PERGAMON

Available at
www.ElsevierComputerScience.com
POWERED BY SCIENCE DIRECT

Pattern Recognition 38 (2005) 587–598

PATTERN RECOGNITION
THE JOURNAL OF THE PATTERN RECOGNITION SOCIETY
www.elsevier.com/locate/patcog

A robust watermarking scheme using phase shift keying with the combination of amplitude boost and low amplitude block selection

Wen-Yuan Chen[a,*], Chin-Hsing Chen[b]

[a]*Department of Electronic Engineering, National Chin-Yi Institute of Technology, Taichung, Taiwan, R.O.C.*
[b]*Department of Electrical Engineering, National Cheng Kung University Tainan, 70101 Taiwan, R.O.C.*

Received 10 December 2002; received in revised form 25 August 2003; accepted 10 October 2004

Abstract

Watermarking is a potential method for copyright protection and authentication of multimedia data in the internet. The watermarking process can be viewed as a communication task, where the watermark acting like information is embedded into a host image acting like noise in a communication channel which is susceptible to all kinds of attacks acting like jamming. In a previous paper, we proposed a robust watermarking scheme using frequency shift keying (FSK). In the scheme, high-variance block selection (HVBS) is employed to enhance robustness. In this paper, a novel watermarking scheme using phase shift keying (PSK) modulation with amplitude boost (AB) and low amplitude block selection (LABS) is proposed. AB is hired to increase the robustness while LABS is employed to improve the imperceptibility. With proper combination of AB and LABS, the proposed scheme achieves superior performance in terms of robustness and imperceptibility.

In order to demonstrate the effectiveness of the proposed scheme, simulations under various conditions were conducted. The empirical results showed that QPSK is the best choice among other PSKs and the proposed scheme can sustain most common attacks including JPEG compression, rotating, resizing, cropping, painting, noising and blurring etc. The empirical results also showed that the scheme with AB and LABS properly combined outperforms the scheme without. The gain of the former over the latter is more significant for host images with smooth characteristics than those with high-frequency characteristics. Simulation comparison with two other schemes (the Hsu's scheme and the Chen's scheme) showed that the proposed scheme is the most robust among the three.

Keywords: Spread spectrum (SS); Phase shift keying (PSK); Discrete Fourier transform (DFT); Pseudo-random number sequence (PN); Joint photographic experts group (JPEG)

1. Introduction

Because digital information is easy to transmit and duplicate unauthorized reproduction becomes a serious problem. While copyright and authentication gradually lose its security, the need for protecting intellectual property becomes more and more important. Recently, digital watermarking has been proposed as one solution to the problem of protecting the intellectual property [1–9]. Unlike the traditional visible watermark found on papers, a digital watermark does not change the perceived quality of the image content. It is a potential method to discourage unauthorized copying or attesting origin of the image. Generally, a digital watermark must fulfill the following requirements: imperceptible, robust and secure.

* Corresponding author. Tel.: +886 4 2392450; fax: +886 423919642.
E-mail addresses: cwy@chinyi.ncit.edu.tw (W.-Y. Chen), chench@eembox.ncku.edu.tw (C.-H. Chen).

0031-3203/$30.00
doi:10.1016/j.patcog.2004.10.001

Watermarking techniques can be classified into two categories, one is processed in the spatial domain and the other is accomplished in the transform domain. In the spatial domain [1,2], the visual modes derived from data compression are very suitable for digital watermarking. Many excellent hiding methods published are based on just noticeable distortion (JND) [9]. Vector quantization is one of the widely used schemes to embedding watermarks. Lu and Sun [10] used codeword indices to carry the watermark information. However, the watermarks embedded in the spatial domain are not as robust as most of those embedded in the transform domain.

In the transform domain many approaches [3–7] are based on the Discrete Cosine Transform (DCT). Hsu and Wu [4] proposed a scheme by block-based image-dependent permutation of the watermarks in the middle band of the DCT coefficients and obtained good performance. Wu and Hsieh [6] used zerotree structure to embed watermark by rearranging the DCT coefficients in a way similar to the multiresolution analysis (MRA) of wavelet transforms. Moreover, Langelaar and Lagendijk [7] proposed a scheme that employs three parameters to guarantee the performance. That is, first use a large number of the DCT blocks to embed single information bit; next, use small JPEG quality factor to enhance the watermark robustness against re-encoding attacks; third, adopt the so-called minimal cutoff index in the zigzag scanned fashion of the DCT coefficients that can be removed from the watermarked image.

The discrete wavelet transform (DWT) is another effective transform-domain method for concealing watermarks. Tsia et al. [8] utilizes the wavelet multi-resolutional structure to decompose the image and scatter the two-dimensional watermark to select the location during the secret data embedding. Wei et al. [9] controlled the wavelet coefficients so that the watermark noises do not exceed the just-noticeable difference (JND) of wavelet coefficients during watermark insertion. More papers based on the DWT for watermarking can be found in Refs. [11,12].

Another method in the transform domain is to hide watermarks in the discrete Fourier transform (DFT) coefficients of the host image. Ruanaidh et al. [13] presented a phase-based method in the DFT domain and used an optimal detector for watermark recovery. Based on the Fourier–Mellin Transform Ruanaidh and Pun [14] presented a watermarking scheme that achieves rotation, scale and translation (RST) invariant. The scheme achieves robustness while sustains the RST attacks. Premaratne and Ko [15] proposed a new concept for embedding and detecting the watermark in the Discrete Fourier Transform. Since the embedding is independent of the image content, speedy embedding highly suitable for video streams can be achieved. Solachidis and Pitas [16] proposed a watermarking scheme which embeds a circularly symmetric watermark on a ring in the 2D DFT domain. The circularly symmetric watermark was used to solve the rotation invariance problem in the watermark detection in which a correlation operation was used.

In a previous paper [17], we proposed a DCT domain watermarking scheme using the frequency shift keying (FSK). In the scheme, high-variance block selection (HVBS) is employed to enhance robustness. In this paper, we proposed a DFT domain watermarking scheme using the phase shift keying (PSK). In our proposed scheme, the watermark bits are first expanded by spread spectrum and then concealed by PSK modulation in the DFT coefficients of the host image. The PSK embedding is employed due to its superior noise immunity. In the PSK embedding, the watermark information is embedded in the phase part of the host image. Thus, the threshold effect in which the quality of the recovered watermark plunges when the amplitudes of the DFT coefficients used for embedding the secret bits are below a threshold value may occur [18]. In this paper, a novel idea combining amplitude boost (AB) and low-amplitude block selection (LABS) is proposed to curb the threshold effect raised by PSK. We demonstrated that by properly combining AB and LABS robustness can be enhanced without sacrificing imperceptibility. Meanwhile, in our scheme neither the original host image nor the original watermark is required during the watermark detection process.

The remainder of this paper is organized as follows. In Section 2, the proposed concealing algorithm is presented. The watermark extracting process is presented in Section 3. Empirical results are presented in Section 4. Finally, Section 5 concludes this paper.

2. Concealing algorithm

A robust watermarking scheme must survive all kinds of attacks, and at the same time sustain the virtual quality of the host image when the watermark is concealed. Besides, security is also an important factor required by a watermarking scheme. In order to construct a superior watermarking scheme, several skills are used in this paper to achieve the goal. The overall concealing process of our proposed scheme is shown in Fig. 1. The watermark W is first transformed to H by toral automorphism (TA) [19] using a pseudo random sequence (PN) generated by a private key to enhance the security. It is then spreaded by spread spectrum (SS) [20,21] to a binary random sequence $\{m\}$. On the other hand, the host image X is transformed to Z by DFT. Then a low amplitude block B is selected from Z using the LABS strategy. Two DFT coefficients $ae^{j\phi}$ and $ae^{-j\phi}$ which from a complex conjugate pair are selected from B for the following AB process in which a is boosted to a' to combat attacks. In the PSK modulation, ϕ is modulated by m into ϕ'. After AB and PSK, $a'e^{j\phi'}$ and $a'e^{-j\phi'}$ in which ϕ' contains the secret information are then embedded into Z at the selected block and coefficient pair locations by watermark bits embedding (WBE). The above embedding process is repeated for each secret bit in $\{m\}$ and its corresponding block. The resultant image Z' after embedding is then inversely transformed to obtain the watermarked image R. The details of

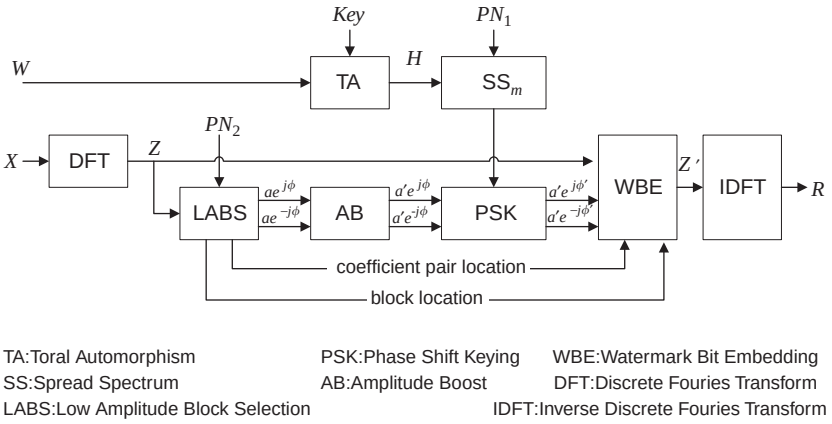

Fig. 1. The flow chart of the proposed embedding process.

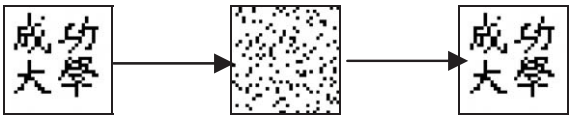

Fig. 2. The images transformed by toral automorphism.

each block of our embedding algorithm are presented in the following.

2.1. Toral automorphism

For security, the watermark image is pre-permuted into noises by the toral automorphism with a user's key. The toral automorphism scatters the image shape in some iterated operations less than a specified number of times, and will return to the original shape while it is further iterated totally the specified number of times. The specified number is determined by the toral automorphism parameters and the image size. In this paper, the toral automorphism is used to transfer the shape of the original image into chaotic to protect the watermark from being stolen. The transfer function between H and W is given by

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}\ n). \tag{1}$$

Where (x, y) and (x', y') express the pixel locations of W and H respectively, k denotes the control parameter and n denotes the image size, respectively. An example of images transformed by toral automorphism is shown in Fig. 2.

2.2. Spread Spectrum

SS is used to defense noises in many communication systems. A robust watermarking must be able to survive various attacks. In this paper, we hired the SS skill to enhance the robustness of the watermarking scheme. Spread Spectrum expands an information bit into several bits with random values. The expanded bits created when the information bit is high are the inverse of those created when the information bit is low. To randomize the expanded bits, PN sequences are used to accomplish the job. By raster scanning, H is converted into a bit sequence $d(j)$, $j=1, 2, 3 \ldots n$. For each $d(j)$, we generate a PN sequence $r_j(i)$, $i = 1, 2, 3 \ldots l$, l is the length of expansion. By multiplying $d(j)$ by $r_j(i)$, a watermark-bearing bit is chopped up into chips. The expanded bit sequence is given by

$$m_j(i) = d(j) \cdot r_j(i), \quad i = 1, 2, 3 \ldots l, \quad j = 1, 2, 3 \ldots n. \tag{2}$$

2.3. Low-amplitude block selection

In this paper, two complementary strategies, amplitude boost (AB) and low-amplitude block selection (LABS) are employed to design a novel embedding scheme using the PSK modulation. The amplitude boost is a skill used to enhance robustness, while the low-amplitude block selection is used to preserve the imperceptibility as much as possible. The details of the former will be presented latter and the details of the later is given below. The low amplitude block selection strategy selects blocks of low amplitude to embed the secret bits. First, blocks are selected by a PN sequence and every b_1+b_2 blocks are regarded as a group. Second, in each group only the first b_1 lowest amplitude blocks are used for embedding the secret bits. That is, LABS is performed locally within a group. This local selection strategy makes synchronization much easier during the watermark detection process when compared with the global strategy in which selection is made over the whole image.

To make a watermarking scheme robust, a good strategy is to embed the watermark bits into the significant portion of the host signal, because this portion of the host data is highly sensitive to alteration. A watermark concealed in the

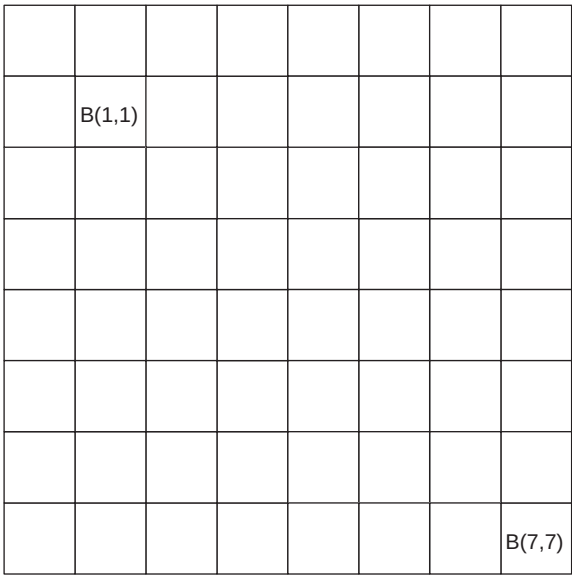

Fig. 3. The coefficient pair selected within a block for embedding the secret bit.

high or middle frequency bands is easier to be removed or altered without affecting the host image by attacks [22]. In this paper, we embedded the secret data in lower frequency bands to enhance the robustness. The DFT of a block image B of size 8×8 is given by

$$B(u, v) = \frac{1}{\sqrt{64}} \sum_{x=0}^{7} \sum_{y=0}^{7} b(x, y) e^{-j2\pi xu/8 - j2\pi yv/8}, \quad 0 \leqslant u \leqslant 7, 0 \leqslant v \leqslant 7 \tag{3}$$

with the inverse transform given by

$$b(x, y) = \frac{1}{\sqrt{64}} \sum_{x=0}^{7} \sum_{y=0}^{7} B(u, v) e^{j2\pi xu/8 - j2\pi yv/8}, \quad 0 \leqslant x \leqslant 7, 0 \leqslant y \leqslant 7. \tag{4}$$

For a real-value image, the following constraint is satisfied.

$$B(u, v) = B^*(N - u, N - v) \tag{5}$$

or

$$|B(u, v)| = |B(N - u, N - v)| \tag{6}$$

$$\angle B(u, v) = -\angle B(N - u, N - v). \tag{7}$$

Therefore, during the PSK embedding the odd symmetry expressed by Eq. (7) must be preserved. By taking this constraint into account, we select B(1,1) and its complex conjugate B(7,7) for embedding the secret bit. Fig. 3 shows the location of B(1,1) and B(7,7) in the lower frequency bands of a selected block. The amplitude and phase of B(1,1) is denoted by a and ϕ respectively. That is $a \equiv |B(1, 1)|$ and $\phi \equiv \angle B(1, 1)$.

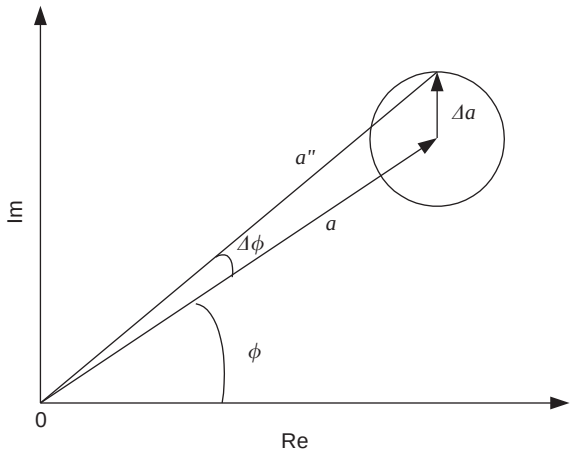

Fig. 4. The phase change of a phasor $ae^{j\phi}$ subjected to a two-dimensional additive Gaussian noise of standard deviation Δa.

2.4. Amplitude boost

In the PSK modulation, the watermark information is contained in the phase of the DFT coefficients. When a watermarked image is attacked, the DFT coefficients of the watermarked image are altered, which produces distortion when a watermark is recovered from the attacked watermarked image. Fig. 4 shows the distortion $\Delta\phi$ of a DFT coefficient of value $ae^{j\phi}$ subjected to a two-dimensional additive Gaussian noise of standard deviation Δa. From Fig. 4, we obtain

$$a'' \cos \Delta\phi = a + n_1, \tag{8}$$

$$a'' \sin \Delta\phi = n_2, \tag{9}$$

where n_1 and n_2 are two independent one-dimensional Gaussian noise of standard deviation Δa. a'' denotes the amplitude of the distorted phasor. The joint probability density function $p(n_1, n_2)$ of n_1 and n_2 is given by

$$p(n_1, n_2) = \frac{1}{2\pi\Delta a^2} \exp\left[-\frac{n_1^2 + n_2^2}{2\Delta a^2}\right]. \tag{10}$$

Expressing Eq. (10) in terms of a'' and $\Delta\phi$ by using Eqs. (8) and (9), we obtain

$$p(a'', \Delta\phi) = \frac{1}{2\pi(\Delta a)^2} \exp\left[-\frac{(a^2 - 2aa'' \cos \Delta\phi + a''^2)}{2(\Delta a)^2}\right]. \tag{11}$$

The probability density function $p(\Delta\phi)$ of $\Delta\phi$ is obtained by integrating $p(a'', \Delta\phi)$ with respect to a''. Assume $a \gg \Delta a$,

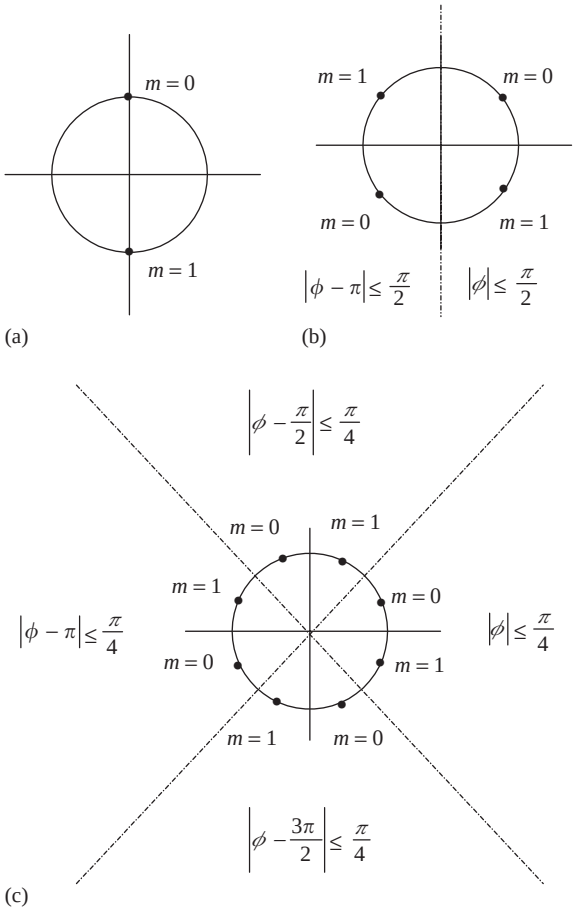

Fig. 5. The signal constellation of the PSK for (a) $s=1$, (b) $s=1/2$, and (c) $s=1/4$.

it can be shown

$$p(\Delta\phi) = \frac{1}{\sqrt{2\pi}\left(\frac{\Delta a}{a}\right)} \exp\left[-\frac{(\Delta\phi)^2}{2\left(\frac{\Delta a}{a}\right)^2}\right]. \tag{12}$$

Thus, the standard deviation of $\Delta\phi$ is equal to $\frac{\Delta a}{a}$, which shows that the distortion of a DFT coefficient due to an additive Gaussian noise is inversely proportional to the amplitude of the coefficient. In order to avoid the large distortion caused by DFT coefficients of small amplitudes, a novel strategy called AB is employed.

The AB strategy is to boost the amplitude of a selected DFT coefficient to a threshold value *th* when its value is below *th* so that the phase distortion under attacks can be keep below a certain level. In other words, after AB the amplitude of all the DFT coefficients used for embedding the secret bits are all above *th*. That is,

$$a' = \begin{cases} th, & \text{if} \quad a \leqslant th \\ a, & \text{if} \quad a > th. \end{cases} \tag{13}$$

2.5. PSK embedding

In the PSK modulation, the phase ϕ is modified into ϕ' according to

$$\phi' = \alpha(\phi, s) + s\beta(m), \tag{14}$$

where s denotes the watermark strength factor, α and β denote the offset function and the embedding function respectively given by

$$\alpha(\phi, s) = 2\pi s i, \quad \text{if } |\phi - 2\pi s i| \leqslant |\phi - 2\pi s j| \quad \text{for } j = 0, 1, 2, \ldots, \frac{1}{s} - 1,\ j \neq i \tag{15}$$

$$\beta(m) = \begin{cases} \pi/2, & \text{if} \quad m = 0 \\ -\pi/2, & \text{if} \quad m = 1. \end{cases} \tag{16}$$

Fig. 5 shows the signal constellation of the PSK modulation for $s=1$, $s=1/2$ and $s=1/4$.

3. Watermark extraction algorithm

Robustness, imperceptibility and security are three issues concerned in our watermarking scheme. In the embedding process, the DFT, the PSK modulation and the SS are used to enhance the robustness. The LABS is used to increase the imperceptibility. The SS, the TA and the set of bit sequences (PN_1, PN_2, *Key*) are hired for the security reason. In the extracting process, the secret data must be extracted from the same positions where they are embedded. Therefore, the same set of bit sequences (PN_1, PN_2, *Key*) used in the embedding process is used in the extracting process. Beside, the PSK demodulation, ISS and ITA are used in the extracting process to inverse the operations of PSK modulation, SS and TA in the embedding process respectively.

The flow chart of the recovering process is shown in Fig. 6. The watermarked image R is transformed to Z' by DFT. The same PN sequence PN_2 used in the concealing process is used to select the embedded blocks from Z' for the PSK demodulation. In the PSK demodulation, the secret bit m' is extracted from the phase ϕ'' of the selected DFT coefficient for each selected block. After all the secret bits are extracted from the PSK demodulation, they are contracted by inverse spread spectrum (ISS) and rearranged into the two-dimensional image H'. By passing H' through the inverse toral automorphism (ITA), the recovered watermark W' is obtained.

3.1. PSK demodulation

In the process of the PSK demodulation the angle ϕ'' is processed to recover the embedded secret bit m'. Let $\phi_{0,i}$ and $\phi_{1,i}$, $i = 0, 1, \ldots, \frac{1}{s} - 1$, denote the values of the PSK modulated phase for $m=0$ and 1 respectively. According to

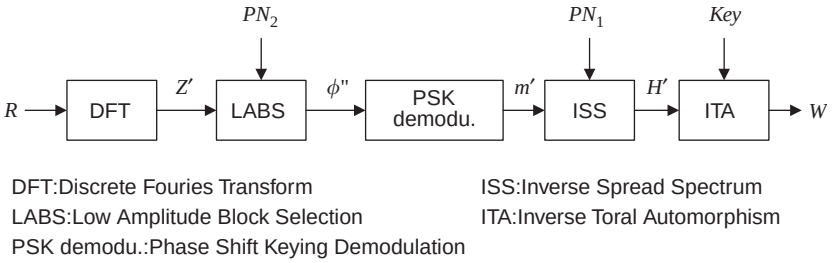

Fig. 6. The flow chart of watermark detection.

the minimum distance decision rule, m' is detected as

$$m' = \begin{cases} 0, & \text{if} \quad |\phi'' - \phi_{1i}| \leqslant |\phi'' - \phi_{jk}|, \quad j = 1,2; k = 0,1,2,\ldots,\frac{1}{s} - 1, \quad k \neq i, \quad \text{when} \quad j = 1 \\ 1, & \text{if} \quad |\phi'' - \phi_{2i}| \leqslant |\phi'' - \phi_{jk}|, \quad j = 1,2; k = 0,1,2,\ldots,\frac{1}{s} - 1, \quad k \neq i, \quad \text{when} \quad j = 2. \end{cases} \tag{17}$$

3.2. Inverse spread spectrum

Since SS expands watermark bits before embedding, they will be reconstructed by contraction. A bit $d'(j)$ in H' is obtained by contracting its expanded sequence $m'_j(i)$, $i = 1, 2, 3 \ldots l$, using $r_j(i)$ generated by PN_1. The value of $d'(j)$ is determined by

$$d'(j) = \begin{cases} 1, & \text{if } \sum_{i}^{l} m'_j(i) \oplus r_j(i) < \frac{l}{2} \\ 0, & \text{if } \sum_{i}^{l} m'_j(i) \oplus r_j(i) \geqslant \frac{l}{2} \end{cases} \quad j = 1, 2, \ldots n, \tag{18}$$

where $\oplus$ denotes the XOR operator.

4. Experimental results

Imperceptibility is an important factor for watermarking. In this paper we employ the *PSNR* to indicate the degree of transparency. The *PSNR* of R is given by

$$PSNR = 10\log_{10} \frac{255^2}{\frac{1}{N \times N} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} (X(i,j) - R(i,j))^2}, \tag{19}$$

where $X(i, j)$ and $R(i, j)$, are the gray values at (i, j) of the host image X and the watermarked image R of size $n = N \times N$, respectively. The watermark similarity measurement is dependent on factors such as the knowledge of the experts, the experimental conditions, etc. Therefore a quantitative measurement is necessary to provide fair judgment of the extracted fidelity. In this paper, we use the normalized correlation (*NC*) between the reference watermark W and the extracted watermark W' as the similarity measurement,

$$NC = \frac{\sum_i \sum_j [W(i,j)W'(i,j)]}{\sum_i \sum_j [W(i,j)]^2}. \tag{20}$$

NC is normalized by the reference watermark energy to give unity as the peak correction.

The images Lena (512×512) and Baboon (512×512) are used in simulation for demonstrating the performance of the proposed scheme. The logo image, National Cheng Kung University (32×32) in Chinese was used as the watermark. The block size used is 8×8. The values of parameters used in the simulations are: $k = 5$, $s = \frac{1}{2}$, $l = 3$, $b_1 = 3$, $b_2 = 1$, $th = 9$ for the Baboon image and $th = 13$ for the Lena image. The number of the secret bits after SS expansion is equal to $32 \times 32 \times l = 3072$. The total number of blocks is equal to $(512 \times 512) \div (8 \times 8) = 4096$. The number of blocks selected for concealing the secret bits is equal to $4096 \times \frac{b_1}{b_1 + b_2} = 3072$ which is equal to the total number of the secret bits.

Attacks include rotating, resizing, cropping, painting, blurring, noising and JPEG compression are used in the simulations to demonstrate the robustness of our scheme. For the rotating attack, the watermarked image is rotated 90° CW followed by 90° CCW before proceeding the extracting process. For the resizing attack, the watermarked image is shrunk from 512×512 to 192×192 followed by expanding from 192×192 to 512×512 before proceeding the extracting process. For the cropping attack, the watermarked image is cropped 25% before proceeding the extracting process. For the painting attack, several paints are added to the watermarked image before proceeding the extracting process. For the blurring attack, the watermarked image is blurred by Gaussian convolution before proceeding the extracting process. For the noising attack, Gaussian noises are added into the test image before proceeding extracting

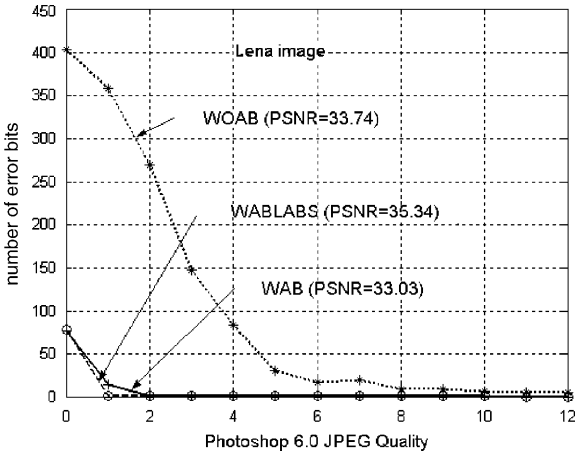

Fig. 7. Comparison of the number of the error bits of the recovered watermark among WABLABS, WAB and WOAB under the Photoshop 6.0 JPEG attack for the Lena image.

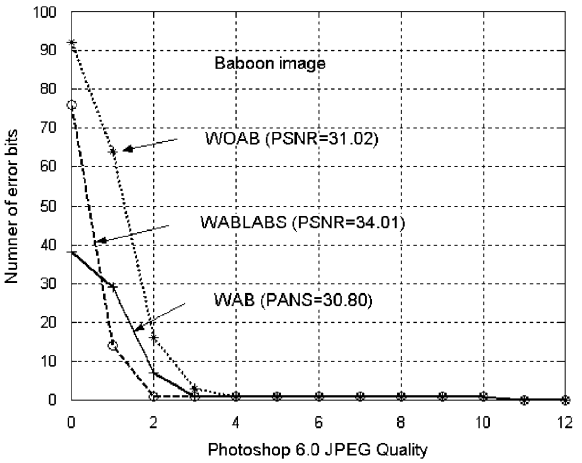

Fig. 8. Comparison of the number of the error bits of the recovered watermark among WABLABS, WAB and WOAB under the Photoshop 6.0 JPEG attack for the Baboon image.

process. Finally, the JPEG attack was used to compress the test image before proceeding extracting process.

4.1. Comparison among the WABLABS, WAB and WOAB schemes

As stated above, AB is hired to enhance the robustness while LABS is used to preserve the imperceptibility. For $b_1 = 3$ and $b_2 = 1$, LABS selects three blocks of lowest-amplitude blocks out of four in a group to embed the secret bits. The embedding scheme with AB and LABS is called WABLABS, the embedding scheme with AB but without LABS is called WAB and the embedding scheme without AB and LABS is called WOAB. In order to demonstrate the effectiveness of AB and LABS, simulations using the WABLABS, WAB and WOAB embedding schemes were conducted. Figs. 7 and 8, show the comparison results among WABLABS, WAB and WOAB from the JPEG lossy compression attacks using Photoshop 6.0 with quality levels from 0 to 12 for images Lena and Baboon, respectively. The empirical results reveal that WABLABS and WAB are significantly superior to WOAB in terms of the number of error bits. For example, under the JPEG lossy compression of quality level 1, the number of error bits is 1 for WABLABS, 14 for WAB and 358 for WOAB for the Lena image; and 14 for WABLABS, 29 for WAB and 64 for WOAB for the Baboon image. The empirical results also reveal that WABLABS is superior to WAB in terms of the PSNR for both Lena and Baboon images, for example, the PSNR of the watermarked images are 35.34 for the WABLABS and 33.03 for the WAB for the Lena images; and 34.01 for the WABLABS and 30.80 for the WAB for the Baboon images, respectively. Thus, the combination of AB and LABS in the embedding scheme is very effective in reducing the bit error of the reconstructed watermark and raising the PSNR of the embedded image.

Tables 1 and 2 show the empirical comparison results among WABLABS, WAB and WOAB under the rotating, resizing, cropping, painting, noising and blurring attacks for the Lena and Baboon images, respectively. From the results, we find that the numbers of error bits of the WABLABS and the WAB scheme are both lower than those of the WOAB scheme. The numbers of error bits of the WABLABS and the WAB are about the same, but the PSNR of the WABLABS is higher than that of the WAB by 2.3 db for the Lena image and 3.2 db for the Baboon image, respectively. This shows that the WABLABS scheme is superior to the WAB scheme and the WOAB scheme.

Fig. 9 shows the original image and the watermarked images of the WABLABS embedding scheme. The PSNR of the watermarked images are 35.34 and 34.01 for the Lena and Baboon images, respectively. From Fig. 9, one could hardly perceive the difference between the watermarked image and the original image.

The normalized correlation and the extracted watermarks corresponding to Figs. 7 and 8 are shown in Table 3 and Fig. 10, as well as Table 4 and Fig. 11, respectively. From the test results, the values of *NC* are all above 0.91 and the extracted watermarks are clearly identified by the human vision.

Fig. 12 a–f show the 90° rotated, the resized, the cropped, the painted, the noised, and the blurred watermarked images and Fig. 12g–l show their corresponding extracted watermarks using the WABLABS scheme for the Baboon image. The corresponding numbers of error bits of the extracted watermarks are listed in Table 2. The visual quality of the extracted watermarks revealed in Fig. 12g–l demonstrated that our proposed scheme can sustain all the above attacks.

Table 1
Comparison of the number of the error bits of the recovered watermark among WABLABS, WAB and WOAB under various attacks for the Lena image

Item	Parameter	WABLABS PSNR = 35.34	WAB PSNR = 33.03	WOAB PSNR = 33.74
Rotating	90° rotated	0	0	5
Resizing	From 512 × 512 to 192 × 192	60	63	209
Cropping	Cropping a quarter image	84	42	25
Painting	Painting three bars	57	25	42
Noising	15.06% noises contamination	104	72	292
Blurring	Gaussian blurring ratio 2.0	74	74	255

Table 2
Comparison of the number of the error bits of the recovered watermark among WABLABS, WAB and WOAB under various attacks for the Baboon image

Item	Parameter	WABLABS PSNR = 34.01	WAB PSNR = 30.80	WOAB PSNR = 31.02
Rotating	90° rotated	0	0	1
Resizing	From 512 × 512 to 192 × 192	129	157	175
Cropping	Cropping a quarter image	81	24	71
Painting	Painting three bars	47	19	30
Noising	15.06% noises contamination	66	67	57
Blurring	Gaussian blurring ratio 1.4	73	107	110

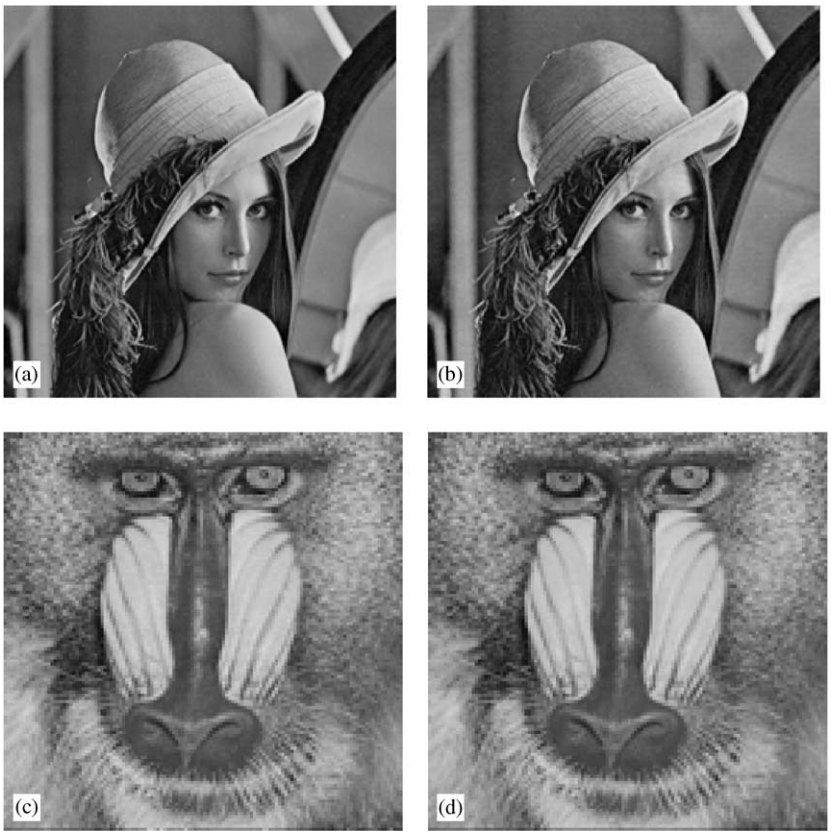

Fig. 9. (a) the original image of Lena, (b) the embedded image of Lena with the *PSNR* = 35.34, (c) the original image of Baboon, (d) the embedded image of Baboon with *PSNR* = 34.01.

Table 3
The NC values corresponding to the number of error bits for the image Lena shown in Fig. 7

Quality level	0	1	2	3	4	5	6	8	10	12
Error bits no	78	1	0	0	0	0	0	0	0	0
NC	0.92	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0

Fig. 10. The extracted watermarks corresponding to the number of error bits for the image Lena shown in Fig. 7.

Table 4
The NC values corresponding to the number of error bits for the image Baboon shown in Fig. 8

Quality level	0	1	2	3	4	5	6	8	10	12
Error bits no	76	29	2	0	0	0	0	0	0	0
NC	0.91	0.95	0.99	1.0	1.0	1.0	1.0	1.0	1.0	1.0

Fig. 11. The extracted watermarks corresponding to the number of error bits for the image Baboon shown in Fig. 8.

4.2. Comparison with the Hsu scheme

The comparison of the NC value under JPEG lossy compression attacks between the Hsu scheme [4] and our scheme is listed in Table 5. From Table 5, the NC values of our proposed scheme is higher than those of the Hsu scheme, the difference becomes significant as compression rate is greater than 7.16. The comparison of image manipulation attacks between the two schemes is listed in Table 6, which indicates that our scheme can sustain the rotation and the resampling attacks which the Hsu scheme cannot.

4.3. Comparison between the FSK scheme and the PSK scheme

The FSK scheme proposed by the authors [17] was shown to be superior to the watermarking schemes based on the amplitude shift keying. The comparison between our proposed PSK and FSK schemes is listed in Table 7. The results revels that the PSK scheme is superior to the FSK scheme on encountering strong noise attacks. As for the best choice of the s value in the PSK scheme, Fig. 13 shows the noise performance of the PSK scheme for the case of $s=1$, $s=1/2$ and $s=1/4$ under the same condition. According to the results, the case $s=1$ can sustain 22% noise attack, the case $s=1/2$ can sustain 18% noise attacks and the case $s=1/4$ can only sustain 3% noise attacks. However, the PSNR is 34.1 for the case $s=1$, 35.21 for the case of $s=1/2$ and 37.1 for the case of $s=1/4$. When robustness and imperceptibility are both considered, $s=1/2$ is the best choice.

5. Conclusions

Digital watermarking is a potential method to discourage unauthorized copying or attest origin of digital data that includes audio, video and images. In this paper we present a robust watermarking scheme for still images using PSK with amplitude boost and low amplitude block selection. The amplitude boost strategy is used to enhance the robustness and the low amplitude block selection strategy is used to reduce the degradation of the host image caused by watermark concealing. Empirical results show that the proposed scheme can sustain attacks like JPEG lossy compression,

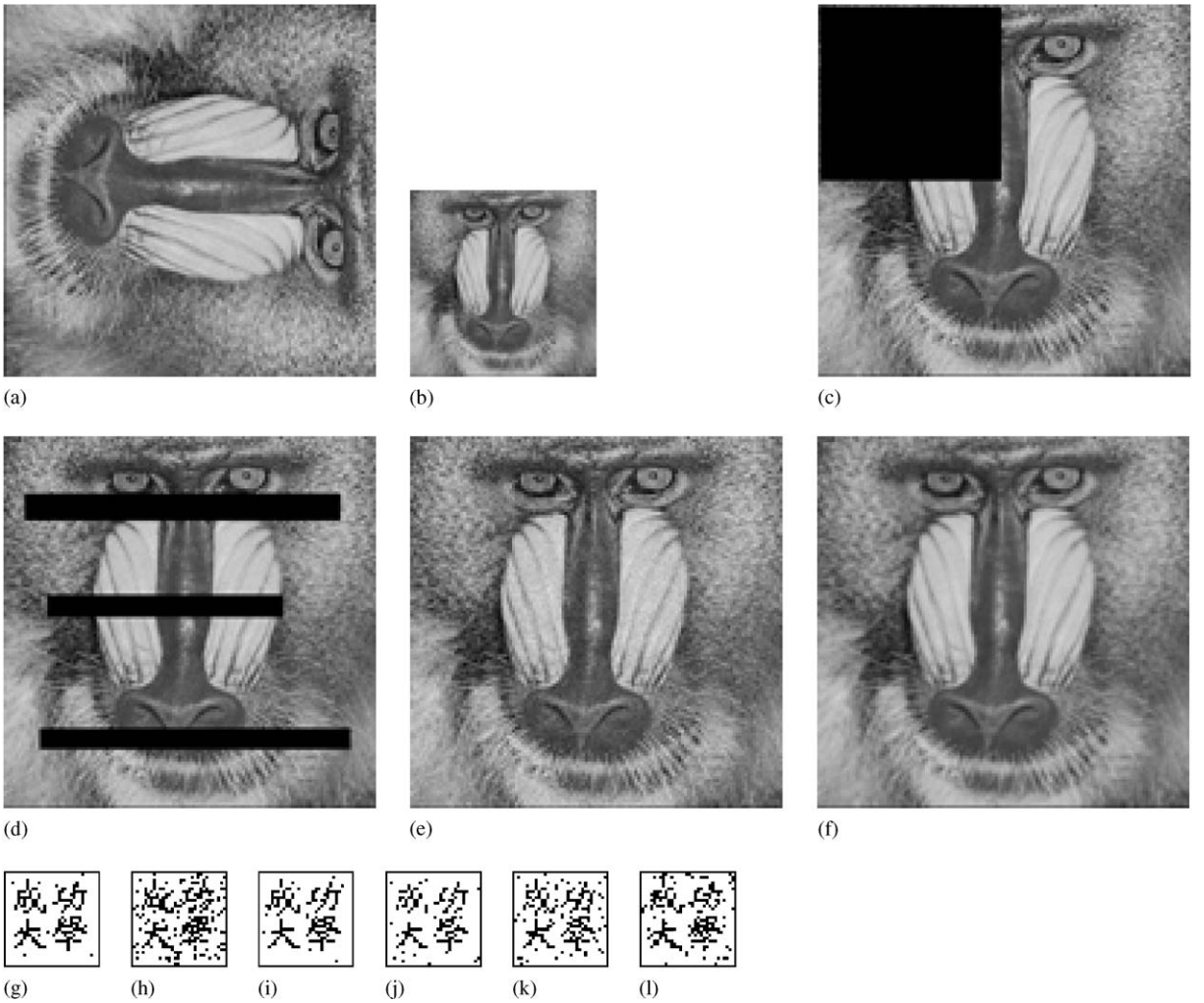

Fig. 12. The attacked watermarked images (a)–(f), (a) the 90° rotated, (b) the resized, (c) the cropped, (d) the painted, (e) the noised, and (f) the blurred. The corresponding extracted watermarks (g)–(l), (g) the 90° rotated, (h) the resized, (i) the cropped, (j) the painted, (k) the noised, and (l) the blurred.

Table 5
The performance comparison of the NC value under JPEG lossy compression attacks between the proposed scheme and the Hsu's scheme for Lena image

Compression ratio	3.49	4.41	5.18	5.92	6.55	7.16	7.81	8.46	9.05	9.81	10.74
Our scheme	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	0.920
The Hsu's scheme [4]	0.999	0.98	0.998	0.990	0.942	0.883	0.830	0.726	0.661	0.493	0.431

Table 6
The performance comparison of the image manipulation attacks between the proposed scheme and the Hsu's scheme for Lena image

Attack item	Cropping	Resampling	Painting	Blurring	Noising	Rotating
Our scheme	Pass	Pass	Pass	Pass	Pass	Pass
The Hsu's scheme [4]	Pass	Fail	No test	Pass	No test	Fail

Table 7
The performance comparison of the image manipulation attacks between the PSK scheme and the FSK scheme for Lena image

Attack item	Cropping	Resampling	Painting	Blurring	Rotating	Noising (6.86%)	Noising (15.06%)
PSK scheme	Pass	Pass	Pass	Pass	Pass	Pass	Pass
FSK scheme [17]	Pass	Pass	Pass	Pass	Pass	Pass	Fail

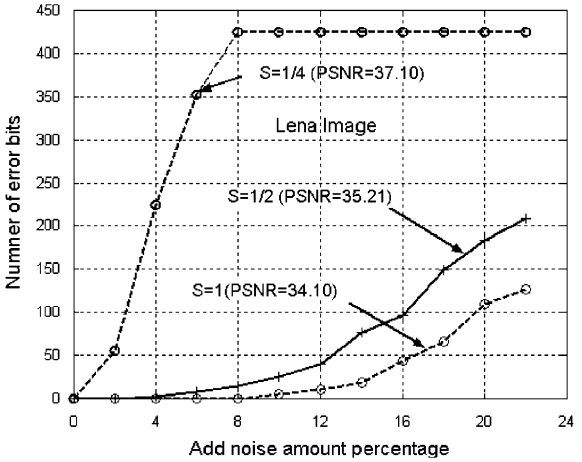

Fig. 13. Number of error bits vs. noise percentage with the watermarking strength $s = 1$, $s = 1/2$ and $s = 1/4$ for Lena image.

rotation, resizing, cropping, painting, noising and blurring. From the experiment results, we can see that the WABLABS scheme with AB and LABS properly combined is superior to the scheme without. Furthermore, the AB strategy is especially effective at encountering the resizing, noising and blurring attacks for which the WOAB scheme simply fails for the smooth images like Lena. The other advantage of our scheme is that the original host image and watermark are not needed during the watermark detection process.

References

[1] C.I. Podilchuk, W. Zeng, Image-adaptive watermarking using visual models, IEEE Trans. on Selected Area in Communications 16 (4) (1998) 525–539.

[2] W.N. Lie, L.C. Chang, Spatial-domain image watermarking by data embedding at adaptive bit position, Proceedings of the IPPR Conference on Computer Vision, Graphics and Image Processing, 1999, pp. 16–21.

[3] S.C. Pei, Y.H. Chen, R.F. Torng, Digital image and video watermarking utilizing just-noticeable-distortion model, IPPR Conference on Computer Vision, Graphics and Image Processing, 1999, pp. 174–182.

[4] C.T. Hsu, J.L. Wu, Hidden Digital Watermarks in Images, IEEE Trans. on Image Processing 8 (1) (1999) 58–68.

[5] C.T. Hsu, J.L. Wu, DCT-Based Watermarking for Video, IEEE Trans. on Consumer Electronics 44 (1) (1998) 206–216.

[6] C.F. Wu, W.S. Hsieh, Digital Watermarking Using ZeroTree of DCT, IEEE Trans. on Consumer Electronics 46 (1) (2000) 87–94.

[7] G.C. Langelaar, R.L. Lagendijk, Optimal Differential Energy Watermarking of DCT Encoded Images and Video, IEEE Trans. on Image Processing 10 (1) (2001) 148–158.

[8] M.J. Tsai, K.Y. Yu, Y.Z. Chen, Joint Wavelet and Spatial Transformation for Digital Watermarking, IEEE Trans. on Consumer Electronics 46 (1) (2000) 241–245.

[9] Z.H. Wei, P. Qin, Y.Q. Fu, Perceptual digital watermark of images using wavelet transform, IEEE Trans. on Consumer Electronics 44 (4) (1998) 1267–1272.

[10] Z.M. Lu, S.H. Sun, Digital image watermarking technique based on vector quantization, Electron. Lett. 36 (4) (2000) 303–305.

[11] H. Inoue, A. Miyazaki, A. Yamamoto, T. Katsura, A digital watermark technique based on the wavelet transform and its robustness on image compression and transformation, IEICE Trans. Fundamentales E 82-A (1) (1999) 2–10.

[12] N. Kaewkamnerd, K.R. Rao, Wavelet based image adaptive watermarking scheme, Electron. Lett. 36 (4) (2000) 312–313.

[13] J.J.K. Q Ruanaidh, W.J. Dowling, F.M. Boland, Phase watermarking of digital images, IEEE Int. Conf. on Image Process. 3 (1996) 239–242.

[14] J.J.K. Q Ruanaidh, T. Pun, Rotation, Scale and Translation Invariant Digital Image Watermarking, IEEE Int. Conf. Image Process. 1 (1997) 536–539.

[15] P. Premaratne, C.C. Ko, A novel watermark embedding and detection scheme for images in DFT domain, IEEE Int. Conf. Image Process. and its Appl. 2 (1999) 780–783.

[16] V. Solachidis, I. Pitas, Circularly symmetric watermark embedding in 2-D DFT domain, IEEE Trans. Image Process. 10 (465) (2001) 1741–1753.

[17] Wen-Yuan Chen, Chin-Hsing Chen, Robust watermarking scheme for still images using frequency shift keying with high-variance block selection, Opt. Eng. 42 (6) (2003) 1826–1835.

[18] S. Haykin, Communication System, third ed., Wiley, New York, 1994.

[19] G. Voyatzis, I. Pitas, Application of Toral automorphisms in Image Watermarking, IEEE Int. Conf. Image Process. 3 (1996) 237–240.

[20] I.J. Cox, J. Kilian, F.T. Leighton, T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Trans. Image Process. 6 (12) (1997) 1673–1687.

[21] L.M. Marvel, C.G. Boncele Jr., C.T. Retter, Spread spectrum image steganography, IEEE Trans. on Image Process. 8 (8) (1999) 1075–1083.

[22] S. Voloshynovskiy, S. Pereira, T. Pun, J. Eggers, J.K. Su, Attacks on digital watermarks: classification, estimation-based attacks, and benchmarks, IEEE Commun. Mag. (2001).

About the Author—WEN-YUAN CHEN was born in Taichung, Taiwan, in 1957. He received the B.S. and M.S. degrees in Electronic Engineering from National Taiwan University of Science and Technology in 1982 and 1984, respectively, and the Ph.D. degree in Electrical Engineering from National Cheng Kung University at Tainan Taiwan, in 2003. Since 2003, he has been an associate professor with the department of Electronic Engineering at National Chin-Yi Institute of Technology. His research interests include digital signal processing, image compression, pattern recognition and watermarking.

About the Author—CHIN-HSING CHEN received the B.S. degree in electrical engineering from National Taiwan University, Taiwan, in 1980, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of California at Santa Barbara, in 1983 and 1987, respectively. Since 1988, he has been with the Department of Electrical Engineering at National Cheng Kung University in Taiwan where he is now a professor. His current research interests include pattern recognition, image processing and VLSI array design. He has published over 160 papers and given more than 80 technical presentations in public in more than 15 countries.