A Digital Image Copyright Protection Scheme Based on Visual Cryptography

Ren-Junn Hwang

Department of Computer Science and Information Engineering, TamKang University, Tamsui, Taipei Hsien, 251, Taiwan, R.O.C.
E-mail: junhwang@ms35.hinet.net

Abstract

A simple and efficient watermark method is proposed in this paper. The watermark method is an excellent technique to protect the copyright ownership of a digital image. The proposed watermark method is built up on the concept of visual cryptography. According to the proposed method, the watermark pattern does not have to be embedded into the original image directly, which makes it harder to detect or recover from the marked image in an illegal way. It can be retrieved from the marked image without making comparison with the original image. The notary also can off-line adjudge the ownership of the suspect image by this method. The watermark pattern can be any significant black/white image that can be used to typify the owner. Experimental results show that the watermark pattern in the marked image has good transparency and robustness. By the proposed method, all the pixels of the marked image are equal to the original image.

Key Words**:** image watermark, visual cryptography, copyright protection.

1. Introduction

The rapid growth of digital media such as Internet and CD's has made the digital images easy to distribute, duplicate, and modify. It is creating a pressing need for copyright enforcement methods that can protect copyright ownership. An image watermark method is now drawing the attention as a good technology of protecting copyrights for digital data [2, 7, 13]. It is realized by embedding identification information into the original image. We call the embedding identification information the "watermark pattern". The original image containing the watermark pattern is named "marked image". The watermark pattern in the marked image can be either visible [2] or invisible [3, 4, 8, 9, 11, 12, 14, 15,]. The visible watermark is limited in many applications. It distorts the original image fidelity and is susceptibly to attacks through direct image processing [3].

Generally speaking, an image watermark method must satisfy the following two requirements.

(1) Transparency: the embedded watermark pattern does not visually spoil the original image fidelity and should be perceptually invisible.

(2) Robustness: the watermark pattern is hard to detect and remove in an illegal way.

There are many research articles [3, 4, 8, 9, 11, 12, 14, 15,] exploring the watermark method. Some methods hide the watermark pattern in the spatial domain [8, 11, 15] and the others embed the watermark pattern into the frequency domain [3, 9, 12, 14,]. However, several watermark methods listed above are not robust, and the watermark pattern is easy to remove [7].

In 1994, Naor and Shamir [10] proposed the concept of visual cryptography. By their method, a shared image can be reconstructed by stacking some authorized shadow images without performing any computation. Any subset of

unauthorized shadow images cannot infer any knowledge about the shared image. We shall briefly review their idea in Section 2. In this paper, we devise a watermark method based on the visual cryptography. By the proposed method, the watermark pattern is difficult to detect and remove since the security characteristics of the visual cryptography. It is efficient to adjudge the ownership of a suspect image by easily retrieving the watermark pattern from the suspect image. Additionally, the watermark pattern can be any significant black/white image for the owner in our proposed method, which makes them superior to some watermark method that use numerical codes as watermark patterns. In our new method, the watermark pattern can be retrieved from the marked image in a legal way without any information about the original image.

This paper is organized as follows. Section 2 briefly reviews Naor and Shamir's visual cryptography. Section 3 presents our watermark method based on visual cryptography. Section 4 reports some experimental results and makes some discussions concerning our method. Finally, conclusions appear in Section 5.

2. Naor and Shamir's Visual Cryptography

The visual cryptography is a new concept defined by Naor and Shamir [10]. It is an extended type of (t, n)-threshold scheme which is also named the (t, n)-visual threshold scheme. In [10], the shadow of each participant is a transparency showing random dots. The shared secret is an image composed of black and white pixels. Any t out of these n shadows can make the shared secret recognized through the human visual system when they are stacked together. Any t-1 (or less) shadows stacked together can generate no knowledge about the shared secret. In this section, we shall take a (2,2)-visual threshold scheme created by Naor and Shamir for example. This (2,2)-visual threshold scheme is also to be used to construct the new image watermark scheme in Section 3.

The image stored in the computer system can be considered a composition of pixels. Let each pixel be stored in d bits. Then, a 2^d gray-leveled image can be shown by using a set of pixels. The watermark pattern discussed in this paper is composed of black or white pixels. It only uses one bit to express each pixel. Table 1 illustrates a simple (2,2)-threshold scheme based on Naor and Shamir's idea [10]. It also specifies the algorithm to encode each pixel in the shared image. This algorithm is applied to each pixel in the shared image in order to generate the corresponding subpixels in its corresponding two shadows. Each pixel P in the shared image is divided into two subpixels in each of these two shadows. If P is black, then the dealer randomly selects one of the first two rows in Table 1. If P is white, then the dealer randomly selects one of the last two rows in Table 1. Then the dealer puts two two-subpixels blocks from Columns 2 and 3 to the corresponding positions in Shadows 1 and 2, respectively.

Table 1. A (2, 2)-visual threshold scheme

Pixel	block 1	block 2	block 1 superimposes on block 2
■	■□ (1, 0)	□■ (0, 1)	■■ (1, 1)
■	□■ (0, 1)	■□ (1, 0)	■■ (1, 1)
□	■□ (1, 0)	■□ (1, 0)	■□ (1, 0)
□	□■ (0, 1)	□■ (0, 1)	□■ (0, 1)

Note: bit "1" denotes black and bit "0" denotes white.

Let's consider the result when these two shadows are stacked together. For each pixel P in the shared image, if P is black, then it generates a block with two black subpixels when these two shadows are stacked together. If P is white, then it generates a block with one black subpixel and one white subpixel when these two shadows are stacked together. The result is a collection of two black/white subpixels, which are printed in close proximity to each other so that the human visual system averages their individual black/white contributions. Through the human visual system, the block with two black subpixels will be recognized as a black dot while the block with one black subpixel and one white subpixel will be recognized as a white dot. Obviously, we can readily recognize if an image is the shared image with our visual system when these two shadows are stacked together.

3. The Proposed Watermark Method

This section shall describe the proposed watermark method to embed a watermark pattern into an image. This method is based on the simple (2,2)-visual threshold scheme described in Section 2. Section 4 shall show the experimental results of the proposed method.

Figure 1 presents the diagram of this method. The owner should select an h×n black/white image as her/his watermark pattern P. In the embedding process, she/he generates the verification information from the original image based on the (2,2)-visual cryptography (which is presented in Section 2) by defining the watermark pattern as the shared image. Virtually, the verification information is one shadow of the visual cryptography. The owner should register the watermark pattern of her-/himself and the verification information of her/his image at the notarial organization.

In the embedding processes, the owner should randomly select a number as her/his secret key, S, to embed the watermark pattern into the image M. The secret keys for different images either are equal or not. The owner should keep it secretly. We assume that the owner wants to embed the h×n watermark pattern into the image M that is a k×l 256 gray-leveled image. The owner embeds the watermark pattern P into the image M by generating the secret key, S, and the verification information, V, as the following steps.

Step E-1. Select a random number S as the secret key of the image M.

Step E-2. Use S as the seed to generate h×n different random numbers over the interval [0, k×l]. (We use R_i to denote the i-th random number.)

Step E-3. Assign the i-th pair (v_{i1}, v_{i2}) of the verification information V based on Table 2.

Step E-4. Assemble all the (v_{i1}, v_{i2}) pairs to construct the verification information V.

Note that Step E-3 constructs the verification information based on the watermark pattern. The proposed method does not embed the watermark pattern into Image M or alter any pixel of Image M.

Table 2. The rules to assign the value of verification information

The color of the *i*-th pixel in *watermark pattern* is	The left most bit of the R_i-th pixel of Image *M* is	Assign the *i*-th pair, (v_{i1}, v_{i2}), of *verification information V* to be
Black	"1"	(0, 1)
Black	"0"	(1, 0)
White	"1"	(1, 0)
White	"0"	(0, 1)

If the owner wants to prove that somebody is appropriating the image M as the image F, she/he has to provide the secret key S to the notarial organization. The notarial organization retrieves the verification information V and the watermark pattern P, which the owner has registered, and verifies the ownership of the image F as follows:

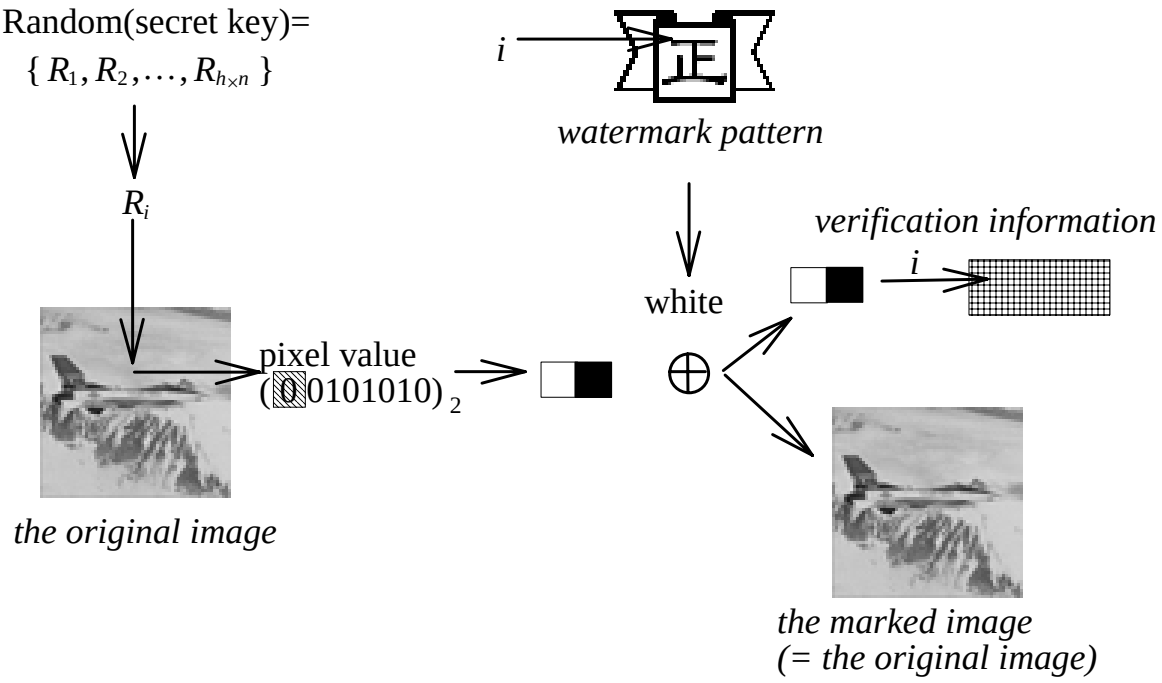
Step V-1. Use S as the seed to generate h×n different random numbers over the interval [0, k×l]. (We use R_i to denote the i-th random number.)

Step V-2. Assign the color of the i-th pixel of the watermark pattern P' based on Image F as follows:

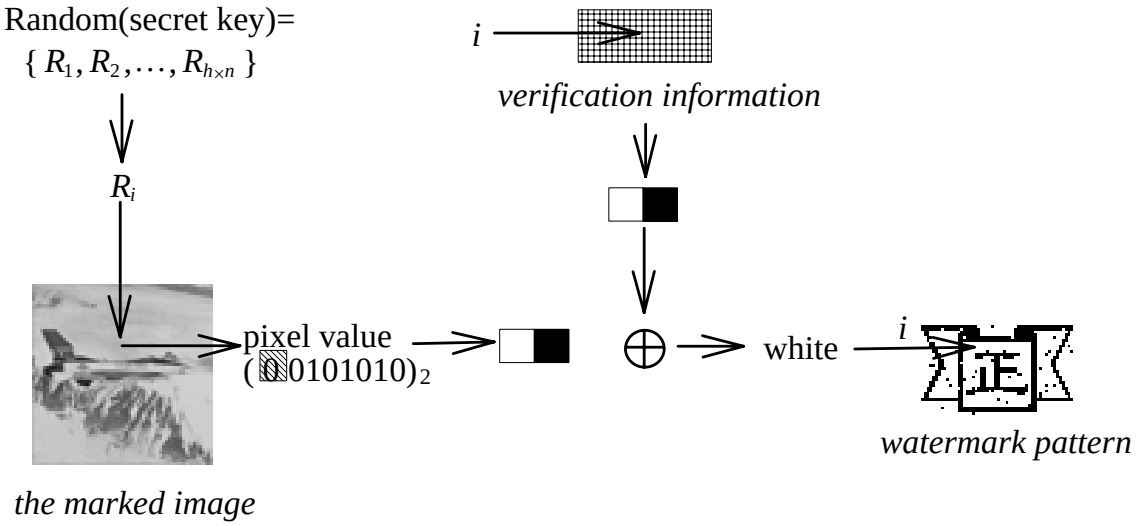
Step V-2-1. Get the left-most bit, b, of the R_i-th pixel of Image F, and, if b is "1", then assign f_i=(1, 0); otherwise, f_i=(0, 1).

Step V-2-2. If f_i is equal to the i-th pair of V then assign the color of the i-th pixel of P' to be white; otherwise, assign it to be black.

Step V-3. If P' can be recognized as P through the human visual system, the notarial organization shall adjudge that the image F is a copy of M.



(a) the embedding process



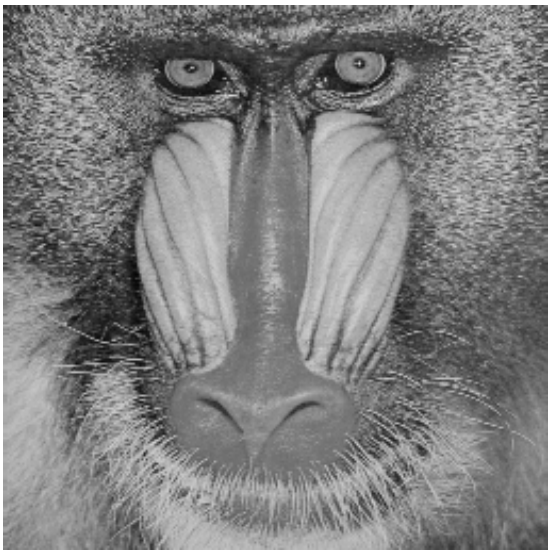
(b) the verification process

Figure 1. The diagram of our method

4. Experimental Results and Discussions

It is hard to evaluate the effect of a watermark method only theoretically. This section presents some experimental results concerning the proposed methods. All our experiments are performed on a personal computer with Intel Pentium 100. Three monochrome images with 256×256 pixels, “Lena”, “Baboon” and “F-16” (shown in Figure 2), are used in our experiments. In these images, each pixel contains 256 gray levels. Figure 3 shows the black/white watermark pattern, “Cheng”, which we want to embed into these three images. By Step E-3, The proposed method does not alter any pixel value of the original image to generate the marked image. In other words, the marked image is the same as

(a) Lena



(b) Baboon

(c) F-16

Figure 2. Three monochrome images of our experiments

Figure 3. The black/white watermark pattern: “Cheng”

the original image. The transparency is good for the proposed methods. The experimental results are shown in Table 3.

The fourth column of Table 3 shows the watermark patterns which are retrieved from the decompressed marked images with loss JPEG compression. The watermark pattern can be recovered clearly in our method, although the marked image has been compressed by loss JPEG compression in each quality level of Photoshop. The robustness of the watermark pattern embedding by our method in these results is good.

The proposed method uses different verification information for different marked images. This is the weakness of the proposed method. However, this will imply that each pixel of the marked image is the same as its corresponding pixel in the original image.

The watermark pattern is not embedded into the marked image directly in the proposed method. The secret information is one of the shadows generated from the watermark pattern as is in the (2,2)-visual threshold scheme in Section 2. The verification information is the other one. As far as visual cryptography is concerned, it is hard to recover the watermark pattern from only one shadow (secret information). In addition, the secret information is got from some random positions based on the secret key, which is kept secretly by the owner. It is difficult for anybody except the owner to detect the pixels concerning the watermark pattern. Nobody can recover or detect the watermark pattern from the marked image without the owner’s secret key and the registered verification information. The watermark pattern is hard to detect in an illegal way.

In the verification processes of the proposed methods, the watermark pattern can be recovered without any information about the original image. The notary adjudges the ownership of the image in a computer system. Actually, it can be done off-line. By assigning “1” as the black color and “0” as white, the verification information can be printed as a black/white image on a slide. The owner registers this slide instead of the verification information at the notarial organization. In the same way, in the verification process, we can

PSNR of the *marked image*	The image quality of JPEG compression with Adobe Photoshop (version 4.0)	The recovered *watermark pattern* : "Cheng"
Marked Image = Original Image	0/low (the size of the compressed file is 10582 Bytes)	
	1/low (the size of the compressed file is 12620 Bytes)	
	2/low (the size of the compressed file is 14029 Bytes)	
	3/middle (the size of the compressed file is 15781 Bytes)	
	4/middle (the size of the compressed file is 17590 Bytes)	
	5/middle (the size of the compressed file is 16127 Bytes)	
	6/high (the size of the compressed file is 21012 Bytes)	
	7/high (the size of the compressed file is 25348 Bytes)	
	8/maximal (the size of the compressed file is 31793 Bytes)	
	9/maximal (the size of the compressed file is 40088 Bytes)	
	10/maximal (the size of the compressed file is 48611 Bytes)	

(a) Use our method to embed "Cheng" into "Lena" (with 65536 Bytes)

PSNR of the *marked image*	The image quality of JPEG compression with Adobe Photoshop (version 4.0)	The recovered *watermark pattern* : "Cheng"
Marked Image = Original Image	0/low (the size of the compressed file is 18277 Bytes)	
	1/low (the size of the compressed file is 22242 Bytes)	
	2/low (the size of the compressed file is 24562 Bytes)	
	3/middle (the size of the compressed file is 27163 Bytes)	
	4/middle (the size of the compressed file is 30870 Bytes)	
	5/middle (the size of the compressed file is 28524 Bytes)	
	6/high (the size of the compressed file is 33629 Bytes)	
	7/high (the size of the compressed file is 38331 Bytes)	
	8/maximal (the size of the compressed file is 45158 Bytes)	
	9/maximal (the size of the compressed file is 54393 Bytes)	
	10/maximal (the size of the compressed file is 63970 Bytes)	

(b) Use our method to embed "Cheng" into "Baboon" (with 65536 Bytes)

PSNR of the *marked image*	The image quality of JPEG compression with Adobe Photoshop (version 4.0)	The recovered *watermark pattern* : “Cheng”
Marked Image = Original Image	0/low (the size of the compressed file is 9867 Bytes)	
	1/low (the size of the compressed file is 11846 Bytes)	
	2/low (the size of the compressed file is 12994 Bytes)	
	3/middle (the size of the compressed file is 14479 Bytes)	
	4/middle (the size of the compressed file is 16579 Bytes)	
	5/middle (the size of the compressed file is 15342 Bytes)	
	6/high (the size of the compressed file is 18295 Bytes)	
	7/high (the size of the compressed file is 21440 Bytes)	
	8/maximal (the size of the compressed file is 26413 Bytes)	
	9/maximal (the size of the compressed file is 33451 Bytes)	
	10/maximal (the size of the compressed file is 41627 Bytes)	

(c) Use our methodto embed “Cheng” into “F-16” (with 65536 Bytes)

Table 3. Experimental results

generate another slide based on f_i's. The notary can stack these two slides together and recognize the result to adjudge the ownership. There is no need to perform any computation at all.

5. Conclusion

The proliferation of digitized image is creating a pressing need for copyright enforcement schemes that protect copyright ownership. The watermarking scheme is an excellent method to protect copyright ownership [6]. In this paper, we propose a watermark method based on visual cryptography. We summarize the characteristics of the proposed method as follows:

(1) The watermark pattern can be any significant black/white image that can be used to typify the owner.
(2) The watermark pattern does not have to be embedded into the original image directly. (All the pixels of the marked image are the same as those of the original image.)
(3) The watermark pattern can be retrieved without any information about the original image.
(4) It is hard to detect the pixel concerning the watermark pattern without the secret key that is kept secretly by the owner.
(5) The watermark pattern can not be retrieved from the marked image unless the retriever has the secret key and the verification information simultaneously.
(6) The notary can adjudge the ownership of the image off-line.

Reference

[1] Bender W., Gruhl D., Morimoto N. and Lu A., "Techniques for Data Hiding," *IBM System Journal*. Vol. 35, No. 3, pp. 313-336 (1996).

[2] Braudaway G. W., Magerlein K. A. and Mintzer F., "Protecting Publicly-available Images with a Visible Image Watermark," In *the Proceedings of SPIE*, Vol. 2659, pp. 126-133(1996).

[3] Cox I. J., Kiliant J., Leighton T. and Shamoon T., "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions on Image Processing*, Vol. 6, No. 12, pp. 1673-1687(1997).

[4] Hsu C. and Wu J., "DCT-Based Watermarking for Video," *IEEE Transactions on Consumer Electronics*, Vol. 44, No.1, pp.206-215(1998).

[5] Hsu C. T. and Wu J. L., "Hidden Digital Watermarks in Images," *IEEE Transactions on Image Processng*, Vol. 8, No. 1, Jan, pp. 58-68(1999).

[6] Hwang M. S., Chang C. C., and Hwang K. F., "A Watermarking Technique Based on One-way Hash Functions," *IEEE Transactions on Consumer Electronics*, Vol. 45, No. 2, pp. 286-294(1999).

[7] Inoue H., Miyazaki A., Yamamoto A. and Katsura T., "A Digital Watermark Technique Based on the Wavelet Transform and Its Robustness on Image Compression and Transformation," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E82-A, No. 1, pp.2-10(1999).

[8] Low S. and Maxemchuk N., "Performance Comparison of Two Text Marking Methods," *IEEE Journal on Selected Areas in Communications*, Vol. 16, No. 4, pp.561-572(1998).

[9] Matsui K., Ohnishi J., and Nakamura Y., "Embedding a Signature to Pictures under Wavelet Transform," *IEICE Transactions*, Vol. J79-D-II, No. 6, pp. 1017-1024(1996).

[10] Naor N. and Shamir A. "Visual Cryptography," *Advances in Cryptology: Eurocrypt'94*, Springer-Verlag, Berlin, pp. 1-12(1995).

[11] Ohbuchi R., Masuda H., and Aono M., "Watermarking Three-Dimensional Polygonal Models Through Geometric and Topological Modifications," *IEEE Journal on Selected Areas in Communications*, Vol. 16, No. 4, pp.551-560(1998).

[12] Ohnishi J. and Matsui K., "Embedding a Seal into a Picture under Orthogonal Wavelet Transform," *The Proceedings of IEEE International Conference on Multimedia Computing and Systems*, pp. 514-512(1996).

[13] O'Ruanaidh J. J. K., Dowling W. J., and Boland F. M., "Watermarking Digital

Images for Copyright Protection," *IEE Proceedings-Visual Image Signal Processing*, Vol. 143, No. 4, pp. 250-256(1996).
[14] Swanson M. D., Zhu B. and Tewfik A. H., "Transparent Robust Image Watermarking," *The Proceedings of IEEE International Conference on Image Processing*, Vol. 3, pp. 211-214(1996).
[15] Voyatzis G. and Pitas I. "Applications of Toral Automorphisms in Image Watermarking," *The Proceedings of IEEE International Conference on Image Processing*, Vol. 2, pp. 237-240(1996).
[16] Xia X. G., Boncelet C. G. and Arce G. R., "A Multiresolution Watermark for Digital Images," *The Proceedings of IEEE International Conference on Image Processing*, Vol. 1, pp. 548-551(1997).

Accepted: Sep. 20, 2000