Enhancing Image Quality in Visual Cryptography with Colors

Chun-Yuan Hsiao
Department of Computer Science and Information Engineering
National Kaohsiung University of Applied Sciences
Kaohsiung, Taiwan
cyhsiao@cc.kuas.edu.tw

Hao-Ji Wang
Department of Computer Science and Information Engineering
National Kaohsiung University of Applied Sciences
Kaohsiung, Taiwan
1099308110@cc.kuas.edu.tw

Abstract—**The notion of Visual Cryptography was first introduced by Naor and Shamir in 1994 [NS94]. Here "visual" means that the decryption is done by human eyes instead of by any computing devices. To retrieve the ciphertext, simply stack the encrypted images together. In fact, it is more like an image secret sharing scheme than an encryption scheme. Both the secret and the shares are black-and-white pictures, and the shares are drawn on transparent slides to be later stacked together.**

The shares of the original Naor and Shamir scheme [NS94] are random black-and-white pixels--meaningless images. Chiu [C02] proposed a scheme where shares can be any (meaningful) pictures. Unfortunately, its reconstructed image (stacked share images) is not as clear. To improve the reconstructed image quality, we adopt the color model proposed by De Prisco and De Santis [DD11]. Our input secret image is still black-and-white, but we inject color pixels into the share images. The reconstructed image contains color pixels but looks much more alike to the input black-and-white secret image. The technical difficulty of this work is how and where to inject the color pixels so that both the share and the reconstructed images have high quality.

Keywords- visual cryptography, secret-sharing scheme.

I. INTRODUCTION

The notion of Visual Cryptography was first introduced by Naor and Shamir in 1994 [NS94]. Here "visual" means that the decryption is done by human eyes instead of by any computing devices. To retrieve the ciphertext, simply stack the encrypted images together. In fact, it is more like an image secret sharing scheme than an encryption scheme. Both the secret and the shares are black-and-white pictures, and the shares are drawn on transparent slides to be later stacked together.

One of the biggest disadvantages of the original Naor and Shamir scheme [NS94] is that the reconstructed image (stacked share image) is, either horizontally or vertically, twice as big as the input secret image. Several subsequent works [ABDS96, ABDS02, KT99, C02] fixed this problem. Another property of the scheme is that the shares are random black-and-white pixels--meaningless images. This provides perfect secrecy for the secret image, but eavesdroppers know something valuable is hidden inside. A steganography approach would hide the secret inside "innocent" share images (by innocent we mean ordinary meaningful images). Ateniese et al. [ABDS96] and Chiu [C02] proposed schemes not only maintain the reconstructed (secret) image size, but also use ordinary meaningful images as share images. Unfortunately, the reconstructed image of Chiu's scheme does not have satisfying quality. More precisely, the reconstructed image can be quite different from the input secret image. See figure 1.

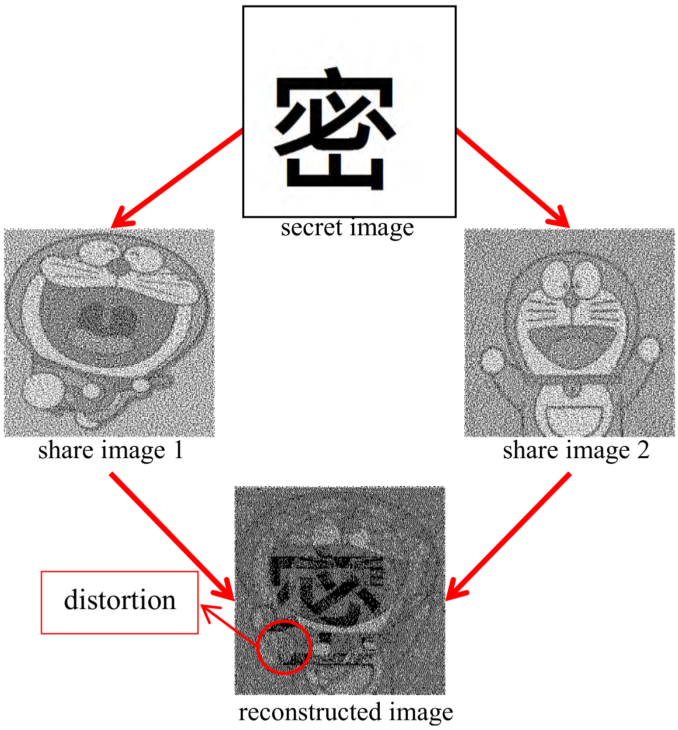

Figure 1

De Prisco and De Santis [DD11] proposed a color model that uses random colored share images to hide black-and-white secret. Their scheme maintains the reconstructed (secret) image size. They also proved lower bounds for general colored (n, t)-threshold image secret sharing schemes. However, in De Prisco and De Santis scheme, the share images are random (meaningless) color images.

In this paper, we greatly improve the image quality of the reconstructed image of Chiu's scheme [C02] by using the color model of De Prisco and De Santis [DD11]. See figure 2. Our input secret image is still black-and-white, but we inject color pixels into the share images. The reconstructed image contains color pixels but looks much more alike to the input black-and-white secret image. The reconstructed image also has the same size as the input secret image. The technical difficulty of this work is how and where to inject the color pixels so that both the shares and the reconstructed images have high quality.

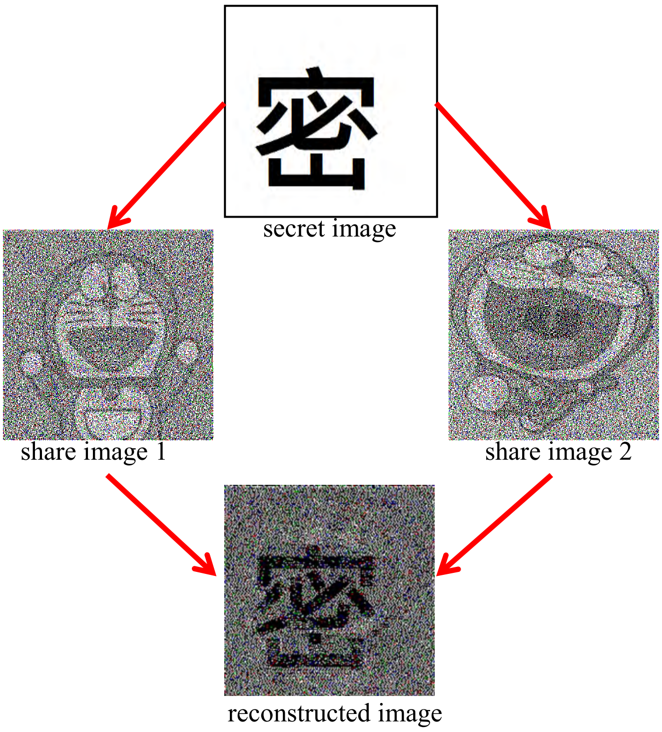

Figure 2

II. RELATED WORK

A. Half-Tone(see [GW02])

In Chiu's scheme [C02] and in ours, color images are turned into grayscale first, and then into half-tone. Both the secret image and share images are in half-tone. The pixel value in grayscale ranges from 0 (black) to 255 (white). But in half-tone, the pixel value is either 0 or 255. We can control the density of the black pixels in the half-tone images to approximate grayscale ones; the denser the darker.

B. Chiu's Scheme [C02]

The share images of the original Naor and Shamir scheme [NS94] consist of random black-and-white pixels, i.e., they are meaningless images. Ateniese et al. [ABDS96] and Chiu [C02] showed how to use ordinary meaningful images as share images. We briefly explain Chiu's scheme here. First, transform both secret image and share images into half-tone. Divide all the half-tone images into 2-by-2-pixel blocks. Then for each block in the share images, permute the pixels so that the corresponding block in the reconstructed image (stacked share images) best matches that in secret image.

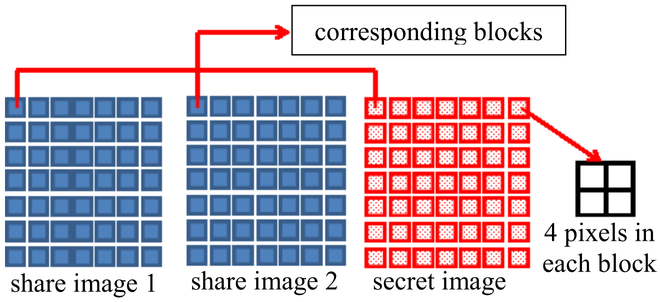

Figure 3.

C. De Prisco and De Santis Scheme [DD11]

In the original Naor and Shamir scheme [NS94] and in most of the subsequent works, both the secret image and the share images are black-and-white. De Prisand and De Santis [DD11] first proposed a color model that hide black-and-white secret image into color share images. Their main goal is to keep the expansion factor low (ideally 1, and 2 in [NS94]) in the (n,t)-threshold image secret-sharing scheme, so that the reconstructed image does not expand too much. Here n represents the number of share images and t represents the threshold (stacking t or more share images reveals the secret). In this paper, we adopt their color model: using color pixels in share images to hide black-and-white secret. However, we only consider n = t = 2. The reason why we choose this model is a property that used implicitly in [DD11]. In this model, stacking two color pixels can produce a black one, so color pixels can be used as black ones. On the other hand, color pixels adjacent to black ones look like white ones to human eyes, if the black pixels form the secret as in our case. So color pixels can also be used as white ones. See Section III for more details.

III. OUR METHOD

Our method is based on Chiu's scheme [C02], but we inject color pixels into (originally black-and-white) share images. However, unlike the color model of De Prisco and De Santis [DD11] where the share images consist of entirely color pixels, our share images consist of mainly black and white ones, with relatively few color ones. These relatively few color pixels do not change the share images too much, to the human eyes, i.e., they look like white ones, but when two different colors stack, they produce black pixels. This solves the problem in Chiu's scheme [C02] that shortage of black pixels in the share images cannot produce desired reconstructed secret (usually represented by black pixels), see Figure 1 in Section 1. Our scheme consists of the following steps.

Step 1:
Transform both secret images and share images into half-tone with appropriate darkness, i.e., the black-pixel density of the secret image should be roughly equal to the sum of the densities of the share images.

Step 2:
For each 2-by-2-pixel block, randomly pick one pixel (out of four). If it's white, make it colored with probability 60%; if it's black, do nothing. The intuition is that if the block has fewer black pixels, it is more likely that the reconstructed (stacked) image does not match the secret image. Notice that this step is global (for each block) instead of local (for those non-matching blocks). This is because locally injecting color pixels into the share images can leak partial information of the secret image.

Step 3:
For each block, we choose the best permutation (there are 24) according to the following scoring system:

■ :black □ :white ▤ :color ("white + black = black" is omitted)

reconstructed image pixel	secret image pixel ■	secret image pixel □
black + black = black	10	0
black + white = black	10	0
black + color = black	10	0
white + white = white	0	10
white + color = color	5	5
color + color = color	20	10

If we were to stack two color pixels and produce a black one (20 points), we later set the pixels in the share images to different colors, e.g., one red and one green. If we were to stack two color pixels and produce a white one (10 points), we later set the pixels in the share images to the same color, e.g., both red.

Step 4:
In step 2 we globally inject color pixels, but sometimes this does not produce enough black pixels in the reconstructed image. So in this step we inject few more according to the following threshold rule.

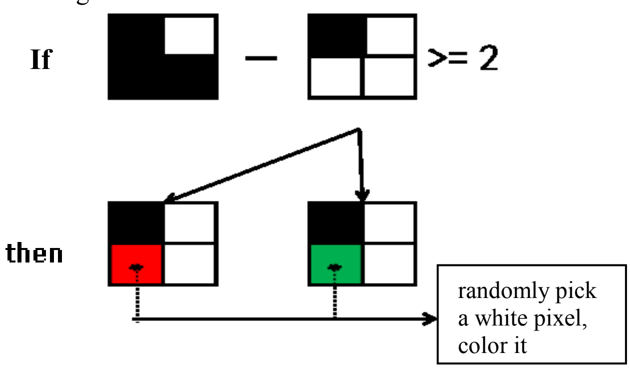

Figure 4. Threshold Rule

IV. EXPERIMENTAL RESULTS

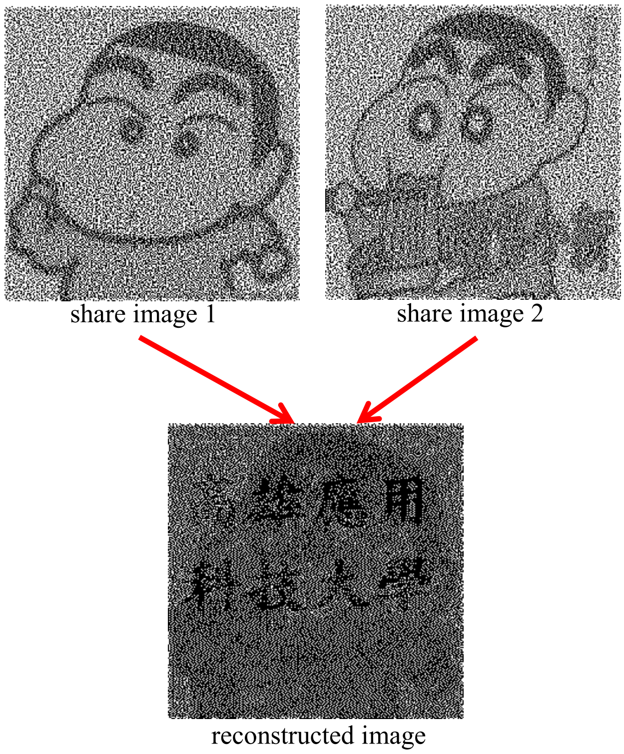

Figure 5. Chiu's method

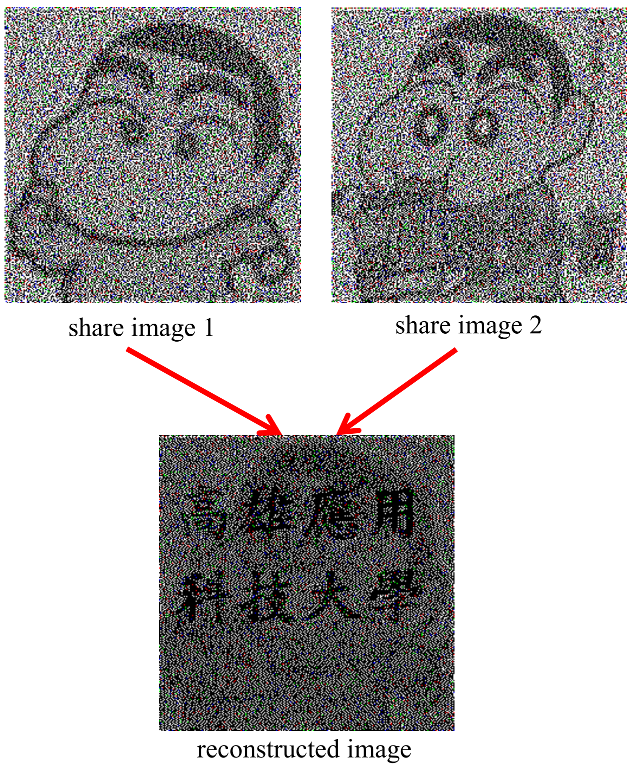

Figure 6. our method

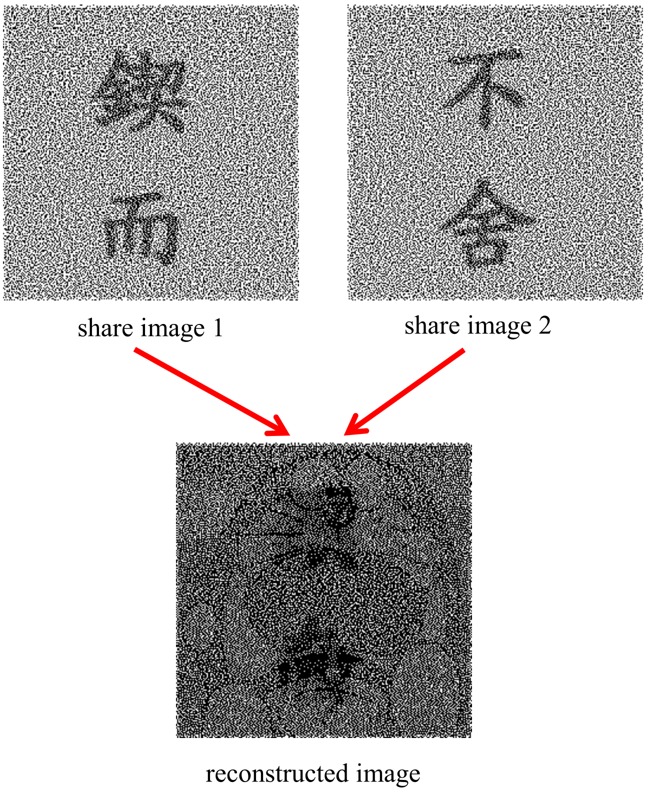

Figure 7. Chiu's method

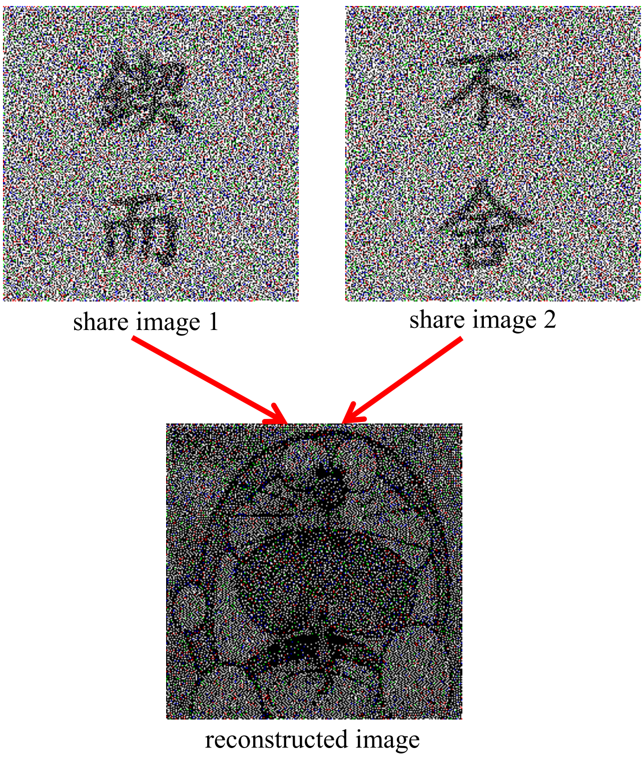

Figure 8. our method

V. CONCLUSIONS

We use the color model of Ateniese et al. [DD11] to improve the image quality of the reconstructed image of Chiu's image secret sharing scheme [C02]. The intuition behind is that a color pixel can be used either as a white or black one, thus solving the problem that the share images do not produce (when stacked) enough black pixels for the reconstructed image in [C02]. The technical difficulty of this work is how and where to inject the color pixels so that both the shares and the reconstructed images have high quality, as described in Section III, step 2 and step 4.

REFERENCES

[ABDS96] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis and Douglas R. Stinson, "Extended Schemes for Visual Cryptography," Theoretical Computer Science, 1996.

[ABDS01] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis and Douglas R. Stinson, "Extended Capabilities for Visual Cryptography," Theoretical Computer Science Vol. 250, 143-161, 2001.

[C02] Wen-Yi Chiu, "On Applying Image Processing and Genetic Algorithms to Visual Cryptography," National Chung Hsing University, Master's Thesis, 2002. (Chinese version.)

[DD11] Roberto De Prisco and Alfredo De Santis, "Using Colors to Improve Visual Cryptography for Black and White Images," ICITS 2011, LNCS 6673, pp. 182-201, 2011.

[GW02] R.C. Gonzalez and R. E. Woods, *Digital Image Processing,* 2nd Edition ,Prentice Hall; ISBN:0130946508.

[KT99] R. Ito H.Kuwakado and H. Tanaka, "Image Size Invariant Visual Cryptography," *IEICE Trans. Fundamentals*, Vol. E82-A, No.10, 1999.

[NS94] Moni Naor and Adi Shamir, "Visual Cryptography," *Advances in Cryptography-EUROCRYPT'94*, pp.1-12, 1994.