Controllable Transparency Image Sharing Scheme for Grayscale and Color Images with Unexpanded Size

Yi-Chong Zeng*, and Chi-Hung Tsai†
*Advanced Research Institute, Institute for Information Industry, Taipei, Taiwan, R.O.C.
E-mail: yichongzeng@iii.org.tw Tel:+886-2-66072958
†Advanced Research Institute, Institute for Information Industry, Taipei, Taiwan, R.O.C.
E-mail: brick@iii.org.tw Tel:+886-2-66072922

***Abstract*—Aimed at transparency controlling to secret image, we propose an image sharing scheme to encrypt secret image among two or more sharing images. The overall effects of the proposed method are the achievements of controllable transparency of secret image and unexpanded size of sharing images. The controllable transparency image sharing scheme is realized based on the principle of penetrability. While light passes through a medium, medium declines illumination of light. We treat pixel as medium and adjust pixels' value of multiple sharing images, so that transparency of decrypted-secret image is controllable. The experiment results will demonstrate that our scheme can be applied to grayscale and color images for visual cryptography. Furthermore, similarity between sharing image and secret image is low by using the proposed scheme.**

I. INTRODUCTION

Visual cryptography techniques encrypted secret information among two or more shares. For *n*-out-of-*n* visual cryptography method [1, 2], secret is decrypted incorrect while number of sharing images is not equal to *n*. In the past studies, researchers presented numerous visual cryptography techniques for black-and- white images, and crypto-array the base of sharing image was mentioned in literatures. Furthermore, researchers intended to use *k*-out-of-*n* visual cryptography methods performed on grayscale and color images, such as [3-9].

Blude et al. analyze and defined visual cryptography schemes for gray-level images in [3]. They emphasized on how to employ *k*-out-of-*n* visual cryptography applied to grayscale shares. In [4], Lin and Tsai used dithering technique to convert a grayscale image to an approximate binary image, and then *k*-out-of-*n* visual cryptography was implemented to the approximate binary image. In [5], Chang and Yu introduced a sharing method hided gray-level secret image into color sharing images. Furthermore, Chang et al. adopted voting strategies to modify the previous method in [6]. The major contribution of this method is to improve quality of reconstructed grayscale image. In [7], Katta proposed a visual image sharing method applied to grayscale image, which is a probabilistic 2-out-of-3 sharing method. Kandar and Maiti introduced a *k*-out-of-*n* secret sharing method for color image [8], which utilized random number generator to yield sharing images. During decryption process, the bitwise OR operator was performed to pixels of sharing images in order to reconstruct secret image. The integration of color halftoning and *k*-out-of-*n* visual cryptography was presented in [9]. Rao et al.'s method generated meaningful sharing images which hide color secret image.

In this work, two issues are considered in the development of grayscale and color image sharing schemes: physical realization and size of sharing image. Naor and Shamir's method [1, 2] can print sharing images on transparencies, then the transparencies are superposed together to reveal secret. Therefore, the conventional *k*-out-of-*n* visual cryptography can be realized on physical medium. Review to [3-9], these methods were performed by arithmetic operation, but cannot be realized on physical medium. The issue of image size expanding is unavoidable due to visual cryptography method employed crypto-array to generate sharing images. The size of sharing image is depended on that of crypto-array.

In this paper, we propose an image sharing scheme, which is capable of performing on grayscale and color images. The overall effects of the proposed method are the achievements of controllable transparency of secret image and unexpanded size of sharing images. The controllable transparency image sharing scheme is realized based on the principle of penetrability. While light passes through a medium, medium declines illumination of light. We treat pixel as medium and adjust pixels' value of multiple sharing images, so that transparency of decrypted-secret image is controllable. Furthermore, the proposed method can be realized on physical medium. Table I lists the comparisons of the six existing methods and the proposed scheme. The single-bit means sharing image consists of 1-bit pixels; the multi-bit means pixels of sharing image are larger than or equal to 2 bits. The rest of this paper is organized as follows: the controllable transparency image sharing scheme for grayscale image and color image will be introduced in Sections II and III, respectively. Experiment results will be shown in Section IV, and the concluding remarks will be drawn in Section V.

II. CONTROLLABLE TRANSPARENCY IMAGE SHARING

The controllable transparency image sharing (CTIS) scheme is realized based on the principle of penetrability. While light penetrates through a medium, it declines illumination of light. A medium carried low rate of penetration is more serious than one carried high rate of penetration in illumination declining. In this work, we treat pixel as medium. White pixel consists of none of ink/powder in printing system, therefore, it carries high rate of penetration. In contrast, black pixel carries low one. Fig.1 depicts illumination declining of light penetrated through two media with different rates of penetration. Let $\mathbf{M}_1$ and $\mathbf{M}_2$ be the first medium and the second medium carried the rates of penetration r_1 and r_2, respectively. Assume that the denotation I represents

TABLE I
COMPARISONS OF THE SIX EXISTING METHODS AND THE PROPOSED SCHEME

	[4]	[5]	[6]	[7]	[8]	[9]	Ours
Grayscale	√	√	√	√			√
Color					√	√	√
Single-bit		√	√	√	√	√	
Multi-bit (bit)	√ (2)						√ (8)
Size Expanding	√	√		√		√	
Physical Medium							√
Operation	OR	XOR	XOR	OR	OR	XOR	Multiplication

the initial light illumination. After light penetrates through two media, the light illumination is declined as,

$$I' = I \times r_1 \times r_2 , \tag{1}$$

where I' denotes the declined illumination of light, and $0 \le r_1, r_2 \le 1$.

In our study, light penetrates two or more sharing pixels for revealing hidden secret image. According to the above hypothesis, we define p_1 and p_2 as the pixel values of the first and the second sharing images, respectively. The rate of penetration is depended on pixel value, which is given by,

$$r_1 = \frac{p_1}{255}, \text{ and } r_2 = \frac{p_2}{255}, \tag{2}$$

where $p_1, p_2 \in \{0, 1, ..., 255\}$. The pixel value of secret image (p_s) is defined as the following equation,

$$\begin{aligned} \alpha \times p_s &= I_{\text{init}} \times r_1 \times r_2 \\ &= \frac{p_1 \times p_2}{255} \end{aligned}, \tag{3}$$

where I_{init} denotes the initial light illumination, and I_{init} is set 255 in all of our experiments. The variable α is a factor to control transparency of secret image, where $0 < \alpha \le \frac{255}{\max(I_{\text{init}})}$ and $\max(I_{\text{init}})$ denotes the maximum pixel value of I_{init}. We can adjust α to achieve transparency controlling.

In the beginning of the CTIS scheme, we have a grayscale secret image of sized $w \times h$. Analyze (3), p_s is a given pixel value, but p_1 and p_2 are two unknown pixel values. We will find the proper p_1 and p_2, so that the estimated pixel value of secret image (p'_s, where $p'_s = p_1 \times p_2/255$) approximates to $\alpha \times p_s$. The limitation of p_1 and p_2 is that those pixel values must be larger than or equal to $\alpha \times p_s$. If one of two sharing pixel values is smaller than $\alpha \times p_s$, it results in the other pixel value is larger than 255, which contradicts to (2). The procedure of the CTIS scheme is described as below,

Step 1. Set the transparency factor α, where $0 < \alpha \le 1$.

Step 2. Input a pixel value of secret image p_s.

Step 3. Yield a random integer p_1 which ranges from $\alpha \times p_s$ and 255. Hence, the pixel of the second sharing image is given by,

$$p_2 = round\left(\frac{\alpha \times p_s \times 255}{p_1}\right), \tag{4}$$

where the function $round(x)$ rounds the variable x to the nearest integer.

Step 4. Yield a random number R and $0 \le R \le 1$. If the number R is smaller than 0.5, we swap p_1 and p_2 to each other. Otherwise, p_1 and p_2 are unaltered.

Step 5. Repeat the steps 2 to 4 until all pixels of sharing image are estimated completely.

The CTIS scheme can be further performed on sharing image to generate another two new sharing images. Therefore, the number of sharing images is flexible. In the step 4, the objective of pixel swapping is for improving security of sharing images. For example, Fig.2(a) shows the secret image and the two sharing images. It is obvious that the second sharing image is similar to the secret image. After implementing pixel swapping, the problem has been solved. Swapping pixel randomly, it disintegrates similar structure between a pixel and its neighbor ones. During decryption process, secret image is decrypted by manipulating all sharing images using (3).

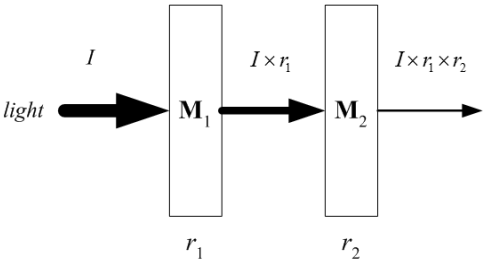

Fig.1. Illumination declining of light penetrated through two media with different rates of penetration

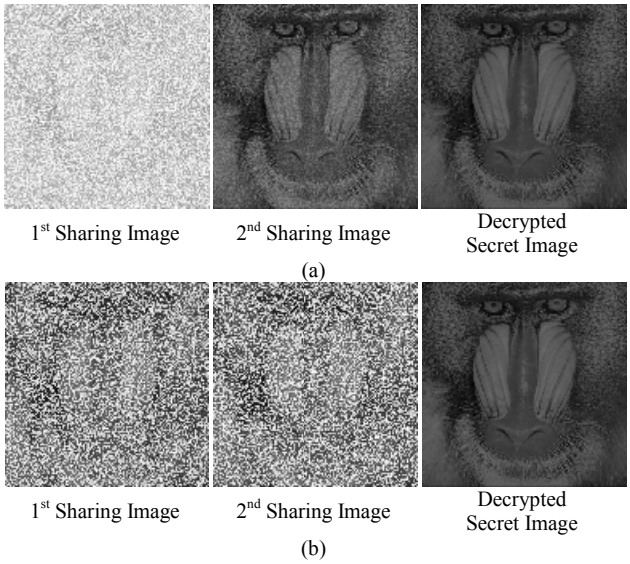

Fig.2. Experiments of image sharing (a) without using pixel swapping, and (b) by using pixel swapping.

III. CONTROLLABLE TRANSPARENCY COLOR IMAGE SHARING

The CTIS scheme is only applied to grayscale image (or called luminance component). In order to increase the applicability of the CTIS scheme, we further propose the controllable transparency color image sharing (CTCIS) scheme. The CTCIS scheme is realized based on not only the principle of

penetrability but also principle of color mixing. We transform a color image from RGB colorspace to HSL colorspace. Subsequently, the CTIS scheme is applied to luminance component, and the color mixing is performed to hue component. Saturation component is unaltered. Consequently, the encrypted hue, the encrypted luminance and the saturation are combined together and transformed to RGB colorspace.

Fig.3 is a hue disk and depicts arrangement to all colors. We assume that a hue is the mixture of two neighboring hues. For example, red is the mixture of magenta and yellow. The denotation h_s and h_i are, respectively, the hues of the secret pixel and the i-th sharing pixel, where $i \in \{1, 2\}$. In addition, the hue difference between the secret pixel and the sharing pixel is defined as θ. h_s can be generated by mixing h_1 and h_2. The procedures of color mixing are described as follows:

Step 1. Input a pixel p_s of secret image, which is transformed from RGB colorspace to HSL colorspace. Let h_s, s_s, and l_s be the hue, the saturation, and the luminance of p_s, where $0° \le h_s < 360°$.

Step 2. Select a random number θ, where $0° \le \theta < 90°$

Step 3. Computer hues of two sharing pixels, which are expressed as follows:

$$h_1 = \mathrm{mod}(h_s - \theta, 360), \text{ and}$$
$$h_2 = \mathrm{mod}(h_s + \theta, 360), \quad (5)$$

where the function mod(x,y) gives the modulus of x divided by y.

Step 4. Repeat the steps 1 to 3 until hues of all sharing pixels are estimated completely.

After implementing the CTCIS scheme, the hue components of two sharing images are obtained. The luminance component of secret image is encrypted by using the CTIS scheme, and the luminance components of two sharing images are generated. In this work, we set that the saturations of two sharing images are the same as that of secret image. Consequently, two sharing images are yielded by transforming HSL colorspace to RGB colorspace.

In the decryption process, we extract the hue and the luminance components of two sharing images. The luminance of secret pixel is computed by manipulating the luminance of two sharing pixels using (3). The hue of secret pixel is computed by,

$$h_s = \begin{cases} \frac{h_1+h_2}{2}, & \text{if } (h_2 - h_1) < 180° \\ \frac{h_1+h_2}{2} - 180°, & \text{otherwise} \end{cases} \quad (6)$$

where h_1 and h_2 are, respectively, the hues of two sharing pixels, and $h_2 \ge h_1$. The saturation of secret image is the same as that of sharing image. Therefore, the secret image is decrypted by transforming HSL colorspace to RGB colorspace.

IV. The Experiment Results

A. Grayscale Image Sharing

We implemented the CTIS scheme for grayscale image. A grayscale secret image of sized 256×256 is shown in Fig.4(a). The control factor was set α=0.5. Figs.4(c) and 4(d) show the two sharing images of sized 256×256 derived from Fig.4(a). Finally, the decrypted secret image is shown in Fig.4(b). Two quantitative measures, namely peak signal-to-noise ratio (PSNR) and structure similarity (SSIM) index, were used to assess

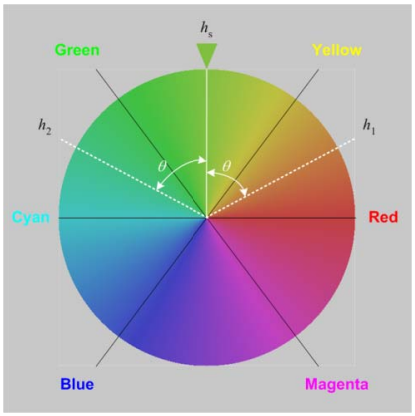

Fig.3. Hue Disc: the hue (denoted as h_s) of secret pixel is mixed by the hues (denotes as h_1 and h_2) of two sharing pixels.

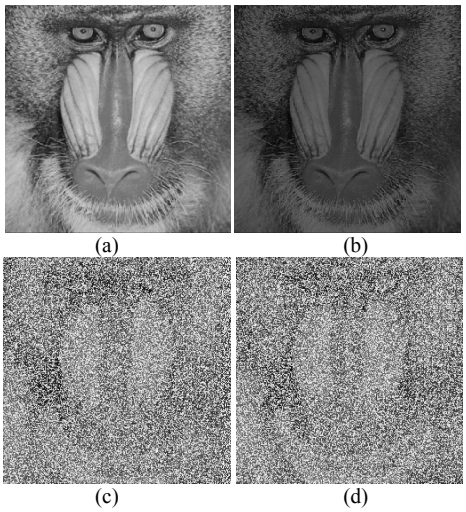

Fig.4. Results of grayscale image sharing: (a) the original image, (b) the decrypted secret image (PSNR=59.98dB, SSIM=0.999), (c) the first sharing image (PSNR=7.75dB, SSIM=0.039), and (d) the second sharing image (PSNR=7.77dB, SSIM=0.039).

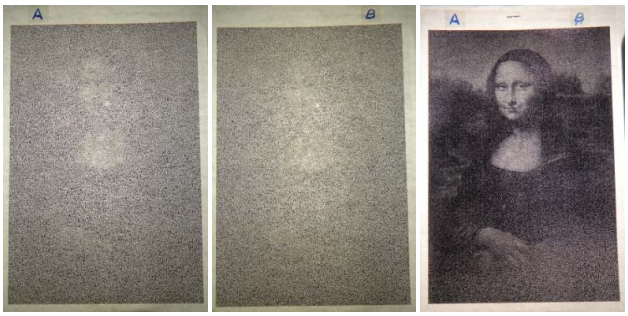

Fig.5. The left and the middle figures are two grayscale sharing images printed on two transparencies. The right figure is the decrypted secret image.

similarities between half-transparency secret image and decrypted secret image, and between half-transparency secret image and sharing images. Hence, the PSNRs of Figs.4(b)-4(d) are 59.98dB, 7.75dB, and 7.77dB. Moreover, the SSIM indices of Figs.4(b)-4(d) are 0.999, 0.039, and 0.039. As we mentioned in the previous section, our scheme can be realized on physical medium. Figs.5(a) and 5(b) are, respectively, the two sharing

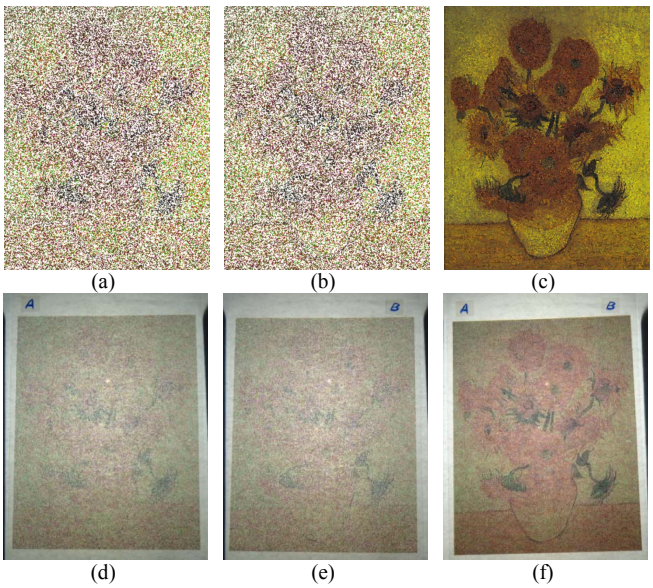

Fig.6. Results of color image sharing: (a) the first sharing image, (b) the second sharing image, and (c) the decrypted secret image. Transparencies of two sharing images are shown in (d) and (e), and (f) is the transparency of the decrypted secret image.

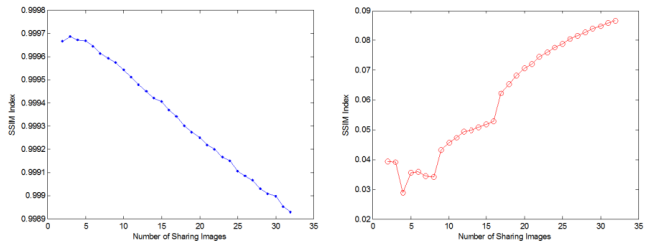

Fig.7. (a) SSIM indices of decrypted secret images and (b) averaged SSIM indices of sharing images against various number of sharing images.

images of The Mona Lisa printed on two transparencies, and the decrypted secret image is shown in Fig.5(c).

B. Color Image Sharing

In the second experiment, the CTCIS scheme was implemented for color image, and it was realized on physical medium as well. We tested the color image of sized 265×342, Sunflowers. The control factor was set α=0.5. In Figs.6(a)-6(c) show two color sharing images and the decrypted secret images. The PSNRs of these images are 6.12dB, 6.11dB, and 33.42dB, and the average SSIM values of these images are 0.043, 0.040, and 0.944. Figs.6(d)-6(f) are the transparencies of two color sharing images and the decrypted secret image.

C. Characteristics of Controllable Transparency Image Sharing

Two issues were presented for performance evaluation: image quality and security under the situations of various numbers of sharing images. For image quality, we used SSIM index to assess similarity between original and decrypted secret images. Fig.7(a) illustrates the quality curve of decrypted secret images against various numbers of sharing images. The SSIM index is decreased while the number of sharing image is increased. The function of (4) is to compute sharing image. The rounding operation in (4) truncates pixels' value as well as degrades quality of decrypted secret image. While number of sharing image is increased, in other words, number of rounding operation is increased. Consequently, quality of decrypted secret image is inversely proportioned to number of sharing images.

The other issue is security to sharing image. The SSIM index was employed to assess similarity between secret image and sharing image. Small SSIM index represents two images are dissimilar to each other. Fig.7(b) illustrates averaged SSIM indices of sharing images against various number of sharing images, and SSIM indices are smaller than 0.09. It means sharing image is dissimilar to secret image. Therefore, the CTIS scheme is secure in this work.

V. CONCLUSION

The contributions of this paper have two: the first one is that we proposed a controllable transparency image sharing scheme for grayscale and color images. The other one is that our method can be realized on physical medium. The experiment results demonstrate that quality of decrypted secret image is inversely proportioned to number of sharing images, and the SSIM indices of decrypted secret images are over 0.99. Furthermore, the averaged SSIM indices of sharing images are smaller than 0.09, it means sharing image is dissimilar to secret image. In other words, the CTIS scheme is secure in this work.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," *Eurocrypt'94*, *Lecture Notes in Computer Science*, vol.950, pp.1-12, Springer-Verlag, 1994.

[2] M. Naor and A. Shamir, "Visual cryptography II: improving the contrast via the cover base," *in Proc. of the Int'l Workshop on Security Protocols*, Springer-Verlag, pp.69-74, 1997.

[3] C. Blude, A. D. Santis, and M. Naor, "Visual cryptography for grey level images," *Information Processing Letters*, vol.75, pp. 255-259, 2000.

[4] C.-C. Lin and W.-H. Tsai, "Visual cryptography for gray-level images by dithering techniques," *Pattern Recognition Letters*, vol.24, pp.349-358, 2003.

[5] C.-C. Chang, and Tai-Xing Yu, "Sharing a secret gray image in multiple images," First Int'l Symp. on Cyber World, pp.230-237, 2002.

[6] C.-C. Chang, C.-C. Lin, T. H. N. Le, and H. B. Le, "A probabilistic visual secret sharing scheme for grayscale images with voting strategy," *Int'l Journal of Intelligent Information Technology Application*, vol.1, no.1, pp.1-9, 2008.

[7] S. Katta, "Visual secret sharing scheme using grayscale images," pp.1-6, 2011. http://arxiv.org/ftp/arxiv/papers/1106/1106.6242.pdf

[8] S. Kandar, and A. Maiti, "K-n secret sharing visual cryptography scheme for color image using random number," *Int'l Journal of Engineering Science and Technology*, vol.3, no.3, pp.1851-1857,May 2011.

[9] B. S. Rao, C. S. Rao, P. Divya, S. M. Riyazoddin, "Analysis of secret sharing & review on extended visual cryptography scheme," *Int'l Journal of Emerging Trends & Technology in Computer Science*, vol.1, no.1, pp.90-95, May-June, 2012.