figure 7 that the NC values of the extracted watermark are all greater than 80%.



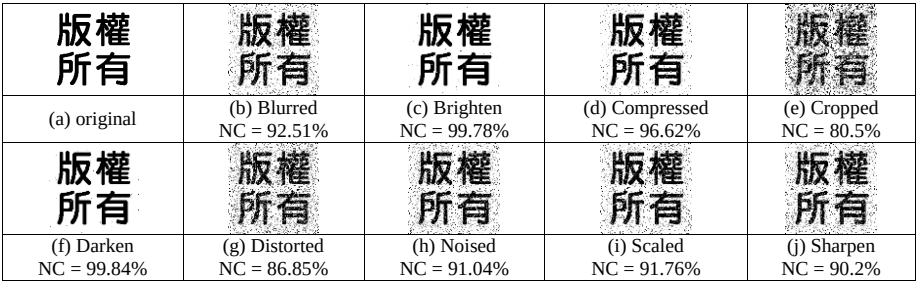
(a) Original	(b) Blurred PSNR = 25.86 dB	(c) Brighten PSNR = 18.66 dB	(d) Compressed PSNR = 32.82 dB	(e) Cropped PSNR = 12.77 dB
(f) Darken NR = 18.64 dB	(g) Distorted PSNR = 20.77 dB	(h) Noised PSNR = 24.47 dB	(i) Scaled PSNR = 25.49 dB	(j) Sharpen PSNR = 18.98 dB

Figure 6: The Host Image and Nine Different Attacks on the Host Image (384 × 384 pixels, 300 dpi).

Besides objective measurement, human eyes are also a good subjective measurement. It is obvious that the words on the extracted watermarks are still distinguishable.

Conclusions

In this article, a novel scheme for digital watermarking based on BTC is proposed. The presented method applies BTC to extract the features of the host image. Then, the ownership share is constructed by combining the features of the host image with the watermark. Since the watermark is cast according to the features of the host image, the authors believe that it is highly possible the watermark to survive under attacks. Actually, the experimental results also show the robustness of the new scheme.



(a) original	(b) Blurred NC = 92.51%	(c) Brighten NC = 99.78%	(d) Compressed NC = 96.62%	(e) Cropped NC = 80.5%
(f) Darken NC = 99.84%	(g) Distorted NC = 86.85%	(h) Noised NC = 91.04%	(i) Scaled NC = 91.76%	(j) Sharpen NC = 90.2%

Figure 7: The Original Watermark and Revealed Watermarks Extracted from Figure 6(b)-6(j) (192 × 192 pixels, 300 dpi).

In summary, the proposed scheme has the following advantages. First, the host image is not altered or damaged by the watermark casting procedure due to the fact that the watermark is not actually embedded into the host image. Hence, the image quality will not be degraded and the risk of deliberately detecting or erasing the watermark from the host image can be avoided. Second, the method can identify the ownership without resorting to the original image. Third, the proposed scheme allows multiple watermarks to be cast into a single host image without causing any damage to other hidden watermarks. Fourth, the security of the scheme can be ensured by the ownership share and the secret key held secretly by the copyright owner. Finally, the scheme seems robust according to the experimental results.

Although the present version of the proposed scheme only deals with bi-level watermarks, it is possible to extend the method to gray-level or color watermarks. For example, each pixel of a gray-level watermark can be encoded into a block of 3×3 pixels, where the first eight pixels of the block map to the eight bits of a pixel value of the watermark. To deal with color watermarks, we can employ the last pixel of the block to store the palette of 256 colors. Thus, the first eight pixels can be used to represent the index of colors. In the future, the issue of gray-level and color watermarks will be further studied.

Notes:

[1] Gordon W. Braudaway, Karen A. Magerlein, and Frederick C. Mintzer, "Protecting Publicly-Available Images with a Visible Image Watermark," in *Proceedings of the SPIE International Conference on Electronic Imaging, Science and Technology: Optical Security and Counterfeit Deterrence Techniques* (San Jose, CA, 1-2 February 1996), Volume 2659 (Bellingham, Wa.: SPIE, 1996), 126-133.

[2] Ingemar J. Cox, Joe Kilian, Tom Leighton, and Talal Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions on Image Processing* 6, no. 12 (1997): 1673-1687.

[3] Stephen H. Low and Nicholas F. Maxemchuk, "Performance Comparison of Two Text Marking Methods," *IEEE Journal on Selected Areas in Communications* 16, no. 4 (May 1998): 561-572.

[4] Kineo Matsui, Junji Ohnishi, and Yasuhiro Nakamura, "Embedding a Signature to Pictures under Wavelet Transform," *IEICE Transactions* J79-D-II, no. 6 (June 1996): 1017-1024.

[5] Ryutarou Ohbuchi, Hiroshi Masuda, and Masaki Aono, "Watermarking Three-Dimensional Polygonal Models through Geometric and Topological Modifications," *IEEE Journal on Selected Areas in Communications* 16, no. 4 (May 1998): 551-560.

[6] Cox, Kilian, Leighton, and Shamoon, "Secure Spread Spectrum Watermarking for Multimedia."

[7] Stefan Katzenbeisser and Fabien A.P. Petitcolas, eds., *Information Hiding Techniques for Steganography and Digital Watermarking* (Norwood, MA: Artech House Inc., January 2000), 101-109.

[8] Eckhard Koch, Jochen Rindfrey, and Jian Zhao, "Copyright Protection for Multimedia Data" (paper presented at the International Conference on Digital Media and Electronic Publishing, Leeds, UK, December 1994), 6-8.

[9] Nikos Nikolaidis and Ioannis Pitas, "Copyright Protection of Images using Robust Digital Signatures," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing(ICASSP-96)*, Volume 4 (Atlanta, Georgia, May 1996), 2168-2171.

[10] Young-Chang Hou and Pei-Min Chen, "An Asymmetric Watermarking Scheme Based on Visual Cryptography," in *Proceedings of the Fifth Signal Processing Conference*, Volume 2 (Beijing, China, 21-25 August 2000), 992-995.

[11] Low and Maxemchuk, "Performance Comparison of Two Text Marking Methods."

[12] Ohbuchi, Masuda, and Aono, "Watermarking Three-Dimensional Polygonal Models through Geometric and Topological Modifications."

[13] Chin-Chen Chang, Ju Yuan Hsiao, and Jyh-Chiang Yeh, "A Colour Image Copyright Protection Scheme based on Visual Cryptography and Discrete Cosine Transform," *The Imaging Science Journal* 50 (2002): 133-140.

[14] Cox, Kilian, Leighton, and Shamoon, "Secure Spread Spectrum Watermarking for Multimedia."

[15] Chiou-Ting Hsu and Ja-Ling Wu, "Hidden Digital Watermarks in Images," *IEEE Transactions on Image Processing* 8, no. 1 (January 1999): 58-68.

[16] Young-Sik Kim, O-Hyung Kwon, and Rae-Hong Park, "Wavelet Based Watermarking Method for Digital Images using the Human Visual System," *Electronics Letters* 35, no. 6 (March 1999): 466-468.

[17] Chang, Hsiao, and Yeh, "A Colour Image Copyright Protection Scheme based on Visual Cryptography and Discrete Cosine Transform."

[18] Chang, Hsiao, and Yeh, "A Colour Image Copyright Protection Scheme based on Visual Cryptography and Discrete Cosine Transform."

[19] Edward J. Delp and O. Robert Mitchell, "Image Compression using Block Truncation Coding," *IEEE Transactions on Communications* 27, no. 9 (September 1979): 1335-1342.

[20] Pasi Fränti, Olli Nevalainen, and Timo Kaukoranta, "Compression of Digital Images by Block Truncation Coding: A Survey," *The Computer Journal* 37, no. 4 (1994): 308-332.

[21] Delp and Mitchell, "Image Compression using Block Truncation Coding."

[22] Fränti, Nevalatinen, and Kaukoranta, "Compression of Digital Images by Block Truncation Coding: A Survey."

[23] Chang, Hsiao, and Yeh, "A Colour Image Copyright Protection Scheme based on Visual Cryptography and Discrete Cosine Transform."

SHU-FEN TU received a BS degree in Management Information System from the National Cheng Chi University, Taiwan, R.O.C., in 1996 and a MS degree in Information Management from the National Chi Nan University, Taiwan, R.O.C., in 1998. From 1998 to 1999, she was a software engineer at The Syscom Group Co., Taiwan, R.O.C. Currently, she is pursuing her Ph.D degree in Information Management at the National Central University, Taiwan, R.O.C. Her research interests include steganography, document protection, and secret sharing. *Address for correspondence*: Department of Information Management, National Central University, P.O. Box 9-277, Jhongli, Taoyuan County 32099, Taiwan, R.O.C.; *Phone:* +886-3-420-4131; *E-mail:* ariel_tu@anet.net.tw.

CHING-SHENG HSU received a BS degree in Management Information Systems from the National Cheng Chi University, Taiwan, R.O.C., in 1994, and a MS degree in Information Management from the National Chi Nan University, Taiwan, R.O.C., in 1998. From 1998 to 1999, he was a software engineer at The Syscom Group Co., Taiwan, R.O.C. Currently, he is pursuing his Ph.D degree in Information Management at the National Central University, Taiwan, R.O.C. His research interests include steganography, copyright protection, cryptography, evolutionary computation, and distance learning. *Address for correspondence*: Department of Information Management, National Central University, P.O. Box 9-236, Jhongli, Taoyuan County 32099, Taiwan, R.O.C.; *Phone:* +886-3-420-3157; *E-mail:* jacketcc@mgt.ncu.edu.tw.