PAPER *Special Section on Information Theory and Its Applications*

A Construction Method of Visual Secret Sharing Schemes for Plural Secret Images*

Mitsugu IWAMOTO[†a)], ***Student Member and*** **Hirosuke YAMAMOTO**[†], ***Regular Member***

SUMMARY In this paper, a new method is proposed to construct a visual secret sharing scheme with a general access structure for plural secret images. Although the proposed scheme can be considered as an extension of Droste's method that can encode only black-white images, it can encode plural gray-scale and/or color secret images.

key words: *visual secret sharing schemes, plural secret images, general access structures*

1. Introduction

The visual secret sharing scheme (VSS scheme), which originates from the visual cryptography proposed by Naor and Shamir [14], is a method to encode a secret image into several *shares*. Since each share is usually printed on a transparency, the secret image can easily be decrypted only by peering at several shares stacked in an arbitrary order. Hence, the VSS scheme needs no computation in decryption.

The first VSS scheme [14] is the (k,n)-threshold scheme for a monotone black-white single image. The (k,n)-threshold scheme means that any k out of n shares can decrypt the secret, but any $k-1$ or less shares must not leak out any information of the secret. The (k,n) structure can be extended to a general access structure which is specified by qualified sets and forbidden sets [1]. A qualified set is a subset of n shares that can decrypt the secret image while a forbidden set is a subset of shares that can gain no information of the secret image. Furthermore, VSS schemes for black-white images [1], [4], [5], [14] are extended to gray-scale images [3], [7], [9] and color images [9], [10], [16] in the case of general access structures, and the quality optimizations of decrypted images are discussed in [1], [3]–[5], [7], [10], [12], [15], [16].

VSS schemes for plural secret images are also studied [5], [8], [15]. Kato-Imai [8] proposed a method to reproduce different secret images as the number of shares is increased, and Suga et al. [15] treated VSS schemes for plural secret images and some access structures which can be represented by a graph. Furthermore, Droste [5] showed a method to decrypt different black-white secret images for every subset of n shares. However, VSS schemes for plural gray-scale or color secret images have not yet been studied.

In this paper, we propose a method to construct a VSS scheme for q plural images, a VSS-q-PI scheme for short, which can treat color and/or gray-scale images. In the framework of the VSS-q-PI scheme, we assume that each participant holds one share, and hence, usual VSS schemes for one secret image can be treated as the VSS-1-PI schemes. Note that it is difficult to realize the VSS-q-PI schemes, compared with the VSS-1-PI schemes, because each pixel of plural secret images must be encoded under the condition that any decrypted images must not leak out any informations of the other secret images. In fact, as we will show in Sect. 2.3, decrypted images of VSS-q-PI schemes treated in [8], [15] leak out some information of the other secret images. But, defining the correct security conditions of VSS-q-PI schemes, we clarify the construction method of VSS-q-PI schemes that attains perfectly the security conditions without degenerating the quality of decrypted images compared with the methods in [8], [15].

This paper is organized as follows. In Sect. 2, the access structures of the VSS-q-PI schemes are formally defined, and a color matrix is introduced to describe the colors of plural secret images. Section 3 is devoted to show how to construct the VSS-q-PI schemes. Furthermore, in Sect. 4, we discuss an extended construction method by duplicating secret images, which can extend the range of the VSS-q-PI schemes that our method can be applied to. Finally, in Sect. 5, we consider what advantages of the VSS-q-PI schemes have compared with trivial schemes consisting of q individual VSS-1-PI schemes.

2. Definitions

2.1 Access Structures

Let $\mathcal{N} = \{1, 2, \ldots, n\}$ and $2^{\mathcal{N}}$ be the set of n shares and the family of all the subsets of $\mathcal{N}$, respectively.

Manuscript received January 17, 2003.
Manuscript revised April 17, 2003.
Final manuscript received June 6, 2003.

[†] The authors are with the Department of Mathematical Informatics, Graduate School of Information Science and Technology, the University of Tokyo, Tokyo, 113-0033 Japan.

a) E-mail: mitsugu@sr3.t.u-tokyo.ac.jp

[*] This paper was presented in part at Symposium on Information Theory and its Applications, 2001, the technical meeting on ISEC of IEICE, 2002, and the IEEE International Symposium on Information Theory, 2003.

We suppose that all secret images are encrypted at once into n shares. Each secret image is denoted by $SI^{(i)}$, $i = 1, 2, \ldots, q$, which has the same size. Let $\Gamma^{(i)}_{\mathsf{Qual}}$, $i = 1, 2, \ldots, q$, be the family of *qualified sets for the i-th secret image*, and let Γ_{Forb} be the family of *forbidden sets*. Then, any set in $\Gamma^{(i)}_{\mathsf{Qual}}$ can decrypt the i-th secret image $SI^{(i)}$ while any set in Γ_{Forb} cannot gain any information of any secret image. We call $\Gamma = (\{\Gamma^{(i)}_{\mathsf{Qual}}\}^{q}_{i=1}, \Gamma_{\mathsf{Forb}})$ an *access structure for q secret images*.

Note that each $\Gamma^{(i)}_{\mathsf{Qual}}$ and Γ_{Forb} satisfy the following *monotonicity*.

$$\mathcal{Q}^{(i)} \in \Gamma^{(i)}_{\mathsf{Qual}} \Rightarrow \mathcal{Q}' \in \Gamma^{(i)}_{\mathsf{Qual}} \text{ for any } \mathcal{Q}' \supseteq \mathcal{Q}^{(i)} \quad (1)$$

$$\mathcal{F} \in \Gamma_{\mathsf{Forb}} \Rightarrow \mathcal{F}' \in \Gamma_{\mathsf{Forb}} \text{ for any } \mathcal{F}' \subseteq \mathcal{F} \quad (2)$$

Therefore, for each $\Gamma^{(i)}_{\mathsf{Qual}}$ and Γ_{Forb}, the *minimal* qualified sets of the i-th secret image $\Gamma^{(i)-}_{\mathsf{Qual}}$ and the *maximal* forbidden sets $\Gamma^{+}_{\mathsf{Forb}}$ can be defined as follows.

$$\Gamma^{(i)-}_{\mathsf{Qual}} = \{\mathcal{Q}^{(i)} \in \Gamma^{(i)}_{\mathsf{Qual}} : \mathcal{Q}' \notin \Gamma^{(i)}_{\mathsf{Qual}} \text{ for any } \mathcal{Q}' \subsetneq \mathcal{Q}^{(i)}\} \quad (3)$$

$$\Gamma^{+}_{\mathsf{Forb}} = \{\mathcal{F} \in \Gamma_{\mathsf{Forb}} : \mathcal{F}' \notin \Gamma_{\mathsf{Forb}} \text{ for any } \mathcal{F}' \supsetneq \mathcal{F}\} \quad (4)$$

$\Gamma^{(i)-}_{\mathsf{Qual}}$ and Γ_{Forb} are naturally required to satisfy

$$\left\{\bigcup_{i=1}^{q} \Gamma^{(i)}_{\mathsf{Qual}}\right\} \cup \Gamma_{\mathsf{Forb}} = 2^{\mathcal{N}}, \quad (5)$$

$$\Gamma^{(i)}_{\mathsf{Qual}} \cap \Gamma_{\mathsf{Forb}} = \emptyset, \quad (6)$$

$$\Gamma^{(i)-}_{\mathsf{Qual}} \cap \Gamma^{(i')-}_{\mathsf{Qual}} = \emptyset \quad \text{for } i \neq i'. \quad (7)$$

The requirement Eq. (7) comes from the assumption that all the secret images are different. It is worth noting that the VSS-1-PI scheme with the access structure $(\Gamma^{(1)}_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ coincides with the usual VSS scheme with the same access structure for one secret image, which is treated in [1], [3], [4], [10].

We also define $\mathcal{N}^{(i)}$, the set of significant shares for the i-th secret image, as follows.

$$\mathcal{N}^{(i)} = \bigcup_{\mathcal{Q}^{(i)-} \in \Gamma^{(i)-}_{\mathsf{Qual}}} \mathcal{Q}^{(i)-}. \quad (8)$$

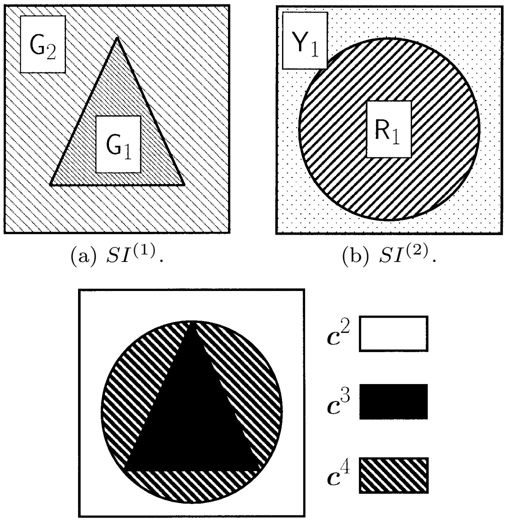
Example 1: Let $\mathcal{N} = \{1, 2, 3, 4\}$ be the set of shares. Suppose that any two out of three shares $\{1, 2, 3\}$ can decrypt the secret image $SI^{(1)}$ shown in Fig. 1(a), and set $\{3, 4\}$ can decrypt the secret image $SI^{(2)}$ shown in Fig. 1(b). But, set $\{1, 4\}$, $\{2, 4\}$ or any one share must not leak out any information of both secret images. This access structure can be represented as follows.

$$\Gamma^{(1)}_{\mathsf{Qual}} = \{\{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}, \{1,2,3,4\}\} \quad (9)$$

$$\Gamma^{(2)}_{\mathsf{Qual}} = \{\{3,4\}, \{1,3,4\}, \{2,3,4\}, \{1,2,3,4\}\} \quad (10)$$

$$\Gamma_{\mathsf{Forb}} = \{\{1\}, \{2\}, \{3\}, \{4\}, \{1,4\}, \{2,4\}\} \quad (11)$$

In this case, it holds that $\Gamma^{(1)-}_{\mathsf{Qual}} = \{\{1,2\}, \{1,3\}, \{2,3\}\}$, $\Gamma^{(2)-}_{\mathsf{Qual}} = \{\{3,4\}\}$, $\Gamma^{+}_{\mathsf{Forb}} = \{\{3\}, \{1,4\}, \{2,4\}\}$, $\mathcal{N}^{(1)} = \{1,2,3\}$, $\mathcal{N}^{(2)} = \{3,4\}$. Note that set $\{1,2,3\}$ must not leak out any information of $SI^{(2)}$ because of $\{1,2,3\} \notin \Gamma^{(2)}_{\mathsf{Qual}}$, although it can decrypt $SI^{(1)}$. □



(a) $SI^{(1)}$.

(b) $SI^{(2)}$.

(c) Location of shapes in (a) and (b).

Fig. 1 An example of plural secret images.

2.2 Color Matrix

In this paper, colors are expressed by lowercase sanserif fonts. For example, we denote black, red, green, blue, yellow, magenta, cyan, and white by z, r, g, b, y, m, c and a, respectively. A general color is expressed by k.

Let $\sqcup$ represent the subtractive mixture of colors which corresponds to overlapping the colors printed on transparencies. Then, $\mathsf{z} \sqcup \mathsf{g} = \mathsf{g} \sqcup \mathsf{z} = \mathsf{z}$, and $\mathsf{c} \sqcup \mathsf{y} = \mathsf{y} \sqcup \mathsf{c} = \mathsf{g}$ hold, for example. Let color set $\mathcal{E}$ be the set of both the colors printed on shares and the mixtures of such colors. Note that $\sqcup$ is commutative in $\mathcal{E}$ and $\mathcal{E}$ is closed with respect to $\sqcup$. In the case of $\mathcal{E} = \{\mathsf{z}, \mathsf{r}, \mathsf{g}, \mathsf{b}, \mathsf{y}, \mathsf{m}, \mathsf{c}, \mathsf{a}\}$, it is known that $\mathcal{E}$ forms a bounded upper semilattice with the join operation $\sqcup$ [9].

In the VSS-q-PI scheme, a pixel on a decrypted secret image $DI^{(i)}$, which corresponds to a secret image $SI^{(i)}$, is constructed by a set of m subpixels where m is called *pixel expansion* and each subpixel takes a color in $\mathcal{E}$. We consider the case that every subpixel in a pixel takes the same color k or black z for some k in $\mathcal{E}$. Then, the brightness of a pixel in $DI^{(i)}$ can be expressed by the composition ratio of k and z.

We express the colors of pixels in $DI^{(i)}$ by capital san-serif fonts K_{ℓ}, $\ell = 1, 2 \ldots, L_{\mathsf{k}}$, which is composed of $\mathsf{k}(\neq \mathsf{z})$ and z and stands for the ℓ-th bright color of k. We assume that K_{ℓ_1} is brighter than K_{ℓ_2}, i.e., K_{ℓ_1} contains more k than K_{ℓ_2} if $\ell_1 > \ell_2$. In the case that all subpixels in a decrypted pixel are z, we represent the pixel color by Z. For the simplicity of notation, we define $\mathsf{K}_0 = \mathsf{Z}$ for any $\mathsf{k} \in \mathcal{E}$. Note that $\mathsf{K}_1 \neq \mathsf{Z}$ for any $\mathsf{k}(\neq \mathsf{z}) \in \mathcal{E}$, and in the case of $\mathsf{k} = \mathsf{a}$, the set $\{\mathsf{A}_0(=\mathsf{Z}), \mathsf{A}_1, \mathsf{A}_2, \ldots, \mathsf{A}_{L_\mathsf{a}}\}$ represents a gray scale with $L_\mathsf{a} + 1$ depths [3], [7].

For a set $\{\mathsf{K}_0(=\mathsf{Z}), \mathsf{K}_1, \mathsf{K}_2, \ldots, \mathsf{K}_{L_\mathsf{k}}\}$, let $d_{\mathsf{k},\ell}$ denote the difference of the numbers of k between K_ℓ and $\mathsf{K}_{\ell+1}$. In case of $\mathsf{k} = \mathsf{z}$, define that $d_{\mathsf{z},0} = 0$. Note that $d_{\mathsf{k},\ell} \geqq 1$ for any $\mathsf{k} \neq \mathsf{z}$ and $\ell \geqq 0$. Then we assume that the color of each pixel on $SI^{(i)}$ can be approximated by selecting a color $\mathsf{k} \in \mathcal{E}$ and parameter $d_{\mathsf{k},\ell}$ adequately, and hence, there exists one-to-one correspondence between the set of colors of $SI^{(i)}$ and that of $DI^{(i)}$.

Let $\mathcal{D}^{(i)}$ be the set of all the colors with all kinds of brightness included in the decrypted image $DI^{(i)}$. Then, for K_ℓ and $\mathsf{Z} \in \mathcal{D}^{(i)}$, we can define mapping $\gamma : \mathcal{D}^{(i)} \to \mathcal{E}$ that gives the hue $\gamma(\mathsf{K}_\ell) = \mathsf{k} \in \mathcal{E}$ and $\gamma(\mathsf{Z}) = \mathsf{z}$.

Remark 1: The above definition of decrypted pixel colors includes both the definition for the *lattice-based* VSS schemes [9], [10], [12] and the *gray-scale* VSS schemes [3], [7]. On the other hand, the *meanvalue-color mixing* (MCM)-VSS scheme [13], [16] cannot be treated by the above definition because in the MCM-VSS scheme, each pixel on decrypted images is composed of the three primary colors $(\mathsf{r}, \mathsf{g}, \mathsf{b})$ and z. But, since the MCM-VSS schemes requires large pixel expansion, it seems to be hard to realize a VSS scheme for a general access structure with $n \geqq 3$. □

Now we define a color matrix. Let $\mathcal{D}$ be $\mathcal{D} = \mathcal{D}^{(1)} \times \mathcal{D}^{(2)} \times \cdots \times \mathcal{D}^{(q)}$. Then, in the VSS-$q$-PI scheme, all the combinations of colors appeared in decrypted images can be represented by a color matrix $\boldsymbol{D}$ which is defined as follows.

$$\begin{aligned}\boldsymbol{D} = &\ \left[\ \boldsymbol{c}^1\ \boldsymbol{c}^2\ \cdots \boldsymbol{c}^K\ \right] \\ = &\begin{bmatrix} \mathsf{D}^{(1),1} & \mathsf{D}^{(1),2} & \cdots & \mathsf{D}^{(1),K} \\ \mathsf{D}^{(2),1} & \mathsf{D}^{(2),2} & \cdots & \mathsf{D}^{(2),K} \\ \vdots & \vdots & \ddots & \vdots \\ \mathsf{D}^{(q),1} & \mathsf{D}^{(q),2} & \cdots & \mathsf{D}^{(q),K} \end{bmatrix} = \begin{bmatrix} \boldsymbol{r}^{(1)} \\ \boldsymbol{r}^{(2)} \\ \vdots \\ \boldsymbol{r}^{(q)} \end{bmatrix},\end{aligned} \tag{12}$$

where $K = \prod_{i=1}^{q} |\mathcal{D}^{(i)}|$, $\boldsymbol{c}^j \in \mathcal{D}$ and $\boldsymbol{r}^{(i)}$ are a q-dimensional column vector and a K-dimensional row vector, respectively, and $\mathsf{D}^{(i),j}$ is a color included in $\mathcal{D}^{(i)}$.

We assume that $\boldsymbol{D}$ is public. In the usual VSS schemes, i.e., VSS-1-PI schemes, $\boldsymbol{D}$ becomes a row vector with $\boldsymbol{c}^j = \mathsf{D}^{(1),j} \in \mathcal{D}^{(1)}$. Although one color $\mathsf{D}^{(1),j}$ is encrypted for each pixel in the VSS-1-PI schemes, color vector $\boldsymbol{c}^j$ with q colors must be encrypted for each pixel in the VSS-q-PI schemes.

Example 2: In the case of Example 1 with two secret images $SI^{(1)}$ and $SI^{(2)}$ shown in Figs. 1(a) and (b), $\mathcal{D}^{(1)}$ and $\mathcal{D}^{(2)}$ are given by $\mathcal{D}^{(1)} = \{\mathsf{G}_1, \mathsf{G}_2\}$ and $\mathcal{D}^{(2)} = \{\mathsf{Y}_1, \mathsf{R}_1\}$, respectively, and hence the color matrix becomes

$$\boldsymbol{D} = \left[\ \boldsymbol{c}^1\ \boldsymbol{c}^2\ \boldsymbol{c}^3\ \boldsymbol{c}^4\ \right] = \begin{bmatrix} \mathsf{G}_1\mathsf{G}_2\mathsf{G}_1\mathsf{G}_2 \\ \mathsf{Y}_1\mathsf{Y}_1\mathsf{R}_1\mathsf{R}_1 \end{bmatrix} = \begin{bmatrix} \boldsymbol{r}^{(1)} \\ \boldsymbol{r}^{(2)} \end{bmatrix}. \tag{13}$$

Note that $\mathcal{D}^{(1)}$ consists of green pixels with two levels of brightness while $\mathcal{D}^{(2)}$ consists of yellow and red pixels. □

Remark 2: Consider the case that the shapes in Figs. 1(a) and (b) are located as shown in Fig. 1(c). There are three regions in Fig. 1(c), which correspond to the column vectors $\boldsymbol{c}^2, \boldsymbol{c}^3$ and $\boldsymbol{c}^4$ in $\boldsymbol{D}$. But the color matrix $\boldsymbol{D}$ should be composed of four column vectors $\boldsymbol{c}^1, \boldsymbol{c}^2, \boldsymbol{c}^3$, and $\boldsymbol{c}^4$ because of $K = 4$. Note that if the public $\boldsymbol{D}$ consists of $\boldsymbol{c}^2, \boldsymbol{c}^3$ and $\boldsymbol{c}^4$, we can know from $DI^{(2)}$ that the color of the region $\boldsymbol{c}^2$ shown in Fig. 1(c) is G_2 on $DI^{(1)}$ because Y_1 on $DI^{(2)}$ corresponds only to G_2 on $DI^{(1)}$. Therefore, all vectors in $\mathcal{D}$ must be included in $\boldsymbol{D}$ even if some vectors are not appeared in the secret images. □

2.3 Definition of VSS-q-PI Scheme

Pixel expansion m, which is the number of subpixels necessary to represent one pixel, should be as small as possible in the viewpoint of the resolution of decrypted images. We encrypt each $\boldsymbol{c}^j$ into an $n \times m$ matrix $T^j = [\mathsf{t}^j_{uv}] \in \mathcal{E}^{nm}$ where $\mathsf{t}^j_{uv} \in \mathcal{E}$, $1 \leqq u \leqq n$, $1 \leqq v \leqq m$, denotes the color of the v-th subpixel on the u-th share in a pixel represented by the vector $\boldsymbol{c}^j$.

We introduce an equivalence relation $\sim$ into matrices in $\mathcal{E}^{nm}$. For two matrices $A, B \in \mathcal{E}^{nm}$, $A \sim B$ means that A can be obtained by the column permutation of B. In other words, it holds that for any permutation $\sigma : \{1, 2, \ldots, m\} \to \{1, 2, \ldots, m\}$,

$$[\boldsymbol{a}_1 \boldsymbol{a}_2 \cdots \boldsymbol{a}_m] \sim [\boldsymbol{a}_{\sigma(1)} \boldsymbol{a}_{\sigma(2)} \cdots \boldsymbol{a}_{\sigma(m)}], \tag{14}$$

where $\boldsymbol{a}_i$'s are column vectors of a matrix $A \in \mathcal{E}^{nm}$. It is easy to check that this relation satisfies the three conditions of the equivalence relation, i.e., the reflective law, the symmetric law, and the transitive law. Hence we can consider the quotient set $\mathcal{E}^{nm}/\!\sim$, which consists of the equivalence classes. An equivalence class is represented as $\langle R \rangle$ by a representative R in the class.

For two matrices $X \in \mathcal{E}^{nm_1}$ and $Y \in \mathcal{E}^{nm_2}$, we define the concatenation operation $X \odot Y \in \mathcal{E}^{n(m_1+m_2)}$ by, for example,

$$\begin{bmatrix} \mathsf{aaa} \\ \mathsf{aaa} \\ \mathsf{aaa} \end{bmatrix} \odot \begin{bmatrix} \mathsf{zz} \\ \mathsf{zz} \\ \mathsf{zz} \end{bmatrix} = \begin{bmatrix} \mathsf{aaazz} \\ \mathsf{aaazz} \\ \mathsf{aaazz} \end{bmatrix}. \tag{15}$$

Furthermore, we can define naturally that $\langle X\rangle \odot \langle Y\rangle \overset{\text{def}}{=} \langle X\odot Y\rangle$.

For m-dimensional row vectors of colors $\boldsymbol{x} = [\,\mathsf{x}_1\,\mathsf{x}_2\cdots\,\mathsf{x}_m\,]$, $\boldsymbol{y} = [\,\mathsf{y}_1\,\mathsf{y}_2\cdots\,\mathsf{y}_m\,]$ where $\mathsf{x}_i,\mathsf{y}_i\in\mathcal{E}$, we define an operation $\overset{m}{\sqcup}$ as

$$\boldsymbol{x}\overset{m}{\sqcup}\boldsymbol{y} = [\,\mathsf{x}_1\sqcup\mathsf{y}_1\;\mathsf{x}_2\sqcup\mathsf{y}_2\cdots\;\mathsf{x}_m\sqcup\mathsf{y}_m\,], \tag{16}$$

which represents the subtractive mixtures of two pixels with m subpixels. For a matrix $S = {}^t[\boldsymbol{x}_1\boldsymbol{x}_2\cdots\boldsymbol{x}_n]\in\mathcal{E}^{nm}$, where t means the transpose of the matrix, and an arbitrary set $\mathcal{X}=\{u_1,u_2,\ldots,u_r\}\subseteq\mathcal{N}$, an $|\mathcal{X}|\times m$ matrix $S[\![\mathcal{X}]\!]$ is defined as $S[\![\mathcal{X}]\!] = {}^t[\boldsymbol{x}_{u_1}\boldsymbol{x}_{u_2}\cdots\boldsymbol{x}_{u_r}]\in\mathcal{E}^{|\mathcal{X}|m}$. Then, the colors obtained by stacking the u_i-th shares, $i=1,2,\ldots,r$, are represented by the mapping $\beta:\mathcal{E}^{|\mathcal{X}|m}\to\mathcal{E}^m$ defined by

$$\beta(S[\![\mathcal{X}]\!]) = \boldsymbol{x}_{u_1}\overset{m}{\sqcup}\boldsymbol{x}_{u_2}\overset{m}{\sqcup}\cdots\overset{m}{\sqcup}\boldsymbol{x}_{u_r}. \tag{17}$$

For a given set $\mathcal{X}\subseteq\mathcal{N}$, the set of indices of the secret images that can be decrypted from $\mathcal{X}$, say $\mathcal{I}(\mathcal{X})$, is represented as

$$\mathcal{I}(\mathcal{X}) = \left\{ i : \mathcal{X}\in\Gamma^{(i)}_{\mathsf{Qual}}, 1\leqq i\leqq q\right\}. \tag{18}$$

For instance, $\mathcal{I}(\mathcal{N}) = \{1,2,\ldots,q\}$, and $\mathcal{I}(\mathcal{F})=\emptyset$ for any $\mathcal{F}\in\Gamma_{\mathsf{Forb}}$.

Now we define the VSS-q-PI scheme for a general access structure Γ.

Definition 1: A VSS-q-PI scheme for an access structure Γ is called a $(\Gamma,\mathcal{N},\mathcal{E},\boldsymbol{D})$-VSS-$q$-PI scheme if it has color matrix $\boldsymbol{D}$ for color set $\mathcal{E}$, and for every $j\in\{1,2,\ldots,K\}$ each pixel associated with $\boldsymbol{c}^j$ is determined by a matrix T^j randomly selected from $\langle B^j\rangle\in\mathcal{E}^{nm}/\!\sim$, where B^j is the basis matrix of the secret image $SI^{(i)}$ that must satisfy the following conditions:

(i) It holds for any B^j and any $\mathcal{Q}^{(i)-}\in\Gamma^{(i)-}_{\mathsf{Qual}}$ that

$$\begin{aligned}&\beta\left(B^j\left[\!\!\left[\mathcal{Q}^{(i)-}\right]\!\!\right]\right)\\ &\sim\left[\,\gamma\left(\mathsf{D}^{(i),j}\right)\gamma\left(\mathsf{D}^{(i),j}\right)\cdots\gamma\left(\mathsf{D}^{(i),j}\right)\;\mathsf{z}\,\mathsf{z}\cdots\mathsf{z}\right].\end{aligned} \tag{19}$$

In the case that $B^j[\![\mathcal{Q}^{(i)-}]\!]$ represents K_ℓ for $\ell\geqq 1$, $\mathsf{k}=\gamma\left(\mathsf{D}^{(i),j}\right)$ appears $\sum_{l=0}^{\ell-1} d^{(i)}_{\mathsf{k},l}$ times in Eq. (19). Note that $d^{(i)}_{\mathsf{k},\ell}$ may depend on $DI^{(i)}$ and k, but not on j. In the case of $\ell=0$, the right hand side of Eq. (19) consists of only z's.

(ii) For any set $\mathcal{X}\subseteq\mathcal{N}$, it holds that $B^j[\![\mathcal{X}]\!]\sim B^{j'}[\![\mathcal{X}]\!]$ for any j and $j'(\neq j)$ satisfying $\boldsymbol{c}^j[\![\mathcal{I}(\mathcal{X})]\!] = \boldsymbol{c}^{j'}[\![\mathcal{I}(\mathcal{X})]\!]$[†]. □

Example 3: In the VSS-2-PI scheme treated in Examples 1 and 2, the basis matrices B^1, B^2, B^3 and B^4 are given by

$$B^1=\begin{bmatrix}\mathsf{zggzzz}\\\mathsf{gzgzzz}\\\mathsf{ggzyrz}\\\mathsf{zzzyzr}\end{bmatrix},\ B^2=\begin{bmatrix}\mathsf{zggzzz}\\\mathsf{zggzzz}\\\mathsf{zggyrz}\\\mathsf{zzzyzr}\end{bmatrix},$$

$$B^3=\begin{bmatrix}\mathsf{zggzzz}\\\mathsf{gzgzzz}\\\mathsf{ggzryz}\\\mathsf{zzzrzy}\end{bmatrix},\ B^4=\begin{bmatrix}\mathsf{zggzzz}\\\mathsf{zggzzz}\\\mathsf{zggryz}\\\mathsf{zzzrzy}\end{bmatrix}. \tag{20}$$

It is easy to check that Eq. (20) satisfies the conditions (i) and (ii) in Def.1. For example, it holds for $\{1,2\}\in\Gamma^{(1)-}_{\mathsf{Qual}}$ that $\beta\left(B^3[\![\{1,2\}]\!]\right)\sim[\mathsf{gzzzzz}]$, and $\beta\left(B^4[\![\{1,2\}]\!]\right)\sim[\mathsf{ggzzzz}]$, $d^{(1)}_{\mathsf{g},0}=1$ and $d^{(1)}_{\mathsf{g},1}=1$. These relations mean that B^3 and B^4 represent G_1 and G_2 on $DI^{(1)}$, respectively. Furthermore, it holds for $\{3,4\}\in\Gamma^{(2)-}_{\mathsf{Qual}}$ that $\beta\left(B^2[\![\{3,4\}]\!]\right)\sim[\mathsf{yzzzzz}]$, $\beta\left(B^4[\![\{3,4\}]\!]\right)\sim[\mathsf{rzzzzz}]$, $d^{(2)}_{\mathsf{y},0}=d^{(2)}_{\mathsf{r},0}=1$, which mean that B^2 and B^4 represent Y_1 and R_1 on $DI^{(2)}$, respectively.

It holds that for $\mathcal{X}_{123}=\{1,2,3\}$, $B^1[\![\mathcal{X}_{123}]\!]\sim B^3[\![\mathcal{X}_{123}]\!]$ and $B^2[\![\mathcal{X}_{123}]\!]\sim B^4[\![\mathcal{X}_{123}]\!]$, i.e., $\mathcal{X}_{123}$ does not leak out the colors of pixels on $DI^{(2)}$. Hence, the basis matrices given by Eq. (20) attains that both $\mathcal{X}_{123}\in\Gamma^{(1)}_{\mathsf{Qual}}$ and $\mathcal{X}_{123}\notin\Gamma^{(2)}_{\mathsf{Qual}}$. Furthermore, it can easily be checked that $B^1[\![\mathcal{F}]\!]\sim B^2[\![\mathcal{F}]\!]\sim B^3[\![\mathcal{F}]\!]\sim B^4[\![\mathcal{F}]\!]$ for any $\mathcal{F}\in\Gamma_{\mathsf{Forb}}$. □

Remark 3: The condition (i) in Def.1 means that any $\mathcal{Q}^{(i)-}\in\Gamma^{(i)-}_{\mathsf{Qual}}$ can decrypt the secret image $SI^{(i)}$. But, $SI^{(i)}$ cannot always be decrypted by stacking all the shares included in $\mathcal{Q}^{(i)}\in\Gamma^{(i)}_{\mathsf{Qual}}$. For instance, in Example 3, $\beta(B^j[\![\mathcal{N}]\!])\sim[\mathsf{zzzzzz}]$ for all j, which does not satisfy the condition (i) in Def.1, although $\mathcal{N}\in\Gamma^{(1)}_{\mathsf{Qual}}$ and $\mathcal{N}\in\Gamma^{(2)}_{\mathsf{Qual}}$. We must select a set $\mathcal{Q}^{(i)-}$ included in $\mathcal{Q}^{(i)}$ to decrypt $SI^{(i)}$. □

Note that $\mathcal{F}\in\Gamma_{\mathsf{Forb}}$ satisfies the following condition from $\mathcal{I}(\mathcal{F})=\emptyset$ and Eq. (6).

(ii)′ For any $\mathcal{F}\in\Gamma_{\mathsf{Forb}}$, all $B^j[\![\mathcal{F}]\!]$, $j=1,2,\ldots,K$, are included in the same equivalence class in $\mathcal{E}^{nm}/\!\sim$.

In the case of the VSS-1-PI scheme, any $\mathcal{X}(\subseteq\mathcal{N})$ satisfies either $\mathcal{X}\in\Gamma^{(1)}_{\mathsf{Qual}}$ or $\mathcal{X}\in\Gamma_{\mathsf{Forb}}$ since the access structure has only two categories $\Gamma^{(1)}_{\mathsf{Qual}}$ and Γ_{Forb}. Hence, in this case, it suffices to consider only the conditions (i) and (ii)′, which coincide with the conditions described in [1], [3], [10] by slight modifications. Based on this consideration, the VSS-q-PI scheme is defined by (i), (ii)′ in [8], [15]. However, the conditions (i) and (ii)′ are not sufficient for $q\geqq 2$ because as shown in the

[†] $\boldsymbol{c}^j[\![\mathcal{I}(\mathcal{X})]\!] = {}^t[\mathsf{D}^{(i_1),j}\ \mathsf{D}^{(i_2),j}\cdots\mathsf{D}^{(i_r),j}]$ if $\mathcal{I}(\mathcal{X})=\{i_1,i_2,\ldots,i_r\}$. $\boldsymbol{c}^j[\![\emptyset]\!]=\boldsymbol{c}^{j'}[\![\emptyset]\!]$ for any j and j'.

following example, the condition (ii)′ does not guarantee that any $\mathcal{X} \notin \Gamma^{(i)}_{\mathsf{Qual}}$ does not leak out any information of the secret image $SI^{(i)}$ even if $\mathcal{X} \in \Gamma^{(i')}_{\mathsf{Qual}}$ for some other secret image $SI^{(i')}$.

Example 4: Consider the access structure given by Eqs. (9)–(11) in Example 1 again. Then, the matrices $\tilde{B}^1, \tilde{B}^2, \tilde{B}^3$, and $\tilde{B}^4$ defined by Eq. (21) satisfy conditions (i) and (ii)′.

$$\tilde{B}^1 = \begin{bmatrix} \mathsf{ggzzzzz} \\ \mathsf{gzgzzzz} \\ \mathsf{zggzyrz} \\ \mathsf{zzzzyzr} \end{bmatrix}, \ \tilde{B}^2 = \begin{bmatrix} \mathsf{zzggzzz} \\ \mathsf{zzggzzz} \\ \mathsf{zzggyrz} \\ \mathsf{zzzzyzr} \end{bmatrix},$$
$$\tilde{B}^3 = \begin{bmatrix} \mathsf{zzggzzz} \\ \mathsf{zgzgzzz} \\ \mathsf{gzzgryz} \\ \mathsf{zzzzrzy} \end{bmatrix}, \ \tilde{B}^4 = \begin{bmatrix} \mathsf{zzggzzz} \\ \mathsf{zzggzzz} \\ \mathsf{zzggryz} \\ \mathsf{zzzzrzy} \end{bmatrix}. \tag{21}$$

Note that $\mathcal{X}_{12} = \{1,2\}$, $\mathcal{X}_{13} = \{1,3\}$, $\mathcal{X}_{23} = \{2,3\}$, $\mathcal{X}_{123} = \{1,2,3\}$ are not included in $\Gamma^{(2)}_{\mathsf{Qual}}$. The above matrices satisfy that

$$\begin{aligned} &\tilde{B}^1[\![\mathcal{X}_{12}]\!] \sim \tilde{B}^3[\![\mathcal{X}_{12}]\!],\ \tilde{B}^2[\![\mathcal{X}_{12}]\!] \sim \tilde{B}^4[\![\mathcal{X}_{12}]\!], \\ &\tilde{B}^1[\![\mathcal{X}_{13}]\!] \sim \tilde{B}^3[\![\mathcal{X}_{13}]\!],\ \tilde{B}^2[\![\mathcal{X}_{13}]\!] \sim \tilde{B}^4[\![\mathcal{X}_{13}]\!], \\ &\tilde{B}^1[\![\mathcal{X}_{23}]\!] \sim \tilde{B}^3[\![\mathcal{X}_{23}]\!],\ \tilde{B}^2[\![\mathcal{X}_{23}]\!] \sim \tilde{B}^4[\![\mathcal{X}_{23}]\!]. \end{aligned} \tag{22}$$

Hence, any one of $\mathcal{X}_{12}$, $\mathcal{X}_{13}$, $\mathcal{X}_{23}$ does not leak out any information about $DI^{(2)}$. But, it holds that $\tilde{B}^1[\![\mathcal{X}_{123}]\!] \not\sim \tilde{B}^3[\![\mathcal{X}_{123}]\!]$, $\beta(\tilde{B}^1[\![\mathcal{X}_{123}]\!]) \sim [\mathsf{zzzzzz}]$ and $\beta(\tilde{B}^3[\![\mathcal{X}_{123}]\!]) \sim [\mathsf{gzzzzz}]$. This means that for pixels with G_1 on $DI^{(1)}$, we can distinguish yellow pixels from red pixels on $DI^{(2)}$, which correspond to $\tilde{B}^1$ and $\tilde{B}^3$, respectively, by investigating the shares of $\mathcal{X}_{123}$. Hence, the matrices given by Eq. (21) are inadequate for the basis matrices. On the contrary, the basis matrices B^1, B^2, B^3 and B^4 given by Eq. (20) satisfy $B^1[\![\mathcal{X}_{123}]\!] \sim B^3[\![\mathcal{X}_{123}]\!]$ and $B^2[\![\mathcal{X}_{123}]\!] \sim B^4[\![\mathcal{X}_{123}]\!]$. □

3. Construction Method of VSS-q-PI Scheme

3.1 Construction Method

In this subsection, we describe a method to construct the $(\Gamma, \mathcal{N}, \mathcal{E}, \boldsymbol{D})$-VSS-$q$-PI scheme.

First, for a given access structure Γ, define $\tilde{\Gamma}^{(i)}_{\mathsf{Qual}}$ and $\tilde{\Gamma}^{(i)}_{\mathsf{Forb}}$ as follows.

$$\tilde{\Gamma}^{(i)}_{\mathsf{Qual}} = \{\mathcal{Q}^{(i)} \in \Gamma^{(i)}_{\mathsf{Qual}} : \mathcal{Q}^{(i)} \subseteq \mathcal{N}^{(i)}\}, \tag{23}$$
$$\tilde{\Gamma}^{(i)}_{\mathsf{Forb}} = \{\mathcal{F} \subset \mathcal{N}^{(i)} : \mathcal{F} \notin \Gamma^{(i)}_{\mathsf{Qual}}\}. \tag{24}$$

It is easy to check that $\tilde{\Gamma}^{(i)}_{\mathsf{Qual}} \cap \tilde{\Gamma}^{(i)}_{\mathsf{Forb}} = \emptyset$, $\tilde{\Gamma}^{(i)}_{\mathsf{Qual}} \cup \tilde{\Gamma}^{(i)}_{\mathsf{Forb}} = 2^{\mathcal{N}^{(i)}}$, $\tilde{\Gamma}^{(i)}_{\mathsf{Qual}}$ and $\tilde{\Gamma}^{(i)}_{\mathsf{Forb}}$ have the monotonicity in the same way as $\Gamma^{(i)}_{\mathsf{Qual}}$ and Γ_{Forb}, respectively. Therefore, $\Gamma^{(i)} = (\tilde{\Gamma}^{(i)}_{\mathsf{Qual}}, \tilde{\Gamma}^{(i)}_{\mathsf{Forb}})$ can be considered as an access structure of the VSS-1-PI scheme with the secret image $SI^{(i)}$ for the share set $\mathcal{N}^{(i)}$. Then, letting $\mathcal{E}^{(i)}$ be the set of colors necessary to encrypt $SI^{(i)}$, the basis matrices of the $(\Gamma^{(i)}, \mathcal{N}^{(i)}, \mathcal{E}^{(i)}, \boldsymbol{r}^{(i)})$-VSS-1-PI scheme can be constructed by the known methods proposed in [1], [3], [6], [7], [9]–[12] with slight modifications. See the Appendix for more details. In such construction, letting $|\mathcal{N}^{(i)}| \times m^{(i)}$ matrices $U^{(i),j}$, for $j = 1, 2, \ldots, K$, be the basis matrices of the $(\Gamma^{(i)}, \mathcal{N}^{(i)}, \mathcal{E}^{(i)}, \boldsymbol{r}^{(i)})$-VSS-1-PI scheme, where $m^{(i)}$ is the pixel expansion for the secret image $SI^{(i)}$, then $U^{(i),j}$ represents a color $\mathsf{D}^{(i),j}$ and satisfies that $U^{(i),j} = U^{(i),j'}$ if $\mathsf{D}^{(i),j}$ and $\mathsf{D}^{(i),j'}$ are the same color. Furthermore, the basis matrix $U^{(i),j}$ satisfies conditions (i), (ii)′, i.e., the number of $\gamma(\mathsf{D}^{(i),j})$ included in $\beta(U^{(i),j}[\![\mathcal{Q}^{(i)-}]\!])$, $\sum_{l=0}^{\ell-1} d^{(i)}_{\gamma(\mathsf{D}^{(i),j}),l}$, is constant for any $\mathcal{Q}^{(i)-} \in \Gamma^{(i)-}_{\mathsf{Qual}}$, and it holds that $U^{(i),1}[\![\mathcal{F}^{(i)}]\!] \sim U^{(i),2}[\![\mathcal{F}^{(i)}]\!] \sim \cdots \sim U^{(i),K}[\![\mathcal{F}^{(i)}]\!]$ for any $\mathcal{F}^{(i)} \in \Gamma^{(i)}_{\mathsf{Forb}}$.

Next, we construct an $n \times m^{(i)}$ matrix $V^{(i),j}$ defined by

$$V^{(i),j}\left[\!\left[\mathcal{N}^{(i)}\right]\!\right] = U^{(i),j}, \tag{25}$$
$$V^{(i),j}\left[\!\left[\overline{\mathcal{N}^{(i)}}\right]\!\right] = J, \tag{26}$$

where the matrix J consists of only z's and $\overline{\mathcal{N}^{(i)}}$ means the complement set of $\mathcal{N}^{(i)}$ on $\mathcal{N}$. Then we construct $n \times m$ basis matrices B^j, $j = 1, 2, \ldots, K$, by

$$B^j = \bigodot_{i=1}^{q} V^{(i),j}, \tag{27}$$

where $m = \sum_{i=1}^{q} m^{(i)}$.

We now consider two categories Δ_1 and Δ_2 for the access structures of the VSS-q-PI schemes.

Definition 2:

(i) An access structure Γ is in Δ_1 if it satisfies $\mathcal{Q}^{(i)-} \cap \overline{\mathcal{N}^{(i')}} \neq \emptyset$ for any i and i' such that $\mathcal{Q}^{(i)-} \in \Gamma^{(i)-}_{\mathsf{Qual}}$ and $i' \in \mathcal{I}(\mathcal{Q}^{(i)-}) \backslash \{i\}$.

(ii) An access structure Γ is in Δ_2 if it satisfies that $\mathcal{Q}^{(i)-} \cap \overline{\mathcal{N}^{(i')}} \neq \emptyset$ for any i and $i' (\neq i)$. □

Remark 4: It is obvious from the above definition that $\Delta_2 \subset \Delta_1$, and it holds generally that $\Delta_2 \subsetneq \Delta_1$. Furthermore, there exist access structures that are not included in Δ_1. □

Example 5: Assume that an access structure Γ_{ID} is defined by

$$\Gamma_{\mathsf{Forb}} = \{\{2\}\}, \tag{28}$$
$$\Gamma^{(1)-}_{\mathsf{Qual}} = \{\{1\}\}, \tag{29}$$

$$\Gamma^{(2)-}_{\mathsf{Qual}} = \{\{1,2\}\}. \tag{30}$$

Then, Γ_{ID} does not belong to Δ_1, and hence, nor Δ_2. From Eq. (29), the secret image $SI^{(1)}$ can be obtained only from share 1. Hence, $SI^{(1)}$ can be considered as the identification (ID) image of share 1 although $SI^{(2)}$ is the secret image. The above access structure Γ_{ID} is a modified version of the $(2,2)$-VSS scheme with two ID images [2], [12], and note that the VSS-q-PI schemes include such VSS schemes with ID images as a special case.

Next, consider the access structure Γ_g treated in [15], which is given by

$$\Gamma_{\mathsf{Forb}} = \{\{1\},\{2\},\{3\},\{4\},\{5\}\}, \tag{31}$$

$$\Gamma^{(1)-}_{\mathsf{Qual}} = \{\{1,2\},\{1,5\},\{2,3\},\{3,4\},\{4,5\}\}, \tag{32}$$

$$\Gamma^{(2)-}_{\mathsf{Qual}} = \{\{1,3\},\{1,4\},\{2,4\},\{2,5\},\{3,5\}\}. \tag{33}$$

Then, Γ_g is included in Δ_1 but not in Δ_2. □

Theorem 1: B^j, $j = 1, 2, \ldots, K$, given by Eq. (27) are the basis matrices of the $(\Gamma, \mathcal{N}, \mathcal{E}, \boldsymbol{D})$-VSS-$q$-PI scheme, if $|\mathcal{E}| = 2$ and $\Gamma \in \Delta_1$, or if $|\mathcal{E}| \geqq 3$ and $\Gamma \in \Delta_2$. □

Example 6: We show how the basis matrices given by Eq. (20) can be derived from Theorem 1 for the access structures Γ given by Eqs. (9)–(11) in Example 1 and the color matrix $\boldsymbol{D}$ given by Eq. (13) in Example 2. Note that the access structure Γ belongs to Δ_2. From Eqs. (23), (24), we have $\tilde{\Gamma}^{(1)}_{\mathsf{Forb}} = \{\{1\},\{2\},\{3\}\}$ and $\tilde{\Gamma}^{(2)}_{\mathsf{Forb}} = \{\{3\},\{4\}\}$. Then the basis matrices $U^{(i),j}$ of $(\Gamma^{(1)}, \mathcal{N}^{(1)}, \mathcal{E}^{(1)}, \boldsymbol{r}^{(1)})$-VSS-1-PI scheme and $(\Gamma^{(2)}, \mathcal{N}^{(2)}, \mathcal{E}^{(2)}, \boldsymbol{r}^{(2)})$-VSS-1-PI scheme are given by

$$U^{(1),1} = U^{(1),3} = \begin{bmatrix} \mathsf{zbb} \\ \mathsf{bzb} \\ \mathsf{bbz} \end{bmatrix},\ U^{(1),2} = U^{(1),4} = \begin{bmatrix} \mathsf{zbb} \\ \mathsf{zbb} \\ \mathsf{zbb} \end{bmatrix},$$

and

$$U^{(2),1} = U^{(2),2} = \begin{bmatrix} \mathsf{yzr} \\ \mathsf{yrz} \end{bmatrix},\ U^{(2),3} = U^{(2),4} = \begin{bmatrix} \mathsf{ryz} \\ \mathsf{rzy} \end{bmatrix}, \tag{34}$$

respectively. Hence we obtain from Eqs. (25), (26) that

$$V^{(1),1} = V^{(1),3} = \begin{bmatrix} \mathsf{zbb} \\ \mathsf{zbb} \\ \mathsf{zbb} \\ \mathsf{zzz} \end{bmatrix},\ V^{(1),2} = V^{(1),4} = \begin{bmatrix} \mathsf{zbb} \\ \mathsf{bzb} \\ \mathsf{bbz} \\ \mathsf{zzz} \end{bmatrix},$$
$$V^{(2),1} = V^{(2),2} = \begin{bmatrix} \mathsf{zzz} \\ \mathsf{zzz} \\ \mathsf{ryz} \\ \mathsf{rzy} \end{bmatrix},\ V^{(2),3} = V^{(2),4} = \begin{bmatrix} \mathsf{zzz} \\ \mathsf{zzz} \\ \mathsf{yzr} \\ \mathsf{yrz} \end{bmatrix}. \tag{35}$$

Finally, basis matrices B^1, B^2, B^3 and B^4 are given from Eq. (27) as follows.

$$B^1 = V^{(1),1} \odot V^{(2),1},\ B^2 = V^{(1),2} \odot V^{(2),2},$$
$$B^3 = V^{(1),3} \odot V^{(2),3},\ B^4 = V^{(1),4} \odot V^{(2),4}, \tag{36}$$

which is equivalent to Eq. (20). □

Remark 5: In [15], it is shown that the access structure Γ_g given by Eqs. (31)–(33) in Example 5 can be represented by a graph. In the case of $|\mathcal{E}| = 2$, as treated in [15], Eq. (27) gives the basis matrices. But in the case of $|\mathcal{E}| \geqq 3$, Eq. (27) does not give the basis matrices for Γ_g generally because Γ_g does not satisfy the condition of Theorem 1, i.e., $\Gamma_g \notin \Delta_2$. □

3.2 Proof of Theorem 1

In this subsection, we prove Theorem 1. We first show that matrices $V^{(i),j}$ given by Eqs. (25), (26) satisfy the next lemma.

Lemma 1: For any $i \notin \mathcal{I}(\mathcal{X})$, it holds that

$$V^{(i),1}\llbracket\mathcal{X}\rrbracket \sim V^{(i),2}\llbracket\mathcal{X}\rrbracket \sim \cdots \sim V^{(i),K}\llbracket\mathcal{X}\rrbracket. \tag{37}$$

□

Proof of Lemma 1: From Eq. (18), we note that $\mathcal{X} \in \tilde{\Gamma}^{(i)}_{\mathsf{Forb}}$ if $i \notin \mathcal{I}(\mathcal{X})$. Hence, from the monotonicity of $\tilde{\Gamma}^{(i)}_{\mathsf{Forb}}$, it holds that $\mathcal{X} \cap \mathcal{N}^{(i)} \in \tilde{\Gamma}^{(i)}_{\mathsf{Forb}}$ for $i \notin \mathcal{I}(\mathcal{X})$.

$V^{(i),j}\llbracket\mathcal{X}\rrbracket$ can be represented as

$$V^{(i),j}\llbracket\mathcal{X}\rrbracket = V^{(i),j}\left\llbracket\left(\mathcal{X} \cap \mathcal{N}^{(i)}\right) \cup \left(\mathcal{X} \cap \overline{\mathcal{N}^{(i)}}\right)\right\rrbracket. \tag{38}$$

In Eq. (38), it holds for $i \notin \mathcal{I}(\mathcal{X})$ that $V^{(i),1}\llbracket\mathcal{X} \cap \mathcal{N}^{(i)}\rrbracket \sim V^{(i),2}\llbracket\mathcal{X} \cap \mathcal{N}^{(i)}\rrbracket \sim \cdots \sim V^{(i),K}\llbracket\mathcal{X} \cap \mathcal{N}^{(i)}\rrbracket$ since $V^{(i),j}\llbracket\mathcal{N}^{(i)}\rrbracket$ satisfies Eq. (25) and $\mathcal{X} \cap \mathcal{N}^{(i)} \in \tilde{\Gamma}^{(i)}_{\mathsf{Forb}}$. On the other hand, from Eq. (26), all the elements of $V^{(i),j}\llbracket\mathcal{X} \cap \overline{\mathcal{N}^{(i)}}\rrbracket$ are z for every j. Therefore, Eq. (37) holds for any $i \notin \mathcal{I}(\mathcal{X})$. □

Proof of Theorem 1: First, we show that B^j given by Eq. (27) satisfies the condition (i) in Def.1. Substituting Eq. (27) into $\beta(B^j\llbracket\mathcal{Q}^{(i)-}\rrbracket)$, we have

$$\begin{aligned} \beta\left(B^j\llbracket\mathcal{Q}^{(i)-}\rrbracket\right) &= \beta\left(\bigodot_{i'=1}^{q} V^{(i'),j}\llbracket\mathcal{Q}^{(i)-}\rrbracket\right) \\ &\sim \beta(V^{(i),j}\llbracket\mathcal{Q}^{(i)-}\rrbracket) \odot \beta\left(\bigodot_{\substack{i'=1 \\ i' \neq i}}^{q} V^{(i'),j}\llbracket\mathcal{Q}^{(i)-}\rrbracket\right) \\ &\sim \beta(U^{(i),j}\llbracket\mathcal{Q}^{(i)-}\rrbracket) \odot \beta(X^{(i),j}) \odot \beta(Y^{(i),j}), \end{aligned} \tag{39}$$

where $X^{(i),j}$ and $Y^{(i),j}$ are defined as

$$X^{(i),j} = \bigodot_{i' \in \mathcal{I}(\mathcal{Q}^{(i)-}) \setminus \{i\}} V^{(i'),j}\llbracket\mathcal{Q}^{(i)-}\rrbracket, \tag{40}$$

$$Y^{(i),j} = \bigodot_{i' \notin \mathcal{I}(\mathcal{Q}^{(i)-})} V^{(i'),j}[\![\mathcal{Q}^{(i)-}]\!]. \tag{41}$$

Note that since $U^{(i),j}$ is the basis matrix of $(\Gamma^{(i)}, \mathcal{N}^{(i)}, \mathcal{E}^{(i)}, \boldsymbol{r}^{(i)})$-VSS-1-PI schemes, it satisfies the condition (i) in Def.1 for the $(\Gamma^{(i)}, \mathcal{N}^{(i)}, \mathcal{E}^{(i)}, \boldsymbol{r}^{(i)})$-VSS-1-PI scheme. First consider the case of $|\mathcal{E}| = 2$ with $\mathcal{E} = \{\mathsf{z}, \mathsf{k}\}$. In this case, $\beta(U^{(i),j})$, $\beta(X^{(i),j})$, and $\beta(Y^{(i),j})$ are vectors with two colors, k and z. Hence, if for each i, $\beta(X^{(i),j}) \odot \beta(Y^{(i),j})$ are equivalent with respect to $\sim$ for any j, Eq. (19) is satisfied for $\beta(B^j[\![\mathcal{Q}^{(i)-}]\!])$. From Lemma 1, we have that

$$V^{(i'),1}[\![\mathcal{Q}^{(i)-}]\!] \sim V^{(i'),2}[\![\mathcal{Q}^{(i)-}]\!] \sim \cdots \sim V^{(i'),K}[\![\mathcal{Q}^{(i)-}]\!] \tag{42}$$

for any $i' \notin \mathcal{I}(\mathcal{Q}^{(i)-})$. Hence, for each i, $\beta(Y^{(i),j})$ are equivalent for any j. Furthermore, for any $i' \in \mathcal{I}(\mathcal{Q}^{(i)-}) \backslash \{i\}$, $\beta(V^{(i'),j}[\![\mathcal{Q}^{(i)-}]\!])$ can be represented as

$$\begin{aligned} &\beta(V^{(i'),j}[\![\mathcal{Q}^{(i)-}]\!]) \\ &= \beta\left(V^{(i'),j}\left[\!\!\left[\left(\mathcal{Q}^{(i)-} \cap \mathcal{N}^{(i')}\right) \cup \left(\mathcal{Q}^{(i)-} \cap \overline{\mathcal{N}^{(i')}}\right)\right]\!\!\right]\right). \end{aligned} \tag{43}$$

Since Eq. (26) holds and we have that $\mathcal{Q}^{(i)-} \cap \overline{\mathcal{N}^{(i')}} \neq \emptyset$ for such i' from the assumption $\Gamma \in \Delta_1$ in Theorem 1, $\beta(V^{(i'),j}[\![\mathcal{Q}^{(i)-}]\!])$ consists of only z's. Hence, all $\beta(X^{(i),j})$ are also equivalent for any j.

In the case of $|\mathcal{E}| \geqq 3$, $\beta(X^{(i),j})$ and $\beta(Y^{(i),j})$ may have three or more colors, and hence Eq. (19) may not be satisfied even if $\beta(X^{(i),j}) \odot \beta(Y^{(i),j})$ are equivalent for any j. But, because for any $i' \neq i$, $\mathcal{Q}^{(i)-} \cap \overline{\mathcal{N}^{(i')}} \neq \emptyset$ in Eq. (43) holds from the assumption $\Gamma \in \Delta_2$ in Theorem 1, all elements in $\beta(X^{(i),j}) \odot \beta(Y^{(i),j})$ are z from Eq. (26). Hence, Eq. (19) holds for $\beta(B^j[\![\mathcal{Q}^{(i)-}]\!])$.

Next, let us check that B^j's satisfy the condition (ii) in Def.1. $B^j[\![\mathcal{X}]\!]$ can be represented as

$$\begin{aligned} B^j[\![\mathcal{X}]\!] &= \bigodot_{i=1}^{q} V^{(i),j}[\![\mathcal{X}]\!] \\ &\sim \left[\bigodot_{i \in \mathcal{I}(\mathcal{X})} V^{(i),j}[\![\mathcal{X}]\!]\right] \odot \left[\bigodot_{i \notin \mathcal{I}(\mathcal{X})} V^{(i),j}[\![\mathcal{X}]\!]\right]. \end{aligned} \tag{44}$$

Suppose for a set $\mathcal{X} \subseteq \mathcal{N}$ that j and $j' (\neq j)$ satisfy $\boldsymbol{c}^j[\![\mathcal{I}(\mathcal{X})]\!] = \boldsymbol{c}^{j'}[\![\mathcal{I}(\mathcal{X})]\!]$, which means that $\mathsf{D}^{(i),j} = \mathsf{D}^{(i),j'}$ for any $i \in \mathcal{I}(\mathcal{X})$. Then, it holds that $U^{(i),j} = U^{(i),j'}$ from the definition of $U^{(i),j}$, and hence $V^{(i),j} = V^{(i),j'}$ from Eqs. (25), (26). Furthermore, for any $i \notin \mathcal{I}(\mathcal{X})$, it holds from Lemma 1 that $V^{(i),1}[\![\mathcal{X}]\!] \sim V^{(i),2}[\![\mathcal{X}]\!] \sim \cdots \sim V^{(i),K}[\![\mathcal{X}]\!]$. Therefore, it holds that $B^j[\![\mathcal{X}]\!] \sim B^{j'}[\![\mathcal{X}]\!]$. □

4. Construction Method by Duplicating Secret Images

In the previous sections, we have shown how to construct the VSS-q-PI schemes for the case that the access structures Γ are included in Δ_1 or Δ_2 for $|\mathcal{E}| = 2$ or $|\mathcal{E}| \geqq 3$, respectively. In this section, we treat the case that Γ is not included in Δ_1 or Δ_2.

In the previous sections, we assumed that all the secret images are different. But we note that even if some secret images are the same, we can encrypt the plural secret images including the same images in the same way as the case of all different secret images.

Suppose that an access structure $\Gamma = (\{\Gamma_{\mathsf{Qual}}^{(i)}\}_{i=1}^{q}, \Gamma_{\mathsf{Forb}})$ is given, which may not be included in Δ_1 nor Δ_2. For this Γ, we consider the union of all $\Gamma_{\mathsf{Qual}}^{(i)-}$. Let us assume that the union has $\hat{q}$ elements $\hat{\mathcal{Q}}^{(i)-}$, $i = 1, 2, \ldots, \hat{q}$, i.e.,

$$\bigcup_{i=1}^{q} \Gamma_{\mathsf{Qual}}^{(i)-} = \{\hat{\mathcal{Q}}^{(1)-}, \hat{\mathcal{Q}}^{(2)-}, \ldots, \hat{\mathcal{Q}}^{(\hat{q})-}\}. \tag{45}$$

Then, for each $\hat{\mathcal{Q}}^{(i)-}$, we define $\hat{\Gamma}_{\mathsf{Qual}}^{(i)-}$ by

$$\hat{\Gamma}_{\mathsf{Qual}}^{(i)-} = \{\hat{\mathcal{Q}}^{(i)-}\} \ \text{ for } \ 1 \leqq i \leqq \hat{q}. \tag{46}$$

For such $\{\hat{\Gamma}_{\mathsf{Qual}}^{(i)-}\}_{i=1}^{\hat{q}}$, we can define a new access structure $\hat{\Gamma} = (\{\hat{\Gamma}_{\mathsf{Qual}}^{(i)}\}_{i=1}^{\hat{q}}, \Gamma_{\mathsf{Forb}})$ for the set of secret images, $\hat{SI}^{(i)}$, $i = 1, 2, \ldots, \hat{q}$, some of which may be the same image. Furthermore, we define the set of significant shares $\hat{\mathcal{N}}^{(i)}$ for $\hat{SI}^{(i)}$ like Eq. (8), the set of colors $\hat{\mathcal{D}}^{(i)}$, and the color matrix $\hat{\boldsymbol{D}}$.

Note that the forbidden sets of $\hat{\Gamma}$ are the same as Γ, and it holds that $\hat{\mathcal{Q}}^{(i)-} = \hat{\mathcal{N}}^{(i)}$ for all i.

Remark 6: In the case of $\Gamma_{\mathsf{Forb}} = \{\emptyset\}$, $\hat{\Gamma}$ coincides with the access structure proposed in [5] for black-white plural secret images. Furthermore, applying Eqs. (45), (46) to the access structure of VSS-1-PI scheme for a black-white secret image, the basis matrix obtained by Eq. (27) coincides with the basis matrix given in [4]. □

Lemma 2: For the access structure $\hat{\Gamma}$, the following two statements hold.

1. For any $i' \in \mathcal{I}(\hat{\mathcal{Q}}^{(i)-}) \backslash \{i\}$, it holds that $\hat{\mathcal{Q}}^{(i)-} \cap \overline{\hat{\mathcal{N}}^{(i')}} \neq \emptyset$.
2. If

$$\mathcal{I}(\hat{\mathcal{Q}}^{(i)-}) = \{i\}, \tag{47}$$

then it holds that $\hat{\mathcal{Q}}^{(i')-} \cap \overline{\hat{\mathcal{N}}^{(i)}} \neq \emptyset$ for any $i' (\neq i)$. □

Proof of Lemma 2: Note from the definition of

$\hat{\mathcal{Q}}^{(i)-}$ that $\hat{\mathcal{Q}}^{(i)-} \neq \hat{\mathcal{Q}}^{(i')-}$ for any $i \neq i'$.

1. For any $i' \in \mathcal{I}(\hat{\mathcal{Q}}^{(i)-})\backslash\{i\}$, it holds that $\hat{\mathcal{Q}}^{(i)-} \supsetneq \hat{\mathcal{Q}}^{(i')-} = \hat{\mathcal{N}}^{(i')}$, which means that $\hat{\mathcal{Q}}^{(i)-}\cap\overline{\hat{\mathcal{N}}^{(i')}} \neq \emptyset$.
2. Suppose that $\hat{\mathcal{Q}}^{(i')-}\cap\overline{\hat{\mathcal{N}}^{(i)}} = \hat{\mathcal{Q}}^{(i')-}\cap\overline{\hat{\mathcal{Q}}^{(i)-}} = \emptyset$ for some $i'(\neq i)$. Then we have that $\hat{\mathcal{Q}}^{(i')-} \subsetneq \hat{\mathcal{Q}}^{(i)-}$, which implies that $i' \in \mathcal{I}(\hat{\mathcal{Q}}^{(i)-})\backslash\{i\}$ and violates Eq. (47). □

From Lemma 2 and Theorem 1, the next theorem holds for the access structure $\hat{\Gamma}$.

Theorem 2: Suppose that the access structure $\hat{\Gamma}$ is constructed by Eqs. (45), (46) from Γ. Then, in the case of $|\mathcal{E}| = 2$, or in the case that $|\mathcal{E}| \geqq 3$ and $\hat{\Gamma}$ satisfies Eq. (47) for all i, the basis matrices of $(\hat{\Gamma}, \mathcal{N}, \mathcal{E}, \hat{\boldsymbol{D}})$-VSS-$q$-PI scheme can be obtained by Eq. (27). □

Theorem 2 implies that the basis matrices of the VSS-q-PI scheme with the access structure $\hat{\Gamma}$ can always be constructed by Eq. (27) if $|\mathcal{E}| = 2$. However, in the case of $|\mathcal{E}| \geqq 3$, if the access structure requires ID images, we cannot obtain the basis matrices of the access structure from Eq. (27) because $\hat{\mathcal{Q}}^{(i)-}$ must reproduce the ID image and the secret image, and hence, Eq. (47) does not hold. The VSS scheme with color ID images is proposed for $|\mathcal{E}| \geqq 3$ in [12], where the basis matrices not satisfying Eq. (19) are used.

Finally, we note that for the construction shown in the Appendix, pixel expansion m is given from Eq. (A$\cdot$16) by

$$m = \sum_{i=1}^{\hat{q}} m^{(i)} = \sum_{i=1}^{\hat{q}} \sum_{\mathsf{k}\in\mathcal{E}^{(i)}} \sum_{l=0}^{L_{\mathsf{k}}-1} d_{\mathsf{k},l}^{(i)}\ 2^{|\hat{\mathcal{N}}^{(i)}|-1}. \quad (48)$$

For example, the pixel expansion of the VSS-2-PI scheme with the access structure given by Eqs. (31)–(33) for black-white secret images is 12 if the method shown in Sect. 3 is used with the star graph decomposition [15]. But, if we use Eqs. (45), (46), we have $\hat{q} = 10$, and the pixel expansion becomes 20 from Eq. (48). In general, the pixel expansion attained by the method shown in this section is larger than the method in Sect. 3. However, it is reported that the VSS scheme with 144(= 12 × 12) subpixels can be used [13], and hence, it is not hard to use the VSS-2-PI with 20 subpixels in practice.

5. Comparison with Trivial Schemes

In the framework of the VSS-q-PI scheme, we assume that each participant has one share. But, in some cases each participant may be allowed to have two or more shares. In such cases, VSS schemes for q plural secret images can easily be constructed by using q individual usual VSS schemes, i.e., VSS-1-PI schemes, with the access structure $\Gamma^{(i)} = (\tilde{\Gamma}_{\mathsf{Qual}}^{(i)}, \tilde{\Gamma}_{\mathsf{Forb}}^{(i)})$ for each secret image $SI^{(i)}$. In such trivial VSS schemes, shares $\{s_1^{(i)}\ s_2^{(i)}, \ldots, s_n^{(i)}\}$ are constructed for the i-th secret image, and the ℓ-th participant has the share set $\{s_\ell^{(1)}, s_\ell^{(2)}, \ldots, s_\ell^{(q)}\}$. In this section we compare the VSS-q-PI schemes with such trivial schemes.

The trivial schemes can realize any access structures although the VSS-q-PI schemes cannot realize them if they don't satisfy the conditions described in Theorems 1 or 2. Furthermore, the pixel expansion of the trivial scheme is less than the VSS-q-PI scheme for the same access structure. This means that the trivial schemes attain higher resolution than the VSS-q-PI schemes in decrypted images. However, in the trivial schemes each participant must hold securely q plural shares. On the contrary, each participant must hold securely only one share in the VSS-q-PI scheme.

Furthermore, the VSS-q-PI schemes have the following advantages compared with the trivial schemes.

1. The VSS scheme with the ID images [2], [12], which is considered as a special case of the VSS-q-PI scheme, cannot be realized by the trivial scheme[†].
2. Consider the case that a lot with *win* and *lose* is made by a VSS scheme, where secret images $SI^{(W)}$ and $SI^{(L)}$ represent *win* and *lose*, respectively.

   In the case of the trivial scheme, letting $\mathcal{S}^{(W)} = \{s_1^{(W)}, s_2^{(W)}\}$ and $\mathcal{S}^{(L)} = \{s_1^{(L)}, s_2^{(L)}\}$ be the share sets of the $(2,2)$-threshold VSS-1-PI scheme for the secret images $SI^{(W)}$ and $SI^{(L)}$, respectively, the lot can be realized if a dealer holds $\{s_1^{(W)}, s_1^{(L)}\}$ and distributes $s_2^{(W)}$ or $s_2^{(L)}$ to people participating in the lot. In this case, two times decryption, i.e., stacking the shares, is required to know the result of the lot.

   On the contrary, in the case of the VSS-q-PI scheme, we can use the access structure $\Gamma^{(W,L)}$ with $\Gamma_{\mathsf{Qual}}^{(W)-} = \{\{1,2\}\}$, $\Gamma_{\mathsf{Qual}}^{(L)-} = \{\{1,3\}\}$ and $\Gamma_{\mathsf{Forb}}^{+} = \{\{2,3\}\}$. Letting $\{s_1, s_2, s_3\}$ be the share set, a dealer holds s_1 and distributes s_2 or s_3 to the people. In this case, by only once decryption, we can know the result of the lot[††].

   This advantage of speedy decryption becomes larger as the number of results in the lot becomes larger, and the advantage is essential in commercial uses.
3. Next, consider a case that a VSS scheme is used as a tally. We have groups X, Y, Z, and Alice, Bob and Carol belong to X and Y, X and Z, Y, respectively. Each of them wants to prove to Peggy

[†] The VSS schemes with color ID images are treated in [12]. However, the VSS schemes with color ID images cannot be constructed by our method. See the next paragraph of Theorem 2.

[††] This kind of lot is now commercialized by TOPPAN PRINTING co., ltd.

which groups he/she belongs to. In the case of the trivial schemes, the tally can be realized by letting $\mathcal{S}^{(X)} = \{s_1^{(X)}, s_2^{(X)}\}$, $\mathcal{S}^{(Y)} = \{s_1^{(Y)}, s_2^{(Y)}\}$, and $\mathcal{S}^{(Z)} = \{s_1^{(Z)}, s_2^{(Z)}\}$ be the sets of shares of the $(2,2)$-threshold VSS-1-PI schemes for the secret images $SI^{(X)}, SI^{(Y)}, SI^{(Z)}$, respectively, and distributing the sets $\{s_1^{(X)}, s_1^{(Y)}, s_1^{(Z)}\}$, $\{s_2^{(X)}, s_2^{(Y)}\}$, $\{s_2^{(X)}, s_2^{(Z)}\}$, and $s_2^{(Y)}$, to Peggy, Alice, Bob, and Carol, respectively.

In the case of the VSS-q-PI scheme, the tally can be realized by letting $\{s_1, s_2, \ldots, s_6\}$ be the share set of the VSS-q-PI scheme for the access structure given by $\Gamma_{\mathsf{Qual}}^{(X)-} = \{\{1,4\},\{1,5\}\}$, $\Gamma_{\mathsf{Qual}}^{(Y)-} = \{\{2,4\},\{2,6\}\}$, and $\Gamma_{\mathsf{Qual}}^{(Z)-} = \{\{3,5\}\}$, and distributing the shares $\{s_1, s_2, s_3\}$, s_4, s_5, s_6 to Peggy, Alice, Bob, and Carol, respectively.

In either case, by showing his/her shares to Peggy, each person can prove the groups that he/she belongs to. However, note that, for instance, the following attacks are possible in the case of the trivial scheme although the same attacks cannot succeed in the case of VSS-q-PI scheme.

(a) If Alice conspires with Bob, Alice can deceive Peggy by showing $\{s_2^{(X)}, s_2^{(Y)}, s_2^{(Z)}\}$ to prove that Alice belongs to all of X, Y, Z. (b) Bob can hide by showing only $s_2^{(Z)}$ that he belongs to X. (c) Assume that an adversary wants to impersonate Alice. Such impersonation attack can be achieved by stealing $s_2^{(X)}$ from Bob and $s_2^{(Y)}$ from Carol besides by stealing $\{s_2^{(X)}, s_2^{(Y)}\}$ from Alice.

As shown above, the VSS-q-PI schemes have advantages than the trivial schemes in many cases.

6. Conclusion

In this paper, we considered a method to construct visual secret sharing schemes for q plural secret images (VSS-q-PI scheme) with general access structures. In the proposed VSS-q-PI schemes, each qualified set of shares can decrypt their own secret images, but it does not leak out any information of the other secret images. Furthermore, the proposed scheme can encode color and/or gray-scale secret images in addition to black-white images. Finally in Sect. 5, we discussed the merits of the VSS-q-PI schemes compared with the trivial schemes.

Acknowledgments

The authors thank Dr. Hiroki Koga for his helpful comments. The work of H. Yamamoto was supported in part by the MEXT Grants-in-Aid for Scientific Research No.14019028 and No.15017227.

References

[1] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, "Visual cryptography for general access structures," Inf. Comput., vol.129, pp.86–106, 1996.

[2] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, "Extended capabilities for visual cryptography," Theoretical Computer Science, vol.250, no.1–2, pp.143–161, 2001.

[3] C. Blundo, A. De Santis, and M. Naor, "Visual cryptography for gray-level images," Inf. Process. Lett., vol.75, Issue 6, pp.255–259, 2001.

[4] C. Blundo, A. De Bonis, and A. De Santis, "Improved schemes for visual cryptography," Designs, Codes and Cryptography, 24, pp.255–278, 2001.

[5] S. Droste, "New results on visual cryptography," Advances in Cryptology-CRYPTO'96, LNCS-1109, pp.401–15, Springer-Verlag, 1996.

[6] M. Itoh, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing general access structure," IEEE Globcom'87, pp.99–102, 1987.

[7] M. Iwamoto and H. Yamamoto, "The optimal n-out-of-n visual secret sharing scheme for gray-scale images," IEICE Trans. Fundamentals, vol.E85-A, no.10, pp.2238–2247, Oct. 2002.

[8] T. Kato and H. Imai, "An extended construction method of visual secret sharing scheme," IEICE Trans. Fundamentals (Japanese Edition), vol.J79-A, no.8, pp.1344–1351, Aug. 1996.

[9] H. Koga and H. Yamamoto, "Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images," IEICE Trans. Fundamentals, vol.E81-A, no.6, pp.1262–1269, June 1998.

[10] H. Koga, M. Iwamoto, and H. Yamamoto, "An analytic construction of the visual secret sharing scheme for color images," IEICE Trans. Fundamentals, vol.E84-A, no.1, pp.262–272, Jan. 2001.

[11] H. Kuwakado and H. Tanaka, "Polynomial representation of visual secret sharing scheme and its application," IEICE Trans. Fundamentals, vol.E85-A, no.6, pp.1379–1386, June 2002.

[12] T. Ishihara and H. Koga, "New constructions of the lattice - based visual secret sharing scheme using mixture of colors," IEICE Trans. Fundamentals, vol.E85-A, no.1, pp.158–166, Jan. 2002.

[13] T. Ishihara and H. Koga, "A visual secret sharing scheme for color images based on meanvalue-color mixing," IEICE Trans. Fundamentals, vol.E86-A, no.1, pp.194–197, Jan. 2003.

[14] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology-EUROCRYPT'94, LNCS-950, pp.1–12, Springer-Verlag, 1994.

[15] Y. Suga, K. Iwamura, K. Sakurai, and H. Imai, "Extended graph-type visual secret sharing schemes with embedded plural images," Inf. Process. Soc. Jpn. J., vol.42, no.8, pp.2106–2113, 2001.

[16] E.R. Verheul and H.C.A. van Tilborg, "Constructions and properties of k out of n visual secret sharing scheme," Designs, Codes, and Cryptography, vol.1, no.2, pp.179–196, 1997.

Appendix: Construction of VSS-1-PI Scheme

In this appendix, we give a construction of the basis matrices of the VSS-1-PI scheme for readers' convenience. First, we describe a method to obtain the basis matrices of the (n, n)-threshold VSS-1-PI scheme based on the polynomial representations of the basis matrices [7], [10]–[12]. Then, a general $(\Gamma^{(1)}_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$-VSS-1-PI scheme can be derived by the cumulative map [1], [6], [10] from the (n, n)-threshold VSS-1-PI scheme.

A.1 Analytical Construction of VSS Schemes

Let $\boldsymbol{v}$ be an n-dimensional row vector, each element of which is a color in $\mathcal{E}$. Then, define an $n \times n!$ matrix $C_n(\boldsymbol{v})$ called a *column permutation* (CP) matrix which consists of all $n!$ permutations of ${}^t\boldsymbol{v}$. For example,

$$C_3\left([\mathsf{gzz}]\right) \sim \begin{bmatrix} \mathsf{gzzgzz} \\ \mathsf{zgzzgz} \\ \mathsf{zzgzzg} \end{bmatrix}. \tag{A$\cdot$1}$$

Note that in the permutation, all n colors in $\boldsymbol{v}$ are treated different colors even if two or more elements in $\boldsymbol{v}$ are the same color. In the case that all the elements of $\boldsymbol{v}$ are different, there are $(n!)!$ matrices that are equivalent to $C_n(\boldsymbol{v})$ in the equivalence relation $\sim$ introduced in Sect. 2.3. However, by the benefit of the equivalence relations $\sim$, it suffices to consider only one matrix that is the representative in the equivalence class.

Now assume that a color k in $\mathcal{E}$ is a mixture of r_{k} different colors $\mathsf{k}^{\langle e\rangle}$, $e = 1, 2, \ldots, r_{\mathsf{k}}$, in $\mathcal{E}$, i.e.,

$$\mathsf{k} = \mathsf{k}^{\langle 1\rangle} \sqcup \mathsf{k}^{\langle 2\rangle} \sqcup \cdots \sqcup \mathsf{k}^{\langle r_{\mathsf{k}}\rangle}, \tag{A$\cdot$2}$$

and an n-dimensional row vector $\boldsymbol{v}_{\mathsf{k}}$ is given by

$$\begin{aligned}\boldsymbol{v}_{\mathsf{k}} &= [\underbrace{\mathsf{k}^{\langle 1\rangle} \cdots \mathsf{k}^{\langle 1\rangle}}_{u_1 \text{ times}} \cdots \underbrace{\mathsf{k}^{\langle r_{\mathsf{k}}\rangle} \cdots \mathsf{k}^{\langle r_{\mathsf{k}}\rangle}}_{u_{r_{\mathsf{k}}} \text{ times}}] \\ &\overset{\text{def}}{=} \left[\left(\mathsf{k}^{\langle 1\rangle}\right)^{u_1} \cdots \left(\mathsf{k}^{\langle r_{\mathsf{k}}\rangle}\right)^{u_{r_{\mathsf{k}}}}\right],\end{aligned} \tag{A$\cdot$3}$$

where $\mathsf{k}^{\langle e\rangle}$ appears u_e times in $\boldsymbol{v}_{\mathsf{k}}$, and $\sum_{e=1}^{r_{\mathsf{k}}} u_e = n$. Then the number of the different column vectors obtained by the permutations of $\boldsymbol{v}_{\mathsf{k}}$ is given by $N(\boldsymbol{v}_{\mathsf{k}}) \overset{\text{def}}{=} \binom{n}{u_1, u_2, \ldots, u_{r_{\mathsf{k}}}}$. The *different column permutation* (DP) matrix $D_n(\boldsymbol{v}_{\mathsf{k}})$ is defined as the matrix that consists of such $N(\boldsymbol{v}_{\mathsf{k}})$ different columns. For example, in the case of $\boldsymbol{v}_{\mathsf{g}} = [\mathsf{cyy}]$,

$$D_3(\boldsymbol{v}_{\mathsf{g}}) = D_3\left(\left[\mathsf{c}^1\mathsf{y}^2\right]\right) \sim \begin{bmatrix} \mathsf{cyy} \\ \mathsf{ycy} \\ \mathsf{yyc} \end{bmatrix}. \tag{A$\cdot$4}$$

We note that any CP matrix can be represented by the concatenations of DP matrices. For instance, $C_3([\mathsf{cyy}])$ and $D_3([\mathsf{c}^1\mathsf{y}^2])$ satisfies from Eqs.(A· 1)(A· 4) that

$$C_3([\mathsf{cyy}]) \sim D_3([\mathsf{c}^1\mathsf{y}^2]) \odot D_3([\mathsf{c}^1\mathsf{y}^2]). \tag{A$\cdot$5}$$

It is worth noting that any $n-1$ rows of a DP matrix $D_n(\boldsymbol{v}_{\mathsf{k}})$, say $D'_n(\boldsymbol{v}_{\mathsf{k}})$, is equivalent to the concatenations of DP matrices with $n-1$ rows. For example, it holds that

$$D'_3([\mathsf{c}^1\mathsf{y}^2]) \sim \begin{bmatrix} \mathsf{c\ y\ y} \\ \mathsf{y\ c\ y} \end{bmatrix} \sim D_2([\mathsf{c}^1\mathsf{y}^1]) \odot D_2([\mathsf{c}^0\mathsf{y}^2]), \tag{A$\cdot$6}$$

where $[\mathsf{c}^0\mathsf{y}^2] = [\mathsf{y}^2]$. Generally, it holds for $u_e \geqq 1$, $e = 1, 2, \ldots, r_{\mathsf{k}}$, that

$$\begin{aligned}&\left\langle D'_n\left(\left[(\mathsf{k}^{\langle 1\rangle})^{u_1}(\mathsf{k}^{\langle 2\rangle})^{u_2}\cdots(\mathsf{k}^{\langle r_{\mathsf{k}}\rangle})^{u_{r_{\mathsf{k}}}}\right]\right)\right\rangle \\ &= \left\langle D_{n-1}\left(\left[(\mathsf{k}^{\langle 1\rangle})^{u_1-1}\ (\mathsf{k}^{\langle 2\rangle})^{u_2}\cdots(\mathsf{k}^{\langle r_{\mathsf{k}}\rangle})^{u_{r_{\mathsf{k}}}}\right]\right)\right\rangle \\ &\odot \left\langle D_{n-1}\left(\left[(\mathsf{k}^{\langle 1\rangle})^{u_1}\ (\mathsf{k}^{\langle 2\rangle})^{u_2-1}\cdots(\mathsf{k}^{\langle r_{\mathsf{k}}\rangle})^{u_{r_{\mathsf{k}}}}\right]\right)\right\rangle \\ &\odot \cdots \odot \left\langle D_{n-1}\left(\left[(\mathsf{k}^{\langle 1\rangle})^{u_1}\ (\mathsf{k}^{\langle 2\rangle})^{u_2}\cdots(\mathsf{k}^{\langle r_{\mathsf{k}}\rangle})^{u_{r_{\mathsf{k}}}-1}\right]\right)\right\rangle.\end{aligned} \tag{A$\cdot$7}$$

We now describe the *polynomial representations* of basis matrices. We identify each equivalence class of a basis matrix with a homogeneous polynomial of degree n in the following way:

First, we identify colors $\mathsf{k}^{\langle e\rangle}$ and z with variables $k^{\langle e\rangle}$ and z, respectively. We also identify the equivalence class of the DP matrix $\langle D_n(\boldsymbol{v}_{\mathsf{k}})\rangle$ and the concatenations operation $\odot$ with a monomial $\prod_{e=1}^{r_{\mathsf{k}}} \frac{(k^{\langle e\rangle})^{u_e}}{u_e!}$ and the operation $+$, respectively.

Assume that the equivalence classes of the basis matrices $B_{\mathsf{k},\ell}$, $0 \leqq \ell \leqq L_{\mathsf{k}}$, representing colors K_ℓ are constructed by the concatenation of the equivalence classes of the DP matrices $D_n(\boldsymbol{v}_{\mathsf{k}})$ as follows.

$$\langle B_{\mathsf{k},\ell}\rangle = \underbrace{\langle D_n(\boldsymbol{v}_{\mathsf{k}})\rangle \odot \cdots \odot \langle D_n(\boldsymbol{v}_{\mathsf{k}})\rangle}_{\sum_{l=0}^{\ell-1} d^{(1)}_{\mathsf{k},l} \Big/ N(\boldsymbol{v}_{\mathsf{k}}) \text{ times}} \odot \langle X\rangle, \tag{A$\cdot$8}$$

where $\sum_{l=0}^{\ell-1} d^{(1)}_{\mathsf{k},l}$ is a multiple of $N(\boldsymbol{v}_{\mathsf{k}})$ and X consists of the concatenations of DP matrices that contain at least one z in every column†. In such cases, $\langle B_{\mathsf{k},\ell}\rangle$ can be identified with the *basis polynomials* $F_{\mathsf{k},\ell}$, which is a homogeneous polynomial of degree n.

From the assumption Eq.(A· 8), the basis polynomial $F_{\mathsf{k},\ell}$ corresponding to $B_{\mathsf{k},\ell}$ must satisfy that

$$F_{\mathsf{k},\ell}|_{z=0} = \frac{\sum_{l=0}^{\ell-1} d^{(1)}_{\mathsf{k},l}}{N(\boldsymbol{v}_{\mathsf{k}})} \prod_{e=1}^{r_{\mathsf{k}}} \frac{(k^{\langle e\rangle})^{u_e}}{u_e!}. \tag{A$\cdot$9}$$

On the other hand, the polynomial corresponding to the right hand side of Eq. (A· 7) is given by

$$\begin{aligned}&\sum_{e=1}^{r_{\mathsf{k}}}\left[\frac{(k^{\langle e\rangle})^{u_e-1}}{(u_e-1)!}\prod_{\substack{e'=1\\e'\neq e}}^{r_{\mathsf{k}}}\frac{(k^{\langle e'\rangle})^{u_{e'}}}{u_{e'}!}\right] \\ &= \varphi\prod_{e=1}^{r_{\mathsf{k}}}\frac{(k^{\langle e\rangle})^{u_e}}{u_e!}\end{aligned} \tag{A$\cdot$10}$$

†In the case of $\mathsf{K}_0 = \mathsf{Z}$, $\langle B_{\mathsf{k},0}\rangle$ is obtained by letting $\sum_{l=0}^{\ell-1} d^{(1)}_{\mathsf{k},l} = 0$.

where $\varphi = \sum_{e=1}^{r_{\mathsf{k}}} \frac{\partial}{\partial k^{\langle e\rangle}}$. Therefore, if any $n-1$ rows of $B_{\mathsf{k},\ell}$ are equivalent for any k and ℓ, the basis polynomial $F_{\mathsf{k},\ell}$ must satisfy that

$$\psi F_{\mathsf{k},\ell} = F, \tag{A$\cdot$11}$$

where $\psi = \sum_{\mathsf{k}\in\mathcal{E}} \frac{\partial}{\partial k}$ and F is a homogeneous polynomial of degree $n-1$ that depends on neither k nor ℓ.

Summarizing the above, we have the following theorem.

Theorem 3: Suppose that the basis matrices $B_{\mathsf{k},\ell}$ are obtained by the concatenations of the DP matrices as shown in Eq. (A· 8). Then, the basis polynomials $F_{\mathsf{k},\ell}$ corresponding to $B_{\mathsf{k},\ell}$ satisfy Eqs. (A· 9) and (A· 11). □

In the case that $L_{\mathsf{k}} = 1$ for all k and all the basis matrices consist of CP matrices, the basis polynomials can be obtained by solving the partial differential equations Eqs. (A· 9) and (A· 11) as shown in [10], [12]. But in general cases, it is difficult to derive the explicit solutions of Eqs. (A· 9), (A· 11). Hence, we consider the case that $r_{\mathsf{k}} = 1$ and $u_1 = n$ for all k. In this case, it holds that $N(\boldsymbol{v}_{\mathsf{k}}) = 1$ for all k, and Eq. (A· 9) becomes

$$F_{\mathsf{k},\ell}|_{z=0} = \sum_{l=0}^{\ell-1} d_{\mathsf{k},l}^{(1)} \frac{k^n}{n!}. \tag{A$\cdot$12}$$

Then, the basis polynomials are given by

$$\begin{aligned} F_{\mathsf{k},\ell} = {} & \sum_{l=0}^{\ell-1} d_{\mathsf{k},l}^{(1)} f^0(k) + \sum_{l=\ell}^{L_{\mathsf{k}}-1} d_{\mathsf{k},l}^{(1)} f^1(k) \\ & + \sum_{\mathsf{h}\in\mathcal{E}\backslash\{\mathsf{z},\mathsf{k}\}} \sum_{l=0}^{L_{\mathsf{h}}-1} d_{\mathsf{h},l}^{(1)} f^1(h), \end{aligned} \tag{A$\cdot$13}$$

where f^0 and f^1 are represented as

$$f^0(k) = \sum_{\substack{t=0\\ t:\text{even}}}^{n} \frac{z^t}{t!(n-t)!} k^{n-t}, \tag{A$\cdot$14}$$

$$f^1(k) = \sum_{\substack{t=1\\ t:\text{odd}}}^{n} \frac{z^t}{t!(n-t)!} k^{n-t}. \tag{A$\cdot$15}$$

and they satisfy $(\frac{\partial}{\partial k} + \frac{\partial}{\partial z}) f^0(k) = (\frac{\partial}{\partial k} + \frac{\partial}{\partial z}) f^1(k)$. Eqs. (A· 14), (A· 15) can easily be obtained from the results shown in [7], [9], [11], and hence we omit the derivation.

Furthermore, it is easy to check that the pixel expansion of $B_{\mathsf{k},\ell}$ corresponding to Eq. (A· 13) is given by

$$m^{(1)} = \sum_{\mathsf{k}\in\mathcal{E}} \sum_{l=0}^{L_{\mathsf{k}}-1} d_{\mathsf{k},l}^{(1)}\ 2^{n-1}. \tag{A$\cdot$16}$$

Example 7: Let us consider the $(3,3)$-threshold VSS-1-PI scheme which has colors $\{\mathsf{G}_1, \mathsf{G}_2, \mathsf{Y}_1\}$ on the decrypted image for $\mathcal{E} = \{\mathsf{g},\mathsf{y},\mathsf{z}\}$. If we set $d_{\mathsf{g},0}^{(1)} = d_{\mathsf{y},0}^{(1)} = 1$ and $d_{\mathsf{g},1}^{(1)} = 1$, Eqs. (A· 12), (A· 11) are given by

$$F_{\mathsf{g},1}|_{z=0} = \frac{g^3}{3!},\quad F_{\mathsf{g},2}|_{z=0} = 2\frac{g^3}{3!},\quad F_{\mathsf{y},1}|_{z=0} = \frac{y^3}{3!}, \tag{A$\cdot$17}$$

$$\psi F_{\mathsf{g},1} = \psi F_{\mathsf{g},2} = \psi F_{\mathsf{y},1}, \tag{A$\cdot$18}$$

where $\psi = \frac{\partial}{\partial z} + \frac{\partial}{\partial g} + \frac{\partial}{\partial y}$. Then, from Eq. (A· 13), the solutions of Eqs. (A· 17), (A· 18) are given by

$$F_{\mathsf{g},1} = f^0(g) + f^1(g) + f^1(y), \tag{A$\cdot$19}$$

$$F_{\mathsf{g},2} = 2f^0(g) + f^1(y), \tag{A$\cdot$20}$$

$$F_{\mathsf{y},1} = f^0(y) + 2f^1(g). \tag{A$\cdot$21}$$

Since $f^0(k)$ and $f^1(k)$ correspond to

$$D_3([\mathsf{k}^3]) \odot D_3([\mathsf{k}\mathsf{z}^2]) = \begin{bmatrix} \mathsf{kkzz} \\ \mathsf{kzkz} \\ \mathsf{kzzk} \end{bmatrix}, \tag{A$\cdot$22}$$

$$D_3([\mathsf{z}^3]) \odot D_3([\mathsf{k}^2\mathsf{z}]) = \begin{bmatrix} \mathsf{zzkk} \\ \mathsf{zkzk} \\ \mathsf{zkkz} \end{bmatrix}, \tag{A$\cdot$23}$$

respectively, the basis matrices corresponding to $F_{\mathsf{g},1}$, $F_{\mathsf{g},2}$, $F_{\mathsf{y},1}$ are given as follows:

$$B_{\mathsf{g},1} = \begin{bmatrix} \mathsf{ggzzzzggzzyy} \\ \mathsf{gzgzzgzgzyzy} \\ \mathsf{gzzgzggzzyyz} \end{bmatrix}, \tag{A$\cdot$24}$$

$$B_{\mathsf{g},2} = \begin{bmatrix} \mathsf{ggzzggzzzzyy} \\ \mathsf{gzgzgzgzzyzy} \\ \mathsf{gzzggzzgzyyz} \end{bmatrix}, \tag{A$\cdot$25}$$

$$B_{\mathsf{y},1} = \begin{bmatrix} \mathsf{yyzzzzggzzgg} \\ \mathsf{yzyzzgzgzgzg} \\ \mathsf{yzzyzggzzggz} \end{bmatrix}. \tag{A$\cdot$26}$$

Note that we can eliminate the column ${}^t[\mathsf{zzz}]$ from Eqs. (A· 24)–(A· 26), since ${}^t[\mathsf{zzz}]$ is included in all B's and plays no role in Def.1 (i) and (ii). □

A.2 VSS-1-PI Schemes for General Access Structures

According to [1], [6], [10], we describe how to construct the VSS scheme for a general access structure from the basis matrices of the (n,n)-threshold VSS-1-PI scheme.

Assume that a $(\Gamma_{\mathsf{Qual}}^{(1)}, \Gamma_{\mathsf{Forb}})$-VSS-1-PI scheme has $\Gamma_{\mathsf{Forb}}^{+} = \{\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_t\}$. Then, for $\mathcal{T} = \{1, 2, \ldots, t\}$, introduce the *cumulative map* $\alpha : \mathcal{N} \to 2^{\mathcal{T}}$ that is defined by

$$\alpha(p) = \{i : p \notin \mathcal{F}_i, 1 \leqq i \leqq t\} \quad \text{for } p \in \mathcal{N}. \tag{A$\cdot$27}$$

Then, letting $\tilde{B}_{\mathsf{k},\ell}$ and $B_{\mathsf{k},\ell}$ be the basis matrices of the (t,t)-threshold VSS-1-PI scheme and the $(\Gamma_{\mathsf{Qual}}^{(i)}, \Gamma_{\mathsf{Forb}})$-VSS-1-PI scheme, respectively, $B_{\mathsf{k},\ell}$ can be obtained from $\tilde{B}_{\mathsf{k},\ell}$ as follows:

$$B_{\mathsf{k},\ell}[\![\{p\}]\!] = \beta(\tilde{B}_{\mathsf{k},\ell}[\![\alpha(p)]\!]) \quad \text{for } p \in \mathcal{N}. \qquad (\mathrm{A}\cdot 28)$$

It is shown in [1], [10] that the basis matrices obtained by Eq. (A·28) satisfy the definition of $(\Gamma^{(1)}_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$-VSS-1-PI scheme.

Finally, if the same column vectors are included in all $B_{\mathsf{k},\ell}$, we can eliminate them from every $B_{\mathsf{k},\ell}$'s, because the same column vectors in $B_{\mathsf{k},\ell}$'s play no role, and the pixel expansion can be reduced by the elimination.

Mitsugu Iwamoto was born in Fukuoka, on 29 July, 1976. He received the B.E. and M.E. degrees from the University of Tokyo, Japan, in 1999 and 2001, respectively. Currently, he is a doctor course student in the Department of Mathematical Informatics, Graduate School of Information Science and Technology, the University of Tokyo. His research interest includes information security and cryptography.

Hirosuke Yamamoto was born in Wakayama, Japan, on November 15, 1952, He received the B.E. degree from Shizuoka University, in 1975 and the M.E. and Ph.D. degrees from University of Tokyo, in 1977 and 1980, respectively, all in electrical engineering. In 1980, he joined Tokushima University. He was an Associate Professor at Tokushima University, University of Electro-Communications, and University of Tokyo, from 1983 to 1987, from 1987 to 1993, and from 1993 to 1999, respectively. Since 1999, he has been a Professor at University of Tokyo and is now with the Department of Mathematical Informatics in the university. In 1989 and 1990, he was a Visiting Scholar at the Information Systems Laboratory, Stanford University. He is the chair of IEEE Information Theory Society Japan Chapter in 2002 and 2003. His research interests are in Shannon theory, data compression algorithms, coding theory, cryptology, and communication theory. Dr. Yamamoto is a member of the IEEE Information Theory Society and the SITA (Society of Information Theory and Its Applications).