Copyright protection scheme for digital images using visual cryptography and sampling methods

Ching-Sheng Hsu
National Central University
Department of Information Management
P.O. Box 9-236
Jhongli City, Taoyuan County, Taiwan 320
E-mail: jacketcc@mgt.ncu.edu.tw

Young-Chang Hou
Tamkang University
Department of Information Management
151 Ying-Chuan Road
Tamshui, Taipei County, Taiwan 251

Abstract. A novel copyright protection scheme for digital images based on visual cryptography and statistics is proposed. The proposed method employs sampling distribution of means and visual cryptography to achieve the requirements of robustness and security. Our method can register multiple secret images without altering the host image and can identify the rightful ownership without resorting to the original image. Moreover, the proposed method enables the secret images to be of any size regardless of the size of the host image. Finally, experimental results show that the proposed scheme can resist several common attacks.
[DOI: 10.1117/1.1951647]

Subject terms: copyright protection; digital watermarking; sampling distribution.

Paper 040840R received Nov. 9, 2004; revised manuscript received Jan. 21, 2005; accepted for publication Feb. 2, 2005; published online Jul. 15, 2005.

1 Introduction

With the coming era of the Internet, more and more data are transmitted and exchanged on the networked systems to enjoy the rapid speed and convenience. In cyberspace, however, the availability of duplication methods encourages the violation of intellectual property rights of digital data, such as document, image, audio, and video. Therefore, the protection of the rightful ownership of digital data has become an important issue recently. Today, researchers have proposed many techniques to protect the intellectual property rights for digital images. Digital watermarking, a type of such technique, is a method that hides a meaningful signature, or the so-called digital watermark, in a host image for the purpose of copyright protection, image authentication, copy protection, and captioning. When the rightful ownership of the image must be identified, the hidden watermark can be extracted for ownership verification. During the watermark detection process, the original image may or may not be used. However, in many cases such as image monitoring, the original image is usually unavailable, thus those techniques that can reveal watermarks without the aid of the original image become better solutions. Digital watermarks can be either visible[1] or invisible.[2–5] In this paper, we focus on invisible watermarks. In general, an effective watermarking scheme should satisfy certain requirements, such as imperceptibility, robustness, unambiguousness, security, capacity, and low computational complexity.[2,6–8] Some of these requirements may conflict with each other, thereby introducing many technical challenges. For example, imperceptibility and capacity may conflict with robustness. Therefore, a reasonable compromise between some requirements is required to achieve better performance for the intended applications.

Based on the taxonomy found in many literature sources, we can group watermarking techniques into two categories: one is the spatial-domain approach[3,5,9] and the other is the transform-domain approach.[2,10–12] Most related techniques use many pixels or transform coefficients to conceal one bit of information. Usually, the data of the host image should be adequately adjusted or altered to embed the digital signature. Thus, the watermark should be much smaller than the host image so that the requirements of imperceptibility and robustness can be satisfied. Such a property makes it impossible to embed a larger watermark into a smaller host image. In addition, if multiple watermarks must be registered for a single image, it is also impossible for such methods to embed the latter watermark without destroying the former ones. Moreover, when the rightful ownership of the image must be identified, many of the methods require the aid of the original image to extract the watermark.

In 1995, Naor and Shamir introduced a perfectly secure way called visual cryptography (VC) for the protection of secret images.[13] In addition to the property of perfect secrecy, the prominent feature provided by VC is the decryption method done by human eyes. Recently, many VC based copyright protection schemes were proposed, such as those in Refs. 9, 10, and 14. Hou and Chen[9] use a modified two-out-of-two VC scheme to split the watermark into two meaningless shares, and the first share is embedded into the host image by decreasing the gray levels of some specific pixels. When the rightful ownership must be identified, the second share and the watermarked image are superimposed to reveal the watermark. The drawbacks of their method are that the host image should be altered and that the robustness to some attacks, such as jitter, geometric distortion, cropping, and rotation attacks, is rather weak. Chang et al.'s copyright protection scheme[10] utilizes VC and discrete cosine transform (DCT) to satisfy the requirement of security and robustness, and enables registering multiple watermarks without destroying other hidden signatures. Their

method comprises the ownership share construction and the watermark revelation phases. During the ownership share construction phase, the dc coefficients of all 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 does not really provide the key advantage of visual cryptography that uses human eyes to decrypt the secret without the aid of computers. In addition, 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 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. Hwang's method[14] uses the most significant bits of the host image to generate the first share so as to satisfy the requirement of robustness. Then, the first share is used together with the watermark to construct the second share according to the two-out-of-two VC scheme. The method has the advantages that the watermark can be of any size, and that the host image is not altered. However, the use of the most significant bits may result in violation of the probability setting required by VC; thus, the security can not be ensured.

In this paper, we propose a copyright protection scheme for digital images to remedy the drawbacks presented in Refs. 9, 10, and 14. Our method uses the theories and properties of sampling distribution of means (SDM) to generate a binary master share from a gray-level image. Then, the master share and the secret image (conceptually similar to the watermark) are used to construct the ownership share according to some predefined rules of VC. When the rightful ownership must be identified, the master share, generated from the image to be identified, and the ownership share are superimposed to reveal the secret image without the aid of computers. Our method can provide all the advantages presented in Refs. 9, 10, and 14, but their respective drawbacks are avoided. For example, the host image will not be altered; the rightful ownership can be identified without the aid of the original image; the secret image can be of any size; multiple secret images are allowed to be registered for a single image without causing any damage to other hidden images; and the advantage of VC, which uses human eyes to recover secret images without the aid of computers, can be fully utilized. In addition, our method can attain the requirement of robustness because the characteristics and parameters of statistics of an image can not be easily changed by many attacks. Finally, the security of the scheme is ensured by the properties of VC. Altogether, our method has more applications than copyright protection. For example, it can be applied to cover the transmission of confidential images.

The rest of this paper is organized as follows. Section 2 introduces VC. Section 3 provides a brief description of sampling distribution of means. In Sec. 4, we demonstrate how the properties of SDM and VC can be applied to construct a copyright protection scheme for digital images. Section 5 presents the experimental results, which demonstrate the robustness of our method. Finally, a brief conclusion is given in Sec. 6.

2 VC

VC schemes were first introduced by Naor and Shamir to encrypt a secret image into n shadow images called shares such that any k or more shares can recover the secret image, whereas less than k shares cannot leak any information about the secret.[13] Unlike traditional cryptographic schemes, VC uses human eyes to decrypt the secret without any complex decryption algorithms or the aid of computers. Usually, the decryption of the secret image consists of printing more than k shares onto transparences and superimposing these transparences altogether; then, participants can identify the recovered secret from the stacked image with their eyes. Therefore, it is a quite simple but secure way to protect the secret. Basically, VC schemes should satisfy some security and contrast conditions. The following definition formally defines a k-out-of-n visual cryptography scheme.[13]

Definition 1. A k-out-of-n visual cryptography scheme with m subpixels, contrast $\alpha > 0$, threshold d consists of two collections of $n \times m$ Boolean matrices $\mathbf{C}_0 = [C_{0,1}, C_{0,2}, \ldots, C_{0,u}]$ and $\mathbf{C}_1 = [C_{1,1}, C_{1,2}, \ldots, C_{1,v}]$. To share a white (resp. black) pixel, the dealer randomly chooses one of the matrices in $\mathbf{C}_0$ (resp. $\mathbf{C}_1$). The chosen matrix defines the color of the m subpixels in each one of the n transparencies. The solution is considered valid if the following three conditions are satisfied:

1. For any matrix $\mathbf{S} \in \mathbf{C}_0$, the m vector $\mathbf{V}$ of ORing any k out of n rows of $\mathbf{S}$ satisfies $w(V) \leqslant d - \alpha m$.
2. For any matrix $\mathbf{S} \in \mathbf{C}_1$, the m vector $\mathbf{V}$ of ORing any k out of n rows of $\mathbf{S}$ satisfies $w(V) \geqslant d$.
3. For any subset $\{i_1, i_2, \ldots, i_q\}$ of $\{i_1, i_2, \ldots, i_n\}$ with $q < k$, the two collections of $q \times m$ matrices $\mathbf{D}_t$ obtained by restricting each $n \times m$ matrix in $\mathbf{C}_t$, where $t \in \{0, 1\}$ to rows $i_1, i_2, \ldots, i_q$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

The Hamming weight of the m vector $\mathbf{V}$, denoted by $w(\mathbf{V})$, is the number of 1 within $\mathbf{V}$, and the gray level of the stacked image is proportional to $w(\mathbf{V})$. The first two properties are related to the contrast of the image. The value α is called relative difference, and αm is referred to as the contrast of the image. The third property is called security, since it implies that less than k shares cannot gain any information of the secret image. To share a white (resp. black) pixel, we randomly choose one of the matrices in $\mathbf{C}_0$ (resp. $\mathbf{C}_1$), and then the i'th row is used to represent the m subpixels on the i'th share. For example, the two-out-of-two visual cryptography scheme can be represented by the following two collections:

$$\mathbf{C}_0 = \left\{ \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \right\}, \tag{1}$$

Table 1 The 2-out-of-2 visual cryptography scheme.

Pixels	Probability	Encryption rules: Share 1	Encryption rules: Share 2	Stacked results
□	0.5			
□	0.5			
■	0.5			
■	0.5			

$$\mathbf{C}_1 = \left\{ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}. \tag{2}$$

Note that the preceding two collections $\mathbf{C}_0$ and $\mathbf{C}_1$ will lead to distortion of the image. To remedy the drawback, one can use more subpixels to maintain the aspect ratio. Table 1 shows an alternative two-out-of-two VC scheme that can avoid distortion of the image. In such scheme, every secret pixel is expanded to 4 subpixels in each share to maintain the aspect ratio of the image. In the following sections, this scheme is used to construct the copyright protection scheme for digital images.

3 SDM

According to the theory of sampling distribution, the SDM from a normal population is also a normal distribution.[15] In statistics, many important properties are related to SDM of a normal population, such as unbiasedness, efficiency, and consistency. The unbiased property, which will be helpful to our copyright protection scheme, means that the average of all the possible sample means of a given sample size n will be equal to the population mean μ. In many cases, it is not a simple task to distinguish whether or not a population is normally distributed. Fortunately, the central limit theorem can be employed to solve this problem. According to the central limit theorem, as the sample size gets large enough, the SDM can be approximated by the normal distribution. In practice, the sample size $n \geqslant 30$ is considered sufficient for a SDM to approximate to a normal distribution.

Let $-\infty < X < +\infty$ be a normal random variable with population mean μ and standard deviation σ. Also let $-\infty < \bar{X} < +\infty$ be a random variable of the sample mean drawn from the population with the normal random variable X. Then, the normalized sampling distribution of $\bar{X}$ has the mean

$$\mu_{\bar{X}} = \mu \tag{3}$$

and the standard error of means

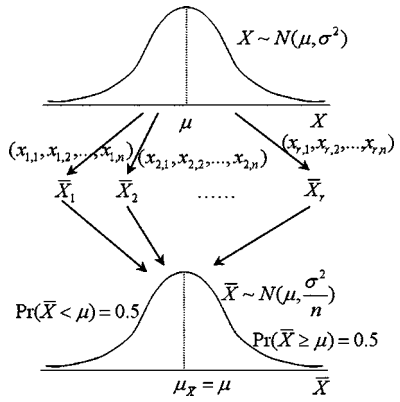


Fig. 1 Sampling distribution of means from a normal population.

$$\sigma_{\bar{X}} = \frac{\sigma}{\sqrt{n}}. \tag{4}$$

Theoretically, normal distribution is bell-shaped and symmetrical in its appearance, and the probability density function for X is given by

$$f(X) = \frac{1}{\sigma\sqrt{2\pi}} \exp[-(X-\mu)^2/2\sigma^2]. \tag{5}$$

Then, for a fixed x, the probability of $X \leqslant x$, denoted by $\Pr(X \leqslant x) = \alpha$, can be computed by

$$\alpha = \int_{-\infty}^{\infty} \frac{1}{\sigma\sqrt{2\pi}} \exp[-(X-\mu)^2/2\sigma^2] \mathrm{d}X. \tag{6}$$

Therefore, we have that $\Pr(X \geqslant \mu) = \Pr(X < \mu) = 0.5$. Similarly, it is easy to conclude that $\Pr(\bar{X} \geqslant \mu_{\bar{X}}) = \Pr(\bar{X} \geqslant \mu) = 0.5$ and that $\Pr(\bar{X} < \mu_{\bar{X}}) = \Pr(\bar{X} < \mu) = 0.5$. The preceding properties are illustrated in Fig. 1. In the following sections, the application of SDM is further discussed.

4 Proposed Scheme

In this section, we introduce the proposed copyright protection scheme based on VC and SDM. Essentially, the scheme comprises the ownership registration and the ownership identification phases. In the ownership registration phase, the master share M will be generated from the host image by SDM. Then, the master share M is used together with the secret image **S** to generate the ownership share **O** according to some predefined encryption rules of VC. During the process of sampling, a private key K is used so that the identical sequence of pixel values can be drawn out from the host image in both phases. Finally, the private key K is kept in secret by the copyright owner, and the ownership share **O** must be registered with a trusted third party for further authentication. When a controversy over the ownership of the host image happens so that the copyright owner wants to prove his or her rightful ownership, the ownership identification procedure should be performed. Thus, the private key K and the ownership share **O** are used

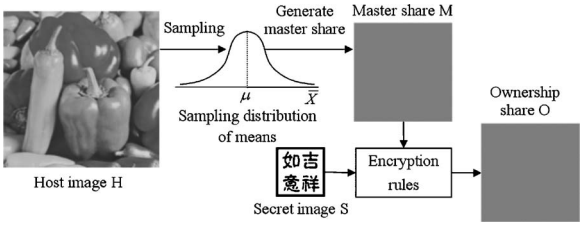


Fig. 2 Process of master and ownership shares construction procedure.

to reveal the hidden secret image for settling the dispute. In the following sections, we describe our scheme in more detail.

4.1 *Ownership Registration Phase*

Assume that a copyright owner wants to hide a bilevel secret image **S** of size $N_1 \times N_2$ pixels into a gray-level host image of size $M_1 \times M_2$ pixels for protecting his or her ownership. In the beginning, the population mean μ of the pixel values of the host image should be calculated in advance. In addition, a private key K should be used for sampling so that a list of random numbers, $L=(l_1, l_2, \ldots)$, can be generated by a pseudorandom number generator seeded by K, where each random number $l_m \in \{1, 2, \ldots, M_1 \times M_2\}$ corresponds to the location of a pixel in the host image. For example, the first n elements in L are used to compute the first sample mean, the next n elements are used to compute the second sample mean, etc. Assume that $\bar{X}_t$ denotes a sample mean with sample size $n \geq 30$ randomly selected (according to L) from the host image. Thus, according to the central limit theorem and the unbiased property of SDM, we have that $\Pr(\bar{X}_t \geq \mu) = \Pr(\bar{X}_t < \mu) = 0.5$. Also assume that $m_{i,j}$ denotes a pixel (with 4 subpixels) of the master share **M**. Then each pixel $m_{i,j}$ of the master share **M** can be generated by the following generation rules (*M_Rule*_1 and *M_Rule*_2):

Master Share Generation Rules:

Master Share Generation Rules:

***M_Rule*_1:** if $\bar{X}_t < \mu$ then $m_{i,j} =$  .

***M_Rule*_2:** if $\bar{X}_t \geq \mu$ then $m_{i,j} =$  .

Now, we can start to generate the ownership share. Assume that $s_{i,j}$ denotes a pixel of the secret image **S**, and $o_{i,j}$ denotes a pixel (with 4 subpixels) of the ownership share **O**. Also assume that 0 denotes a white pixel and 1 denotes a black pixel. Then, the resultant master share **M** is used together with the secret image **S** to generate the ownership share **O** according to the following generation rules (*O_Rule*_1, *O_Rule*_2, *O_Rule*_3, and *O_Rule*_4):

Ownership Share Generation Rules:

***O_Rule*_1:** if $s_{i,j} = 0$ and $m_{i,j} =$  then $o_{i,j} =$.

***O_Rule*_2:** if $s_{i,j} = 0$ and $m_{i,j} =$  then $o_{i,j} =$.

***O_Rule*_3:** if $s_{i,j} = 1$ and $m_{i,j} =$  then $o_{i,j} =$.

***O_Rule*_4:** if $s_{i,j} = 1$ and $m_{i,j} =$  then $o_{i,j} =$.

The process of ownership share construction is illustrated in Fig. 2. Altogether, the ownership share construction procedure is formally described by the following algorithm.

4.1.1 *Algorithm ownership share construction procedure*

Input. A gray-level host image **H** with $M_1 \times M_2$ pixels, a bilevel secret image **S** with $N_1 \times N_2$ pixels, and a private key K.

Output. An ownership share **O** of size $N_1 \times N_2$ pixels (each of which is composed of 4 subpixels).

Step 1. Compute the population mean μ of the pixel values of the host image **H**.

Step 2. Generate a list of random numbers $L = (l_1, l_2, \ldots)$, where $l_m \in \{1, 2, \ldots, M_1 \times M_2\}$, by a random number generator seeded by K.

Step 3. Randomly select $n (n \geq 30)$ pixel values $x_{t,1}, x_{t,2}, \ldots, x_{t,n}$ from the host image **H** (according to L) to form a sample mean $\bar{X}_t$.

Step 4. For each pixel $s_{i,j}$ of the secret image **S**, determine the color of the pixel $o_{i,j}$ (with 4 subpixels) in the ownership share **O** according to the following encryption rules:

If $s_{i,j} = 0$ and $\bar{X}_t < \mu$ then $o_{i,j} =$  ,

else if $s_{i,j} = 1$ and $\bar{X}_t \geq \mu$ then $o_{i,j} =$  ,

else if $s_{i,j} = 1$ and $\bar{X}_t < \mu$ then $o_{i,j} =$  ,

else $o_{i,j} =$  .

Step 5. Repeat steps 3 to 4 until all pixels of the secret image **S** are processed.

Finally, the private key K must be kept secretly by the copyright owner for proving his or her ownership, and the ownership share **O** should be registered with a trusted third party for further authentication. Since perfect secrecy is guaranteed by the two-out-of-two VC scheme of which the required probability setting is satisfied by SDM, without the correct private key, no one can recover any meaningful image. Thus, any one who can provide the correct private key to reveal a meaningful image must be the copyright owner of the image. In the next section, we introduce the procedure for ownership identification.

4.2 *Ownership Identification Phase*

In the Internet era, it is very possible that a digital image is held or abused without the permission of the copyright owner. When a controversy over the ownership of the image happens so that the copyright owner wants to prove his or her rightful ownership, the ownership identification procedure should be performed accordingly. In the ownership identification phase, the copyright owner should provide the same private key K used in the ownership registration

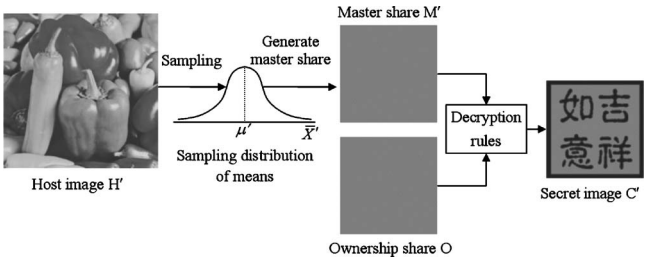


Fig. 3 Process of ownership identification procedure.

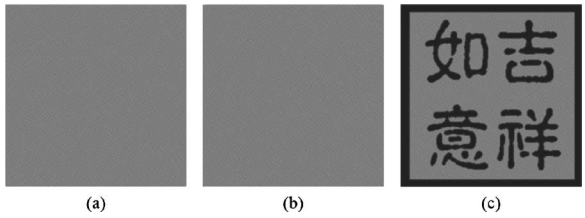


Fig. 5 (a) Master share generated from the original image (512 $\times$512 pixels), (b) the ownership share (512$\times$512 pixels), and (c) stacked result of (a) and (b).

phase so that the correct sequence of pixel values can be obtained during the sampling process. Then, the master share **M′** is generated from the controversial image **H′** by the following algorithm:

4.2.1 *Algorithm master share construction procedure*

Input. A gray-level host image H′ with $M_1 \times M_2$ pixels, a bilevel ownership share O with $N_1 \times N_2$ pixels (each of which is composed of 4 subpixels), and a private key K.

Output. A master share M′ of size $N_1 \times N_2$ pixels (each of which is composed of 4 subpixels).

Step 1. Compute the population mean μ' of the pixel values of the host image H′.

Step 2. Generate a list of random numbers $L = (l_1, l_2, \ldots)$, where $l_m \in \{1, 2, \ldots, M_1 \times M_2\}$, by a random number generator seeded by K.

Step 3. Randomly select $n (n \geq 30)$ pixel values $x'_{t,1}, x'_{t,2}, \ldots, x'_{t,n}$ from the host image H′ (according to L) to form a sample mean $\bar{X}'_t$.

Step 4. For each pixel $o_{i,j}$ (with 4 subpixels) of the ownership share O, the corresponding color of the pixel $m'_{i,j}$ (with 4 subpixels) in the master share M′ is determined by

$m'_{i,j}$ = ■ if $\bar{X}'_t < \mu'$ and $m'_{i,j}$ = ■ otherwise.

Step 5. Repeat step 3 to 4 until all pixels of the ownership share are processed.

After the master share **M′** is created, the secret image **S′** can be revealed by visual cryptography. We can simply print both shares onto transparencies and then superimpose them to reveal the secret image without the aid of computers. On the other hand, the secret image can also be revealed by computers, and the algorithm is as follows:

4.2.2 *Algorithm secret image revelation procedure (by computers)*

Input. A gray-level host image H′ with $M_1 \times M_2$ pixels, a bilevel ownership share O with $N_1 \times N_2$ pixels (each of which is composed of 4 subpixels), and a private key K.

Output. A recovered secret image S′ of size $N_1 \times N_2$ pixels.

Step 1. Compute the population mean μ' of the pixel values of the host image H′.

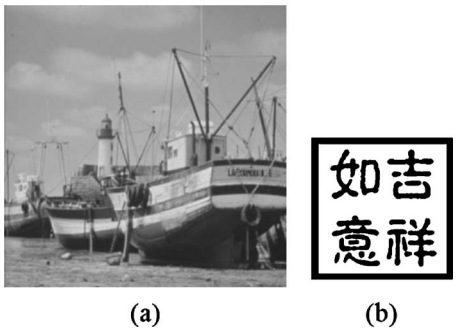


Fig. 4 (a) Gray-level host image (512$\times$512 pixels) and (b) bilevel secret image (256$\times$256 pixels).

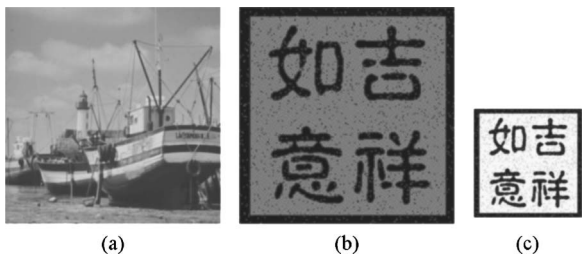
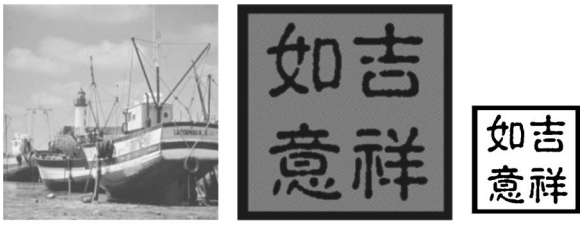
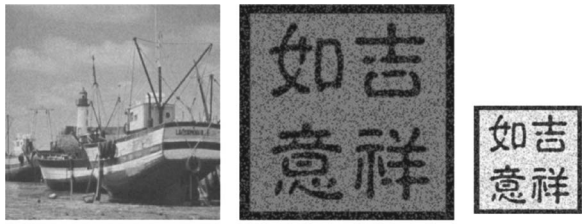


Fig. 6 (a) JPEG-compressed image with compression ratio of 5:1 (PSNR=37.77 dB), (b) the secret image revealed by VC (NC =98.88%), and (c) secret image revealed by computers (NC =97.76%).



(a) (b) (c)

Fig. 7 (a) Lightened image (PSNR=18.59 dB), (b) the secret image revealed by VC (NC=100.0%), and (c) the secret image revealed by computers (NC=100.0%).



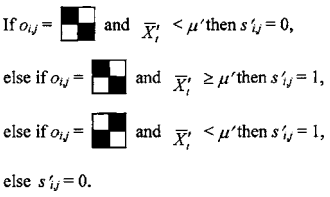
(a) (b) (c)

Fig. 9 (a) Image with 10% monochromatic noises (PSNR =24.45 dB), (b) the secret image revealed by VC (NC=95.02%), and (c) the secret image revealed by computers (NC=90.05%).

Step 2. Generate a list of random numbers $L=(l_1,l_2,\ldots)$, where $l_m \in \{1,2,\ldots,M_1\times M_2\}$, by a random number generator seeded by K.

Step 3. Randomly select $n(n \geqslant 30)$ pixel values $x'_{t,1},x'_{t,2},\ldots,x'_{t,n}$ from the host image H' (according to L) to form a sample mean $\bar{X}'_t$.

Step 4. For each pixel $o_{i,j}$ (with 4 subpixels) of the ownership share O, determine the color of the pixel $s'_{i,j}$ in the secret image S' according to the following decryption rules:



Step 5. Repeat steps 3 to 4 until all pixels of the ownership share are processed.

The process of ownership identification is illustrated in Fig. 3. Note that the controversial image $\mathbf{H}'$ may be altered or modified by the image processing filters or lossy compression techniques, such as darkening, brightening, rescaling, blurring, sharpening, distortion, cropping, JPEG, and so on. Consequently, the revealed secret image $\mathbf{S}'$ may be different from the original secret image $\mathbf{S}$ to some extent.

5 Experimental Results

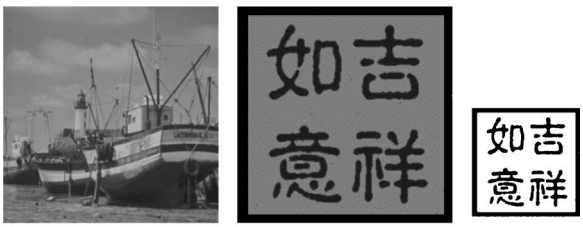
In this section, experiments are performed to demonstrate the robustness of the proposed scheme against several common attacks, including darkening, lightening, rescaling, blurring, sharpening, noise, distortion, cropping, jitter, JPEG lossy compression, and rotation. The gray-level host image of size 512×512 pixels is shown in Fig. 4(a) and the bilevel secret image of size 256×256 pixels is shown in Fig. 4(b). The master share generated from the original image [Fig. 4(a)] is shown in Fig. 5(a), the corresponding ownership share is shown in Fig. 5(b), and the stacked result of Fig. 5(a) and Fig. 5(b) is illustrated in Fig. 5(c). In the master share, the ratio of black pixels to white pixels is 50.21 to 49.79%, which reflects the central limit theorem holds. In addition, two common similarity measurements are introduced to evaluate the proposed copyright protection 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 bilevel images. The first measurement, PSNR, is defined as follows:

$$\mathrm{PSNR} = 10 \times \log \frac{255^2}{\mathrm{MSE}}, \tag{7}$$

where

$$\mathrm{MSE} = \frac{1}{M_1 \times M_2} \sum_{i=1}^{M_1} \sum_{j=1}^{M_2} (h_{i,j} - h'_{i,j})^2, \tag{8}$$

$h_{i,j}$ denotes a pixel color of the original host image, $h'_{i,j}$ denotes a pixel color of the attacked image, $M_1\times M_2$ is the

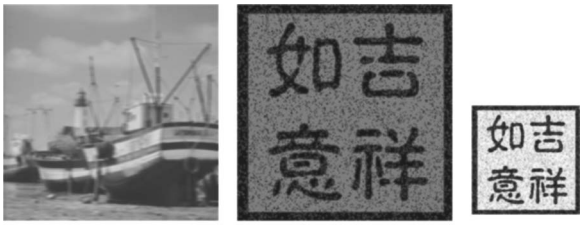


(a) (b) (c)

Fig. 8 (a) Darkened image (PSNR=18.59 dB), (b) the secret image revealed by VC (NC=99.99%), and (c) the secret image revealed by computers (NC=99.98%).

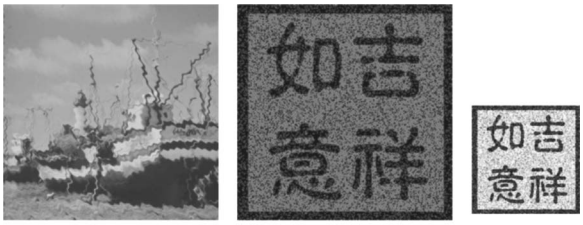
(a) (b) (c)

Fig. 10 (a) Sharpened image (PSNR=24.65 dB), (b) the secret image revealed by VC (NC=95.72%), and (c) the secret image revealed by computers (NC=91.43%).



(a) (b) (c)

Fig. 11 (a) Blurred image (PSNR=25.39 dB), (b) the secret image revealed by VC (NC=95.38%), and (c) the secret image revealed by computers (NC=90.77%).



(a) (b) (c)

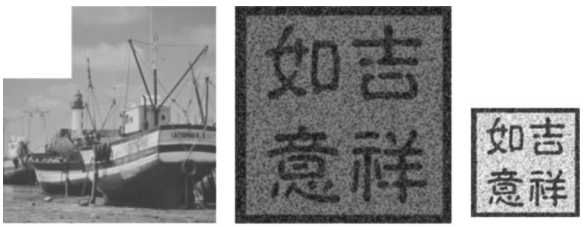
Fig. 13 (a) Distorted image (PSNR=21.05 dB), (b) the secret image revealed by VC (NC=92.48%), and (c) the secret image revealed by computers (NC=84.95%).

image size, and MSE is the mean squared error. The second measurement, NC, is defined as follows:

$$\mathrm{NC} = \frac{\sum_{i=1}^{N_1} \sum_{j=1}^{N_2} \overline{s_{i,j} \oplus s'_{i,j}}}{N_1 \times N_2} \times 100\,\%\,, \tag{9}$$

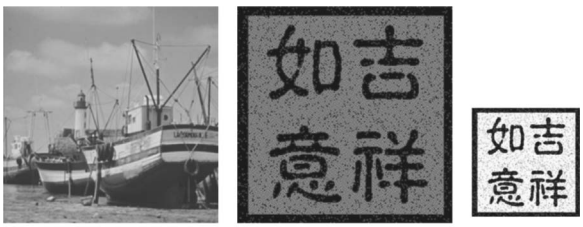
where $s_{i,j}$ denotes a pixel color of the original secret image $\mathbf{S}$, $s'_{i,j}$ denotes a pixel color of the revealed secret image $\mathbf{S}'$, $\oplus$ denotes the exclusive OR operation, and $N_1 \times N_2$ is the image size. Besides, the sample size $n=30$ is used to proceed all of the experiments.

In the following experiments, the NC values of the revealed secret images generated by computers are measured according to Fig. 4(b). However, the NC values of the revealed secret images generated by VC are measured according to Fig. 5(c) since they have the same image size. First, the JPEG lossy compression with compression ratio of 5:1 is performed to evaluate the robustness. The similarity between the compressed image shown in Fig. 6(a) and the original image shown in Fig. 4(a) is PSNR=37.77 dB. The similarity between the revealed secret image generated by VC shown in Fig. 6(b) and the unattacked secret image shown in Fig. 5(c) is NC=98.88%. The similarity between the revealed secret image generated by computers shown in Fig. 6(c) and the original secret image shown in Fig. 4(b) is NC=97.76%. Next, experimented with the lightening and darkening attacks. Figures 7(a) and Fig. 8(a) are the lightened and darkened images, respectively. The similarity of the lightened image is PSNR=18.59 dB and that of the darkened image is also 18.59 dB. The similarities of the revealed secret images generated by VC and by computers from the lightened image are NC=100.0%, and that from the darkened image are NC=99.99% and NC=99.98%, respectively. The following experiment concerns the noising attack. Figure 9(a) is the image with 10% monochromatic noises, and its similarity measure is PSNR=24.45 dB. The revealed secret image shown in Figs. 9(b) and 9(c) have similarity measures NC=95.02% and NC=90.05%, respectively. The sharpening and blurring attacks were also performed to evaluate the robustness. The sharpened image with PSNR=24.65 dB and the blurred image with PSNR =25.39 dB are shown in Figs. 10(a) and 11(a), respectively. The revealed secret images generated by VC with NC =95.72% and by computers with NC=91.43% from the sharpened image are shown in Figs. 10(b) and 10(c), respectively. The secret images recovered by VC with NC =95.38% and by computers with NC=90.77% from the blurred image are shown in Figs. 11(b) and 11(c), respectively. Next is the cropping attack, which erases the top left area (about 11%) of the image. The cropped image with PSNR=18.49 dB is shown in Fig. 12(a), and the revealed secret images recovered by VC and by computers from the cropped image, shown in Figs. 12(b) and 12(c), are NC =92.09% and NC=84.18%, respectively. We also consider the distorting and rescaling attacks. The distorted image with PSNR=21.05 dB is shown in Fig. 13(a), and the result of the revealed secret images recovered by VC with NC =92.48% and by computers with NC=84.95% from the distorted image are shown in Figs. 13(b) and 13(c), respectively. The rescaled image with PSNR=31.79 dB, shown in Fig. 14(a), is obtained by first downscaling the image by a factor of 2 in each direction and then upscaling the downscaled image to the original size. The result of the revealed secret images recovered by VC with NC=97.77% and by computers with NC=95.54% from the rescaled image are shown in Fig. 14(b) and 14(c), respectively. The jitter attack was also conducted.[16] We removed two distinct col-



(a) (b) (c)

Fig. 12 (a) Image with 11% of the top left area cropped (PSNR =18.49 dB), (b) the secret image revealed by VC (NC=92.09%), and (c) the secret image revealed by computers (NC=84.18%).



(a) (b) (c)

Fig. 14 (a) Rescaled image (PSNR=31.79 dB), (b) the secret image revealed by VC (NC=97.77%), and (c) the secret image revealed by computers (NC=95.54%).

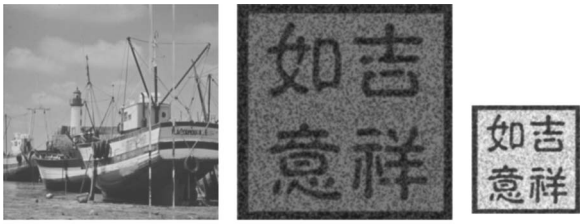


Fig. 15 (a) Jitter-attacked image (PSNR=20.33 dB), (b) the secret image revealed by VC (NC=91.87%), and (c) the secret image revealed by computers (NC=83.75%).

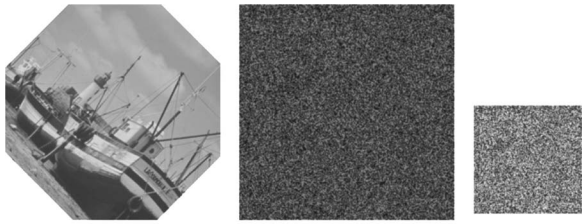


Fig. 16 (a) Image rotated 45 deg to the right (PSNR=10.31 dB), (b) the secret image revealed by VC (NC=76.03%), and (c) the secret image revealed by computers (NC=52.06%).

umns (with a width of 5 pixels) on the left half of the image and then inserted them into other positions on the right half. The jitter-attacked image with PSNR=20.33 dB is shown in Fig. 15(a) and the revealed secret images recovered by VC with NC=91.87% and by computers with NC =83.75% from the jitter-attacked image are shown in Figs. 15(b) and 15(c), respectively. Finally, the image was rotated 45 deg to the right and was examined. The rotated image with PSNR=10.31 dB is shown in Fig. 16(a) and the revealed secret images recovered by VC with NC=76.03% and by computers with NC=52.06% from the rotated image are shown in Figs. 16(b) and 16(c), respectively.

The preceding attacks with the same parameters were also used on some test images to further evaluate the robustness, and the results are shown in Tables 2 and 3. In Table 2, the revealed secret images are recovered by computers, and in Table 3, the revealed secret images are decoded by VC. According to the experimental results, we found that JPEG, sharpening, lightening, darkening, rescaling, and blurring attacks can merely cause little damage to the revealed secret images. On the other hand, cropping, noising, distorting, rotating, and jitter attacks may lead to more damage to the revealed secret images. Among these attacks, some may lead to low PSNR values such as lightening, darkening, cropping, distorting, and jitter attacks; however, it seems that the corresponding NC values will not decrease too much and hence the secret image can also be clearly identified. Especially, we found that the proposed method can effectively resist the lightening and darkening attacks. Since many compression techniques were developed in the frequency domain, the transform-domain watermarking schemes are inherently more robust against compression attacks than other spatial-domain approaches. Therefore, our method may to some extent not be as robust against compression attacks compared with transform-domain approaches. Finally, we observed that the proposed

Table 2 The PSNR and NC values of different test images on different attacks (by computers).

	"Airplane"		"Lenna"		"Peppers"		"Monalisa"	
Attacks	PSNR (dB)	NC (%)	PSNR (dB)	NC (%)	PSNR (dB)	NC (%)	PSNR (dB)	NC (%)
JPEG (compression ratio=5:1)	38.90	97.60	39.54	98.17	38.98	98.18	33.32	97.46
Sharpening	26.42	91.80	29.15	94.39	29.18	94.78	23.40	92.50
Lightening	18.59	100.0	18.59	100.0	18.59	100.0	18.60	99.78
Darkening	18.59	100.0	18.59	100.0	18.72	98.63	19.51	97.39
10% noising	24.44	88.18	24.47	89.77	24.44	90.92	24.58	93.20
11% cropping	18.84	79.82	14.87	74.75	14.73	76.1	15.33	84.00
Blurring	26.71	90.58	26.83	92.04	28.20	93.96	28.21	95.47
Distorting	21.93	83.57	22.49	86.73	22.57	88.33	23.72	92.44
Rescaling	32.91	95.42	37.23	97.67	36.64	97.71	30.64	96.59
Jitter	20.56	80.47	19.08	80.19	19.58	83.51	19.96	88.28
Rotation (45 deg to the right)	12.60	54.50	9.79	50.56	9.55	53.31	7.60	55.79

Note: The gray-level test images are of size 512×512 pixels and the revealed secret images are of size 256×256 pixels.

Table 3 The PSNR and NC values of different test images upon different attacks (by VC).

	"Airplane"		"Lenna"		"Peppers"		"Monalisa"	
Attacks	PSNR (dB)	NC (%)	PSNR (dB)	NC (%)	PSNR (dB)	NC (%)	PSNR (dB)	NC (%)
JPEG (compression ratio=5:1)	38.90	98.80	39.54	99.08	38.98	99.09	33.32	98.73
Sharpening	26.42	95.90	29.15	97.20	29.18	97.39	23.40	96.25
Lightening	18.59	100.0	18.59	100.0	18.59	100.0	18.60	99.89
Darkening	18.59	100.0	18.59	100.0	18.72	99.32	19.51	98.70
10% noising	24.44	94.09	24.47	94.88	24.44	95.46	24.58	96.60
11% cropping	18.84	89.91	14.87	87.37	14.73	88.05	15.33	92.00
Blurring	26.71	95.29	26.83	96.02	28.20	96.98	28.21	97.73
Distorting	21.93	91.78	22.49	93.36	22.57	94.17	23.72	96.22
Rescaling	32.91	97.71	37.23	98.84	36.64	98.86	30.64	98.29
Jitter	20.56	90.24	19.08	90.09	19.58	91.75	19.96	94.14
Rotation (45 deg to the right)	12.60	77.25	9.79	75.28	9.55	76.65	7.60	77.90

Note: The gray-level test images and the revealed secret images are of size 512×512 pixels.

scheme is vulnerable to the rotating attack or the cropping attack with more than 25% of the area cropped. In total, we can conclude that our scheme meets the requirements of unambiguousness and robustness against several common attacks.

6 Conclusions

A novel copyright protection scheme for digital images based on visual cryptography and statistics was proposed. The requirements of robustness and unambiguousness were satisfied by the use of SDM, since the parameters of the statistics of an image can not be easily changed by many common attacks. The experimental results proved that the proposed scheme can resist several common attacks, especially, the lightening and darkening attacks. Additionally, the proposed scheme does not alter the host image, and can identify the ownership without resorting to the original image. Hence, it is very suitable to protect those digital images that can not be altered, such as medical images. Next, our scheme enables multiple secret images to be cast into a single host image without causing any damage to other hidden images, and allows the secret image to be of any size regardless of the size of the host image.

In our method, we fully utilized the advantages of VC, which can recover the secret image with human eyes without the aid of computers. Security is also guaranteed by the two-out-of-two VC scheme, of which the required probability setting is satisfied by SDM. Thus, without the correct private key, no one can recover any meaningful image or obtain any secret information. Thus, the scheme is also suitable to cover the transmission of secret images.

Although the present version of the proposed scheme deals only with bilevel secret images, it is possible to extend the method to gray-level or color secret images. For example, to deal with gray-level secret images, we can transform the continuous-tone secret images into halftone images by halftoning methods, such as ordered dither, error diffusion, blue noise masks, green noise halftoning, direct binary search, dot diffusion, etc. Then, the same procedure that is used to deal with bilevel secret images can be employed to cast the halftone secret images. In the future, the issue of gray-level and color secret images will be further studied.

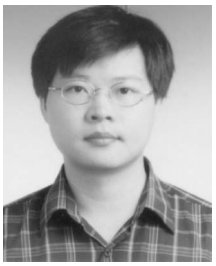
Acknowledgments

This work was supported in part by a grant from National Science Council of the Republic of China under the Project No. NSC-93-2213-E-032-033.

References

1. G. W. Braudaway, K. A. Magerlein, and F. Mintzer, "Protecting publicly-available images with a visible image watermark," *Proc. SPIE* **2659**, 126–133 (1996).
2. I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.* **6**(12), 1673–1687 (1997).
3. S. Low and N. Maxemchuk, "Performance comparison of two text marking methods," *IEEE J. Sel. Areas Commun.* **16**(4), 561–572 (1998).
4. K. Matsui, J. Ohnishi, and Y. Nakamura, "Embedding a signature to pictures under wavelet transform," *IEICE Trans.* **J79-D-II**(6), 1017–1024 (1996).
5. R. Ohbuchi, H. Masuda, and M. Aono, "Watermarking three-dimensional polygonal models through geometric and topological modifications," *IEEE J. Sel. Areas Commun.* **16**(4), 551–560 (1998).
6. S. Katzenbeisser and F. A. P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, pp. 101–109, Artech House, Norwood, MA (2000).
7. E. Koch, J. Rindfrey, and J. Zhao, "Copyright protection for multimedia data," in *Proc. Int. Conf. on Digital Media and Electronic Publishing*, pp. 6–8, Leeds, UK (Dec. 1994).

8. N. Nikolaidis and I. Pitas, "Copyright protection of images using robust digital signatures," in *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, Vol. **4**, pp. 2168–2171 (May 1996).
9. Y. C. Hou and P. M. Chen, "An asymmetric watermarking scheme based on visual cryptography," in *Proc. 5th Signal Process. Conf.*, Vol. **2**, pp. 992–995 (2000).
10. C. C. Chang, J. Y. Hsiao, and J. C. Yeh, "A colour image copyright protection scheme based on visual cryptography and discrete cosine transform," *Imaging Sci. J.* **50**, 133–140 (2002).
11. C. T. Hsu and J. L. Wu, "Hidden digital watermarks in image," *IEEE Trans. Image Process.* **8**, 58–68 (1999).
12. W. S. Kim, O. H. Hyung, and R. H. Park, "Wavelet based watermarking method for digital images using the human visual system," *Electron. Lett.* **35**, 466–468 (1999).
13. M. Naor and A. Shamir, "Visual cryptography," in *Proc. Advances in Cryptology-EUROCRYPT'94, LNCS 950*, pp. 1–12, Springer-Verlag (1995).
14. R. J. Hwang, "A digital image copyright protection scheme based on visual cryptography," *Tamkang J. Sci. Eng.* **3**(2), 97–106 (2000).
15. M. L. Berenson and D. M. Levine, *Basic Business Statistics: Concepts and Applications*, pp. 337–353, Prentice-Hall, Upper Saddle River, NJ (1999).
16. F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Attacks on copyright marking systems," in *Proc. of 2nd Workshop on Information Hiding*, Vol. **1525**, pp. 218–238, Portland, OR (Apr. 1998).



Ching-Sheng Hsu received his BA degree in 1994 from the Department of Information Management, National Cheng-Chi University, and his MA degree in 1998 from the Institute of Information Management, National Chi-Nan University, where he is currently pursuing his PhD degree in information management. His current research interests include information hiding, digital watermarking and copyright protection, cryptography, genetic algorithms, and computer-assisted learning and testing.

Young-Chang Hou received his BS degree in atmospheric physics from the National Central University, Taiwan, in 1972, his MS degree in computer applications from the Asian Institute of Technology, Bangkok, Thailand, in 1983, and his PhD degree in computer science and information engineering from the National Chiao-Tung University, Taiwan, in 1990. From 1976 to 1987, he was a senior engineer of air navigation and weather services with the Civil Aeronautical Administration, where his work focused on the automation of weather services. From 1987 to 2004 he was with the faculty at the National Central University. He is currently a professor with the Department of Information Management, TamKang University. His research interests include digital watermarking and information hiding, fuzzy logic, genetic algorithms, and cryptography.