International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:1, No:2, 2007

A Visual Cryptography and Statistics Based Method for Ownership Identification of Digital Images

Ching-Sheng Hsu and Young-Chang Hou

***Abstract*—**In this paper, a novel copyright protection scheme for digital images based on Visual Cryptography and Statistics is proposed. In our scheme, the theories and properties of sampling distribution of means and visual cryptography are employed to achieve the requirements of robustness and security. Our method does not need to alter the original image and can identify the ownership without resorting to the original image. Besides, our method allows multiple watermarks to be registered for a single host image without causing any damage to other hidden watermarks. Moreover, it is also possible for our scheme to cast a larger watermark into a smaller host image. Finally, experimental results will show the robustness of our scheme against several common attacks.

***Keywords*—**Copyright protection, digital watermarking, sampling distribution, visual cryptography.

I. Introduction

With the coming era of Internet, more and more data are transmitted and exchanged on the networked systems to enjoy the rapid speed and convenience. However, in the cyberspace, the availability of duplication methods encourages the violation of intellectual property rights of digital data. Therefore, the protection of rightful ownership of digital data has become an important issue in recent years. Digital watermarking, a kind of such techniques, is a method that hides a meaningful signature, or the so-called digital watermark, in an original image for the purpose of copyright protection, integrity checking, and captioning. In general, an effective watermarking scheme should satisfy certain requirements including imperceptibility, robustness, unambiguousness, security, capacity, and low computational complexity [1]–[4]. Some of these requirements may conflict each other and thereby introducing many technical challenges. For example, imperceptibility and capacity may conflict with robustness. Therefore, a reasonable compromise is required to achieve better performance for the intended applications.

In general, watermarking techniques can be grouped into two categories: one is the spatial-domain approach [5]–[7], and the other is the transform-domain approach [1][8]–[10]. Most related techniques use many pixels or transform coefficients to conceal one bit of information. Thus, the watermark should be much smaller than the original image so that the requirement of imperceptibility can be satisfied. Such property makes it impossible to embed a larger watermark into a smaller host image. Usually, the data of the original image should be adequately adjusted or altered for embedding the digital signature. If multiple watermarks need to be registered for a single digital image, it is also impossible for such methods to embed the latter watermark without destroying the former ones. Moreover, when the ownership of the image needs to be identified, many of the methods require the aid of the original image to extract the watermark.

In this paper, we propose a copyright protection scheme for digital images without restricting the size of watermarks. Our method does not need the image to be transformed between the spatial and frequency domains. Instead, the theories and properties of sampling distribution of the mean (SDM) are used to generate a master share from a host image. Then, the master share and the watermark are used to construct the ownership share according to some predefined rules of visual cryptography (VC). When the rightful ownership needs to be identified, the master share, generated from the image to be identified, and the ownership share are superimposed to reveal the watermark without the aid of computers. Our method can fully utilize the advantage of visual cryptography since we can use human eyes to recover the hidden watermarks without the aid of computers. Besides, the proposed scheme dose not needs to alter the original image and can identify the ownership without resorting to the original image. It is also possible for our scheme to register multiple watermarks for a single image without causing any damage to other hidden watermarks. Moreover, our method can attain the requirement of robustness because the characteristics and parameters of Statistics can not be easily changed by many attacks. Finally, the security of the scheme is ensured by the properties of visual cryptography.

II. Visual Cryptography

Visual cryptography 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 out any information about the secret [11]. Unlike traditional cryptographic schemes, visual cryptography uses human eyes to decrypt the secret without any complex decryption algorithms and the aid of computers. Usually, the decryption of the secret image consists of xeroxing more than k shares onto

Ching-Sheng Hsu is with the Department of Information Management, National Central University, P.O. Box 9-236, Jhongli, Taoyuan County 32099, Taiwan, R.O.C. (e-mail: jacketcc@mgt.ncu.edu.tw).

Young-Chang Hou is with the Department of Information Management, TamKang University, 151 Ying-Chuan Road, Tamshui, Taipei County, Taiwan 251, R.O.C. (phone: 886-2-2621-5656 ext. 3514; fax: 886-2-2620-9737; e-mail: ychou@mail.im.tku.edu.tw).

transparences and superimposing these transparences altogether; then, participants can identify the recovered secret from the stacked image by their eyes. Therefore, it is a quite simple but secure way to protect the secret. Basically, visual cryptography schemes should satisfy some security and contrast conditions. The following definition formally defines a *k*-out-of-*n* visual cryptography scheme [11]:

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 $C_0 = [C_{0,1}, C_{0,2}, \ldots, C_{0,u}]$ and $C_1 = [C_{1,1}, C_{1,2}, \ldots, C_{1,v}]$. To share a white (resp. black) pixel, the dealer randomly chooses one of the matrices in C_0 (resp. 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 $S \in C_0$, the *m*-vector *V* of ORing any *k* out of *n* rows of *S* satisfies $w(V) \le d - \alpha \cdot m$.
(2) For any matrix $S \in C_1$, the *m*-vector *V* of ORing any *k* out of *n* rows of *S* satisfies $w(V) \ge d$.
(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 D_t obtained by restricting each $n \times m$ matrix in 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 *V*, denoted by $w(V)$, is the number of '1' within *V*, and the gray-level of the stacked image is proportional to $w(V)$. The first two properties are related to the contrast of the image. The value α is called relative difference, and $\alpha \cdot m$ 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 C_0 (resp. C_1), and then the *i*-th row is used to represent the *m* subpixels on the *i*-th share. For example, the 2-out-of-2 visual cryptography scheme can be represented by the following two collections:

$$C_0 = \left\{ \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \right\}, \quad (1)$$

$$C_1 = \left\{ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}. \quad (2)$$

Note that the above two collections C_0 and C_1 will lead to distortion of the image. To remedy the drawback, one can use more subpixels to maintain the aspect ratio. Table I shows an alternative 2-out-of-2 visual cryptography scheme that can avoid distortion of the image. In such scheme, every secret pixel is expanded to four subpixels in each share to maintain the aspect ratio of the image. In the following sections, this scheme will be used to construct the copyright protection scheme for digital images.

TABLE I
THE 2-OUT-OF-2 VISUAL CRYPTOGRAPHY SCHEME

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

III. BASIC CONCEPTS OF STATISTICS

According to the theory of sampling distribution in Statistics, the sampling distribution of means (SDM) from a set of normally distributed data is also a normal distribution [12]. In Statistics, the arithmetic mean from a normally distributed population has several important mathematical properties, such as unbiasedness, efficiency, and consistency. The unbiased property signifies that the average of all the possible sample means of a given sample size *n* will be equal to the population mean μ. Note that the unbiased property is based on the assumption that the population itself is normally distributed. However, in many cases, it is not easy to know whether a population is normally distributed or not. To solve this problem, we introduce a useful theorem, the central limit theorem, to deal with the population with unknown distribution. According to the central limit theorem, as the sample size gets large enough, the sampling distribution of means can be approximated by the normal distribution. Statisticians have found a general rule that, for many population distributions, once the sample size is at least 30, the sampling distribution of means will be approximately normal. Therefore, a randomly selected sample mean $\overline{X}_t$ (with sample size $n \ge 30$) has identical probability of being greater or less than the population mean μ.

IV. THE PROPOSED SCHEME

In this section, we introduce the proposed watermarking scheme based on visual cryptography and the properties of SDM. Essentially, the scheme comprises the ownership share construction and the watermark revelation phases. In the following, we describe our scheme in more detail.

A. Ownership Share Construction

Assume that a copyright owner wants to cast a bi-level watermark W of size $N_1 \times N_2$ pixels into a gray-level host image of any size for protecting his/her ownership. Before we start to construct the ownership share O, the population mean μ of the pixel values of the host image should be calculated in advance. Besides, a random key $L = (l_1, l_2, \ldots)$, in which each random number corresponds to the location of a pixel in the host image, should be generated for sampling. For example, the first *n* elements are used to compute the first sample mean, the next *n* elements are used to compute the second sample mean, etc. Then, according to the central limit theorem and the unbiased property of SDM, we can form a normal distribution with a mean of μ by sampling from the host image. Assume that $\overline{X}_t$ denotes a sample mean with sample size $n \ge 30$ randomly

selected from the host image. Then, the occurrence of $\overline{X}_t \geq \mu$ and the occurrence of $\overline{X}_t < \mu$ have the identical probability of 0.5. Assume that $m_{i,j}$ denotes a pixel (with four subpixels) of the master share M. To generate a pixel $m_{i,j}$ of the master share M, we randomly choose n pixel values (according to L) to form a sample mean $\overline{X}_t$. Then, the comparison between the sample and population means is used to generate the master share according to the following generation rules:

Master Share Generation Rules:

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

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

Now, we can start to generate the ownership share. Assume that $w_{i,j}$ denotes a pixel of the watermark W, and $o_{i,j}$ denotes a pixel (with four subpixels) of the ownership share O. Also assume that 0 denotes a white pixel and 1 denotes a black pixel. After the master share M is generated, the watermark W and M are used to generate the ownership share O according to the following generation rules:

Ownership Share Generation Rules:

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

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

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

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

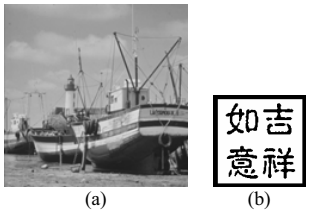
Finally, the random key L must be kept secretly by the copyright owner for proving his/her ownership, and the ownership share O should be sent to a trusted third party for further authentication.

B. Watermark Revelation

In the watermark revelation phase, the copyright owner should provide the same secret key L used in the ownership share construction 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 same rules presented in the previous section. After the master share M′ is created, the watermark W′ can be revealed by the principles of visual cryptography. That is, we can simply print both shares onto transparencies and then superimpose them. Thus, the rightful ownership of the image can be identified from the stacked transparency by our eyes.

V. Results And Discussions

In this section, several experiments are performed to demonstrate the robustness of the proposed scheme against several common attacks, including darken, lighten, rescale, blur, sharpen, noise, distortion, crop, jitter, and JPEG lossy compression. The gray-level host image of size 512 × 512 pixels is shown in Fig. 1(a), the bi-level watermark of size 256 × 256 pixels is shown in Fig. 1(b). The master share generated



(a) (b)

Fig. 1. (a) The gray-level host image (512 × 512 pixels); (b) the bi-level watermark (256 × 256 pixels).

from the original image (Fig. 1(a)) is shown in Fig. 2(a), the corresponding ownership share is shown in Fig. 2(b), and the stacked result of Fig 2(a) and Fig. 2(b) is illustrated in Fig. 2(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 hold. Besides, two common similarity measurements are introduced to evaluate the proposed watermarking scheme. One is the peak signal-to-noise ratio (*PSNR*) used to evaluate the similarity of two gray-level images, and the other is the normalized correlation (*NC*) used to measure the similarity between two bi-level images. The first measurement, peak signal-to-noise ratio, is defined as follows:

$$PSNR = 10 \times \log \frac{255^2}{MSE}, \tag{3}$$

where

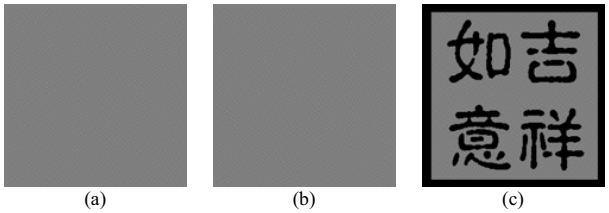
$$MSE = \frac{1}{M_1 \times M_2} \sum_{i=1}^{M_1} \sum_{j=1}^{M_2} (c_{i,j} - c'_{i,j})^2, \tag{4}$$

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

$$NC = \frac{\sum_{i=1}^{N_1} \sum_{j=1}^{N_2} \overline{w_{i,j} \oplus w'_{i,j}}}{N_1 \times N_2} \times 100\%, \tag{5}$$

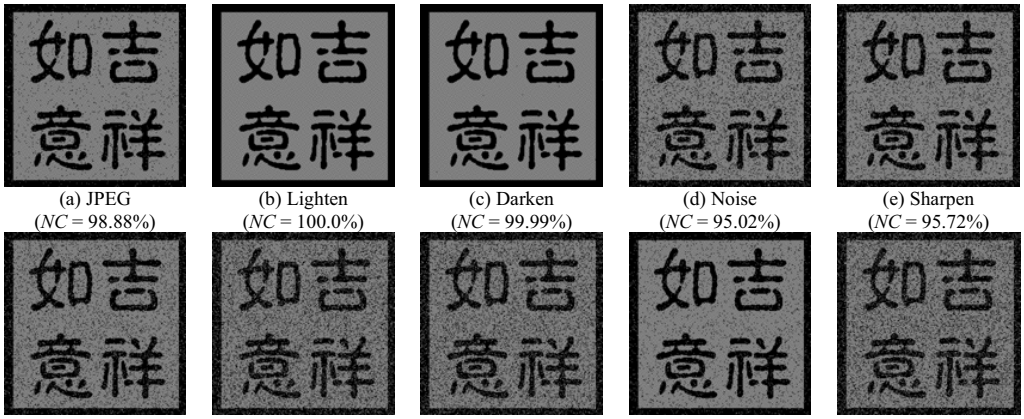
where $w_{i,j}$ denotes a pixel color of the original watermark W, $w'_{i,j}$ denotes a pixel color of the revealed watermark W′, and $N_1 \times N_2$ is the image size. Moreover, we use the sample size $n = 30$ to proceed all of the experiments.

The *PSNR* values of the attacked images with different image processing operations are as follows: *PSNR*(JPEG) = 37.77 dB, *PSNR*(Lighten) = 18.59 dB, *PSNR*(Darken) = 18.59 dB, *PSNR*(Noise) = 24.45 dB, *PSNR*(Sharpen) = 24.65 dB, *PSNR*(Blur) = 25.39 dB, *PSNR*(Crop) = 18.49 dB, *PSNR*(Distort) = 21.05 dB, *PSNR*(Rescale) = 31.79 dB, and *PSNR*(Jitter) = 20.33 dB. Note that the noised image is with 10% monochromatic noises. The cropped attack is used to erase



(a) (b) (c)

Fig. 2. (a) The master share generated from the original image (512 × 512 pixels); (b) the ownership share (512 × 512 pixels); (c) the stacked result of (a) and (b).



(a) JPEG (*NC* = 98.88%) (b) Lighten (*NC* = 100.0%) (c) Darken (*NC* = 99.99%) (d) Noise (*NC* = 95.02%) (e) Sharpen (*NC* = 95.72%)

(f) Blur (*NC* = 95.38%) (g) Crop (*NC* = 92.09%) (h) Distort (*NC* = 92.48%) (i) Rescale (*NC* = 97.77%) (j) Jitter (*NC* = 91.87%)

Fig. 3. The revealed watermarks from different attacked images and their corresponding *NC* values.

the top left area (about 1/3 × 1/3) of the image. The rescaled image 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. Besides, the jitter attack is used to remove two distinct columns (with the width of five pixels) on the left half of the image and then insert them into the other positions on the right half. Also note that the *NC* values of the revealed watermarks are measured according to Fig. 2(c) since they have the same image size. The revealed watermarks from different attacked images and their corresponding *NC* values are shown in Fig. 3.

According to the experimental results, we can find that JPEG, sharpened, lightened, darkened, rescaled, blurred, and noised attacks can merely cause little damage to the revealed watermark. On the other hand, cropped, distorted, and jitter attacks may lead to more damage to the revealed watermark. Among these attacks, some of them may lead to low *PSNR* values such as lightened, darkened, cropped, distorted, and jitter attacks; however, it seems that the corresponding *NC* values will not decrease too much and hence the watermarks can also be clearly identified. Besides, it is worth mentioning that our method can effectively resist the lighted and darkened attacks. Totally speaking, we can conclude that our scheme meets the requirements of unambiguousness and robustness against several common attacks.

In this paper, a novel copyright protection scheme for digital images based on visual cryptography and Statistics was proposed. The proposed scheme does not alter the original image, and can identify the ownership without resorting to the original image. Moreover, our scheme allows multiple watermarks to be cast into a single host image without causing any damage to other hidden watermarks. Finally, the size of the watermark is not restricted by that of the host image, thereby allowing casting a larger watermark into a smaller host image.

REFERENCES

[1] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Processing*. vol. 6, no. 12, pp. 1673-1687, 1997.

[2] S. Katzenbeisser and F. A. P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech house, Norwood, MA, 2000, pp. 101-109.

[3] E. Koch, J. Rindfrey, and J. Zhao, "Copyright protection for multimedia data," *Proc. Int. Conf. on Digital Media and Electronic Publishing*, Leeds, UK, pp. 6-8, December 1994.

[4] N. Nikolaidis and I. Pitas, "Copyright protection of images using robust digital signatures," *Proc. IEEE Int. Conf. On Acoustics, Speech and Signal Processing*, vol. 4, pp. 2168-2171, May 1996.

[5] Y. C. Hou and P. M. Chen, "An asymmetric watermarking scheme based on visual cryptography," *Proc. Fifth Signal Process. Conf.,* vol. 2, pp. 992-995, 2000.

[6] S. Low and N. Maxemchuk, "Performance comparison of two text marking methods," *IEEE J. Selected Areas in Communications*, vol. 16, no. 4, pp. 561-572, 1998.

[7] R. Ohbuchi, H. Masuda, and M. Aono, "Watermarking three-dimensional polygonal models through geometric and topological modifications," *IEEE J. Selected Areas in Communications,* vol. 16, no. 4, pp. 551-560, 1998.

[8] C. C. Chang, J. Y. Hsiao, and J. C. Yeh, "A colour image copyright protection scheme based on visual cryptography and discrete cosine transform," *The Imaging Science J.,* vol. 50, no. 133-140, 2002.

[9] C. T. Hsu and J. L. Wu, "Hidden digital watermarks in image," *IEEE Trans. Image Processing*, vol. 8, no. 58-68, 1999.

[10] W. S. Kim, O. H. Hyung, and R. H. Park, "Wavelet based watermarking method for digital images using the human visual system," *Electron. Lett.*, vol. 35, pp. 466-468, 1999.

[11] M. Naor and S A. Shamir, "Visual cryptography," *Advances in Cryptology-EUROCRYPT '94, LNCS 950, Springer-Verlag*, pp. 1-12, 1995.

[12] M. L. Berenson and D. M. Levine, *Basic Business Statistics: Concepts and Applications*. Prentice-Hall, New Jersey, 1999, pp. 337-353.