FORMULATION OF VISUAL SECRET SHARING SCHEMES ENCRYPTING MULTIPLE IMAGES

Manami Sasaki and Yodai Watanabe

Department of Computer Science and Engineering, University of Aizu
Aizu-Wakamatsu City, Fukushima 9658580, Japan

ABSTRACT

Secret sharing is a method of generating multiple shares from secret information so that only a qualified set of shares can be employed to recover this secret information. Visual secret sharing (VSS) is an example of secret sharing; its decryption can be performed by using human eyes without a computer. This paper provides a formulation of encryption for multiple secret images, which is a generalization of the existing ones, and also a general method of constructing VSS schemes encrypting multiple secret images.

Index Terms— Visual secret sharing, Information-theoretic security, Multiple secret images

1. INTRODUCTION

A secret sharing (SS) scheme is a method of generating multiple shares from a secret so that any qualified set of shares can be employed to recover the secret, but no forbidden set of shares reveals any information about the secret. Therefore, an SS scheme can be used to control participants' access to secret information and to diversify risks of leaking of secret information. A (k, n)-threshold SS scheme [1, 2] is a typical example of the SS schemes; this is a method of sharing a secret among n participants in such a way that any k or more participants can recover the secret with their shares, but no $k-1$ or less participants can obtain any information about the secret from their shares.

There exist SS schemes whose decryption requires no numerical computations but can be performed by a human. A visual secret sharing (VSS) scheme [3] is an example of such SS schemes. In VSS schemes, secrets and shares are both visual data such as printed texts, hand written notes, pictures, and so on. The VSS schemes encrypt a visual secret into visual shares so that humans can recover the visual secret with their eyes by superposing a qualified set of visual shares printed on transparencies. Figure 1 illustrates an example of two shares and their superposition of a $(2, 2)$-threshold VSS scheme.

This work was supported in part by a Grant-in-Aid for Young Scientists (B) No. 21700021, and Fukushima Prefectural Foundation for Advancement of Science and Education.

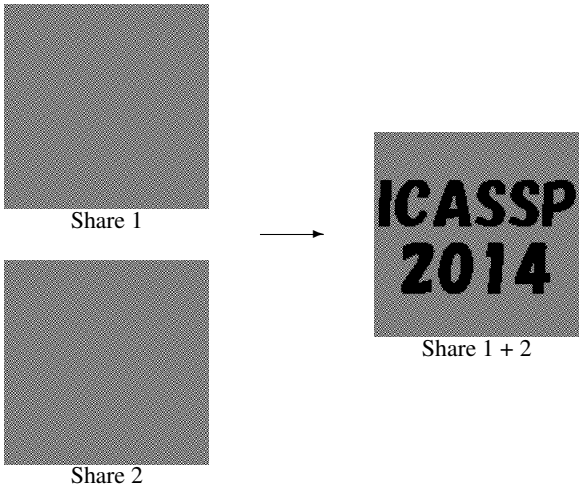


Fig. 1. Two shares and their superposition of a $(2, 2)$-threshold VSS scheme

Table 1. Comparison among the existing works and this work

	Restriction on access structure
EVCS [4]	Each share has to be an image
VSS-q-PI [5]	The forbidden sets have to be identical
This work	No restrictions

There have been proposed two types of VSS schemes encrypting multiple images: extended visual cryptography schemes (EVCS) [4] and VSS schemes for plural secret images (VSS-q-PI) [5]. In EVCS, additional secret images are associated with each share, while in VSS-q-PI, multiple secret images are associated with the corresponding qualified sets of shares but the forbidden sets of shares have to be identical. The aim of this paper is to generalize the formulation of encryption for multiple images so that those of the existing schemes may be included as a special case. Table 1 summarizes the existing works as well as this work.

The rest of this paper is organized as follows. In Section 2, we provide notations and definitions that will be used later. Section 3 is devoted to providing a formulation and a construction method of VSS schemes encrypting multiple se-

978-1-4799-2893-4/14/$31.00 ©2014 IEEE

cret images. Section 4 concludes this paper with mentioning a problem for future work.

2. 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. [6, 7].

2.1. Basic definitions and notations

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

$$(A)_- = \{a \in A | \forall a' \in A(a' \not\subset a)\}.$$

For random variables X and Y over the same domain, we write $X \sim Y$ 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:

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

The gray level $\mathrm{Gray}(x)$ of $x \in \{0,1\}^n$ is given by

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

2.2. Access structure and secret sharing

Let $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$ be the set of all the shares. The subset of $2^{\mathcal{P}}$ whose elements can decrypt the secret is called the *qualified set* and is denoted by A_Q. The subset of $2^{\mathcal{P}}$ whose element can obtain no information about the secret is called the *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* $\mathcal{P}$. Any access structure has to satisfy the following *monotonicity*:

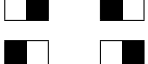
$$A \in A_Q \wedge A \subseteq B \Rightarrow B \in A_Q,$$
$$B \in A_F \wedge A \subseteq B \Rightarrow A \in A_F,$$

for any $A, B \subseteq \mathcal{P}$. A qualified set A_Q is uniquely determined by its minimal elements $(A_Q)_-$:

$$(A_Q)_- = (A'_Q)_- \Rightarrow A_Q = A'_Q.$$

An access structure is called *perfect* if every subsets of the shares are included in either the qualified set or the forbidden set. The perfect access structure can be determined by only a qualified set.

Table 2. How to encrypt 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  Share 2 	$\mathcal{C}^0 = \left\{ \begin{pmatrix} 01 \\ 01 \end{pmatrix}, \begin{pmatrix} 10 \\ 10 \end{pmatrix} \right\}$
	Share 1  Share 2 	$\mathcal{C}^1 = \left\{ \begin{pmatrix} 01 \\ 10 \end{pmatrix}, \begin{pmatrix} 10 \\ 01 \end{pmatrix} \right\}$

Example 2.1 ((k,n)-threshold access structure)**.** Let $\mathcal{P}$ be a finite set of size n. A (k,n)-*threshold access structure on* $\mathcal{P}$ consists of the qualified set A_Q and the forbidden set A_F given by

$$A_Q = \big\{a \subseteq \mathcal{P} \big| k \leq |a|\big\} \quad \text{and} \quad A_F = \big\{a \subseteq \mathcal{P} \big| k > |a|\big\}.$$

A secret sharing scheme realizing a (k,n)-threshold access structure is called a (k,n)-*threshold secret sharing scheme*.

2.3. Visual secret sharing

In the ordinary SS schemes, the secret information and shares are both numerical data, and their decryption can be performed by computers. In contrast, in the VSS schemes, the secret information (secret image) and shares are both visual, and their decryption can be performed by human eyes. 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 (Figure 1: left). Each share is indistinguishable from noise images, and so leaks no information about the secret. On the other hand, the secret image can be recovered when both of the shares are superposed (Figure 1: right). 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 2 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 2; 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

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

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 recovered images. A VSS scheme is called *optimal* if it has the highest contrast.

2.4. Notations for matrices

In the same way as [5], we introduce an equivalence relation $\sim$ on the set $\mathcal{M} = \{0,1\}^{nm}$ of $n \times m$ matrices for $n, m \in \mathbb{N}$; for two matrices A and B of the same size, $A \sim B$ represents that 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 2 (see section 2.3) can be written as

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

For an ordered set $\mathcal{S} = (s_1, s_2, \cdots, s_k)$ of finite size, the order of s_i in $\mathcal{S}$ is denoted by $\mathrm{ord}_{\mathcal{S}}(s_i)$: $\mathrm{ord}_{\mathcal{S}}(s_i) = i$. Let $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$ be an ordered set of size n, and a be an ordered subset of $\mathcal{P}$. For an $n \times m$ matrix $M = (m_{ij})$ (where $n = |\mathcal{P}|$), let $[M]_a$ denote the $|a| \times m$ submatrix of M defined by

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

for $P_i \in a$. For a $|a| \times m$ matrix $M = (m_{ij})$, let $[M]^a$ denote the $n \times m$ matrix defined by

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

For two matrices A and B of the same number of rows, let $A|B$ denote the concatenation of A and B.

3. VISUAL SECRET SHARING SCHEMES ENCRYPTING MULTIPLE IMAGES

3.1. Formulation and construction

We first extend the definition of an access structure to the case for multiple secrets.

Definition 1 (Access structure for multiple secrets)**.** Let $\mathcal{P}$ be a finite set, and $q \in \mathbb{N}$. For $i \in [q]$, let A_Q^i and A_F^i be subsets of $2^{\mathcal{P}}$ such that $A_Q^i \cap A_F^i = \emptyset$. The pairs Γ^q of the subsets A_Q^i and A_F^i, $\Gamma^q = \left\{(A_Q^i, A_F^i)\right\}_{i=1}^q$, is called an *access structure on $\mathcal{P}$ for q secrets* if A_Q^i and A_F^i satisfy the monotonicity:

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

for any $A, B \subseteq \mathcal{P}$ and $i \in [q]$, and the uniqueness:

$$(A_Q^i)_- \cap (A_Q^j)_- = \emptyset$$

for any $i, j \in [q]$ such that $i \neq j$. For an access structure $\Gamma^q = \left\{(A_Q^i, A_F^i)\right\}_{i=1}^q$, A_Q^i and A_F^i are called the *qualified set* and the *forbidden set for the i-th secret*, respectively. An access structure $\Gamma^q = \left\{(A_Q^i, A_F^i)\right\}_{i=1}^q$ is called *minimally refined* if $|(A_Q^i)_-| = 1$ for any $i \in [q]$.

If we pose the restriction

$$(A_Q^i)_- = \{\{P_i\}\} \text{ with } q = |\mathcal{P}| + 1 \quad \big(\text{resp. } A_F^i = A_F\big)$$

for all i, then the above definition coincides with that introduced by [4] (resp. [5]). Therefore, the above definition can be considered as a generalization of the existing ones.

We next give a definition of VSS schemes encrypting multiple secret images.

Definition 2 (VSS schemes encrypting multiple images)**.** Let $\mathcal{P}$ be a finite set, $m, q \in \mathbb{N}$ and $q' \in [q]$. Let $\Gamma^q = \left\{(A_Q^i, A_F^i)\right\}_{i=1}^q$ be an access structure on $\mathcal{P}$ for q secrets. Let Enc be a probabilistic function from $\{0,1\}^q$ to $\{0,1\}^{qm}$ and Dec be a deterministic function from $\{0,1\}^{q'm}$ to $\{0,1\}^m$. 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 $M = (m_{ij})$:

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

for any $j \in [m]$, and Enc and Dec satisfy the following conditions:

$$\forall a \in (A_Q^i)_- \Big(\min_{b \in \{0,1\}^q} g_i(a; b, 1) > \max_{b \in \{0,1\}^q} g_i(a; b, 0) \Big),$$
$$\forall a \in A_F^i \forall b \in \{0,1\}^q \big([\mathrm{Enc}(b_{b_i=0})]_a \sim [\mathrm{Enc}(b_{b_i=1})]_a \big),$$

for any $i \in [q]$, where

$$g_i(a; b, b') = \mathrm{Gray}(\mathrm{Dec}([\mathrm{Enc}(b_{b_i=b'})]_a)).$$

To provide a construction of VSS schemes encrypting multiple images, we introduce a notation for representing matrices. For $b \in \{0,1\}$ and $n \in \mathbb{N}$, let $C_{(n,n)}^b$ denote matrices such that $\left\langle C_{(n,n)}^0 \right\rangle$ and $\left\langle C_{(n,n)}^1 \right\rangle$ constitute the sets of

representing matrices for an (n, n)-threshold VSS scheme. For example,

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

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

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

Construction 1. Let $\mathcal{P}$ be a finite set, and $q \in \mathbb{N}$. Let $\Gamma^q = \{(A^i_Q, A^i_F)\}^q_{i=1}$ be a minimally refined access structure on $\mathcal{P}$ for q secrets. For $i \in [q]$, let a^i_q be the element of $(A^i_Q)_-$: $(A^i_Q)_- = \{a^i_q\}$ with $a^i_q \subseteq \mathcal{P}$. For $b \in \{0, 1\}$ and $i \in [q]$, let $C^b_i = [C^b_{(n_i,n_i)}]^{a^i_q}$ with $n_i = |a^i_q|$. Define Enc by

$$\mathrm{Enc}(b) := \left\langle C^{b_1}_1 | C^{b_2}_2 | \cdots | C^{b_q}_q \right\rangle_U$$

for $b \in \{0, 1\}^q$, and Dec as in Definition 2.

From the above definition of C^b_i, it is straightforward to verify the following theorem. Since any access structure can be transformed into a minimally refined one (with the duplication of secret images allowed), Construction 1 applies to general access structures for multiple secrets.

Theorem 1. Let $\mathcal{P}$ be a finite set, and $q \in \mathbb{N}$. Let $\Gamma^q = \{(A^i_Q, A^i_F)\}^q_{i=1}$ be a minimally refined access structure on $\mathcal{P}$ for q secrets. Then, $VSS = (\mathrm{Enc}, \mathrm{Dec})$ given by Construction 1 is a visual secret sharing scheme realizing Γ^q.

3.2. Illustrative example

We now construct a VSS scheme according to Construction 1. Let $\mathcal{P} = \{P_1, P_2, P_3\}$ be a set of shares. We consider the following minimally refined perfect access structure $\Gamma^7 = \{(A^i_Q, A^i_F)\}^7_{i=1}$ for seven secret images $\{v_i\}^7_{i=1}$ of the same size, where

$$(A^1_Q)_- = \{\{P_1\}\},\ (A^2_Q)_- = \{\{P_2\}\},\ (A^3_Q)_- = \{\{P_3\}\},$$
$$(A^4_Q)_- = \{\{P_1, P_2\}\},\ (A^5_Q)_- = \{\{P_1, P_3\}\},$$
$$(A^6_Q)_- = \{\{P_2, P_3\}\},\ (A^7_Q)_- = \{\{P_1, P_2, P_3\}\},$$

with $(A^i_F)_- = 2^{\mathcal{P}} - A^i_Q$ for all $i \in [7]$. It should be noted that no existing schemes, neither EVCS [4] nor VSS-q-PI [5], can realize Γ^7. From the definition of C^b_i, we have

$$C^0_1 = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix},\ C^0_2 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix},\ C^0_3 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix},\ C^0_7 = \begin{pmatrix} 0011 \\ 0101 \\ 0110 \end{pmatrix},$$

$$C^1_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix},\ C^1_2 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix},\ C^1_3 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix},\ C^1_7 = \begin{pmatrix} 1001 \\ 1010 \\ 1100 \end{pmatrix},$$

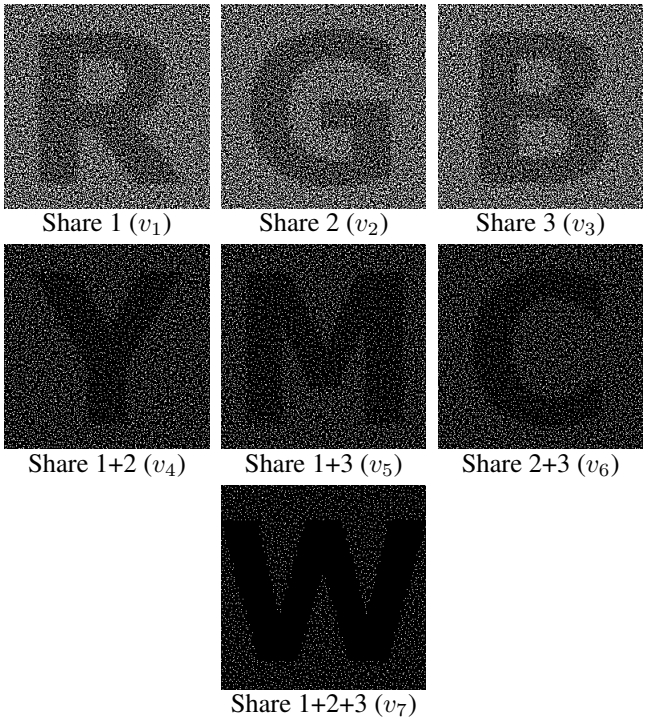


Fig. 2. VSS scheme realizing Γ^7 with secret images $\{v_i\}^7_{i=1}$ representing the additive mixture of the primary colors

$$C^0_4 = \begin{pmatrix} 01 \\ 01 \\ 11 \end{pmatrix},\ C^0_5 = \begin{pmatrix} 01 \\ 11 \\ 01 \end{pmatrix},\ C^0_6 = \begin{pmatrix} 11 \\ 01 \\ 01 \end{pmatrix},$$

$$C^1_4 = \begin{pmatrix} 01 \\ 10 \\ 11 \end{pmatrix},\ C^1_5 = \begin{pmatrix} 01 \\ 11 \\ 10 \end{pmatrix},\ C^1_6 = \begin{pmatrix} 11 \\ 01 \\ 10 \end{pmatrix}.$$

Suppose that the top-left pixels of the secret images $\{v_i\}^7_{i=1}$ 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 $\mathrm{Enc}(b) := \left\langle C^{b_1}_1 | C^{b_2}_2 | \cdots | C^{b_7}_7 \right\rangle_U$. All the other pixels of the secret images are encrypted in the same way. Figure 2 shows an example of this VSS scheme[1].

4. CONCLUSION

In this paper, we generalized the formulation of VSS encryption for multiple secret images so that those of the existing schemes, EVCS [4] and VSS-q-PI [5], may be included as a special case. We then provided a general method of constructing VSS schemes encrypting multiple secret images. We also provided an example of VSS schemes which cannot be formulated as the existing ones. It will be the subject of future work to examine the optimality of Construction 1.

[1] In this example, $C^{b_1}_1$, $C^{b_2}_2$ and $C^{b_3}_3$ are concatenated twice to make the pixel expansion m a square: $m = 1 \times 3 \times 2 + 2 \times 3 + 4 = 4^2$. Hence, Contrast = $\frac{2}{16}$ for $\{v_i\}^3_{i=1}$ and $\frac{1}{16}$ for $\{v_i\}^7_{i=4}$.

5. REFERENCES

[1] George Robert Blakley, "Safeguarding cryptographic keys," in *Proceedings of the National Computer Conference*, Monval, NJ, USA, 1979, pp. 313–317, AFIPS Press.

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

[3] Moni Naor and Adi Shamir, "Visual cryptography," in *Proceedings of Advances in Cryptology – Eurocrypt '94*, Perugia, Italy, 1994, vol. 950 of *Lecture Notes in Computer Science*, pp. 1–12, Springer-Verlag.

[4] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis, and Douglas R. Stinson, "Extended capabilities for visual cryptography," *Theoretical Computer Science*, vol. 250, no. 1–2, pp. 143–161, 2001.

[5] Mitsugu Iwamoto and Hirosuke 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.

[6] Thomas M. Cover and Joy A. Thomas, *Elements of Information Theory*, Wiley-Interscience, 2nd edition, 2006.

[7] Douglas Robert Stinson, *Cryptography: Theory and Practice*, Chapman & Hall, CRC, 3rd edition, 2005.