Visual Secret Sharing Schemes for Multiple Secret Images Allowing the Rotation of Shares*

Mitsugu IWAMOTO†a, Member, Lei WANG†, Nonmember, Kazuki YONEYAMA††, Student Member, Noboru KUNIHIRO†††, and Kazuo OHTA††††, Members

SUMMARY In this paper, a method is proposed to construct a visual secret sharing (VSS) scheme for multiple secret images in which each share can be rotated with 180 degrees in decryption. The proposed VSS scheme can encrypt more number of secret images compared with the normal VSS schemes. Furthermore, the proposed technique can be applied to the VSS scheme that allows to turn over some shares in decryption. From the theoretical point of view, it is interesting to note that such VSS schemes cannot be obtained from so-called basis matrices straightforwardly.

key words: visual secret sharing schemes, visual cryptography, secret sharing schemes, multiple secret images, rotation of shares

1. Introduction

A visual secret sharing (VSS) scheme, which originates from visual cryptography proposed by Naor-Shamir [1], is one realization of secret sharing schemes [2]. In VSS schemes, a secret image is encrypted into several images called shares, each of which does not reveal any information of the secret image. Each share is usually printed on a transparency, and the secret image can be decrypted only by stacking the transparencies in arbitrary order. Hence, VSS schemes need no computation in decryption. First VSS scheme proposed by Naor-Shamir is a (k, n)-threshold VSS scheme for black and white binary secret images. The (k, n)-threshold VSS scheme means that the secret image can be decrypted by stacking arbitrary k out of n shares and no information of the secret image must leak out from any k − 1 or less shares.

After [1], the improvements in the quality of decrypted images for (k, n)-threshold VSS schemes are extensively studied [3]–[15], and many extensions of the VSS schemes are proposed. In [4], [8], [9], [16]–[23], not only black-white secret images but also color or gray scale secret images are treated, and the (k, n)-threshold access structures in VSS schemes are extended to so-called general access structures [8], [24]. General access structures consist of qualified sets and forbidden sets where the secret image can be decrypted from every qualified set, and no information can be obtained from any forbidden set. Furthermore, VSS schemes for q multiple secret images are proposed in [3], [25]–[28], especially, it is discussed in [28] how to construct the VSS schemes for q multiple secret images with general access structures, VSS-q-MI schemes for short.

We note that, in the VSS schemes shown above, each secret image is obtained only by stacking a set of shares. Recently, new and interesting VSS schemes that allow the other operations in decryption besides stacking are proposed [29], [30]. In such VSS schemes, black and white in each subpixel can be exchanged in decryption, and it is shown that the secret image can completely be reproduced by such method [30]. However, such VSS schemes have a disadvantage such that the decryption cannot be achieved only by human eyes since they use copy machines in order to exchange two colors. Hence, we consider the VSS schemes which include the other operations of shares besides stacking, e.g., rotating or tuning over the shares. By using such operations, more secret images can be encrypted compared with the normal VSS schemes. For example, assume that we have two shares denoted by V1 and V2. Then, in the normal VSS schemes, only one secret image may be decrypted from V1 and V2. On the other hand, if we allow rotating the shares** before stacking, a new VSS scheme can be considered such that one secret image can be obtained by stacking V1 and V2, and the other secret image can be decrypted by stacking up V1 and V2 upside-down. In the following, we call VSS schemes with q multiple secret images allowing the rotation of shares, VSS-q-MI-R schemes for short. In general, we can encrypt at most (3q − 1)/2 images*** by using the VSS schemes allowing the rotation of shares although at most 2q − 1 secret images can be encrypted in the normal VSS schemes for multiple secret images [3], [28]. Therefore, for example, VSS-q-MI-R schemes are very useful in the following application:

**Throughout this paper, assume that “rotation” means the rotation with 180 degrees, and hence, we do not consider the case of the rotation with 90 and 270 degrees, etc.

***In the same way as [28], n ID images which identify each share [26] are assumed to be secret images.

Manuscript received August 22, 2005.
Manuscript revised November 21, 2005.
Final manuscript received December 26, 2005.
†The author is with the Graduate School of Information Systems, University of Electro-Communications, Chofu-shi, 182-8585 Japan.
††The author is with the School of Electronic, Information and Electrical Engineering, Shanghai Jiao Tong University, P.R. China.
†††The authors are with the Graduate School of Electrical Communications, University of Electro-Communications, Chofu-shi, 182-8585 Japan.
††††This paper was presented in part at Symposium on Cryptography and Information Security and Symposium on Information Theory and Its Applications, 2005.
a) E-mail: mitsugu@hn.is.uec.ac.jp
DOI: 10.1093/ietfce/e89-a.5.1382

Copyright © 2006 The Institute of Electronics, Information and Communication Engineers
Example 1. Consider the case where Alice requests some services from a server. In order to receive a service, she will be required the password adaptively chosen according to her request. If Alice has \( n \) shares, we can consider the following protocol: First, Alice sends a request of a service to the server. Then, the server sends her the qualified set adaptively chosen according to the service. The server provides the service if she can send the password decrypted from the qualified set.

Let \( r \) be the number of services that the server can provide. If Alice’s shares are encrypted by VSS-\(r\)-MI schemes, we have \( r \leq 2^n - 1 \), but \( r \) can be increased to at most \((3^n - 1)/2\) if VSS-\(r\)-MI-R schemes are used. For instance, in the case of \( n = 4 \), the number of services is less than or equal to 15 if we use VSS-4-MI schemes, but at most 40 services are available if VSS-4-MI-R schemes are realized.

Furthermore, let us consider the following case:

Example 2. Suppose that there are three participants \( V = \{V_1, V_2, V_3\} \) and four secrets \( S I^{(0)}, S I^{(1)}, S I^{(2)}, \) and \( S I^{(3)} \). Then, we assume that \( S I^{(0)} \) can be decrypted from 2 out of 3 participants, and \( S I^{(0)}, \ell = 1, 2, 3 \) \(-\{i, j\}\) can be decrypted only from a share set \( \{V_i, V_j\} \). Furthermore, we impose the requirement that each participant must hold only one share.

It is easy to see that Example 2 cannot be realized by VSS-\(q\)-MI schemes but can be realized by VSS-4-MI-R schemes as shown in Example 5. Hence, VSS-\(q\)-MI-R schemes have advantages compared with the normal VSS schemes.

In order to construct normal VSS schemes, we usually use so-called basis matrices. However, as shown in Sect. 3, it is interesting to note that VSS-\(q\)-MI-R schemes cannot be obtained by using the basis matrices straightforwardly because we rotate some shares in decryption. The VSS-\(q\)-MI-R scheme is the first VSS scheme in which basis matrices cannot directly be utilized. This is one of the contributions of this paper in the theoretical point of view.

This paper is organized as follows: In Sect. 2, access structures of VSS-\(q\)-MI-R schemes are defined as extensions of VSS-\(q\)-MI schemes [28], and the definition of VSS-\(q\)-MI schemes are reviewed. Then, we define the VSS-\(q\)-MI-R schemes in Sect. 3, and a new method to construct the VSS-\(q\)-MI-R schemes is proposed in Sect. 4. Furthermore, it is pointed out in Sect. 5 that the technique used in VSS-\(q\)-MI-R schemes can easily be applied to VSS-\(q\)-MI schemes allowing some shares to be turned over before stacked up. Some examples of shares and decrypted images are shown in Appendix.

2. Preliminaries and Backgrounds

2.1 Access Structures of VSS-\(q\)-MI-R Schemes

Let \( V = \{V_1, V_2, \ldots, V_n\} \) and \( 2^V \) be the set of \( n \) shares and the family of all subsets of \( V \), respectively\(^{11}\). Then, denote by \( \tilde{V}_i \) the rotated \( V_i \in V \) with 180 degrees, and define \( \mathbb{V} \overset{\text{def}}{=} \{\tilde{V}_1, \tilde{V}_2, \ldots, \tilde{V}_n\} \). For example, a set \( \{V_1, V_2, V_3\} \) means the set of shares \( V_1, V_2, \) and rotated \( V_3 \). For a set \( A \subseteq \mathbb{V} \), let \( I(A) \subseteq \{1, 2, \ldots, n, \infty\} \) be a set of indices of shares belonging to \( A \), where we define \( I(\emptyset) = \{\infty\} \). As an example, \( I(\{\tilde{V}_1, \tilde{V}_2, \tilde{V}_3\}) = \{1, 2, 3\} \). Then, we define a family of all combinations of shares allowing their rotations as follows:

\[
\mathbb{V} \overset{\text{def}}{=} \{A \cup \tilde{B} : A \subseteq \mathbb{V}, \tilde{B} \subseteq \tilde{V}, \text{ where } I(A) \cap I(\tilde{B}) = \emptyset, \min I(A) < \min I(\tilde{B})\}.
\]

Remark 3. The reason why we impose the requirement \( \min I(A) < \min I(\tilde{B}) \) in (1) is to avoid \( \mathbb{V} \) including two share sets representing the same decrypted image. For example, although \( \{V_1, V_2\} \) and \( \{\tilde{V}_1, \tilde{V}_2\} \) are different, the image decrypted by stacking \( V_1 \) and \( V_2 \) is equivalent to the rotated image which is obtained by stacking \( \tilde{V}_1 \) and \( \tilde{V}_2 \). Hence, it is not necessary for \( \mathbb{V} \) to include both share sets \( \{V_1, V_2\} \) and \( \{\tilde{V}_1, \tilde{V}_2\} \), and we assume that the share with the smallest index is not rotated. From (1), we can check that \( \{V_1, V_2\} \in \mathbb{V} \) but \( \{V_1, V_2\} \notin \mathbb{V} \).

Furthermore, in the case of VSS-\(q\)-MI schemes, it is easy to see that \( \mathbb{V} \) reduces to \( 2^V \) if we substitute \( \emptyset \) for \( \tilde{V} \) in (1). Hence, \( \mathbb{V} \) can be considered as an extension of \( 2^V \) in VSS-\(q\)-MI schemes.

Under the assumption (1), and if we regard the ID image of each share as a secret image [26], [28], at most \((3^n - 1)/2\) secret images can be encrypted\(^{11}\). In the case of \( n = 3 \), we can assign at most \((3^3 - 1)/2 = 13\) secret images to share sets \( \{V_1\}, \{V_2\}, \{V_3\}, \{V_1, V_2\}, \{V_2, V_3\}, \{V_1, V_3\}, \{V_1, V_2, V_3\}, \{V_2, V_3\}, \{V_1, V_3\}, \{V_1, V_2, V_3\}, \{V_1, V_2\}, \{V_1, V_3\}, \{V_1, V_2, V_3\} \).

In VSS-\(q\)-MI-R schemes, \( q \) secret images denoted by \( S I^{(j)}, j = 1, 2, \ldots, q \), are collectively encrypted into \( n \) shares\(^{11}\). Let \( \mathbb{A}^{(q)}_{\mathcal{F}} \subseteq \mathbb{V}, j = 1, 2, \ldots, q \), be the family of qualified sets for the \( j \)-th secret image, and let \( \mathcal{F} \subseteq \mathbb{V} \) be the family of forbidden sets. We call \( \mathcal{F} = \{(\mathbb{A}^{(q)}_{\mathcal{F}})_{\ell=1}^{\mathcal{F}}, \mathcal{A}\} \) an access structure for \( q \) secret images. Note that the \( j \)-th secret image \( SI^{(j)} \) can be decrypted by stacking the shares in \( A \in \mathbb{A}^{(q)}_{\mathcal{F}} \), and no information of all secret images can be obtained from any set in \( \mathcal{F} \).

For each \( \mathbb{A}^{(q)}_{\mathcal{F}} \), denote its closure by \( \gamma(\mathbb{A}^{(q)}_{\mathcal{F}}) \) defined as

\(^{11}\)Throughout this paper, a set of shares and a family of share sets are represented by upper case bold-face and calligraphic font letters, respectively. Furthermore, let \( A - B \) be a difference set of \( A \) and \( B \), and the cardinality of a set \( A \) is denoted by \( |A| \).

\(^{11}\)All elements in any set are assumed to be in ascending order. For instance, for \( \{V_{i_1}, V_{i_2}, \ldots, V_{i_k}\} \) and \( \{i_1, i_2, \ldots, i_k\} \), we assume that \( i_1 < i_2 < \cdots < i_k \).

\(^{11}\)This claim can be verified as follows: We can uniquely determine a share set \( A \in \mathbb{V} \) by assigning each share \( V_i \in V \) any of \( V_i \notin A \) or \( V_i \in A \). Noticing the fact that no secret image can be decrypted from the empty share set, and the share with the smallest index in \( A \) is assumed not to be rotated, we have \(|V| = (3^n - 1)/2\).

\(^{11}\)It is assumed that every secret image has the same size.
follows:
\[ \gamma(\mathcal{A}_Q^{(j)}) = \{ B \in \mathcal{V} : A \in \mathcal{A}_Q^{(j)}, I(A) \subseteq I(B) \}. \]
Notice that each \( \gamma(\mathcal{A}_Q^{(j)}) \) and \( \mathcal{A}_F \) must satisfy the following monotonicity:
\[ A \in \gamma(\mathcal{A}_Q^{(j)}) \Rightarrow A' \in \gamma(\mathcal{A}_Q^{(j)}) \]
for any \( A' \in \{ B \in \mathcal{V} : I(A) \subseteq I(B) \} \),
\[ A \in \mathcal{A}_F \Rightarrow A' \in \mathcal{A}_F \]
for any \( A' \in \{ B \in \mathcal{V} : I(A) \subseteq I(B) \} \).
Furthermore, \( \mathcal{A}_Q^{(j)} \) and \( \mathcal{A}_F \) are required to satisfy
\[ \left\{ \bigcup_{j=1}^{q} \gamma(\mathcal{A}_Q^{(j)}) \right\} \cup \mathcal{A}_F = \mathcal{V}, \]
\[ \gamma(\mathcal{A}_Q^{(j)}) \cap \mathcal{A}_F = \emptyset \] for all \( j \),
\[ \mathcal{A}_Q^{(j)} \cap \mathcal{A}_Q^{(j')} = \emptyset \] for \( j \neq j' \).

The requirement (7) comes from the assumption that all secret images are different. Note that the access structures of VSS-\( q \)-MI schemes can be defined by replacing \( \mathcal{V} \) with \( 2^{qF} \) in the above definitions. Hence, the access structures of VSS-\( q \)-MI-R schemes defined above include the access structures of VSS-\( q \)-MI schemes as special cases.

**Example 4** ((2,2)-VSS-2-MI-R scheme). Let \( \mathcal{V} = \{ V_1, V_2 \} \) be the set of shares. Then, we have \( \mathcal{V} = \{ \{ V_1 \}, \{ V_2 \}, \{ V_1, V_2 \}, \{ V_1, V_2 \} \} \). Suppose that two secret images \( S^{(1)} \) and \( S^{(2)} \) shown in Fig. 1 can be decrypted by stacking \( \{ V_1, V_2 \} \) and \( \{ V_1, V_2 \} \), respectively. But, we assume that each share must not leak out any information of both secret images. This access structure can be represented as follows.
\[ \mathcal{A}_Q^{(1)} = \{ \{ V_1, V_2 \} \}, \quad \mathcal{A}_Q^{(2)} = \{ \{ V_1, V_2 \} \}, \quad \mathcal{A}_F = \{ \{ V_1 \}, \{ V_2 \} \}. \]

In this case, it holds that \( \gamma(\mathcal{A}_Q^{(1)}) = \gamma(\mathcal{A}_Q^{(2)}) = \{ \{ V_1, V_2 \}, \{ V_1, V_2 \} \} \).

**Example 5.** The requirement described in Example 2 can be realized by the following access structure:
\[ \mathcal{A}_Q^{(0)} = \{ \{ V_1, V_2 \}, \{ V_2, V_3 \}, \{ V_1, V_3 \} \}, \]
\[ \mathcal{A}_Q^{(1)} = \{ \{ V_2, V_3 \} \}, \quad \mathcal{A}_Q^{(2)} = \{ \{ V_1, V_3 \} \}, \]
\[ \mathcal{A}_Q^{(3)} = \{ \{ V_1, V_2 \} \}, \]
\[ \mathcal{A}_F = \{ \{ V_1 \}, \{ V_2 \} \}. \]

where \( \mathcal{A}_Q^{(0)} \) is the family of qualified sets for the secret image \( S^{(0)} \). From the above access structure, we note that any information of \( S^{(1)} \) must not be known to the share sets \( \{ V_1, V_2 \} \) and \( \{ V_1, V_3 \} \) since it holds that \( \{ V_1, V_2 \}, \{ V_1, V_3 \} \notin \gamma(\mathcal{A}_Q^{(1)}) \).

\[ \square \]

**Remark 6.** In an access structure \( \Gamma = \{ \{\mathcal{A}_Q^{(j)}\}_{j=1}^{q}, \mathcal{A}_F \} \), secret image \( S^{(j)} \) can be decrypted by stacking the share set \( A \in \mathcal{A}_Q^{(j)} \). However, we note that \( S^{(3)} \) cannot always be decrypted by stacking the shares in \( B \in \gamma(\mathcal{A}_Q^{(3)}) \) although \( B \) has enough information of \( S^{(3)} \). For example, in the case of Example 4, we can decrypt the secret image \( S^{(1)} \) by stacking \( \{ V_1, V_2 \} \in \mathcal{A}_Q^{(1)} \), but it cannot be obtained by stacking \( \{ V_1, V_2 \} \in \gamma(\mathcal{A}_Q^{(3)}) \). However, note that \( \{ V_1, V_2 \} \均有 enough information of \( S^{(1)} \) since it can be obtained by stacking \( V_1 \) and \( V_2 \), i.e., \( V_2 \).

\[ \square \]

**Example 7** (VSS-2-MI scheme). Let \( \mathcal{V} = \{ V_1, V_2, V_3 \} \) be the set of shares, and denote two secret images by \( S^{(1)} \) and \( S^{(2)} \) as shown in Figs. 1(a) and (b), respectively. Suppose that \( S^{(1)} \) and \( S^{(2)} \) are decrypted from the share sets \( \{ V_1, V_2 \} \) and \( \{ V_2, V_3 \} \), respectively, but, the set \( \{ V_1, V_3 \} \) or any one share must not leak out any information of both secret images. This access structure of the VSS-2-MI scheme can be represented as follows.
\[ \mathcal{A}_Q^{(1)} = \{ \{ V_1, V_2 \} \}, \quad \mathcal{A}_Q^{(2)} = \{ \{ V_2, V_3 \} \}, \quad \mathcal{A}_F = \{ \{ V_1 \}, \{ V_2 \}, \{ V_3 \}, \{ V_1, V_3 \} \}. \]

In this case, we have \( \gamma(\mathcal{A}_Q^{(1)}) = \{ \{ V_1, V_2 \}, \{ V_1, V_2 \} \}, \gamma(\mathcal{A}_Q^{(2)} = \{ \{ V_2, V_3 \}, \{ V_1, V_2 \} \} \) since we use \( 2^q \) instead of \( \mathcal{V} \) in the VSS-2-MI scheme. Noticing that \( \{ V_1, V_2 \} \notin \gamma(\mathcal{A}_Q^{(2)}) \) but \( \{ V_1, V_2 \} \in \gamma(\mathcal{A}_Q^{(1)}) \), the set \( \{ V_1, V_2 \} \) must not leak out any information of \( S^{(2)} \) although it can decrypt \( S^{(1)} \).

\[ \square \]

### 2.2 Notation

In this paper, we treat binary black-white secret images, and they are encoded into \( n \) shares. Each encrypted pixel on a share is represented by \( m \) pixels called subpixels, and \( m \) is called pixel expansion. From a viewpoint of resolution of decrypted images, pixel expansion \( m \) should be as small as possible. We denote black and white pixels by \( 1 \) and \( 0 \), respectively. Then, a mixture of colors on transparencies can be represented by a binary “OR” operation denoted by \( \vee \). For example, the mixture of black and white can be represented as \( 1 \lor 0 = 1 \). Similarly, \( 0 \lor 1 = 1 \lor 1 = 1 \), and \( 0 \lor 0 = 0 \) hold. Denote by \( w(a) \) the Hamming weight of an \( m \)-dimensional vector \( a \in \{ 0, 1 \}^m \).

For \( m \)-dimensional vectors of colors \( a = [a_1, a_2, \ldots, a_m], \quad b = [b_1, b_2, \ldots, b_m] \) where \( a_i, b_i \in \{ 0, 1 \} \), define an operation \( \lor \) by

\[ 1 \in this paper, all vectors are assumed to be row vectors.\]
which represents the mixtures of two pixels with \( m \) subpixels. For an \( n \times m \) matrix \( S = [a_1, a_2, \ldots, a_n]^T \in \{0, 1\}^{n \times m} \), where superscript \( T \) means the transpose of a matrix, and an arbitrary set of positive integers \( X = \{u_1, u_2, \ldots, u_t\} \subseteq \{1, 2, \ldots, n\} \), an \( |X| \times m \) matrix \( S\{X\} \) is defined as \( S\{X\} = [a_{u_1}, a_{u_2}, \ldots, a_{u_t}]^T \in \{0, 1\}^{|X| \times m} \). Then, the pixel obtained by stacking all shares represented by \( S \) can be obtained by the mapping \( \eta : \{0, 1\}^{n \times m} \rightarrow \{0, 1\}^m \) defined by \( \eta(S) = a_1 \lor a_2 \lor \cdots \lor a_n \). Hence, for a set of positive integers \( X = \{u_1, u_2, \ldots, u_t\} \subseteq \{1, 2, \ldots, n\} \), the pixel obtained by stacking the \( u_1 \)-th, \( u_2 \)-th, \ldots, \( u_t \)-th shares of \( S \) can be represented as \( \eta(S\{X\}) = a_{u_1} \lor a_{u_2} \lor \cdots \lor a_{u_t} \).

Next, we introduce an equivalence relation \( \sim \) into a set of matrices \( \{0, 1\}^{n \times m} \). For two matrices \( A, B \in \{0, 1\}^{n \times m} \), \( A \sim B \) means that \( A \) can be obtained by a column permutation of \( B \). In other words, it holds for any permutation \( \sigma : \{1, 2, \ldots, m\} \rightarrow \{1, 2, \ldots, m\} \)

\[
[a_1^T, a_2^T, \ldots, a_n^T] \sim [a_{\sigma(1)}^T, a_{\sigma(2)}^T, \ldots, a_{\sigma(m)}^T],
\]

where \( a_i \) are \( n \)-dimensional vectors of a matrix \( A \in \{0, 1\}^{n \times m} \). By using the equivalence relation \( \sim \), we can consider the quotient set \( \{0, 1\}^{n \times m} / \sim \), which consists of the equivalence classes. An equivalence class is represented as \( \langle B \rangle \) by a representative \( B \) in the class. In normal VSS-\( q \)-MI schemes, as we will see in Sect. 2.3, each encrypted pixel can be represented by a matrix selected from a quotient set \( \langle B \rangle \) where the representative \( B \) is called a basis matrix. Hence, if it holds that \( A \sim B \) for matrices \( A, B \in \{0, 1\}^{n \times m} \), \( A \) and \( B \) are assumed to be selected from the same quotient set \( \langle B \rangle \), and they represent the same color of the secret images.

Finally, for the notational simplicity, define the concatenation \( A \lor B \) of matrices \( A \in \{0, 1\}^{n_1 \times m} \) and \( B \in \{0, 1\}^{n_2 \times m} \) to be

\[
A \lor B \defeq \begin{bmatrix} A \\ B \end{bmatrix}.
\]

### 2.3 Definition of VSS-\( q \)-MI Schemes

In this section, we briefly review the definition of VSS-\( q \)-MI schemes according to [3], [28]. As shown in Fig. 2, all combinations of colors appeared in the secret images are encrypted at once into \( n \) shares in VSS-\( q \)-MI schemes, and each combination can be represented by binary numbers as follows: Let \( p^{(j)} \in \{0, 1\} \) be a color of a pixel on the \( j \)-th secret image for \( j = 1, 2, \ldots, q \). Then, all combinations of colors on \( q \) secret images can be represented by a \( q \)-bit binary numbers denoted by \( p^{(1)} p^{(2)} \cdots p^{(q)} \).

**Example 8.** In the case of Example 7 for two secret images \( S^{(1)} \) and \( S^{(2)} \) shown in Figs. 1(a) and 1(b), all combinations of colors can be represented by 2-bit binary numbers \( 00, 01, 10, \) and \( 11 \). In this example, three combinations \( 00, 01 \), and \( 11 \) are used as shown in Fig. 3(a).

For a positive integer \( \ell \) and a nonnegative integer \( k (\leq 2^\ell - 1) \), let \( b(\ell, k) \) denote the \( \ell \)-bit binary representa-

\[\text{Note that [3] considered the VSS-(2^n - 1)-MI schemes for black white binary secret images, and the VSS-\( q \)-MI schemes with general access structures are studied in [28] for color secret images with shades.}\]
tion of $k$. Then, as illustrated in Fig. 2, we encrypt each $p \in \{0, 1, \ldots, 2^q - 1\}$ into an $n \times m$ matrix $S^p = [s^p_{i,j}]_{1 \leq i \leq n, 1 \leq j \leq m}$, where $p$ denotes a set of $q$ colors by $b_x(p) = p^{(1)}\eta^{(2)} \cdots p^{(q)}$, and $s^p_{i,j} \in \{0, 1\}$ denotes a color of the $u$-th subpixel on the $w$-th share. The matrix $S^p$ is assumed to be selected from a code set denoted by $\mathcal{B}^p$ with probability $1/|\mathcal{B}^p|$. Hence, in order to construct VSS schemes, we have to design the code sets $\mathcal{B}^p$.

For a matrix $S^p$ and a set of shares $A \subseteq V$, let $S^p[A]$ be a matrix obtained by the restriction of rows in $S^p$ corresponding to the share set $A$. In other words, $S^p[A]$ can be defined as follows:

$$S^p[A] \equiv S^p(I(A)),$$

(14)

If a given set $A \subseteq V$ is included in two or more $\gamma(\mathcal{A}_Q^{(j)})$, two or more secret images can be decrypted from $A$. Let $J_f(A)$ be a set of indices of the secret images that can be decrypted from $A$ according to the access structure $\Gamma = \{\mathcal{A}_Q^{(j)} q=1, \mathcal{A}_\Gamma\}$, i.e.,

$$J_f(A) = \{j : A \in \gamma(\mathcal{A}_Q^{(j)}), 1 \leq j \leq q\}.$$  

(15)

For instance, $J_f(V) = \{1, 2, \ldots, q\}$, and $J_f(A) = \emptyset$ for any $A \in \mathcal{A}_\Gamma$. Note that a share set $A$ can decrypt secret images $S^{(j)}$ for all $j \in J_f(A)$ although $A$ cannot obtain any information of $S^{(j)}$ for every $j \notin J_f(A)$.

Now, we define VSS-$q$-MI schemes for general access structures as follows:

**Definition 9** ([3], [28]). Let $V = \{V_1, V_2, \ldots, V_n\}$ and $\Gamma = \{\mathcal{A}_Q^{(j)} q=1, \mathcal{A}_\Gamma\}$ be the set of shares and the access structure for $V$, respectively. For each $p = 0, 1, \ldots, 2^q - 1$, an $n \times m$ matrix $B^p$ is called a basis matrix of the VSS-$q$-MI scheme for $V$ and $\Gamma$ if each $B^p$ satisfies the following conditions:

(i) For every $j = 1, 2, \ldots, q$ and any $A \in \mathcal{A}_Q^{(j)}$, it holds that

$$w(\eta(B^p[A])) = \begin{cases} \mu_A & \text{if } p^{(j)} = 1 \\ \mu_A - \delta_A & \text{if } p^{(j)} = 0 \end{cases},$$

(16)

where $\mu_A$ and $\delta_A$ are positive integers depending on $A$, and $b_x(p) = p^{(1)}\eta^{(2)} \cdots p^{(q)}$.

(ii) For any set $A \in 2^V$ satisfying $J_f(A) = \emptyset$, it holds that

$$B^p[A] \sim B^q[A] \sim \cdots \sim B^{2^q-1}[A].$$

(17)

(iii) In the case of $J_f(A) \neq \emptyset$, it holds that $B^p[A] \sim B^q[A]$ for any $p$ and $p'$ satisfying $p^{(j)} = p'^{(j)}$ for all $j \in J_f(A)$ where $b_x(p) = p^{(1)}\eta^{(2)} \cdots p^{(q)}$ and $b_x(p') = p'^{(1)}\eta^{(2)} \cdots p'^{(q)}$.

A VSS-$q$-MI scheme for an access structure $\Gamma$ is called a $(\Gamma, V)$-VSS-$q$-MI scheme if, for every $p \in \{0, 1, \ldots, 2^q - 1\}$, each pixel associated with $p$ is determined by a matrix $S^p$ selected from a code set obtained by $\mathcal{B}^p = (B^p)$ with probability $1/|\mathcal{B}^p|$, where $B^p$ is the basis matrix of $p$.

**Example 10.** In the VSS-2-MI scheme treated in Example 7, basis matrices $B^0, B^1, B^2$ and $B^3$ are given by

$$B^0 = \begin{bmatrix} 1011 \\ 1010 \\ 1110 \\ 1101 \end{bmatrix}, \quad B^1 = \begin{bmatrix} 1011 \\ 1010 \\ 1110 \\ 1101 \end{bmatrix},$$

$$B^2 = \begin{bmatrix} 1011 \\ 0110 \\ 1110 \\ 1101 \end{bmatrix}, \quad B^3 = \begin{bmatrix} 1011 \\ 0110 \\ 1110 \\ 1101 \end{bmatrix}. \quad (18)$$

It is easy to check that (18) satisfies the conditions (i)–(iii) in Definition 9. For example, it holds for $A_{12}^{(2)} \equiv \{V_1, V_2\} \in A_{Q}^{(2)}$ that $w(\eta(B^0[A_{12}^{(2)}])) = w(\eta(B^1[A_{12}^{(2)}])) = w(\{1 0 1 1\}) = 3$, and $w(\eta(B^2[A_{12}^{(2)}])) = w(\{1 1 0 1\}) = 4$. These relations mean that $\mu_{A_{12}} = 4$ and $\delta_{A_{12}} = 1$, and $B^0, B^1$ and $B^2, B^3$ represent white and black on $S^{(1)}$, respectively. Similarly, it holds for $A_{23}^{(2)} = \{V_2, V_3\} \in A_{Q}^{(2)}$ that $w(\eta(B^0[A_{23}^{(2)}])) = w(\eta(B^2[A_{23}^{(2)}])) = 4$, and $w(\eta(B^1[A_{23}^{(2)}])) = w(\eta(B^3[A_{23}^{(2)}])) = 3$, which means that $B^0, B^2$ and $B^1, B^3$ represent white and black on $S^{(2)}$, respectively.

Then, it can easily be checked that $B^0[A] \sim B^1[A] \sim B^2[A] \sim B^3[A]$ for any $A \in \mathcal{A}_\Gamma$. Furthermore, it holds for $A_{12}$ that $B^0[A_{12}] \sim B^1[A_{12}]$ and $B^2[A_{12}] \sim B^3[A_{12}]$, which implies that $A_{12}$ does not leak out the colors of pixels on $S^{(2)}$ even if the colors on $S^{(1)}$ can be decrypted from $A_{12}$. Hence, the basis matrices given by (18) attain both $A_{12} \in A_{Q}^{(1)}$ and $A_{12} \notin \gamma(\mathcal{A}_Q^{(2)})$. \hfill $\Box$

3. Definition of VSS-$q$-MI-R Schemes

3.1 Pixels on Secret Images

In this subsection, we describe how to treat the pixels on secret images encrypted in VSS-$q$-MI-R schemes. First, we introduce a simple example of $(2, 2)$-threshold VSS-2-MI-R schemes as shown in Fig. 4.

**Example 11.** Consider the $(2, 2)$-VSS-2-MI-R scheme with the access structure given by (8) in Example 4. In this case, the relation between shares and secret images are illustrated in Fig. 4, which is described as follows: Since we rotate $V_2$ and stack it with $V_1$ in order to decrypt $S^{(2)}$, point symmetrical two pixels with respect to the centroid of the secret images must be treated collectively. Hence, denote by $U$ and $L$ the point symmetrical two positions in the upper and the lower halves of the secret images, respectively. Then, let $p^0_U \in [0, 1]$ and $p^0_L \in [0, 1]$ be the colors of pixels on the position $U$ in $S^{(1)}$ and $S^{(2)}$, respectively, and denote by $p^1_U \in [0, 1]$ and $p^1_L \in [0, 1]$ the colors of pixels on the position $L$ in $S^{(1)}$ and $S^{(2)}$, respectively.

By regarding the quadruple of colors $p^0_U, p^1_U, p^0_L, p^1_L$ as a 4-bit binary number and letting $b_x(p) = p^0_U p^0_L p^1_U p^1_L$, each pixel in $\{0, 1, \ldots, 15\}$ must be encrypted into 2 shares. In the case where the secret images are given by Figs. 1(a) and (b), 4-bit binary numbers representing $p^0_U, p^1_U, p^0_L, p^1_L$ are shown in (b) of Fig. 3. In this example, 0000, 0101, 0111, 1101, and 1111 are used. \hfill $\Box$
In a general case with \( n \) shares, let \( U \) and \( L \) be the point symmetrical two positions in the upper and the lower halves of the secret images, respectively. Denote the colors of the \( j \)-th secret image corresponding to the positions \( U \) and \( L \) by \( p_U^{(j)} \) and \( p_L^{(j)} \), respectively. Then, each set of \( 2q \) colors \((p_U^{(1)}, p_U^{(2)}, \ldots, p_U^{(q)}, p_L^{(1)}, p_L^{(2)}, \ldots, p_L^{(q)})\) must be treated collectively, and hence, we encrypt every \( p \in \{0, 1, \ldots, 2^{(2q-1)}\} \) satisfying \( b_{2q}(p) = p_U^{(1)}p_U^{(2)} \cdots p_U^{(q)}p_L^{(1)}p_L^{(2)} \cdots p_L^{(q)} \) into \( n \) shares in the same way as VSS-q-MI schemes.

### 3.2 Definition of VSS-\( q \)-MI-R Schemes

In this section, we define the VSS-\( q \)-MI-R schemes as extensions of VSS-\( q \)-MI schemes given in section 2.3. As stated in Sect. 3.1, we denote by \( p \in \{0, 1, \ldots, 2^{2q} - 1\} \) the set of \( 2q \) colors on the positions \( U \) and \( L \), and it is encrypted into \( n \) shares. Hence, each \( p \) must be encrypted into a set of two \( n \times m \) matrices denoted by \( S_U^p \) and \( S_L^p \), respectively, where an \( m \)-dimensional vector \( s_{X_i}^p, X \in \{U, L\}, i = 1, 2, \ldots, n \) denotes a pixel with \( m \) subpixels for the \( i \)-th share corresponding to the position \( X \). Furthermore, since \( S_U^p \) and \( S_L^p \) must also be treated collectively, we assume that each \( p \) is encrypted into

\[
S^p \overset{\text{def}}{=} S_U^p \cup S_L^p
\]

\[
= \left[ s_{U1}^p s_{U2}^p \cdots s_{Un}^p s_{L1}^p s_{L2}^p \cdots s_{Lm}^p \right]^T,
\]

which is selected from a code set \( \mathcal{B}^p \) consisting of \( 2n \times m \) matrices with probability \( 1/|\mathcal{B}^p|\).

For a given permutation \( \sigma : \{1, 2, \ldots, m\} \rightarrow \{1, 2, \ldots, m\} \) and a given \( n \times m \) matrix \( A = [a_1^T a_2^T \cdots a_m^T] \), define a permutation of columns of \( A \) by \( \pi_\sigma(A) \overset{\text{def}}{=} [a_{\sigma(1)}^T a_{\sigma(2)}^T \cdots a_{\sigma(m)}^T] \). Now, we define the permutation \( \pi_R \) by

\[
\pi_R(v) \overset{\text{def}}{=} m - v + 1,
\]

for \( v = 1, 2, \ldots, m \). Then, for \( i = 1, 2, \ldots, n \) and \( X \in \{U, L\}, \pi_{\pi_R}(s_X^p) \) represents a pixel obtained by rotating the pixel \( s_X^p \).

Furthermore, define the following restrictions of rows in a \( 2n \times m \) matrix \( S^p \) corresponding to a set \( A \in \mathcal{V} \).

\[
S^p\langle\{i : V_i \in A\}\rangle \overset{\text{def}}{=} S^p\langle\{i : \pi_R(V_i) \in A\}\rangle \cap \pi_{\pi_R}(S^p\langle\{i : \pi_R(V_i) \in A\}\rangle),
\]

\[
S^p\langle\{i : V_i \in A\}\rangle \overset{\text{def}}{=} \pi_{\pi_R}(S^p\langle\{i : \pi_R(V_i) \in A\}\rangle) \cap S^p\langle\{i : \pi_R(V_i) \in A\}\rangle.
\]

Since the same image can be obtained by stacking the shares in arbitrary order, two pixels in the position \( U \) and \( L \) obtained by stacking the shares corresponding to \( A \in \mathcal{V} \) coincide with \( \eta(S^p\langle\{i : V_i \in A\}\rangle) \) and \( \eta(S^p\langle\{i : V_i \in A\}\rangle) \), respectively.

Furthermore, we define

\[
S^p\langle\{i : i \in I(A)\}\rangle \overset{\text{def}}{=} S^p\langle\{i : i \in I(A)\}\rangle \cap \{n + i : i \in I(A)\},
\]

which contains whole information obtained from the share set \( A \in \mathcal{V} \).

**Example 12.** In the case of \((2,2)\)-VSS-2-MI-R schemes, we assume that each \( p \in \{0, 1, \ldots, 15\} \) is encrypted into a \( 4 \times m \) matrix denoted by

\[
S^p = \left[ s_{U1}^p s_{U2}^p s_{L1}^p s_{L2}^p \right]^T \in \{0, 1\}^{4 \times m},
\]

where \( p \) represents a set of 4 colors given by \( b_4(p) = p_U^{(1)}p_U^{(2)}p_L^{(1)}p_L^{(2)} \).

For a set \([V_1, V_2]\), (21) and (22) become

\[
S^p\langle[V_1, V_2]\rangle = S^p\langle[1, 2]\rangle = \left[ s_{U1}^p s_{U2}^p \right],
\]

\[
S^p\langle[V_1, V_2]\rangle = S^p\langle[3, 4]\rangle = \left[ s_{L1}^p s_{L2}^p \right],
\]

\(^1\text{For example, see the last equality of (28) in Example 12.}\)
respectively, and hence, we can check that the pixels \( p_U^{(1)} \) and \( p_L^{(1)} \) can be decrypted as \( \eta(S^p(A)[V_i, V_j]_U) \) and \( \eta(S^p(A)[V_i, V_j]_L) \), respectively. Similarly, it can be checked that two vectors representing \( p_U^{(0)} \) and \( p_L^{(0)} \) are obtained by
\[
\begin{align*}
\eta(S^p([V_1, V_2]_U)) &= \eta(S^p([1, 3]) \cap \pi_{\sigma_{\eta}}(S^p([4]))) \\
&= \eta\left(\begin{bmatrix}
p_{U_i}^{0} \\
\pi_{\sigma_{\eta}}(s_{U,j}^{0}) 
\end{bmatrix}\right), \quad (27)
\eta(S^p([V_1, V_2]_L)) &= \eta(\pi_{\sigma_{\eta}}(S^p([2, 4])) \cap \eta(S^p([3]))) \\
&= \eta\left(\begin{bmatrix}
ds_{L_i}^{0} \\
\pi_{\sigma_{\eta}}(s_{L,j}^{0}) 
\end{bmatrix}\right) \\
&= \eta\left(\begin{bmatrix}
p_{L_i}^{0} \\
\pi_{\sigma_{\eta}}(s_{L,j}^{0}) 
\end{bmatrix}\right), \quad (28)
\end{align*}
\]
respectively. Finally, information of pixels obtained from \( V_i \) (or \( V_j \)), \( i = 1, 2 \), can be represented as follows.
\[
S^p([V_i])_w = \begin{cases} 
S^p([1, 3]) & \text{if } i = 1 \\
S^p([2, 4]) & \text{if } i = 2 
\end{cases} \\
= \begin{bmatrix}
p_{U,i}^{p} \\
\pi_{\sigma_{\eta}}(s_{U,j}^{p}) 
\end{bmatrix}. \quad (29)
\]

In the same way as VSS-\( q \)-MI schemes, two or more secret images can be decrypted from \( A \in \mathcal{V} \) if the set \( A \) is included in two or more \( \gamma(\mathcal{A}_Q(1)) \). Hence, we also define \( J_1(A) \) by (15) for \( A \in \mathcal{V} \). Note that \( J_1(A) \) is the set of indices of secret images that can be decrypted from \( A \in \mathcal{V} \) for given access structure \( \Gamma \).

Now, we can define VSS-\( q \)-MI-R schemes for general access structures as extensions of VSS-\( q \)-MI schemes as follows:

**Definition 13.** Let \( \mathcal{V} = \{V_1, V_2, \ldots, V_n\} \) and \( \Gamma = \{\mathcal{A}_Q(1), \mathcal{A}_R\} \) be the set of shares and the access structure for \( V \), respectively. If each set of \( 2n \times m \) matrices denoted by \( B^p \) satisfies the following conditions for \( p = 0, 1, \ldots, 2^{2q} - 1 \), we call \( B^p \) a code set, and the family of code sets \( \{B^0, B^1, \ldots, B^{2^{2q} - 1}\} \) is called a \((V, \Gamma)\)-VSS-\( q \)-MI-R scheme.

(i) For every \( j = 1, 2, \ldots, q \) and any set \( A \in \mathcal{A}_Q(1) \), every matrix \( S^p \in B^p \) satisfies for \( X \in \{U, L\} \) that
\[
w(\eta(S^p(A)_X)) = \begin{cases} 
\mu_A & \text{if } p^{(j)}_A = 1 \\
\mu_A - \delta_A & \text{if } p^{(j)}_A = 0,
\end{cases} \quad (30)
\]
where \( \mu_A \) and \( \delta_A \) are positive integers depending on \( A \in \mathcal{V} \), and \( b_{2q}(p) = p^{(1)} L_1 \cdots p^{(q)} L_1 \cdots p^{(q)} L_1 \cdots p^{(q)} L_1 \).  
(ii) For any set \( A \in \mathcal{V} \) satisfying \( J_1(A) = 0 \), it holds that
\[
B^p[A]_w = B^1[A]_w = \cdots = B^{2^{2q} - 1}[A]_w, \quad (31)
\]
where \( B^p[A]_w, p = 0, 1, \ldots, 2^{2q} - 1 \) are defined by
\[
B^p[A]_w = \{S^p[A]_w : S^p \in B^p\}. \quad (32)
\]
(iii) In the case of \( J_1(A) \neq 0 \), it holds that \( B^p[A]_w = B^0[A]_w \) for any \( p \) and \( p' \) satisfying \( p^{(j)} = p'^{(j)} \) for every \( j \in J_1(A) \) and \( X \in \{U, L\} \) where \( b_{2q}(p) = p^{(1)}_U p^{(2)}_L \cdots p^{(q)}_U p^{(q)}_L \cdots p^{(q)}_L \) and \( b_{2q}(p') = p'^{(1)}_U p'^{(2)}_L \cdots p'^{(q)}_U p'^{(q)}_L \cdots p'^{(q)}_L \).

Since Definition 13 is an extension of Definition 9, share set \( A \in \mathcal{V} \) can decrypt \( S^p(X) \) if and only if \( j \in J_1(A) \), i.e., no information of \( S^p(X) \) cannot be obtained from \( A \in \mathcal{V} \) if \( j \notin J_1(A) \).

**Remark 14.** In VSS-\( q \)-MI schemes of Definitions 9, each code set \( B^p \) can be obtained from a basis matrix \( B^p \) such that \( B^p = (B^p) \), and each pixel corresponding to \( p \) can be determined by a matrix selected from a code set \( B^p \) with probability \( 1/|B^p| \). Similarly, in VSS-\( q \)-MI-R schemes of Definition 13, each combination of \( 2q \) colors represented by \( p \) is encrypted into a matrix selected from \( B^p \) with probability \( 1/|B^p| \). However, we note that \( B^p \) in VSS-\( q \)-MI-R schemes cannot be an equivalence class of some matrix because we rotate some shares in decryption, i.e., the permutation of columns \( \pi_{\sigma_{\eta}} \) is used.

### 4. Construction of VSS-\( q \)-MI-R Schemes

As is pointed out in Remark 14, each code set \( B^p \) cannot be obtained from an equivalence class of some matrix. Hence, we show a new technique to construct each code set \( B^p \) for \( p = 0, 1, \ldots, 2^{2q}-1 \) in VSS-\( q \)-MI-R schemes satisfying Definition 13. First, we introduce the following operation \( \theta_n \) for a \( 2n \times m \) matrix \( S^p \) defined by
\[
\theta_n(S^p) \overset{\text{def}}{=} S^p[[1, 2, \ldots, n]] \cap \pi_{\sigma_{\eta}}(S^p[[n + 1, n + 2, \ldots, 2n]]).
\]
Noticing that \( \pi_{\sigma_{\eta}} \) is an identity map, it is easy to check that \( \theta_n(\theta_n(S^p)) = S^p \).

It is also easy to verify for any set \( A \in \mathcal{V} \) that
\[
[\theta_n(S^p)[A]_w = \theta_n(S^p[A]_w]. \quad (35)
\]
Furthermore, the following relations generally hold:
\[
S^p[A]_w = \theta_n([\theta_n(S^p)]_w) \cap [\theta_n([\theta_n(S^p)]_w) \cap [\theta_n([\theta_n(S^p)]_w)] = \pi_{\sigma_{\eta}}([\theta_n(S^p)])[[n + i : V_i \in A] \cap [n + i : V_i \in A]]. \quad (37)
\]
Therefore, we have
\[
\eta(S^p[A]_w) = \eta([\theta_n(S^p)]_w) \cap [\theta_n([\theta_n(S^p)]_w) \cap [\theta_n([\theta_n(S^p)]_w)] = \pi_{\sigma_{\eta}}([\theta_n(S^p)])[[n + i : V_i \in A] \cap [n + i : V_i \in A]] \cap [\theta_n([\theta_n(S^p)]_w) \cap [\theta_n([\theta_n(S^p)]_w)] = \eta([\theta_n(S^p)])[[n + i : V_i \in A] \cap [n + i : V_i \in A]]. \quad (39)
\]
Theorem 15. For a share set \( V = \{V_1, V_2, \ldots, V_n\} \), assume that the access structure \( \Gamma = \{\{A_h\}_{h=1}^{|A_h|}, \mathcal{A}_F\} \) of the VSS-\( q \)-MI-R scheme is given. Then, each code set \( B^p \) of the \((V, \Gamma)\)-VSS-\( q \)-MI-R scheme satisfying Definition 13 can be obtained by

\[
B^p = \{\theta_n(B) : B \in (B^p)\},
\]

for \( p = 0, 1, \ldots, 2^q - 1 \), where \( B^p \) are the basis matrices of the \((U, \widetilde{\Gamma})\)-VSS-2-qi-MI scheme. Here, the access structure \( \widetilde{\Gamma} = \{\{\mathcal{A}^h_{(j)}\} \}_{j=1}^{n} \mathcal{A}_F\) for the share set \( U = \{U_1, U_2, \ldots, U_{2^n}\} \) is given as follows:

\[
\mathcal{A}^h_{(j)} = \{B : B = \{U_i : V_i \in A\} \cup \{U_{n+i} : \hat{V}_i \in A\}
\]

for \( A \in \mathcal{A}^h_{(j)} \), \( j = 1, 2, \ldots, q \),

\[
\mathcal{A}^{q+j}_{(j)} = \{B : B = \{U_i : \hat{V}_i \in A\} \cup \{U_{n+i} : V_i \in A\}
\]

for \( A \in \mathcal{A}^{q+j}_{(j)} \), \( j = 1, 2, \ldots, q \),

\[
\mathcal{A}_F = \{B : B = \{U_i : i \in I(A)\} \cup \{U_{n+i} : \hat{i} \in I(A)\}, A \in \mathcal{A}_F\}.
\]

\( \square \)

Remark 16. In the above theorem, notice that the relation between the \((V, \Gamma)\)-VSS-\( q \)-MI-R scheme and corresponding \((U, \widetilde{\Gamma})\)-VSS-2-qi-MI scheme is given by

\[
b_{2q}(p) = \frac{p_U^{(1)} p_V^{(2)} \cdots p_{U_q}^{(q)} p_{V_l}^{(q+1)} p_{V_l}^{(q+2)} \cdots p_{V_l}^{(2q)}}{p_U^{(1)} p_V^{(2)} \cdots p_{U_q}^{(q)}},
\]

for all \( p = 0, 1, \ldots, 2^q - 1 \). Furthermore, according to [28], the basis matrices of the \((U, \widetilde{\Gamma})\)-VSS-2-qi-MI schemes can always be constructed if \( \Gamma \) satisfies the monotonicity (3) and (4). Hence, from Theorem 15, we can construct \((V, \Gamma)\)-VSS-\( q \)-MI-R scheme for any given access structure by constructing the corresponding \((U, \widetilde{\Gamma})\)-VSS-2-qi-MI scheme. \( \square \)

Proof of Theorem 15: From (34), it holds for any matrix \( S^p \in \{\theta_n(B) : B \in (B^p)\} \) that

\[
\theta_n(S^p) \in (B^p).
\]

Hence, we have

\[
\eta(S^p[I]) = \left\langle \left\langle \left\langle \theta_n(S^p) \{i : V_i \in A\} \cup \{n+i : \hat{V}_i \in A\} \right\rangle \right\rangle \right\rangle.
\]

where the marked equality (a) holds because of (38), and the marked equivalence relations (b) and (c) follow from (45) and (39), respectively. Therefore, noticing (41) and (42), we have

\[
\begin{align*}
&\eta(S^p[I]) = w(\eta(S^p[I])) \\
&= w(\eta(B^p[I]) \{i : V_i \in A\} \cup \{n+i : \hat{V}_i \in A\}) \\
&= w(\eta(B^p[I]) \{U_i : \hat{V}_i \in A\} \cup \{U_{n+i} : V_i \in A\})
\end{align*}
\]

for all \( i \in I(A) \). Therefore, noticing (44) and (48), we have

\[
\begin{align*}
&\eta(S^p[I]) = w(\eta(S^p[I])) \\
&= w(\eta(S^p[I]) \{i : V_i \in A\} \cup \{n+i : \hat{V}_i \in A\}) \\
&= w(\eta(S^p[I]) \{U_i : \hat{V}_i \in A\} \cup \{U_{n+i} : V_i \in A\})
\end{align*}
\]

for all \( i \in I(A) \). Therefore, noticing (43) and (44), we have

\[
\begin{align*}
&\eta(S^p[I]) = w(\eta(S^p[I])) \\
&= w(\eta(S^p[I]) \{i : V_i \in A\} \cup \{n+i : \hat{V}_i \in A\}) \\
&= w(\eta(S^p[I]) \{U_i : \hat{V}_i \in A\} \cup \{U_{n+i} : V_i \in A\})
\end{align*}
\]

for all \( i \in I(A) \). Therefore, noticing (41) and (42), we have
Therefore, from (35), it holds for all $A \in \mathcal{A}_F$ that

\[
\{(\theta_n(B))[A\bigwedge I] : B \in (B^q)\} =\{(\theta_n(B))[A\bigwedge I] : B \in (B^q)\}
\]

\[
\cdots = \{(\theta_n(B))[A\bigwedge I] : B \in (B^{2n-1})\},
\]

which means that (40) satisfies (31) in the condition (ii) of Definition 13.

Finally, we verify the condition (iii) in Definition 13. Since we assume for $A \in \mathcal{V}$ that $J_f(A) \neq \emptyset$, we have from (41) and (42) that $\zeta(I(A)) \in \gamma(\mathcal{R}_Q)$ and $\zeta(I(A)) \in \gamma(\mathcal{R}_Q)$ for all $j \in J_f(A)$. Hence, by letting $J_f(A) = \{j_1, j_2, \ldots, j_s\}$, we have $J_f(\zeta(I(A))) \supseteq \{j_1, j_2, \ldots, j_s, q + j_1, q + j_2, \ldots, q + j_s\}$. This implies that, from the condition (iii) of Definition 9 for the $(U, \Gamma)$-VSS-2q-MI scheme, $B^q[\zeta(I(A))] \sim B^q[\zeta(I(A))]$ holds for any $p$ and $p'$ satisfying that $p^{(j)} = p'^{(j)}$ and $p^{(q+i-j)} = p'^{(q+i-j)}$, $\ell = 1, 2, \ldots, u$ where $b_{2\ell}(p) = p^{(1)}p^{(2)} \cdots p^{(2q)}$ and $b_{2\ell}(p') = p'^{(1)}p'^{(2)} \cdots p'^{(2q)}$. Therefore, it holds from (44) and (51) that $B^q[A\bigwedge I] \sim B^q[A\bigwedge I]$ for any $p$ and $p'$ satisfying that $p^{(j)} = p'^{(j)}$, $\ell = 1, 2, \ldots, u$, and $X \in \{U, L\}$ by assuming $b_{2\ell}(p) = p^{(1)}p^{(2)} \cdots p^{(2q)}$, $b_{2\ell}(p') = p'^{(1)}p'^{(2)} \cdots p'^{(2q)}$, and $b_{2\ell}(p') = p'^{(1)}p'^{(2)} \cdots p'^{(2q)}$. Therefore, we can verify that $B^q[A\bigwedge I] \sim B^q[A\bigwedge I]$ holds for such $p$ and $p'$ in the same way as (53)-(55).

Therefore, it is shown that $B^q$ given by (40) satisfies all conditions in Definition 13.

\[\square\]

Example 17. From Theorem 15, the (2, 2)-VSS-2-MI-R scheme treated in Example 4 can be realized by (40) where the corresponding $(U_{\bigwedge I}, \Gamma_{\bigwedge I})$-VSS-4-MI scheme are given by $U_{\bigwedge I} = \{U_1, U_2, U_3, U_4\}$, and

\[
\mathcal{A}_Q = \{\{U_1, U_2\}, \{U_1, U_4\}, \{U_3, U_4\}, \{U_2, U_3\}\},
\]

\[
\mathcal{A}_F = \{\{U_1, U_2, U_3\}, \{U_2, U_3, U_4\}\}.
\]

\[
\begin{align*}
B^0 = & \begin{bmatrix} 10101111 \\ 01111110 \\ 11111010 \\ 11010111 \end{bmatrix}, & B^1 = & \begin{bmatrix} 10101111 \\ 01111110 \\ 11111010 \\ 11010111 \end{bmatrix}, \\
B^2 = & \begin{bmatrix} 10101111 \\ 01111110 \\ 11111010 \\ 11010111 \end{bmatrix}, & B^3 = & \begin{bmatrix} 10101111 \\ 01111110 \\ 11111010 \\ 11010111 \end{bmatrix}, \\
B^4 = & \begin{bmatrix} 10101111 \\ 01111110 \\ 11111010 \\ 11010111 \end{bmatrix}, & B^5 = & \begin{bmatrix} 10101111 \\ 01111110 \\ 11111010 \\ 11010111 \end{bmatrix}, \\
B^6 = & \begin{bmatrix} 10101111 \\ 01111110 \\ 11111010 \\ 11010111 \end{bmatrix}, & B^7 = & \begin{bmatrix} 10101111 \\ 01111110 \\ 11111010 \\ 11010111 \end{bmatrix},
\end{align*}
\]

(56)

The code sets $B^p$, $p = 0, 1, \ldots, 15$ for the $(2, 2)$-VSS-2-MI-R scheme in Example 4 can be obtained by applying these matrices to (40). In this example, $m = 8$ is attained, and shares and decrypted images are shown in Fig. A-1 in Appendix.

\[\square\]

Remark 18. We show that the VSS-q-MI-R schemes obtained in Theorem 15 are natural extensions of the VSS-q-MI schemes. In other words, for the access structure $\Gamma$ in which every share is not rotated, we note that the $(\Gamma, V)$-VSS-q-MI-R scheme constructed by Theorem 15 coincides with the normal $(\Gamma, V)$-VSS-q-MI scheme.

For example, let us construct $(2, 2)$-threshold VSS-1-MI schemes by using Theorem 15. In this case, we have $j = 1$ and $b_2(p) = p^{(1)}p^{(1)}$, and hence, we must construct code sets $B^p$ for $p = 0, 1, 2, 3$. From Theorem 15, $B^p$ can be obtained by substituting

\[
B^0 = \begin{bmatrix} 01 \\ 10 \end{bmatrix}, & B^1 = \begin{bmatrix} 01 \\ 10 \end{bmatrix}, & B^2 = \begin{bmatrix} 01 \\ 10 \end{bmatrix}, & B^3 = \begin{bmatrix} 01 \\ 10 \end{bmatrix},
\]

\[\Longleftrightarrow\]

(58)

into (40). It is easy to verify that the code sets obtained from (58) are equivalent to the normal $(2, 2)$-VSS-1-MI schemes [1] although expressions of code sets in the $(2, 2)$-VSS-1-MI schemes [1] are different from (58) because they are based on the basis matrices.

\[\square\]

Remark 18 implies that the VSS-q-MI-R schemes need more pixel expansion if the qualified sets include rotated shares. However, in the case of $(2, 2)$-VSS-2-MI-R schemes with pixel expansion 8, the decrypted images are sufficiently clear as shown in Fig. A-1.

Furthermore, it is reported that the $12 \times 12$ ($= 144$) pixel expansion can be realized [21] and human eyesight can recognize one white subpixel in 25 subpixels, i.e., 24 subpixels are black [25]. Hence, it will be useful to show an upper bound of the pixel expansion $m$ for given access structure $\Gamma = \{\{\mathcal{A}_I^{(j)}\}_{j=1}^{n}, \mathcal{A}_F\}$. Suppose that we construct a VSS-q-MI-R scheme by using Theorem 15 in which the
corresponding VSS-2-$q$-MI scheme is obtained by the methods shown in [28, Appendix] and [3, Sect. 7]. Then, we can obtain the $(V, \Gamma)$-VSS-$q$-MI-R scheme with pixel expansion
\[
m_r = \sum_{j=1}^{q} \sum_{A \in \mathcal{A}_G} 2^{[A]}.
\]
and hence, $m_r$ can be considered as an upper bound of $m$ for given access structure $\Gamma$. For example, we have $m_r = 24$ in the case of Example 5, and hence, such VSS-4-MI-R scheme is practical\(^1\). Furthermore, observe that the pixel expansion $m_r$ is achieved by (57) in the case of the $(2, 2)$-VSS-2-MI-R schemes shown in Example 4. However, by comparing (57) and (60), the upper bound $m_r$ can be improved.

Summarizing, our method is practical if $n$ and $q$ are small. Note that the normal VSS schemes are realized for small $n$. Hence, the proposed scheme is sufficiently practical.

Remark 19. In constructing VSS-$q$-MI-R schemes, we note that the matrices $B^\varphi$ in (40) are not necessary to be the basis matrices of the corresponding $(U, \Gamma)$-VSS-4-MI schemes.

For example, let us consider the case of $(2, 2)$-VSS-2-MI-R schemes in Example 4. In this case, $p_U^{(1)}$ and $p_U^{(2)}$ are decrypted on the same image, i.e., $S^{(1)}$. Hence, we do not have to worry that the information of $p_U^{(1)}$ leaks out from $p_U^{(2)}$ and vice versa. However, in the corresponding $(U_{ex}, \Gamma_{ex})$-VSS-4-MI scheme, we guarantee that the information of $p_U^{(1)}$ must not leak out from $p_L^{(2)}$ where $p_U^{(1)}$ and $p_U^{(2)}$ correspond to $p_U^{(1)}$ and $p_U^{(2)}$, respectively. Note that the same argument also holds for $p_U^{(2)}$, $p_U^{(1)}$ in (2, 2)-VSS-2-MI-R schemes and $p_U^{(2)}$, $p_U^{(1)}$ for $(U_{ex}, \Gamma_{ex})$-VSS-4-MI schemes. Actually, for the secrecy of (2, 2)-VSS-2-MI-R schemes, it is sufficient to guarantee that any information of both secret images must not leak out from each share. In other words, it must hold for $i = 1, 2$ that $B^\varphi \{[V_i]\}_w = B^\varphi \{[V_i]\}_w = \cdots = B^{15} \{[V_i]\}_w$, which implies that $B^\varphi \{A\} \sim B^\varphi \{A\} \sim \cdots \sim B^{15} \{A\}$ for each $A \in \mathcal{A} = \{[U_1], [U_2, U_4]\}$. Hence, each matrix $B^\varphi$ in (40) for the (2, 2)-VSS-2-MI-R schemes must satisfy only (i) and (ii) in Definition 9, but we need not pay attention to the condition (iii)\(^1\). Hence, the minimum pixel expansion of $(2, 2)$-VSS-2-MI-R schemes may be smaller than that of the $(U_{ex}, \Gamma_{ex})$-VSS-4-MI scheme given by (57). In fact, the following matrices with $m = 6 < 8$ satisfy the Definition 9 (i) and (ii) but do not satisfy (iii).

\[
B^0 = \begin{bmatrix} 000111 \\ 001011 \\ 010011 \\ 100011 \end{bmatrix}, \quad B^1 = \begin{bmatrix} 000111 \\ 001011 \\ 010011 \\ 101001 \end{bmatrix}, \quad B^2 = \begin{bmatrix} 000111 \\ 001011 \\ 010011 \\ 011011 \end{bmatrix}
\]

We can check that these matrices are not the basis matrices of $(U_{ex}, \Gamma_{ex})$-VSS-4-MI schemes. For example, consider the case of $A_{124} = \{U_1, U_2, U_4\}$. If $B^\varphi, \varphi = 0, 1, \ldots, 15$, are the basis matrices of the $(U_{ex}, \Gamma_{ex})$-VSS-4-MI schemes, it must hold from (iii) in Definition 9 that
\[
B^\varphi \{A_{124}\} \sim B^{\ell + 1} \{A_{124}\} \sim B^{\ell + 2} \{A_{124}\} \sim B^{\ell + 3} \{A_{124}\}, \quad \ell = 0, 4, 8, 12
\]
for $\ell = 0, 4, 8, 12$ since $A_{124}$, satisfies that $J_{\varphi} (A_{124}) = \{1, 2\}$. Actually, the basis matrices in (57) satisfy such requirements. However, it is easy to check that $B^\ell \{A_{124}\} \sim B^{\ell + 1} \{A_{124}\}, \quad \ell = 0, 4, 8, 12$ does not hold for the matrices in (60).

5. Concluding Remarks

In this paper, it was shown how to define and construct VSS-$q$-MI-R schemes with general access structures, and we pointed out that the VSS-$q$-MI-R schemes can be constructed from VSS-$2q$-MI schemes. Finally, we note that the technique shown in this paper can be applied to the VSS schemes which allow some shares to be turned over in the proof of Theorem 15, we use the fact that $\sigma^2_{\varphi} = \text{id}$ in (34), but any other property of $\sigma_{\varphi}$ is not used. This implies that we can use the other operation of shares represented by the permutation $\sigma$ if $\sigma$ satisfies $\sigma^2 = \text{id}$. For example, consider the following permutations:

\[^1\text{Actually, it is easy to make } m \text{ smaller than 24.}\]

\[^{11}\text{This fact does not imply that the condition (iii) in Definition 9 is not generally required in constructing } B^\varphi.\]
Example 20. Denote by $\sigma_H$ and $\sigma_V$ the permutations of sub-pixels which represent the operations to turn over the shares around the horizontal and the vertical lines, respectively. Assume that each pixel has $h$ subpixels in hight and $w$ subpixels in width, i.e., the pixel expansion is given by $m = hw$. Then, the permutations $\sigma_H$ and $\sigma_V$ can be represented as follows:

$$\sigma_H(i) = w(h - u - 1) + v,$$

$$\sigma_V(i) = uu + (h - v + 1).$$

where we assume that $i = uu + v$, $0 \leq u \leq h - 1$, $1 \leq v \leq w$. These permutations satisfy that $\sigma_H^2 = \sigma_V^2 = id$, and hence, VSS schemes which include the permutations $\sigma_H$ or $\sigma_V$ can be constructed in the same way as Theorem 15 by replacing $\sigma_R$ with $\sigma_H$ or $\sigma_V$.

Not only $\sigma_H$ and $\sigma_V$, we can construct the VSS schemes allowing to turn over the shares around the diagonal lines in the case of $h = w$.

In the above cases, the point symmetrical two positions $U$ and $L$ introduced in Sect. 3 can be considered as the line symmetrical two positions.

For instance, a VSS scheme with 2 shares using $\sigma_V$ can be realized as shown in Fig. A-2. In this example, secret image $S^1$ can be decrypted by stacking $V_1$ and $V_2$, and the other secret image $S^2$ can be obtained by stacking $V_1$ and $V_2$ turned over around the vertical line.

Acknowledgments

The work of M. Iwamoto was partially supported by the MEXT Grant-in-Aid for Young Scientists (B) No.17760298. The work of L. Wang was carried out during his stay at University of Electro-Communications (UEC), Japan, where he was sponsored by Japanese Government Scholarship (JASSO Scheme). He wishes to express his sincere appreciation to all the member of Ohta-Kunihiro Lab. for their warm supports and hospitality shown during his study time at UEC.

References

Appendix: Examples of Shares and Decrypted Images

In Fig. A-1, we give an example of shares and decrypted images of the (2, 2)-VSS-2-MI-R schemes. In this example, the access structure is given by (8) in Example 4, and the secret images are shown in Fig. 1.

In Fig. A-2, we show an example of the VSS scheme with 2 shares allowing some shares to be turned over around the vertical line. In this example, secret image $SI^{(1)}$ can be decrypted by stacking $V_1$ and $V_2$, and the other secret image $SI^{(2)}$ can be obtained by stacking $V_1$ and $V_2$ turned over around the vertical line.

Fig. A-1 An example of shares and decrypted images in a (2, 2)-VSS-2-MI-R scheme.
Fig. A 2  An example of shares and decrypted images in a VSS scheme allowing the shares to be turned over around the vertical line.

Mitsugu Iwamoto was born in Fukuoka, on 29 July, 1976. He received the B.E., M.E., and Ph.D. in information science and technology from the University of Tokyo, Japan, in 1999, 2001, and 2004, respectively. Currently, he is a research associate in Graduate School of Information Systems, University of Electro-Communications. His research interest includes information security and cryptography. Dr. Iwamoto is a member of the IEEE Information Theory Society and the SITA (Society of Information Theory and Its Applications).

Lei Wang was born in Hebei, China, on 2 October, 1983. He is currently a senior undergraduate student at Shang Hai Jiaotong University. During 2004–2005, he was an exchange student at University of Electro-Communications (UEC), Japan. He has been engaged in research on cryptography.
Kazuki Yoneyama received B.E. and M.E. degrees from the University of Electro-Communications, Tokyo, Japan, in 2004 and 2006, respectively. He is currently a doctor course student at Graduate School of Electro-Communications since 2006. He is presently engaged in research on cryptography.

Noboru Kunihiro was born in Aichi, Japan on June 26, 1971. He received his B.E., M.E. and Ph.D. in mathematical engineering and information physics from the University of Tokyo in 1994, 1996 and 2001, respectively. He is an Associate Professor of the University of Electro-Communications. He was a researcher of NTT Communication Science Laboratories between 1996 and 2002. Since 2002, he has been working for Department of Information and Communication Engineering of the University of Electro-Communications. His research interest includes cryptography, information security and quantum computations. He was awarded the SCIS’97 paper prize.

Kazuo Ohta received his B.S., M.S., and Dr.S. degrees from Waseda University, Tokyo, Japan, in 1977, 1979, and 1990, respectively. He has been a professor at the University of Electro-Communications since 2001. He was a researcher at NTT Laboratories between 1979 and 2001. He is presently engaged in research on information security. Dr. Ohta is a member of the International Association for Cryptologic Research.