A Leakage Suppressed Two-level Security Visual Secret Sharing Scheme

Shenchuan LIU, Masaaki FUJIYOSHI, and Hitoshi KIYA
Tokyo Metropolitan University, Hino, Tokyo 191–0065, Japan
E-mail: liu-shenchuan@sd.tmu.ac.jp, mfujiyoshi@ieee.org, kiya@sd.tmu.ac.jp Tel: +81–42–585–8454

***Abstract*—This paper proposes a new scheme of visual secret sharing which serves two-level security for color images. The proposed scheme splits a secret color image into four pieces referred to as shares; a black-and-white mask share and three color component shares, namely, red, green, and blue. All shares in this scheme are random binary images and each share is delivered to a different user to keep the image secret. In the scheme, the secrecy of the image can remain intact even three color component shares are gathered, that is, two-level security is served. The conventional scheme having the above mentioned features has the risk of information leakage even without the mask share. In contrast, the proposed scheme suppresses the possibility of information leakage in exchange for introducing low contrast recovered images.**

***Index Terms*—Access control, Cryptography, Image Processing**

I. Introduction

In recent years, powerful computers offer even ordinary users the encryption of secret information. To encrypt and decrypt secret information, a key (or a key pair) is used and should be securely and safely guarded. This straightforward key protection, however, still has the risk of key loss and leakage. On the other hand, with the development of fast network technologies, many people collaborate on secret projects over the public Internet. Information should be secret even a few member collude to leak the secret information. To overcome such situations, secret sharing (SS) has been proposed [1].

A SS scheme [1] divides a secret into n pieces referred to as *share*s. n shares are held by n different parties and the secret is recovered if and only if k or more shares are gathered. This scheme is called as a (k,n)-threshold SS scheme. For images, a visual SS (VSS) scheme which divides a secret binary image into random binary shares has been firstly proposed [2]. As the successor, a scheme which uses meaningful structure instead of random shares [3], a scheme for multiple secret images [4], and a scheme for grayscale images [5] have been proposed.

For color images, several VSS schemes have been proposed [6]–[8]. The first color VSS scheme divides a secret color image to four shares; a black-white mask and three color component shares [8]. This structure of shares makes this scheme capable of offering two-level security. That is, the secret image will remain confidential, even all three color shares are gathered to reveal the secret image. In other words, to serve two-level security, stacking three color component shares should not leak any information except the image size.

A literature found that the above mentioned color VSS scheme serving two-level security has the possibility to leak the secret image even without the mask [9]. The conventional scheme [8] supports two-level security control only if the original secret image contains colors chosen from a specific set of colors. It was shown that an adversary will be able to recover the secret image with high probability [9].

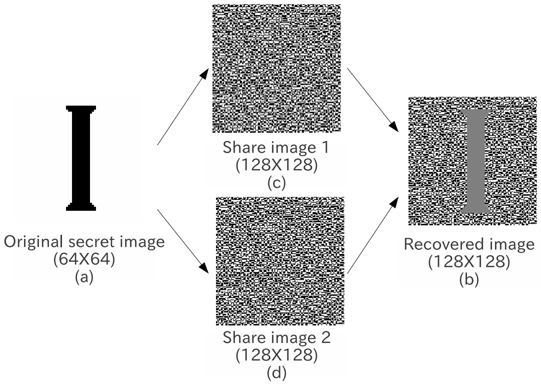


Fig. 1. An example of the first and fundamental visual secret sharing scheme [2]. All two shares are required to recover the secret image in this example; $(2,2)$-threshold implementation.

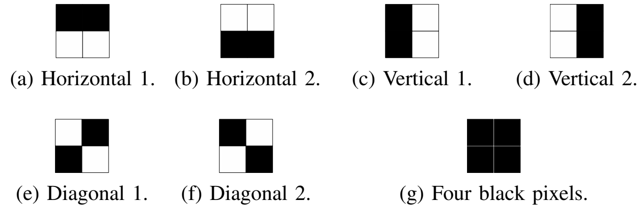
This paper proposes a new VSS scheme serving two-level security for a color image. The proposed scheme splits a color image into black-white mask share and three color component shares as well as the conventional scheme [8]. Introducing a restriction into the rule for generating shares and a contrast degradation into recovered images, the randomness of shares are improved. This feature makes the proposed scheme robust, i.e., the proposed scheme suppresses the information leakage.

In section II, the fundamental VSS scheme [2] and the two-level security VSS scheme for color images [8] are reviewed, and the analysis of the latter scheme [9] is given. A new two-level security VSS scheme for color images is proposed in section III. Experimental results and conclusion are drawn in sections IV and V, respectively.

II. Conventional Visual Secret Sharing Schemes

A. Fundamental Visual Secret Sharing Scheme

Fig. 1 shows the simplest example of the VSS scheme [2]. In the VSS scheme [2], a secret binary image consisting of black and white pixels is split up to n shares in which all shares are random binary images. When k or more shares printed on transparencies are stacked together, the human eyes can do the decryption for recovering the secret image,



(a) Horizontal 1. (b) Horizontal 2. (c) Vertical 1. (d) Vertical 2.

(e) Diagonal 1. (f) Diagonal 2. (g) Four black pixels.

Fig. 2. Random pads for $(2,2)$-threshold visual secret sharing scheme [2]. (a)-(f) six pads for expanding a pixel in a secret image to a 2×2-sized pixel block in a share. (g) a black pixel in the secret image is represented by a black pixel block in stacked shares, i.e., in the decrypted image.

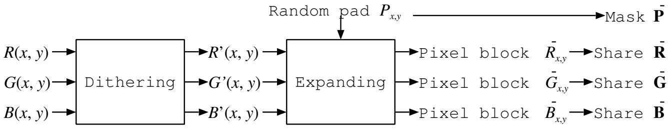


Fig. 3. A conventional visual secret sharing scheme for color images [8]. A dithered pixel in a color component of a secret color image is expanded to a 2×2-sized pixel block by a random pad to generate a share. Used random pads are concatenated to generate a mask.

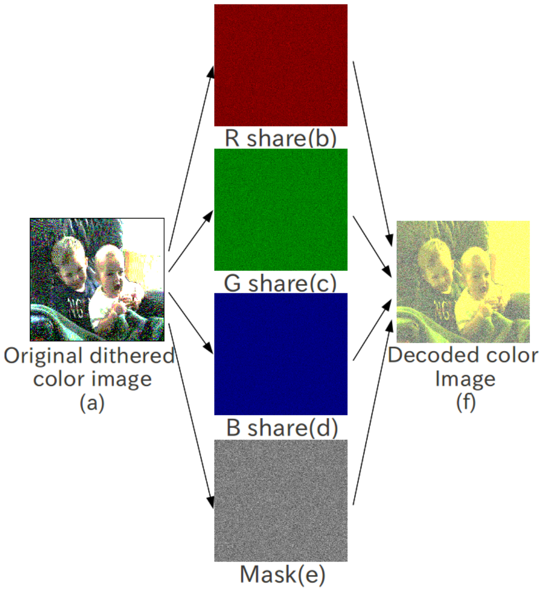


Fig. 4. An example of the conventional visual secret sharing scheme for color images [8] (the dithered image of the original secret image is enlarged four times for display).

whereas the decryption is totally unsuccessful except the size of the secret image if less than k shares are collected and superimposed. This condition is referred to as (k,n)-threshold VSS as well as the ordinary SS [1]. In this scheme, each pixel is handled individually and it should be noted that the white pixel represents the transparent color.

In the $(2,2)$-threshold implementation, i.e., $k=2$ and $n=2$, of the conventional VSS scheme [2], each pixel of a secret binary image is expanded to a 2×2-sized pixel block in share images. To expand a pixel of the secret image, this implementation uses six of 2×2-sized matrices referred to as *random pad*s as shown in Figs. 2; they are horizontal pads (Figs. 2 (a) and (b)), vertical pads (Figs. 2 (c) and (d)), and diagonal pads (Figs. 2 (e) and (f)), i.e., three pad pairs exist.

Two pads are used to generate two shares. When a pixel in the secret binary image is black, one pad pair among three pairs is chosen and a pad and the other are assigned to one share and the other, respectively. On the other hand, if the pixel is white, one pad among six pads is used twice to generate two shares. When the shares are superimposed, the black pixel in the secret image will be represented of a black pixel block as shown in Fig. 2 (g), and the white pixel in the original binary image will be represented of two white and two black pixels as shown in Fig. 2 (a)-(f).

Recall Fig. 1 here. Figure 1 is an example of $(2,2)$-threshold implementation of the conventional VSS scheme [2]. In this example, a 64×64-sized original binary image is expanded to 128×128-sized shares by using six pads shown in Fig. 2, and thus, the recovered image becomes 128×128-sized.

B. Conventional Two-Level Security Visual Secret Sharing Scheme

Figure 3 shows the block diagram of the conventional VSS scheme for color images [8]. This scheme splits a secret color image into four shares; a black-white mask and three color component shares. It is noted that the RGB color model is used in this paper for its simplicity, though this scheme employs the CMYK color model in fact which the CMKY model is useful for printing shares on transparencies.

This scheme firstly divides $X\times Y$-sized original secret color image $\mathbf{f} = \{f(x,y)|f(x,y) = \{R(x,y), G(x,y), B(x,y)\}, 0 \le R(x,y) \le 2^{Q_R}-1, 0 \le G(x,y) \le 2^{Q_G}-1, 0 \le B(x,y) \le 2^{Q_B}-1, 0 \le x \le X-1, 0 \le y \le Y-1\}$ into red ($\mathbf{R} = \{R(x,y)\}$), green ($\mathbf{G} = \{G(x,y)\}$), and blue ($\mathbf{B} = \{B(x,y)\}$) components, where Q_R, Q_G, and Q_B are quantization bits for red, green, and blue components, respectively. Then, components are dithered to generate halftone images $\mathbf{R}' = \{R'(x,y)|R'(x,y) \in \{0,1\}\}$, $\mathbf{G}' = \{G'(x,y)|G'(x,y) \in \{0,1\}\}$, and $\mathbf{B}' = \{B'(x,y)|B'(x,y) \in \{0,1\}\}$, where '0' stands for black. Finally, by using random pads $P_{x,y}$'s where $P_{x,y}$ is one of 2×2-sized pads shown in Figs. 2 (a)-(f), color shares $\bar{\mathbf{R}} = \{\bar{R}_{x,y}\}$, $\bar{\mathbf{G}} = \{\bar{G}_{x,y}\}$, and $\bar{\mathbf{B}} = \{\bar{B}_{x,y}\}$ are generated pixel by pixel where $\bar{R}_{x,y}$, $\bar{G}_{x,y}$, and $\bar{B}_{x,y}$ are 2×2-sized pixel blocks: For the RGB color model,

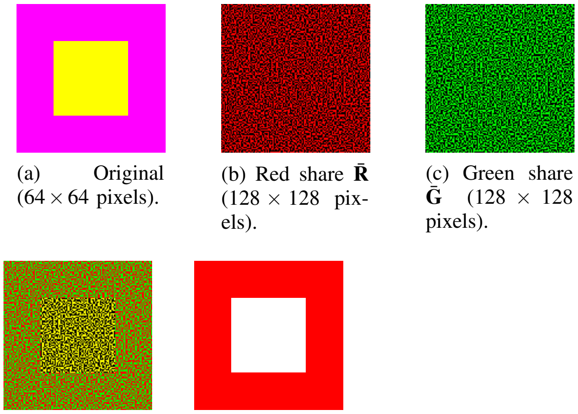
$$\bar{R}_{x,y} = \begin{cases} 1-P_{x,y}, & R'(x,y) = 0 \\ P_{x,y}, & R'(x,y) = 1 \end{cases}, \tag{1}$$

$$\bar{G}_{x,y} = \begin{cases} 1-P_{x,y}, & G'(x,y) = 0 \\ P_{x,y}, & G'(x,y) = 1 \end{cases}, \tag{2}$$

$$\bar{B}_{x,y} = \begin{cases} 1-P_{x,y}, & B'(x,y) = 0 \\ P_{x,y}, & B'(x,y) = 1 \end{cases}. \tag{3}$$

The black-white mask is given as $\bar{\mathbf{P}} = \{P_{x,y}\}$.

Figure 4 shows an example of this scheme. In this example, the size of the original color image is 352×480, so the size of color component shares and the mask are all 704×960. The decrypted image is also four times large than the original



(a) Original (64 × 64 pixels).

(b) Red share $\bar{\mathbf{R}}$ (128 × 128 pixels).

(c) Green share $\bar{\mathbf{G}}$ (128 × 128 pixels).

(d) Superimposition of $\bar{\mathbf{R}}$ and $\bar{\mathbf{G}}$ (128 × 128 pixels).

(e) Recolored image (128 × 128 pixels).

Fig. 5. Revealing the secret image without a mask [9] in the conventional visual secret sharing scheme for color images [8].

secret image in which the red, green, and blue components are given by $\bar{\mathbf{R}} \circ \bar{\mathbf{P}}$, $\bar{\mathbf{G}} \circ \bar{\mathbf{P}}$, and $\bar{\mathbf{B}} \circ \bar{\mathbf{P}}$, respectively, where $\circ$ represents Hadamard production.

It is noteworthy that mask $\bar{\mathbf{P}}$ is considered as the symmetric encryption key in this scheme. In other words, a user can obtains different shares from a secret image by using different $\bar{\mathbf{P}}$. By utilizing this fact, in some applications, the mask may belong to a superordinate and each color share may be held by a subordinate. Even subordinates gather color shares, the secret image is not revealed without the mask. So, this scheme offers two-level security. It is noted that $\bar{\mathbf{P}}$ is common among $\bar{\mathbf{R}}$, $\bar{\mathbf{G}}$, and $\bar{\mathbf{B}}$ as mentioned in Eqs. (1), (2), and (3) in this scheme.

C. Analysis of the Conventional Two-Level Security Visual Secret Sharing Scheme

The above mentioned VSS scheme for color image [8] was analyzed [9], and it was found that in some circumstances, the shape of an original secret image can be recovered from only color shares. The success probability of revealing the shape depends on the number of colors in a dithered secret image and the number of shares an adversary acquires [9], and this section focuses the analysis for the condition that two colors among possible $2^3 = 8$ colors exist in a dithered image and an adversary obtains two color component shares.

Suppose the adversary intercepts the $\bar{\mathbf{R}}$ and $\bar{\mathbf{G}}$ as shown in Figs. 5 (b) and (c) for the secret image shown in Fig. 5 (a). The adversary superimposes the obtained shares as shown as Fig. 5 (d) where the red, green, and blue components are given by $\bar{\mathbf{R}}$, $\bar{\mathbf{G}}$, and an all zero matrix, respectively. If pixel block $\bar{R}_{x,y}$ is identical to $\bar{G}_{x,y}$, the superimposed pixel block consists of two yellow pixels and two black pixels, and if $\bar{R}_{x,y}$ is the compliment of $\bar{G}_{x,y}$, the superimposed pixel block is compounded of two red pixels and two green pixels, as shown in Fig. 5 (d). This fact holds regardless of used pad $P_{x,y}$. Figure 5 (e) is given by filling Fig. 5 (d) with white and red; white for $\bar{R}_{x,y} \neq \bar{G}_{x,y}$ and red for $\bar{R}_{x,y} = \bar{G}_{x,y}$. It is confirmed that the shape of the secret image is completely revealed in Fig. 5 (e) without mask $\bar{\mathbf{P}}$.

TABLE I

Two color groups exist in an image given by superimposing two color shares in the conventional visual secret sharing scheme for color images [8] (red and green shares in this example).

$f'(x,y)$	$\{R'(x,y), G'(x,y), B'(x,y)\}$	$\bar{R}_{x,y}$ and $\bar{G}_{x,y}$
black	$\{0,0,0\}$	identical
blue	$\{0,0,1\}$	identical
yellow	$\{1,1,0\}$	identical
white	$\{1,1,1\}$	identical
green	$\{0,1,0\}$	complementary
cyan	$\{0,1,1\}$	complementary
red	$\{1,0,0\}$	complementary
magenta	$\{1,0,1\}$	complementary

As shown in Eqs. (1) and (2), if dithered pixels $R'(x,y)$ and $G'(x,y)$ are the same, pixel block $\bar{R}_{x,y}$ is identical to $\bar{G}_{x,y}$. On the other hand, if $R'(x,y) \neq G'(x,y)$, $\bar{R}_{x,y}$ is the complementary of $\bar{G}_{x,y}$. When two color shares are superimposed, eight possible colors are grouped into two classes, namely, identical and complementary as listed in Table I. In any of two color shares combination among three color shares, eight colors are classed into identical and supplementary which each consists of four colors similarly to Table I.

In the example described above, the adversary intercepts $\bar{\mathbf{R}}$ and $\bar{\mathbf{G}}$ shown in Figs. 5 (b) and (c). As listed in Table I, magenta and yellow used in the original secret image shown in Fig. 5 (a) belong to different groups. As this example, under the condition that one of two colors used in an original image belongs to the identical group and the other color is simultaneously in the complementary groups, the adversary can reveal the shape of the secret image.

Let E be the event that one color is from the identical group and the other from the complementary group in a two-color original secret image under the condition that two color shares are intercepted. As the cardinality of each groups is four, there are $4 \times 4 = 16$ possible combinations for event E to happen. Since $\binom{8}{2} = 28$ possible combinations for choosing two colors from eight possible colors, the probability of E is

$$Pr[E] = \frac{16}{28} = \frac{4}{7}. \tag{4}$$

In other words, the success probability of an adversary in breaking the first VSS scheme for color images [8] is $4/7$ under the condition that two colors are used in an original secret image and two color shares are intercepted by the adversary.

When all three color shares are intercepted, 8 colors can be divided into 4 groups, {white, balck}, {red, cyan}, {green, magenta} and {yellow, blue}. So, the probability increases to $6/7$ for two-color images, and the probabilities are $4/7$ and $8/35$ for three and four colors in the secret image, respectively [9].

In the next section, the new scheme of VSS which suppresses the above described information leakage is proposed

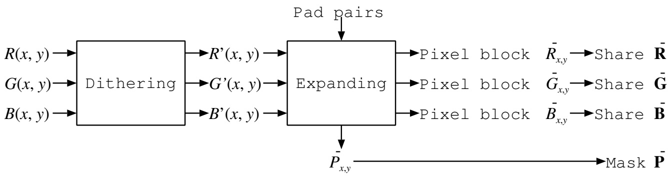


Fig. 6. The proposed scheme.

for color images.

III. Proposed Scheme

A. System Overview

Figure 6 show the proposed scheme. As well as the conventional scheme [8], the proposed scheme transfers a color secret image into four shares pixel by pixel; a black-white mask and red, green, and blue shares. Instead of selecting one random pad among six possible pads randomly for a pixel in the conventional scheme, the proposed scheme uses three different pads for three color components in a pixel. To recover the dithered pixel value, the proposed scheme puts the original state of the pixel in a randomly selected pixel in a 2×2-sized pixel block and the final pad consists of three 0's and one 1 in the proposed scheme.

B. Algorithm

It is assumed $X \times Y$-sized color image $\mathbf{f} = \{f(x,y) | f(x,y) = \{R(x,y), G(x,y), B(x,y)\}, 0 \le R(x,y) \le 2^{Q_R} - 1, 0 \le G(x,y) \le 2^{Q_G} - 1, 0 \le B(x,y) \le 2^{Q_B} - 1, 0 \le x \le X-1, 0 \le y \le Y-1\}$ containing three components $\mathbf{R} = \{R(x,y)\}$, $\mathbf{G} = \{G(x,y)\}$, and $\mathbf{B} = \{B(x,y)\}$ is an original secret image, where quantization bits for components are Q_R, Q_G, and Q_B, respectively. Components $\mathbf{R}$, $\mathbf{G}$, and $\mathbf{B}$ are transferred into halftone images, individually. Let $\mathbf{R}' = \{R'(x,y) | R'(x,y) \in \{0,1\}\}$, $\mathbf{G}' = \{G'(x,y) | G'(x,y) \in \{0,1\}\}$, and $\mathbf{B}' = \{B'(x,y) | B'(x,y) \in \{0,1\}\}$ be the halftone images derived from $\mathbf{R}$, $\mathbf{G}$, and $\mathbf{B}$, respectively, where '0' stands for black.

The following algorithm is applied to each dithered pixel $\mathbf{f}' = \{f'(x,y) | f'(x,y) = \{R'(x,y), G'(x,y), B'(x,y)\}\}$ for generating shares.

Step 1. Randomly assign three pad pairs, namely, the horizontal pair (Figs. 2 (a) and (b)), the vertical pair (Figs. 2 (c) and (d)), and the diagonal pair (Figs. 2 (e) and (f)), to three color components mutually exclusive and collectively exhaustive.

Step 2. Pick a pixel randomly among a 2×2-sized pixel block, and $\bar{P}_{x,y}$ is given as a 2×2-sized matrix consisting of three 0's and one 1 in which 1 is assigned to the position of the chosen pixel.

Step 3. In red component, a pad from the assigned pad pair becomes pixel block $\bar{R}_{x,y}$ in which the position of the above selected pixel in the pad is equal to $R'(x,y)$. The identical rule is applied to green and blue components to generate $\bar{G}_{x,y}$ and $\bar{B}_{x,y}$, respectively.

Gathering pixel blocks to form shares; $\bar{\mathbf{R}} = \{\bar{R}_{x,y}\}$, $\bar{\mathbf{G}} = \{\bar{G}_{x,y}\}$, and $\bar{\mathbf{B}} = \{\bar{B}_{x,y}\}$. Mask is given as $\bar{\mathbf{P}} = \{\bar{P}_{x,y}\}$.

C. Example

A tangible example of the proposed scheme is given here. Let original dithered pixel $f'(x,y)$ is yellow, i.e.

$$R'(x,y) = 1, \tag{5}$$

$$G'(x,y) = 1, \tag{6}$$

$$B'(x,y) = 0. \tag{7}$$

For its simplicity, it is assumed that horizontal, vertical, and diagonal pad pairs are assigned to red, green, blue components, respectively, in step 1. That is,

$$\left\{ \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \right\} \rightarrow \text{ red,} \tag{8}$$

$$\left\{ \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \right\} \rightarrow \text{ green,} \tag{9}$$

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\} \rightarrow \text{ blue.} \tag{10}$$

In step 2, top left pixel is assumed to be chosen among top left, top right, bottom left, and bottom right pixels in a 2×2-sized pixel block. So, $\bar{P}_{x,y}$ is given as

$$\bar{P}_{x,y} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \tag{11}$$

where 0 and 1 are for black and white, respectively.

At step 3, a pad is chosen from the assigned pad pair in each color component based on the color itself and the position of the pixel selected in step 2. That is, the selected pixel is equal to the color itself in the pad. From Eqs. (5), (6), (7), and (11), pixel blocks $\bar{R}_{x,y}$, $\bar{G}_{x,y}$, and $\bar{B}_{x,y}$ are given as

$$\bar{R}_{x,y} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \tag{12}$$

$$\bar{G}_{x,y} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \tag{13}$$

$$\bar{B}_{x,y} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \tag{14}$$

respectively. It is noted that the chosen pixel, the top left, in each pixel block holds the value of the original dithered pixel.

D. Features

The proposed scheme uses three different pads for three color components in a dithered pixel of an original secret image, whereas the conventional scheme [8] uses only one pad for all components as mentioned in section II-B. So, it is difficult for an adversary to grouping pixel blocks in the proposed scheme.

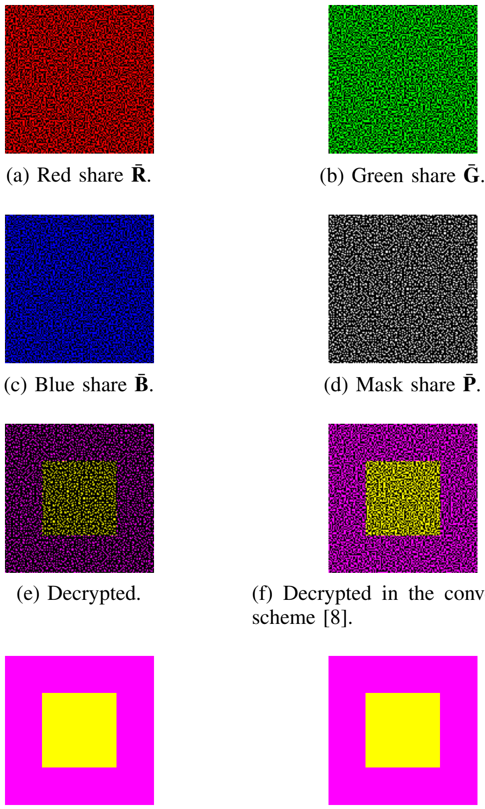
Let one yellow pixel and one magenta pixel similar to Fig. 5 (a) are considered here. It is assumed that an adversary intercepts red and green shares, $\bar{\mathbf{R}}$ and $\bar{\mathbf{G}}$ again, as assumed in section II-C. In the conventional scheme [8], a pixel block consisting of two yellow pixels and two black pixels and a pixel block consisting of two red pixels and two green pixels are easily obtained for the magenta and yellow pixels, by superimposing $\bar{R}_{x,y}$ on $\bar{G}_{x,y}$ as shown in Fig. 5 (d). It is easy for the adversary to distinguish two pixel blocks, and the adversary can recolor the stacked image with two colors as shown in Fig. 5 (e).

From Eqs. (12) and (13), as long as stacking $\bar{\mathbf{R}}$ and $\bar{\mathbf{G}}$, the adversary gets pixel blocks which each block consists of red, green, yellow, and black pixels in the proposed scheme. In the proposed scheme, when 2 color shares are stacked, no matter what color the pixel in the dithered image is, there are 4 colors in each 2×2 block of the stacked image which are impossbile to be grouped. So, the possibility of information leakage is 0, while the conventional schme [8] is $4/7$ [9].

On the other hand, if all three color shares are stacked, eight colors can be divided into two groups in proposed scheme, which are {white, red, green, blue} and {cyan, magenta, yellow, black}. The color of pixel in the dithered image is white, red, green, or blue, the stacked block will consist of white, red, green, and blue pixels. If the color of any pixel in the ditherd image is cyan, magenta, yellow, or black, the stacked block will consist of cyan, magenta, yellow, and black pixels. Because the stacked blocks can be divided into two groups, the possibility of information leakage is $4/7$, whereas the conventional scheme [8] has a possibility of information leakage is $6/7$ [9]. Therefore, the possibility of information leakage is suppressed in the proposed scheme.

As discussed in section II-C, in conventional sheme [8], if three color shares are stacked, eight colors can be divided into four groups. So if the dithered image consists of no more than four colors, it is quite possible to leak information. It is confirmed [9] that the possibility will be $4/7$ or $8/35$, when dithered image consists of three or four colors. On the other hand, if three color shares are stacked, eight colors can only be divided into two groups in the proposed scheme. The proposed scheme generates shares with nearly leakage impossible when the dithered image consists of more than two colors. Consequently, it is difficult for the adversary to distinguish pixel blocks in the proposed scheme, even the dithered image consists of less colors.

The proposed scheme, however, introduces degradation to decrypted images. A pixel block in a decrypted image has two color pixels and two black pixels in the conventional scheme [8] as mentioned in section II-B. In contrast, a pixel block in a decrypted image has one color pixel and three black pixels as final pad $\bar{P}_{x,y}$ is compounded of three 0's and one 1. So decrypted images in the proposed scheme have the disadvantage in terms of contrast. It is noteworthy that resampling pixel blocks to form an image, whose size is the same as the original dithered image, completely recovers the original dithered image in both schemes.



(a) Red share $\bar{\mathbf{R}}$.

(b) Green share $\bar{\mathbf{G}}$.

(c) Blue share $\bar{\mathbf{B}}$.

(d) Mask share $\bar{\mathbf{P}}$.

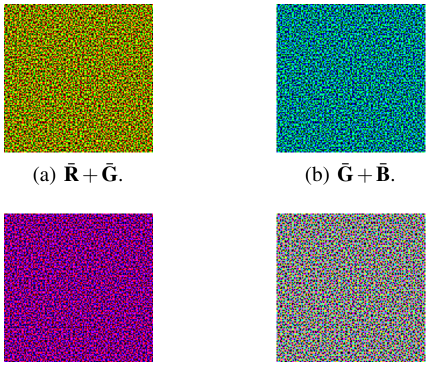
(e) Decrypted.

(f) Decrypted in the conventional scheme [8].

(g) Resample.

(h) Resampled in the conventional scheme [8].

Fig. 7. An example for a two-color image in the proposed scheme. All shares and decrypted images are 128×128-sized. Resampled images are 64×64-sized as well as the original shown in Fig. 5 (a).



(a) $\bar{\mathbf{R}} + \bar{\mathbf{G}}$.

(b) $\bar{\mathbf{G}} + \bar{\mathbf{B}}$.

(c) $\bar{\mathbf{B}} + \bar{\mathbf{R}}$.

(d) $\bar{\mathbf{R}} + \bar{\mathbf{G}} + \bar{\mathbf{B}}$.

Fig. 8. Superimposed images in the proposed scheme for the two-color image shown in Fig. 5 (a). All images are 128×128-sized.

IV. Experimental results

To the image with two colors shown in Fig. 5 (a), the proposed scheme is applied. Figure 7 shows all four shares. All shares are random binary images, and no one can estimate the original image from a share. From Figs. 7 (e) and (f), it is confirmed that the decrypted image of the proposed scheme is darker than that of the conventional scheme [8], as described in section III-D, but resampled images (Figs. 7 (g) and (h)) are the same as the original image (Fig. 5 (a)).

Figure 8 shows three stacked images in which each image is obtained from two shares and one superimposed image generated from all three shares. All pixel blocks in a superimposed image have the same set of colors as described in section III-D. It, thus, an adversary cannot extract the shape of the secret image.

Figure 9 shows (a) a dithered natural color image 'lena', (b) the recolored images superimposed all color shares in the proposed scheme, and (c) in the conventional scheme. As discussed in session II-C, in conventional scheme [8], eight colors can be divided into four groups, {white, black}, {red, cyan}, {green, magenta} and {yellow, blue}. These groups are recolored with white, red, magenta, and yellow, respectively, in Fig. 9 (c). On the other hand, in the proposed scheme, eitht colors can only be divided into two groups, {red, green, blue, white} and {cyan, magenta, yellow, black} as discribed in section III-D. Figure 9 (b) recolors them with white and magenta. It is confirmed that it is more difficult to estimate 'lena' from the Fig. 9 (b) than from Fig. 9 (c). So the leakage of two-level security visual secret sharing scheme is suppressed by the proposed scheme.

V. Conclusions

This paper has proposed a new scheme of color VSS offering two-level security. The proposed scheme reduces the information leakage probability which the conventional scheme [8] has [9], by using three random pads for a pixel instead of one pad, in exchange for an introduction of the contrast degradation to decrypted images.

Suppressing the possibility of information leakage to zero even three color shares are intercepted is one of the future works.

References

[1] A. Shamir, "How to share a secret," *Commun. ACM*, vol.22, pp.612–613, Nov. 1979.

[2] M. Naor and A. Shamir, "Visual cryptography,"in *Proc. IACR EUROCRYPT*, LNCS, vol.950, 1994, pp.1–12.

[3] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, "Extended capabilities for visual cryptography," *Theor. Comput. Sci.*, vol.250, pp.143–161, Jan. 2001.

[4] J. Weir and W. Yan, "Sharing multiple secrets using visual cryptography," in *Proc. IEEE ISCAS*, 2009, pp.509–512.

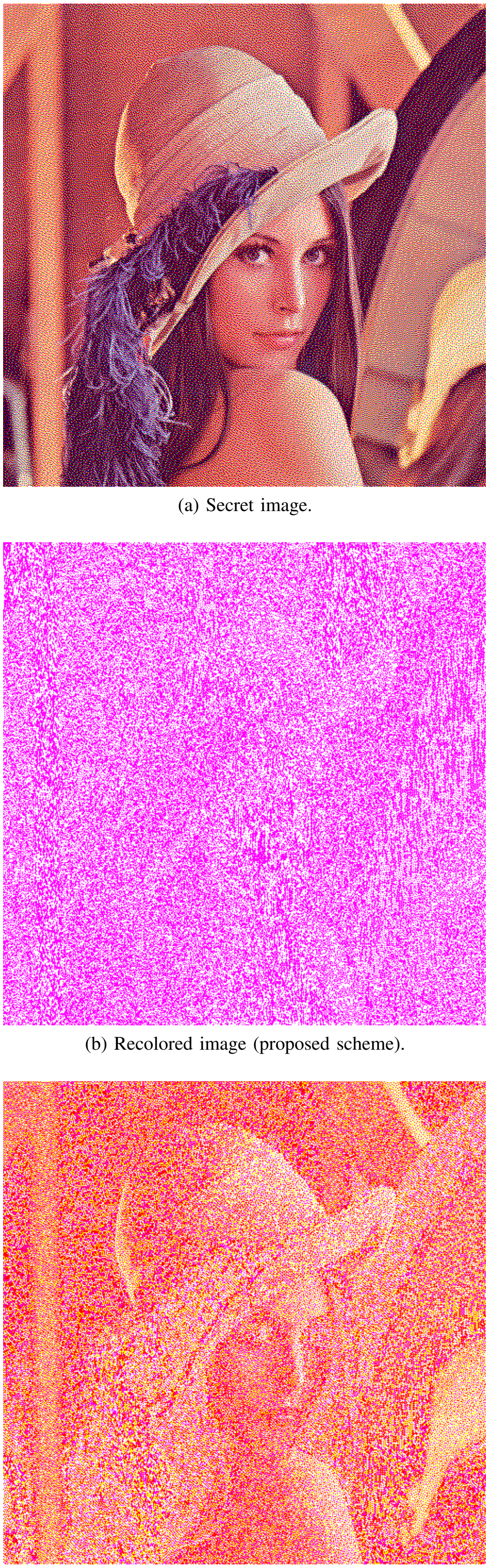
[5] A. Ross and A. Othman, "Visual cryptography for biometric privacy," *IEEE Trans. Inf. Forensics Security*, vol.6, pp.70–81, Mar. 2011.

[6] R. Lukac and K.N. Plataniotis, "Colour image secret sharing," *IEE Electron. Lett.*, vol.40, pp.529–531, Apr. 2004.

[7] D. Jin, W.-Q. Yan, and M.S. Kankanhalli, "Progressive color visual cryptography," *J. Electron. Imag.*, vol.14, Aug. 2005.

[8] Y.C. Hou, "Visual cryptography for color images," *Pattern Recognition*, vol.36, pp.1619–1629, Jul. 2003.

[9] B.W. Leung, F.Y. Ng, and D.S. Wong, "On the security of a visual cryptography scheme for color images," *Pattern Recognition*, vol.42, pp.929–940, May 2009.



(a) Secret image.

(b) Recolored image (proposed scheme).

(c) Recolored image (conventional scheme [8]).

Fig. 9. Experimental results of "Lena".