Visual secret sharing schemes encrypting multiple images

Manami Sasaki and Yodai Watanabe *Member, IEEE*

***Abstract*—The aim of this work is to maximize the range of the access control of visual secret sharing (VSS) schemes encrypting multiple images. First, the formulation of access structures for a single secret is generalized to that for multiple secrets. This generalization is maximal in the sense that the generalized formulation makes no restrictions on access structures; in particular, it includes the existing ones as special cases. Next, a sufficient condition to be satisfied by the encryption of VSS schemes realizing an access structure for multiple secrets of the most general form is introduced, and two constructions of VSS schemes with encryption satisfying this condition are provided. Each of the two constructions has its advantage against the other; one is more general and can generate VSS schemes with strictly better contrast and pixel expansion than the other, while the other has a straightforward implementation. Moreover, for threshold access structures, the pixel expansions of VSS schemes generated by the latter construction are estimated and turn out to be the same as those of the existing schemes called the threshold multiple-secret visual cryptographic schemes (MVCS). Finally, the optimality of the former construction is examined, giving that there exist access structures for which it generates no optimal VSS schemes.**

***Index Terms*—Visual secret sharing, General access structures, Multiple secrets, Information-theoretic security**

I. Introduction

The secret sharing (SS) scheme is a cryptosystem which encrypts a secret into multiple shares so that any qualified combination of shares can reconstruct the secret, while any forbidden combination of shares reveals no information about the secret. Here, the sets of the qualified combinations and the forbidden combinations are called a qualified set and a forbidden set, respectively, and the pair of the qualified and forbidden sets is called an access structure. A typical example of SS schemes is the (k, n)-threshold SS scheme [4], [17], in which a secret is encrypted into n shares so that any k or more shares can reconstruct the secret, while any $k-1$ or less shares leak no information about the secret.

In contrast to the ordinary cryptosystems, there exist SS schemes whose decryption can be performed by humans without any numerical computations. The visual secret sharing (VSS) scheme [15] is an example of such SS schemes. This scheme encrypts a visual secret into visual shares so that humans can visually reconstruct the secret with their eyes by superposing a qualified combination of visual shares each printed on a transparency. One of the applications in which VSS schemes are essential is for the authentication by a human recipient without any trusted communication channels. More precisely, the problem here is to authenticate a message from an informant to a human recipient through an insecure channel which is under full control of an adversary. This arises, for example, in the interactions between a human and an electronic device without screen such as a smartcard. It is hard to provide a solution to this problem without assuming a secure channel,[1] and the authentication based on VSS schemes, called the visual authentication [14], has been the only secure solution so far.

A. Related works

The SS scheme encrypting multiple secrets can trivially be realized by a collection of multiple SS schemes each encrypting each secret. Therefore, this work considers the VSS scheme encrypting multiple secrets in which each participant receives a single visual share and any qualified combination of participants for each visual secret can reconstruct the secret by superposing their visual shares.[2] So far there have been proposed the following VSS schemes encrypting multiple secrets: extended visual cryptographic schemes (EVCS) [1], visual secret sharing schemes for plural secret images (VSS-q-PI) [13] and threshold multiple-secret visual cryptographic schemes (MVCS) [21]. Here, EVCS assumes an access structure such that all but one of its qualified sets consist of (the combination of) a single share, VSS-q-PI an access structure whose forbidden sets are identical for all secrets[3] (although its qualified sets can be arbitrary) and MVCS a threshold access structure (for details, see (3a)–(3c) in section III-A). This work provides the formulation and constructions of VSS schemes realizing a general access structure for multiple secrets without any restrictions. Table I summarizes the existing works as well as this work, where the classification is based on only the range of their access control.[4]

It should be stated that there has been proposed another type of VSS schemes encrypting multiple images in which additional operations in the decryption, such as the rotation of shares with multiple relative angles, are introduced (see

Manuscript received ; revised . A preliminary version of this paper was presented at ICASSP 2014, Florence, Italy, May 2014 [16]. This work was supported in part by JSPS Grants-in-Aid for Young Scientists (B) No. 21700021 and for Scientific Research (C) No. 15K00020.

The authors are with the Department of Computer Science and Engineering, University of Aizu, Aizu-Wakamatsu City, Fukushima 9658580, Japan (yodai@u-aizu.ac.jp).

[1] In using a smartcard for payment, for instance, one is supposed to trust the place of sale to show the correct price charged to the smartcard; in other words, it is assumed that the price is announced from an informant (smartcard) to a human recipient through a secure channel.

[2] This work considers only monochrome images. For VSS schemes encrypting color images, see e.g. [8], [13], [23].

[3] It should be noted that VSS-q-PI can encrypt color images.

[4] From this point of view, (k, n)-visual cryptographic schemes with meaningful shares ((k, n)-VCS-MS) [18] and region incrementing visual cryptographic schemes (RIVCS) [24] are special cases of EVCS and MVCS, respectively, and fully incrementing visual cryptography (FIVC) [7] is equivalent to MVCS.

TABLE I
COMPARISON AMONG THE EXISTING WORKS AND THIS WORK

VSS scheme	Restriction on access structure
EVCS [1]	All but one of the qualified sets have to consist of (the combination of) a single share
VSS-q-PI [13]	Forbidden sets have to be identical for all secrets
MVCS [21]	An access structure has to be of threshold type
This work	No restrictions

e.g. [19], [20], [26]). In VSS schemes of this type, different operations correspond to different secret images, while in the VSS schemes in Table I, different combinations of shares correspond to different secret images. Therefore, from a point of view of the access control, which is the goal of the secret sharing, the former schemes can be reduced to a single VSS scheme encrypting a single secret (into which multiple secret images are connected), while there exist no such simple reductions for the latter ones even for the simplest access structures.[5] This is a major difference between the former and the latter schemes.

B. Our contributions

The aim of this work is to maximize the range of the access control of VSS schemes encrypting multiple images. As a first step, the preliminary version [16] maximally generalized the formulations of access structures and VSS schemes for multiple secrets, and then provided a construction of VSS schemes of the most general form. This paper provides further developments of this generalization described below.[6] First, this paper justifies the above construction in a more general framework. More precisely, this paper introduces a more general construction (Construction 11) which includes the previous one as a special case. In particular, this inclusion is strict in the sense that the former (Construction 11) can generate VSS schemes with strictly better contrast and pixel expansion than the latter, which is demonstrated by the last two examples in section III-C. Then, this paper proves that for any given access structure of the most general form, the former indeed generates a VSS scheme realizing the access structure (in Theorem 12), and also the latter is a special case of the former (in Corollary 14); this completes the justification of the latter (previous) construction, which was not given in [16]. Here, to describe the former construction, this paper has introduced two notions (Definitions 7 and 10), which, together with the proofs to characterize and justify the construction (Lemma 9 and Theorem 12), reveal a sufficient condition to be satisfied by the encryption of VSS schemes for multiple secrets. Moreover, it is demonstrated that for threshold access structures, the latter construction generates VSS schemes with the same pixel expansion as (k, n, s)-MVCS and (k, n, s, R)-MVCS [21] (in section III-D).[7] Finally, the optimality of the former (more general) construction is examined, giving that there exist access structures for which it generates no optimal VSS schemes (in section III-E).

[5]A perfect access structure $\Gamma^2 = \{(A_Q^i, A_F^i)\}_{i=1}^2$ on $\{s_1, s_2\}$ for two secrets with $A_Q^1 = \{\{s_1\}, \{s_1, s_2\}\}$ and $A_Q^2 = \{\{s_2\}, \{s_1, s_2\}\}$ (see Definition 4 for this notation) is an example of such access structures.

[6]All of these are contributions of this paper relative to the preliminary version [16].

[7]It should be noted that our constructions are not restricted to threshold access structures, but can apply to arbitrary ones.

II. PRELIMINARIES

In this section, we provide definitions and notations that will be used later. For details of definitions in information theory and secret sharing, see e.g. [2], [9], [22].

A. Basic definitions and notations

For $n \in \mathbb{N}$, let $[n]$ denote the set of natural numbers less than or equal to n; i.e. $[n] = \{k \in \mathbb{N} | k \leq n\}$. The power set of a set $\mathcal{S}$ is denoted by $2^{\mathcal{S}}$; i.e. $2^{\mathcal{S}} = \{a | a \subseteq \mathcal{S}\}$. For a subset A of a power set partially ordered by inclusion, let $\left(A\right)_0$ denote the set of the minimal elements of A with respect to this order; i.e.

$$\left(A\right)_0 = \{a \in A | \forall a' \in A (a' \not\subset a)\}$$

(where we have used the symbol $\subset$ to represent the strict inclusion). For an ordered set $\mathcal{S} = \{s_1, s_2, \cdots, s_n\}$, the order of s_i in $\mathcal{S}$ is denoted by $\mathrm{ord}_{\mathcal{S}}(s_i)$; i.e. $\mathrm{ord}_{\mathcal{S}}(s_i) = i$.

For random variables X and Y over the same domain, we write $X = Y$ if X and Y are equal almost surely (i.e. $\Pr[X = Y] = 1$), and $X \sim Y$ if X and Y have the same probability distribution. For a set $\mathcal{S}$, let $\mathcal{S}_U$ denote a probabilistic function which outputs an element of $\mathcal{S}$ according to the uniform distribution over $\mathcal{S}$.

For $x \in \{0,1\}^n$, $b \in \{0,1\}$ and $i \in [n]$, let $x_{x_i=b}$ denote the string x with the i-th element x_i replaced by b; i.e.

$$x_{x_i=b} = (x_1, \cdots, x_{i-1}, b, x_{i+1}, \cdots, x_n).$$

For $x \in \{0,1\}^n$, let $\mathrm{Gray}(x)$ denote the gray level of x; i.e.

$$\mathrm{Gray}(x) = \frac{\left|\{i | x_i = 1\}\right|}{n}.$$

The gray level of the empty string ε is defined to be 0; i.e. $\mathrm{Gray}(\varepsilon) = 0$.

B. Access structure and secret sharing

Let $\mathcal{S} = \{s_1, s_2, \cdots, s_n\}$ be the set of all the shares. The subset of $2^{\mathcal{S}}$ any of whose elements can decrypt the secret is called a *qualified set* and is denoted by A_Q. The subset of $2^{\mathcal{S}}$ any of whose elements leaks no information about the secret is called a *forbidden set* and is denoted by A_F. The pair Γ of the qualified and forbidden sets, $\Gamma = (A_Q, A_F)$, is called an *access structure on* $\mathcal{S}$. The access structure has to satisfy the *monotonicity*:

$$A \in A_Q \wedge A \subseteq B \Rightarrow B \in A_Q,$$
$$B \in A_F \wedge A \subseteq B \Rightarrow A \in A_F,$$

for all $A, B \subseteq \mathcal{S}$. A qualified set A_Q is uniquely determined by its minimal elements $\left(A_Q\right)_0$:

$$\left(A_Q\right)_0 = \left(A'_Q\right)_0 \Rightarrow A_Q = A'_Q$$

for all qualified sets A_Q and A'_Q on $\mathcal{S}$. An access structure is called *perfect* if every subsets of the shares are included in

TABLE II
ENCRYPTION OF A SINGLE PIXEL, AND THE SETS $\mathcal{C}^0$ AND $\mathcal{C}^1$ OF REPRESENTING MATRICES (0: WHITE, 1: BLACK, ROW: SHARE, COLUMN: SUBPIXEL IN SHARE)

Pixel		Pattern1	Pattern2	Pattern1 Pattern2
	Share 1			$\mathcal{C}^0 = \left\{ \begin{pmatrix} 01 \\ 01 \end{pmatrix}, \begin{pmatrix} 10 \\ 10 \end{pmatrix} \right\}$
	Share 2			
	Share 1			$\mathcal{C}^1 = \left\{ \begin{pmatrix} 01 \\ 10 \end{pmatrix}, \begin{pmatrix} 10 \\ 01 \end{pmatrix} \right\}$
	Share 2			

either the qualified set or the forbidden set. The perfect access structure can be determined by only a qualified set.

Example 1 ((k,n)-threshold access structure)**.** Let $\mathcal{S}$ be a finite set of size n. A (k,n)-*threshold access structure on* $\mathcal{S}$ consists of the qualified set A_Q and the forbidden set A_F given by $A_Q = \{a \subseteq \mathcal{S} | k \leq |a|\}$ and $A_F = \{a \subseteq \mathcal{S} | k > |a|\}$. Since $A_Q \cup A_F = 2^{\mathcal{S}}$, this access structure is perfect. A secret sharing scheme realizing a (k,n)-threshold access structure is called a (k,n)-*threshold secret sharing scheme*.

C. Visual secret sharing

In the ordinary SS schemes, the secrets and shares are both numerical data, and their decryption is performed by computers. In contrast, in the VSS schemes, the secrets and shares are both visual, and their decryption can visually be performed by human eyes.[8] Each black-white pixel in a secret image is encrypted into a set of black-white subpixels in shares. Hence, the encryption of each pixel can be represented as a pair of matrices $C^b = (c^b_{ij})$ with $b \in \{0,1\}$, where $b = 0$ for a white pixel in a secret image and $b = 1$ otherwise, and $c^b_{ij} = 0$ for a white j-th subpixel in the i-th share and $c^b_{ij} = 1$ otherwise.

For an illustrative purpose, let us consider a $(2,2)$-threshold VSS scheme. A secret image is encrypted into two shares. Each share is indistinguishable from noise images, and so leaks no information about the secret. On the other hand, the secret image can be reconstructed when both of the shares are superposed. This can be constructed as follows. A pixel e in the secret image is encrypted into two subpixels in each of the two shares. If e is white (resp. black), then Pattern 1 or Pattern 2 in the upper (resp. lower) row of Table II is chosen at random. The superposition of the two shares has one black subpixel and one white subpixel (resp. two black subpixels) if e is white (resp. black). This construction can be represented by the sets $\mathcal{C}^0$ and $\mathcal{C}^1$ of matrices in Table II; more precisely, the above encryption and decryption can be represented by the functions $\mathrm{Enc} : \{0,1\} \to \{0,1\}^{2\times 2}$ and $\mathrm{Dec} : \{0,1\}^{2\times 2} \to \{0,1\}^2$ given by

$$\mathrm{Enc}(b) = \mathcal{C}^b_U \quad \text{and} \quad \mathrm{Dec}(M) = (m_{11} \vee m_{21}, m_{12} \vee m_{22})$$

for $b \in \{0,1\}$ and $M = (m_{ij}) \in \{0,1\}^{2\times 2}$, respectively, where $\vee$ denotes the OR operation.

The relative difference in gray level between superposed shares that come from a white pixel and a black pixel in the secret image is called the *contrast*. In the above example, the reconstructed pixel has a gray level of $\frac{2}{2} = 1$ if e is black, and a gray level of $\frac{1}{2}$ if e is white; therefore, Contrast $= \frac{2}{2} - \frac{1}{2} = \frac{1}{2}$. The higher contrast makes it easier to recognize reconstructed images.

The number of subpixels in shares encrypted from a pixel in a secret is called the *pixel expansion*. In the above example, a pixel in a secret is encrypted into two subpixels in shares; therefore, Pixel expansion $= 2$. The lower pixel expansion allows the more practical resolution of share images. A VSS scheme and its encryption are called *optimal* if they have the lowest pixel expansion.

D. Notations for matrices

For two matrices A and B of the same number of rows, let $A|B$ denote the concatenation of A and B. In the same way as [13], we introduce an equivalence relation $\sim$ on the set $\mathcal{M}$ of matrices; for two matrices A and B of the same size, we write $A \sim B$ if A can be obtained by a column permutation of B. For $R \in \mathcal{M}$, let $\langle R \rangle$ denote the set of all the matrices A such that $A \sim R$; i.e.

$$\langle R \rangle = \{A \in \mathcal{M} \mid A \sim R\}.$$

By using this notation, $\mathcal{C}^0$ and $\mathcal{C}^1$ in Table II can be written as

$$\mathcal{C}^0 = \left\langle \begin{pmatrix} 01 \\ 01 \end{pmatrix} \right\rangle \quad \text{and} \quad \mathcal{C}^1 = \left\langle \begin{pmatrix} 01 \\ 10 \end{pmatrix} \right\rangle.$$

A pair of matrices C^0 and C^1 is called *basis matrices* for a VSS scheme with encryption Enc if the random column permutation of them gives the encryption Enc; i.e. $\mathrm{Enc}(b) = \langle C^b \rangle_U$ for $b \in \{0,1\}$. Hence, the above two matrices are basis matrices for the (2,2)-threshold VSS scheme.

For $n \in \mathbb{N}$, let $C^0_{n,n}$ and $C^1_{n,n}$ denote basis matrices for an optimal (n,n)-threshold VSS scheme. For example,

$$C^0_{1,1} = (0), \quad C^0_{2,2} = \begin{pmatrix} 01 \\ 01 \end{pmatrix}, \quad C^0_{3,3} = \begin{pmatrix} 0011 \\ 0101 \\ 0110 \end{pmatrix},$$

$$C^1_{1,1} = (1), \quad C^1_{2,2} = \begin{pmatrix} 01 \\ 10 \end{pmatrix}, \quad C^1_{3,3} = \begin{pmatrix} 1001 \\ 1010 \\ 1100 \end{pmatrix},$$

have been shown to give optimal (n,n)-threshold VSS schemes for $n = 1, 2, 3$, respectively [15].

III. VISUAL SECRET SHARING SCHEMES ENCRYPTING MULTIPLE IMAGES

A. Formulation

In this subsection, we provide a formulation of VSS schemes encrypting multiple images. We begin with the following definition of two matrix operations, which are convenient for describing the security and constructions of VSS schemes.

[8]For audio secret sharing (ASS) schemes, whose decryption can acoustically be performed by human ears, see e.g. [11], [25]

Definition 2 (Supermatrix and submatrix with respect to an ordered subset [16])**.** Let $\mathcal{S} = \{s_1, s_2, \cdots, s_n\}$ be an ordered set of size n, and a be an ordered subset of $\mathcal{S}$ of size n'. For an $n' \times m$ matrix $M = (m_{ij})$, let $[M]^a$ denote the $n \times m$ matrix defined by

$$([M]^a)_{ij} = \begin{cases} m_{\mathrm{ord}_a(s_i)j} & \text{if } s_i \in a, \\ 1 & \text{otherwise.} \end{cases}$$

The matrix $[M]^a$ is called the *supermatrix of M with respect to a*.

For an $n \times m$ matrix $M = (m_{ij})$, let $[M]_a$ denote the $n' \times m$ submatrix of M defined by

$$([M]_a)_{\mathrm{ord}_a(s_i)j} = m_{ij}$$

for $s_i \in a$. The matrix $[M]_a$ is called the *submatrix of M with respect to a*. The submatrix with respect to the empty set $\emptyset$ is defined to be the empty string ε; i.e. $[M]_\emptyset = \varepsilon$ for all M.

Example 3. Let $\mathcal{S} = \{s_1, s_2, s_3\}$ be an ordered set, and a_1 and a_2 be ordered subsets of $\mathcal{S}$ given by $a_1 = \{s_2\}$ and $a_2 = \{s_1, s_3\}$, respectively. Then

$$[(0)]^{a_1} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \qquad \left[\begin{pmatrix} 01 \\ 10 \end{pmatrix}\right]^{a_2} = \begin{pmatrix} 01 \\ 11 \\ 10 \end{pmatrix},$$
$$\left[\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}\right]_{a_1} = (0), \qquad \left[\begin{pmatrix} 1001 \\ 1010 \\ 1100 \end{pmatrix}\right]_{a_2} = \begin{pmatrix} 1001 \\ 1100 \end{pmatrix}.$$

To consider VSS schemes encrypting multiple images, it is necessary to generalize the definition of an access structure for a single secret. The following definition is a natural generalization from a single secret to multiple ones in which each secret is allowed to have its own access structure.

Definition 4 (Access structure for multiple secrets [16])**.** Let $\mathcal{S}$ be a finite set, and $q \in \mathbb{N}$. For $i \in [q]$, let A^i_Q and A^i_F be subsets of $2^{\mathcal{S}}$ such that $A^i_Q \cap A^i_F = \emptyset$. The pairs Γ^q of the subsets A^i_Q and A^i_F, $\Gamma^q = \{(A^i_Q, A^i_F)\}^q_{i=1}$, is called an *access structure on $\mathcal{S}$ for q secrets* if A^i_Q and A^i_F satisfy the monotonicity,

$$\begin{aligned} A \in A^i_Q \wedge A \subseteq B \Rightarrow B \in A^i_Q, \\ B \in A^i_F \wedge A \subseteq B \Rightarrow A \in A^i_F, \end{aligned} \tag{1}$$

for all $A, B \subseteq \mathcal{S}$ and $i \in [q]$, and the uniqueness,

$$i \neq j \Rightarrow \left(A^i_Q\right)_0 \cap \left(A^j_Q\right)_0 = \emptyset \tag{2}$$

for all $i, j \in [q]$. For an access structure $\Gamma^q = \{(A^i_Q, A^i_F)\}^q_{i=1}$, A^i_Q and A^i_F are called the *qualified set* and the *forbidden set for the i-th secret*, respectively. An access structure $\Gamma^q = \{(A^i_Q, A^i_F)\}^q_{i=1}$ is called *minimally refined* if every qualified sets have only one minimal element; i.e. $|\left(A^i_Q\right)_0| = 1$ for all $i \in [q]$.

Note that each access structure (A^i_Q, A^i_F) can be taken independently without any restrictions except for the uniqueness condition (2). This condition is necessary for VSS schemes because their decryption is restricted to the superposition of visual shares, and so each qualified combination of shares has to be assigned a unique visual secret to be decrypted by the superposition. (Hence, this condition may be removed for the ordinary SS schemes).

If we make the restrictions

$$\forall i \in [|\mathcal{S}|]\left(\left(A^i_Q\right)_0 = \{\{s_i\}\}\right) \text{ with } q = |\mathcal{S}| + 1, \tag{3a}$$
$$\exists A_F \forall i \in [q]\left(A^i_F = A_F\right), \tag{3b}$$
$$\forall i \in [q] \exists k \forall a_Q \in A^i_Q \forall a_F \in A^i_F\left(|a_Q| \geq k \wedge |a_F| < k\right), \tag{3c}$$

then Definition 4 coincides with those for EVCS [1], VSS-q-PI [13] and MVCS [21], respectively. That is, this definition includes the existing ones as special cases.

Definition 4 does not consider correlation among secrets, and we may assume any correlation among them. This allows us to introduce equivalence between access structures as follows.

Definition 5 (Equivalence between access structures)**.** Let $\mathcal{S}$ be a finite set and $p, p', q, q' \in \mathbb{N}$. Let $\nu = \{v_i\}_{i \in [q]}$ and $\nu' = \{v'_i\}_{i \in [q']}$ be sets of random variables over the same domain. A partition $\{I_i\}_{i \in [p]}$ of $[q]$ (i.e. $\bigcup_i I_i = [q]$ and $i \neq j \Rightarrow I_i \cap I_j \neq \emptyset$) is called an *index partition of ν* if

$$\forall k \in I_i \forall l \in I_j (i = j \Leftrightarrow v_k = v_l)$$

for all $i, j \in [p]$. Let $\Gamma = \left\{(A^i_Q, A^i_F)\right\}_{i \in [q]}$ and $\Gamma' = \left\{(A'^i_Q, A'^i_F)\right\}_{i \in [q']}$ be access structures on $\mathcal{S}$ for ν and ν', respectively. The pairs (Γ, ν) and (Γ', ν') are called *equivalent* if there exist index partitions $\{I_i\}_{i \in [p]}$ and $\{I'_i\}_{i \in [p']}$ of ν and ν', respectively, such that

$$\bigcup_{k \in I_i} A^k_Q = \bigcup_{k \in I'_i} A'^k_Q, \quad \bigcap_{k \in I_i} A^k_F = \bigcap_{k \in I'_i} A'^k_F \quad \text{and} \quad v_{r_i} = v'_{r'_i}$$

for all $i \in [p]$ with $p = p'$, where r_i and r'_i are any elements (representative indices) of I_i and I'_i, respectively.

It readily follows from this definition that any access structure can equivalently be transformed into a minimally refined one (with the duplication of secret images allowed).

Having provided a definition of an access structure for multiple secrets, we are ready to give a definition of VSS schemes encrypting multiple images.

Definition 6 (VSS schemes encrypting multiple images [16])**.** Let $\mathcal{S}$ be an ordered set of size n, and $m, q \in \mathbb{N}$. Let $\Gamma^q = \left\{(A^i_Q, A^i_F)\right\}^q_{i=1}$ be an access structure on $\mathcal{S}$ for q secrets. Let Enc be a probabilistic function from $\{0,1\}^q$ to $\{0,1\}^{nm}$ and Dec be a deterministic function from $\{0,1\}^{n'm}$ to $\{0,1\}^m$ with $n' \in [n]$. The pair VSS of functions Enc and Dec, $VSS = (\mathrm{Enc}, \mathrm{Dec})$, is called a *visual secret sharing scheme realizing* Γ^q if Dec is given as the bitwise OR of the rows of input matrices $M = (m_{ij})$,

$$(\mathrm{Dec}(M))_j = \bigvee_{i \in [n']} m_{ij} \tag{4}$$

for all $j \in [m]$ (with $\mathrm{Dec}(\varepsilon) = \varepsilon$), and Enc and Dec satisfy the following two conditions, called the *reconstruct and security conditions* respectively,

$$\forall a \in \left(A^i_Q\right)_0 \left(\gamma^i_1(a) - \gamma^i_1(a) > 0\right), \tag{5}$$
$$\forall a \in A^i_F \forall b \in \{0,1\}^q \left([\mathrm{Enc}(b_{b_i=0})]_a \sim [\mathrm{Enc}(b_{b_i=1})]_a\right), \tag{6}$$

for all $i \in [q]$, where we have defined

$$\gamma_1^i(a) = \min_{b\in\{0,1\}^q} \max\{\gamma | \Pr[g(a; b_{b_i=1}) \geq \gamma] = 1\},$$
$$\gamma_0^i(a) = \max_{b\in\{0,1\}^q} \min\{\gamma | \Pr[g(a; b_{b_i=0}) \leq \gamma] = 1\},$$

with

$$g(a; b) = \mathrm{Gray}(\mathrm{Dec}([\mathrm{Enc}(b)]_a)) \tag{7}$$

for $a \subseteq \mathcal{S}$ and $b \in \{0,1\}^q$. The positive constant

$$c^i(a) = \gamma_1^i(a) - \gamma_0^i(a)$$

in (5) is called the *contrast of the i-th secret for a*. For a VSS scheme $VSS = (\mathrm{Enc}, \mathrm{Dec})$, the number m of the subpixels generated by Enc is called the *pixel expansion* of VSS. A VSS scheme and its encryption are called *optimal* if the scheme has the lowest pixel expansion.

Note that the reconstruct condition (5) has a relaxed form in the sense that the reconstructability is required only for the minimal qualified sets $\big(A_Q^i\big)_0$. This relaxation is necessary for VSS schemes for the same reason as before (see the remark below Definition 4).

Let $I(X : Y|Z)$ denote the mutual information between random variables X and Y conditioned on random variable Z. Then, the security condition (6) can be written in an equivalent form

$$\forall a \in A_F^i \big(I(b_i : [\mathrm{Enc}(b)]_a | b_1, \cdots, b_{i-1}, b_{i+1}, \cdots, b_q) = 0\big)$$

for all random variables b over $\{0,1\}^q$. This equivalent form may help to see that b_i may correlate with $[\mathrm{Enc}(b)]_a$ via other secrets b_j, which is sufficient and useful for our purpose. In what follows, we suppose that the decryption function Dec is the bitwise OR given by (4).

B. Constructions

In this subsection, we introduce a sufficient condition to be satisfied by the encryption of a VSS scheme realizing a general access structure for multiple secrets, and then provide two constructions of VSS schemes with encryption satisfying this condition. To describe the sufficient condition, we first introduce the set of share combinations whose superposition has a constant gray level (with probability 1), and then prove a lemma characterizing it.

Definition 7 (Constant gray level set)**.** Let $\mathcal{S}$ be an ordered set of size n, and $m \in \mathbb{N}$. Let Enc be a probabilistic function from $\{0,1\}$ to $\{0,1\}^{nm}$. The *constant gray level set* $Gr_C(\mathrm{Enc})$ *of* Enc is defined by

$$Gr_C(\mathrm{Enc}) = \{a \subseteq \mathcal{S} | \exists\gamma \forall b \big(\Pr[g(a; b) = \gamma] = 1\big)\},$$

where we have defined

$$g(a; b) = \mathrm{Gray}(\mathrm{Dec}([\mathrm{Enc}(b)]_a))$$

for $a \subseteq \mathcal{S}$ and $b \in \{0,1\}$.

Example 8. Let $\mathcal{S} = \{s_1, s_2, s_3\}$ be an ordered set. Let

$$C^0 = \begin{pmatrix} 11 \\ 01 \\ 01 \end{pmatrix} \quad \text{and} \quad C^1 = \begin{pmatrix} 11 \\ 01 \\ 10 \end{pmatrix},$$

and define $\mathrm{Enc}(b) = \langle C^b \rangle_U$. It readily follows that

$$g(\emptyset; b) = 0 \quad \text{and} \quad g(a; b) = 1$$

for all $b \in \{0,1\}$ and $a \subseteq \mathcal{S}$ such that $s_1 \in a$, with probability 1. Note here that any column permutation of a binary matrix does not change the gray level of its (superposed) rows. Hence, it can be seen that

$$g(a; b) = \frac{1}{2}$$

for all $b \in \{0,1\}$ and $a \in \{\{s_2\}, \{s_3\}\}$, with probability 1. On the other hand, it follows that

$$g(\{s_2, s_3\}; 0) = \frac{1}{2} \quad \text{and} \quad g(\{s_2, s_3\}; 1) = 1,$$

with probability 1. Therefore

$$Gr_C(\mathrm{Enc}) = 2^{\mathcal{S}} - \{\{s_2, s_3\}\}.$$

Lemma 9. Let $\mathcal{S}$ be an ordered set of finite size. Suppose that C^0 and C^1 are a pair of matrices such that $(\mathrm{Enc}, \mathrm{Dec})$ with $\mathrm{Enc}(b) = \langle C^b \rangle_U$ for $b \in \{0,1\}$ realizes an access structure (A_Q, A_F) on $\mathcal{S}$ (for a single secret). Then,

$$\big(A_Q\big)_0 \cap Gr_C(\mathrm{Enc}) = \emptyset \quad \text{and} \quad A_F \subseteq Gr_C(\mathrm{Enc}).$$

Moreover, let $\mathcal{S}^*$ be an ordered set of finite size such that $\mathcal{S}$ is its ordered subset. Define $\mathrm{Enc}^*(b) = \langle [C^b]^{\mathcal{S}} \rangle_U$ for $b \in \{0,1\}$ (where we have used $\mathcal{S} \subseteq \mathcal{S}^*$), and

$$A^* = \{a \subseteq \mathcal{S}^* | a \cap (\mathcal{S}^* - \mathcal{S}) \neq \emptyset\}.$$

Then,

$$A^* \subseteq Gr_C(\mathrm{Enc}^*),$$

and $(\mathrm{Enc}^*, \mathrm{Dec})$ realizes (A_Q^*, A_F^*) on $\mathcal{S}^*$ (for a single secret), where we have introduced A_Q^* and A_F^* by

$$\big(A_Q^*\big)_0 = \big(A_Q\big)_0 \text{ and } A_F^* = \{a \cup \hat{a} | a \in A_F, \hat{a} \subseteq (\mathcal{S}^* - \mathcal{S})\}.$$

Furthermore, if (A_Q, A_F) is perfect, then so is (A_Q^*, A_F^*).

Proof. The contrast condition (5) of VSS schemes (see Definition 6) for a single secret implies that

$$\forall a \in \big(A_Q\big)_0 \big(\Pr[g(a; 1) - g(a; 0) > 0] = 1\big),$$

and so $\forall a \in \big(A_Q\big)_0 \big(a \notin Gr_C(\mathrm{Enc})\big)$, or equivalently,

$$\big(A_Q\big)_0 \cap Gr_C(\mathrm{Enc}) = \emptyset.$$

The security condition (6) of VSS schemes for a single secret gives that for all $a \in A_F$,

$$[\mathrm{Enc}(0)]_a \sim [\mathrm{Enc}(1)]_a,$$

which is equivalent to

$$[C^0]_a \sim [C^1]_a.$$

Again, note that any column permutation of a binary matrix does not change the gray level of its (superposed) rows. Hence, for all $a \in A_F$, there exists γ_a such that

$$g(a; 0) = g(a; 1) = \gamma_a$$

with probability 1, and so

$$A_F \subseteq Gr_C(\mathrm{Enc}).$$

Also, it follows from the definition of the supermatrix that for all $b \in \{0,1\}$ and $a \in A^*$, every column of $[\mathrm{Enc}^*(b)]_a$ has 1 at rows corresponding to $(\mathcal{S}^* - \mathcal{S})$, and so

$$g(a;b) = 1,$$

with probability 1. Hence,

$$A^* \subseteq Gr_C(\mathrm{Enc}^*).$$

We next show that $(\mathrm{Enc}^*, \mathrm{Dec})$ realizes (A_Q^*, A_F^*). Since $(\mathrm{Enc}, \mathrm{Dec})$ realizes (A_Q, A_F) and $\left(A_Q^*\right)_0 = \left(A_Q\right)_0$, it follows from the definition of Enc^* that $(\mathrm{Enc}^*, \mathrm{Dec})$ satisfies the contrast condition (5) of VSS schemes for $\left(A_Q^*\right)_0$. Moreover, the definition of the supermatrix gives that for all $\hat{a} \subseteq (\mathcal{S}^* - \mathcal{S})$, both $[\mathrm{Enc}^*(0)]_{\hat{a}}$ and $[\mathrm{Enc}^*(1)]_{\hat{a}}$ are an all-1 matrix with probability 1, and so

$$[\mathrm{Enc}^*(0)]_{\hat{a}} \sim [\mathrm{Enc}^*(1)]_{\hat{a}}.$$

This, together with $[\mathrm{Enc}(0)]_a \sim [\mathrm{Enc}(1)]_a$ for $a \in A_F$, gives

$$[\mathrm{Enc}^*(0)]_{a^*} \sim [\mathrm{Enc}^*(1)]_{a^*}$$

for all $a^* \in A_F^* = \{a \cup \hat{a} | a \in A_F, \hat{a} \subseteq (\mathcal{S}^* - \mathcal{S})\}$, and so $(\mathrm{Enc}^*, \mathrm{Dec})$ satisfies the security condition (6) for A_F^*.

To show the last part of the lemma, suppose that $a^* \notin A_F^*$. Then, on noting that

$$\begin{aligned} A_F^* &= \{a \cup \hat{a} | a \in A_F, \hat{a} \subseteq (\mathcal{S}^* - \mathcal{S})\} \\ &= \{a^* \subseteq \mathcal{S}^* | (a^* \cap \mathcal{S}) \in A_F\}, \end{aligned}$$

we have $(a^* \cap \mathcal{S}) \notin A_F$, and so $(a^* \cap \mathcal{S}) \in A_Q$ because $(a^* \cap \mathcal{S}) \subseteq \mathcal{S}$ and (A_Q, A_F) is perfect. Therefore, the monotonicity (1) of the qualified set A_Q gives that there exists $a \in \left(A_Q\right)_0 = \left(A_Q^*\right)_0$ such that

$$a \subseteq (a^* \cap \mathcal{S}) \subseteq a^*,$$

which implies $a^* \in A_Q^*$. That is, if $a^* \notin A_F^*$, then $a^* \in A_Q^*$, and so (A_Q^*, A_F^*) is also perfect. This completes the proof. □

We are now ready to introduce a property, called the compatibility, for a set of VSS encryptions. The subsequent construction and theorem show that this property is indeed a sufficient condition to be satisfied by a set of VSS encryptions whose concatenation with random column permutation gives the encryption of a VSS scheme realizing a general access structure for multiple secrets.

Definition 10 (Compatible encryption)**.** Let $\mathcal{S}$ be an ordered set of size n, and $q \in \mathbb{N}$. For $i \in [q]$, let Enc_i be a probabilistic function from $\{0,1\}$ to $\{0,1\}^{nm_i}$ with $m_i \in \mathbb{N}$. Let $\Gamma^q = \left\{(A_Q^i, A_F^i)\right\}_{i=1}^q$ be an access structure on $\mathcal{S}$ for q secrets. A set $\{\mathrm{Enc}_i\}_{i=1}^q$ of probabilistic functions is called *compatible with respect to* Γ^q if the following two conditions hold:

1) $(\mathrm{Enc}_i, \mathrm{Dec})$ realizes (A_Q^i, A_F^i) for all $i \in [q]$,
2) $i \neq j \Rightarrow \left(A_Q^i\right)_0 \subseteq Gr_C(\mathrm{Enc}_j)$ for all $i, j \in [q]$.

Construction 11 (General construction)**.** Let $\mathcal{S}$ be an ordered set of finite size, and $q \in \mathbb{N}$. Let $\Gamma^q = \left\{(A_Q^i, A_F^i)\right\}_{i=1}^q$ be an access structure on $\mathcal{S}$ for q secrets. Let $\left\{(C_i^0, C_i^1)\right\}_{i=1}^q$ be pairs of matrices such that the set $\{\mathrm{Enc}_i\}_{i=1}^q$ of encryption functions $\mathrm{Enc}_i(b) = \langle C_i^b \rangle_U$ is compatible with respect to Γ^q. Define Enc by

$$\mathrm{Enc}(b) = \left\langle C_1^{b_1} | C_2^{b_2} | \cdots | C_q^{b_q} \right\rangle_U$$

for $b \in \{0,1\}^q$.

Theorem 12. Let $\mathcal{S}$ be an ordered set of finite size, and $q \in \mathbb{N}$. Let Γ^q be an access structure on $\mathcal{S}$ for q secrets. Then, $VSS = (\mathrm{Enc}, \mathrm{Dec})$ given by Construction 11 is a visual secret sharing scheme realizing Γ^q.

Proof. We first show that $(\mathrm{Enc}, \mathrm{Dec})$ satisfies the contrast condition (5). Let $i \in [q]$ and $a \in \left(A_Q^i\right)_0$. It follows from the condition 2) of the compatible encryption (see Definition 10) that for all $j \in [q]$ such that $j \neq i$, there exists $l_j \in \{0\} \cup [m_j]$ such that

$$g_j(a;0) = g_j(a;1) = \frac{l_j}{m_j}$$

with probability 1, where m_j is the pixel expansion of Enc_j and we have defined

$$g_j(a;b) = \mathrm{Gray}(\mathrm{Dec}([\mathrm{Enc}_j(b)]_a))$$

as before (see (7)). It also follows from the condition 1) of the compatible encryption that there exists $d_i \in [m_i]$ such that

$$g_i(a;1) - g_i(a;0) \geq \frac{d_i}{m_i}$$

with probability 1. Therefore, the contrast of the i-th secret for a is lower-bounded as

$$c^i(a) \geq \frac{d_i}{m} > 0$$

with $m = \sum_{i \in [q]} m_i$, from which the contrast condition (5) follows.

We next show that $(\mathrm{Enc}, \mathrm{Dec})$ satisfies the security condition (6). Let $i \in [q]$ and $a \in A_F^i$. It follows from the condition 1) of the compatible encryption that

$$\left[\left\langle C_i^0 \right\rangle_U\right]_a \sim \left[\left\langle C_i^1 \right\rangle_U\right]_a,$$

which is equivalent to

$$\left[C_i^0\right]_a \sim \left[C_i^1\right]_a.$$

This at once gives

$$\left[C_1^{b_1} | \cdots | C_i^0 | \cdots | C_q^{b_q}\right]_a \sim \left[C_1^{b_1} | \cdots | C_i^1 | \cdots | C_q^{b_q}\right]_a$$

for all $b \in \{0,1\}^q$, and so

$$\left[\left\langle C_1^{b_1} | \cdots | C_i^0 | \cdots | C_q^{b_q} \right\rangle_U\right]_a \sim \left[\left\langle C_1^{b_1} | \cdots | C_i^1 | \cdots | C_q^{b_q} \right\rangle_U\right]_a,$$

from which the security condition (6) follows. This completes the proof. □

It should be stated that Construction 11 assumes the existence of the basis matrices $\left\{(C_i^0, C_i^1)\right\}_{i=1}^q$, and does not specify the way to find them. We now provide another construction which specifies the basis matrices, and so can straightforwardly be implemented. Since any access structure can be transformed into a minimally refined one (with the duplication

of secret images allowed), the following construction also applies to general access structures for multiple secrets (see Definition 4 for minimally refined access structures). As will be seen in the proof of Corollary 14 below, this construction is a special case of Construction 11.

Construction 13 (Construction with a straightforward implementation [16])**.** Let $\mathcal{S}$ be an ordered set of finite size, and $q \in \mathbb{N}$. Let $\Gamma^q = \left\{(A_Q^i, A_F^i)\right\}_{i=1}^q$ be a minimally refined access structure on $\mathcal{S}$ for q secrets. For $i \in [q]$, let a_q^i be the element of $\left(A_Q^i\right)_0$; i.e. $\left(A_Q^i\right)_0 = \{a_q^i\}$ with $a_q^i \subseteq \mathcal{S}$. For $b \in \{0,1\}$ and $i \in [q]$, let $C_i^b = [C_{n_i,n_i}^b]^{a_q^i}$ with $n_i = |a_q^i|$. Define Enc by

$$\mathrm{Enc}(b) = \left\langle C_1^{b_1} | C_2^{b_2} | \cdots | C_q^{b_q} \right\rangle_U$$

for $b \in \{0,1\}^q$ (see section II-D for the definition of $C_{n,n}^b$).

Corollary 14. Let $\mathcal{S}$ be an ordered set of finite size, and $q \in \mathbb{N}$. Let $\Gamma^q = \left\{(A_Q^i, A_F^i)\right\}_{i=1}^q$ be a minimally refined access structure on $\mathcal{S}$ for q secrets. Then, $VSS = (\mathrm{Enc}, \mathrm{Dec})$ given by Construction 13 is a visual secret sharing scheme realizing Γ^q.

Proof. Define $\mathrm{Enc}_i(b) = \langle C_i^b \rangle_U$ for $i \in [q]$ and $b \in \{0,1\}$. We now show that $\{\mathrm{Enc}_i\}_{i=1}^q$ is compatible with respect to Γ^q. Since $\{C_{n,n}^b\}_{b\in\{0,1\}}$ are basis matrices for a VSS scheme realizing an (n,n)-threshold access structure, which is perfect, it follows from Lemma 9 that $(\mathrm{Enc}_i, \mathrm{Dec})$ realizes (A_Q^i, A_F^{i*}) with $A_F^{i*} = 2^{\mathcal{S}} - A_Q^i$. Here, on noting that A_Q^i and A_F^i are disjoint, we have $A_F^i \subseteq A_F^{i*}$. Therefore, the condition 1) of the compatible encryption follows.

Moreover, Lemma 9 yields that

$$\{a_q^i\} \not\subseteq Gr_C(\mathrm{Enc}_i) \quad \text{and} \quad A \subseteq Gr_C(\mathrm{Enc}_i)$$

with

$$A = \{a | a \subset a_q^i\} \cup \{a \subseteq \mathcal{S} | a \cap (\mathcal{S} - a_q^i) \neq \emptyset\}.$$

Therefore,

$$Gr_C(\mathrm{Enc}_i) = 2^{\mathcal{S}} - \{a_q^i\},$$

and so the condition 2) of the compatible encryption follows from the uniqueness (2) of Γ^q. Consequently, the corollary follows from Theorem 12. □

C. Illustrative examples

Let $\mathcal{S} = \{s_1, s_2, s_3\}$ be a set of shares. We now give three VSS schemes according to Constructions 11 and 13. First, we consider the following minimally refined perfect access structure $\Gamma^7 = \left\{(A_Q^i, A_F^i)\right\}_{i=1}^7$ on $\mathcal{S}$ for seven secret images $\{v_i\}_{i=1}^7$ of the same size, where

$$\left(A_Q^1\right)_0 = \{\{s_1\}\},\ \left(A_Q^2\right)_0 = \{\{s_2\}\},\ \left(A_Q^3\right)_0 = \{\{s_3\}\},$$
$$\left(A_Q^4\right)_0 = \{\{s_1, s_2\}\},\ \left(A_Q^5\right)_0 = \{\{s_1, s_3\}\},$$
$$\left(A_Q^6\right)_0 = \{\{s_2, s_3\}\},\ \left(A_Q^7\right)_0 = \{\{s_1, s_2, s_3\}\}$$

with $A_F^i = 2^{\mathcal{S}} - A_Q^i$ for all $i \in [7]$. Since Γ^7 is minimally refined, Construction 13 directly applies to this access structure as follows. Let $\{C_i^0, C_i^1\}_{i=1}^7$ be pairs of matrices defined according to Construction 13; namely,

$$C_1^0 = \begin{pmatrix}0\\1\\1\end{pmatrix},\ C_2^0 = \begin{pmatrix}1\\0\\1\end{pmatrix},\ C_3^0 = \begin{pmatrix}1\\1\\0\end{pmatrix},\ C_7^0 = \begin{pmatrix}0011\\0101\\0110\end{pmatrix},$$
$$C_1^1 = \begin{pmatrix}1\\1\\1\end{pmatrix},\ C_2^1 = \begin{pmatrix}1\\1\\1\end{pmatrix},\ C_3^1 = \begin{pmatrix}1\\1\\1\end{pmatrix},\ C_7^1 = \begin{pmatrix}1001\\1010\\1100\end{pmatrix},$$
$$C_4^0 = \begin{pmatrix}01\\01\\11\end{pmatrix},\ C_5^0 = \begin{pmatrix}01\\11\\01\end{pmatrix},\ C_6^0 = \begin{pmatrix}11\\01\\01\end{pmatrix},$$
$$C_4^1 = \begin{pmatrix}01\\10\\11\end{pmatrix},\ C_5^1 = \begin{pmatrix}01\\11\\10\end{pmatrix},\ C_6^1 = \begin{pmatrix}11\\01\\10\end{pmatrix}.$$

Suppose that the top-left pixels of the secret images $\{v_i\}_{i=1}^7$ have values $b \in \{0,1\}^7$, where $b_i = 0$ if the corresponding pixel in v_i is white and $b_i = 1$ otherwise. Then, the encryption of values b of the top-left pixels is given by

$$\mathrm{Enc}(b) = \left\langle C_1^{b_1} | C_2^{b_2} | \cdots | C_7^{b_7} \right\rangle_U.$$

All the other pixels of the secret images are encrypted in the same way. It follows from Corollary 14 that the VSS scheme with this encryption realizes Γ^7. Figure 1 illustrates an example of this VSS scheme (slightly modified to make the pixel expansion a square).

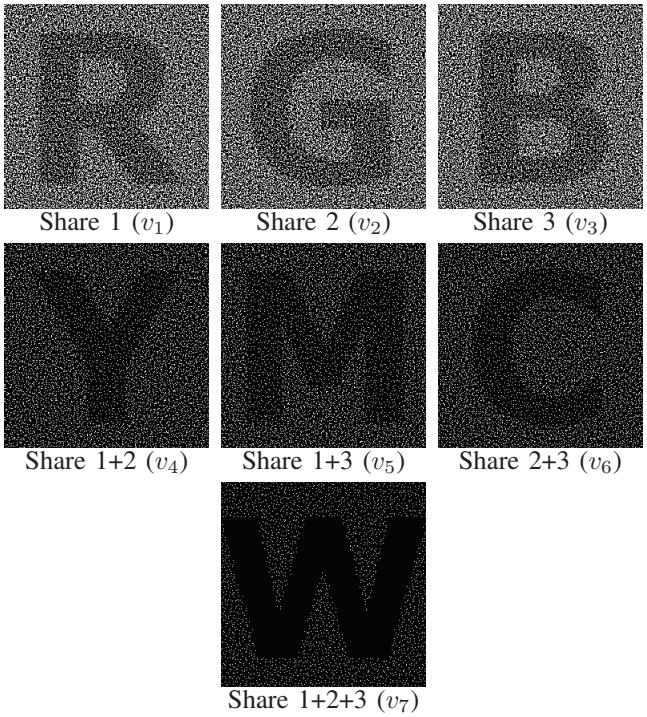

Fig. 1. Example of a VSS scheme realizing Γ^7 with secret images $\{v_i\}_{i=1}^7$ representing the additive mixture of the primary colors red, green and blue. In this example, $C_1^{b_1}$, $C_2^{b_2}$ and $C_3^{b_3}$ are concatenated twice to make the pixel expansion m a square: $m = 1 \times 3 \times 2 + 2 \times 3 + 4 \times 1 = 4^2$. Hence, the contrast is $\frac{2}{16}$ for $\{v_i\}_{i=1}^3$ and $\frac{1}{16}$ for $\{v_i\}_{i=4}^7$.

Next, we consider the following perfect access structure $\Gamma^2 = \left\{(A_Q^i, A_F^i)\right\}_{i=1}^2$ on $\mathcal{S}$ for two secret images $\{v_i\}_{i=1}^2$ of the same size, where

$$\left(A_Q^1\right)_0 = \{\{s_1, s_2\}, \{s_1, s_3\}\},\quad \left(A_Q^2\right)_0 = \{\{s_2, s_3\}\}$$

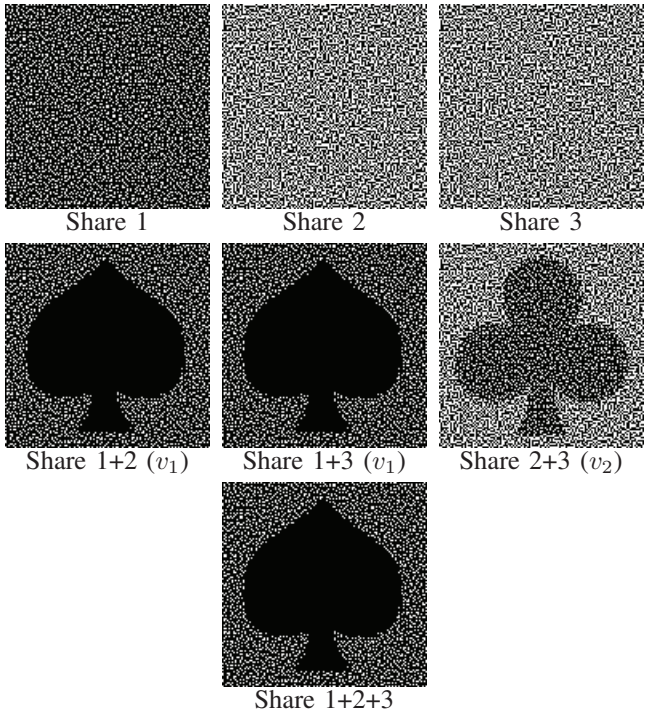

Fig. 2. Example of a VSS scheme realizing Γ^2 with secret images $\{v_i\}_{i=1}^2$. The pixel expansion is $2+2=4$, and the contrast is $\frac{1}{4}$ for all the reconstructed images. In this construction, Share 1+2+3, which is not a minimal element of the qualified sets, reveals the secret v_1.

with $A_F^i = 2^{\mathcal{S}} - A_Q^i$ for all $i \in [2]$. Note that Γ^2 is not minimally refined ($|(A_Q^1)_0| > 1$), and so Construction 13 is not (directly) applicable to this access structure. Hence, we first apply Construction 11 to Γ^2 as follows. Let $\{C_i^0, C_i^1\}_{i=1}^2$ be pairs of matrices defined by

$$C_1^0 = \begin{pmatrix}01\\01\\01\end{pmatrix}, \quad C_2^0 = \begin{pmatrix}11\\01\\01\end{pmatrix},$$
$$C_1^1 = \begin{pmatrix}01\\10\\10\end{pmatrix}, \quad C_2^1 = \begin{pmatrix}11\\01\\10\end{pmatrix},$$

respectively, and define $\mathrm{Enc}_i(b) = \langle C_i^b \rangle$ for $b \in \{0,1\}$ and $i \in [2]$. Then, $\{\mathrm{Enc}_i\}_{i=1}^2$ is compatible with respect to Γ^2. In fact, it can be seen from the above definitions that $(\mathrm{Enc}_i, \mathrm{Dec})$ realizes (A_Q^i, A_F^i) for all $i \in [2]$, and

$$Gr_C(\mathrm{Enc}_1) = \{\emptyset, \{s_1\}, \{s_2\}, \{s_3\}, \{s_2, s_3\}\},$$
$$Gr_C(\mathrm{Enc}_2) = 2^{\mathcal{S}} - \{\{s_2, s_3\}\},$$

and so

$$(A_Q^1)_0 \subseteq Gr_C(\mathrm{Enc}_2), \quad (A_Q^2)_0 \subseteq Gr_C(\mathrm{Enc}_1).$$

Therefore, Theorem 12 ensures that the VSS scheme with the encryption defined by

$$\mathrm{Enc}(b) = \left\langle C_1^{b_1} | C_2^{b_2} \right\rangle_U$$

for $b \in \{0,1\}^2$ realizes Γ^2. Figure 2 illustrates an example of this VSS scheme.

We can also provide a VSS scheme realizing Γ^2 according to Construction 13. For this purpose, we introduce a minimally refined access structure which, together with an appropriate supposition on secret images, is equivalent to Γ^2. Let $\Gamma^3 = \{(A_Q'^i, A_F'^i)\}_{i=1}^3$ be the minimally refined perfect access structure on $\mathcal{S}$ for three secret images $\{v_i'\}_{i=1}^3$ of the same size such that

$$(A_Q'^1)_0 = \{\{s_1, s_2\}\}, \quad (A_Q'^2)_0 = \{\{s_1, s_3\}\},$$
$$(A_Q'^3)_0 = \{\{s_2, s_3\}\},$$

with $A_F'^i = 2^{\mathcal{S}} - A_Q'^i$ for all $i \in [3]$. Since Γ^3 is minimally refined, Construction 13 directly applies to this access structure as before. Let $\{C_i^0, C_i^1\}_{i=1}^3$ be pairs of matrices defined according to Construction 13; namely,

$$C_1^0 = \begin{pmatrix}01\\01\\11\end{pmatrix}, \quad C_2^0 = \begin{pmatrix}01\\11\\01\end{pmatrix}, \quad C_3^0 = \begin{pmatrix}11\\01\\01\end{pmatrix},$$
$$C_1^1 = \begin{pmatrix}01\\10\\11\end{pmatrix}, \quad C_2^1 = \begin{pmatrix}01\\11\\10\end{pmatrix}, \quad C_3^1 = \begin{pmatrix}11\\01\\10\end{pmatrix}.$$

It then follows from Corollary 14 that the VSS scheme with the encryption defined by

$$\mathrm{Enc}(b) = \left\langle C_1^{b_1} | C_2^{b_2} | C_3^{b_3} \right\rangle_U$$

for $b \in \{0,1\}^3$ realizes Γ^3. Here, note that

$$A_Q^1 = A_Q'^1 \cup A_Q'^2, \quad A_Q^2 = A_Q'^3,$$
$$A_F^1 = A_F'^1 \cap A_F'^2, \quad A_F^2 = A_F'^3.$$

Hence, if we suppose that

$$v_1 = v_1' = v_2' \quad \text{and} \quad v_2 = v_3',$$

then $(\Gamma^3, \{v_i'\}_{i=1}^3)$ and $(\Gamma^2, \{v_i\}_{i=1}^2)$ are equivalent. Figure 3 illustrates an example of this VSS scheme (slightly modified to make the pixel expansion a square). The last two examples show that Construction 11 can generate a VSS scheme with strictly better contrast and pixel expansion than Construction 13. We close this subsection by noting that no existing schemes can realize the above access structures for multiple secrets, which can be confirmed by checking that these access structures satisfy none of the formulas (3a)–(3c).

D. Comparison with existing schemes for threshold access structures

For $n \in \mathbb{N}$ and $s \in [n]$, consider the following threshold access structure $\Gamma^s = \{(A_Q^i, A_F^i)\}_{i \in [s]}$ on $\mathcal{S} = \{s_1, \cdots, s_n\}$ for s secrets, where

$$A_Q^i = \{a \subseteq \mathcal{S} \,|\, |a| \geq n - i + 1\}$$

with $A_F^i = 2^{\mathcal{S}} - A_Q^i$ for all $i \in [s]$, which can be realized by (k, n, s)-MVCS with $k = n - s + 1$ [21]. It readily follows from this definition that $|(A_Q^i)_0| = {}_nC_{n-i+1}$, where ${}_nC_k$ denotes the binomial coefficient indexed by n and k. Hence, by transforming Γ^s into a minimally refined one and then applying Construction 13 to it, we have a VSS scheme realizing Γ^s with the pixel expansion

$$\sum_{i=1}^{s} {}_nC_{n-i+1} 2^{(n-i+1)-1} = \sum_{i=k}^{n} {}_nC_i 2^{i-1},$$

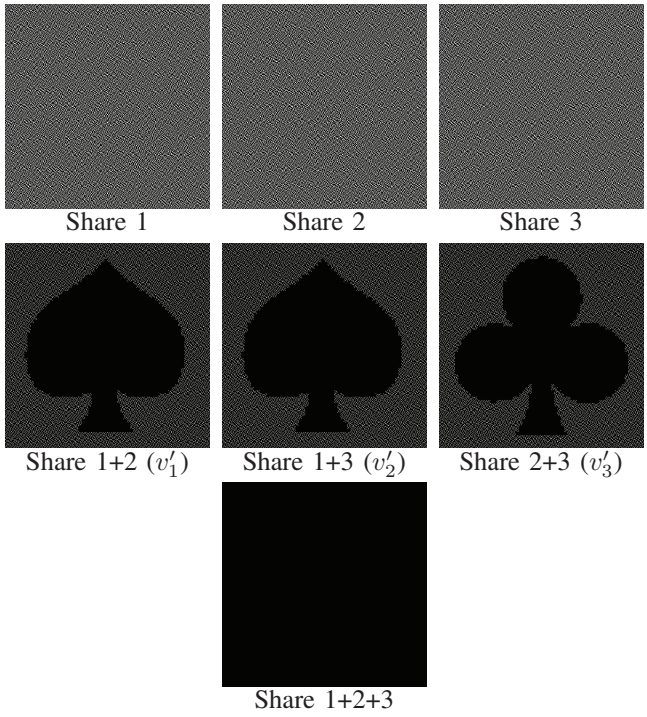

Fig. 3. Example of a VSS scheme realizing Γ^3 with secret images $\{v_i'\}_{i=1}^3$, where $(\Gamma^3, \{v_i'\}_{i=1}^3)$ is equivalent to $(\Gamma^2, \{v_i\}_{i=1}^2)$. In this example, all the matrices are concatenated 6 times to make the pixel expansion m a square: $m = (2+2+2) \times 6 = 6^2$ (we may take $m = 2+2+2 = 6$ if m need not be a square). The contrast is $\frac{1}{6}$ for all the reconstructed images. In this construction, Share 1+2+3, which is not a minimal element of the qualified sets, is an all-black image.

where we have used the fact that the pixel expansion of an optimal (n, n)-threshold VSS scheme is 2^{n-1} [15]. This formula gives exactly the same pixel expansions as those of (k, n, s)-MVCS for $2 \le k \le n \le 8$ and $s = n - k + 1$ (see Table I in [21]). We note that the pixel expansions of (k, n, s)-MVCS are not explicitly given in a general form but determined by solving linear programming problems for each instance.

Next, let $n \in \mathbb{N}$, $k \in [n]$ and $s \in [n-k+1]$, and suppose that a list $R = (r_k, \cdots, r_n)$ satisfies the following two conditions: (i) $r_i \in \{0\} \cup [s]$ for any $i \in \{k, \cdots, n\}$ and (ii) $|\{i \in \{k, \cdots, n\} | r_i = s'\}| = 1$ for any $s' \in [s]$ (see [21] for details of the revealing list R). Now, let us consider the threshold access structure $\hat{\Gamma}^s = \left\{(A_Q^i, A_F^i)\right\}_{i \in [s]}$ on $\mathcal{S} = \{s_1, \cdots, s_n\}$ for s secrets, where

$$A_Q^i = \left\{a \subseteq \mathcal{S} \middle| |a| \ge \mathrm{index}_R(i)\right\}$$

with $A_F^i = 2^{\mathcal{S}} - A_Q^i$ for all $i \in [s]$, which can be realized by (k, n, s, R)-MVCS [21]. Here, for $s' \in [s]$ and $R = (r_k, \cdots, r_n)$ satisfying the above conditions (i) and (ii) such that $r_i = s'$ (where the existence and uniqueness of such r_i follow from the condition (ii)), we have defined

$$\mathrm{index}_R(s') = i$$

(note that $i \in \{k, \cdots, n\}$). By transforming Γ^s into a minimally refined one and then applying Construction 13 to it as before, we have a VSS scheme realizing $\hat{\Gamma}^s$ with the pixel expansion

$$\sum_{i=1}^{s} {}_nC_{\mathrm{index}_R(i)} 2^{\mathrm{index}_R(i)-1}.$$

This formula also gives exactly the same pixel expansions as those of (k, n, s, R)-MVCS for $2 \le k \le n-s$, $k+s \le n \le 8$ and $2 \le s \le 4$ (see Table II–IV in [21]). Again, we note that the pixel expansions of (k, n, s, R)-MVCS are not explicitly given in a general form but determined by solving linear programming problems for each instance.

E. On optimality

In general, it is difficult to (directly) examine the optimality of SS schemes realizing a general access structure (see, e.g., [3], [10]); in fact, the optimality has been shown so far only for very limited classes of SS schemes such as threshold SS schemes [17], threshold VSS schemes [5], [6] and (non-perfect) uniform SS schemes [12].[9] Hence, instead of directly examining the optimality, we now examine the possibility that the optimality of Construction 11 may be reduced to that of each encryption Enc_i. For this purpose, consider first a simple access structure $\Gamma = \left\{(A_Q^i, A_F^i)\right\}_{i=1}^2$ on $\mathcal{S} = \{s_1, s_2\}$ for 2 secrets, given by

$$\left(A_Q^1\right)_0 = \left\{\{s_1\}\right\} \quad \text{and} \quad \left(A_Q^2\right)_0 = \left\{\{s_2\}\right\}$$

with $A_F^i = 2^{\mathcal{S}} - A_Q^i$ for all $i \in [2]$. This access structure can be realized by a VSS scheme with the (deterministic) encryption given by

$$\mathrm{Enc}(b) = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$

for $b \in \{0,1\}^2$, while any VSS scheme generated by Construction 11 has the pixel expansion no less than 2. Note that the above matrix is the concatenation of the basis matrices $C_{1,1}^{b_1}$ and $C_{1,1}^{b_2}$ with respect to the row (not column).

More generally, let $\Gamma = \left\{(A_Q^i, A_F^i)\right\}_{i=1}^q$ be an access structure for q secrets, and for $i \in [q]$, let $\mathcal{S}_0^i$ be the union of $\left(A_Q^i\right)_0$; i.e. $\mathcal{S}_0^i = \bigcup_{a \in (A_Q^i)_0} a$. Moreover, let $A_Q^{i\star}$ and $A_F^{i\star}$ be the restrictions of A_Q and A_F on $\mathcal{S}_0^i$, respectively; i.e.

$$A_Q^{i*} = A_Q^i \cap 2^{\mathcal{S}_0^i} \quad \text{and} \quad A_F^{i*} = A_F^i \cap 2^{\mathcal{S}_0^i}.$$

Suppose further that $\left\{\mathcal{S}_0^i\right\}_{i=1}^q$ are disjoint, $i \ne j \Rightarrow \mathcal{S}_0^i \cap \mathcal{S}_0^j = \emptyset$ for all $i, j \in [q]$, and let $VSS_i = (\mathrm{Enc}_i^\star, \mathrm{Dec})$ be an optimal VSS scheme realizing $(A_Q^{i\star}, A_F^{i\star})$, with pixel expansion m_i. Then we can construct an optimal VSS scheme realizing Γ by defining its encryption to be the concatenation of $\{\mathrm{Enc}_i^\star\}_i$ with respect to the row (with padding 1 if necessary). Hence the optimal pixel expansion for Γ is $\max_i m_i$ (which comes from the row concatenation), while any VSS scheme generated by Construction 11 has the pixel expansion no less than $\sum_i m_i$ (which comes from the column concatenation). Since $\max_i m_i < \sum_i m_i$ for $q \ge 2$, this shows that there exist access structures for which Construction 11 generates no optimal VSS schemes.

[9] An SS scheme is called uniform if it realizes an access structure which is invariant under a permutation of the shares.

IV. Concluding remarks

We close this paper by mentioning an application of our VSS schemes. In the authentication based on VSS schemes encrypting a single secret image, one way to detect tampering by an adversary is to divide the secret image into two disjoint areas: one for a message and the other for the detection (see e.g. the first method "content areas and black areas" in [14]). On the other hand, VSS schemes encrypting multiple images allow the authentication which can take the above two areas identical; for instance, the second example in section III-C allows the authentication in which Shares 1 and 3 are distributed to a human recipient, Share 2 is generated by an informant, and the two secrets v_1 and v_2 are taken to be an all-black image for the detection and an image for a message, respectively. (Here, we note that v_1 and v_2 can be decrypted by superposing two (not three) shares and the reconstructed images have pixel expansion 4 and contrast $\frac{1}{4}$.) This authentication, equipped with the idea behind the third method "black and gray" in [14], ensures that an adversary cannot tamper with the latter image without tampering with the former, which makes its security analysis simpler and more practical. It will be the subject of future work to investigate this authentication in more detail.

References

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

[2] A. Beimel, "Secret-sharing schemes: A survey," in *Proceedings of the 3rd International Workshop on Coding and Cryptology (IWCC 2011)*, ser. Lecture Notes in Computer Science. Springer-Verlag, 2011, vol. 6639, pp. 11–46.

[3] A. Beimel and I. Orlov, "Secret sharing and non-shannon information inequalities," *IEEE Transactions on Information Theory*, vol. 57, no. 9, pp. 5634–5649, 2011.

[4] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of the National Computer Conference*. Monval, NJ, USA: AFIPS Press, 1979, pp. 313–317.

[5] C. Blundo, P. D'Arco, A. D. Santis, and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," *SIAM Journal on Discrete Mathematics*, vol. 16, no. 2, pp. 224–261, 2003.

[6] M. Bose and R. Mukerjee, "Optimal (k, n) visual cryptographic schemes for general k," *Designs, Codes and Cryptography*, vol. 55, no. 1, pp. 19–35, 2010.

[7] Y. C. Chen, "Fully incrementing visual cryptography from a succinct non-monotonic structure," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 5, pp. 1082–1091, May 2017.

[8] S. Cimato, R. De Prisco, and A. De Santis, "Optimal colored threshold visual cryptography schemes," *Designs, Codes and Cryptography*, vol. 35, no. 3, pp. 311–335, 2005.

[9] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Wiley-Interscience, 2006.

[10] L. Csirmaz, "The size of a share must be large," *Journal of Cryptology*, vol. 10, no. 4, pp. 223–231, 1997.

[11] Y. Desmedt, S. Hou, and J.-J. Quisquater, "Audio and optical cryptography," in *Proceedings of Advances in Cryptology – Asiacrypt '98*, ser. Lecture Notes in Computer Science, vol. 1514. Springer-Verlag, 1998, pp. 392–404.

[12] O. Farras, T. Hansen, T. Kaced, and C. Padro, "Optimal non-perfect uniform secret sharing schemes," in *Proceedings of Advances in Cryptology – Crypto 2014*, ser. Lecture Notes in Computer Science, vol. 8617. Springer-Verlag, 2014, pp. 217–234.

[13] M. Iwamoto and H. Yamamoto, "A construction method of visual secret sharing schemes for plural secret images," *IEICE Trans. Fundamentals*, vol. E86-A, no. 10, pp. 2577–2588, 2003.

[14] M. Naor and B. Pinkas, "Visual authentication and identification," in *Proceedings of Advances in Cryptology – Crypto '97*, ser. Lecture Notes in Computer Science, vol. 1294. Springer-Verlag, 1997, pp. 322–336.

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

[16] M. Sasaki and Y. Watanabe, "Formulation of visual secret sharing schemes encrypting multiple images," in *Proceedings of the 39th IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2014)*. IEEE, 2014, pp. 7391–7395.

[17] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[18] S. J. Shyu, "Threshold visual cryptographic scheme with meaningful shares," *IEEE Signal Processing Letters*, vol. 21, no. 12, pp. 1521–1525, 2014.

[19] S. J. Shyu and K. Chen, "Visual multiple-secret sharing by circle random grids," *SIAM Journal on Imaging Sciences*, vol. 3, no. 4, pp. 926–953, 2010.

[20] S. J. Shyu, S.-Y. Huang, Y.-K. Lee, R.-Z. Wang, and K. Chen, "Sharing multiple secrets in visual cryptography," *Pattern Recognition*, vol. 40, no. 12, pp. 3633–3651, 2007.

[21] S. J. Shyu and H.-W. Jiang, "General constructions for threshold multiple-secret visual cryptographic schemes," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 5, pp. 733–743, 2013.

[22] D. R. Stinson, *Cryptography: Theory and Practice*, 3rd ed. Chapman & Hall, CRC, 2005.

[23] E. R. Verheul and H. C. van Tilborg, "Constructions and properties of k out of n visual secret sharing schemes," *Designs, Codes and Cryptography*, vol. 11, no. 2, pp. 179–196, 1997.

[24] R.-Z. Wang, "Region incrementing visual cryptography," *IEEE Signal Processing Letters*, vol. 16, no. 8, pp. 659–662, 2009.

[25] S. Washio and Y. Watanabe, "Security of audio secret sharing scheme encrypting audio secrets with bounded shares," in *Proceedings of the 39th IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2014)*. IEEE, 2014, pp. 7396–7400.

[26] C.-N. Yang and T.-H. Chung, "A general multi-secret visual cryptography scheme," *Optics Communications*, vol. 283, no. 24, pp. 4949–4962, 2010.