Multi secret image color visual cryptography schemes for general access structures*

YI Feng, WANG Daoshun**, LUO Ping, HUANG Liansheng and DAI Yiqi

(Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)

Received June 9, 2005; revised September 16, 2005

Abstract In the proposed visual cryptography schemes for general access structures, the single secret image black-and-white visual cryptography schemes with meaningful shares have been constructed, in which the shares are innocent looking images. The meaningful shares have not been realized in single secret image color schemes; neither have the multi secret images color schemes. In this paper, the multi secret images color visual cryptography schemes for general access structures with meaningful shares are constructed by the method of matrix concatenation, the pixel expansion is obtained, and the validity of the scheme is proven. In our scheme, the different combination of meaningful color shares can be used to recover distinct color secret images. The multi secret images black-and-white visual cryptography scheme is a special case of our color scheme.

Keywords: ***visual cryptography, secret sharing scheme, general access structure.***

In 1979, Blakely and Shamir[1,2] independently proposed a secret sharing scheme to construct robust key management scheme. A secret sharing scheme is a method of sharing a secret among a group of participants. Each participant holds a piece of information, called a share concerning the secret. Any least k shares can be used to recover the secret; however, any $k-1$ or less shares are not sufficient to reconstruct any information of the secret image in a (k, n)-threshold scheme. In 1994, Naor and Shamir[3] firstly introduced visual cryptography in Eurocrypt'94" and constructed (k, n)-threshold visual cryptography scheme for a black-and-white secret image (black-and-white (k, n)-VCS, for short). Shares are used by visual cryptography to conceal the original data that can be recovered from the overlap of several modified images through the contrast abilities of human vision. The reconstruction can be performed by the human visual system without any knowledge of cryptography or cryptographic computations. Being easily utilized by common people, the unique attribute of secret images reconstruction has attracted the attention of many researchers.

Verheul and Tilborg[4] studied the black-and-white (k, n)-VCS and improved the definition of Naor and Shamir[3]. Other related researches can be referred to Refs. [5—16]. The concept of Naor and Shamir[3] was extended by Ateniese et al.[17—19], where general techniques can be used to construct visual cryptography schemes for general access structure ($(\Gamma_{Qual}, \Gamma_{Forb})$-VCS, for short), and (n, n)-VCS was obtained, which are optimal with respect to the pixel expansion. Color visual cryptography scheme is another interesting research topic, through which users can share a color secret image. Verheul and Van Tilborg[4] introduced a theoretical construction for a color (k, n)-VCS. Other related researches can be referred to Refs. [20—26].

From the above mentioned studies we know that, in the so far used models of visual cryptography schemes for single secret image, researchers have constructed black-and-white visual cryptography schemes with meaningful shares, including the schemes for general access structures, but in color $(\Gamma_{Qual}, \Gamma_{Forb})$-VCS, meaningful shares have not been obtained. Many factors should be considered to share a color secret image, for instance, color diversification in secret images, color variance of meaningful shares, and distinct content which is correctly displayed in each share. Meanwhile, the pixel expansion, contrast and validity of schemes should also be taken into consideration. Due to the above reasons, single secret image color visual cryptography schemes for general access structures with meaningful shares (color $(\Gamma_{Qual}, \Gamma_{Forb})$-EVCS for short, while EVCS for extended VCS) have not been resolved, neither have the multi

* Supported by National Natural Science Foundation of China (Grant No. 90304014) and the Major State Basic Research Development Program of China (Grant No. 2003CB314805)

** To whom correspondence should be addressed. E-mail: daoshun@mail.tsinghua.edu.cn

secret images color visual cryptography schemes for general access structure with meaningful shares (color (Γ_{Qual}, Γ_{Forb})-MVCS for short, while MVCS for multi secret images VCS).

1 Visual cryptography schemes for general access structures

Our schemes will use the results of previous visual cryptography schemes, so we give a brief review about the related knowledge here.

In black-and-white visual cryptography schemes, we assume that the secret image consists of a collection of black and white pixels. Each pixel appears in n versions called shares, one for each transparency. Each share is a collection of m black and white subpixels, which are printed in so close proximity to each other that the human visual system averages their individual black/white contributions. The set of subpixels can be represented by an $n \times m$ Boolean matrix $\boldsymbol{S} = [s_{ij}]$, where element s_{ij} represents the jth subpixel in the ith share. A white subpixel is represented as 0, and a black subpixel is represented as 1. Therefore, the larger the Hamming weight $H(V)$ of the OR of s rows $r_{i_1}, \cdots, r_{i_s}$ of $\boldsymbol{S}$, the higher the grey level of the combined share, obtained by stacking the transparencies $i_1, \cdots, i_s$ associated with the rows $r_{i_1}, \cdots, r_{i_s}$. This grey level is interpreted by the visual system of the participants as black or as white according to some rule of contrast.

Definition 1.[18] Let (Γ_{Qual}, Γ_{Forb}) be an access structure on a set of n participants. Two collections (multisets) of $n \times m$ Boolean matrices $\boldsymbol{C}_0$ and $\boldsymbol{C}_1$ constitute a (Γ_{Qual}, Γ_{Forb})-VCS if there exist the value $\alpha(m)$ and the set $\{(\boldsymbol{X}, t_{\boldsymbol{X}})\}_{\boldsymbol{X}\in\Gamma_{Qual}}$ satisfying:

(1) Any (qualified) set $\boldsymbol{X} = \{i_1, i_2, \cdots, i_p\} \in \Gamma_{Qual}$ can recover the share by stacking their transparencies. Formally, for any $\boldsymbol{M} \in \boldsymbol{C}_0$, the OR V of rows $i_1, i_2, \cdots, i_p$ satisfies $w(V) \leqslant t_{\boldsymbol{X}} - \alpha(m) \cdot m$; whereas, for any $\boldsymbol{M} \in \boldsymbol{C}_1$, it satisfies $w(V) \geqslant t_{\boldsymbol{X}}$.

(2) Any (forbidden) set $\boldsymbol{X} = \{i_1, i_2, \cdots, i_p\} \in \Gamma_{Forb}$ has no information on the share. Formally, the two collections of $p \times m$ matrices $\boldsymbol{D}_t$ with $t \in \{0, 1\}$, obtained by restricting each $n \times m$ matrix in $\boldsymbol{C}_t$ to rows $i_1, i_2, \cdots, i_p$, are indistinguishable in the sense that they contain the same matrices with the same frequencies.

In this definition, parameter m is called the pixel expansion, which refers to the number of subpixels in a share required to represent a single pixel in the original image. It is desirable to minimize pixel expansion as much as possible. The set $\{t_{\boldsymbol{X}}\}_{\boldsymbol{X}\in\Gamma_0}$ is called the set of thresholds.

According to the definition of black-and-white (Γ_{Qual}, Γ_{Forb})-VCS, the following definition of grey-level (Γ_{Qual}, Γ_{Forb})-VCS is proposed.

Definition 2.[20] Let (Γ_{Qual}, Γ_{Forb}) be an access structure on a set of n participants and let $g \geqslant 2$ be an integer. The g collections (multisets) of $n \times m$ Boolean matrices $\boldsymbol{C}_0, \cdots, \boldsymbol{C}_{g-1}$ constitute a (Γ_{Qual}, Γ_{Forb})-VCS for g grey levels, if there exist the values $\alpha_0, \cdots, \alpha_{g-2}$ and sets $\{(\boldsymbol{X}, t_{i,\boldsymbol{X}})\}_{\boldsymbol{X}\in\Gamma_{Qual}}$ for $i = 0, \cdots, g-2$ satisfying:

(1) Any (qualified) set $\boldsymbol{X} = \{j_1, j_2, \cdots, j_p\} \in \Gamma_{Qual}$ can recover the share by stacking their transparencies. Formally, for $i = 0, \cdots, g-2$ for any $\boldsymbol{M} \in \boldsymbol{C}_i$, the OR V of rows $j_1, j_2, \cdots, j_p$ satisfies $w(V) \leqslant t_{i,\boldsymbol{X}} - \alpha_i \cdot m$; whereas, for any $\boldsymbol{M} \in \boldsymbol{C}_{i+1}$, it results in that $w(V) \geqslant t_{i,\boldsymbol{X}}$.

(2) Any (forbidden) set $\boldsymbol{X} = \{j_1, j_2, \cdots, j_p\} \in \Gamma_{Forb}$ has no information on the share. Formally, the g collections of $p \times m$ matrices $\boldsymbol{D}_i$, with $i = 0, \cdots, g-1$, obtained by restricting each $n \times m$ matrix in $\boldsymbol{C}_i$ to rows $j_1, j_2, \cdots, j_p$, are indistinguishable in the sense that they contain the same matrices with the same frequencies.

To share a pixel with the lth grey level, the dealer randomly chooses one of the matrices in $\boldsymbol{C}_l$, and distributes the ith row to the participant i. Thus, the chosen matrix defines the color of the m subpixels in each of the n transparencies. According to Definition 2, it is a black-and-white (Γ_{Qual}, Γ_{Forb})-VCS when $g = 2$.

2 Multi secret images color VCS for general access structures

Our scheme supports the RGB model. Red, green and blue are the primary color components of the RGB color space. All the other desired colors can be obtained by using additive color mixing of different RGB components. An RGB color is equal to a set of three intensity values, one for each primary color. This RGB color may be reproduced by mixing the

red, green and blue component sets to these intensity values. We defined an RGB color palette as a set of RGB colors. The intensity of a primary color can be defined as the grey level in the grey-level palette. A primary color will have an intensity range between 0 and 255, with 0 representing black and 255 representing the maximum possible intensity of that color. The RGB color palette is created from three grey-level palettes, which represent the intensity palettes for red, green and blue. Combining the members in the grey-level palettes in all possible ways creates the color palette.

In a real color system, R (red), G (green), and B (blue) are each represented by 8 bits, and therefore each single color based on R, G, and B can represent 0—255 variations of scale. When RGB is used to represent a color pixel, (0,0,0) represents full black and (255,255,255) represents the maximum possible intensity of that color, namely white.

In this paper, we will use the RGB model to represent colors. The RGB color palette is created from grey-level palettes. Therefore, we can construct a color scheme based on grey-level schemes.

2.1 Multi secret images grey-level VCS for general access structures

In a grey-level VCS, the shares are black and white. Through stacking these shares, human visual system feels the overall effect of each share so that the shares with different Hamming weights show different grey levels. In an image with g grey levels, the possible grey level of each pixel is $1, \cdots, g$. Suppose that the difference of neighboring grey levels is the same, where at least $g-1$ bits are needed to represent these grey levels, the $g-1$ bits being all 0's represent the first grey level, and all 1's represent the gth grey level.

In the following $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$-MVCS, the combination of all the meaningful shares in different qualified sets will recover a distinct secret image, while the combination of those in forbidden set can obtain no secret information.

Lemma 1.[16] Let $\boldsymbol{B}_0$ and $\boldsymbol{B}_1$ be basis matrices of an (n, n)-VCS. Then for any Boolean matrix $\boldsymbol{R}$ with n rows, the matrices $\boldsymbol{B}_0 \circ \boldsymbol{R}$ and $\boldsymbol{B}_1 \circ \boldsymbol{R}$ are basis matrices of a valid (n, n)-VCS, where the symbol $\circ$ denotes the concatenation of matrices.

Theorem 1. Suppose m is the pixel expansion of a $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$-VCS for g_0 grey levels on n participants. We extend the shares with random patterns to meaningful ones. Let the n cover images corresponding to the n shares be $h_1, \cdots, h_n$ grey levels, respectively. Suppose m_{E} is the pixel expansion of the grey-level $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$-EVCS. Thus, the grey-level $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$-EVCS exists with the added pixel expansion $m_0 = m_{\text{E}} - m = \sum_{i=1}^{n} (h_i - 1)$, and the relative difference of the meaningful share is $\alpha_0 = 1/m_{\text{E}}$.

Proof. To represent $1, \cdots, h_i$ different grey levels, at least $h_i - 1$ bits are required. For $i = 1, \cdots, n$, let $\boldsymbol{A}_i$ be a Boolean matrix with the size $n \times (h_i - 1)$. The ith row in $\boldsymbol{A}_i$ is referred to as r_i, representing the grey level of the pixel p_i in the ith cover image. If p_i is the h_{ij}th grey level, r_i includes $(h_i - h_{ij})$ 0's and $(h_{ij} - 1)$ 1's, where $j = 1, \cdots, h_i$. All the rows in $\boldsymbol{A}_i$ are all 1's except the r_ith row, thus whatever the value of r_i, the OR $V_{A_i}^l$ of any $l (2 \leqslant l \leqslant n)$ rows in $\boldsymbol{A}_i$ has Hamming weight $w(V_{A_i}^l) = h_i - 1$.

First, we will prove that the contrast condition is satisfied. Let $\boldsymbol{A} = \boldsymbol{A}_1 \circ \cdots \circ \boldsymbol{A}_n$ with the size of $n \times \sum_{i=1}^{n} (h_i - 1)$. Letting R_i denote the ith row in matrix $\boldsymbol{A}$, we get $w(R_i) = \sum_{\substack{j=1 \\ j \neq i}}^{n} (h_j - 1) + w(r_i)$. If $p_i = 1, \cdots, h_i$, $w(R_i) = \sum_{\substack{j=1 \\ j \neq i}}^{n} (h_j - 1), \cdots, \sum_{\substack{j=1 \\ j \neq i}}^{n} (h_j - 1) + (h_i - 1)$, which present h_i different grey levels, the contrast condition of the ith share is satisfied. Obviously, the relative difference of the meaningful share is $\alpha_0 = 1/m_{\text{E}}$.

Next, we will prove the security of the scheme. The OR V_A^l of any $l (2 \leqslant l \leqslant n)$ rows in $\boldsymbol{A}$ has Hamming weight $w(V_{A_i}^l) = \sum_{i=1}^{n} (h_i - 1)$. Thus, the security of the scheme is ensured.

Let the basis matrices of $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$-VCS for g_0 grey levels be $\boldsymbol{B}_t$, $t \in \{1, \cdots, g_0\}$. From Lemma 1, $\boldsymbol{B}_t \circ \boldsymbol{A}$ are basis matrices of a valid grey-level $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$-EVCS. Q.E.D.

Lemma 2.[20] In any (k, k)-VCS for g grey levels, it holds that $m \geqslant (g-1) \cdot 2^{k-1}$.

Theorem 2. Suppose m_E is the pixel expansion of a grey-level $(\Gamma_{Qual}, \Gamma_{Forb})$-MVCS on n participants. Let n distinct cover images have grey levels $h_1, \cdots, h_n$. Let $\Gamma_{Qual} = \{T_i \mid 1 \leqslant i \leqslant q\}$, $|T_i| = t_i$, and q distinct secret images have grey levels $g_1, \cdots, g_q$, respectively. Thus, the grey-level $(\Gamma_{Qual}, \Gamma_{Forb})$-MVCS exists with pixel expansion $m_E = \sum_{i=1}^{n} (h_i - 1) + \sum_{j=2}^{q} (g_j - 1) \times 2^{t_j - 1}$ and the relative difference of the reconstructed image is $\alpha_E = 1/m_E$.

Proof. From theorem 1, a grey-level $(\Gamma_{Qual}, \Gamma_{Forb})$-EVCS can be constructed with pixel expansion $m_0 = \sum_{i=1}^{n} (h_i - 1)$, where the m_0 columns constitute a matrix $\boldsymbol{A}$.

For $i = 1, \cdots, q$, let $\boldsymbol{D}_{ij}$ be the basis matrices of a (t_i, t_i)-VCS for g_i grey levels, where $j = 1, \cdots, g_i$. From Lemma 2, the size of $\boldsymbol{D}_{ij}$ is $t_i \times [(g_i - 1) \cdot 2^{t_i - 1}]$.

We will prove that the q secret images can be shared with pixel expansion $m = \sum_{i=2}^{q} (g_i - 1) \times 2^{t_i - 1}$. Let $\boldsymbol{B}_i$ be an $n \times [(g_i - 1) \cdot 2^{t_i - 1}]$ matrix, and $T_i = \{r_1, \cdots, r_{t_i}\}$, where $r_1 < \cdots < r_{t_i}$. Suppose $\boldsymbol{B}_i[T_i]$ is a Boolean matrix with size $t_i \times [(g_i - 1) \cdot 2^{t_i - 1}]$, the 1st row, $\cdots$, the t_ith row in $\boldsymbol{B}_i[T_i]$ are the r_1th, $\cdots$, the r_{t_i}th row in $\boldsymbol{B}_i$, respectively. If the original pixel p_i in the ith secret images is the g_{ij}th grey level, we have $\boldsymbol{B}_i[T_i] = \boldsymbol{D}_{ij}$. All the rows in $\boldsymbol{B}_i$ are all 1's except the r_1th, $\cdots$, the r_{t_i}th rows.

Now, we will prove the contrast condition is satisfied. Let $\boldsymbol{B} = \boldsymbol{B}_1 \circ \cdots \circ \boldsymbol{B}_q$ with the size of $n \times \sum_{j=2}^{q} (g_j - 1) \times 2^{t_j - 1} = n \times m$. Select the r_1th row, $\cdots$, the r_{t_i}th row in $\boldsymbol{B}$, from the above analysis we know that OR of the t_i rows in $\boldsymbol{B}_j$ $(j = 1, \cdots, i - 1, i + 1, \cdots, j)$ is a constant. For $\boldsymbol{B}_i[T_i] = \boldsymbol{D}_{ij}$, the contrast of the ith recovered secret image is ensured by the contrast condition of the g_i grey levels (t_i, t_i)-VCS. Obviously, the relative difference of the reconstructed image is $\alpha_E = 1/m_E$.

Next, we will prove the security of the scheme. Considering the ith share, the secret information is in $\boldsymbol{B}_i$. Randomly selecting the s_1th row, $\cdots$, the s_lth row in $\boldsymbol{B}$, where $2 \leqslant l \leqslant t_i - 1$. The security of the ith share is ensured by the security condition of the g_i grey levels (t_i, t_i)-VCS.

According to Lemma 1, $\boldsymbol{B} \circ \boldsymbol{A}$ are basis matrices of a valid grey-level $(\Gamma_{Qual}, \Gamma_{Forb})$-MVCS. Q.E.D.

From theorem 2, we have known that $m_E = n + \sum_{j=2}^{q} 2^{t_j - 1}$ is the pixel expansion of a black-and-white $(\Gamma_{Qual}, \Gamma_{Forb})$-MVCS with n participants, where $|\Gamma_{Qual}| = q$, and the size of the q qualified sets are $t_1, \cdots, t_q$. If any combination of no less than two shares can recover a distinct secret image, the qualified sets are all the subsets with no less than two participants. The number of the qualified sets with size of k is C_k^n, $k = 2, \cdots, n$, from which we obtain $m_E = n + \sum_{k=2}^{n} 2^{k-1} \times C_k^n = \sum_{k=1}^{n} 2^{k-1} \times C_k^n$. Our calculated m_E is equivalent to the result in Ref. [16], which can verify the validity of the scheme constructed in this section.

2.2 Color multi secret images VCS for general access structures

An RGB image includes the Red, Green and Blue components, and each of them is a grey-level image. Therefore, we can construct a color $(\Gamma_{Qual}, \Gamma_{Forb})$-MVCS by using the grey-level $(\Gamma_{Qual}, \Gamma_{Forb})$-MVCS. The following theorem is an immediate consequence of Theorem 2.

Theorem 3. Let the pixel expansion be m_E in a color $(\Gamma_{Qual}, \Gamma_{Forb})$-MVCS with n participants. Let the color value of n distinct cover images be $d_1, \cdots, d_n$. Let $\Gamma_{Qual} = \{T_i \mid 1 \leqslant i \leqslant q\}$, $|T_i| = t_i$, and the color value of q distinct secret images be $c_1, \cdots, c_q$, respectively. Thus, we can construct a color $(\Gamma_{Qual}, \Gamma_{Forb})$-MVCS with pixel expansion

$$m_E = \sum_{k=1}^{3} \left(\sum_{i=1}^{n} (d_i^{(k)} - 1) + \sum_{j=2}^{q} (c_j^{(k)} - 1) \times 2^{t_j - 1} \right)$$

and relative difference $\alpha_E = 1/(3 \times m_E)$, where the superscripts $k = 1$, $k = 2$, $k = 3$ represents the red, green and blue components of an original pixel.

4 Results

Based on a grey-level $(\Gamma_{Qual}, \Gamma_{Forb})$-VCS, we have constructed a grey-level $(\Gamma_{Qual}, \Gamma_{Forb})$-EVCS with meaningful shares, and a grey-level $(\Gamma_{Qual}, \Gamma_{Forb})$-MVCS and color $(\Gamma_{Qual}, \Gamma_{Forb})$-MVCS have

been realized. Next, we will specify the construction method for color (Γ_{Qual}, Γ_{Forb})-MVCS through an example.

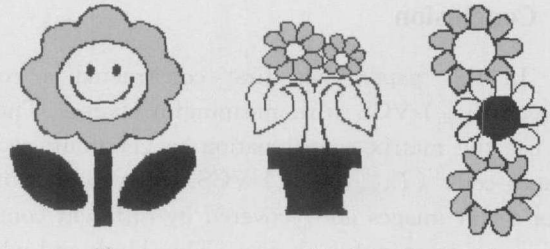
Example 1

Consider a grey-level (Γ_{Qual}, Γ_{Forb})-MVCS with three participants, in which two secret images with three grey levels denoted as S_1 and S_2 are shared, and three cover images are all three grey levels. The grey levels of S_1 and S_2 are expressed by $g_1 = 3$ and $g_2 = 3$, while the grey levels of three cover images are denoted by $h_1 = 3$, $h_2 = 3$ and $h_3 = 3$. Let the participant set be $\boldsymbol{P} = \{1, 2, 3\}$, the qualified set to recover S_1 be $\boldsymbol{T}_1 = \{1, 2\}$, the qualified set to recover S_2 be $\boldsymbol{T}_2 = \{1, 3\}$, that is, $\Gamma_{Qual} = \{\boldsymbol{T}_1, \boldsymbol{T}_2\} = \{\{1, 2\}, \{1, 3\}\}$. In addition, $t_1 = |\boldsymbol{T}_1| = 2$, and $t_2 = |\boldsymbol{T}_2| = 2$, and the forbidden set is $\Gamma_{Forb} = 2^{\boldsymbol{P}} - \Gamma_{Forb}$. From Theorem 1, we can construct meaningful shares with pixel expansion $m_0 = \sum_{i=1}^{3} (h_i - 1) = (3 - 1) + (3 - 1) + (3 - 1) = 6$. From Theorem 2, the pixel expansion for sharing S_1 is $(g_1 - 1) \times 2^{t_1 - 1} = (3 - 1) \times 2^{2-1} = 4$; the pixel expansion for sharing S_2 is $(g_2 - 1) \times 2^{t_2 - 1} = (3 - 1) \times 2^{2-1} = 4$. Therefore, the pixel expansion to realize the above grey-level (Γ_{Qual}, Γ_{Forb})-MVCS is $m_E = m_0 + m = 6 + 4 + 4 = 14$. Next, we explicate the construction method through a concrete matrix.

Suppose the two original pixels are the 1st and 3rd grey levels, respectively, the corresponding three pixels in cover images are the 1st, 2nd and 3rd grey levels. Then the basis matrix is

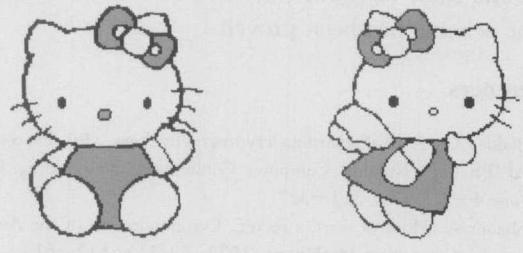
$$\boldsymbol{B} = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

From the above method, we can construct the basis matrices with any grey level of secret pixels and cover pixels. A concrete example is given in Figs. 1—4. The combination of the 1st and the 2nd shares can recover S_1; the combination of the 1st and the 3rd shares can recover S_2. However, the combination of the 2nd and the 3rd shares can gain nothing but a black image.



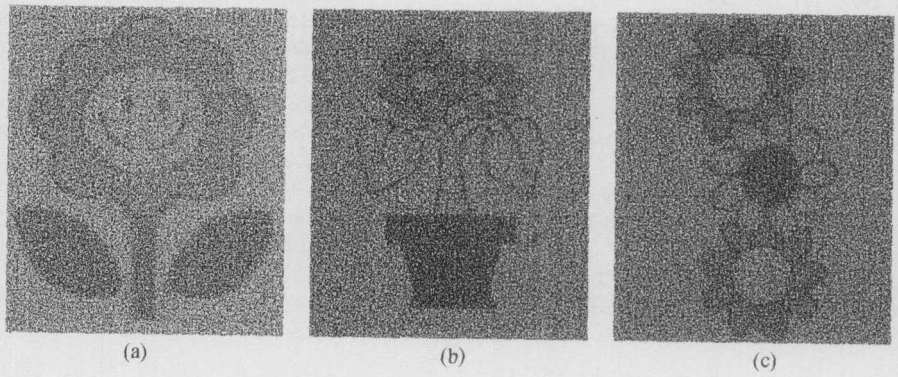
(a) (b) (c)

Fig. 1. Cover images. (a) Cover image 1; (b) cover image 2; (c) cover image 3.



(a) (b)

Fig. 2. Secret images. (a) Secret image 1; (b) secret image 2.



(a) (b) (c)

Fig. 3. Shares. (a) Share of participant 1; (b) share of participant 2; (c) share of participant 3.

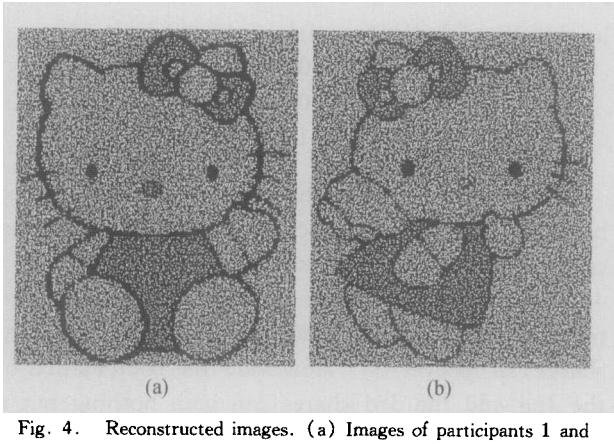


Fig. 4. Reconstructed images. (a) Images of participants 1 and 2; (b) images of participants 1 and 3.

5 Conclusion

In this paper, we first constructed a color (Γ_{Qual}, Γ_{Forb})-VCS with meaningful shares. Then, we use the matrix concatenation to get multi secret images color (Γ_{Qual}, Γ_{Forb})-VCS, in which distinct color secret images are recovered by different combination of meaningful shares. The black-and-white (Γ_{Qual}, Γ_{Forb})-MVCS[16] is the special case of the above color (Γ_{Qual}, Γ_{Forb})-MVCS. Meanwhile, we obtain the pixel expansion and contrast of the grey-level and color (Γ_{Qual}, Γ_{Forb})-MVCS, and the validity of the scheme has been proved.

References

1 Blakley G. R. Safeguarding cryptography keys. In: Proceedings AFIPS 1979 National Computer Conference, New York, USA, June 4—7, 1979, 313—317.
2 Shamir A. How to share a secret. Communication of the Association for Computing Machinery, 1979, 22(11): 612—613.
3 Naor M. and Shamir A. Visual cryptography. In: Advances in Cryptology-Eurocrypt' 94" (ed. De Santis A.), Lecture Notes in Computer Science, Berlin: Springer, 1995, 950: 1—12.
4 Verheul E. R. and Van Tilborg H. C. A. Constructions and properties of k out of n visual secret sharing schemes. Designs, Codes and Cryptography, 1997, 11: 179—196.
5 Su Z. M. and Lin X. L. The arbitrary share of visual secrets. Chinese Journal of Computers (in Chinese), 1996, 19(4): 293—299.
6 Ding W. and Qi D. X. Digital image transformation and information hiding and disguising Technology. Chinese Journal of Computers (in Chinese), 1998, 21(9): 838—843.
7 Xia G. S. and Yang Y. X. A new secret sharing scheme-image covering. Journal of Beijing University of Posts and Telecommunications (in Chinese), 1999, 22(1): 57—61.
8 Wang D. S. A minimum pixels scheme of 2 out of 2 visual cryptography. Journal of Sichuan University (Natural Science) (in Chinese), 2000, 37(3): 325—330.
9 Wang D. S. and Qi D. X. A new scheme for (k, k) visual cryptography by XOR operation. Journal of Image and Graphics, 2000, 5: 486—489.
10 Su Z. M., Lin X. L. and Dai Y. Q. The improvement of a simple threshold scheme. Journal of Software (in Chinese), 1997, 8(2): 128—136.
11 Yang K., Lin X. L., Pan P. et al. Minimum size of (2, n) data sharing scheme under XOR operation. Journal of Tsinghua University (Sci. & Tech.) (in Chinese), 1998, 38(SI): 48—51.
12 Wang D. S. and Yang L. Visual hiding scheme using secret image. Chinese Journal of Computers (in Chinese), 2000, 23(9): 943—948.
13 Wang D. S. and Qi D. X. Visual hiding of digital image. In: 16th World Computer Congress 2000, IFIP/SEC2000: Information Security (ed. Qing S. H. et al.). Beijing: International Academic Publishers, 2000: 21—24.
14 Wang D. S., Luo P., Yang L. et al. Shift visual cryptography scheme of two secret images. Process in Natural Science, 2003, 13(6): 457—463.
15 Xia G. S., Yang Z. L., Yang Y. X. et al. A new visual cryptography algorithm to hide a two-color image in a single shared image, Journal of Beijing University of Posts Telecommunications (in chinese), 2002, 25(3): 12—16.
16 Droste S. New results on visual cryptography. In: Advances in Cryptology"—CRYPTO'96 (ed. Koblit N.). Berlin: Springer-Verlag, LNCS, 1996, 1109: 401—415.
17 Ateniese G., Blundo C., De Santis A. et al. Constructions and bounds for visual cryptography. In: 23rd International Colloquium on Automata, Languages and Programming (ICALP'96), Berlin: Springer, 1996, 1099: 416—428.
18 Ateniese G., Blundo C. and De Santis A. et al. Visual cryptography for general access structures. Information and Computation, 1996, 129(2): 86—106.
19 Alteniese G., Blundo C., De Santis A. et al. Extended capabilities for visual cryptography. Theoretical Computer Science, 2001, 250: 143—161.
20 Blundo C., De Santis A. and Naor M. Visual cryptography for grey level images. Information Processing Letters, 2000, 75(6): 255—259.
21 Koga H. and Yamamoto H. Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images. IEICE Trans. Fundamentals, 1998, E81-A(6): 1262—1269.
22 Koga H., Iwamoto M. and Yamamoto H. An analytic construction of the visual secret sharing scheme for color images. IEICE Trans. Fundamentals, 2001, E84-A(1): 262—272.
23 Ishihara T. and Koga H. New constructions of the lattice-based visual secret sharing scheme using mixture of colors. IEICE Trans. Fundamentals, 2002, E85-A(1): 158—166.
24 Iwamoto M. and Yamamoto H. The optimal n out of n visual secret sharing scheme for gray-scale images. IEICE Trans. Fundamentals, 2002, E85-A(10): 2238—2247.
25 Kuwakado H. and Tanaka H. Polynomial representation of a visual secret sharing scheme and its application. IEICE Trans. Fundamentals, 2002, E85-A(6): 1379—1386.
26 Ishihara T. and Koga H. A visual secret sharing scheme for color images based on mean-value color mixing. IEICE Trans. Fundamentals, 2003, E86-A(1): 194—197.