Visual Cryptography and Image Watermarking Scheme for Generating Meaningful Information

Yung-Hsiang Chen[1], Shen-Jwu Su[2]

[1] *Instrument Technology Research Center, National Applied Research Laboratories*

[1]yschen@itrc.org.tw

[2] *Department of Aviation Mechanical Engineering, China University of Science and Technology*

[2]susj@cc.chit.edu.tw

***Abstract*—This paper proposes a visual cryptography and image watermarking scheme for generating meaningful information. In the proposed scheme, the watermark is embedded into the protected image and visual cryptography scheme for generating two meaningful transparencies. The scheme is used to generate two public images and a secret image by using the visual cryptography technique. Then the secret image is registered to key watermark for further protection. In the step of watermark extraction, the watermark can be acquired by performing operation between the secret image and the public images. The experimental results show that the proposed scheme not only can clearly verify the copyright of the digital image, but also is robust to with stand several image processing attacks, such as random noise, holding, and crossing attacks.**

***Keywords*—Cryptography, visual secret sharing, digital image watermarking, image processing.**

1. INTRODUCTION

Visual cryptography is proposed by Naor and Shamir [1], that is a process of image sharing to uses human visual ability to decrypt. Recently, more and more researches [2-5] about visual cryptography were proposed. In most researches about the topic, secret image is encrypted into noise-like transparencies.

Among the most popular contents where digital watermarking is applied on are images. An example scenario is where a renowned photographer puts his photo collection online, i.e. creates an art gallery on his website to share with the rest of the world, but at the same time he would want to lay claim to those photos and not want anyone who downloads his photos to claim them for his own. Digital watermarking schemes typically require two phases: watermark embedding and watermark detection, and they are often designed to ensure that the scheme is robust against various types of attacks. The robustness [6] of a watermarking scheme is the ability of the watermarked content to survive signal processing operations and also intentional tampering. On the other hand, some watermarking schemes are fragile [6], in that the watermark easily becomes undetectable after even minor modifications of the watermarked content in which it is embedded. Though this is normally undesirable for most applications, this fragility property can be useful for content authentication, i.e. checking the content's integrity against unauthorized tampering.

2. THE PROPOSED SCHEME

Fig. 1 is the flow chart of our proposed method proposes a visual cryptography and image watermarking scheme for generating meaningful information. We proposed scheme, the watermark is embedded into the protected image and visual cryptography scheme for generating two meaningful transparencies. The scheme is used to generate two public images and a secret image by using the visual cryptography technique.

Visual cryptography is the core of the proposed copyright protection scheme. The concept of (k, n) visual cryptography technique is firstly proposed by Naor and Shamir [1] to protect the security of a secret image. The main advantage of their method is simple computation and security. A secret image can be divided into n different sharing images and the secret image can be recovered from k or more than k sharing images. However, the more the sharing images are, the harder the management is [1]. Hence, in the paper, a simple and secure (2, 2) visual

cryptography technique is adapted in the proposed scheme.

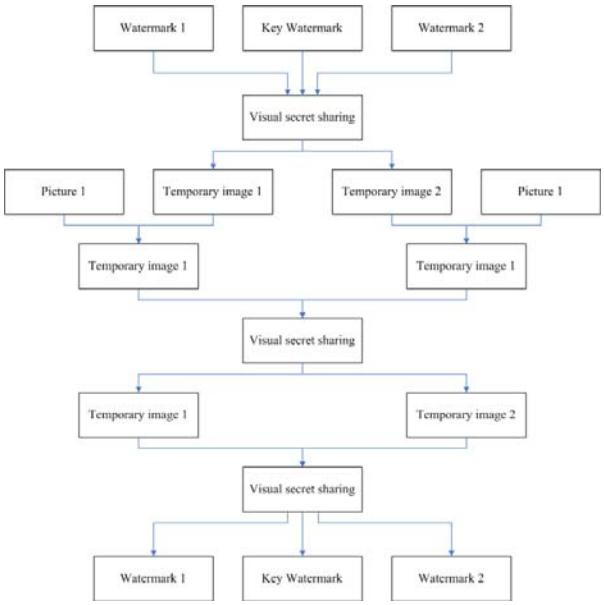


Fig. 1. The flow chart of our proposed method

Fig. 2 is the concept of visual cryptography technique. According to the concept of Naor and Shamir scheme, each pixel of an image is replaced by 2×2 pixels. Hence, a secret image with M by N pixels can be divided into two sharing images with 2M by 2N pixels. In addition, the secret image can be recovered by stacking the two sharing images.

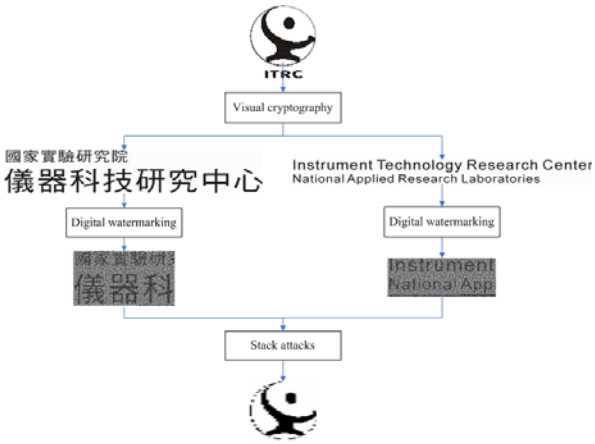


Fig. 2. The concept of visual cryptography technique

We describe an example of the black and white definition of a block in table 1. Table 2 shows all cases of the stacking results of proposed scheme. Fig. 3 shows an example of the pixel exchange method: (a) Secret pixel 1;(b)Secret pixel 2;(c)Stacking result. Fig. 4 shows the experimental result of share-1, share-2, and the retrieved secret image: (a)original F16 image; (b)binary image; (c) share-1;(d) share-2;(e) the retrieved secret image from share-1 superimposed on share-2.

Table 1. An example of the black and white definition of a block

2×2	Secret pixel	Stacking result
White	(2,2)	(3,1)
Black	(3,1)	(4,0)

.

Table 2. All cases of the stacking results of proposed scheme

Image	Secret pixel (white)				Secret pixel (black)			
Key	□	□	□	□	■	■	■	■
W1	■	■	□	□	■	■	□	□
W2	■	□	■	□	■	□	■	□
Share1								
Share2								
Stacking								

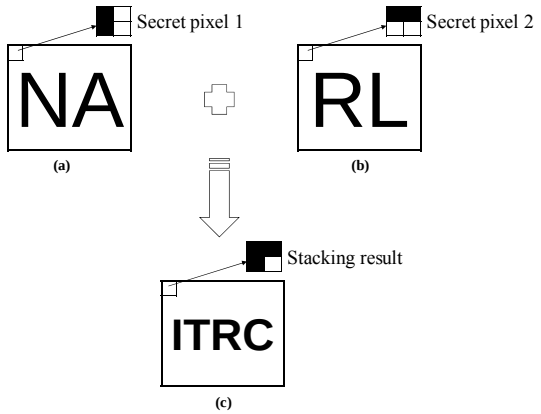
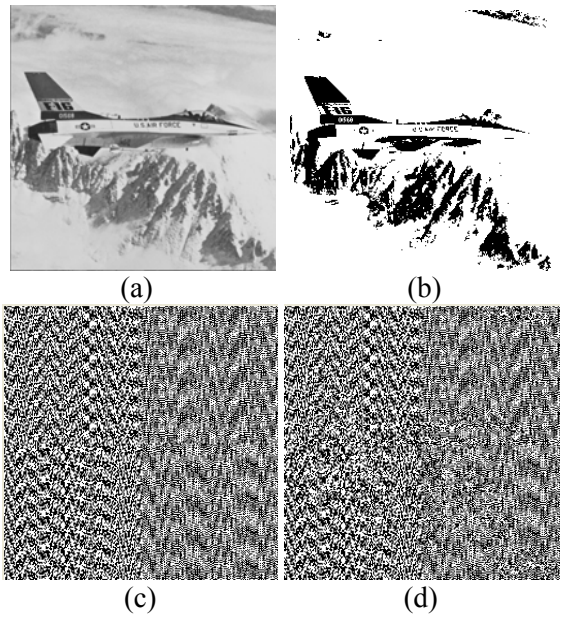
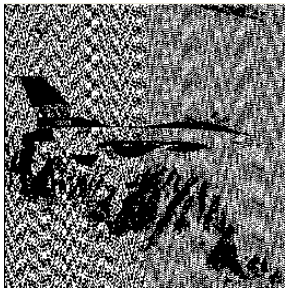


Fig. 3. An example of the pixel exchange method





(e)

Fig. 4. The experimental result of share-1, share-2, and the retrieved secret image

3. EXPERIMENTAL RESULTS AND ANALYSIS

This section presents some experiments to show that the proposed scheme can meet the requirements for copyright protection. Our experiments were executed on a personal computer using C++ programming language. Fig. 5 shows the secret image "ITRC" with 75×75 pixels. Fig. 6 (a)(b) shows the host images "logo-1" and "logo-2" with 336×66 pixels and 469×48 pixels. Fig. 7 (a)(b) shows two meaningful transparencies, which are generated after the proposed encoding process. Fig. 8 shows watermark images. We used two gray-level images, "Lena" and "Baboon" with a size of 512×512 pixels as our watermark images. In addition, the peak signal to noise ratio (PSNR) is used to measure the image quality, which is defined as follows:

$$PSNR = 10\log_{10}\frac{255^2}{MSE}(dB) \quad (1)$$

$$MSE = \frac{1}{m \times n}\sum^{m-1}\sum^{n-1} \quad (2)$$

The watermarked image1 quality PSNR = 36.16, and the watermarked image2 quality PSNR = 36.13. The experimental results show that the proposed scheme not only can clearly verify the copyright of the digital image, but also is robust to with stand several image processing attacks.

Fig. 9 shows the stacking result of all the meaningful transparencies. We also perform several image attacks such as random noise, holding, and crossing attacks on the watermark images "Lena" and "Baboon". We used the image-processing to implement the above image attacks. The experimental results are listed in Fig. 10-12.

Fig. 5. Secret image

(a)

(b)

Fig. 6. Host images

(a) (b)

Fig. 7. Two meaningful transparencies

(a) (b)

Fig. 8. Watermark images

(a)

(b)

(c)

Fig. 9. Stacking result of all the meaningful transparencies

3.1 The experimental result under random noise attack

Fig. 10 is the experimental result under random noise attack. Fig. 10(a)(b) are the watermark image 1 and watermark 2. Fig. 10 (c)-(e) shows the stacking result of all the meaningful transparencies. The watermarked image1 quality PSNR = 20.65, and the watermarked image 2 quality PSNR = 20.85.

(a) (b)

(c)

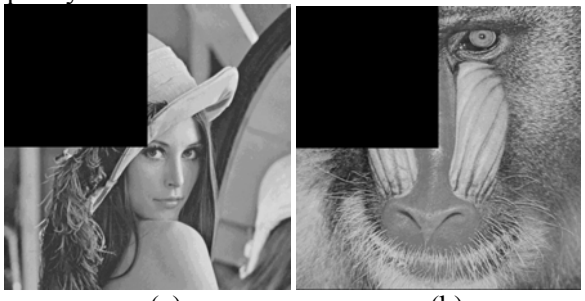
(d)

(e)

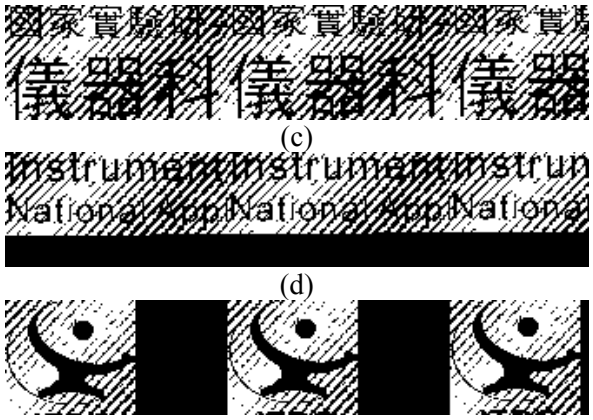
Fig. 10. The experimental result under random noise

3.2 The experimental results under holding attack

Fig. 11 is the experimental result under holding attack. Fig. 11(a)(b) are the watermark image 1 and watermark 2. Fig. 11 (c)-(e) shows the stacking result of all the meaningful transparencies. The watermarked image1 quality PSNR = 11.58, and the watermarked image2 quality PSNR = 11.56.



(a) (b)



(c)

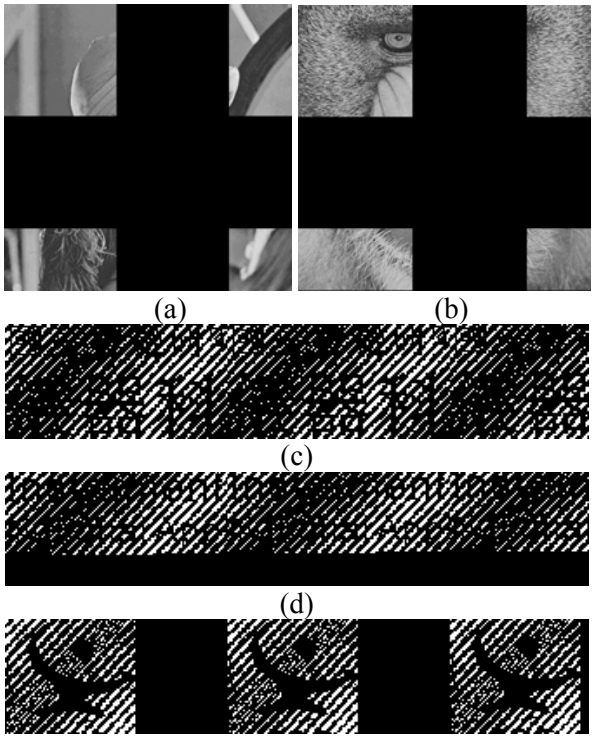
(d)

(e)

Fig. 11. The experimental results under holding attack

3.3 The experimental results under crossing attack

Fig. 12 is the experimental result under crossing attack. Fig. 12(a)(b) are the watermark image 1 and watermark 2. Fig. 12 (c)-(e) shows the stacking result of all the meaningful transparencies. The watermarked image1 quality PSNR = 7.03, and the watermarked image2 quality PSNR = 7.25.



(a) (b)

(c)

(d)

(e)

Fig. 12. The experimental results under crossing attack

4. CONCLUSIONS

This paper proposes a visual cryptography and image watermarking scheme for generating meaningful information. In the proposed scheme, the watermark is embedded into the protected image and visual cryptography scheme for generating two meaningful transparencies. The scheme is used to generate two public images and a secret image by using the visual cryptography technique. Then the secret image is registered to key watermark for further protection. In the step of watermark extraction, the watermark can be acquired by performing operation between the secret image and the public images. The experimental results show that the proposed scheme not only can clearly verify the copyright of the digital image, but also is robust to with stand several image processing attacks, such as random noise, holding, and crossing attacks.

REFERENCES

[1] M. Naor, and A. Shamir, "Visual Cryptography". *In Advances in Cryptology – Eurocrypt 94*, Springer, Berlin, pp. 1-12, 1995.

[2] Y. H. Chen, and S. J. Su, "Attack and benchmark of digital watermarks". *The 22th IPPR Conference on Vision Graphics and Image Processing*, pp. 1227-1233, 2009.

[3] S. C. Chu, J. F. Roddick, Z. M. Lu, J. S. Pan, "A digital image watermarking method based on labeled bisecting clustering algorithm". *IEICE Transactions on Fundamentals,* pp. 282-285, 2004.

[4] C. C. Chang, T. S. Chen, L. Z. Chung, "A steganographic method based upon JPEG and quantization table modification". *Information Sciences,* pp. 123-138, 2002.

[5] D. C. Wu, W. H. Tsai, "A steganographic method for images by pixel-value differencing". *Pattern Recognition Letters,* pp. 1613-1626, 2003.

[6] R. C. Gonzalez, R. E. Woods, "Digital Image Processing". Prentice Hall, 2002.