Journal of Electronic Imaging

SPIEDigitalLibrary.org/jei

Robust copyright-protection scheme based on visual secret sharing and Bose–Chaudhuri–Hocquenghem code techniques

Tzuo-Yau Fan
Bin-Chang Chieu
Her-Chang Chao

SPIE

IS&T imaging.org

Robust copyright-protection scheme based on visual secret sharing and Bose–Chaudhuri–Hocquenghem code techniques

Tzuo-Yau Fan
Bin-Chang Chieu
National Taiwan University of Science and Technology
Department of Electronic Engineering
Taipei, Taiwan

Her-Chang Chao
Ming Chuan University
Department of Computer Science and Information Engineering
Taoyuan, Taiwan
E-mail: herchang@mail.mcu.edu.tw

Abstract. *A robust copyright scheme for image protection based on visual secret sharing (VSS) and Bose–Chaudhuri–Hocquenghem (BCH) code techniques is proposed. This scheme not only maintains the quality of a host image without the change of any pixel value but also generates a meaningful ownership share to improve the management of image copyright. In addition, no codebook is required to store, and the watermark size is independent of the host image. The robustness of watermarking can be enhanced by BCH code. The proposed scheme contains ownership share construction and watermark extraction. In the first phase, an encoded watermark is generated by BCH code from a watermark. Next, an image feature is then extracted by the discrete wavelet transform decomposing from the host image. Finally, an ownership share can be generated by VSS technique from the image feature and the encoded watermark. In the second phase, a master share can be produced from a suspect image. By stacking the master and the ownership shares and using BCH code, an extracted watermark can be obtained. The experimental results show that the proposed scheme using the BCH(15,5) has better robust performance and practicability than existing schemes. © 2012 SPIE and IS&T.* [DOI: 10.1117/1.JEI.21.4.043018]

1 Introduction

In the past two decades, as the Internet has become popular, the distribution of digitized data (e.g., digital images, MP3, and video) has made it faster and easier to reproduce misappropriated data without the owner's consent, resulting in loss and damage to intellectual property. Thus, authentication and copyright protection from illegitimate manipulation of digital images and video have become necessary concerns in the Internet era.

The proposed digital watermarking technique provides a solution for the protection of intellectual property. Digital watermarking can embed a logo into the digital media for verification. The logo is then called a watermark. Depending on the embedding domain, watermarking technique can be classified into two categories: (a) spatial domain technique and (b) transform domain technique. The spatial domain technique embeds a watermark by directly modifying the pixel values of a host image. This scheme has an advantage of rapid process speed, but it cannot resist various image processing attacks. The transform domain technique embeds a watermark by modifying the coefficients in the frequency domain of a host image. The transformation approaches employ the discrete Fourier transform,[1] the discrete cosine transform (DCT),[2] or the discrete wavelet transform (DWT)[3,4] to generate the frequency coefficients of the host image. In general, the watermark embedded into the transform domain has higher robustness than the spatial domain.[5] In addition, the Refs. 6 and 7 suggest that watermarks should be encrypted by an error control code (ECC) before being embedded into host image. ECC can enhance the robustness of watermarking. However, the above watermarking schemes may adjust the pixel value of the host image and decrease the image quality. These schemes cannot be suitable for images that require maintenance of the image quality, such as military images, medical images, etc.

There are several watermarking schemes,[8–10] called reversible watermarking, that can recover the protected host image from the watermarked image in an extracting procedure. Unfortunately, these schemes focus on the relationship between the amount of embedded information and the quality of the embedded image, and ignore the watermark antidestruction. Moreover, the distorted watermarked image is not suitable for artistic appreciation.

In recent years, a number of scholars[11–18] have begun to focus on image copyright protection based on a combination of the visual secret sharing (VSS)[19] and traditional watermarking techniques. In this scheme, a verification image, called ownership share, can be produced from the host image feature and watermark; then the ownership share is registered to a certified authority (CA). In watermark extraction, the

Paper 12031 received Feb. 10, 2012; revised manuscript received Sep. 7, 2012; accepted for publication Nov. 7, 2012; published online Dec. 3, 2012.

host image is used to generate a master image, called master share. An extracted watermark can be extracted by stacking the master share and the ownership share. The main purpose of the above robust watermarking schemes is to retain the watermark information when the digitized data is attacked or modified; furthermore, these techniques not only protect the intellectual property of the host image and achieve high security by VSS, but also maintain the quality of the host image.

Chang et al. proposed a copyright protection scheme[11] based on VSS in the spatial domain; however, the robustness of this scheme has a tendency to decrease when the JPEG compression ratio increases.[13] Hsu et al. adopted VSS and statistics in the spatial domain to achieve the requirements of robustness and security.[12] Based on DWT and VSS, Hsieh et al. proposed a copyright protection scheme[13] to resist common image processing attacks. Other copyright protection schemes based on DWT and VSS have been presented in the last few years.[14–16] Based on the singular value decomposition (SVD) and VSS, Wang et al. proposed a copyright protection scheme[17] that can use a watermark with arbitrary size; however, a CA needs to store the codebook. In the following year, Wang et al. proposed a copyright protection scheme[18] based on DCT and VSS, and a codebook is not required. However, the ownership shares from the above-mentioned copyright protection schemes, except for one method,[11] are noise-like binary images. The management of ownership share is difficult when the legal owner or creator owns more than one image.

In this paper, a novel robust copyright scheme for image protection based on VSS and Bose–Chaudhuri–Hocquenghem (BCH) code is proposed. This scheme will give the ownership share a specific pattern for ease of management. Besides, the robustness of watermarking can be enhanced by BCH code. Then the ownership share is registered to a CA who does not require any codebook. The owner is the only one who has a secret key, which can protect the watermark information. In addition, the protected image will not cause any distortion.

The plan of the paper is as follows. Section 2 briefly presents the concepts of VSS, BCH code, and DWT techniques. Section 3 presents the algorithm of proposed scheme. Several simulation examples are provided in Sec. 4. Finally, we conclude this paper in Sec. 5.

2 Related Techniques

This section describes the basic concepts of the techniques, including VSS, BCH code, and DWT.

2.1 *VSS*

The core of the proposed copyright protection scheme is the VSS technique, which was first formally introduced by Naor and Shamir.[19] By (k, n)-VSS technique, a secret image can be encoded into n shares. The decryption process is performed by stacking any k or more shares, and the secret image can be visualized by the human visual system without any complex cryptographic computation. This can achieve the purpose of VSS technique. In this paper, the (2, 2)-VSS technique is used for the proposed copyright scheme for image protection. Figure 1 shows the encryption/decryption process flow of traditional (2, 2)-VSS.

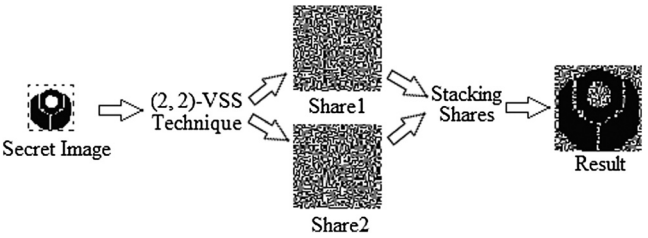


Fig. 1 Encryption/decryption process flow of traditional (2, 2)-VSS.

2.2 *BCH Code*

BCH code[20–22] is one of ECC, and it is a technique that can decrease error occurrence during signal transmission. BCH code is an abbreviation of Bose, Chaudhuri and Hocquenghem, and it belongs to the linear cyclic code group. By the linear cyclic code, the transmitted signal information can be separated into many blocks with fixed length; then the block can be encoded into an encoded block. Due to the addition of redundancy bits, the number of the digit in the encoded block is larger than that of the original block. During decryption, errors can be corrected based on the features.

If original signal information has q digits, the encoded block will have p bits. In the encoded block, there are q bits which are the same as a part of the original signal, and $p - q$ bits which are generated by encryption. The $p - q$ bits are called the generalized parity check bits or parity bits. Any positive integer m and t that satisfy $m \geq 3$ and $t < 2^m - 1$ can construct a binary BCH(p, q) to meet the following parameters:

$$\text{Code Length}: p = 2^m - 1$$

$$\text{Number of Parity Check Digits}: p - q \leq mt$$

$$\text{Minimum Distance}: d \geq 2t + 1$$

The BCH(p, q) having the above parameters can correct errors of combination equal to or smaller than t, known as the t-error correcting BCH code.

2.3 *DWT*

The DWT[4] is one of the techniques to decompose an image by rows, then by columns into four quarters, as shown in Fig. 2. The upper-left quarter is called an LL (low-low) sub-band, which is a half-sized version of the image. The other quarters are low-high (LH), high-low (HL), and high-high (HH) sub-bands. These quarters contain the high-frequency edge of the image. In general, the LL sub-band contains most of the information of the image. The same process can repeat to generate the next level sub-band of decomposition from

Fig. 2 1-level DWT decomposition of an image.

the LL sub-band, in that we have a smaller version of the LL sub-band at upper-left quarter, and so on.

3 Proposed Scheme

In this section, a novel robust copyright scheme for image protection based on VSS and BCH code is proposed. The flow for image protection scheme is shown in Fig. 3. It is divided into two phases: ownership share construction and watermark extraction. In the ownership share construction phase, BCH code encodes a watermark into an encoded watermark. By setting the three least significant bits (LSBs) of the pixel values of a host image to 0, we have a retained image. Besides, the feature of the host image is extracted by the DWT decomposing from the retained image. Using a secret key to randomly select the coefficients from the image feature, a master matrix is formed. Moreover, a three-level quantized image is produced by scaling the host image to the size of watermark in order to create a meaningful ownership share that is similar to the host image in the vision. According to VSS, the meaningful ownership share can be generated from the master matrix, the quantized image, and the encoded watermark. In the watermark extraction phase, a suspect master matrix is extracted from the suspect image by the above procedures in the ownership share construction phase with the secret key; moreover, a master share can be created according to the magnitude between the pixel values in the nonoverlapping block of the master matrix. Stacking the master share and the ownership share, the encoded watermark can be obtained. BCH code decrypts the encoded watermark into the watermark. The scheme is described hereinafter.

3.1 *Ownership Share Construction*

An $m \times m$ binary watermark $\mathbf{W}$ is encoded by every q pixels through the BCH(p, q) along the column and row to produce an encoded watermark $\mathbf{W}'$ with size $(pm/q) \times (pm/q)$. To improve the security of the encoded watermark, a scrambled watermark, $\mathbf{E}$, is processed with a scrambled pixel arrangement according to the method of torus automorphism (TA) proposed by Voyatzis and Pitas.[23] The TA function is defined as

$$\begin{bmatrix} \tilde{x} \\ \tilde{y} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ \alpha & \alpha+1 \end{bmatrix}^t \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{1}$$

where N denotes the size of an image, α is an adjustable integer between 1 to N, (x, y) is the original coordinate of a certain pixel, and $(\tilde{x}, \tilde{y})$ is the new coordinate of (x, y) after t times of the TA transformation. In addition, the TA function is periodic by T, which means that all the original pixel coordinates will return to their starting values after T times of the TA transformation.

Assume that $\mathbf{H}$ denotes an $M \times N$ 256-level host image. Since the most significant bit (MSB) of each pixel of a host image has the greatest effect in terms of the pixel value, we let the three LSBs of pixels of $\mathbf{H}$ be 0 so as to enhance the feature of $\mathbf{H}$. Therefore, a retained image $\mathbf{H}'$ can be formed. The $\mathbf{H}'$ is then partitioned into $k \times k$ nonoverlapping retained blocks $\mathbf{H}'_i$, $i = 1, \ldots, (M/k)(N/k)$. All of the LL_n coefficients by n-level DWT decomposing $\mathbf{H}'_i$, $i = 1, \ldots, (M/k)(N/k)$, form a coefficient matrix $\mathbf{F}_c$ sized $(M/k) \times (N/k)$, where $n = \log_2 k$. Next, we utilize a secret key K to randomly select the coefficients from $\mathbf{F}_c$, a master matrix $\mathbf{A}$ with size $(pmb/q) \times (pmb/q)$ is formed. The $\mathbf{A}$ is then partitioned into $b \times b$ nonoverlapping master blocks $\mathbf{A}_i$, $i = 1, \ldots, (pm/q) \times (pm/q)$.

By scaling the host image $\mathbf{H}$ to the size of $(pm/q) \times (pm/q)$ and uniformly quantizing the scaled pixel value to three-level value, (i.e., 0, 1, and 2), a quantized image $\mathbf{G}$ of size $(pm/q) \times (pm/q)$ is produced. The master block $\mathbf{A}_i$, and the pixel values e_i and g_i, $i = 1, \ldots, (pm/q) \times (pm/q)$,

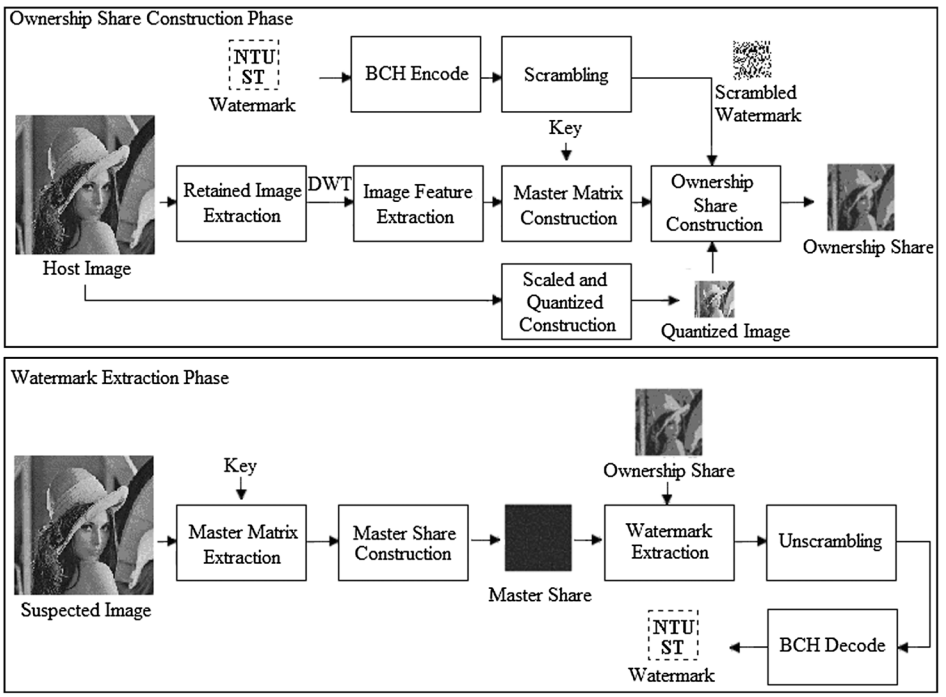


Fig. 3 Proposed scheme flow diagram.

are sequentially selected from $\mathbf{A}$, $\mathbf{E}$, and $\mathbf{G}$ to map the following three rules to produce the $b \times b$ block $\mathbf{O}_i$ of an ownership share $\mathbf{O}$ of size $(pmb/q) \times (pmb/q)$.

a. Assume that the pixel value e_i equals 0, the maximum coefficient in the master block $\mathbf{A}_i$ is set to be 0 while the $b - g_i$ coefficients are set to be 0 by randomly selecting. The others are set to be 1.
b. Assume that the pixel value e_i equals 1, the maximum coefficient in the master block $\mathbf{A}_i$ is set to be 1 while the $b - g_i + 1$ coefficients are set to be 0 by randomly selecting. The others are set to be 1.
c. The block $\mathbf{O}_i$ is then a duplicate of $\mathbf{A}_i$.

A coefficient of 1 corresponds to white and 0 represents black. After each of master block $\mathbf{A}_i$ is correspondingly mapped with the pixel value e_i, all of the $\mathbf{O}_i$ blocks can form the ownership share $\mathbf{O}$. According to the pixel value g_i, each $\mathbf{O}_i$ contains different number of black pixels. We utilize the density of black pixels to simulate the ownership share as a three-level image by the human visual system and similar the host image. This is reasonable, since the black pixels in the ownership share are dense (sparse) when the corresponding area of the host image is relatively darker (brighter). The ownership share construction algorithm is as follows:

Algorithm 1 Ownership share construction.

Input: Host image $\mathbf{H}$ with size $M \times N$; secret key K; watermark $\mathbf{W}$ with size $m \times m$; parameters p and q of BCH code; retained block size k; master block size b.

Output: Ownership share $\mathbf{O}$ with size $(pmb/q) \times (pmb/q)$.

Step 1: Form a retained image $\mathbf{H}'$ by setting all of the three LSBs of the pixel values of $\mathbf{H}$ to 0.

Step 2: Partition the retained image $\mathbf{H}'$ into nonoverlapping $k \times k$ retained blocks $\mathbf{H}'_i$, $i = 1, \cdots, (M/k)(N/k)$, and decompose each retained block $\mathbf{H}'_i$ by n-level DWT to form a coefficient matrix $\mathbf{F}_c$ of size $(M/k) \times (N/k)$ from the LL_n coefficients.

Step 3: Form a master matrix $\mathbf{A}$ of size $(pmb/q) \times (pmb/q)$ by the secret key K to randomly select the coefficients from $\mathbf{F}_c$.

Step 4: Extract the nonoverlapping master block $\mathbf{A}_i$, $i = 1, \ldots, (pm/q) \times (pm/q)$, by the size of $b \times b$ from $\mathbf{A}$.

Step 5: Scale the host image $\mathbf{H}$ and quantize the scaled pixel value to produce a three-level quantized image $\mathbf{G}$ of size $(pm/q) \times (pm/q)$.

Step 6: Encode the binary watermark $\mathbf{W}$ to generate an encoded watermark $\mathbf{W}'$ of size $(pm/q) \times (pm/q)$ by BCH(p, q).

Step 7: Scramble $\mathbf{W}'$ and generate a scrambled watermark $\mathbf{E}$ by TA.

Step 8: Generate an ownership share $\mathbf{O}$ according to the rules of (a)–(c) with the pixels g_i and e_i, and the master block $\mathbf{A}_i$, $i = 1, \ldots, (pm/q) \times (pm/q)$.

Step 9: Register the $\mathbf{O}$ to CA.

4 Watermark Extraction

When the image owner wants to verify the ownership of a suspect image $\tilde{\mathbf{H}}$ with size $M \times N$, a watermark $\tilde{\mathbf{W}}$ of size $m \times m$ is extracted as follows. Steps 1 to 4 of the ownership share construction algorithm are performed to generate the $b \times b$ nonoverlapping master blocks $\tilde{\mathbf{A}}_i$, $i = 1, \ldots, (pm/q) \times (pm/q)$, which are the partition blocks of a master matrix $\tilde{\mathbf{A}}$. The maximum coefficient of each master block $\tilde{\mathbf{A}}_i$ is set to 1; the others are set to 0. We can then form a binary master share $\mathbf{M}$ of size $(pmb/q) \times (pmb/q)$ by merging $\tilde{\mathbf{A}}_i$, $i = 1, \ldots, (pm/q) \times (pm/q)$, for verifying the suspect image $\tilde{\mathbf{H}}$. Based on Eq. (2), a $(pmb/q) \times (pmb/q)$ stacked image $\mathbf{D}$ can be generated.

$$d_i = m_i \wedge o_i, \qquad i = 1, \ldots, (pmb/q)(pmb/q), \tag{2}$$

where m_i and o_i are the pixel values of $\mathbf{M}$ and $\mathbf{O}$, respectively. The symbol $\wedge$ denotes the AND logical operation. In the stacked image $\mathbf{D}$, each nonoverlapping $b \times b$ block $\mathbf{D}_i$, $i = 1, \ldots, (pm/q)(pm/q)$, is used to generate a pixel value $\tilde{e}_i$ of a scrambled watermark $\tilde{\mathbf{E}}$ according to Eq. (3).

$$\tilde{e}_i = \begin{cases} 1, & \text{if } \sum_{x=1}^{b} \sum_{y=1}^{b} \mathbf{D}_i(x, y) = 1 \\ 0, & \text{otherwise} \end{cases}. \tag{3}$$

At last, the pixel position of scrambled watermark $\tilde{\mathbf{E}}$ can be restored by TA, and an encoded watermark $\tilde{\mathbf{W}}'$ is extracted. BCH(p, q) can decode $\tilde{\mathbf{W}}'$ into an extracted watermark $\tilde{\mathbf{W}}$. The ownership of the suspect image $\tilde{\mathbf{H}}$ can be verified by observing $\tilde{\mathbf{W}}$. The watermark extraction algorithm is as follows:

Algorithm 2 Watermark extraction.

Input: Suspect image $\tilde{\mathbf{H}}$ with size $M \times N$; ownership share $\mathbf{O}$ with size $(pm/q) \times (pm/q)$; secret key K; parameters p and q of BCH code; retained block size k; master block size b.

Output: Extracted watermark $\tilde{\mathbf{W}}$ with size $m \times m$.

Step 1: Generate the $b \times b$ nonoverlapping master blocks $\tilde{\mathbf{A}}_i$, $i = 1, \ldots, (pm/q) \times (pm/q)$, which are the partition blocks of the master matrix $\tilde{\mathbf{A}}$ from the suspect image $\tilde{\mathbf{H}}$, according to steps 1 through 4 of the ownership share construction algorithm.

Step 2: Set the maximum coefficient of each master block $\tilde{\mathbf{A}}_i$, $i = 1, \ldots, (pm/q) \times (pm/q)$, to 1; the others to 0. The master share $\mathbf{M}$ is a duplicate of $\tilde{\mathbf{A}}$.

Step 3: Generate a stacked image $\mathbf{D}$ from $\mathbf{M}$ and $\mathbf{O}$ by Eq. (2).

Step 4: Generate a scrambled watermark $\tilde{\mathbf{E}}$ from $\mathbf{D}$ by Eq. (3).

Step 5: Restore the pixel position of $\tilde{\mathbf{E}}$ by TA, and generate an encoded watermark $\tilde{\mathbf{W}}'$.

Step 6: Apply BCH(p, q) to decode $\tilde{\mathbf{W}}'$ and construct an extracted watermark $\tilde{\mathbf{W}}$.

5 Experimental Results

The original images were damaged and attacked in the experiment, and then the attacked images were used for image verification. Figure 4(a) and 4(b) shows two 256-level host images, Lena and F16 of the same size 512×512, were used in the experiment. Figure 4(c) and 4(d) shows two binary watermarks with size 35×35 and 32×32, respectively. The size of the nonoverlapping master block is 2×2. In the following robustness experiment, several common attacks were

(a) (b)

(c) (d)

Fig. 4 Experimental images and watermarks. (a) Lena (512 × 512); (b) F16 (512 × 512); (c) watermark (35 × 35); and (d) watermark (32 × 32).

Table 1 Image attack parameters.

Attack	Parameter
JPEG	Quality factor = 10%
Gaussian noise	mean = 0 variance = 0.05
Salt-pepper noise	Noise density = 20%
Gaussian blur	Radius = 9
Median filtering	Window size = 4 × 4
Rotation	Rotate 3 degrees
Cropping	Cropped area of 25%
Scaling	Reduced 1/16
Sharpening	Standard Laplacian sharpening
Mixed	JPEG, Gaussian noise and sharpening

used to measure the robustness of the proposed scheme, such as JPEG compression, Gaussian noise, salt-pepper noise, Gaussian blur, median filtering, rotation, cropping, scaling, sharpening, and mixed. Table 1 lists several common attacks and their parameters.

Peak signal to noise ratio (PSNR) and the normalized correlation (NC) are adopted to test the indicators of the image distortion and the robustness of watermarking. PSNR is defined as follows:

$$\mathrm{PSNR} = 10 \times 1\log_{10}\left(\frac{255^2}{\mathrm{MSE}}\right)(\mathrm{dB}) \tag{4}$$

$$\mathrm{MSE} = \frac{1}{M \times N}\sum_{x=1}^{M}\sum_{y=1}^{N}[H(x,y) - \hat{H}(x,y)]^2 \tag{5}$$

Table 2 Simulation results of the proposed scheme with 16 × 16 retained block size.

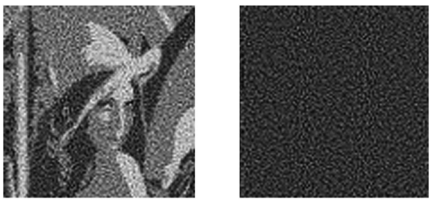
		BCH(15,7)		BCH(15,5)	
Attack	PSNR	Extracted watermark	NC	Extracted watermark	NC
JPEG	30.3748		1		1
Gaussian noise	14.7321		1		1
Salt-pepper noise	12.4339		1		1
Gaussian blur	21.3843		1		1
Median filtering	28.9217		1		1
Rotation	16.2678		0.9086		0.9820
Cropping	13.5651		0.9918		1
Scaling	20.5458		0.9845		1
Sharpening	21.1217		1		1
Mixed	13.0480		1		1

where $H(x,y)$ and $\hat{H}(x,y)$, respectively denote the pixel values at the position (x,y) of the host image and the attacked image, and $M \times N$ is the image size. A smaller PSNR indicates that the attacked image and the original image are more dissimilar. NC is defined as follows:

$$\mathrm{NC} = \frac{\sum_{i=1}^{J}\overline{w_i \oplus \tilde{w}_i}}{J}, \tag{6}$$

where w_i and $\tilde{w}_i$ are, respectively the pixel value of original watermark $\mathbf{W}$ and extracted watermark $\tilde{\mathbf{W}}$, i is the index of the watermark pixel, J is the total number of watermark pixels, and $\oplus$ is the Exclusive-OR logical operation. The NC value ranges from 0 to 1. The closer the NC value is to 1, the smaller the distortion of the watermark.

The simulation results in the common image processing attacks for Lena are listed in Table 2. The size of the retained block is 16 × 16. As shown by the data in Table 2, the watermarks retrieved after most of the image processing attacks can still retain the original information. Figure 5(a) shows the ownership share of Lena by the BCH(15,5). All of the attacked master shares are noise-like binary image, such as Fig. 5(b).



(a) (b)

Fig. 5 (a) Ownership share (210 × 210); (b) master share (210 × 210).

Table 3 Comparison of Lena between three watermarking methods and our proposed method by BCH(15,5) with 16 × 16 retained block size.

	NC			
Attacks	**Proposed scheme**	**[18] Scheme**	**[15] Scheme**	**[14] Scheme**
JPEG	1	0.9998	0.9930	0.6409
Gaussian noise	1	0.9993	0.9874	0.9405
Salt-pepper noise	1	0.9988	0.9868	0.9358
Gaussian blur	1	0.9951	0.9809	0.9183
Median filtering	1	0.9996	0.9970	0.9469
Rotation	0.9820	0.9604	0.9614	0.8320
Cropping	1	0.9228	0.9876	0.7649
Scaling	1	0.9885	0.9786	0.8783
Sharpening	1	0.9996	0.9948	0.9552
Mixed	1	0.9975	0.9829	0.9276

We compared the proposed scheme with other schemes.[14,15,18] Lena and the watermark shown in Fig. 4(d) are used for the experiment, and the retained block size is 16 × 16. As shown in Table 3, the proposed scheme is better than the other schemes[14,15,18] in the robustness against JPEG compression, Gaussian noise, salt-pepper noise, Gaussian blur, median filtering, rotation, cropping, scaling, sharpening, and mixed attacks. The curves for Lena and the watermark shown in Fig. 4(d) by the common image processing attacks with 16 × 16 retained block size are plotted in Figs. 6 to 12. The experimental results show that the proposed scheme performs better performance than the other methods[14,15,18] except for the rotation attack and the Gaussian blur attack by the BCH(15,7); moreover, the benefit of BCH code is exhibited.

At last, we will utilize three different retained block sizes (e.g., 8 × 8, 16 × 16, and 32 × 32) to explore the watermarking robustness of our method. By the BCH(15,5) code, the simulation results for Lena, F16, and the watermark shown in Fig. 4(c) are listed in Table 4. As shown by the data in Table 4, the watermark retrieved after most of the image processing attacks can still retain its original information,

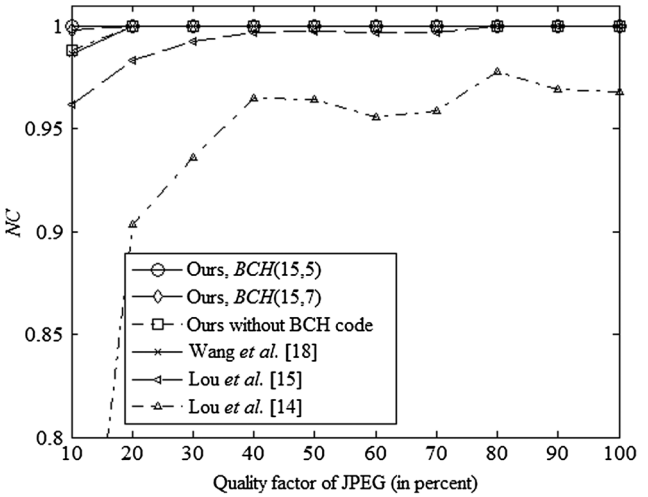


Fig. 6 Performance comparison of Lena after the JPEG compression attack.

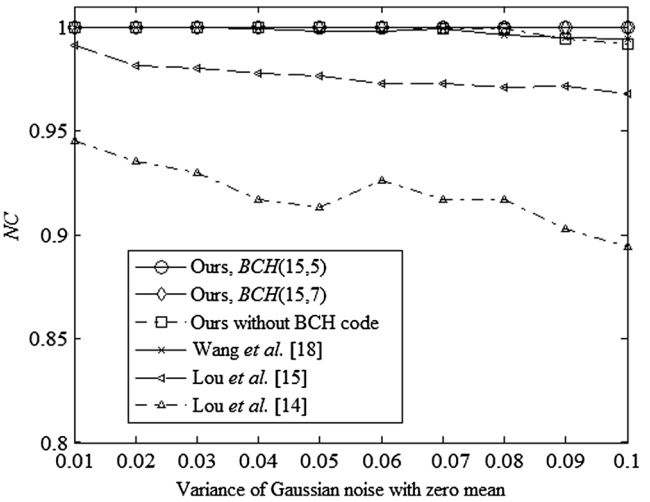


Fig. 7 Performance comparison of Lena after the Gaussian noise attack.

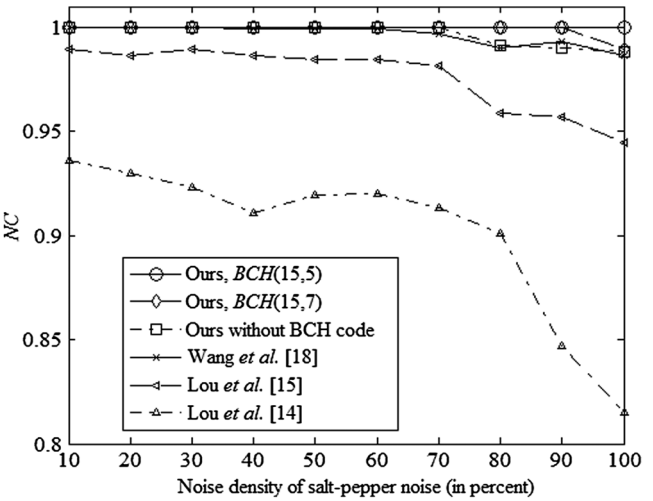


Fig. 8 Performance comparison of Lena after the salt-pepper noise attack.

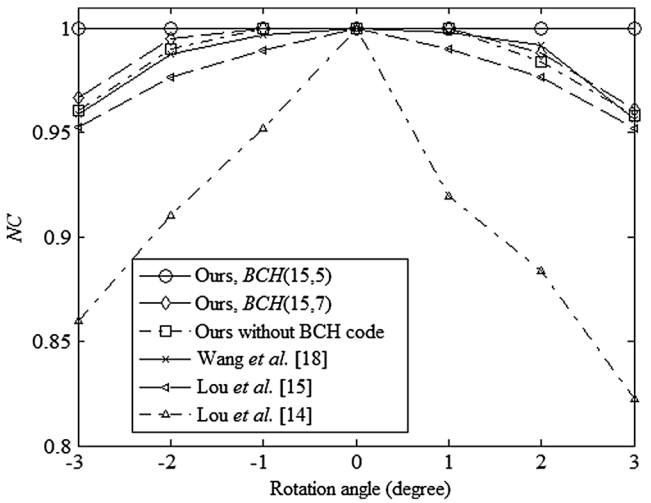


Fig. 9 Performance comparison of Lena after the rotation attack.

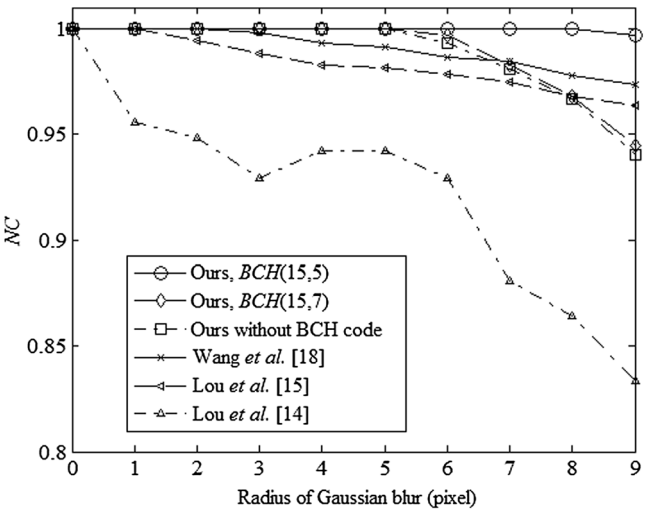


Fig. 10 Performance comparison of Lena after the Gaussian blur attack.

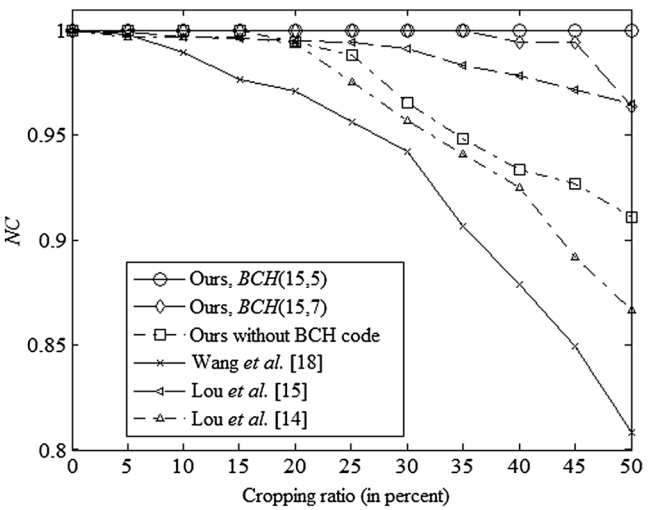


Fig. 11 Performance comparison of Lena after the cropping attack.

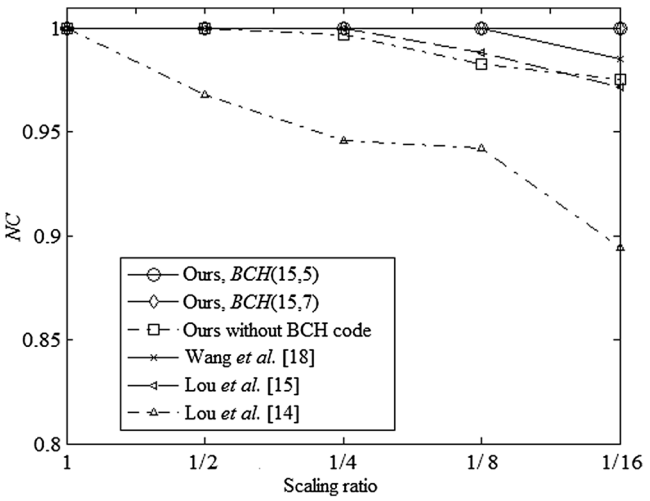


Fig. 12 Performance comparison of Lena after the scaling attack.

Table 4 Simulation results of the proposed scheme by BCH(15,5).

	Lena			F16		
	NC			NC		
Attacks	**8 × 8**	**16 × 16**	**32 × 32**	**8 × 8**	**16 × 16**	**32 × 32**
JPEG	1	1	1	0.9988	1	1
Gaussian noise	1	1	1	0.9861	1	1
Salt-pepper noise	1	1	1	0.9722	1	1
Gaussian blur	0.9984	1	1	0.9976	1	1
Median filtering	1	1	1	1	1	1
Rotation	0.9486	0.9820	0.9975	0.9771	0.9820	0.9856
Cropping	1	1	1	0.9967	0.9976	0.9989
Scaling	0.9927	1	1	0.9927	1	1
Sharpening	1	1	1	1	1	1
Mixed	1	1	1	0.9673	1	1

especially showing good results in resisting attacks such as JPEG compression, noise, cropping, median filtering, sharpening, and mixed attacks. Moreover, our method with a larger retained block size can provide better robustness of watermarking.

6 Conclusions

Most of the existing plans cannot guarantee the integrity of the image quality. Those schemes cannot be suitable for images that require maintenance of the image quality, such as military images, medical images, art images, etc. In this paper, a robust copyright scheme for image protection based on the VSS and BCH code is proposed. The advantages of

this scheme lie in that does not need to modify the host image, which maintains image quality and is suitable for artistic appreciation and certain images with sensitive contents. In addition, no codebook is required to store, and the watermark size is independent of the host image. The ownership share that is generated for image verification is no longer a noise-like image. In other words, it is a binary image with meaningful contents, which leads to easier image management. When the protected image is sabotaged by malicious attackers, the characteristics within the image are destroyed, which will affect the encoded watermark. However, since the watermark used for protection is capable of correction after the BCH decode, it enables the watermark to be more resistant to malicious attacks. As shown by the experimental results, the proposed scheme can always retrieve the watermark perfectly in the case of general image processing attacks, such as sharpening, cropping, tampering, noise, JPEG image compression attacks, or the arbitrary combination of the aforementioned. This way, there will be no ambiguity in watermark retrieval. The proposed scheme can relatively enhance robustness; however, it will require more space to store ownership share. Our future work is to decrease the number of ownership share or reduce the size of ownership share.

References

1. V. Solachidis and I. Pitas, "Circularly symmetric watermark embedding in 2-D DFT domain," in *Proc. IEEE Int. Conf. on Acoust., Speech and Signal Process*, Phoenix, Arizona, Vol. 6, pp. 3469–3472 (1999).
2. I. J. Cox et al., "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.* **6**(12), 1673–1687 (1997).
3. X. G. Xia, C. G. Boncelet, and G. R. Arce, "A multiresolution watermark for digital images," in *Proc. IEEE Int. Conf. Image Process.*, Santa Barbara, California, Vol. 1, pp. 548–551 (1997).
4. D. Kundur and D. Hatzinakos, "A robust digital image watermarking method using wavelet-based fusion," in *Proc. Int. Conf. Image Process*, Vol. 1, pp. 544–547 (1997).
5. C. C. Chang and P. Y. Lin, "Adaptive watermark mechanism for rightful ownership protection," *J. Syst. Software* **81**(7), 1118–1129 (2008).
6. C. H. Kung, P. T. Wu, and Y. C. Lee, "The design of an innovative method for digital video surveillance system with watermarking and error control codes," in *Proc. IEEE Conf. on Instrumentation and Measurement Technology*, Ottawa, Ontario, Vol. 1, pp. 633–638 (2005).
7. H. C. Huang and W. C. Fang, "Metadata-based image watermarking for copyright protection," *Simul. Modell. Pract. Theor.* **18**(4), 436–445 (2010).
8. F. Mintzer, J. Lotspiech, and N. Morimoto, "Safeguarding digital library contents and users: digital watermarking," *D-Lib Mag.* **3**(12) (1997).
9. Z. Ni et al., "Reversible data hiding," *IEEE Trans. Circ. Syst. Video Technol.* **16**(3), 354–362 (2006).
10. J. Tian, "Reversible watermarking using a difference expansion," *IEEE Trans. Circ. Syst. Video Technol.* **13**(8), 890–896 (2003).
11. C. C. Chang and J. C. Chuang, "An image intellectual property protection scheme for gray-level images using visual secret sharing strategy," *Pattern Recogn. Lett.* **23**(8), 931–941 (2002).
12. C. S. Hsu and Y. C. Hou, "Copyright protection scheme for digital images using visual cryptography and sampling methods," *Opt. Eng.* **44**(7), 077003 (2005).
13. S. L. Hsieh and B. Y. Huang, "A copyright protection scheme for gray-level images based on image secret sharing and wavelet transformation," in *Proc. Int. Computer Symp.*, Taipei, Taiwan, pp. 661–666 (2004).
14. D. C. Lou, J. L. Liu, and H. K. Tso, "Copyright protection scheme based on chaos and secret sharing techniques," *Opt. Eng.* **44**(11), 117004 (2005).
15. D. C. Lou, H. K. Tso, and J. L. Liu, "A copyright protection scheme for digital images using visual cryptography technique," *Computer Stand. Interfaces* **29**(1), 125–131 (2007).
16. Y. B. Xing and J. H. He, "A new robust copyright protection scheme for digital image based on visual cryptography," in *Int. Conf. on Wavelet Analysis and Pattern Recognition*, Qingdao, pp. 6–11 (2010).
17. M. S. Wang and W. C. Chen, "Digital image copyright protection scheme based on visual cryptography and singular value decomposition," *Opt. Eng.* **46**(6), 067006 (2007).
18. M. S. Wang and W. C. Chen, "Robust copyright protection scheme based on discrete cosine transform and secret sharing techniques," *J. Electron. Imaging* **17**(2), 023006 (2008).
19. M. Naor and A. Shamir, "Visual cryptography," in *Cryptology-EuroCrypt'94*, Vol. 950, pp. 1–12, Lecture Notes in Computer Science, Springer-Verlag, Berlin (1995).
20. W. W. Peterson and E. J. Weldon Jr., "Error-Correcting Codes," MIT Press, Cambridge, Massachusetts (1971).
21. R. C. Bose and D. K. Ray-Chaudhuri, "On a class of error-correcting binary group codes," *Inform. Control.* **3**, 68–79 (1960).
22. A. Hocquenghem, "Codes correcteurs d'erreurs," *Chiffres (Paris)* **2**, 147–159 (1959).
23. G. Voyatzis and I. Pitas, "Chaotic mixing of digital images and applications to watermark," in *Proc. European Conf. on Multimedia Applications, Services and Techniques*, Louvain-La-Neuve, Belgium, Vol. 2, pp. 687–695 (1996).

Tzuo-Yau Fan received his BS and MS degrees, both in the Department of Computer Science and Information Engineering, from Ming Chuan University, Taoyuan, Taiwan, in 2008 and 2010, respectively. He is currently a PhD student of the Department of Electronic Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan. His research interests are in the areas of image processing, digital signal processing, and computer vision.

Bin-Chang Chieu received his PhD degree in electrical engineering from Rensselaer Polytechnic Institute, Troy, New York, in 1989. He is now professor at the Department of Electronic Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan. His current research interests are in image processing, digital signal processing, neural networks, and computer vision.

Her-Chang Chao received his BS degree and PhD degrees, both in electronic engineering, from National Taiwan University of Science and Technology, Taipei, Taiwan, in 1991 and 1998, respectively. He is now associate professor at the Department of Computer Science and Information Engineering, Ming Chuan University, Taoyuan, Taiwan. His research interests are in the area of image processing, digital signal processing, multimedia information security, data hiding, digital watermark, and computer vision.