General Construction Methods of Secret Sharing Schemes and Visual Secret Sharing Schemes

（秘密分散法および視覚復号型秘密分散法の一般的構成法）

岩本 貢

Abstract

A *secret sharing* (SS) scheme is a method to encrypt a secret S into n pieces called *shares*, each of which has no information of the secret, but S can be decrypted from some specified collection of shares. For example, in (k, n)-*threshold* SS schemes, any k out of n shares can decrypt S while $k-1$ or less shares do not leak out any information of S. The (k, n) threshold access structure can be extended to a *general access structure*, which is specified by the families of qualified sets and forbidden sets, such that a qualified set can decrypt the secret, and a forbidden set does not leak out any information of the secret. SS schemes are one of the most important techniques for secure data storage, and hence, many researches have been devoted to this subject.

The decoding of ordinary SS schemes is implemented by a computer. But, the decoding of *visual secret sharing* (VSS) schemes is realized based on human eyesight by peering at several shares stacked up. In this thesis, we propose some new efficient construction methods of SS and VSS schemes, which are treated in Part I and Part II, respectively.

We aim in Part I to construct efficient ordinary SS schemes. First, we derive the lower bounds of coding rates for *ramp* SS schemes. Ramp SS schemes are extensions of ordinary SS schemes, which we call *perfect* SS schemes in order to distinguish them from ramp SS schemes. Hence, our results include some known results of coding rates for prefect SS schemes as special cases.

In order to derive the lower bounds of coding rates in ramp SS schemes, we classify shares into three categories called *super-additive*, *additive*, and *sub-additive*. Then, we clarify that the coding rates for sub-additive shares are less efficient than the other two types of shares. We also derive the lower bounds of coding rates for super-additive and additive shares.

In previous works for the lower bounds of coding rates for perfect SS schemes, they are often classified into two categories called *ideal* or *non-ideal* SS schemes, and the properties of access structures are investigated in each category. In this thesis, we extend the notion of ideal perfect SS schemes to define *well-realized* ramp SS schemes. By evaluating the lower bounds of coding rates for ramp SS schemes, we analyze what kind of access structures cannot be well-realized as ramp SS schemes. These results are extensions of known ones for non-ideal perfect SS schemes and ramp SS schemes with general access structures.

Next, we propose a new method to construct SS schemes with general access structures in Part I. It is well known how to construct efficient (k, n)-threshold SS schemes although no efficient construction method is known for arbitrarily given general access structures. The *cumulative map*, which is a special case of *multiple assignment map*, is a known simple construction method of SS schemes with general access structures. But, it is generally inefficient, especially in the case that access structures are close to (k, n)-threshold access structures. In this thesis, we design the *optimal* multiple assignment maps using integer programming. The coding rate obtained by our method is optimal in the multiple assignment maps, and hence, it is more efficient than the cumulative map. Furthermore, since the proposed construction is very simple, it can easily be applied to SS schemes with general ramp and/or incomplete access structures.

In Part II, we propose some construction methods of VSS schemes, which are superior in the viewpoint of the quality of decrypted images and the generalities of access structures.

In VSS schemes, each pixel of a decrypted image consists of a set of *subpixels* which is represented by a *basis matrix*. In previous works, it was difficult to derive basis matrices since they are combinatorially defined. Hence, many known studies on VSS schemes treated only black-white (BW) binary secret images, and there are few studies of VSS schemes for color secret images because they must deal with more combinations of colors in basis matrices compared with the case of BW binary secret images. Based on such backgrounds, a simple construction method was proposed to derive VSS schemes with color images called *algebraic* construction, which does not use the combinatorial methods. It is known that the algebraic construction can realize an efficient VSS scheme, but it could not be applied to VSS schemes for BW binary secret images. In order to improve such defects, a modified algebraic construction was proposed. However, the performance of the modified method has not been studied. In this thesis, we clarify that the modified algebraic construction can attain the *optimal* (n, n)-threshold VSS schemes for gray-scale images, and we also derive the basis matrices for the optimal (n, n)-threshold VSS schemes for gray-scale images.

We also consider VSS schemes for plural secret images in this thesis. We note that the known VSS schemes for plural secret images can treat only BW binary secret images. Furthermore, some definitions of such VSS schemes are not accurate in the sense of security. In other words, decrypted images may leak out some information of the other decrypted images in such VSS schemes. Hence, we carefully define the security condition of VSS schemes for plural secret images. We also propose the construction methods of the secure VSS schemes that satisfy such security conditions. Furthermore, we note that the proposed VSS scheme can treat color secret images with shades, and hence, our VSS scheme includes most of previous VSS schemes as special cases.

Acknowledgement

I would like to express my sincere gratefulness to my supervisor, Prof. Hirosuke Yamamoto for his continuous encouragements and suggestions, that led to this thesis, during many years in his laboratory. He gave me the discipline required to study in the research of information security. Furthermore, he gave me many opportunities to present our results in conferences or technical meetings. This thesis would not have been accomplished without his invaluable day-to-day support.

I would like to acknowledge all my co-authors, Prof. Hiroki Koga in University of Tsukuba, Dr. Tomohiro Ogawa, Mr. Akira Sasaki in University of Tokyo, and Mr. Hirohisa Ogawa in C4 Technologies Inc., who cooperated with me during this research. Especially, Prof. Hiroki Koga introduced me visual secret sharing schemes and gave me many suggestions and encouragements on this research. I also thank him for providing me his software program of visual secret sharing schemes. I had many interesting discussions with Dr. Tomohiro Ogawa, and he taught me many things in information theory and related mathematics. The results of Chapter 4 in this thesis came from the studies to solve problems shown by Mr. Hirohisa Ogawa.

I am also indebted to Prof. Hideki Imai, Prof. Satoru Iwata, Prof. Kazuo Murota, and Prof. Kokichi Sugihara for their careful reading of this manuscript in its original form and giving me many helpful comments and suggestions. I would like to give my special thanks to Prof. Satoru Iwata who always gave me his encouragements and many suggestions about algorithms and methods of mathematical optimizations.

I have been working as a research assistant of the Superrobust Computation Project of the 21st Century COE Program, "Information Science and Technology Strategic Core," from October in 2002. I like to thank all the people who related to the project.

Many thanks go to all the members of Mathematical Information Laboratory #3, with whom I enjoyed seminars, discussions, and my life in university.

Finally, it is my pleasure to thank my parents, sister and brother for supporting me for my education.

December, 2003
Mitsugu Iwamoto
Tokyo, Japan

Contents

List of Figures

Chapter 1

Overview of the Thesis

1.1 What is a Secret Sharing Scheme?

Due to the recent development of computers and computer networks, huge amount of digital data can easily be transmitted or stored. However, we note that transmitted data in networks or stored data in computers may easily be eavesdropped or substituted by enemies if the data are not enciphered by some cryptographic tools. Therefore, information security is one of the most important technologies in modern computerized society.

For secure data transmission against eavesdropping or substitution attacks, two important technologies were invented in 1970's, and the development of secure computer networks was accelerated by the methods. They are the *public key* cryptosystem, which was proposed by Diffie-Hellman in 1976 [34], and the *Data Encryption Standard* (DES), which is a *secret key* cryptosystem adopted by the National Bureau of Standards in U.S.A. in 1977 [75]. The *RSA* cryptosystem, which is the first practical public key cryptosystem proposed by Rivest-Shamir-Adleman in 1978 [97], cleared the *key distribution* problem in secret key cryptosystems. Furthermore, it is shown in [97] that the *digital signature* scheme can be realized by the public key cryptosystems. Based on these public key cryptosystems, many useful cryptographic protocols are designed. The DES was taken over by *Rijndael* [31] as the *Advanced Encryption Standard* (AES) adopted by National Institute of Standard and Technology in U.S.A. in 2000. In this way, information security for data transmission has been extensively studied.

In the case of secure data storage, we have the same problems such as eavesdropping and substituting, and such threats can be overcome by the same cryptographic technologies. However, we may have other threats such as troubles of storage devices or attacks of destruction. In order to prevent such attacks, we must make as many copies of the secret as possible. But, if we have many copies of the secret, the secret tends to leak out, and hence, the number of the copies should be as small as possible. This contradictive requirement can be solved by a secret sharing scheme, which was proposed independently by Shamir [99] and Blakley [8] in 1979.

A *secret sharing* (SS) scheme is a method to encrypt secret information S into n pieces called *shares* $V_1, V_2, \ldots, V_n$, each of which has no information of secret S, but S can be decrypted by collecting several shares. For example, consider a (k, n)-*threshold* SS scheme illustrated in

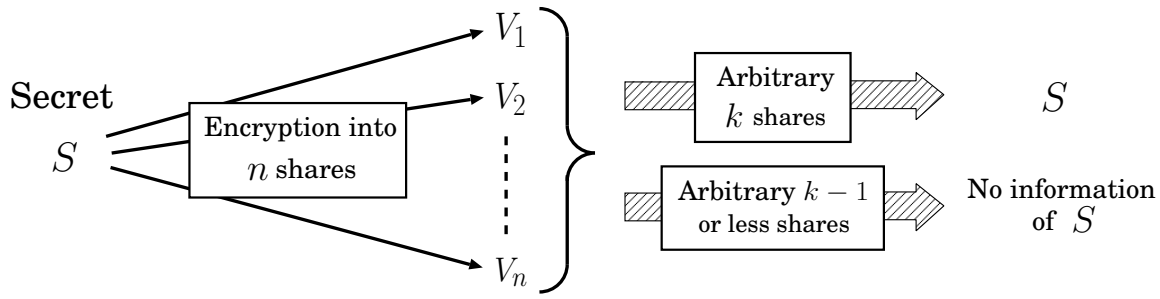


Figure 1.1. A (k, n)-threshold secret sharing scheme

Figure 1.1. In this SS scheme, any k out of n shares can decrypt secret S but any $k-1$ or less shares do not leak out any information of S. Hence, even if $n-k$ shares are destroyed by an enemies, we can recover S from the remaining k shares. Furthermore, even if an enemy steals $k-1$ shares, any information about S does not leak out. This means that the SS scheme is secure against both destruction and stealing. We also note that the SS scheme is *unconditionally secure* because the SS scheme is not based on any assumption of computational difficulties like the factorization of integers or the calculation of discrete logarithms. Hence, it is appropriate for a long time data storage. Furthermore, the SS schemes are expected to be used in the environment of ubiquitous networks to share secrets among many entities.

1.2 Extensions of Threshold Secret Sharing Schemes

The original SS scheme by Shamir [99] and Blakley [8] is a (k, n)-threshold SS scheme. But, it can be extended in two ways, which is shown in Table 1.1 and summarized as follows.

In the case of (k, n)-threshold access structure, we assume that every share is equally important, but there are cases such that we want to make some shares more important than the others. For example, consider the case that a secret is shared in a company as follows: A president wants to distribute the shares of a secret S to directors of the company in such a way as S can be decrypted if and only if two vice-presidents or more than five directors except vise-presidents cooperate with each other. In such cases, the shares of directors are less important than those of vice-presidents. Since this decoding aspect cannot be realized by (k, n)-threshold SS schemes, a *general access structure* must be introduced to attain the desired security. A general access

Table 1.1. Extensions of (k, n)-threshold secret sharing schemes

	Threshold Type	General Access Structure
Perfect SS schemes	Shamir [99], Blakley [8]	Itoh et al. [47]
Ramp SS schemes	Blakley-Meadows [9], Yamamoto [118], [119]	Kurosawa et al. [71]

structure consists of *qualified sets* and *forbidden sets*. A qualified set is the set of shares that can decrypt the secret while a forbidden set is the set of shares that must not leak out any information of the secret. In order to realize a secure data storage efficiency, we must make a size of each share as small as possible, and hence, efficient coding methods for SS schemes with general access structures must be established. It is known how to construct efficient (k, n)-threshold SS schemes [99]. However, we have known no method to obtain efficient SS schemes for given general access structures.

As another extension of (k, n)-threshold SS schemes, *ramp* SS schemes were proposed independently by Blakley-Meadows [9] and Yamamoto [118], [119] in 1984. A ramp SS scheme is a SS scheme with intermediate properties between qualified sets and forbidden sets. The first ramp SS schemes [9], [119] are threshold SS schemes called (k, L, n)-threshold ramp SS schemes. The (k, L, n)-threshold ramp SS schemes are designed such that a secret S can be decrypted from arbitrary k-out-of-n shares but no information of S cannot be obtained from arbitrary $k - L$ or less shares. Furthermore, from arbitrary $k - j$ shares for $j = 1, 2, \ldots, L - 1$, some information of S leak out with the amount of $\frac{j}{L}$ in S. In the case of $L = 1$, (k, L, n)-threshold ramp SS schemes reduce to (k, n)-threshold SS schemes, and hence, ramp SS schemes can be considered as an extension of (k, n)-threshold SS schemes treated in Section 1.1. Furthermore, by introducing ramp SS schemes, the coding rates of shares can be reduced compared with ordinal SS schemes, and hence, ramp SS schemes can attain efficient coding rates at a little sacrifice of security. To distinguish ordinal SS schemes from ramp SS schemes, ordinal SS schemes are called *perfect* SS schemes. Furthermore, ramp SS schemes with general access structures were proposed by Kurosawa et al. [71].

In the case that the number of shares n is large, it is cumbersome to specify whether each subset of shares is a qualified set or a forbidden set in perfect SS schemes since the number of subset of shares is 2^n. Hence, it is desirable to construct a SS scheme even in the case that we don't care the properties of some subsets of n shares. We call such an access structure *incomplete*. Note that incomplete access structures can be considered for ramp SS schemes in addition to perfect SS schemes.

1.3 Variations of Secret Sharing Schemes

SS schemes introduced in previous sections, e.g., [8], [99], are based on algebraic calculations in their realizations. But there are some different realizations from ordinal SS schemes. In such other realizations, some physical informations are used instead of numbers on finite fields. Table 1.2 shows what kind of secret information is used to realize each SS scheme. In this section, we introduce such SS schemes.

Since we treat visual secret sharing (VSS) schemes in Part II of this thesis, we first give a brief introduction to VSS schemes in the Section 1.3.1 and the other SS schemes will be reviewed in Section 1.3.2.

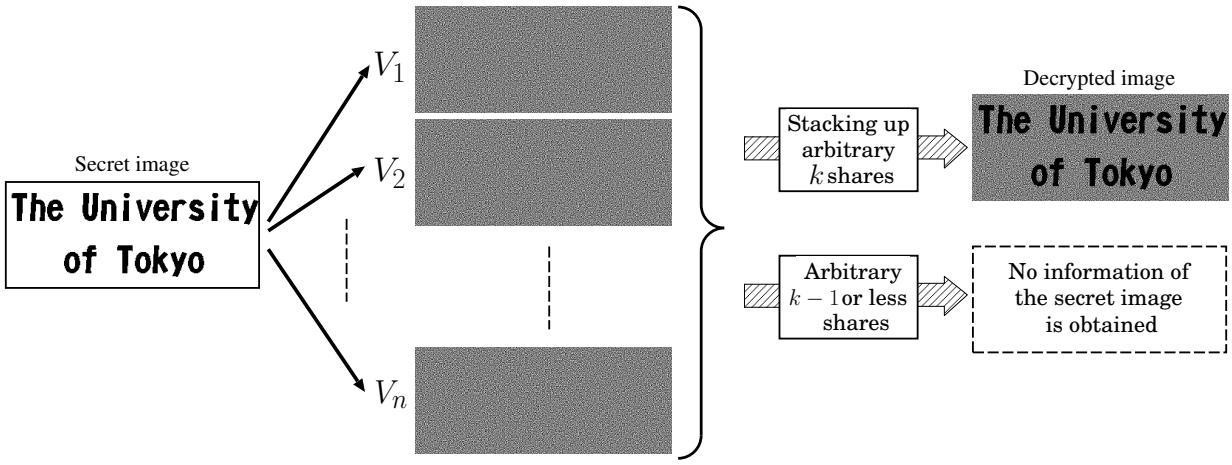


Figure 1.2. An example of a (k, n)-threshold VSS scheme

1.3.1 Visual Secret Sharing Schemes

A *visual secret sharing* (VSS) scheme, which originates from the *visual cryptography* proposed by Naor-Shamir [81], may be one of the most well known realization of SS schemes.

The VSS scheme is a method to encode a secret image into several shares, each of which does not reveal any information of the secret image. Each share is printed on a transparency, and is distributed to one of n participants. The secret image can easily be decrypted only by stacking the shares in an arbitrary order. For instance, an example of a (k, n)-threshold VSS scheme is illustrated in Figure 1.2. Note that VSS schemes can be realized for not only (k, n)-threshold access structures but also general access structures. Furthermore, VSS schemes for color and/or gray-scale secret images can be constructed although the example in Figure 1.2 treats black-white (BW) binary secret image.

We note that VSS schemes need no computation in decryption. This fact distinguishes VSS

Table 1.2. Variations of secret sharing schemes

Based on	Name	Secret information	Proposed first by
Computers	SS schemes	Numbers in finite fields	Shamir [99], Blakley [8]
Human sense	Visual cryptography	Images	Naor-Shamir [81]
	Cerebral cryptography	3D images	Desmedt et al. [33]
	Optical cryptography	Lights	Desmedt et al. [32]
	Audio cryptography	Sounds	Desmedt et al. [32]
	Tempo-based audio cryptography	Rhythms	Chiou-Laih [26]
Quantum information	Quantum SS scheme	Numbers	Hillery et al. [41]
	Quantum SS scheme	Quantum states	Cleve et al. [28]

scheme from ordinary SS schemes. Hence, VSS schemes can be used even in the case that any electrical power or any computers cannot be used, e.g., in the case of disasters. We note that VSS schemes are unconditionally secure. Therefore, VSS schemes are important and interesting realizations of SS schemes.

In VSS schemes, we must have importance on the realization of clear decrypted images with high contrast and high resolution rather than efficient coding rates.

1.3.2 Other Secret Sharing Schemes

In this section, we summarize several different realizations of SS schemes from ordinal SS and VSS schemes.

The *audio cryptography* [26], [32], the *optical cryptography*, [32] and the *cerebral cryptography* [33] are also SS schemes which use human senses in decryption in the same way as VSS schemes. In the audio and optical cryptography [32], a secret and shares are sounds or lights which can be considered as *waves*, and the interference of waves are used in decryption. In other words, the waves of shares corresponding to a qualified set are strengthened each other to listen to or to see the secret, but the waves of shares for a forbidden set are weakened each other to hide the secret. The audio cryptography [32] is not unconditionally secure, although the *tempo-based* audio cryptography proposed in [26] can guarantee unconditional security. In the tempo-based audio cryptography, secret bits are encrypted into rhythms, and security assumptions are similar to VSS schemes. The cerebral cryptography is a SS scheme based on the so-called *stereogram*. The stereogram [56] is an illusion of eyesight that can perceive a 3-dimensional image from two 2-dimensional images. However, the security conditions are not clarified in [33].

Recently, *quantum cryptography* is extensively studied. As is the case with classical cryptography, quantum cryptography is also designed for secure data transmissions or secure data storage. The first quantum cryptography for data transmission is the so-called *BB84 protocol* proposed by Bennett-Brassard in 1984 [5], which is a key distribution protocol. On the other hand, for secure data storage, *quantum secret sharing schemes* are proposed in [28], [39], [41], [57]. Compared with classical cryptography, quantum cryptography has remarkable advantages such that it can detect an eavesdropper and a dishonest participant by measurements of quantum states. QSS schemes also have such advantages.

The first QSS scheme [41] is a three-party protocol based on three entangled particles called *Greenberger-Horne-Zeilinger* (GHZ) state. In this QSS scheme, the measurement result for one share can be determined by combining measurement results for the other two shares. Hence, this method in [41] can be considered as an extension of a quantum key sharing scheme rather than a QSS scheme. A (k, n)-threshold QSS scheme is considered in [57] as an extension of the method in [41]. In QSS schemes treated in [41], [57], secret information is ordinary bits which are encoded into quantum states. On the other hand, it is proposed in [28], [39] to encrypt a secret quantum state into shares. It is shown in [28] that (k, n)-threshold QSS schemes can be realized only in the case that $n \leq 2k - 1$, which comes from the requirement of the so-called *no-cloning theorem*. Furthermore, in the case that a secret quantum state is a *pure-state*, it must hold that

$n = 2k - 1$. It is also shown in [39] that QSS schemes for general access structures can be constructed for any mixed-state secret quantum states if access structures satisfy the no-cloning theorem. The coding efficiency of QSS schemes is also treated in [39], [87].

SS, VSS, and QSS schemes can guarantee unconditional security, but *computationally secure* SS schemes are considered in [23], [69]. In the case of computationally secure SS schemes, the coding rates of shares are much more efficient than unconditionally secure SS schemes [69]. Furthermore, such SS schemes can treat plural secrets dynamically without redistributing new shares to participants secretly [23].

1.4 Overview of Backgrounds and Main Results

In this thesis, we treat SS and VSS schemes which will be appeared in Part I and II, respectively. The background and the obtained results in both topics are summarized as follows.

1.4.1 Part I: Secret Sharing Schemes

We aim in Part I to construct efficient ordinary SS schemes. In order to establish efficient coding methods of SS schemes, we have to derive the optimal coding rates or the lower bounds of coding rates for SS schemes with a given general access structure.

In previous works for deriving the lower bounds for coding rates of perfect SS schemes, they are often classified into two categories called *ideal* or *non-ideal* SS schemes, and the property of access structures of SS schemes in each category is investigated. However, it is still difficult to derive the lower bounds of coding rates for a SS scheme with a given general access structure although it is easy to derive it for (k, n)-threshold access structures. Furthermore, there are few studies of the evaluation of coding rates for ramp SS schemes with general access structures. Hence, in this thesis, we analyze the coding rates of ramp SS schemes. As we have described in Section 1.2, ramp SS schemes are extensions of perfect SS schemes, and our results include some known results of coding rates for prefect SS schemes as special cases.

In order to derive the lower bounds of coding rates in ramp SS schemes, we first classify shares into three categories called *super-additive*, *additive*, and *sub-additive*. Note that such classification is not needed in perfect SS schemes since all the shares are super-additive in prefect SS schemes. Then, we clarify that the lower bounds of coding rates for sub-additive shares must be different from the other two types of shares. Furthermore, we derive the lower bounds of coding rates for super-additive and additive shares. Based on these results, we define a *well-realized* ramp SS scheme as an extension of an ideal prefect SS scheme, and we analyze the access structures that cannot be well-realized as ramp SS schemes by deriving the lower bounds of coding rates for such ramp SS schemes. These lower bounds are extensions of the lower bounds for non-ideal perfect SS schemes derived by Blundo et al. [15]. Furthermore, our result also includes the lower bounds of coding rates for ramp SS schemes with general access structures given in [88] as special cases.

We also propose a method to construct SS schemes with general access structures in Part I. It is well known how to construct efficient (k, n)-threshold SS schemes although no efficient construction method is known for arbitrary given general access structures. Actually, the *cumulative map* by Itoh et al. [47]–[49] is a known simple construction method of SS schemes with general access structures. But, it is generally inefficient, especially in the case that access structures are close to (k, n)-threshold access structures. Note that the cumulative map is a realization of so-called a *multiple assignment map* due to Itoh et al. [47]–[49]. The multiple assignment map realizes a SS scheme with a given access structures by distributing shares of a (t, m)-threshold SS scheme such that t or more shares of the (t, m)-threshold SS scheme are assigned to qualified sets but $t - 1$ or less shares are assigned to forbidden sets.

In this thesis, we design the *optimal* multiple assignment maps using integer programming. It is shown that the coding rate obtained by our method is more efficient than the coding rate obtained by cumulative maps. Furthermore, the proposed construction is very simple, and hence, it can easily be applied to SS schemes with general ramp and/or incomplete access structures. Furthermore, this method may be applied to some other realizations of SS schemes with general access structures shown in Section 1.3.2.

1.4.2 Part II: Visual Secret Sharing Schemes

In Part II, we propose some construction methods of VSS schemes, which are superior in the viewpoint of the quality of decrypted images and the generalities of access structures.

In VSS schemes, each pixel of a decrypted image consists of a set of *subpixels* which is represented by *basis matrices*. Hence, the construction of VSS schemes is equivalent to the design of basis matrices. In previous works, however, it was difficult to derive basis matrices for general VSS schemes since they are combinatorially defined. Therefore, many known studies on VSS schemes treated only BW binary secret images, and there are few studies of VSS schemes for color secret images because they must deal with more combinations of colors in basis matrices compared with the VSS schemes for BW binary secret images. Based on such backgrounds, in order to derive (k, n)-threshold VSS schemes with color images, a simple construction method, which does not use combinatorial methods, was proposed by Koga [63] and developed in our joint work [66]. This method is called *algebraic* construction, which can easily be implemented compared with the known VSS schemes. However, this method could not be applied to VSS schemes for BW binary secret images.

To improve such defects, Kuwakado-Tanaka modified the algebraic construction to deal with BW binary images [72]. However, they proposed only the modification, but they did not analyze the performance of the modified method. Hence, we clarify that the modified algebraic construction can attain the *optimal* (n, n)-threshold VSS schemes for gray-scale images, and we derive the basis matrices of the optimal (n, n)-threshold VSS schemes for gray-scale images.

We also consider VSS schemes for plural secret images as extensions of VSS schemes for single secret images. We note that known VSS schemes for plural secret images can treat only BW binary secret images. Furthermore, some definitions of such VSS schemes are not accurate.

In other words, it may occur that decrypted images leak out some information of the other decrypted images. Hence, we carefully define the security condition of VSS schemes for plural secret images. We also propose the construction methods of the desired VSS schemes and it is proved that the proposed VSS schemes satisfy such security conditions. Furthermore, we note that the proposed VSS scheme can treat color secret images with shades, and hence, our VSS scheme includes most of the previous VSS schemes as special cases.

1.5 Organization of Thesis

This thesis is organized into two parts. Part I treats ordinal SS schemes that are implemented by algebraic computations on finite fields in computers, and Part II is devoted to give the general construction methods of VSS schemes. The backgrounds and the known constructions of ordinary SS and VSS schemes are summarized in Chapters 2 and 6, respectively.

Part I is organized as follows: In Chapter 3, we evaluate the coding rates of *ramp* SS schemes. Chapter 4 is devoted to propose an efficient construction method of SS schemes. The proposed method can be applied to SS schemes with ramp and/or incomplete access structures, which are also treated in the same chapter.

Part II consists of two topics. In Chapter 7, we apply the algebraic construction given in Chapter 6 and [66], [72] to VSS schemes for gray-scale images, and it will be shown that the algebraic construction can attain the optimal VSS schemes for gray-scale images in the case of (n, n)-threshold access structures. Then, in Chapter 8, we consider VSS schemes for plural secret images. In this chapter, security conditions are carefully defined for such VSS schemes, and we show how to construct VSS schemes satisfying the security conditions.

Finally, the summaries of obtained results and future works of Parts I and II will be given in Chapters 5 and 9, respectively.

1.6 Notation

In this thesis, we use the following notation.

- X: A random variable. Random variables are usually represented by upper-case italic letters in this thesis.
- $\mathbb{F}_X$: A finite field in which random variable X takes a value.
- x: An instance of X, i.e., $x \in \mathbb{F}_X$
- $P_X(x)$: Probability that X takes value $x \in \mathbb{F}_X$.
- $H(X)$: The Shannon entropy of X, which is defined by

$$H(X) \stackrel{\text{def}}{=} -\sum_{x \in \ X} P_X(x) \log P_X(x). \tag{1.1}$$

The base of logarithm is 2 in this thesis.

- $H(X|Y)$: The conditional entropy of X given Y, which is defined by

$$H(X|Y) \stackrel{\text{def}}{=} \sum_{y \in \ _Y} P_Y(y) H(X|Y=y)$$
$$= -\sum_{x \in \ _X} \sum_{y \in \ _Y} P_{XY}(x,y) \log P_{X|Y}(x|y). \tag{1.2}$$

- $I(X;Y)$: The mutual information between X and Y, which is defined by

$$I(X;Y) \stackrel{\text{def}}{=} H(X) - H(X|Y). \tag{1.3}$$

- $I(X;Y|Z)$: The conditional mutual information between X and Y given Z, which is defined by

$$I(X;Y|Z) \stackrel{\text{def}}{=} H(X|Z) - H(X|YZ). \tag{1.4}$$

- $\boldsymbol{X}$: A set. Sets are usually denoted by upper-case bold-faced letters.
- $\mathbb{F}$: A finite field in which set $\boldsymbol{X}$ takes values.
- $|\boldsymbol{X}|$: The cardinality of $\boldsymbol{X}$.
- $\overline{\boldsymbol{X}}$: The complement of $\boldsymbol{X}$.
- $\boldsymbol{X} - \boldsymbol{Y}$: The difference of sets $\boldsymbol{X}$ and $\boldsymbol{Y}$, i.e., $\boldsymbol{X} - \boldsymbol{Y} \stackrel{\text{def}}{=} \boldsymbol{X} \cap \overline{\boldsymbol{Y}}$.
- $\boldsymbol{X} \times \boldsymbol{Y}$: The Cartesian product of $\boldsymbol{X}$ and $\boldsymbol{Y}$, i.e., $(X,Y) \in \boldsymbol{X} \times \boldsymbol{Y}$ if $X \in \boldsymbol{X}$ and $Y \in \boldsymbol{Y}$.
- $\mathcal{X}$: A family of sets. Families are represented by upper-case script faced letters.
- $\boldsymbol{x}$: A vector. Vectors are usually represented by lower-case bold-faced letters.
- ${}^t\boldsymbol{x}$: Transpose of a vector $\boldsymbol{x}$.
- x: A color. We represent colors by lower-case san-serif faced letters. For example, red, green, blue, yellow, magenta, and cyan are expressed by r, g, b, y, m and c, respectively. Especially, black and white are expressed by $\mathsf{1}$ and $\mathsf{0}$, and a general color is represented by x.
- $\mathsf{x} \sqcup \mathsf{x}'$: The mixture of colors x and x'. As an example, $\mathsf{c} \sqcup \mathsf{y} = \mathsf{g}$, which means that the mixture of cyan and yellow is green.
- $A \odot B$: The concatenation of matrices A and B which have the same number of rows, e.g.,

$$\begin{bmatrix} \mathsf{0} & \mathsf{0} & \mathsf{0} \\ \mathsf{0} & \mathsf{0} & \mathsf{0} \\ \mathsf{0} & \mathsf{0} & \mathsf{0} \end{bmatrix} \odot \begin{bmatrix} \mathsf{1} & \mathsf{1} \\ \mathsf{1} & \mathsf{1} \\ \mathsf{1} & \mathsf{1} \end{bmatrix} = \begin{bmatrix} \mathsf{0} & \mathsf{0} & \mathsf{0} & \mathsf{1} & \mathsf{1} \\ \mathsf{0} & \mathsf{0} & \mathsf{0} & \mathsf{1} & \mathsf{1} \\ \mathsf{0} & \mathsf{0} & \mathsf{0} & \mathsf{1} & \mathsf{1} \end{bmatrix}. \tag{1.5}$$

Part I

Secret Sharing Schemes

Chapter 2

Introduction to Secret Sharing Schemes

2.1 Background and Motivations

A Secret Sharing (SS) scheme is a method to encrypt secret information S into n pieces called *shares* $V_1, V_2, \ldots, V_n$, each of which has no information of secret S, but S can be decrypted by collecting several shares. As we have described in Chapter 1, SS schemes are important techniques for secure data storages. The SS scheme originated by Shamir [99] and Blakley [8] is a (k, n)-threshold SS scheme, which means that any k out of n shares can decrypt secret S but any $k-1$ or less shares do not leak out any information of S. The (k, n)-threshold access structure can be generalized to so-called *general access structures* which consist of the families of *qualified sets* and *forbidden sets*. A qualified set is a set of shares that can decrypt secret S, but a forbidden set is a share set that does not leak out any information of S. In this thesis, we usually assume that every set of shares in 2 is specified with a qualified set or a forbidden set. We call such an access structure *complete*. However, in the case that n is large, it is cumbersome to specify an access structure completely, and hence, SS schemes with *incomplete* access structures may be considered in practical uses.

The information theoretic analysis of SS schemes was first studied by Karnin et al. [58]. They evaluate the efficiency of SS schemes by the entropy of each share. Furthermore, it is shown in [58] that $H(V_i) \geq H(S)$ must hold for the entropies of secret S and shares V_i, $i = 1, 2, \ldots, n$, in the case of (k, n)-threshold SS schemes. This means that the rate of each share, $\rho_i \stackrel{\text{def}}{=} H(V_i)/H(S)$, must be $\rho_i \geq 1$. This result is extended to SS schemes with general access structures in [24].

In case that some sets of shares are allowed to have intermediate properties between the qualified sets and forbidden sets, it is possible to decrease the entropy of each share $H(V_i)$ less than $H(S)$, i.e., $\rho_i < 1$, although the security is a little weakened. SS schemes which have the trade-off between security and coding efficiency is called *ramp* SS schemes, which are proposed independently by Blakley [9] and Yamamoto [118], [119]. To distinguish ordinal SS schemes from ramp SS schemes, ordinal SS schemes are called *perfect* SS schemes. Note that perfect SS schemes can be considered as special cases of ramp SS schemes. Although the ramp SS schemes proposed in [9], [118], [119] are threshold schemes, ramp SS schemes are also extended to have

general access structures in [71], [86], [88].

The perfect SS scheme attaining $H(S) = H(V_i)$ for all i is called *ideal*. There are many studies of the ideal perfect SS schemes [21], [38], [84], [85], [98], [112], some of which point out the correspondence between the access structures of ideal SS schemes and matroids. On the other hand, the access structures of non-ideal SS schemes are investigated in [15], [22], [24], [30], [70], [89], [114], [115]. Some examples of non-ideal SS schemes are first described in [24], and more general examples of non-ideal SS schemes are presented in [15]. But, their examples cannot include some non-ideal SS schemes, e.g., the case shown in [89] or [114], the former of which is constructed based on combinatorial methods. In other words, it is not known what kinds of access structures can be or cannot be realized as ideal perfect SS schemes.

In Chapter 3, we consider the coding rates of ramp SS schemes with general access structures from the viewpoint of ideal and non-ideal ramp SS schemes. Ideal ramp SS schemes are defined in [71] as extensions of ideal perfect SS schemes. But, we note from the lower bound of the coding rate derived in [88] that many ramp access structures cannot be realized as ideal ramp SS schemes. In other words, if we adopt the definition of ideal ramp SS schemes in [71], the considerations of ideal ramp SS schemes tell nothing about the coding rates of most ramp SS schemes. Hence, we introduce a notion of *well-realized* ramp SS schemes as other extensions of ideal perfect SS schemes, and we evaluate the coding rates of ramp SS schemes based on this new notion of well-realized ramp SS schemes as follows: First, we classify shares into three categories, *super-additive*, *additive*, and *sub-additive* shares. Depending on this classification, we show that the coding rates of sub-additive shares are larger than the ones of additive or super-additive shares, and therefore, ramp SS schemes with sub-additive shares cannot be well-realized. Next, by evaluating the lower bound of coding rate, we derive the condition that ramp access structures only with additive and sub-additive shares cannot be well-realized. The lower bound is an extension of the lower bound by Blundo et al. [15] for non-ideal perfect SS schemes. Furthermore, it is shown that it includes not only the lower bounds of coding rates in [88] as special cases, but also gives tighter bounds for some access structures. By using them, we can discriminate the ramp access structures that cannot be well-realized.

(k, n)-threshold SS schemes have been studied by many researchers for perfect SS schemes. But, there are only a few construction method that can be applied to general access structures. Most of them are modifications of a *monotone circuit construction* [4] or a *cumulative map* [47], which will be introduced in Sections 2.2.3.2 and 4.2, respectively. But, they are much inefficient, especially in the case that an access structure is close to a (k, n)-threshold access structure with $k \neq n$. Hence, the monotone circuit construction is extended to the so-called *decomposition construction* [16], [104], [116], which can be used to derive the optimal SS schemes for some special access structures. For instance, by the decomposition construction, we can derive the optimal SS scheme if the number of shares are less than four [105], [106], or if access structures can be represented by graphs with six vertices [113], [115]. However, the decomposition construction cannot generate an efficient SS scheme in the case that the decomposed SS schemes cannot be realized efficiently. Hence, this method is applied mainly to the access structures represented by graphs [16], [104].

In the case of ramp SS schemes for general access structures, construction methods are proposed only in [71], [103]. But, the construction method in [71] always gives that $H(V_i) \geq H(S)$, i.e., $\rho_i \geq 1$, which does not take advantage of ramp SS schemes to decrease coding rates. On the other hand, a construction method in [103] is much complicated since the construction is based on *monotone span programming*.

In Chapter 4, based on these backgrounds, we propose a simple but efficient construction method of SS schemes based on integer programming and a multiple assignment map, which is a generalized concept of the cumulative map. Our method can attain the *optimal* multiple assignment schemes, and hence, our method can always generate more efficient SS schemes than the cumulative map. Furthermore, our method can also be applied to incomplete and/or ramp access structures to derive the optimal multiple assignments. We show some examples that our method can attain more efficient coding rates than the cumulative map.

We note that there are many researches for SS schemes outside of the scope of this thesis. In the following, we summarize some of them.

The relations between SS schemes and error correcting codes are pointed out in [58], [76]. Especially it is shown in [58] that the substitution attack cannot be detected in ideal SS schemes. In the case of Shamir's threshold scheme [99], the secret leak out to a cheater if the cheater submits a false share and legitimate participants try to detect the cheater. Hence, in [110], a method is proposed to detect the cheater with high probability without leaking out the secret to the cheater. A *verifiable* SS scheme is a SS scheme that can verify whether every participant with a share in a qualified set decrypts the *same* secret, which is proposed first by Chor et al. [27] and there are many researches on these subjects [3], [37], [93]–[95].

SS schemes can be considered as extensions of Shannon's cipher communication system [100]. Based on such considerations, source coding problems for secret sharing communication systems are studied by Yamamoto [120], which can also be considered as more general settings of ramp SS schemes with two or three shares. Furthermore, SS communication systems with two discrete noisy channels [121] and with two Gaussian wiretap channels [122] are treated.

It is desirable to change a secret dynamically for the sake of security, and hence, a *dynamic* SS scheme is proposed by Laih et al. [73]. On the other hand, the SS schemes that can change shares dynamically without changing a secret is proposed by Herzberg et al. [40]. Furthermore, Blundo et al. treat the dynamic SS schemes that can change a secret and an access structure [11]. Their results include the SS schemes with *disenrollment* proposed by Blakley et al. [7], which can invalidate some shares when a secret is changed. These methods are called *pre-positioned* SS schemes since all the changes of secrets and access structures must be previously known and they must be encoded in pre-distributed shares in advance. In order to change a secret and an access structure, a common public message is sent to all the participants. On the other hand, a method is proposed in [90], [108] that SS schemes can change secrets and access structures even if they are not known previously. But, it is pointed out that such protocols are insecure [74].

A SS scheme with plural secrets, which is called *multi* SS scheme, is first proposed by Karnin-Greene-Hellman [58] and studied by Simmons [101]. This kind of SS schemes are related to ramp SS schemes and dynamic SS schemes, which are pointed out in [18] and [55], respectively.

Furthermore, the comparisons between SS schemes with plural secrets and with one secret are considered in [29], and ideal SS schemes with plural secrets are treated in [54].

A secret function sharing scheme, in which a secret is a function rather than a value, is proposed by Naor-Pinkas [80] as an extension of Shamir's threshold schemes. They also proposed an unconditionally secure 1-out-of-2 oblivious transfer based on the secret function sharing schemes. This method is extended to ramp secret function sharing schemes, which can be applied to a 1-out-of-ℓ oblivious transfer, by Kawamoto-Yamamoto [61].

Finally, we note that the decryption of Shamir's threshold scheme requires the identification information of each share. The *anonymous* SS schemes [20] is the threshold SS scheme that can decrypt the secret from k shares even if the ID information of shares are not known.

2.2 Basic Model of Secret Sharing Schemes

2.2.1 Access Structures

In the rest of this chapter, we describe basic models of SS schemes, according to [77], [91], [105].

Let $\boldsymbol{V} = \{V_1, V_2, \ldots, V_n\}$ be a set of shares, and denote by $2^{\boldsymbol{V}}$ the family of all subsets of $\boldsymbol{V}$. We represent the family of qualified sets that can decrypt secret information S and the family of forbidden sets that cannot gain any information of S by $\mathcal{A}_1$ and $\mathcal{A}_0$, respectively. $\Gamma = \{\mathcal{A}_1, \mathcal{A}_0\}$ is called an *access structure*. If the access structure satisfies (2.1) and (2.2), then it is called a (k, n)-threshold SS scheme.

$$\mathcal{A}_1 = \{\boldsymbol{A} \in 2^{\boldsymbol{V}} : k \leq |\boldsymbol{A}| \leq n\}, \tag{2.1}$$

$$\mathcal{A}_0 = \{\boldsymbol{A} \in 2^{\boldsymbol{V}} : 0 \leq |\boldsymbol{A}| \leq k-1\}. \tag{2.2}$$

In SS schemes, it obviously holds that $\mathcal{A}_1 \cap \mathcal{A}_0 = \emptyset$. If it also holds that $\mathcal{A}_1 \cup \mathcal{A}_0 = 2^{\boldsymbol{V}}$, the access structure is called *complete*. Note that any access structure must satisfy the following *monotonicity*.

$$\boldsymbol{A} \in \mathcal{A}_1 \Rightarrow \boldsymbol{A}' \in \mathcal{A}_1 \text{ for all } \boldsymbol{A}' \supseteq \boldsymbol{A} \tag{2.3}$$

$$\boldsymbol{A} \in \mathcal{A}_0 \Rightarrow \boldsymbol{A}' \in \mathcal{A}_0 \text{ for all } \boldsymbol{A}' \subseteq \boldsymbol{A} \tag{2.4}$$

Therefore, we can define the family of *minimal* qualified sets and the family of *maximal* forbidden sets as follows:

$$\mathcal{A}_1^- = \{\boldsymbol{A} \in \mathcal{A}_1 : \boldsymbol{A} - \{V\} \notin \mathcal{A}_1 \text{ for any } V \in \boldsymbol{A}\}, \tag{2.5}$$

$$\mathcal{A}_0^+ = \{\boldsymbol{A} \in \mathcal{A}_0 : \boldsymbol{A} \cup \{V\} \notin \mathcal{A}_0 \text{ for any } V \in \boldsymbol{V} - \boldsymbol{A}\}. \tag{2.6}$$

Note that the complete access structure can be determined from the minimal qualified set $\mathcal{A}_1^-$ or the maximal forbidden set $\mathcal{A}_0^+$ from the monotonicity in (2.3) and (2.4) and the definition of completeness, i.e., $\mathcal{A}_1 \cup \mathcal{A}_0 = 2^{\boldsymbol{V}}$.

Definition 2.1 For a given access structure $\Gamma = \{\mathcal{A}_1, \mathcal{A}_0\}$, we call $V \in \boldsymbol{V}$ a *significant* share if there exists a share set $\boldsymbol{A} \in 2 \quad$ such that $\boldsymbol{A} \cup \{V\} \in \mathcal{A}_1$ but $\boldsymbol{A} \in \mathcal{A}_0$. A non-significant share is called a *vacuous* share. □

Example 2.2 Consider the following minimal qualified sets $\mathcal{A}_1^-$ with four shares $\boldsymbol{V} = \{V_1, V_2, V_3, V_4\}$.

$$\mathcal{A}_1^- = \{\{V_1, V_2\}, \{V_1, V_3\}, \{V_1, V_4\}, \{V_2, V_3\}, \{V_2, V_4\}\}. \tag{2.7}$$

From the monotonicity in (2.3), the qualified set $\mathcal{A}_1$ becomes

$$\begin{aligned}\mathcal{A}_1 = \{&\{V_1, V_2, V_3, V_4\}, \{V_1, V_2, V_3\}, \{V_1, V_2, V_4\}\{V_2, V_3, V_4\}, \{V_2, V_3, V_4\},\\ &\{V_1, V_2\}, \{V_1, V_3\}, \{V_1, V_4\}, \{V_2, V_3\}, \{V_2, V_4\}\}.\end{aligned} \tag{2.8}$$

Since we assume that the access structure is complete, the family of forbidden sets are obtained by $\mathcal{A}_0 = 2 \quad - \mathcal{A}_1$ as follows.

$$\mathcal{A}_0 = \{\{V_3, V_4\}, \{V_1\}, \{V_2\}, \{V_3\}, \{V_4\}, \emptyset\}. \tag{2.9}$$

From the monotonicity in (2.4), (2.9) is equivalent to

$$\mathcal{A}_0^+ = \{\{V_3, V_4\}, \{V_1\}, \{V_2\}\}. \tag{2.10}$$

□

For simplicity, we define the access structures of SS schemes by $\mathcal{A}_1^-$ and/or $\mathcal{A}_0^+$ instead of $\Gamma = \{\mathcal{A}_1, \mathcal{A}_0\}$ in the following sections. Furthermore, we omit the empty set $\emptyset$ from the forbidden sets since it is obvious that $\emptyset \in \mathcal{A}_0$.

2.2.2 Definitions of Secret Sharing Schemes

In this section, we define SS schemes for general access structures. We assume that secret S and each share V_i are random variables, which take values in finite fields $\mathbb{F}_S$ and $\mathbb{F}_{V_i}$, respectively. Then, a set $\boldsymbol{A} = \{V_{i_1}, V_{i_2}, \ldots, V_{i_u}\} (\subseteq \boldsymbol{V})$ takes values in $\mathbb{F} \stackrel{\text{def}}{=} \mathbb{F}_{V_{i_1}} \times \mathbb{F}_{V_{i_2}} \times \cdots \times \mathbb{F}_{V_{i_u}}$.

In the case that $\boldsymbol{A} \subseteq \boldsymbol{V}$ is a qualified set, S is uniquely determined from $\boldsymbol{A}$. Hence, we have $H(S|\boldsymbol{A}) = 0$, where $H(S|\boldsymbol{A})$ is the conditional entropy defined by (1.2).

On the other hand, in the case that $\boldsymbol{A} \subseteq \boldsymbol{V}$ is a forbidden set, S must be independent from $\boldsymbol{A}$. Letting $P_S \quad$ be the joint probability distribution of $(S, \boldsymbol{A})$, it must hold that

$$P_{S|} \quad (s|\boldsymbol{a}) = P_S(s) \tag{2.11}$$

for any $s \in \mathbb{F}_S$ and $\boldsymbol{a} \in \mathbb{F} \quad$. If we represent the independence by the entropy functions, we have $H(S|\boldsymbol{A}) = H(S)$ where $H(S)$ is the entropy defined by (1.1). Therefore, SS schemes can be defined as follows.

Definition 2.3 Let $\Gamma = \{\mathcal{A}_1, \mathcal{A}_0\}$ be a given access structure with $\boldsymbol{V} = \{V_1, V_2, \ldots, V_n\}$. Then, $\{\Gamma, \boldsymbol{V}, S\}$ is called a *secret sharing* (SS) scheme if it satisfies

$$H(S|\boldsymbol{A}) = 0 \qquad \text{for any } \boldsymbol{A} \in \mathcal{A}_1, \tag{2.12}$$
$$H(S|\boldsymbol{A}) = H(S) \quad \text{for any } \boldsymbol{A} \in \mathcal{A}_0. \tag{2.13}$$

□

In the case of (k, n)-threshold SS schemes, (2.12) and (2.13) become

$$H(S|\boldsymbol{A}) = H(S) \quad \text{for any } 0 \le |\boldsymbol{A}| \le k-1, \tag{2.14}$$
$$H(S|\boldsymbol{A}) = 0 \qquad \text{for any } k \le |\boldsymbol{A}| \le n. \tag{2.15}$$

For any SS scheme, the following theorem holds.

Theorem 2.4 (Karnin et al. [58], Capocelli et al. [24]) Let $\Gamma = \{\mathcal{A}_1, \mathcal{A}_0\}$ be a given access structure with shares $\boldsymbol{V} = \{V_1, V_2, \ldots, V_n\}$. Then, it holds for every significant share V_i that

$$H(V_i) \ge H(S). \tag{2.16}$$

□

Note that Theorem 2.4 is proved for any general access structures [24] in addition to (k, n) threshold access structures [58]. The proof of Theorem 2.4 is omitted since it will be given in Chapter 3 as a special case of ramp SS schemes. The SS scheme attaining $H(S) = H(V_i)$ for all $i = 1, 2, \ldots, n$ is called *ideal*.

Next, we consider what kind of S can be realized as an ideal SS scheme.

Theorem 2.5 (Blundo et al. [19]) Let $\{\Gamma, \boldsymbol{V}, S\}$ be a SS scheme with a secret S. Then, for any other secret S' such that $\mathbb{F}_{S'} = \mathbb{F}_S$ and $P_S(s) > 0$, $P_{S'}(s) > 0$ for all $s \in \mathbb{F}_S$, a SS scheme $\{\Gamma, \boldsymbol{V}, S'\}$ can be constructed from the SS scheme $\{\Gamma, \boldsymbol{V}, S\}$ without changing the entropy of every $\boldsymbol{A} \in \mathcal{A}_0$. □

Now, consider the case that S' is uniformly distributed on $\mathbb{F}_S$. Then, from Theorems 2.4 and 2.5, it must hold for any significant share V_i that $H(V_i) \ge \log |\mathbb{F}_S|$ since we have $H(V_i) \ge H(S') = \log |\mathbb{F}_{S'}| = \log |\mathbb{F}_S|$. Hence, the following theorem holds.

Theorem 2.6 (Blundo et al. [19]) Let $\Gamma = \{\mathcal{A}_1, \mathcal{A}_0\}$ be a given access structure with shares $\boldsymbol{V} = \{V_1, V_2, \ldots, V_n\}$. Then, it must hold for each significant share V_i that

$$H(V_i) \ge \log |\mathbb{F}_S|. \tag{2.17}$$

□

Note that any ideal SS scheme must satisfy $H(V_i) = H(S) \leq \log |\mathbb{F}_S|$ for all i, where the last inequality holds with equality if and only if P_S is an uniformly distribution. Hence, from (2.17), an ideal SS scheme can be constructed only when S is uniformly distributed on $\mathbb{F}_S$.[1]

It is also known that in the case of (k, n)-threshold SS schemes, an ideal SS scheme can easily be constructed for any k and n [99], which will be shown in the next section. Now, let us define the coding rate of a share V_i as $\rho_i \stackrel{\text{def}}{=} H(V_i)/H(S)$, for $i = 1, 2, \ldots, n$. Since each ρ_i may be different in the case of general access structures, it is cumbersome to treat every ρ_i independently in the case that n is large. Hence, we consider only the following *average* coding rate $\tilde{\rho}$ and *worst* coding rate ρ^* in this thesis.

$$\tilde{\rho} \stackrel{\text{def}}{=} \frac{1}{n} \sum_{i=1}^{n} \rho_i, \tag{2.18}$$

$$\rho^* \stackrel{\text{def}}{=} \max_{1 \leq i \leq n} \rho_i. \tag{2.19}$$

Note that if $\rho_i = 1$ for all i, the SS scheme is ideal. Since $\rho_i \geq 1$, $i = 1, 2, \ldots, n$, must hold for any access structures from Theorem 2.4, $\tilde{\rho} = 1$ or $\rho^* = 1$ are the necessary and sufficient conditions for a SS scheme to be ideal [24], [58].

Remark 2.7 Note that a vacuous share, i.e., a non-significant share, plays no roll in SS schemes, and hence, $\rho_i = 0$ can always be attained for every vacuous share V_i in any access structure Γ. Furthermore, if there exists a vacuous share V_i with $\rho_i > 0$, the average coding rate can be reduced by letting $\rho_i = 0$ without changing the rates of significant shares. Hence, in this thesis, we assume that every share in SS schemes is significant. □

2.2.3 Examples of Secret Sharing Schemes

In this section, we introduce two kinds of SS schemes proposed by Shamir [99] and Benaloh-Leichter [4].

2.2.3.1 Shamir's Threshold Schemes

Shamir's threshold scheme is an ideal (k, n)-threshold SS scheme, which is constructed by the following procedures.

Construction 2.8 (Shamir [99]) For a given secret $S \in \mathbb{F}_S$, let $R_1, R_2 \ldots, R_{k-1}$ be independent uniform random numbers on $\mathbb{F}_S$. Then, the i-th share V_i is constructed by $V_i = f(i)$, where $f(x)$ is the following polynomial of degree $k - 1$ on $\mathbb{F}_S$.

$$f(x) = S + R_1 x^1 + R_2 x^2 + \cdots + R_{k-1} x^{k-1}. \tag{2.20}$$

In this case, it holds that $\mathbb{F}_{V_1} = \mathbb{F}_{V_2} = \cdots = \mathbb{F}_{V_n} = \mathbb{F}_S$. □

[1] Note that Theorems 2.4–2.6 also hold in quantum settings, which is proved in [87].

Next, we check that the share set $\boldsymbol{V}$ obtained by Construction 2.8 satisfies Definition 2.3. Now, we assume that S is uniformly distributed on $\mathbb{F}_S$, i.e., $H(S) = \log|\mathbb{F}_S|$. Then, for any share set $\boldsymbol{A} = \{V_{i_1}, V_{i_2}, \ldots, V_{i_q}\}$, we have the following relation.

$$\begin{bmatrix} f(0) \\ f(i_1) \\ f(i_2) \\ \vdots \\ f(i_q) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & i_1 & i_1^2 & \cdots & i_1^{k-1} \\ 0 & i_2 & i_2^2 & \cdots & i_2^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & i_q & i_q^2 & \cdots & i_q^{k-1} \end{bmatrix} \begin{bmatrix} S \\ R_1 \\ R_2 \\ \vdots \\ R_{k-1} \end{bmatrix} \stackrel{\text{def}}{=} \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & M & \\ 0 & & & \end{bmatrix} \begin{bmatrix} S \\ R_1 \\ R_2 \\ \vdots \\ R_{k-1} \end{bmatrix}. \quad (2.21)$$

In the case of $q = k$, the matrix M is the so-called Vandermond matrix, which has the determinant

$$\det M = \prod_{1 \le u < v \le k} (i_v - i_u). \quad (2.22)$$

Note that $\det M \neq 0$ holds since $i_u \neq i_v$ for any $u \neq v$. Hence, S and $R_1, R_2, \ldots, R_{k-1}$ can be determined uniquely from $f(i_1), f(i_2), \ldots, f(i_k)$ by solving (2.21).

We also note that the solution of (2.21) can be obtained by the polynomial interpolation. From k coordinates $(i_1, f(i_1)), (i_2, f(i_2)), \ldots, (i_k, f(i_k))$, $f(x)$ can be constructed as

$$f(x) = \sum_{u=1}^{k} f(i_u) \prod_{\substack{v=1 \\ v \neq u}}^{k} \frac{x - i_v}{i_u - i_v}. \quad (2.23)$$

Hence, S is obtained by $S = f(0)$, i.e.,

$$S = \sum_{u=1}^{k} f(i_u) \prod_{\substack{v=1 \\ v \neq u}}^{k} \frac{i_v}{i_v - i_u}. \quad (2.24)$$

On the other hand, in the case of $q \le k-1$, we have the following relation.

$$\begin{aligned} H(S|\boldsymbol{A}) &= H(S\boldsymbol{A}) - H(\boldsymbol{A}) \\ &\stackrel{\text{(a)}}{=} H(SR_1R_2\cdots R_{k-1}) - H(\boldsymbol{A}) \\ &\stackrel{\text{(b)}}{=} H(S) + H(R_1) + H(R_2) + \cdots + H(R_{k-1}) - H(\boldsymbol{A}) \\ &= k\log|\mathbb{F}_S| - H(\boldsymbol{A}) \\ &\stackrel{\text{(c)}}{\ge} k\log|\mathbb{F}_S| - (k-1)\log|\mathbb{F}_S| \\ &= \log|\mathbb{F}_S| = H(S), \end{aligned} \quad (2.25)$$

where (a)(b)(c) hold because of the following reasons.

(a): $S\boldsymbol{A}$ and $(S, R_1, R_2, \ldots, R_{k-1})$ has one to one correspondence from (2.21).

(b): $S, R_1, R_2, \ldots, R_{k-1}$ are mutually independent.

(c): $H(\boldsymbol{A}) \leq \log |\mathbb{F}_S|^{k-1}$.

Since it always holds that $H(S) \geq H(S|\boldsymbol{A})$, we have $H(S|\boldsymbol{A}) = H(S)$. Therefore, any share set $\boldsymbol{V}$ obtained by Construction 2.8 satisfies Definition 2.3. Finally, in the case that S is uniformly distributed, Shamir's threshold scheme is an ideal SS scheme since it holds that $H(V_i) = |\mathbb{F}_{V_i}| = |\mathbb{F}_S| = H(S)$ for all i.

Example 2.9 Let us consider a $(3, 4)$-threshold SS scheme over GF(17) with $S = 10$. If $R_1 = 5$ and $R_2 = 7$, the polynomial of degree 2 becomes

$$f(x) = 10 + 5x + 7x^2. \tag{2.26}$$

Then, we have shares $V_1 = 5$, $V_2 = 14$, $V_3 = 3$, and $V_4 = 6$. From (2.24), it is easy to check that any three out of four shares can decrypt secret S. As an example, from V_1, V_2, and V_4, we can calculate secret S as follows.

$$S = 5\frac{2}{2-1}\frac{4}{4-1} + 14\frac{1}{1-2}\frac{4}{4-2} + 6\frac{1}{1-4}\frac{2}{2-4} = 2 + 6 + 2 = 10. \tag{2.27}$$

□

2.2.3.2 Monotone Circuit Construction

A *monotone circuit construction* is a construction method of SS schemes for general access structures, which uses (t, t)-threshold SS schemes.

Construction 2.10 (Benaloh-Leichter, [4]) Consider a SS scheme for a secret S with a given general access structure $\Gamma = \{\mathcal{A}_1, \mathcal{A}_0\}$ where $\mathcal{A}_1^- \stackrel{\text{def}}{=} \{\boldsymbol{A}_1, \boldsymbol{A}_2, \ldots, \boldsymbol{A}_q\}$. For $\boldsymbol{A}_j = \{V_{i_1}, V_{i_2}, \ldots, V_{i_{|\ j|}}\}$, $j = 1, 2, \ldots, q$, let $\boldsymbol{W}^{\ j} \stackrel{\text{def}}{=} \left\{W_{i_1}{}^{j}, W_{i_2}{}^{j}, \ldots, W_{i_{|\ j|}}{}^{j}\right\}$ be the share set of an $(|\boldsymbol{A}_j|, |\boldsymbol{A}_j|)$-threshold SS scheme with secret S, and let $Z_i{}^{j}$ be defined by

$$Z_i{}^{j} = \begin{cases} \left\{W_i{}^{j}\right\} & \text{if} \quad V_i \in \boldsymbol{A}_j \\ \emptyset & \text{if} \quad V_i \notin \boldsymbol{A}_j. \end{cases} \tag{2.28}$$

Then, each share for access structure Γ is given by

$$V_i = \bigcup_{j=1}^{q} Z_i{}^{j}. \tag{2.29}$$

□

It can be checked by the next example that the share set $\boldsymbol{V}$ obtained by Construction 2.10 satisfies Definition 2.3.

Example 2.11 Let us consider a SS scheme for a secret S with the access structure given by (2.8) and (2.9) in Example 2.2. From (2.7), we have that $\boldsymbol{A}_1 = \{V_1, V_2\}$, $\boldsymbol{A}_2 = \{V_1, V_3\}$, $\boldsymbol{A}_3 = \{V_1, V_4\}$, $\boldsymbol{A}_4 = \{V_2, V_3\}$, and $\boldsymbol{A}_5 = \{V_2, V_4\}$. Since it holds that $|\boldsymbol{A}_i| = 2$ for all i, we first construct $(2, 2)$-threshold SS schemes for secret S as follows.

$$\boldsymbol{W}^{\,1} = \left\{W_1^{\,1}, W_2^{\,1}\right\} = \{R_1, S - R_1\}, \tag{2.30}$$
$$\boldsymbol{W}^{\,2} = \left\{W_1^{\,2}, W_3^{\,2}\right\} = \{R_2, S - R_2\}, \tag{2.31}$$
$$\boldsymbol{W}^{\,3} = \left\{W_1^{\,3}, W_4^{\,3}\right\} = \{R_3, S - R_3\}, \tag{2.32}$$
$$\boldsymbol{W}^{\,4} = \left\{W_2^{\,4}, W_3^{\,4}\right\} = \{R_4, S - R_4\}, \tag{2.33}$$
$$\boldsymbol{W}^{\,5} = \left\{W_2^{\,5}, W_4^{\,5}\right\} = \{R_5, S - R_5\}, \tag{2.34}$$

where $R_1, R_2, \ldots, R_5$ are uniform random numbers on $\mathbb{F}_S$. From (2.28) and (2.29), the set of shares are determined as follows.

$$V_1 = \left\{W_1^{\,1}, W_1^{\,2}, W_1^{\,3}\right\} = \{R_1, R_2, R_3\}, \tag{2.35}$$
$$V_2 = \left\{W_2^{\,1}, W_2^{\,4}, W_2^{\,5}\right\} = \{S - R_1, R_4, R_5\}, \tag{2.36}$$
$$V_3 = \left\{W_3^{\,2}, W_3^{\,4}\right\} = \{S - R_2, S - R_4\}, \tag{2.37}$$
$$V_4 = \left\{W_4^{\,3}, W_4^{\,5}\right\} = \{R_3, S - R_5\}. \tag{2.38}$$

It can easily be checked that (2.35)–(2.38) satisfy Definition 2.3. This construction method is not ideal since it holds that $\rho_1 = \rho_2 = 3$, $\rho_3 = \rho_4 = 2$, i.e., $\tilde{\rho} = \frac{5}{2}$, and $\rho^* = 3$. □

Remark 2.12 Construction 2.10, which is proposed originally in [4], is called the monotone circuit construction because this method it is based on monotone boolean circuits as follows.

First, consider a binary representation $\{v_1, v_2, \ldots, v_n\} \in \{0, 1\}^n$ for a share set $\boldsymbol{A} \subseteq \boldsymbol{V}$ defined by

$$v_i = \begin{cases} 1 & \text{if } V_i \in \boldsymbol{A} \\ 0 & \text{if } V_i \notin \boldsymbol{A}. \end{cases} \tag{2.39}$$

Then, let $\mathbf{C}(v_1, v_2, \ldots, v_n)$ be a boolean function such that its output does not change from 1 to 0 even if any input v_i changes from 0 to 1. Such a boolean circuit is called a monotone boolean circuit. Note that, from the monotonicity of access structures in (2.3), we can construct a monotone boolean function such that the output is 1 if and only if all the inputs corresponding to a qualified set are 1.

One realization of such a monotone boolean circuit is given by the following disjunctive normal boolean formula,

$$\mathbf{C}(v_1, v_2, \ldots, v_n) = \bigvee_{\in \mathcal{A}_1^-} \left[\bigwedge_{V_i \in} v_i \right], \tag{2.40}$$

where disjunction $\vee$ and conjunction $\wedge$ are "and" and "or" gates, respectively. In Construction 2.10, $\left[\bigvee_{V_i \in} v_i\right]$ corresponds to the decoding of the $(|\boldsymbol{A}|, |\boldsymbol{A}|)$-threshold SS scheme. See [4] for more details. □

Chapter 3

Evaluations of Coding Rates in Secret Shairng Schemes

3.1 Introduction

In a SS scheme, as shown in Theorem 2.4, the coding rate ρ_i must satisfy that $\rho_i \geq 1$ for each significant share V_i, and the SS scheme is called *ideal* if it holds that $\rho_i = 1$ for any i. Note that, in SS schemes introduced in Chapter 2, we assume that every subset $\boldsymbol{A} \in 2$ is either a qualified set or a forbidden set. But, in the case of ramp access structures such that some subsets of $\boldsymbol{V}$ are allowed to have intermediate properties between the qualified and forbidden properties, it is possible to decrease the coding rate ρ_i less than 1. The SS schemes having ramp access structure are called *ramp* SS schemes [9], [119].

For example, in (k, L, n)-ramp SS schemes [9], [119], secret information S can be decrypted completely from any k out of n shares, while no information of S can be obtained from $k - L$ or less shares. Furthermore, the information of S leaks out from arbitrary $k - j$ $(1 \leq j \leq L - 1)$ out of n shares with the amount of $\frac{j}{L}H(S)$. It is known that arbitrary (k, L, n)-ramp SS schemes must satisfy that $H(V_i) \geq \frac{H(S)}{L}$ for all $i = 1, 2, \ldots, n$, and how to construct (k, L, n)-ramp SS schemes attaining the equality [119]. Therefore, ramp SS schemes can achieve efficient coding rate at a little sacrifice of security. Ramp SS schemes for general access structures are discussed in [71], [86], [88]. In the case of $L = 1$, ramp SS scheme coincides with ordinal SS schemes, and hence, ramp SS schemes are extensions of ordinal SS schemes. To distinguish ordinal SS schemes from ramp SS schemes with $L \geq 2$, we call the access structure of ordinal SS schemes *perfect*.

In this chapter, we consider the coding rates of ramp SS schemes for general access structures. First, we point out that there may exist non-significant shares in ramp SS schemes, and we classify shares into three categories as *super-additive, additive,* and *sub-additive*. Then, we show that the lower bound of coding rate must be different depending on the categories. Based on these arguments, we define *well-realized* ramp SS schemes as extensions of ideal perfect SS schemes, which were defined in [71], and we analyze what kind of ramp SS schemes cannot be well-realized. In perfect SS schemes, it is known that some access structures cannot become

ideal [22], [24], [30]. Especially in [15], general access structures for non-ideal SS schemes are represented, which includes the results of [22], [24], [30] as special cases. In this chapter, we clarify the general access structures of ramp SS schemes that cannot be well-realized. The result can be considered as an extension of the result in [15]. We note our result also include the examples of ramp SS schemes that are not well-realized in [88] as special cases.

This chapter is organized as follows: In the next section, we define ramp SS schemes for general access structures. In Section 3.3.1, we point out that there may exist non-significant shares in ramp SS schemes and we classify the shares of ramp SS schemes into three categories. Furthermore, we show that the lower bound of each share depends on the category of shares, and we define well-realized ramp SS schemes as extensions of deal SS schemes defined in Section 2.2.2. Section 3.3.2 is devoted to give the sufficient condition that ramp SS scheme is not well-realized, which is an extension of the result in [15]. Furthermore, we show that the ramp access structure satisfying such condition includes the examples of non-ideal ramp SS schemes in [88] as special cases. The contents of this chapter are appeared in [51].

3.2 Definition of Ramp Secret Sharing Schemes

In this section, we define ramp SS schemes based on [9], [71], [119] as an extension of SS schemes presented in Section 2.2.2.

Let $\boldsymbol{V}$ be the set of shares and denote by $2^{\boldsymbol{V}}$ all the subsets of $\boldsymbol{V}$. Suppose that $L+1$ families $\mathcal{A}_j \subseteq 2^{\boldsymbol{V}}$, $j = 0, 1, 2, \ldots, L$, satisfy the following.

$$H(S|\boldsymbol{A}) = \frac{L-j}{L} H(S), \quad \text{for any } \boldsymbol{A} \in \mathcal{A}_j \tag{3.1}$$

Equation (3.1) implies that secret S leaks out from any set $\boldsymbol{A} \in \mathcal{A}_j$ with the amount of $\frac{j}{L}H(S)$. Especially, S can be decrypted completely from any $\boldsymbol{A} \in \mathcal{A}_L$, and every $\boldsymbol{A} \in \mathcal{A}_0$ leaks out no information of S. Note that, in the case of $L = 1$, ramp SS scheme reduces to ordinal SS scheme defined in Section 2.2.2. To distinguish ordinal SS schemes from ramp schemes, ordinal SS schemes are called *perfect* SS schemes. We call $\Gamma^R = \{\mathcal{A}_0, \mathcal{A}_1, \ldots, \mathcal{A}_L\}$ the access structure of the ramp SS scheme with $L+1$ levels. Without loss of generality, we can assume that $\mathcal{A}_j \cap \mathcal{A}_{j'} = \emptyset$ for $j \neq j'$. Furthermore, the access structure Γ^R is called *complete* if Γ^R satisfies that $\bigcup_{j=0}^{L} \mathcal{A}_j = 2^{\boldsymbol{V}}$.

For example, the access structure of a (k, L, n)-threshold ramp SS scheme [9], [119] is defined as follows:

$$\mathcal{A}_0 = \{\boldsymbol{A} \in 2^{\boldsymbol{V}} : 0 \leq |\boldsymbol{A}| \leq k-L\}, \tag{3.2}$$

$$\mathcal{A}_j = \{\boldsymbol{A} \in 2^{\boldsymbol{V}} : |\boldsymbol{A}| = k-L+i\} \text{ for } 1 \leq j \leq L-1, \tag{3.3}$$

$$\mathcal{A}_L = \{\boldsymbol{A} \in 2^{\boldsymbol{V}} : k \leq |\boldsymbol{A}| \leq n\}. \tag{3.4}$$

Note that (k, L, n)-threshold ramp SS schemes can easily be constructed by modifying Shamir's threshold SS schemes in (2.20) in Construction 2.8 as follows.

$$f(x) = S_0 + S_1 x^1 + \cdots + S_{L-1} x^{L-1} + R_L x^L + R_{L+1} x^{L+1} + \cdots + R_{k-1} x^{k-1}, \tag{3.5}$$

where a secret is an L-tuple $\{S_0, S_1, \ldots, S_{L-1}\}$ and $R_L, R_{L+1}, \ldots, R_{k-1}$ are independent uniform random numbers. It is known that this construction can attain that $\rho_i = \frac{1}{L}$, $i = 1, 2, \ldots, n$, for any k, L and n.

Now, defining families $\check{\mathcal{A}}_j$ and $\hat{\mathcal{A}}_j$, $j = 0, 1, \ldots, L$, as

$$\check{\mathcal{A}}_j \stackrel{\text{def}}{=} \bigcup_{k=j}^{L} \mathcal{A}_k, \tag{3.6}$$

$$\hat{\mathcal{A}}_j \stackrel{\text{def}}{=} \bigcup_{k=1}^{j} \mathcal{A}_k, \tag{3.7}$$

the monotonicity of perfect SS schemes in (2.3) and (2.4) are extended as follows:

$$\boldsymbol{A} \in \check{\mathcal{A}}_j \;\Rightarrow\; \boldsymbol{A}' \in \check{\mathcal{A}}_j \text{ for all } \boldsymbol{A}' \supseteq \boldsymbol{A} \tag{3.8}$$

$$\boldsymbol{A} \in \hat{\mathcal{A}}_j \;\Rightarrow\; \boldsymbol{A}' \in \hat{\mathcal{A}}_j \text{ for all } \boldsymbol{A}' \subseteq \boldsymbol{A} \tag{3.9}$$

Therefore, the minimal and the maximal families of an access structure denoted by $\Gamma^{R-} = \{\mathcal{A}_0^-, \mathcal{A}_1^-, \ldots, \mathcal{A}_L^-\}$ and $\Gamma^{R+} = \{\mathcal{A}_0^+, \mathcal{A}_1^+, \ldots, \mathcal{A}_L^+\}$, respectively, can be defined as

$$\mathcal{A}_j^- = \{\boldsymbol{A} \in \mathcal{A}_j : \boldsymbol{A} - \{V\} \notin \check{\mathcal{A}}_j \text{ for any } V \in \boldsymbol{A}\}, \tag{3.10}$$

$$\mathcal{A}_j^+ = \{\boldsymbol{A} \in \mathcal{A}_j : \boldsymbol{A} \cup \{V\} \notin \hat{\mathcal{A}}_j \text{ for any } V \in 2^{} - \boldsymbol{A}\}. \tag{3.11}$$

The coding rates ρ_i, $i = 1, 2, \ldots, n$, the average coding rate $\tilde{\rho}$, and the worst coding rate ρ^* can also be defined in the same way as perfect SS schemes in (2.18) and (2.19).

From the above considerations, we can define the set function $\ell : 2^{} \to \{0, 1, \ldots, L\}$ that gives the level of $\boldsymbol{A} \in 2^{}$, i.e., if $\boldsymbol{A} \in \mathcal{A}_j$, then $\ell(\boldsymbol{A}) = j$. Clearly, it holds that $\ell(\emptyset) = 0$ and $\ell(\boldsymbol{V}) = L$. From the monotonicity defined by (3.8), it also holds that

$$\ell(\boldsymbol{A}) \le \ell(\boldsymbol{B}), \tag{3.12}$$

for any share sets $\boldsymbol{A}$ and $\boldsymbol{B}$ satisfying $\boldsymbol{A} \subseteq \boldsymbol{B}$. Furthermore, we have from (3.1) that

$$H(S|\boldsymbol{A}) = \left(1 - \frac{\ell(\boldsymbol{A})}{L}\right) H(S). \tag{3.13}$$

3.3 Lower Bounds of Coding Rates in Secret Sharing Schemes

In this section, we consider the lower bound of coding rate ρ_i in ramp SS schemes. First, we define a *well-realized* ramp SS scheme as an extension of an ideal perfect SS scheme. Then, we discuss what kind of ramp access structures cannot be well-realized.

3.3.1 Well-realized Ramp Secret Sharing Schemes

The following lemma holds for ramp SS schemes.

Lemma 3.1 Let Γ^R be an access structure with $L+1$ levels. Then, for share sets $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C} \subseteq \boldsymbol{V}$, it holds that

$$I(\boldsymbol{A}; \boldsymbol{B}; S|\boldsymbol{C}) = \frac{\ell(\boldsymbol{AC}) + \ell(\boldsymbol{BC}) - \{\ell(\boldsymbol{ABC}) + \ell(\boldsymbol{C})\}}{L} H(S), \tag{3.14}$$

where $I(\boldsymbol{A}; \boldsymbol{B}; S|\boldsymbol{C})$ is defined by $I(\boldsymbol{A}; \boldsymbol{B}; S|\boldsymbol{C}) \stackrel{\text{def}}{=} I(\boldsymbol{A}; \boldsymbol{B}|\boldsymbol{C}) - I(\boldsymbol{A}; \boldsymbol{B}|S\boldsymbol{C})$ and the conditional mutual information $I(X; Y|Z)$ is defined by (1.4).[1] □

Remark 3.2 The left hand side of (3.14) can be considered as the information commonly contained in random variables $\boldsymbol{A}, \boldsymbol{B}$ and S with given $\boldsymbol{C}$, intuitively. However, we note that $I(X; Y; Z|W)$ may be negative although the conditional mutual information $I(X; Y|Z)$ is always non-negative [124]. We also note that $I(X; Y; Z|W)$ takes the same value for any permutation of X, Y, Z, e.g., $I(X; Y; Z|W) = I(Z; Y; X|W)$. □

Proof of Lemma 3.1

$$\begin{aligned} I(\boldsymbol{A}; \boldsymbol{B}; S|\boldsymbol{C}) &= I(S; \boldsymbol{A}; \boldsymbol{B}|\boldsymbol{C}) = I(S; \boldsymbol{A}|\boldsymbol{C}) - I(S; \boldsymbol{A}|\boldsymbol{BC}) \\ &= H(S|\boldsymbol{C}) - H(S|\boldsymbol{AC}) - \{H(S|\boldsymbol{BC}) - H(S|\boldsymbol{ABC})\} \\ &= \frac{\ell(\boldsymbol{AC}) + \ell(\boldsymbol{BC}) - \{\ell(\boldsymbol{ABC}) + \ell(\boldsymbol{C})\}}{L} H(S), \end{aligned} \tag{3.15}$$

where the last equality follows from (3.13). □

From the definition of $I(\boldsymbol{A}; \boldsymbol{B}; S|\boldsymbol{C})$, (3.14) can be transformed into

$$I(\boldsymbol{A}; \boldsymbol{B}|\boldsymbol{C}) = I(\boldsymbol{A}; \boldsymbol{B}|\boldsymbol{C}S) + \frac{\ell(\boldsymbol{AC}) + \ell(\boldsymbol{BC}) - \{\ell(\boldsymbol{ABC}) + \ell(\boldsymbol{C})\}}{L} H(S). \tag{3.16}$$

Hence, the following theorem by Dijk can easily be obtained by letting $L = 1$ in (3.16).

Corollary 3.3 (Dijk [115, Theorem 2.1.5]) Let Γ be an access structure for a perfect SS scheme. Then, for share sets $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C} \subseteq \boldsymbol{V}$, it holds that

$$I(\boldsymbol{A}; \boldsymbol{B}|S\boldsymbol{C}) = \begin{cases} I(\boldsymbol{A}; \boldsymbol{B}|\boldsymbol{C}) - H(S) & \text{if } \boldsymbol{AC}, \boldsymbol{BC} \in \mathcal{A}_1 \text{ and } \boldsymbol{C} \in \mathcal{A}_0, \\ I(\boldsymbol{A}; \boldsymbol{B}|\boldsymbol{C}) + H(S) & \text{if } \boldsymbol{AC}, \boldsymbol{BC} \in \mathcal{A}_0 \text{ and } \boldsymbol{ABC} \in \mathcal{A}_1, \\ I(\boldsymbol{A}; \boldsymbol{B}|\boldsymbol{C}) & \text{otherwise.} \end{cases} \tag{3.17}$$

□

Note that the proof of Lemma 3.1 is simpler than Dijk's proof. Furthermore, the next corollary holds by letting $\boldsymbol{C} = \emptyset$ in (3.16).

Corollary 3.4 For any access structure Γ^R with $L+1$ levels, it holds that

$$I(\boldsymbol{A}; \boldsymbol{B}) = I(\boldsymbol{A}; \boldsymbol{B}|S) + \frac{\ell(\boldsymbol{A}) + \ell(\boldsymbol{B}) - \ell(\boldsymbol{AB})}{L} H(S) \tag{3.18}$$

for any $\boldsymbol{A}, \boldsymbol{B} \subseteq \boldsymbol{V}$. □

[1] For simplicity of notion, we use $\boldsymbol{AB}$ to represent the union of sets $\boldsymbol{A}$ and $\boldsymbol{B}$, i.e., $\boldsymbol{AB} \stackrel{\text{def}}{=} \boldsymbol{A} \cup \boldsymbol{B}$.

Letting $\boldsymbol{B} = \{V_i\} \subseteq \boldsymbol{V}$ in (3.18), we have

$$\frac{\ell(\boldsymbol{A}\{V_i\}) - \ell(\boldsymbol{A}) - \ell(\{V_i\})}{L} H(S) = -I(\boldsymbol{A}; V_i; S). \tag{3.19}$$

The left hand side of (3.19) represents how the security level changes when V_i cooperates with $\boldsymbol{A}$. Now, we classify each share according to the sign of the change.

Definition 3.5 In a ramp SS scheme for an access structure Γ^R with $L+1$ levels, if share $V_i \in \boldsymbol{V}$ satisfies

$$\max_{\subseteq\ -\{V_i\}} \{\ell(\boldsymbol{A}\{V_i\}) - \ell(\boldsymbol{A}) - \ell(\{V_i\})\} > 0, \tag{3.20}$$

$$\max_{\subseteq\ -\{V_i\}} \{\ell(\boldsymbol{A}\{V_i\}) - \ell(\boldsymbol{A}) - \ell(\{V_i\})\} = 0, \tag{3.21}$$

$$\max_{\subseteq\ -\{V_i\}} \{\ell(\boldsymbol{A}\{V_i\}) - \ell(\boldsymbol{A}) - \ell(\{V_i\})\} < 0, \tag{3.22}$$

then V_i is called *super-additive, additive, sub-additive*, respectively. If V_i is an additive share with $\ell(V_i) = 0$, then it is called a *vacuous* share. □

In the case that V_i is a super-additive share, there exists a share set $\boldsymbol{A}$ such that $\boldsymbol{A}$ and V_i can obtain more information of S if they cooperate with each other than they do not gather together. In the case of perfect SS schemes, i.e., $L = 1$, a super-additive share must satisfy that $\ell(\boldsymbol{A}\{V_i\}) = 1$ and $\ell(\boldsymbol{A}) = 0$ for some $\boldsymbol{A} \subseteq \boldsymbol{V}$. Hence, a super-additive share becomes a significant share in this case.

If an additive share V_i satisfies that $\ell(V_i) = 0$, V_i plays no roll, and hence, such V_i is called *vacuous*. However, in the case of additive share V_i with $\ell(V_i) > 0$, there exists a share set $\boldsymbol{A} \subseteq \boldsymbol{V} - \{V_i\}$ that has the supplementary information of V_i for S. For instance, let $S = \{S^{\langle 1\rangle}, S^{\langle 2\rangle}, \ldots, S^{\langle L\rangle}\}$ and $V_i = S^{\langle i\rangle}$, $i = 1, 2, \ldots, L$, be a secret and shares, respectively. Then, every share V_i, $i = 1, 2, \ldots, L$, is an additive share with $\ell(V_i) > 0$.

A sub-additive share may also occur in ramp SS schemes. From (3.22), sub-additive shares may contain the same information of S. As an example, letting $S = \{S^{\langle 1\rangle}, S^{\langle 2\rangle}, \ldots, S^{\langle L\rangle}\}$ be a secret, and $V_1 = S^{\langle 1\rangle}$, $V_i = \{S^{\langle 1\rangle}, S^{\langle i\rangle}\}$, $i = 2, 3, \ldots, L$, be shares, the share V_1 is sub-additive.

Note that in perfect SS schemes with no vacuous shares, there is no additive and sub-additive shares because each share $V \in \boldsymbol{V}$ must satisfy that $\ell(\{V\}) = 0$. In the case of ramp SS schemes, we also assume that no vacuous shares exist in the same way as perfect SS schemes, but non-vacuous additive shares and/or sub-additive shares may exist.

The next corollary holds from (3.16).

Corollary 3.6 (Okada-Kurosawa [88]) In any ramp SS scheme for access structure Γ^R with $L+1$ levels, it holds for any $\boldsymbol{A}, \boldsymbol{B} \subseteq \boldsymbol{V}$ that

$$H(\boldsymbol{B}|\boldsymbol{A}) = I(\boldsymbol{B}; S|\boldsymbol{A}) + H(\boldsymbol{B}|\boldsymbol{A}S) \overset{\text{(a)}}{=} \frac{\ell(\boldsymbol{A}\boldsymbol{B}) - \ell(\boldsymbol{A})}{L} H(S) + H(\boldsymbol{B}|\boldsymbol{A}S), \tag{3.23}$$

$$H(\boldsymbol{B}) \geq \max_{\subseteq\ -} H(\boldsymbol{B}|\boldsymbol{A}) \geq \max_{\subseteq\ -} \frac{\ell(\boldsymbol{A}\boldsymbol{B}) - \ell(\boldsymbol{A})}{L} H(S). \tag{3.24}$$

Especially, by letting $\boldsymbol{B} = \{V_i\} \subseteq \boldsymbol{V}$ in (3.24), we have

$$\rho_i \geq \max_{\subseteq\ -\{V_i\}} \frac{\ell(\boldsymbol{A}\{V_i\}) - \ell(\boldsymbol{A})}{L}. \tag{3.25}$$

□

Note that equality (a) in (3.23) is obtained by replacing $\boldsymbol{A}$ and $\boldsymbol{C}$ with $\boldsymbol{B}$ and $\boldsymbol{A}$, respectively in (3.16). In the case of perfect SS schemes, i.e., $L = 1$, it holds for any significant share V_i that $\max_{\subseteq\ -\{V_i\}} \{\ell(\boldsymbol{A}\{V_i\}) - \ell(\boldsymbol{A})\} = 1$. Hence, Theorem 2.4, which gives the lower bound of ρ_i for perfect SS schemes, can be derived from Corollary 3.6.

We note that the lower bound of ρ_i given by (3.25) may not be tight because $I(\boldsymbol{A}; \boldsymbol{B}) = H(\boldsymbol{B}) - H(\boldsymbol{B}|\boldsymbol{A})$ may be positive for the first inequality in (3.24). Actually, we show that (3.25) is not tight in the case of sub-additive shares.

Theorem 3.7 In any ramp SS scheme for access structure Γ^R with $L + 1$ levels, if $V^\flat \in \boldsymbol{V}$ is sub-additive, then the coding rate of $V^\flat$, say $\rho^\flat$, satisfies that

$$\rho^\flat \geq \frac{\ell(\{V^\flat\})}{L} > \max_{\subseteq\ -\{V^\flat\}} \frac{\ell(\boldsymbol{A}\{V^\flat\}) - \ell(\boldsymbol{A})}{L}. \tag{3.26}$$

□

Proof of Theorem 3.7 From (3.18) and (3.23), we have

$$\begin{aligned}
&H(V^\flat) \\
&= H(V^\flat|\boldsymbol{A}) + I(V^\flat; \boldsymbol{A}) \\
&= \frac{\ell(\boldsymbol{A}\{V^\flat\}) - \ell(\boldsymbol{A})}{L} H(S) + H(V^\flat|\boldsymbol{A}S) + \frac{\ell(\boldsymbol{A}) + \ell(\{V^\flat\}) - \ell(\boldsymbol{A}\{V^\flat\})}{L} H(S) + I(\boldsymbol{A}; V^\flat|S) \\
&\geq \frac{\ell(\boldsymbol{A}\{V^\flat\}) - \ell(\boldsymbol{A})}{L} H(S) + \frac{\ell(\boldsymbol{A}) + \ell(\{V^\flat\}) - \ell(\boldsymbol{A}\{V^\flat\})}{L} H(S) \\
&= \frac{\ell(\{V^\flat\})}{L} H(S).
\end{aligned} \tag{3.27}$$

Hence, the first inequality in (3.26) holds. Furthermore, in the case of sub-additive shares, it holds from (3.22) that for any $\boldsymbol{A} \subseteq \boldsymbol{V}$

$$\frac{\ell(\boldsymbol{A}) + \ell(\{V^\flat\}) - \ell(\boldsymbol{A}\{V^\flat\})}{L} H(S) > 0. \tag{3.28}$$

This means that the second inequality in (3.26) holds. □

From Theorem 3.7, sub-additive shares are inefficient. But, their coding rates can be improved by decreasing only the level of $V^\flat$, i.e., $\ell(\{V^\flat\})$, to $\max_{\subseteq\ -\{V^\flat\}} \{\ell(\boldsymbol{A}\{V^\flat\}) - \ell(\boldsymbol{A})\}$, which means that secret S becomes more secure against $V^\flat$. Note that the new access structure obtained by this modification still satisfies the monotonicity. This modification means that the sub-additive share $V^\flat$ becomes additive, and hence, the lower bound of the modified $V^\flat$ can be evaluated by (3.25). Hence, from the viewpoint of coding rates and security, we should take this modification, by which all the shares become additive or super-additive and they satisfy (3.25). Based on (3.25), we now extend the notion of ideal perfect SS schemes to ramp SS schemes.

Definition 3.8 A ramp SS scheme is called *well-realized* if every share $V_i \in \boldsymbol{V}$ satisfies

$$\rho_i = \max_{\boldsymbol{A} \subseteq \boldsymbol{V} - \{V_i\}} \frac{\ell(\boldsymbol{A}\{V_i\}) - \ell(\boldsymbol{A})}{L}. \tag{3.29}$$

□

It is defined in [71] that a ramp SS scheme is ideal if ρ_i satisfies $\rho_i = \frac{1}{L}$ for all i since any ρ_i must satisfy $\rho_i \geq \frac{1}{L}$. Since it holds that

$$\max_{\boldsymbol{A} \subseteq \boldsymbol{V} - \{V_i\}} \frac{\ell(\boldsymbol{A}\{V_i\}) - \ell(\boldsymbol{A})}{L} \geq \frac{1}{L}, \tag{3.30}$$

an ideal ramp SS scheme is a well-realized ramp SS scheme. Actually, any (k, L, n)-threshold ramp SS schemes are ideal and well-realized.

But, there exist many ramp access structures that satisfies (3.30) with strict inequality. Hence, from (3.25) in Corollary 3.6, there are many ramp SS schemes that are well-realized but not ideal. The following is such an example.

Example 3.9 Consider the following ramp access structure Γ_1^R with three levels for three shares $\boldsymbol{V} = \{V_1, V_2, V_3\}$.

$$\mathcal{A}_2^- = \{\{V_1, V_2\}\}, \tag{3.31}$$
$$\mathcal{A}_1 = \{\{V_2, V_3\}\}, \tag{3.32}$$
$$\mathcal{A}_0^+ = \{\{V_1\}, \{V_1, V_3\}\}. \tag{3.33}$$

Then, a ramp SS scheme for Γ_1^R is realized as follows.

$$V_1 = \{R_1, R_2\}, \tag{3.34}$$
$$V_2 = \{S_1 - R_1, S_2 - R_2\}, \tag{3.35}$$
$$V_3 = \{R_1\}, \tag{3.36}$$

where a secret S is given by $S = \{S_1, S_2\}$ and R_1, R_2 are independent uniform random numbers. It is easy to check that $\rho_1 = \rho_2 = 1$ and $\rho_3 = \frac{1}{2}$, and hence, the ramp SS scheme for Γ_1^R is well-realized but not ideal. □

In the case of ideal perfect SS schemes with $L = 1$, both sides of (3.30) becomes 1 because for any significant share $V_i \in \boldsymbol{V}$, there exist a share set $\boldsymbol{A} \subseteq \boldsymbol{V} - \{V_i\}$ such that $\ell(\boldsymbol{A}\{V_i\}) = 1$ and $\ell(\boldsymbol{A}) = 0$. Hence, both of ideal ramp SS schemes and well-realized ramp SS schemes are extensions of ideal perfect SS schemes. But, ideal ramp SS schemes may not be well-realized.

From Theorem 3.7, the following theorem obviously holds.

Theorem 3.10 Any ramp SS schemes with sub-additive shares cannot be well-realized. □

Note that we need not care Theorem 3.10 in the case of perfect SS schemes since there exists no sub-additive share. In the next section, we show that there exist ramp access structures that cannot be well-realized.

3.3.2 Ramp Access Structures With No Well-realized Ramp Secret Sharing Schemes

In this section, we show that even if all the shares V_i, $i = 1, 2, \ldots, n$, are super-additive or additive shares, there exist an access structures that cannot be well-realized.

Lemma 3.11 For a ramp SS scheme with access structure Γ^R with $L+1$ levels, let $\{\boldsymbol{X}_i\}_{i=1}^m$ and $\{\boldsymbol{Y}_i\}_{i=1}^m$ be partitions of $\boldsymbol{A}$ and $\boldsymbol{B}$, respectively, i.e., $\boldsymbol{A} = \bigcup_{k=1}^m \boldsymbol{X}_k$, $\boldsymbol{B} = \bigcup_{k=1}^m \boldsymbol{Y}_k$, $\boldsymbol{X}_k \cap \boldsymbol{X}_{k'} = \boldsymbol{Y}_k \cap \boldsymbol{Y}_{k'} = \emptyset$ for $k \neq k'$. Note that $\boldsymbol{X}_k$ and $\boldsymbol{Y}_k$ may be empty. Then, $I(\boldsymbol{A}; \boldsymbol{B})$ can be represented as

$$I(\boldsymbol{A}; \boldsymbol{B}) = \left(\sum_{j=1}^m \vartheta_j + \ell(\boldsymbol{A}) - \ell(\boldsymbol{AB}) \right) \frac{H(S)}{L} + \Upsilon, \tag{3.37}$$

where ϑ_j and Υ are defined for $\boldsymbol{B}_i = \bigcup_{k=1}^i \boldsymbol{Y}_i$ and $\boldsymbol{B}_0 = \emptyset$ by

$$\vartheta_j \stackrel{\text{def}}{=} \ell(\boldsymbol{X}_j \boldsymbol{B}_j) - \ell(\boldsymbol{X}_j \boldsymbol{B}_{j-1}), \tag{3.38}$$

$$\Upsilon \stackrel{\text{def}}{=} \sum_{j=1}^m \left\{ I(\boldsymbol{X}_j; \boldsymbol{Y}_j | \boldsymbol{B}_{j-1}) + I(\boldsymbol{A} - \boldsymbol{X}_j; \boldsymbol{Y}_j | \boldsymbol{X}_j \boldsymbol{B}_{j-1} S) \right\}, \tag{3.39}$$

which are non-negative. □

Proof of Lemma 3.11

$$\begin{aligned}
& I(\boldsymbol{A}; \boldsymbol{B}) \\
&\stackrel{\text{(a)}}{=} I(\boldsymbol{A}; \boldsymbol{B} | S) + \frac{\ell(\boldsymbol{A}) + \ell(\boldsymbol{B}) - \ell(\boldsymbol{AB})}{L} H(S) \\
&= \sum_{j=1}^m I(\boldsymbol{A}; \boldsymbol{Y}_j | \boldsymbol{B}_{j-1} S) + \frac{\ell(\boldsymbol{A}) + \ell(\boldsymbol{B}) - \ell(\boldsymbol{AB})}{L} H(S) \\
&= \sum_{j=1}^m \{ I(\boldsymbol{X}_j; \boldsymbol{Y}_j | \boldsymbol{B}_{j-1} S) + I(\boldsymbol{A} - \boldsymbol{X}_j; \boldsymbol{Y}_j | \boldsymbol{X}_j \boldsymbol{B}_{j-1} S) \} + \frac{\ell(\boldsymbol{A}) + \ell(\boldsymbol{B}) - \ell(\boldsymbol{AB})}{L} H(S) \\
&\stackrel{\text{(b)}}{=} \sum_{j=1}^m \Bigg\{ I(\boldsymbol{X}_j; \boldsymbol{Y}_j | \boldsymbol{B}_{j-1}) + I(\boldsymbol{A} - \boldsymbol{X}_j; \boldsymbol{Y}_j | \boldsymbol{X}_j \boldsymbol{B}_{j-1} S) \\
&\quad + \frac{\ell(\boldsymbol{X}_j \boldsymbol{B}_j) + \ell(\boldsymbol{B}_{j-1}) - \ell(\boldsymbol{X}_j \boldsymbol{B}_{j-1}) - \ell(\boldsymbol{B}_j)}{L} H(S) \Bigg\} + \frac{\ell(\boldsymbol{A}) + \ell(\boldsymbol{B}) - \ell(\boldsymbol{AB})}{L} H(S) \\
&\stackrel{\text{(c)}}{=} \left(\sum_{j=1}^m \vartheta_j + \ell(\boldsymbol{B}_0) - \ell(\boldsymbol{B}_m) \right) \frac{H(S)}{L} + \frac{\ell(\boldsymbol{A}) + \ell(\boldsymbol{B}) - \ell(\boldsymbol{AB})}{L} H(S) + \Upsilon \\
&= \left(\sum_{j=1}^m \vartheta_j + \ell(\boldsymbol{A}) - \ell(\boldsymbol{AB}) \right) \frac{H(S)}{L} + \Upsilon,
\end{aligned} \tag{3.40}$$

where equalities (a) and (b) are obtained from (3.18) and (3.16), respectively, and equality (c) holds because $\boldsymbol{B}_m = \boldsymbol{B}$ and $\ell(\boldsymbol{B}_0) = 0$. □

From (3.23), we have

$$H(\boldsymbol{A}|\boldsymbol{B}) = \frac{\ell(\boldsymbol{AB}) - \ell(\boldsymbol{B})}{L} H(S) + H(\boldsymbol{A}|\boldsymbol{B}S). \tag{3.41}$$

Hence, adding both sides of (3.37) and (3.41), we obtain

$$H(\boldsymbol{A}) = \left(\sum_{j=1}^{m} \vartheta_j + \ell(\boldsymbol{A}) - \ell(\boldsymbol{B}) \right) \frac{H(S)}{L} + \Upsilon + H(\boldsymbol{A}|\boldsymbol{B}S). \tag{3.42}$$

Since Υ and $H(\boldsymbol{A}|\boldsymbol{B}S)$ are nonnegative, the next theorem holds.

Theorem 3.12 In any ramp SS scheme for access structure Γ^R with $L+1$ levels, $H(\boldsymbol{A})$ is bounded by

$$H(\boldsymbol{A}) \geq \left(\sum_{j=1}^{m} \vartheta_j + \ell(\boldsymbol{A}) - \ell(\boldsymbol{B}) \right) \frac{H(S)}{L}, \tag{3.43}$$

where ϑ_j is defined in (3.38). Hence, at least one share $V_i \in \boldsymbol{A}$ must satisfy

$$\rho_i \geq \frac{1}{L|\boldsymbol{A}|} \max_{\subseteq} \left(\sum_{j=1}^{m} \vartheta_j + \ell(\boldsymbol{A}) - \ell(\boldsymbol{B}) \right). \tag{3.44}$$

□

Letting $L = 1$ in Theorem 3.12, we have the following corollary.

Corollary 3.13 (Blundo et al. [15], Padró-Sáez [92]) In perfect SS schemes, if there exist partitions of $\boldsymbol{A}, \boldsymbol{B} \subseteq \boldsymbol{V}$ such that $\ell(\boldsymbol{X}_i\boldsymbol{B}_i) = 1, \ell(\boldsymbol{X}_i\boldsymbol{B}_{i-1}) = 0, i = 1, 2, \ldots, m$, and $\ell(\boldsymbol{B}) = 0$, it holds that

$$H(\boldsymbol{A}) \geq \begin{cases} (m+1)H(S) & \text{if } \boldsymbol{A} \in \mathcal{A}_1 \\ mH(S) & \text{if } \boldsymbol{A} \in \mathcal{A}_0. \end{cases} \tag{3.45}$$

Therefore, in the case of $\boldsymbol{A} \in \mathcal{A}_1$, at least one share $V_i \in \boldsymbol{A}$ must satisfy $\rho_i \geq \frac{m+1}{m}$, and hence, such SS schemes are non-ideal. □

We can know from Corollary 3.13 that the access structure treated in [24], [30] cannot be realized by ideal perfect SS scheme as shown in the following example.

Example 3.14 (Capocelli et al. [24]) Let us consider the following access structure with four shares.

$$\mathcal{A}_1^- = \{\{V_1, V_2\}, \{V_2, V_3\}, \{V_3.V_4\}\}. \tag{3.46}$$

Let $\boldsymbol{A} = \{V_1, V_2\} \in \mathcal{A}_1$ and $\boldsymbol{B} = \{V_3, V_4\}$, and consider their partitions such that $\boldsymbol{X}_1 = \{V_2\}$, $\boldsymbol{X}_2 = \{V_1\}$, $\boldsymbol{Y}_1 = \{V_3\}$, and $\boldsymbol{Y}_2 = \{V_4\}$. Then, we can obtain from (3.45) that $H(V_1V_2) \geq 3H(S)$, and hence, it must hold for $i = 1$ or $i = 2$ that $\rho_i \geq \frac{3}{2}$. In the same way, we obtain that $H(\boldsymbol{A}) \geq 3H(S)$ for any $\boldsymbol{A} \in \mathcal{A}_1^-$. Therefore, this access structure cannot be realized as an ideal SS scheme. □

Next, based on Theorem 3.12, we consider the ramp SS schemes treated in [88] and we show that they are not well-realized.

Example 3.15 Consider the following access structure Γ_2^R with 3 levels for share set $\boldsymbol{V} = \{V_1, V_2, V_3, V_4\}$.

$$\mathcal{A}_1^- = \{\{V_1, V_4\}, \{V_2, V_4\}\}, \tag{3.47}$$
$$\mathcal{A}_2^- = \{\{V_1, V_2, V_3\}\}. \tag{3.48}$$

Then, it must hold that $H(V_1V_4) \geq 2H(S)$ and $H(V_2V_4) \geq 2H(S)$. □

Note that each share in Γ_2^R is super-additive. We can easily prove that $H(V_1V_2) \geq 2H(S)$ from Theorem 3.12 by letting $\boldsymbol{A} = \{V_1, V_4\}$, $\boldsymbol{B} = \{V_2, V_3\}$, $\boldsymbol{X}_1 = \{V_4\}$, $\boldsymbol{X}_2 = \{V_1\}$, $\boldsymbol{Y}_1 = \{V_2\}$ and $\boldsymbol{Y}_2 = \{V_3\}$. Similarly, by letting, $\boldsymbol{X}_1 = \{V_4\}$, $\boldsymbol{X}_2 = \{V_2\}$, $\boldsymbol{Y}_1 = \{V_1\}$ and $\boldsymbol{Y}_2 = \{V_3\}$, we have $H(V_2V_4) \geq 2H(S)$.

In order to realize the access structure Γ_2^R as a well-realized SS scheme, it must hold that $H(V_1) = H(S)$, $H(V_2) = H(S)$, and $H(V_4) = \frac{1}{2}H(S)$ from Definition 3.8. But this contradicts the result of Example 3.15. Hence, the ramp access structure Γ_2^R cannot be well-realized.

Example 3.16 (Okada-Kurosawa [88]) For the access structure Γ_2^R defined in (3.47)–(3.48), it must hold that $H(V_1V_4) \geq 2H(S)$ and $H(V_2V_4) \geq 2H(S)$, and hence, if S is uniformly distributed,

$$\log|\mathbb{F}_{V_1}| + \log|\mathbb{F}_{V_4}| \geq 2\log|\mathbb{F}_S|, \tag{3.49}$$
$$\log|\mathbb{F}_{V_2}| + \log|\mathbb{F}_{V_4}| \geq 2\log|\mathbb{F}_S|. \tag{3.50}$$

The ramp SS scheme attaining the inequalities (3.49) and (3.50) with equalities is realized as follows.

$$V_1 = \{R_1, R_3\}, \tag{3.51}$$
$$V_2 = \{R_2, R_4\}, \tag{3.52}$$
$$V_3 = \{R_1 + R_4 + S_1, R_2 + R_3 + S_2\}, \tag{3.53}$$
$$V_4 = \{R_1 + S_1, R_2 + S_1\}, \tag{3.54}$$

where secret S is given by $S = \{S_1, S_2\}$ and $R_1, R_2, \ldots, R_4$ are independent uniform distributed random numbers. □

Example 3.17 Consider the following access structure Γ_3^R with $L = 2$ for share set $\boldsymbol{V} = \{V_1, V_2, V_3, V_4, V_5\}$.

$$\mathcal{A}_1^- = \{\{V_1\}, \{V_5\}\}, \tag{3.55}$$
$$\mathcal{A}_2^- = \{\{V_1, V_5\}, \{V_2, V_5\}, \{V_3, V_5\}, \{V_1, V_2, V_3, V_4\}\}. \tag{3.56}$$

Then, it must hold that $H(V_2V_5) \geq 2H(S)$. □

Example 3.17 holds from Theorem 3.12 by letting $\boldsymbol{A} = \{V_2, V_5\}$, $\boldsymbol{B} = \{V_1, V_2, V_3, V_4\}$, $\boldsymbol{X}_1 = \emptyset$, $\boldsymbol{X}_2 = \{V_5\}$, $\boldsymbol{X}_3 = \{V_2\}$, $\boldsymbol{X}_4 = \emptyset$, $\boldsymbol{Y}_1 = \{V_4\}$, $\boldsymbol{Y}_2 = \{V_3\}$, $\boldsymbol{Y}_3 = \{V_1\}$, and $\boldsymbol{Y}_4 = \{V_2\}$. It is easy to check that each share in Γ_3^R is super-additive but Γ_3^R cannot be well-realized.

Furthermore, since it must hold from (3.25) that $H(V_1) \geq H(S)$, we have $H(V_1)+H(V_2V_5) \geq 3H(S)$, we have the following example.

Example 3.18 (Okada-Kurosawa [88]) For the access structure Γ_3^R defined in (3.55) and (3.56), if S is uniformly distributed, we have that

$$\log|\mathbb{F}_{V_1}| + \log|\mathbb{F}_{V_2}| + \log|\mathbb{F}_{V_5}| \geq 3\log|\mathbb{F}_S|. \tag{3.57}$$

The ramp SS scheme attaining the inequality in (3.57) with equality is realized as follows.

$$V_1 = \{S_1, R_1\}, \tag{3.58}$$
$$V_2 = \{R_2\}, \tag{3.59}$$
$$V_3 = \{R_3\}, \tag{3.60}$$
$$V_4 = \{R_1 + R_2 + R_3 + S_2\}, \tag{3.61}$$
$$V_5 = \{S_2, R_2 + S_1, R_3 + S_3\}, \tag{3.62}$$

where secret S is given by $S = \{S_1, S_2\}$ and R_1, R_2, R_3 are independent uniformly distributed random numbers. □

Note that Example 3.17 cannot be derived from Example 3.18.

From the above examples, Theorem 3.12 can be used to check whether given access structures, e.g., the ones treated in [15], [88], can be well-realized or not. However, a general coding method to attain the inequality in (3.43) with equality is not known although the inequalities (3.49), (3.50), and (3.57) can be attained with equality by known methods.

3.4 Conclusion

In this chapter, we defined ramp SS schemes for general access structures and considered their coding rates. In ramp SS schemes, we classified shares into three categories, and we derived the lower bound of coding rates for each category of shares. Then, we defined well-realized ramp SS schemes as extensions of perfect ideal SS schemes. Furthermore, we showed that Theorem 3.12 can be used to check whether given access structures can be well-realized or not.

Chapter 4

Constructions of Secret Sharing Schemes Based on Integer Programming

4.1 Introduction

In this chapter, we consider the construction method of SS schemes for general access structures. As shown in Section 2.2.2, the efficiency of SS schemes is measured by the entropy of each share. It is known that the entropies of secret S and shares V_i, $i = 1, 2, \ldots, n$, must satisfy $H(V_i) \geq H(S)$ for any access structures [24], [30], [58]. On the other hand, in the case of (k, n)-threshold SS schemes, the optimal SS schemes attaining $H(V_i) = H(S)$ can easily be constructed [99]. However, it is hard to derive efficient SS schemes for arbitrarily given general access structures although several construction methods have been proposed.

For example, the *monotone circuit construction* [4] shown in Section 2.2.3.2 is a method to realize a SS scheme by combining several (m, m)-threshold SS schemes. This method is simple but inefficient, and hence, it is extended to the *decomposition construction* [104], which uses several decomposed general SS schemes. Although the decomposition construction can attain the optimal coding rates for some special access structures, it cannot construct an efficient SS scheme in the case that decomposed SS schemes cannot be realized efficiently.

On the other hand, for any given general access structure, a SS scheme can be constructed from a (t, m)-threshold SS scheme by a *multiple assignment map* such that t or more shares of the (t, m)-threshold SS scheme are assigned to qualified sets but $t - 1$ or less shares are assigned to forbidden sets. A *cumulative map* is a simple realization of the multiple assignment map [47]–[49], and from its simplicity, it is often used in visual secret sharing schemes for general access structures [1], [66], which will be treated in Section 6.4. However, it is known that SS schemes constructed by the cumulative map are generally inefficient, especially in the case that access structures are close to (k, n)-threshold SS schemes with $k \neq n$. Recently, a *modified* cumulative map is proposed to overcome this defect [109]. But, the modified cumulative map is not always more efficient than the original cumulative map.

In this chapter, we propose a new construction method that can derive the optimal multiple assignment map by integer programming. The proposed construction method is not only very

simple but also optimal in the sense of multiple assignment maps. Furthermore, it can be applied to incomplete and/or ramp access structures.

This chapter is organized as follows. In Section 4.2, we introduce the multiple assignment map. We also introduce the construction methods of the cumulative map and the modified cumulative map, and we point out their defects. To overcome such defects, we propose a new construction method of the optimal multiple assignment map by integer programming in Section 4.3. Finally, Sections 4.4 and 4.5 are devoted to present the applications of the proposed method to incomplete access structures and general ramp access structures, respectively. The contents of this chapter are appeared in [50].

4.2 Multiple Assignment Schemes

Let $\Gamma = \{\mathcal{A}_1, \mathcal{A}_0\}$ be a given general access structure with family of qualified sets $\mathcal{A}_1$, family of forbidden sets $\mathcal{A}_0$, and share set $\boldsymbol{V} = \{V_1, V_2, \ldots, V_n\}$. Then, for a share set of a (t, m)-threshold SS scheme, $\boldsymbol{W}_{(t,m)} = \{W_1^{(t)}, W_2^{(t)}, \ldots, W_m^{(t)}\}$, we consider a map $\varphi_\Gamma : \{1, 2, \ldots, n\} \to 2^{\boldsymbol{W}_{(t,m)}}$ and a map $\Phi_\Gamma(\boldsymbol{A})$ which is defined as $\Phi_\Gamma(\boldsymbol{A}) \stackrel{\text{def}}{=} \bigcup_{V_i \in \boldsymbol{A}} \varphi_\Gamma(i)$ for share subset $\boldsymbol{A} \subseteq \boldsymbol{V}$. Then, φ_Γ is called a *multiple assignment map* for access structure Γ if each share V_i is determined by $V_i = \varphi_\Gamma(i)$ and $\Phi_\Gamma(\boldsymbol{A})$ satisfies the following conditions:

$$|\Phi_\Gamma(\boldsymbol{A})| \geq t \qquad \text{if } \boldsymbol{A} \in \mathcal{A}_1, \tag{4.1}$$

$$|\Phi_\Gamma(\boldsymbol{A})| \leq t-1 \quad \text{if } \boldsymbol{A} \in \mathcal{A}_0, \tag{4.2}$$

$$\Phi_\Gamma(\boldsymbol{V}) = \boldsymbol{W}_{(t,m)}. \tag{4.3}$$

To distinguish $W_j^{(t)} \in \boldsymbol{W}_{(t,m)}$ from the shares V_i of Γ, we call $W_j^{(t)}$ a *primitive* share.

Since any (t, m)-threshold SS scheme can easily be constructed as an ideal SS scheme [58], [99], we assume in this chapter that the (t, m)-threshold SS scheme with $\boldsymbol{W}_{(t,m)} = \{W_1^{(t)}, W_2^{(t)}, \ldots, W_m^{(t)}\}$ is ideal. Then, the average and worst coding rates defined by (2.18) and (2.19) become

$$\tilde{\rho} = \frac{1}{n}\sum_{i=1}^{n} |\varphi_\Gamma(i)|, \tag{4.4}$$

$$\rho^* = \max_{1 \leq i \leq n} |\varphi_\Gamma(i)|, \tag{4.5}$$

respectively, since it holds that $\rho_i = |\varphi_\Gamma(i)|$.

In the case of $t = m$, it is known that the multiple assignment map φ_Γ satisfying (4.1)–(4.3) can be realized for any access structures [47]–[49]. Suppose that access structure $\Gamma = \{\mathcal{A}_1, \mathcal{A}_0\}$ has

$$\mathcal{A}_0^+ = \{\boldsymbol{F}_1, \boldsymbol{F}_2, \ldots, \boldsymbol{F}_m\}. \tag{4.6}$$

Note that $m = |\mathcal{A}_0^+|$. Then, consider a map $\psi_\Gamma : \{1, 2, \ldots, n\} \to 2^{\boldsymbol{W}_{(m,m)}}$ defined by

$$\psi_\Gamma(i) = \bigcup_{j : V_i \notin \boldsymbol{F}_j} \left\{ W_j^{(m)} \right\}, \tag{4.7}$$

where $\boldsymbol{F}_j \in \mathcal{A}_0^+$ and $\boldsymbol{W}_{(m,m)} = \left\{W_1^{(m)}, W_2^{(m)}, \ldots, W_m^{(m)}\right\}$ is the set of primitive shares of an (m,m)-threshold SS scheme. The multiple assignment map ψ_Γ is called a *cumulative map*.

Example 4.1 Assume that $n = 4$ and an access structure Γ_1 is defined by

$$\mathcal{A}_1^- = \{\{V_1, V_2, V_3\}, \{V_1, V_4\}, \{V_2, V_4\}, \{V_3, V_4\}\}, \tag{4.8}$$
$$\mathcal{A}_0^+ = \{\{V_1, V_2\}, \{V_1, V_3\}, \{V_2, V_3\}, \{V_4\}\}. \tag{4.9}$$

Then, $m = |\mathcal{A}_0^+| = 4$, and the cumulative map ψ_{Γ_1} is given from (4.7) as follows.

$$V_1 = \psi_{\Gamma_1}(1) = \left\{W_3^{(4)}, W_4^{(4)}\right\}, \tag{4.10}$$
$$V_2 = \psi_{\Gamma_1}(2) = \left\{W_2^{(4)}, W_4^{(4)}\right\}, \tag{4.11}$$
$$V_3 = \psi_{\Gamma_1}(3) = \left\{W_1^{(4)}, W_4^{(4)}\right\}, \tag{4.12}$$
$$V_4 = \psi_{\Gamma_1}(4) = \left\{W_1^{(4)}, W_2^{(4)}, W_3^{(4)}\right\}. \tag{4.13}$$

In this example, it holds that $\tilde{\rho} = \frac{9}{4}$ and $\rho^* = 3$. □

It is known that the next theorem holds for the cumulative map ψ_Γ.

Theorem 4.2 (Simmons et al. [102]) For any multiple assignment map $\varphi_\Gamma : \{1, 2, \ldots, n\} \to 2^{(t,m)}$ with $t = m$, it must hold that $|\boldsymbol{W}_{(m,m)}| \geq |\mathcal{A}_0^+|$, i.e., $m \geq |\mathcal{A}_0^+|$. The equality holds if and only if $\varphi_\Gamma(i)$ is equal to the cumulative map $\psi_\Gamma(i)$ defined by (4.7).[1] □

Theorem 4.2 means that, in the case of $t = m$, the cumulative map ψ_Γ can minimize the number of primitive shares m. But, the minimization of m does not mean the realization of an efficient SS scheme generally because it does not minimize the average coding rate $\tilde{\rho}$ and/or the worst coding rate ρ^*.

For instance, consider the case that Γ is a (k,n)-threshold access structure with $k \neq n$. If we construct shares V_i by the cumulative map ψ for this Γ, each V_i must consist of the $\binom{n-1}{k-1}$ primitive shares of an $\left(\binom{n}{k-1}, \binom{n}{k-1}\right)$-threshold SS scheme because of $|\mathcal{A}_0^+| = \binom{n}{k-1}$. This means that $\tilde{\rho} = \rho^* = \binom{n}{k-1}$. But, if we use the (k,n)-threshold SS scheme itself, we have $\tilde{\rho} = \rho^* = 1$ because each V_i consists of one primitive share. Hence, the cumulative map is quite inefficient in the case that Γ is close to a (k,n)-threshold access structure. In order to overcome this defect, a *modified* cumulative map is proposed in [109] based on (t,m)-threshold SS schemes. The modified cumulative map ψ'_Γ is constructed as follows.

Construction 4.3 (Tochikubo [109]) For a given $\Gamma = \{\mathcal{A}_0^+, \mathcal{A}_1^-\}$ and a positive integer $g \stackrel{\text{def}}{=} \min_{\boldsymbol{A} \in \mathcal{A}_1^-} |\boldsymbol{A}|$, let $\mathcal{G}_0 \subseteq \mathcal{A}_0^+$ be the family defined by

$$\mathcal{G}_0 = \{\boldsymbol{G} \in \mathcal{A}_0^+ : |\boldsymbol{G}| \geq g\}. \tag{4.14}$$

[1] We assume that all ψ_Γ's obtained by all permutations of $\boldsymbol{F}_j$'s in (4.6) are the same.

When $\mathcal{G}_0 = \{\boldsymbol{G}_1, \boldsymbol{G}_2, \ldots, \boldsymbol{G}_u\}$, let $p_i \stackrel{\text{def}}{=} |\boldsymbol{G}_i| - g + 1$ for $i = 1, 2, \ldots, u$, and $q_i \stackrel{\text{def}}{=} \sum_{j=1}^{i} p_j$. Then, consider a $(g+q_u, n+q_u)$-threshold SS scheme and the set of primitive shares $\boldsymbol{W}_{(g+q_u, n+q_u)} = \{W_1^{(g+q_u)}, W_2^{(g+q_u)}, \ldots, W_{n+q_u}^{(g+q_u)}\}$. Furthermore, let $\boldsymbol{U}_i$ be the subset of primitive shares defined by

$$\boldsymbol{U}_i = \left\{ W_{n+q_{i-1}+1}^{(g+q_u)}, W_{n+q_{i-1}+2}^{(g+q_u)}, \ldots, W_{n+q_i}^{(g+q_u)} \right\}, \tag{4.15}$$

where $q_0 = 0$. Then, the modified cumulative map ψ'_Γ is defined by

$$\psi'_\Gamma(i) = \left\{ W_i^{(g+q_u)} \right\} \cup \left\{ \bigcup_{j: V_i \notin \ _j} \boldsymbol{U}_j \right\}. \tag{4.16}$$

□

In the case that Γ is a (k, n)-threshold access structure, it holds that $\psi'_\Gamma(i) = \{W_i^{(k)}\}$ for $i = 1, 2, \ldots, n$ [109]. Hence, the modified cumulative map ψ'_Γ is efficient if Γ is close to a (k, n)-threshold access structures. Furthermore, it is shown [109] that if the access structure Γ satisfies

$$|\mathcal{A}_0^+| - |\mathcal{G}_0| - (q_u - |\mathcal{G}_0|)^2 \geq \frac{n}{n - g + 1}, \tag{4.17}$$

then it holds that $\sum_{V_i \in \ } |\psi'_\Gamma(i)| \leq \sum_{V_i \in \ } |\psi_\Gamma(i)|$, which means that the average coding rate $\tilde{\rho}$ of ψ'_Γ is smaller than ψ_Γ.

But, as shown in the following example, ψ'_Γ is not always more efficient than ψ_Γ if Γ does not satisfy (4.17).

Example 4.4 Consider the access structure Γ_1 given by (4.8) and (4.9) in Example 4.1, which does not satisfy (4.17). Since we have that $g = 2$ from (4.8), $\mathcal{G}_0$ becomes $\mathcal{G}_0 = \{\{V_1, V_2\}, \{V_1, V_3\}, \{V_2, V_3\}\} \stackrel{\text{def}}{=} \{\boldsymbol{G}_1, \boldsymbol{G}_2, \boldsymbol{G}_3\}$. Furthermore, since we have that $p_1 = p_2 = p_3 = 1$ and $q_3 = 3$, $\boldsymbol{U}_i$'s are determined as $\boldsymbol{U}_1 = \{W_5^{(5)}\}$, $\boldsymbol{U}_2 = \{W_6^{(5)}\}$, $\boldsymbol{U}_3 = \{W_7^{(5)}\}$ for $\boldsymbol{W}_{(5,7)} = \{W_1^{(5)}, W_2^{(5)}, \ldots, W_7^{(5)}\}$. Finally, we have from (4.16) that

$$V_1 = \psi'_{\Gamma_1}(1) = \left\{ W_1^{(5)}, W_7^{(5)} \right\}, \tag{4.18}$$

$$V_2 = \psi'_{\Gamma_1}(2) = \left\{ W_2^{(5)}, W_6^{(5)} \right\}, \tag{4.19}$$

$$V_3 = \psi'_{\Gamma_1}(3) = \left\{ W_3^{(5)}, W_5^{(5)} \right\}, \tag{4.20}$$

$$V_4 = \psi'_{\Gamma_1}(4) = \left\{ W_4^{(5)}, W_5^{(5)}, W_6^{(5)}, W_7^{(5)} \right\}. \tag{4.21}$$

In this example, the coding rates are given by $\tilde{\rho} = \frac{5}{2}$ and $\rho^* = 4$, which are larger than the coding rates of Example 4.1, i.e., $\tilde{\rho} = \frac{9}{4}$ and $\rho^* = 3$. □

Note that (4.17) does not guarantee that the worst coding rate ρ^* of ψ'_Γ is smaller than ψ_Γ. Actually, the next example shows the case that ψ'_Γ attains smaller average coding rate but gives larger worst coding rate than ψ_Γ.

Example 4.5 Consider the access structure Γ_2 given by

$$\begin{aligned}\mathcal{A}_1^- = \{&\{V_1, V_2, V_3, V_5\}, \{V_1, V_2, V_4\}, \{V_1, V_3, V_4\}, \{V_1, V_4, V_5\},\\ &\{V_2, V_3, V_4\}, \{V_2, V_4, V_5\}, \{V_3, V_4, V_5\}\} \qquad (4.22)\\ \mathcal{A}_0^+ = \{&\{V_1, V_2, V_3\}, \{V_1, V_2, V_5\}, \{V_1, V_3, V_5\}, \{V_2, V_3, V_5\},\\ &\{V_1, V_4\}, \{V_2, V_4\}, \{V_3, V_4\}, \{V_4, V_5\}\}. \qquad (4.23)\end{aligned}$$

Then, the cumulative map ψ_{Γ_2} is constructed as follows:

$$V_1 = \psi_{\Gamma_2}(1) = \left\{W_4^{(8)}, W_6^{(8)}, W_7^{(8)}, W_8^{(8)}\right\}, \qquad (4.24)$$

$$V_2 = \psi_{\Gamma_2}(2) = \left\{W_3^{(8)}, W_5^{(8)}, W_7^{(8)}, W_8^{(8)}\right\}, \qquad (4.25)$$

$$V_3 = \psi_{\Gamma_2}(3) = \left\{W_2^{(8)}, W_5^{(8)}, W_6^{(8)}, W_8^{(8)}\right\}, \qquad (4.26)$$

$$V_4 = \psi_{\Gamma_2}(4) = \left\{W_1^{(8)}, W_2^{(8)}, W_3^{(8)}, W_4^{(8)}\right\}, \qquad (4.27)$$

$$V_5 = \psi_{\Gamma_2}(5) = \left\{W_1^{(8)}, W_5^{(8)}, W_6^{(8)}, W_7^{(8)}\right\}, \qquad (4.28)$$

which attains that $\tilde{\rho} = \rho^* = 4$. On the other hand, the modified cumulative map ψ'_{Γ_2} is given by

$$V_1 = \psi'_{\Gamma_2}(1) = \left\{W_1^{(7)}, W_9^{(7)}\right\}, \qquad (4.29)$$

$$V_2 = \psi'_{\Gamma_2}(2) = \left\{W_2^{(7)}, W_8^{(7)}\right\}, \qquad (4.30)$$

$$V_3 = \psi'_{\Gamma_2}(3) = \left\{W_3^{(7)}, W_7^{(7)}\right\}, \qquad (4.31)$$

$$V_4 = \psi'_{\Gamma_2}(4) = \left\{W_4^{(7)}, W_6^{(7)}, W_7^{(7)}, W_8^{(7)}, W_9^{(7)}\right\}, \qquad (4.32)$$

$$V_5 = \psi'_{\Gamma_2}(5) = \left\{W_5^{(7)}, W_6^{(7)}\right\}. \qquad (4.33)$$

Observe that the rates of ψ'_{Γ_2} are given by $\tilde{\rho} = \frac{13}{5},\ \rho^* = 5$. Hence, ψ'_{Γ} gives smaller $\tilde{\rho}$ but larger ρ^* than ψ_{Γ}. □

As shown in Examples 4.4 and 4.5, the modified cumulative map cannot always overcome the defects of the original cumulative maps. Hence, in the next section, we propose a construction method of multiple assignment maps that can attain the optimal average or worst coding rates based on integer programming.

4.3 Optimal Multiple Assignment Maps

For a multiple assignment map $\varphi_\Gamma : \{1, 2, \ldots, n\} \to 2^{(t,m)}$ $\boldsymbol{A} \subseteq \boldsymbol{V}$, and $k \in \{0, 1, \ldots, 2^n - 1\}$, let $\boldsymbol{X}_{[k]_2^n}$ be a subset of $\boldsymbol{W}_{(t,m)}$ defined by

$$\boldsymbol{X}_{[k]_2^n} = \left[\bigcap_{i:[k]_2^{n,i}=1} \varphi_\Gamma(i)\right] \cap \left[\bigcap_{i:[k]_2^{n,i}=0} \overline{\varphi_\Gamma(i)}\right], \qquad (4.34)$$

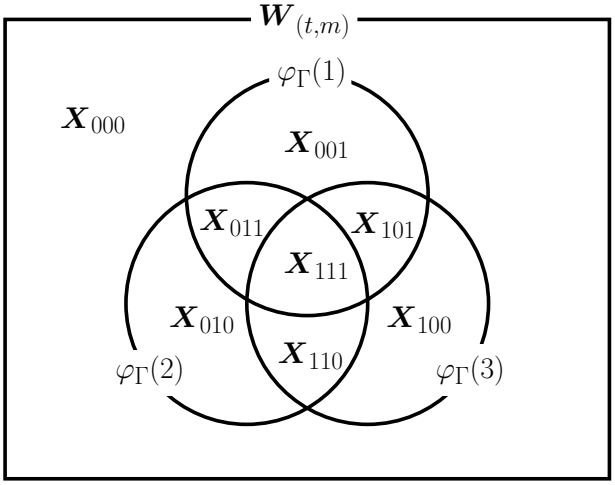


Figure 4.1. Relation between $\varphi_\Gamma(i)$'s and $\boldsymbol{X}_k$'s in the case of $n = 3$.

where $[k]_2^n$ denotes the binary number of integer k with n bits, and $[k]_2^{n,i}$ is the i-th least significant bit of $[k]_2^n$. For example, in the case of $k = 5$ and $n = 4$, it holds that $[5]_2^4 = 0101$, $[5]_2^{4,1} = [5]_2^{4,3} = 1$, and (4.34) becomes $\boldsymbol{X}_{0101} = \overline{\varphi_\Gamma(4)} \cap \varphi_\Gamma(3) \cap \overline{\varphi_\Gamma(2)} \cap \varphi_\Gamma(1)$. For simplicity, we abbreviate $\boldsymbol{X}_{[k]_2^n}$ as $\boldsymbol{X}_k$. Figure 4.1 is the Venn diagram which shows the relation between $\boldsymbol{X}_k$'s and $\varphi_\Gamma(i)$'s in the case of $n = 3$. Then, it is easy to check that $\boldsymbol{X}_k$'s satisfy the following equations for an arbitrary n, $N \stackrel{\text{def}}{=} 2^n - 1$, and any $\boldsymbol{A} \subseteq \boldsymbol{V}$.

$$\boldsymbol{X}_0 = \emptyset \tag{4.35}$$

$$\boldsymbol{X}_k \cap \boldsymbol{X}_{k'} = \emptyset \qquad \text{if } k \neq k' \tag{4.36}$$

$$\varphi_\Gamma(i) = \bigcup_{k:[k]_2^{n,i}=1} \boldsymbol{X}_k \tag{4.37}$$

$$\Phi_\Gamma(\boldsymbol{A}) = \bigcup_{V_i \in} \varphi_\Gamma(i) = \bigcup_{\substack{k:[k]_2^{n,i}=1 \\ \text{for some } V_i \in}} \boldsymbol{X}_k \tag{4.38}$$

$$\Phi_\Gamma(\boldsymbol{V}) = \bigcup_{k=1}^{N} \boldsymbol{X}_k \tag{4.39}$$

Note that (4.35), which means that $\bigcap_{i=1}^n \overline{\varphi_\Gamma(i)} = \emptyset$, follows from the fact that primitive shares not contained in any share are not necessary in Γ. Hence, we consider only $\boldsymbol{X}_k$ for $k = 1, 2, \ldots, N$ in the following.

Letting $x_k = |\boldsymbol{X}_k|$, the cardinality of $\Phi_\Gamma(\boldsymbol{A})$ is given by

$$|\Phi_\Gamma(\boldsymbol{A})| = \sum_{\substack{k:[k]_2^{n,i}=1 \\ \text{for some } V_i \in}} x_k, \tag{4.40}$$

from (4.36) and (4.38). For a set of shares $\boldsymbol{A} = \{V_{i_1}, V_{i_2}, \ldots, V_{i_u}\}$, define an N-dimensional

row vector $\boldsymbol{a}(\boldsymbol{A}) \stackrel{\text{def}}{=} [a(\boldsymbol{A})_1, a(\boldsymbol{A})_2, \ldots, a(\boldsymbol{A})_N] \in \{0,1\}^N$ as

$$a(\boldsymbol{A})_k = \begin{cases} 0 & \text{if } [k]_2^{n,i_1} = [k]_2^{n,i_2} = \cdots = [k]_2^{n,i_u} = 0 \\ 1 & \text{otherwise.} \end{cases} \tag{4.41}$$

Then, the right hand side of (4.40)can be represented by inner product $\boldsymbol{a}(\boldsymbol{A}) \cdot \boldsymbol{x}$ where $\boldsymbol{x} \stackrel{\text{def}}{=} [x_1, x_2, \ldots, x_N]$. Furthermore, denoting the Hamming weight of $[k]_2^n$ by h_k, it holds from (4.37) that

$$\sum_{i=1}^{n} |\varphi_\Gamma(i)| = \sum_{i=1}^{n} \sum_{k:[k]_2^{n,i}=1} x_k = \sum_{k=1}^{N} h_k x_k = \boldsymbol{h} \cdot \boldsymbol{x}, \tag{4.42}$$

where $\boldsymbol{h} = [h_1, h_2, \ldots, h_N] \in \mathbb{Z}^N$. Hence, the average coding rate $\tilde{\rho}$ in (4.4) is given by $\frac{1}{n}\, \boldsymbol{h} \cdot \boldsymbol{x}$.

Now, from (4.40)–(4.42), we can formulate the integer programming problem $\text{IP}_{\tilde{\rho}}(\Gamma)$ that minimizes the average coding rate $\tilde{\rho}$ under the constraints of (4.1) and (4.2) as follows:

$$\begin{array}{lrll} \underline{\text{IP}_{\tilde{\rho}}(\Gamma)} & & & \\ \text{minimize} & \boldsymbol{h} \cdot \boldsymbol{x} & & \\ \text{subject to} & \boldsymbol{a}(\boldsymbol{A}) \cdot \boldsymbol{x} \geq t & \text{for} & \boldsymbol{A} \in \mathcal{A}_1^- \\ & \boldsymbol{a}(\boldsymbol{A}) \cdot \boldsymbol{x} \leq t-1 & \text{for} & \boldsymbol{A} \in \mathcal{A}_0^+ \\ & \boldsymbol{x} \geq \boldsymbol{0} & & \end{array}$$

The optimal multiple assignment map $\tilde{\varphi}_\Gamma$ that attains the minimum average coding rate can be constructed as follows. First, let $\tilde{\boldsymbol{x}} = [\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_N]$ and $\tilde{t}$ be the minimizers of the integer programming problem $\text{IP}_{\tilde{\rho}}(\Gamma)$. Then, for $\tilde{m} \stackrel{\text{def}}{=} |\Phi_\Gamma(\boldsymbol{V})| = \sum_{k=1}^{N} \tilde{x}_k$, we use a $\big(\tilde{t}, \tilde{m}\big)$-threshold SS scheme with primitive shares $\boldsymbol{W}_{(\tilde{t},\tilde{m})} = \left\{W_1^{(\tilde{t})}, W_2^{(\tilde{t})}, \ldots, W_{\tilde{m}}^{(\tilde{t})}\right\}$, and for each k we assign $\tilde{x}_k$ different primitive shares of $\boldsymbol{W}_{(\tilde{t},\tilde{m})}$ to $\boldsymbol{X}_k$ under the conditions (4.36) and (4.39). Finally, the multiple assignment map $\tilde{\varphi}_\Gamma$ is obtained by (4.37).

Remark 4.6 In the case of perfect SS schemes, without loss of generality, we can assume that $x_N = 0$, i.e., $\boldsymbol{X}_N = \bigcap_{i=1}^{n} \varphi_\Gamma(i) = \emptyset$ because it is not necessary to consider the set of primitive shares commonly contained in all the shares. □

In the same way as $\text{IP}_{\tilde{\rho}}(\Gamma)$, the integer programming problem $\text{IP}_{\rho^*}(\Gamma)$ that minimizes the worst coding rate ρ^* can be formulated as follows:

$$\begin{array}{lrll} \underline{\text{IP}_{\tilde{\rho}}(\Gamma)} & & & \\ \text{minimize} & M & & \\ \text{subject to} & \boldsymbol{a}(\boldsymbol{A}) \cdot \boldsymbol{x} \geq t & \text{for} & \boldsymbol{A} \in \mathcal{A}_1^- \\ & \boldsymbol{a}(\boldsymbol{A}) \cdot \boldsymbol{x} \leq t-1 & \text{for} & \boldsymbol{A} \in \mathcal{A}_0^+ \\ & \boldsymbol{a}(\{V\}) \cdot \boldsymbol{x} \leq M & \text{for} & V \in \boldsymbol{V} \\ & \boldsymbol{x} \geq \boldsymbol{0} & & \end{array}$$

The multiple assignment map φ^*_Γ attaining the minimum ρ^* can also be constructed in the same way as the construction of $\tilde{\varphi}_\Gamma$.

Example 4.7 For the access structure Γ_1 defined by (4.8) and (4.9) in Example 4.1, the integer programming problem $\mathrm{IP}_{\tilde{\rho}}(\Gamma_1)$ can be formulated as follows:

$\underline{\mathrm{IP}_{\tilde{\rho}}(\Gamma_1)}$

$$\begin{aligned}
\text{minimize} \quad & x_1 + x_2 + 2x_3 + x_4 + 2x_5 + 2x_6 + 3x_7 + x_8 + 2x_9 + 2x_{10} \\
& \qquad +3x_{11} + 2x_{12} + 3x_{13} + 3x_{14} \\
\text{subject to} \quad & x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_9 \\
& \qquad +x_{10} + x_{11} + x_{12} + x_{13} + x_{14} \geq t \\
& x_1 + x_3 + x_5 + x_7 + x_8 + x_9 + x_{10} + x_{11} + x_{12} + x_{13} + x_{14} \geq t \\
& x_2 + x_3 + x_6 + x_7 + x_8 + x_9 + x_{10} + x_{11} + x_{12} + x_{13} + x_{14} \geq t \\
& x_4 + x_5 + x_6 + x_7 + x_8 + x_9 + x_{10} + x_{11} + x_{12} + x_{13} + x_{14} \geq t \\
& \\
& x_1 + x_2 + x_3 + x_5 + x_6 + x_7 + x_9 + x_{10} + x_{11} + x_{13} + x_{14} \leq t - 1 \\
& x_1 + x_3 + x_4 + x_5 + x_6 + x_7 + x_9 + x_{11} + x_{12} + x_{13} + x_{14} \leq t - 1 \\
& x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_{10} + x_{11} + x_{12} + x_{13} + x_{14} \leq t - 1 \\
& x_8 + x_9 + x_{10} + x_{11} + x_{12} + x_{13} + x_{14} \leq t - 1 \\
& \\
& x_k \geq 0, k = 1, 2, \ldots, 14
\end{aligned}$$

From Remark 4.6, we assume that $x_{15} = 0$. By solving $\mathrm{IP}_{\tilde{\rho}}(\Gamma_1)$,[2] we obtain that the value of the objective function is 5 which is attained by the following minimizers:

$$\tilde{x}_1 = \tilde{x}_2 = \tilde{x}_4 = 1,\ \tilde{x}_8 = 2,\ \tilde{x}_i = 0 \quad \text{for } i = 3, 5, 6, 7, 9, 10, \ldots, 14, \text{ and } \tilde{t} = 3. \tag{4.43}$$

Then, $\tilde{m}$ is given by $\tilde{m} = \sum_{k=1}^{14} \tilde{x}_k = 5$, and $\boldsymbol{X}_k$'s become

$$\boldsymbol{X}_1 = \left\{W_1^{(3)}\right\},\ \boldsymbol{X}_2 = \left\{W_2^{(3)}\right\},\ \boldsymbol{X}_4 = \left\{W_3^{(3)}\right\},\ \boldsymbol{X}_8 = \left\{W_4^{(3)}, W_5^{(3)}\right\}, \tag{4.44}$$

where $\boldsymbol{W}_{(3,5)} = \left\{W_1^{(3)}, W_2^{(3)}, \ldots, W_5^{(3)}\right\}$. Finally, from (4.37), $\tilde{\varphi}_{\Gamma_1}$ is constructed as

$$V_1 = \tilde{\varphi}_{\Gamma_1}(1) = \left\{W_1^{(3)}\right\}, \tag{4.45}$$

$$V_2 = \tilde{\varphi}_{\Gamma_1}(2) = \left\{W_2^{(3)}\right\}, \tag{4.46}$$

$$V_3 = \tilde{\varphi}_{\Gamma_1}(3) = \left\{W_3^{(3)}\right\}, \tag{4.47}$$

$$V_4 = \tilde{\varphi}_{\Gamma_1}(4) = \left\{W_4^{(3)}, W_5^{(3)}\right\}. \tag{4.48}$$

In this case, we have that $\tilde{\rho} = \frac{5}{4}$ and $\rho^* = 2$, which are smaller than the coding rates of ψ_{Γ_1} and ψ'_{Γ_1}. Integer programming problem $\mathrm{IP}_{\rho^*}(\Gamma_1)$ derives the same solutions as (4.43), and hence, it holds that $\tilde{\varphi}_{\Gamma_1} = \varphi^*_{\Gamma_1}$ in this example. □

[2]Integer programming problems in this Chapter are solved with the aid of a software program called `lp_solve` by M. Berkelaar available in `http://www.cs.sunysb.edu/~algorith/implement/lpsolve/implement.shtml`.

Example 4.8 For the access structure Γ_2 defined by (4.22) and (4.23) in Example 4.5, we can obtain the following multiple assignment map by solving integer programming problem $\mathrm{IP}_{\tilde{\rho}}(\Gamma_2)$.

$$V_1 = \tilde{\varphi}_{\Gamma_2}(1) = \left\{W_1^{(4)}\right\}, \tag{4.49}$$

$$V_2 = \tilde{\varphi}_{\Gamma_2}(2) = \left\{W_2^{(4)}\right\}, \tag{4.50}$$

$$V_3 = \tilde{\varphi}_{\Gamma_2}(3) = \left\{W_3^{(4)}\right\}, \tag{4.51}$$

$$V_4 = \tilde{\varphi}_{\Gamma_2}(4) = \left\{W_4^{(4)}, W_5^{(4)}\right\}, \tag{4.52}$$

$$V_5 = \tilde{\varphi}_{\Gamma_2}(5) = \left\{W_6^{(4)}\right\}, \tag{4.53}$$

where $W_i^{(4)} \in \boldsymbol{W}_{(4,6)}$. Then, it holds that $\tilde{\rho} = \frac{6}{5}$ and $\rho^* = 2$, which are smaller than the coding rates obtained by ψ_{Γ_2} and ψ'_{Γ_2}. We note that $\rho^* = 2$ is optimal because $\varphi^*_{\Gamma_2}(i)$ derived from $\mathrm{IP}_{\rho^*}(\Gamma_2)$ coincides with $\tilde{\varphi}_{\Gamma_2}$. □

Since any access structure can be realized by the cumulative map (and the modified cumulative map), there exists at least one multiple assignment map for any access structure. Therefore, the next theorem holds obviously.

Theorem 4.9 For any access structure Γ that satisfies monotonicity (2.3) and (2.4), integer programming problems $\mathrm{IP}_{\tilde{\rho}}(\Gamma)$ and $\mathrm{IP}_{\rho^*}(\Gamma)$ always have at least one feasible solution, and hence, there exists the optimal solution. □

Furthermore, it is also clear that the proposed construction method has the following properties.

Theorem 4.10 If Γ is a (k, n)-threshold access structure, the multiple assignment maps obtained from integer programming problems $\mathrm{IP}_{\tilde{\rho}}(\Gamma)$ and $\mathrm{IP}_{\rho^*}(\Gamma)$ satisfy that $|\tilde{\varphi}_\Gamma(i)| = |\varphi^*_\Gamma(i)| = 1$ for all i. □

Next, we clarify what kind of access structure can be realized as an ideal SS scheme by the multiple assignment map.

Theorem 4.11 For an access structure Γ, the SS scheme constructed by the optimal multiple assignment map is ideal, i.e., $\rho_i = 1$ for all i, if and only if $\mathcal{A}_1^-$ of Γ can be represented as

$$\mathcal{A}_1^- = \bigcup_{\substack{\forall\{j_1,j_2,\dots,j_t\} \\ \subseteq\{1,2,\dots,m\}}} \{\boldsymbol{A}_{j_1} \times \boldsymbol{A}_{j_2} \times \cdots \times \boldsymbol{A}_{j_t}\}, \tag{4.54}$$

where t is a positive integer and $\{\boldsymbol{A}_1, \boldsymbol{A}_2, \dots, \boldsymbol{A}_m\}$ is a partition of $\boldsymbol{V}$ which satisfies

$$\bigcup_{j=1}^{m} \boldsymbol{A}_j = \boldsymbol{V}, \tag{4.55}$$

$$\boldsymbol{A}_j \neq \emptyset \quad \text{for } j = 1, 2, \dots, m, \tag{4.56}$$

$$\boldsymbol{A}_j \cap \boldsymbol{A}_{j'} = \emptyset \quad \text{if } j \neq j'. \tag{4.57}$$

□

Proof of Theorem 4.11 If there exists such a partition $\{\boldsymbol{A}_1, \boldsymbol{A}_2, \ldots, \boldsymbol{A}_m\}$ satisfying (4.54)–(4.57) for the access structure Γ, an ideal SS scheme can be obtained by letting

$$\varphi_\Gamma(i) = W_j^{(t)} \quad \text{if } V_i \in \boldsymbol{A}_j \tag{4.58}$$

for each $i = 1, 2, \ldots, n$. Next, we show the necessity of (4.54)–(4.57). Suppose that $\rho_i = 1$ holds for all i. Then, we can consider the inverse map of Φ_Γ such that $\Phi_\Gamma^{-1} : \boldsymbol{W}_{(t,m)} \to 2$ satisfies

$$\Phi_\Gamma^{-1}\left(W_j^{(t)}\right) = \boldsymbol{A}_j \tag{4.59}$$

for all $j = 1, 2, \ldots, m$. Hence, $\boldsymbol{A}_j$ satisfies (4.54), (4.55) and (4.56). Furthermore, if there exist $\boldsymbol{A}_j$ and $\boldsymbol{A}_{j'}$, $j \neq j'$, not satisfying (4.57), there exists a share $V_i \in \boldsymbol{A}_j \cap \boldsymbol{A}_{j'}$. This means $\varphi_\Gamma(i) \supseteq \left\{W_j^{(t)}, W_{j'}^{(t)}\right\}$, which contradicts $\rho_i = |\varphi_\Gamma(i)| = 1$. □

In the case of $t = 2$, it is known that an access structure Γ can be realized by an ideal SS scheme if and only if Γ can be represented by a complete multipartite graph [17]. We note that this condition coincides with (4.54)–(4.57) in this case. Furthermore, in the case that $|\boldsymbol{A}_j| = 1$ for $j = 1, 2, \ldots, m$, the access structure coincides with the (t, m)-threshold access structure.

We note that any access structures not satisfying (4.54)–(4.57) must have $\tilde{\rho} > 1$ and $\rho^* \geq 2$ if the multiple assignment map are used. But, an access structure not satisfying (4.54)–(4.57) might be realized as an ideal SS scheme if we use another construction method. For example, refer [104].

We also note that integer programming problems are NP-hard, and hence, the proposed algorithms may take much time in solving for large $n\ (= |\boldsymbol{V}|)$. But, in the case that n is not large, the solution is obtained quickly. For instance, integer programming problem $\mathrm{IP}_\rho(\Gamma_3)$ for the access structure Γ_3 with $n = 6$ in the next example can be solved within 0.1 seconds by a notebook computer.

Example 4.12 Consider the following access structure Γ_3:

$$\begin{aligned}\mathcal{A}_1^- = \{&\{V_1, V_3, V_4, V_5\}, \{V_1, V_3, V_5, V_6\}, \{V_1, V_4, V_5, V_6\}, \{V_3, V_4, V_5, V_6\}, \{V_1, V_2, V_3\},\\ &\{V_1, V_2, V_5\}, \{V_1, V_2, V_6\}, \{V_2, V_3, V_4\}, \{V_2, V_3, V_5\}, \{V_2, V_3, V_6\}, \{V_2, V_4, V_5\},\\ &\{V_2, V_4, V_6\}, \{V_2, V_5, V_6\}\},\end{aligned} \tag{4.60}$$

$$\begin{aligned}\mathcal{A}_0^+ = \{&\{V_1, V_3, V_4, V_6\}, \{V_1, V_2, V_4\}, \{V_1, V_3, V_5\}, \{V_1, V_4, V_5\}, \{V_1, V_5, V_6\}, \{V_3, V_4, V_5\},\\ &\{V_3, V_5, V_6\}, \{V_4, V_5, V_6\}, \{V_2, V_3\}, \{V_2, V_5\}, \{V_2, V_6\}\}.\end{aligned} \tag{4.61}$$

Then, we obtain the following multiple assignment map by solving $\mathrm{IP}_{\tilde{\rho}}(\Gamma_3)$.

$$V_1 = \tilde{\varphi}_{\Gamma_3}(1) = \left\{W_1^{(6)}, W_2^{(6)}\right\}, \tag{4.62}$$

$$V_2 = \tilde{\varphi}_{\Gamma_3}(2) = \left\{W_1^{(6)}, W_3^{(6)}, W_4^{(6)}, W_5^{(6)}\right\}, \tag{4.63}$$

$$V_3 = \tilde{\varphi}_{\Gamma_3}(3) = \left\{W_6^{(6)}\right\}, \tag{4.64}$$

$$V_4 = \tilde{\varphi}_{\Gamma_3}(4) = \left\{W_2^{(6)}, W_5^{(6)}\right\}, \tag{4.65}$$

$$V_5 = \tilde{\varphi}_{\Gamma_3}(5) = \left\{ W_3^{(6)}, W_7^{(6)} \right\}, \tag{4.66}$$

$$V_6 = \tilde{\varphi}_{\Gamma_3}(6) = \left\{ W_8^{(6)} \right\}, \tag{4.67}$$

where $W_i^{(6)} \in \boldsymbol{W}_{(6,8)}$. $\tilde{\varphi}_{\Gamma_3}$ attains that $\tilde{\rho} = 2$ and $\rho^* = 4$. On the other hand, the cumulative map ψ_{Γ_3} for the access structure Γ_3 are given by

$$V_1 = \psi_{\Gamma_3}(1) = \left\{ W_6^{(11)}, W_7^{(11)}, W_8^{(11)}, W_9^{(11)}, W_{10}^{(11)}, W_{11}^{(11)} \right\}, \tag{4.68}$$

$$V_2 = \psi_{\Gamma_3}(2) = \left\{ W_1^{(11)}, W_3^{(11)}, W_4^{(11)}, W_5^{(11)}, W_6^{(11)}, W_7^{(11)}, W_8^{(11)} \right\}, \tag{4.69}$$

$$V_3 = \psi_{\Gamma_3}(3) = \left\{ W_2^{(11)}, W_4^{(11)}, W_5^{(11)}, W_8^{(11)}, W_{10}^{(11)}, W_{11}^{(11)} \right\}, \tag{4.70}$$

$$V_4 = \psi_{\Gamma_3}(4) = \left\{ W_3^{(11)}, W_5^{(11)}, W_7^{(11)}, W_9^{(11)}, W_{10}^{(11)}, W_{11}^{(11)} \right\}, \tag{4.71}$$

$$V_5 = \psi_{\Gamma_3}(5) = \left\{ W_1^{(11)}, W_2^{(11)}, W_9^{(11)}, W_{11}^{(11)} \right\}, \tag{4.72}$$

$$V_6 = \psi_{\Gamma_3}(6) = \left\{ W_2^{(11)}, W_3^{(11)}, W_4^{(11)}, W_6^{(11)}, W_9^{(11)}, W_{10}^{(11)} \right\}, \tag{4.73}$$

where $W_i^{(11)} \in \boldsymbol{W}_{(11,11)}$. ψ_{Γ_3} has $\tilde{\rho} = \frac{35}{6}$ and $\rho^* = 7$. Furthermore, the modified cumulative map for Γ_3, ψ'_{Γ_3}, requires a $(12, 15)$-threshold SS scheme and has $\tilde{\rho} = \frac{31}{6}$ and $\rho^* = 9$. □

In this thesis, we assume that every share is significant. But, if there exist vacuous shares in an access structure Γ, it is cumbersome to check whether each share is significant or vacuous. From Remark 2.7, the optimal multiple assignment map $\tilde{\varphi}_\Gamma$ attaining the minimum average coding rate must satisfy that $|\tilde{\varphi}_\Gamma(i)| = 0$ for any vacuous share V_i. On the other hand, it clearly holds that $|\varphi_\Gamma(i)| \geq 1$ for every significant share V_i since $\rho_i \geq 1$ holds for any significant share. Hence, by solving integer programming problem $\mathrm{IP}_{\tilde{\rho}}(\Gamma)$, we can know whether each share is significant or vacuous.

4.4 Multiple Assignment Maps for Incomplete Access Structures

In the previous sections, we considered how to construct a SS scheme for a complete general access structure $\Gamma = \{\mathcal{A}_1, \mathcal{A}_0\}$. But in practice, it may be cumbersome to specify whether each subset of $\boldsymbol{V}$ is a qualified set or a forbidden set because the number of subsets is 2^n. Hence, a method is proposed in [49] to construct a SS scheme even for the case that we don't care the properties of some subsets of $\boldsymbol{V}$.

We consider only the minimum average coding rate in this section. But, for the minimum worst coding rate, integer programming can be formulated in the similar way.

Theorem 4.13 (Itoh et al. [49]) Let $\Gamma^\sharp = \{\mathcal{A}_1^\sharp, \mathcal{A}_0^\sharp\}$ be an incomplete access structure, which has $\mathcal{A}_1^\sharp \cup \mathcal{A}_0^\sharp \neq 2^{\boldsymbol{V}}$. Then, there exists a complete access structure $\Gamma = \{\mathcal{A}_1, \mathcal{A}_0\}$ such that

$$\mathcal{A}_1^\sharp \subseteq \mathcal{A}_1, \tag{4.74}$$

$$\mathcal{A}_0^\sharp \subseteq \mathcal{A}_0, \tag{4.75}$$

if and only if it holds that for any $\boldsymbol{A} \in \mathcal{A}_1^\sharp$ and $\boldsymbol{B} \in \mathcal{A}_0^\sharp$,

$$\boldsymbol{A} \not\subseteq \boldsymbol{B}. \tag{4.76}$$

□

In the case that (4.76) is satisfied, a SS scheme with the incomplete access structure $\Gamma^\sharp = \{\mathcal{A}_1^\sharp, \mathcal{A}_0^\sharp\}$ can be realized by applying the cumulative map to the complete access structure $\Gamma = \{\mathcal{A}_1, \mathcal{A}_0\}$. In fact, for the access structure $\Gamma^\sharp = \{\mathcal{A}_1^\sharp, \mathcal{A}_0^\sharp\}$, a SS scheme is constructed in [49] by letting $\psi_{\Gamma^\sharp}(i) = \bigcup_{j:V_i \notin \ \ _j} \{W_j^{(t)}\}$ for $\mathcal{A}_0^{\sharp +} = \{\boldsymbol{F}_1, \boldsymbol{F}_2, \ldots, \boldsymbol{F}_m\}$. This construction corresponds to the case that

$$\mathcal{A}_0^+ = \mathcal{A}_0^{\sharp +} \text{ and } \mathcal{A}_1 = 2^{\ \ } - \mathcal{A}_0. \tag{4.77}$$

However, $\psi_{\Gamma^\sharp}$ is not efficient generally because $\psi_{\Gamma^\sharp}$ is based on the cumulative map, which is inefficient as described in Section 4.2. Furthermore, (4.77) may not be the optimal complete access structure to use the cumulative map for the given incomplete access structure $\Gamma^\sharp$.

In our construction based on integer programming, the optimal multiple assignment map for the incomplete access structure $\Gamma^\sharp = \{\mathcal{A}_1^{\sharp -}, \mathcal{A}_0^{\sharp +}\}$ can easily be obtained by applying $\mathrm{IP}_{\tilde{\rho}}(\Gamma)$ or $\mathrm{IP}_{\rho^*}(\Gamma)$ directly to $\Gamma^\sharp$.

Example 4.14 Let us consider the following access structure $\Gamma_3^\sharp = \{\mathcal{A}_1^\sharp, \mathcal{A}_0^\sharp\}$:

$$\mathcal{A}_1^\sharp = \{\{V_1, V_4, V_5, V_6\}, \{V_1, V_2, V_5\}, \{V_1, V_2, V_6\}, \{V_2, V_3, V_6\}, \{V_2, V_4, V_6\}\}, \tag{4.78}$$

$$\mathcal{A}_0^\sharp = \{\{V_1, V_3, V_4, V_6\}, \{V_1, V_3, V_5\}, \{V_1, V_5, V_6\}, \{V_3, V_4, V_5\}, \{V_4, V_5, V_6\}, \{V_2, V_5\}\}, \tag{4.79}$$

Note that $\mathcal{A}_1^\sharp$ and $\mathcal{A}_0^\sharp$ satisfy $\mathcal{A}_1^\sharp \subseteq \mathcal{A}_1^-$ and $\mathcal{A}_0^\sharp \subseteq \mathcal{A}_0^+$ for $\Gamma_3 = \{\mathcal{A}_1, \mathcal{A}_0\}$, which is defined by (4.60) and (4.61) in Example 4.12. Then, by solving $\mathrm{IP}_{\tilde{\rho}}(\Gamma_3^\sharp)$, we obtain the following multiple assignment map.

$$V_1 = \varphi_{\tilde{\Gamma}_3^\sharp}(1) = \left\{W_1^{(4)}\right\}, \tag{4.80}$$

$$V_2 = \varphi_{\tilde{\Gamma}_3^\sharp}(2) = \left\{W_2^{(4)}, W_3^{(4)}\right\}, \tag{4.81}$$

$$V_3 = \varphi_{\tilde{\Gamma}_3^\sharp}(3) = \left\{W_4^{(4)}\right\}, \tag{4.82}$$

$$V_4 = \varphi_{\tilde{\Gamma}_3^\sharp}(4) = \left\{W_4^{(4)}\right\}, \tag{4.83}$$

$$V_5 = \varphi_{\tilde{\Gamma}_3^\sharp}(5) = \left\{W_5^{(4)}\right\}, \tag{4.84}$$

$$V_6 = \varphi_{\tilde{\Gamma}_3^\sharp}(6) = \left\{W_6^{(4)}\right\}, \tag{4.85}$$

where $W_i^{(4)} \in \boldsymbol{W}_{(4,6)}$, and it holds that $\tilde{\rho} = \frac{7}{6}$ and $\rho^* = 2$. If we apply the cumulative map to $\Gamma_3^\sharp$, $\psi_{\Gamma_3^\sharp}$ is constructed from a $(6,6)$-threshold scheme, and it has $\tilde{\rho} = 3$ and $\rho^* = 5$. Finally we note that $\tilde{\rho} = \frac{7}{6}$ and $\rho^* = 2$ are smaller than the rates of Γ_3 obtained in Example 4.12. □

Similarly to the case of complete SS schemes, if there exist vacuous shares V_i in $\Gamma^\sharp = \{\mathcal{A}_1^\sharp, \mathcal{A}_0^\sharp\}$, we can know them from $|\tilde{\varphi}_{\Gamma^\sharp}(i)| = 0$ by solving $\mathrm{IP}_{\tilde{\rho}}(\Gamma^\sharp)$.

4.5 Ramp Secret Sharing schemes with General Access Structures

In this section, we treat the construction of ramp SS schemes based on the multiple assignment maps. We consider only the minimum average coding rate in this section. But, for the minimum worst coding rate, integer programming can be formulated in the similar way. Furthermore, we also assume that access structures are complete although the case of incomplete access structures with $\bigcup_{j=0}^{L} \mathcal{A}_j \neq 2$ can be treated in the same way as Section 4.4.

4.5.1 Preliminaries

Ramp SS schemes can be constructed if and only if the following conditions are satisfied.

Theorem 4.15 (Kurosawa et al. [71]) A ramp SS scheme with access structure $\Gamma^R = \{\mathcal{A}_0, \mathcal{A}_1, \ldots, \mathcal{A}_L\}$ can be constructed if and only if $\check{\mathcal{A}}_j$ (or $\hat{\mathcal{A}}_j$) satisfies the monotonicity (3.8) (or (3.9)) for all $j = 1, 2, \ldots, L$, where $\check{\mathcal{A}}_j$ and $\hat{\mathcal{A}}_j$ are defined in (3.6) and (3.7). □

In Theorem 4.15, the necessity of the condition is obvious, and the sufficiency is established by the next construction.

Construction 4.16 (Kurosawa et al. [71]) Let $S = \left\{S^{\langle 1\rangle}, S^{\langle 2\rangle}, \ldots, S^{\langle L\rangle}\right\}$ be a secret, and let $\Gamma^{\langle j\rangle} = \left\{\check{\mathcal{A}}_j, 2^{} - \check{\mathcal{A}}_j\right\}$, $j = 1, 2, \ldots, L$, be the perfect access structures obtained from a given access structure Γ^R. Since each $\Gamma^{\langle j\rangle}$ is a perfect access structure satisfying the monotonicity (2.3) and (2.4), we can construct a SS scheme for secret $S^{\langle j\rangle}$ and $\Gamma^{\langle j\rangle}$. Letting $\{W_1^{\langle j\rangle}, W_2^{\langle j\rangle}, \ldots, W_n^{\langle j\rangle}\}$ be shares for $S^{\langle j\rangle}$ and $\Gamma^{\langle j\rangle}$, the share $V_i = \{W_i^{\langle 1\rangle}, W_i^{\langle 2\rangle}, \ldots, W_i^{\langle L\rangle}\}$ realizes the access structure Γ^R. For Γ^R, a ramp SS scheme can also be constructed from $\left\{2^{} - \hat{\mathcal{A}}_j, \hat{\mathcal{A}}_j\right\}$ instead of $\Gamma^{\langle j\rangle} = \left\{2^{} - \check{\mathcal{A}}_j, \check{\mathcal{A}}_j\right\}$. □

Remark 4.17 Note that in Construction 4.16, we have $\rho_i \geq 1$ for any access structure. For example, in the case that Construction 4.16 is applied to a (k, L, n)-threshold access structure, the constructed ramp SS scheme has $\rho_i = 1$ although the (k, L, n)-threshold SS scheme can be realized with $\rho_i = \frac{1}{L}$. Therefore, Construction 4.16 is not efficient generally. □

Example 4.18 Consider the following ramp access structure Γ_4^R for $\boldsymbol{V} = \{V_1, V_2, V_3, V_4\}$:

$$\mathcal{A}_3 = \{\{V_1, V_2, V_3, V_4\}\}, \tag{4.86}$$
$$\mathcal{A}_2 = \{\{V_1, V_2, V_3\}, \{V_1, V_3, V_4\}\}, \tag{4.87}$$
$$\mathcal{A}_1 = \{\{V_1, V_2, V_4\}, \{V_2, V_3, V_4\}\}, \tag{4.88}$$
$$\mathcal{A}_0 = \{\boldsymbol{A} : 0 \leq |\boldsymbol{A}| \leq 2\}. \tag{4.89}$$

By Construction 4.16, we obtain that $V_1 = \{P_1^{(3)}, Q_1^{(3)}, R_1^{(4)}\}$, $V_2 = \{P_2^{(3)}, Q_2^{(3)}, R_2^{(4)}\}$, $V_3 = \{P_3^{(3)}, Q_3^{(3)}, R_3^{(4)}\}$, $V_4 = \{P_4^{(3)}, Q_2^{(3)}, R_4^{(4)}\}$, where $R_i^{(4)} \in \boldsymbol{W}_{(4,4)}$, $Q_i^{(3)} \in \boldsymbol{W}_{(3,3)}$, $P_i^{(3)} \in \boldsymbol{W}_{(3,4)}$. Since each share consists of three primitive shares for three secrets $S^{\langle 1\rangle}$, $S^{\langle 2\rangle}$, $S^{\langle 3\rangle}$, the constructed ramp SS scheme has $\tilde{\rho} = \rho^* = 1$. □

Remark 4.19 In Construction 4.16, any $\boldsymbol{A} \in \mathcal{A}_j$ can decode $S^{\langle 1 \rangle}, S^{\langle 2 \rangle}, \ldots, S^{\langle j \rangle}$. In other words, $\boldsymbol{A} \in \mathcal{A}_j$ expose some parts of the secret $S = \left\{S^{\langle 1 \rangle}, S^{\langle 2 \rangle}, \ldots, S^{\langle L \rangle}\right\}$. Since it is insecure in part, such ramp SS schemes are called *weak* ramp SS schemes [119]. On the other hand, *strong* ramp SS schemes are also defined in [119]. The strong ramp SS scheme requires that for any $\boldsymbol{A} \in \mathcal{A}_j$ and $\{\ell_1, \ell_2, \ldots, \ell_u\} \subseteq \{1, 2, \ldots, L\}$, $1 \le u \le L - j$,

$$H\left(S^{\langle \ell_1 \rangle}, S^{\langle \ell_2 \rangle}, \ldots, S^{\langle \ell_u \rangle} \middle| \boldsymbol{A}\right) = \frac{u}{L} H(S) \tag{4.90}$$

in addition to (3.2)–(3.4). Note that the ramp SS scheme given by (3.58)–(3.62) in Example 3.18 is an example of weak ramp SS schemes since S_1 and S_2 exposes to V_1 and V_2, respectively. On the other hand, the (k, L, n)-threshold ramp SS scheme given by (3.5) is an example of strong ramp SS scheme.

It is easy to convert a weak ramp SS scheme to a strong one by transforming the tuple of the secret as follows:

$$\begin{bmatrix} S'^{\langle 1 \rangle} \\ S'^{\langle 2 \rangle} \\ \vdots \\ S'^{\langle L \rangle} \end{bmatrix} = M \begin{bmatrix} S^{\langle 1 \rangle} \\ S^{\langle 2 \rangle} \\ \vdots \\ S^{\langle L \rangle} \end{bmatrix}, \tag{4.91}$$

where M is an $L \times L$ non-singular matrix defined on a finite field. If we select M adequately and encrypt $\left\{S'^{\langle 1 \rangle}, S'^{\langle 2 \rangle}, \ldots, S'^{\langle L \rangle}\right\}$ instead of the original secret $S = \left\{S^{\langle 1 \rangle}, S^{\langle 2 \rangle}, \ldots, S^{\langle L \rangle}\right\}$, the obtained ramp SS scheme becomes strong for S. □

The construction of ramp SS schemes for general access structures are treated in [103]. But, since the construction in [103] is based on *monotone span programming*, it is much complicated compared with the multiple assignment map.

4.5.2 Optimal Multiple Assignment Maps for Ramp Secret Sharing Schemes

First, let $\boldsymbol{W}_{(t,L,m)} = \{W_1^{(t,L)}, W_2^{(t,L)}, \ldots, W_m^{(t,L)}\}$ be the set of primitive shares for a (t, L, m)-threshold ramp SS scheme with coding rate $\rho_i = \frac{1}{L}$. Then, the optimal ramp SS scheme by the multiple assignment map for a general access structure Γ^R can be obtained by solving the following integer programming problem:

$$\begin{array}{ll}
\underline{\mathrm{IP}_{\vec{\rho}}(\Gamma)} & \\
\text{minimize} & \boldsymbol{h} \cdot \boldsymbol{x} \\
\text{subject to} & \boldsymbol{a}(\boldsymbol{A}) \cdot \boldsymbol{x} \ge t \quad \text{for} \quad \boldsymbol{A} \in \mathcal{A}_L^- \\
& \boldsymbol{a}(\boldsymbol{A}) \cdot \boldsymbol{x} = t - j \quad \text{for} \quad \boldsymbol{A} \in \mathcal{A}_j^+ \cup \mathcal{A}_j^- \quad \text{for} \quad 1 \le j \le L - 1 \qquad (\star) \\
& \boldsymbol{a}(\boldsymbol{A}) \cdot \boldsymbol{x} \le t - L \quad \text{for} \quad \boldsymbol{A} \in \boldsymbol{V} \\
& \boldsymbol{x} \ge \boldsymbol{0}
\end{array}$$

Remark 4.20 From the monotonicity defined in (3.8) and (3.9), it is sufficient to consider only $\boldsymbol{A} \in \mathcal{A}_j^+ \cup \mathcal{A}_j^-$ instead of all $\boldsymbol{A} \in \mathcal{A}_j$ on the marked line $(\star)$ in $\mathrm{IP}_{\tilde{\rho}}^R\left(\Gamma^R\right)$. Note that in the case of $\mathcal{A}_0 \neq \emptyset$ in ramp SS schemes, the same primitive shares may be distributed to all the shares. Hence, we may have $x_N \neq 0$ in ramp SS schemes although we can always assume that $x_N = 0$ in perfect SS schemes. □

From Definition 3.5 and Corollary 3.6, non-vacuous shares V_i must satisfy that $|\varphi_\Gamma(i)| \geq 1$ for any multiple assignment map φ_Γ. On the other hand, $|\tilde{\varphi}_\Gamma(i')| = 0$ must hold for vacuous shares $V_{i'}$ in the optimal multiple assignment map $\tilde{\varphi}_\Gamma$ attaining the minimal average coding rate.

Example 4.21 If the access structures Γ_4^R in Example 4.18 is applied to integer programming problem $\mathrm{IP}_{\tilde{\rho}}^R\left(\Gamma_4^R\right)$, the following multiple assignment map is obtained

$$V_1 = \varphi_{\Gamma_4^R}(1) = \left\{W_1^{(7,3)}, W_2^{(7,3)}\right\}, \tag{4.92}$$

$$V_2 = \varphi_{\Gamma_3^R}(2) = \left\{W_3^{(7,3)}, W_4^{(7,3)}\right\}, \tag{4.93}$$

$$V_3 = \varphi_{\Gamma_4^R}(3) = \left\{W_5^{(7,3)}, W_6^{(7,3)}\right\}, \tag{4.94}$$

$$V_4 = \varphi_{\Gamma_4^R}(4) = \left\{W_3^{(7,3)}, W_7^{(7,3)}\right\}, \tag{4.95}$$

where $W_i^{(7,3)} \in \boldsymbol{W}_{(7,3,7)}$. $\varphi_{\Gamma_4}^R$ attains that $\tilde{\rho} = \rho^* = \frac{2}{3}$. □

We note that the coding rates less than 1 cannot be achieved by Construction 4.16. Furthermore, our construction is much simple compared with the method in [103]. But, unfortunately, the integer programming problem may not have any feasible solutions in the case of ramp SS schemes.

Example 4.22 The following access structure Γ_5^R cannot be constructed by any multiple assignment map since the corresponding integer programming problem has no feasible solution.

$$\mathcal{A}_4^- = \{\{V_1, V_2, V_3, V_4\}, \{V_1, V_2, V_4, V_5\}, \{V_2, V_3, V_4, V_5\}\}, \tag{4.96}$$

$$\mathcal{A}_3 = \{\{V_1, V_2, V_3, V_5\}, \{V_1, V_3, V_4, V_5\}, \{V_1, V_2, V_3\}, \{V_1, V_2, V_4\}, \{V_1, V_3, V_4\}, \{V_1, V_3, V_5\}, \{V_2, V_3, V_4\}\}, \tag{4.97}$$

$$\mathcal{A}_2 = \{\{V_1, V_2, V_5\}, \{V_1, V_4, V_5\}, \{V_2, V_3, V_5\}, \{V_2, V_4, V_5\}, \{V_3, V_4, V_5\}, \{V_1, V_3\}, \{V_1, V_5\}\}, \tag{4.98}$$

$$\mathcal{A}_1 = \{\{V_1, V_2\}, \{V_2, V_3\}, \{V_3, V_4\}\}, \tag{4.99}$$

$$\mathcal{A}_0^+ = \{\{V_1, V_4\}, \{V_2, V_5\}, \{V_3, V_5\}\}. \tag{4.100}$$

□

In this case, we can modify the definition of ramp SS schemes given by (3.1) as follows.

$$H(S|\boldsymbol{A}) = 0, \qquad \text{for all } \boldsymbol{A} \in \mathcal{A}_L, \tag{4.101}$$

$$H(S|\boldsymbol{A}) \geq \frac{L-j}{L} H(S), \quad \text{for all } \boldsymbol{A} \in \mathcal{A}_j,\ 1 \leq j \leq L-1, \tag{4.102}$$

$$H(S|\boldsymbol{A}) = H(S), \qquad \text{for all } \boldsymbol{A} \in \mathcal{A}_0. \tag{4.103}$$

In order to implement (4.101)–(4.103) in the integer programming, it suffices to replace the marked line $(\star)$ in $\mathrm{IP}_{\tilde{\rho}}^{R}\left(\Gamma^{R}\right)$ by $\boldsymbol{a}(\boldsymbol{A}_j)\cdot\boldsymbol{x}\le t-j$. Letting $\mathrm{IP}_{\tilde{\rho}}^{R2}\left(\Gamma^{R}\right)$ be the modified integer programming problem, the next theorem holds.

Theorem 4.23 The integer programming problem $\mathrm{IP}_{\tilde{\rho}}^{R2}\left(\Gamma^{R}\right)$ always has at least one feasible solution for any ramp access structure Γ^{R}. □

Proof of Theorem 4.23 Let $\mathcal{V}$ be a multiset in $2^{\{1,2,\ldots,n\}}$, some elements of which may be the same. Then, for $\mathcal{V}$ and $\boldsymbol{A}\subseteq\mathcal{V}$, we define $N(\mathcal{V},\boldsymbol{A})$ as follows.

$$N(\mathcal{V},\boldsymbol{A})=\left|\{\boldsymbol{A}'\in\mathcal{V}:\boldsymbol{A}\subseteq\boldsymbol{A}'\}\right|, \tag{4.104}$$

where all $\boldsymbol{A}'\in\mathcal{V}$ are treated as different ones even if some of them are the same. Now we construct a multiset $\mathcal{U}$ from $\Gamma^{R}=\{\mathcal{A}_0,\mathcal{A}_1,\ldots,\mathcal{A}_L\}$ by the next construction.

Construction 4.24

(1) Let $\mathcal{U}:=\emptyset$ and $j:=1$.

(2) For each $\boldsymbol{A}\in\mathcal{A}_{L-j}^{+}$ satisfying $N(\mathcal{U},\boldsymbol{A})<j$, we add $\boldsymbol{A}$ into $\mathcal{U}$, $(j-N(\mathcal{U},\boldsymbol{A}))$ times.

(3) Let $j:=j+1$.

(4) If $j<L$, go to (2). In case of $j=L$, go to (5).

(5) Output $\mathcal{U}$. □

From the monotonicity of $\check{\mathcal{A}}_j$ in (3.8), family $\mathcal{U}$ can always be constructed. Then, letting $\mathcal{U}=\{\boldsymbol{F}_1,\boldsymbol{F}_2,\ldots,\boldsymbol{F}_m\}$, we can define a map $\check{\psi}:\{1,2,\ldots,n\}\to 2^{(m,L,m)}$ by

$$\check{\psi}(i)=\bigcup_{j:V_i\notin\ _j}\left\{W_j^{(m,L)}\right\}, \tag{4.105}$$

where $W_j^{(m,L)}\in\boldsymbol{W}_{(m,L,m)}$. Noting that in the case of $L=1$, (4.105) coincides with the cumulative map in (4.7), it is easily shown that share $V_i=\check{\psi}(i)$ satisfies (4.101)–(4.103). Hence, $\mathrm{IP}_{\tilde{\rho}}^{R2}\left(\Gamma^{R}\right)$ always has at least one feasible solution. □

Note that as shown in the following example, Construction 4.24 does not give the optimal assignments of primitive shares generally.

Example 4.25 Assume that the access structure Γ_5^{R} in (4.96)–(4.100) satisfies the conditions (4.101)–(4.103). First, we apply Construction 4.24 to the access structure Γ_5^{R}. Then, we obtain the following multiset $\mathcal{U}_{\Gamma_5^{R}}$.

$$\begin{aligned}\mathcal{U}_{\Gamma_5^{R}}=\{&\{V_1,V_2,V_3,V_5\},\{V_1,V_3,V_4,V_5\},\{V_1,V_2,V_4\},\{V_1,V_2,V_5\},\{V_1,V_4,V_5\},\{V_2,V_3,V_5\},\\&\{V_2,V_3,V_4\},\{V_2,V_4,V_5\},\{V_2,V_4,V_5\},\{V_3,V_4,V_5\},\{V_1,V_4\}\}.\end{aligned} \tag{4.106}$$

Hence, we can obtain $V_i = \check{\psi}(i)$, $i = 1, 2, \ldots, 5$, as follows:

$$V_1 = \check{\psi}(1) = \left\{ W_6^{(11,4)}, W_7^{(11,4)}, W_8^{(11,4)}, W_9^{(11,4)}, W_{10}^{(11,4)} \right\}, \tag{4.107}$$

$$V_2 = \check{\psi}(2) = \left\{ W_2^{(11,4)}, W_5^{(11,4)}, W_{10}^{(11,4)}, W_{11}^{(11,4)} \right\}, \tag{4.108}$$

$$V_3 = \check{\psi}(3) = \left\{ W_3^{(11,4)}, W_4^{(11,4)}, W_5^{(11,4)}, W_8^{(11,4)}, W_9^{(11,4)}, W_{11}^{(11,4)} \right\}, \tag{4.109}$$

$$V_4 = \check{\psi}(4) = \left\{ W_1^{(11,4)}, W_4^{(11,4)}, W_6^{(11,4)} \right\}, \tag{4.110}$$

$$V_5 = \check{\psi}(5) = \left\{ W_3^{(11,4)}, W_7^{(11,4)}, W_{11}^{(11,4)} \right\}, \tag{4.111}$$

where $W_i \in \boldsymbol{W}_{(11,4,11)}$. Then, we have $\tilde{\rho} = \frac{21}{20}$ and $\rho^* = \frac{3}{2}$ since it holds that $H(W_i^{(11,4)}) = \frac{1}{4}H(S)$ for each i.

On the other hand, we can construct the following multiple assignment map $\tilde{\varphi}_{\Gamma_5}$ by solving integer programming problem $\mathrm{IP}_{\tilde{\rho}}^{R2}(\Gamma_5^R)$.

$$V_1 = \varphi_{\Gamma_5^R}(1) = \left\{ W_1^{(8,4)}, W_2^{(8,4)} \right\}, \tag{4.112}$$

$$V_2 = \varphi_{\Gamma_5^R}(2) = \left\{ W_3^{(8,4)}, W_4^{(8,4)}, W_5^{(8,4)} \right\}, \tag{4.113}$$

$$V_3 = \varphi_{\Gamma_5^R}(3) = \left\{ W_2^{(8,4)}, W_6^{(8,4)} \right\}, \tag{4.114}$$

$$V_4 = \varphi_{\Gamma_5^R}(4) = \left\{ W_7^{(8,4)}, W_8^{(8,4)} \right\}, \tag{4.115}$$

$$V_5 = \varphi_{\Gamma_5^R}(5) = \left\{ W_9^{(8,4)} \right\}, \tag{4.116}$$

where $W_i^{(8,4)} \in \boldsymbol{W}_{(8,4,9)}$, and it holds that $\tilde{\rho} = \frac{1}{2}$, and $\rho^* = \frac{3}{4}$. Note that (4.107)–(4.111) and (4.112)–(4.116) do not satisfy (3.1) but satisfy (4.101)–(4.103). For instance, in (4.112)–(4.116), it holds for $\{V_1, V_5\} \in \mathcal{A}_2$ that $H(S|V_1V_5) = H(S) > \frac{1}{2}H(S)$.

Finally, consider the case that we apply Construction 4.16 to access structure Γ_5^R. If we use the cumulative map for each perfect SS scheme of access structure $\Gamma_5^{\langle j \rangle}$, $j = 1, 2, 3, 4$, we obtain $\tilde{\rho} = \frac{9}{5}$ and $\rho^* = 2$, which are very inefficient. □

4.6 Conclusion

We proposed a method to construct SS schemes for any given general access structures from (t, m)-threshold SS schemes based on integer programming. The proposed method can attain the *optimal* average and/or worst coding rates in the sense of multiple assignment maps. Hence, the proposed method can attain smaller coding rates compared with the cumulative maps and the modified cumulative maps. Furthermore, the proposed method can be applied to incomplete and/or ramp access structures.

Chapter 5

Conclusions of Part I

5.1 Summary of Results

In Part I, we discussed SS schemes from the viewpoints of coding rates and construction methods.

In Chapter 3, we evaluated the lower bounds of coding rates for ramp SS schemes. We pointed out that there may exist non-significant shares in ramp SS schemes although all shares can be assumed to be significant in perfect SS schemes. Based on such facts, we classified the shares of ramp SS schemes into three categories, i.e., super-additive, additive, and sub-additive, and we proved that the lower bound of the coding rate for sub-additives share is strictly larger than that of the other two types of shares. Then, we defined a well-realized ramp SS scheme as an extension of an ideal perfect SS scheme, and we showed that ramp SS schemes cannot be well-realized if it has sub-additive shares. Finally in Chapter 3, we derived a theorem to discriminate the access structure that cannot be well-realized even if it consists of additive and super-additive shares. We also showed from the theorem that some examples of access structures in [15] cannot be well-realized.

In Chapter 4, we proposed a new efficient construction method of perfect SS schemes for general access structures based on (t, m)-threshold SS schemes and integer programming. Our method uses the *multiple assignment* scheme proposed by Ito et al. [47]–[49]. In the multiple assignment schemes, the shares of (t, m)-threshold SS schemes called *primitive* shares are assigned to each share of a given general access structure in such a way that t or more primitive shares are assigned to qualified sets, but $t - 1$ or less primitive shares are assigned to forbidden sets. The *cumulative map* proposed by Ito et al. [47]–[49] is a simple realization of the multiple assignment scheme, but it is inefficient, especially in the case that access structures are close to (k, n)-threshold access structures. Furthermore, although the *modified* cumulative map [109] is proposed to overcome such defects, it is not always efficient. Hence, we designed the multiple assignment map that can minimize the average or worst coding rates using integer programming, and we presented some examples of access structures to show that the proposed method can attain much lower coding rates than the cumulative map and the modified cumulative map. Our method can also be applied to incomplete and/or ramp access structures, and efficient SS schemes can also be obtained in such cases. Note that integer programming problem is known as NP-hard,

but the optimal multiple assignment map can be obtained quickly by the proposed method in the case that the number of shares is not large.

5.2 Future Works

In Chapter 3, we studied the lower bounds of coding rates in ramp SS schemes. But, it is difficult to determine the exact optimal coding rates, which still remains an important open problem. To approach this problem, we have to specify what kind of access structures can well-realized or not. In other words, we must clarify completely what kind of characteristics in access structures distinguish well-realized and not well-realized ramp SS schemes. The relations between ideal SS schemes and matroids are studied in [21], [38], [84], [85], [98], [112] for perfect SS schemes, although such relations have not been studied for ramp SS schemes except [71]. Hence, it is also an important problem for future works to clarify the relations between well-realized ramp SS schemes and matroids.

For future works concerning Chapter 4, we have to design faster algorithms than the proposed method in the case that the number of shares n is large. In order to obtain faster algorithms, it may be most important to reduce the number of variables in the corresponding integer programming problem, since we use $O(2^n)$ variables in the proposed method. It may possible to design faster algorithms by using some structures of SS schemes, e.g., the monotonicity of access structures. As for other approaches, fast algorithms may be derived if access structures satisfy some properties, e.g., in the case that they can be represented by a matroid or a graph. In all examples treated in the framework of the multiple assignment maps, we note that one of the optimal multiple assignments in the sense of the average coding rates is also optimal in the sense of the worst coding rates. Hence, we conjecture that there exists at least one optimal solution to minimize both the average and the worst coding rates at the same time. It is also a future work to prove this conjecture.

Part II

Visual Secret Sharing Schemes

Chapter 6

Introduction to Visual Secret Sharing Schemes

6.1 Background and Motivations

In Part I, we have discussed ordinary SS schemes in which encryption and decryption are carried out by algebraic calculations on finite fields. Since such calculations are complicated, they are usually processed by computers. However, what should we do in such a case that no computation power is available, for example, in the case of earthquake or electric power failure? From the viewpoint of data security, we should be able to decrypt secret information in any time even if we have no computational power. Visual secret sharing schemes may answer to such problems.

The *visual secret sharing* (VSS) *scheme*, which originates from the *visual cryptography* proposed by Naor-Shamir [81], is a method to encode a secret image into several shares, each of which does not reveal any information of the secret image. Shares are printed on transparencies for example, and distributed to n participants. The secret image can easily be decrypted only by stacking the shares in an arbitrary order. This property, i.e., the VSS scheme needs no computation in decryption, distinguishes the VSS scheme from the ordinary SS schemes.

Naor-Shamir's VSS scheme is a (k, n)-threshold scheme for black-white binary (BW-binary) images, which we call a (k, n)-VSS-BW scheme. An example of a $(2, 2)$-threshold VSS scheme is shown in Appendix A.1. The quality of decrypted images can be evaluated by *contrast* and *pixel expansion* that determine the clearness and the resolution of decrypted images, respectively. The optimization of such parameters is treated in many researches [10], [12], [35], [36], [42], [46], [68], [81], [117].

It is shown in [81] that in any (n, n)-VSS-BW scheme, pixel expansion must be larger than 2^{n-1}. Furthermore, in [81], a simple method is proposed to construct an (n, n)-VSS-BW scheme that attains the optimal 2^{n-1} pixel expansion. However, it is difficult to extend this result to (k, n)-VSS-BW schemes. Actually, although the optimal pixel expansion and/or contrast of (k, n)-VSS-BW schemes are obtained in the case of $k = 2$ [12] and in the cases of $k = 3, 4, 5, n - 1$ under some restrictions [13], their results are too complicated. Hence, the efficient construction methods of (k, n)-VSS-BW schemes are studied in [10], [12], [13], [35],

[36], [42], [46], [68], [117] for general k and n. Furthermore, for (k, n)-VSS-BW schemes, the asymptotic optimal contrast, as n is increased, is derived for fixed k in [13], [42], [68].

The (k, n) structure of VSS-BW scheme can be extended to general access structures which are specified by qualified sets and forbidden sets [1]. A qualified set is a subset of n shares that can decrypt the secret image while a forbidden set is a subset of shares that can gain no information of the secret image. In [1], some methods are proposed to construct VSS schemes with general access structures for BW-binary secret images, and the minimum pixel expansion is derived in the case that the number of shares are less than 4.

VSS schemes with color secret images are also studied in [43], [45], [66], [67], [82], [96], [117], [123] for (k, n)-threshold schemes. The technical difficulty of color VSS schemes comes from how to treat a mixture of colors $\sqcup$ in *basis matrices*, which describe the colors of encrypted pixels on each share. In the case of BW-binary secret images, a mixture of colors can be treated simply as the binary "*OR*" operation, but it is difficult to extend the operation to general colors. Actually, [96], [117], [123] treats only a special case that a mixture of colors {red, green, blue} can be regarded as a "*generalized OR*" operation, and [67] treats the mixture of colors as a join operation in a bounded upper semilattice of colors, as we will see in Section 6.2.1. However, the construction method of VSS schemes proposed in [67] is not applicable to the case that the mixture of colors gives another color, e.g., the case that the mixture of cyan and yellow gives green. In order to overcome this defects, Koga proposed (n, n)-threshold VSS schemes that can deal with any mixture of colors by introducing symmetry into basis matrices, and he pointed out that such basis matrices can be corresponded to polynomials [63]. Furthermore, it is shown in [63] that (k, n)-threshold VSS schemes can easily be obtained from the basis matrices of (k, k)-threshold VSS schemes. However, [63] did not give a systematic construction of (n, n)-threshold VSS schemes for general n.

A systematic construction of (n, n)-threshold VSS schemes based on symmetric basis matrices is developed in our joint work [66], which is called *algebraic* construction.[1]

In this construction, the definition of (n, n)-threshold VSS schemes is rephrased into simultaneous partial differential equations based on the one to one correspondence between basis matrices and homogeneous polynomials of degree n, which are called *basis polynomials*. By introducing these techniques, combinatorial problems in VSS schemes can be transformed to algebraic problems, which can easily be treated. The algebraic construction of VSS schemes for color images will be reviewed in Chapter 6. The algebraic construction can realize (k, n)-threshold VSS schemes for color images, but it has two problems. One is that the algebraic construction cannot be extended to VSS schemes with general access structures, and the second is that VSS schemes for BW-binary images cannot be realized by the algebraic construction. For the first problem, we review in Chapter 6 how to construct VSS schemes for general access

[1]This construction method was originally called *analytic* construction in [66] since it uses simultaneous partial differential equations. However, this construction method has also many algebraic aspects. For example, colors are represented by variables, which satisfy the OR operation or some operation on an upper bounded semilattice. Pixels are represented by matrices, which are classified by equivalence classes. The equivalence classes are identified with polynomials. Furthermore, it is pointed out in [64] that the set of polynomials can be identified with a set of lattice points in some linear space. Hence, this construction method is called *algebraic* rather than analytic in this thesis.

structures from (n, n)-threshold VSS schemes based on the results in [66].

For the second problem, Kuwakado-Tanaka [72] modified basis polynomials for BW-binary secret images. In [52], based on their results, we extend their method to VSS schemes for gray-scale images including BW-binary images as special cases, and we proved that constructed VSS schemes for gray-scale images are optimal in all the (n, n)-threshold VSS schemes for gray-scale images. In Chapter 7, such construction of the optimal (n, n)-VSS schemes will be described. Furthermore, in Chapter 7, a construction method of VSS schemes for color images with shades is presented based on the algebraic constructions. From these results, efficient VSS schemes of (k, n)-threshold access structures for any kind of secret images can easily be constructed only by solving simultaneous partial differential equations.

In the above schemes, we assumed that secret is a single image. But, VSS schemes with plural secret images can also be considered [35], [53], [60], [62], [107]. Kato-Imai [60] proposed a method to reproduce different secret images as the number of shares is increased, and Suga et al. [107] treated VSS schemes for plural secret images with general access structures represented by graphs. Furthermore, Droste [35], Klein-Wessler [62] proposed methods to decrypt different secret images for every subset of n shares. However, note that the previous studies [35], [60], [62], [107] treat only BW-binary secret images, and any VSS schemes have not yet been studied for general cases such that secret images are plural color images with shades and their access structures are general. Moreover, as we will see in Section 8.2, the definitions of VSS schemes in [60], [107] are not accurate, i.e., it occurs that decrypted images leak out some informations of the other secret images, even in the case that the security conditions given in [60], [107] are satisfied.

As other research directions, VSS schemes with identification (ID) images are studied in [2], [25], [43], [78]. In these researches, it is assumed that each share has an identification image instead of a random sandstorm-like image. VSS scheme with BW-binary ID images and their optimizations of contrast are discussed in [2], while VSS schemes with color ID images are proposed in [43]. Furthermore, in [25], [78], $(2, 2)$-VSS schemes with ID images are treated for the case that we attach importance to the quality of decrypted images at the sacrifice of secrecy. Note that VSS schemes with n ID images and a single secret image can be considered as VSS scheme with $(n + 1)$ secret images by treating the ID images as secret images that can be decrypted from a single share.

Based on such background, in [53], we propose VSS schemes with plural secret images for general access structures under accurate security definitions, which guarantee that decrypted images do not leak out any information of the other secret images. We establish the construction method of such VSS schemes that can attain the security conditions perfectly without degenerating the quality of decrypted images compared with the methods in [35], [107]. Furthermore, our VSS schemes proposed in [53] can treat color images with shades. In the sequel, our VSS schemes for plural secret images can be applied to any type of plural secret images and any kind of access structures. In other words, our method includes almost all previous VSS schemes. In Chapter 8, we describe the details of these VSS schemes.

Finally, we note that Koga [64] studied the correspondence of a set of basis polynomials and

a linear space, and he also constructed an algorithm to derive the optimal VSS schemes with BW-binary images for (k, n)-threshold access structures [65]. Furthermore, the results of [64] are extended to color secret images by Ishihara-Koga [44]. Applications of VSS schemes are also studied in [6], [60], [72], [79]. Authentication systems can be constructed from VSS schemes as shown in [60], [79], and it is studied in [6], [72] how we can detect cheaters in VSS schemes. But, these studies of VSS schemes are out of scope of this thesis.

In the remaining of Part II is organized as follows: In Section 6.2, we introduce how to treat colors mathematically and define (k, n)-VSS schemes with color secret images. In Section 6.3, we review the algebraic construction of (n, n) and (k, n)-threshold VSS schemes, and it is shown in Section 6.4 how these results can be extended to general access structures. In Chapter 7, modified basis polynomials [72] are applied to VSS schemes for gray-scale images. Furthermore, we clarify the optimality of the proposed method. In Chapter 8, VSS schemes for plural secret images are treated. Finally in Chapter 9, we summarize our results obtained in Part II and future works are discussed.

In Appendix, we show some examples of VSS schemes treated in this thesis.

6.2 Basic Definitions of Visual Secret Sharing Schemes

6.2.1 Representations of Colors

In this thesis, colors are expressed by lowercase san-serif fonts. For example, we denote black, red, green, blue, yellow, magenta, cyan, and white by $\mathsf{1}$, r, g, b, y, m, c and $\mathsf{0}$, respectively. A general color is expressed by x.

Let $\sqcup$ represent the subtractive mixture of colors which corresponds to overlapping the colors printed on transparencies. Then, $\mathsf{1} \sqcup \mathsf{g} = \mathsf{g} \sqcup \mathsf{1} = \mathsf{1}$, and $\mathsf{c} \sqcup \mathsf{y} = \mathsf{y} \sqcup \mathsf{c} = \mathsf{g}$ hold, for example. Let $\mathcal{E}$ be a set of colors printed on shares. Note that $\sqcup$ is commutative for the elements in $\mathcal{E}$. In the case of $\mathcal{E} = \{\mathsf{1}, \mathsf{r}, \mathsf{g}, \mathsf{b}, \mathsf{y}, \mathsf{m}, \mathsf{c}, \mathsf{0}\}$, it is known that $\mathcal{E}$ forms a bounded upper semilattice represented by a Hasse diagram L_{col} in Figure 6.1 if we consider a mixture of colors $\sqcup$ as a join operation on L_{col} [67].[2] Furthermore, if we restrict L_{col} to two elements $\mathsf{0}$ and $\mathsf{1}$, the mixture of them can also be considered as the binary "*OR*" operation by regarding $\mathsf{0}$ and $\mathsf{1}$ as the binary numbers 0 and 1, respectively.

In VSS schemes, we note that secret images are not completely reproduced. As is illustrated in Figure 6.2, each pixel on a decrypted secret image DI, which corresponds to a pixel on a secret image SI, is constructed by a set of m subpixels, and each subpixel takes a color in $\mathcal{E}$. Hence, the color of each pixel in DI is a little different from the one in SI, but they are similar color. Parameter m is called *pixel expansion*, which should be as small as possible from the viewpoint of the resolution of decrypted image DI. In this thesis, we treat only the case that when the color

[2] A partially orders set L is called an *upper semilattice* if the least upper bound of x and y denoted by $\mathsf{x} \sqcup \mathsf{y}$ belongs to L for any $\mathsf{x}, \mathsf{y} \in L$. In the upper semilattice L, it is known that the idempotent law, the commutative law, and the associative law hold with respect to the join operation.

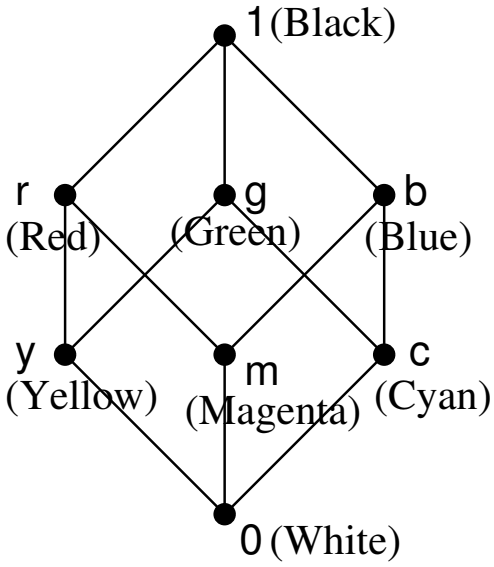


Figure 6.1. Hasse diagram L_{col}

of a pixel is x in SI,[3] each subpixel of the corresponding pixel in DI is x or $\mathsf{1}$. A pixel with color x is called pixel x. Let $\mathcal{D}$ be the set of colors used on DI. Then, we assume that $\mathcal{E}$ is adequately selected for $\mathcal{D}$.

Example 6.1 Let us consider a VSS scheme with a set of decrypted colors $\mathcal{D} = \{\mathsf{c}, \mathsf{y}, \mathsf{g}\}$. Then, $\mathcal{E} = \{\mathsf{0}, \mathsf{c}, \mathsf{y}, \mathsf{1}\}$ may be adequate for $\mathcal{D}$ since it holds that $\mathsf{c} = \mathsf{0} \sqcup \mathsf{c}$, $\mathsf{y} = \mathsf{0} \sqcup \mathsf{y}$, $\mathsf{g} = \mathsf{c} \sqcup \mathsf{y}$. □

6.2.2 Basis Matrices of Visual Secret Sharing Schemes

As we pointed out in the previous section, each pixel on a decrypted secret image DI, which corresponds to a secret image SI, is constructed by a set of m subpixels. Letting $\boldsymbol{V} = \{V_1, V_2, \ldots, V_n\}$ be a set of shares, we encrypt each color $\mathsf{x} \in \mathcal{D}$ of a pixel into an $n \times m$ matrix

$$T = \begin{bmatrix} \mathsf{t}_{11}\mathsf{t}_{12}\cdots\mathsf{t}_{1m} \\ \mathsf{t}_{21}\mathsf{t}_{22}\cdots\mathsf{t}_{2m} \\ \vdots\ \ \vdots\ \ \ddots\ \ \vdots \\ \mathsf{t}_{n1}\mathsf{t}_{n2}\cdots\mathsf{t}_{nm} \end{bmatrix} \in \mathcal{E}^{nm}, \tag{6.1}$$

where $\mathsf{t}_{uv} \in \mathcal{E}$, $1 \leq u \leq n$, $1 \leq v \leq m$, denotes the color of the v-th subpixel of the subpixel on the u-th share V_u. The correspondence between matrix T and subpixel on shares is depicted in Figure 6.3.

We introduce an equivalence relation $\sim$ into matrices in $\mathcal{E}^{nm}$ [52]. For two matrices $A, B \in \mathcal{E}^{nm}$, $A \sim B$ means that A can be obtained by a column permutation of B. In other words, it

[3] Color with shades are treated in Section 7.5.

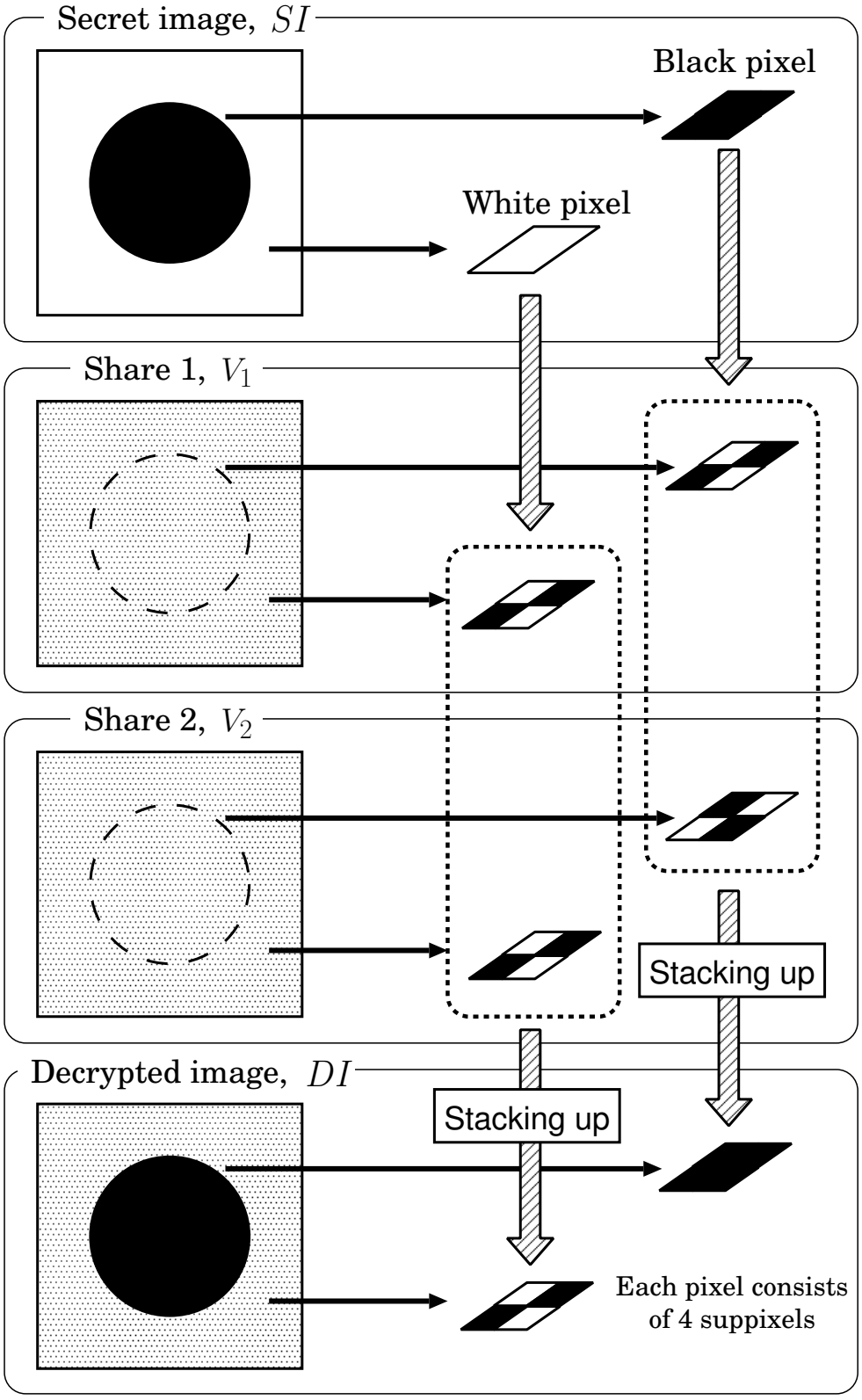


Figure 6.2 Correspondence between pixels on a secret image and a decrypted image in the case of $(2, 2)$-threshold access structure with $\mathcal{E} = \{0, 1\}$ and $m = 4$

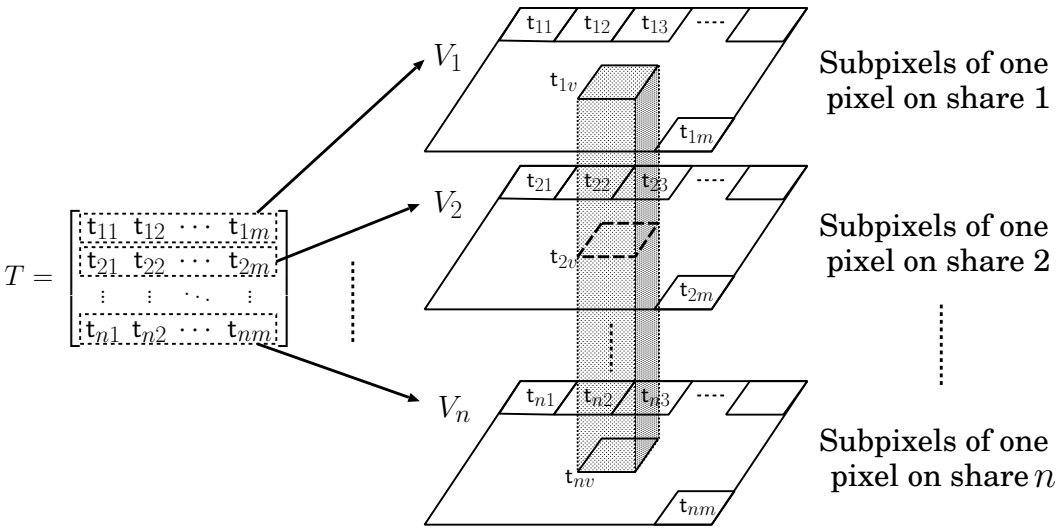


Figure 6.3. A set of pixels on n shares represented by a matrix T

holds that for any permutation $\sigma : \{1, 2, \ldots, m\} \to \{1, 2, \ldots, m\}$,

$$[\boldsymbol{a}_1 \boldsymbol{a}_2 \cdots \boldsymbol{a}_m] \sim [\boldsymbol{a}_{\sigma(1)} \boldsymbol{a}_{\sigma(2)} \cdots \boldsymbol{a}_{\sigma(m)}], \tag{6.2}$$

where $\boldsymbol{a}_i$'s are column vectors of a matrix $T \in \mathcal{E}^{nm}$. It is easy to check that this relation satisfies the three conditions of the equivalence relation, i.e., the reflective law, the symmetric law, and the transitive law. Hence we can consider the quotient set $\mathcal{E}^{nm}/\!\sim$, which consists of the equivalence classes. An equivalence class is represented as $\langle R \rangle$ by a representative R in the class.

For two matrices $X \in \mathcal{E}^{nm_1}$ and $Y \in \mathcal{E}^{nm_2}$, denote by $\odot$ a concatenation operation, i.e., it holds that $X \odot Y \in \mathcal{E}^{n(m_1+m_2)}$. As an example, see (1.5). Furthermore, we can define naturally that $\langle X \rangle \odot \langle Y \rangle \stackrel{\text{def}}{=} \langle X \odot Y \rangle$.

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

$$\boldsymbol{x} \overset{m}{\sqcup} \boldsymbol{y} = [\, \mathsf{x}_1 \sqcup \mathsf{y}_1\ \mathsf{x}_2 \sqcup \mathsf{y}_2 \cdots\ \mathsf{x}_m \sqcup \mathsf{y}_m\,], \tag{6.3}$$

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

$$\eta(S[\![\boldsymbol{X}]\!]) = \boldsymbol{x}_{u_1} \overset{m}{\sqcup} \boldsymbol{x}_{u_2} \overset{m}{\sqcup} \cdots \overset{m}{\sqcup} \boldsymbol{x}_{u_r}. \tag{6.4}$$

A (k, n)-threshold VSS scheme is defined as follows:

Definition 6.2 (Koga-Yamamoto [67]) [4] For $\mathcal{D} = \{\mathsf{d}_1, \mathsf{d}_2, \ldots, \mathsf{d}_J\}$ and pixel expansion m, an $n \times m$ matrix B_{d_j} is called a *basis matrix*[5] of d_j for a (k, n) access structure if all B_{d_j}, $j = 1, 2, \ldots, J$, satisfy the following conditions:

(i) It holds for any $\boldsymbol{A} \subseteq \boldsymbol{V}$ with $|\boldsymbol{A}| = k$ that

$$\eta\left(B_{\mathsf{d}_j}[\![\boldsymbol{A}]\!]\right) \sim [\,\mathsf{d}_j\,\mathsf{d}_j\,\cdots\,\mathsf{d}_j\;\mathsf{1}\,\mathsf{1}\cdots\mathsf{1}\,], \tag{6.5}$$

where the number of d_j is constant. In the case of $\mathsf{d}_j = \mathsf{1}$, the right hand side of (6.5) consists of only $\mathsf{1}$'s.

(ii) For any set $\boldsymbol{A} \subseteq \boldsymbol{V}$ with $|\boldsymbol{A}| = k - 1$, all $B_{\mathsf{d}_j}[\![\boldsymbol{A}]\!]$, $j = 1, 2, \ldots, J$, belong to the same equivalence class in $\mathcal{E}^{|\ \ |m}/\!\sim$.

A VSS scheme is called a $(k, n, \mathcal{E}, \mathcal{D})$-*VSS scheme* if for each color $\mathsf{d}_j \in \mathcal{D}$, $j = 1, 2, \ldots, |\mathcal{D}|$, each pixel d_j is determined by a matrix randomly selected from $\langle B_{\mathsf{d}_j} \rangle \in \mathcal{E}^{nm}/\!\sim$, where B_{d_j} is the basis matrix of d_j. □

Letting N_j be the number of d_j in (6.5), N_j represents the brightness of decrypted pixel d_j. Hence, we define the *contrast* of decrypted images as follows.

Definition 6.3 (Koga et al. [66]) A *contrast* of a $(k, n, \mathcal{E}, \mathcal{D})$-VSS scheme is defined as follows:

$$\alpha = \min_{\mathsf{d}_j \in \mathcal{D},\ \mathsf{d}_j \neq \mathsf{1}} \frac{N_j}{m}, \tag{6.6}$$

where m is pixel expansion. □

Note that, in the case of $\mathcal{E} = \{\mathsf{0}, \mathsf{1}\}$, the contrast in Definition 6.3 coincides with the contrast defined by Naor-Shamir [81]. We also note that contrast α should be as large as possible.

Example 6.4 (Koga-Yamamoto [67]) Let $\mathcal{E} = \{\mathsf{0}, \mathsf{c}, \mathsf{y}, \mathsf{m}, \mathsf{1}\}$ and $\mathcal{D} = \{\mathsf{0}, \mathsf{y}, \mathsf{m}, \mathsf{c}, \mathsf{r}, \mathsf{g}, \mathsf{b}, \mathsf{1}\}$. Then, for the $(2, 2, \mathcal{E}, \mathcal{D})$-VSS scheme, the basis matrices of $\mathcal{D}$ can be realized as follows:

$$B_{\mathsf{0}} = \begin{bmatrix} \mathsf{0ymc1\,1\,11} \\ \mathsf{01\,1\,1ymc1} \end{bmatrix} \tag{6.7}$$

$$B_{\mathsf{y}} = \begin{bmatrix} \mathsf{y0mc\,1\,111} \\ \mathsf{0y\,1\,1mc11} \end{bmatrix} \tag{6.8}$$

$$B_{\mathsf{m}} = \begin{bmatrix} \mathsf{m\,0\,cy1111} \\ \mathsf{\,0\,m11cy11} \end{bmatrix} \tag{6.9}$$

$$B_{\mathsf{c}} = \begin{bmatrix} \mathsf{c0ym1\,1\,11} \\ \mathsf{0c1\,1\,ym11} \end{bmatrix} \tag{6.10}$$

[4] The original definition of $(k, n, \mathcal{E}, \mathcal{D})$-VSS schemes in [67] does not use the notion of equivalence relations, which we introduced in [52].

[5] Basis matrices are firstly defined by Droste [35].

$$B_{\mathsf{r}} = \begin{bmatrix} \mathsf{y\,mc01111} \\ \mathsf{m\,y\,11c011} \end{bmatrix} \tag{6.11}$$

$$B_{\mathsf{g}} = \begin{bmatrix} \mathsf{cym0\,1\,111} \\ \mathsf{yc\,1\,1m011} \end{bmatrix} \tag{6.12}$$

$$B_{\mathsf{b}} = \begin{bmatrix} \mathsf{m\,c\,y01111} \\ \mathsf{c\,m11y011} \end{bmatrix} \tag{6.13}$$

$$B_{1} = \begin{bmatrix} \mathsf{ymc01\,1\,11} \\ \mathsf{1\,1\,11ymc0} \end{bmatrix} \tag{6.14}$$

It is easy to check that (6.11)–(6.13) satisfy Definition 6.2-(i) and (ii). For example, the first rows of (6.11)–(6.13) are equivalent to [y m c 0 1 1 1 1]. Pixel expansion and contrast are given by $m = 8$, $\alpha = \frac{1}{8}$, respectively. □

Example 6.5 For the $(2, 3, \mathcal{E}, \mathcal{D})$-VSS scheme with colors $\mathcal{E} = \{\mathsf{0}, \mathsf{c}, \mathsf{y}, \mathsf{1}\}$ and $\mathcal{D} = \{\mathsf{c}, \mathsf{y}, \mathsf{g}\}$, the basis matrices are given as follows.

$$B_{\mathsf{c}} = \begin{bmatrix} \mathsf{0c101cy11y11} \\ \mathsf{c001c11y11y1} \\ \mathsf{11cc0011y11y} \end{bmatrix} \tag{6.15}$$

$$B_{\mathsf{y}} = \begin{bmatrix} \mathsf{0y101yc11c11} \\ \mathsf{y001y11c11c1} \\ \mathsf{11yy0011c11c} \end{bmatrix} \tag{6.16}$$

$$B_{\mathsf{g}} = \begin{bmatrix} \mathsf{cy1c1y011011} \\ \mathsf{ycc1y1101101} \\ \mathsf{11yycc110110} \end{bmatrix} \tag{6.17}$$

Then, it holds that $m = 12$ and $\alpha = \frac{1}{6}$. □

Remark 6.6 Note that in Example 6.5, a secret image can be reproduced from any two shares, but all pixels become black if we stack all three shares. Hence, in the case that we have more than k shares of a $(k, n, \mathcal{E}, \mathcal{D})$-VSS scheme, we have to use only k shares to stack up in decryption. □

The next theorem is proved for BW-binary secret images in [1] but the same arguments also hold for any kind of secret images.

Theorem 6.7 (Ateniese et al. [1]) Suppose that for a $(k, n, \mathcal{E}, \mathcal{D})$-VSS scheme, basis matrices $B_{\mathsf{d}_1}, B_{\mathsf{d}_2}, \ldots, B_{\mathsf{d}_J}$ contain the same columns. Then, the matrices $\tilde{B}_{\mathsf{d}_j}$ obtained by deleting the same columns from B_{d_j} are also basis matrices for the $(k, n, \mathcal{E}, \mathcal{D})$-VSS scheme. □

We omit the proof since it is clear. Note that we should delete the same columns from basis matrices in order to reduce pixel expansion m.

Example 6.8 Consider basis matrices for the $(2, 2, \mathcal{E}, \mathcal{D})$-VSS scheme with $\mathcal{E} = \{\mathsf{0}, \mathsf{c}, \mathsf{y}, \mathsf{m}, \mathsf{1}\}$ and $\mathcal{D} = \{\mathsf{r}, \mathsf{b}\}$. In this case, from Example 6.4, B_{r} and B_{b} given by (6.11) and (6.13) can be the basis matrices of $\mathcal{D} = \{\mathsf{r}, \mathsf{b}\}$. But, B_{r} and B_{b} commonly contain the following columns

$$\begin{bmatrix} \mathsf{0} \\ \mathsf{1} \end{bmatrix}, \begin{bmatrix} \mathsf{1} \\ \mathsf{0} \end{bmatrix}, \begin{bmatrix} \mathsf{1} \\ \mathsf{1} \end{bmatrix}, \begin{bmatrix} \mathsf{1} \\ \mathsf{1} \end{bmatrix}. \tag{6.18}$$

Hence, by deleting (6.18) from (6.11) and (6.13), we obtain the following basis matrices.

$$\tilde{B}_{\mathsf{r}} = \begin{bmatrix} \mathsf{y\,m\,c\,1} \\ \mathsf{m\,y\,1\,c} \end{bmatrix} \tag{6.19}$$

$$\tilde{B}_{\mathsf{b}} = \begin{bmatrix} \mathsf{m\,c\,y\,1} \\ \mathsf{c\,m\,1\,y} \end{bmatrix} \tag{6.20}$$

In this case, we obtain that $m = 4$, $\alpha = \frac{1}{4}$. Note that $\tilde{B}_{\mathsf{r}}$ and $\tilde{B}_{\mathsf{b}}$ attain higher contrast and lower pixel expansion than B_{r} and B_{b} in Example 6.4. □

6.3 Algebraic Construction of Visual Secret Sharing Schemes

In this section, a simple construction of VSS schemes called *algebraic* construction are described according to [66] with a few modifications. See Remark 6.20 for the differences.

6.3.1 Column-Permutation Matrices and Polynomials

Let $\boldsymbol{v}$ be an n-dimensional row vector, each element of which is a color in $\mathcal{E}$. Then, define an $n \times n!$ matrix $C_n(\boldsymbol{v})$ called a *column permutation* (CP) matrix which consists of all $n!$ permutations of ${}^t\boldsymbol{v}$ [63]. For example, in the case of $\boldsymbol{v} = [\,\mathsf{r\ g\ b}\,]$, we have

$$C_3(\boldsymbol{v}) = \begin{bmatrix} \mathsf{rgrbbg} \\ \mathsf{grbrgb} \\ \mathsf{bbggrr} \end{bmatrix}. \tag{6.21}$$

In the case that all the elements of $\boldsymbol{v}$ are different, there are $(n!)!$ matrices that are equivalent to $C_n(\boldsymbol{v})$ in the equivalence relation $\sim$ introduced in Section 6.2.2 and [52]. However, by the benefit of equivalence relations $\sim$, it suffices to consider only one matrix that is a representative in the equivalence class.

Note that in the permutation of ${}^t\boldsymbol{v}$, all n colors in $\boldsymbol{v}$ are treated different colors even if two or more elements in $\boldsymbol{v}$ are the same color. Hence, as an example, it holds that

$$C_3\left([\mathsf{g11}]\right) \sim \begin{bmatrix} \mathsf{g11g11} \\ \mathsf{1g11g1} \\ \mathsf{11g11g} \end{bmatrix}. \tag{6.22}$$

We now introduce the *polynomial representation* of basis matrices by identifying each equivalence class of basis matrices with a homogeneous polynomial of degree n as follows.[6]

Let us identify colors x with variables x. For instance, r, g, b, y, m, c and d are identified with r, g, b, y, m, c and d, respectively. Especially, $\mathsf{1}$ (black) and $\mathsf{0}$ (white) are identified with z and a, respectively.

Then, for a row vector $\boldsymbol{v} = [\,\mathsf{x}_1\ \mathsf{x}_2\ \cdots\ \mathsf{x}_n\,]$, we can also identify an equivalence class of CP matrices $\langle C_n(\boldsymbol{v})\rangle$ and the concatenation operation $\odot$ defined by (1.5) with a monomial $\prod_{i=1}^{n} x_i$

[6] The polynomial representations were developed in [66] based on [63].

and operation $+$, respectively. For example, an equivalence class of a concatenation of (6.21) and (6.22) is identified with a polynomial $rgb + gz^2$.

Let $C'_n(\boldsymbol{v})$ be an $(n-1) \times n!$ matrix obtained by deleting an arbitrary one row in $C_n(\boldsymbol{v})$. Then, note that $C'_n(\boldsymbol{v})$ consists of a concatenations of CP matrices with $n-1$ rows. For instance, $C'_3([\mathsf{r\ g\ b}])$ can be represented as

$$C'_3([\mathsf{r\ g\ b}]) \sim \begin{bmatrix} \mathsf{rgrbbg} \\ \mathsf{grbrgb} \end{bmatrix} \sim \begin{bmatrix} \mathsf{rg} \\ \mathsf{gr} \end{bmatrix} \odot \begin{bmatrix} \mathsf{rb} \\ \mathsf{br} \end{bmatrix} \odot \begin{bmatrix} \mathsf{bg} \\ \mathsf{gb} \end{bmatrix}$$

$$\sim C_2([\mathsf{r\ g}]) \odot C_2([\mathsf{r\ b}]) \odot C_2([\mathsf{b\ g}]). \tag{6.23}$$

It is worth noting that the polynomial representation for the equivalence class of the right hand side of (6.23) is $ab + bc + ca$, which is obtained by applying a partial differential operator $\frac{\partial}{\partial r} + \frac{\partial}{\partial g} + \frac{\partial}{\partial b}$ to rgb, the monomial representation of $\langle C_3([\mathsf{r\ g\ b}])\rangle$.

It is easy to generalize the above argument. Let $\mathcal{E} = \{\mathsf{e}_1, \mathsf{e}_2, \ldots, \mathsf{e}_I, 1\}$ ($\mathsf{e}_i \neq 1$) be a set of colors used in encryption and $\{\mathsf{x}_1, \mathsf{x}_2, \ldots, \mathsf{x}_n\} \subseteq \mathcal{E}$. Then, the polynomial representation of the matrix that consists of arbitrary $n-1$ rows of $\langle C_n([\mathsf{x}_1\ \mathsf{x}_2\ \cdots\ \mathsf{x}_n])\rangle$ is given by

$$\Xi(x_1 x_2 \cdots x_n) = \sum_{i=1}^{n} \prod_{\substack{j=1 \\ j \neq i}}^{n} x_j, \tag{6.24}$$

where the partial differential operator Ξ is defined as

$$\Xi = \sum_{\ell=1}^{I} \frac{\partial}{\partial e_\ell} + \frac{\partial}{\partial z}. \tag{6.25}$$

Let X be a matrix constructed by a concatenation of CP matrices and X' be the matrix obtained by deleting arbitrary one row of X. Note that when X has n rows, X' has $n-1$ rows. Then, $\langle X\rangle$ can be represented by a homogeneous polynomial F of degree n, and $\langle X'\rangle$ can be represented by ΞF, which is a homogeneous polynomial of degree $n-1$.

Example 6.9 For the set of colors $\mathcal{E} = \{0, \mathsf{c}, \mathsf{y}, 1\}$, let X be the following matrix with three rows, each element of which takes value in $\mathcal{E}$.

$$X = \begin{bmatrix} \mathsf{cy1yc1} & \mathsf{cy0yc0} \\ \mathsf{ycy11c} & \mathsf{ycy00c} \\ \mathsf{11ccyy} & \mathsf{00ccyy} \end{bmatrix} = C_3([\mathsf{c\ y\ 1}]) \odot C_3([\mathsf{c\ y\ 0}]). \tag{6.26}$$

Note that X is constructed by a concatenation of CP matrices, and hence, X' is also constructed by a CP matrices as follows.

$$X' = \begin{bmatrix} \mathsf{cy} & \mathsf{1y} & \mathsf{c1} & \mathsf{cy} & \mathsf{0y} & \mathsf{c0} \\ \mathsf{yc} & \mathsf{y1} & \mathsf{1c} & \mathsf{yc} & \mathsf{y0} & \mathsf{0c} \end{bmatrix}$$

$$= C_2([\mathsf{c\ y}]) \odot C_2([\mathsf{1\ y}]) \odot C_2([\mathsf{c\ 1}]) \odot C_2([\mathsf{c\ y}]) \odot C_2([\mathsf{0\ y}]) \odot C_2([\mathsf{c\ 0}]) \tag{6.27}$$

The polynomial representation of $\langle X\rangle$ and $\langle X'\rangle$ can be represented by $F = cyz + cya$ and $F' = 2cy + ac + ay + az + cy$, respectively. It is easy to check that $F' = \Xi F$ holds where the partial differential operator Ξ is given by $\Xi = \frac{\partial}{\partial a} + \frac{\partial}{\partial c} + \frac{\partial}{\partial y} + \frac{\partial}{\partial z}$. □

6.3.2 Polynomial Representations of Basis Matrices

In this section, we construct basis matrices for an $(n, n, \mathcal{E}, \mathcal{D})$-threshold VSS scheme based on CP matrices. Now, we assume that $\mathcal{D} = \{\mathsf{d}_1, \mathsf{d}_2, \ldots, \mathsf{d}_J\}$ and each color $\mathsf{d}_j \in \mathcal{D}$ is a mixture of h_{d_j} different colors $\mathsf{d}_j^{\langle i \rangle} \in \mathcal{E}$ as follows.

$$\mathsf{d}_j = \mathsf{d}_j^{\langle 1 \rangle} \sqcup \mathsf{d}_j^{\langle 2 \rangle} \sqcup \cdots \sqcup \mathsf{d}_j^{\langle h_{\mathsf{d}_j} \rangle}, \tag{6.28}$$

where each $\mathsf{d}_j^{\langle i \rangle}$ is used in u_i times, and $\sum_{i=1}^{h_{\mathsf{d}_j}} u_i = n$. Then, the corresponding n-dimensional row vector $\boldsymbol{v}_{\mathsf{d}_j}$ is given by

$$\begin{aligned} \boldsymbol{v}_{\mathsf{d}_j} &= [\underbrace{\mathsf{d}_j^{\langle 1 \rangle} \cdots \mathsf{d}_j^{\langle 1 \rangle}}_{u_1 \text{ times}} \underbrace{\mathsf{d}_j^{\langle 2 \rangle} \cdots \mathsf{d}_j^{\langle 2 \rangle}}_{u_2 \text{ times}} \cdots \underbrace{\mathsf{d}_j^{\langle h_{\mathsf{d}_j} \rangle} \cdots \mathsf{d}_j^{\langle h_{\mathsf{d}_j} \rangle}}_{u_{h_{\mathsf{d}_j}} \text{ times}}] \\ &\stackrel{\text{def}}{=} \left[\left(\mathsf{d}_j^{\langle 1 \rangle} \right)^{u_1} \left(\mathsf{d}_j^{\langle 2 \rangle} \right)^{u_2} \cdots \left(\mathsf{d}_j^{\langle h_{\mathsf{d}_j} \rangle} \right)^{u_{h_{\mathsf{d}_j}}} \right]. \end{aligned} \tag{6.29}$$

For an $(n, n, \mathcal{E}, \mathcal{D})$-VSS scheme, a basis matrix of d_j, B_{d_j}, can be constructed by using CP matrix $C_n(\boldsymbol{v}_{\mathsf{d}_j})$ as follows.

$$B_{\mathsf{d}_j} = C_n(\boldsymbol{v}_{\mathsf{d}_j}) \odot X_{\mathsf{d}_j}, \tag{6.30}$$

where $X_{\mathsf{d}_j} \in \mathcal{E}^{nm}$ is a matrix which consists of concatenations of several CP matrices. Then, in order to satisfy the condition (i) in Definition 6.2, i.e., (6.5) for $\boldsymbol{V}$, it is sufficient that $\eta(X_{\mathsf{d}_j}[\![\boldsymbol{V}]\!])$ consists of all 1, because it holds that

$$\eta(B_{\mathsf{d}_j}[\![\boldsymbol{V}]\!]) \sim \eta(C_n(\boldsymbol{v}_{\mathsf{d}_j})[\![\boldsymbol{V}]\!]) \odot \eta(X_{\mathsf{d}_j}[\![\boldsymbol{V}]\!]) \sim [\, \mathsf{d}_j \; \mathsf{d}_j \; \cdots \mathsf{d}_j \; 1 \; 1 \; \cdots 1], \tag{6.31}$$

where $\eta(\cdot)$ is defined in (6.4). Then, X_{d_j} must contain at least one 1 in each column[7] and the polynomial representation of (6.30), say F_{d_j}, is given by

$$F_{\mathsf{d}_j} = \prod_{i=1}^{h_{\mathsf{d}_j}} \left(d_j^{\langle i \rangle} \right)^{u_i} + z f_{\mathsf{d}_j}, \tag{6.32}$$

where f_{d_j} is a homogeneous polynomial of degree $n-1$. We call F_{d_j} the *basis polynomial* corresponding to B_{d_j}. Since F_{d_j} is a homogeneous polynomial of degree n, (6.32) is equivalent to

$$\left[F_{\mathsf{d}_j} - \prod_{i=1}^{h_{\mathsf{d}_j}} \left(d_j^{\langle i \rangle} \right)^{u_i} \right]_{z=0} = 0. \tag{6.33}$$

Note that (6.33) is the condition required for a basis polynomial, which corresponds to the condition (i) in Definition 6.2.

[7] Although it holds that $\mathsf{r} \sqcup \mathsf{b} = 1$ in the case of Figure 6.1 for instance, it is difficult to realize the complete black from the mixture of colors except black in practice. So, we impose this requirement.

Next, let us consider the second condition (ii) in Definition 6.2. In the case of (n, n)-threshold access structures, B'_{d_j} must be required for all d_j, i.e., for all $j = 1, 2, \ldots, J$, that

$$B'_{\mathsf{d}_j} \sim B', \tag{6.34}$$

where $B' \in \mathcal{E}^{(n-1)m}$ is a matrix that does not depend on d_j. This means in the polynomial representation that for Ξ defined in (6.25), F_{d_j} must satisfy

$$\Xi F_{\mathsf{d}_j} = F', \ \text{ for all } \ j \tag{6.35}$$

where F' is a homogeneous polynomial of degree $n-1$ not depending on j. (6.35) is the second condition required for basis polynomials, which corresponds to (6.5) in Definition 6.2-(ii).

Furthermore, it is worth noting that pixel expansion m and contrast α can be calculated as follows:

$$m = n! \cdot F_{\mathsf{d}_j}\big|_{\substack{e_i=1, z=1 \\ 1 \le i \le I}}, \tag{6.36}$$

$$\alpha = \frac{F_{\mathsf{d}_j}\big|_{\substack{e_i=1, z=0 \\ 1 \le i \le I}}}{F_{\mathsf{d}_j}\big|_{\substack{e_i=1, z=1 \\ 1 \le i \le I}}}, \tag{6.37}$$

Summarizing, in the case that every basis matrix consists of the concatenation of CP matrices, we can rephrase Definition 6.2 for (n, n)-threshold access structures by using basis polynomials.

Theorem 6.10 (Koga et al. [66]) Let B_{d_j}, $j = 1, 2, \ldots, J$, be basis matrices for an $(n, n, \mathcal{E}, \mathcal{D})$-VSS scheme which are constructed by the concatenations of some CP matrices. Then, basis polynomials F_{d_j} corresponding to B_{d_j} satisfy (6.33) and (6.35). Furthermore, pixel expansion m and contrast α are given by (6.36) and (6.37), respectively. □

Example 6.11 Let us consider the $(2, 2, \mathcal{E}, \mathcal{D})$-VSS scheme with color sets $\mathcal{E} = \{1, \mathsf{c}, \mathsf{y}, \mathsf{g}, 0\}$ and $\mathcal{D} = \{\mathsf{c}, \mathsf{y}, \mathsf{g}\}$. Then, the basis matrices with $m = 4$ shown in [67] are given by

$$B_{\mathsf{c}} = \begin{bmatrix} \mathsf{0cy1} \\ \mathsf{c01y} \end{bmatrix} = C_2([\mathsf{0\ c}]) \odot C_2([\mathsf{y\ 1}]), \tag{6.38}$$

$$B_{\mathsf{y}} = \begin{bmatrix} \mathsf{0yc1} \\ \mathsf{y01c} \end{bmatrix} = C_2([\mathsf{0\ y}]) \odot C_2([\mathsf{c\ 1}]), \tag{6.39}$$

$$B_{\mathsf{g}} = \begin{bmatrix} \mathsf{cy10} \\ \mathsf{yc01} \end{bmatrix} = C_2([\mathsf{c\ y}]) \odot C_2([\mathsf{1\ 0}]). \tag{6.40}$$

The polynomial representations of B_{c}, B_{y} and B_{g} become

$$F_{\mathsf{c}} = ac + yz, \tag{6.41}$$

$$F_{\mathsf{y}} = ay + cz, \tag{6.42}$$

$$F_{\mathsf{g}} = cy + az, \tag{6.43}$$

respectively. Letting $\Xi = \frac{\partial}{\partial a} + \frac{\partial}{\partial c} + \frac{\partial}{\partial y} + \frac{\partial}{\partial z}$, it is easy to check that F_{c}, F_{y} and F_{g} satisfy (6.33) and (6.35). These basis matrices attain that $m = 4$ and $\alpha = \frac{1}{2}$. □

Theorem 6.10 implies that the basis polynomials obtained by solutions of the simultaneous partial differential equations (6.33) and (6.35) give the basis matrices of $(n, n, \mathcal{E}, \mathcal{D})$-VSS schemes.

Example 6.12 For the $(3, 3, \mathcal{E}, \mathcal{D})$-VSS scheme with $\mathcal{E} = \{0, \mathsf{c}, \mathsf{y}, 1\}$ and $\mathcal{D} = \{\mathsf{c}, \mathsf{y}, \mathsf{g}\}$, let us derive basis matrices from basis polynomials. From (6.32), the basis polynomials F_{c}, F_{g} and F_{y} can be represented as

$$F_{\mathsf{c}} = a^2c + P_1(a, c, y)z + P_2(a, c, y)z^2, \tag{6.44}$$
$$F_{\mathsf{y}} = a^2y + Q_1(a, c, y)z + Q_2(a, c, y)z^2, \tag{6.45}$$
$$F_{\mathsf{g}} = acy + R_1(a, c, y)z + R_2(a, c, y)z^2, \tag{6.46}$$

where $P_1(a, c, y)$, $P_2(a, c, y)$, $Q_1(a, c, y)$, $Q_2(a, c, y)$, $R_1(a, c, y)$, $R_2(a, c, y)$ are homogeneous polynomials of degree 2 which consist of a, c, y. Then, they satisfy the condition (6.33) as follows.

$$\left[F_{\mathsf{c}} - a^2c\right]_{z=0} = 0, \tag{6.47}$$
$$\left[F_{\mathsf{y}} - a^2y\right]_{z=0} = 0, \tag{6.48}$$
$$\left[F_{\mathsf{g}} - acy\right]_{z=0} = 0. \tag{6.49}$$

Furthermore, from (6.35), they must also satisfy

$$\Xi F_{\mathsf{c}} = \Xi F_{\mathsf{y}} = \Xi F_{\mathsf{g}}, \tag{6.50}$$

where $\Xi = \frac{\partial}{\partial a} + \frac{\partial}{\partial c} + \frac{\partial}{\partial y} + \frac{\partial}{\partial z}$. Since we have that

$$\Xi F_{\mathsf{c}} = (a^2 + 2ac + P_1) + (\Xi P_1 + 2P_2)z + (\Xi P_2)z^2, \tag{6.51}$$
$$\Xi F_{\mathsf{y}} = (a^2 + 2ay + Q_1) + (\Xi Q_1 + 2Q_2)z + (\Xi Q_2)z^2, \tag{6.52}$$
$$\Xi F_{\mathsf{g}} = (ac + cy + ya + R_1) + (\Xi R_1 + 2R_2)z + (\Xi R_2)z^2, \tag{6.53}$$

P_1, P_2, Q_1, Q_2, R_1 and R_2 must satisfy that

$$a^2 + 2ac + P_1 = a^2 + 2ay + Q_1 = ac + cy + ya + R_1, \tag{6.54}$$
$$\Xi P_1 + 2P_2 = \Xi Q_1 + 2Q_2 = \Xi R_1 + 2R_2, \tag{6.55}$$
$$\Xi P_2 = \Xi Q_2 = \Xi R_2. \tag{6.56}$$

Therefore, by solving (6.54)–(6.56), we obtain the following basis polynomials:

$$F_{\mathsf{c}} = a^2c + (2ay + cy)z + (a + c)z^2, \tag{6.57}$$
$$F_{\mathsf{y}} = a^2y + (2ac + cy)z + (a + y)z^2, \tag{6.58}$$
$$F_{\mathsf{g}} = acy + (ay + ac + a^2)z + (c + y)z^2, \tag{6.59}$$

which correspond to the following basis matrices.

$$\begin{aligned} B_{\mathsf{c}} &= C_3([\mathsf{00c}]) \odot C_3([\mathsf{0y1}]) \odot C_3([\mathsf{0y1}]) \odot C_3([\mathsf{cy1}]) \odot C_3([\mathsf{011}]) \odot C_3([\mathsf{c11}]) \\ &= \begin{bmatrix} \mathsf{00c00c} & \mathsf{0y101y} & \mathsf{0y101y} & \mathsf{cyy11c} & \mathsf{011011} & \mathsf{c11c11} \\ \mathsf{0c00c0} & \mathsf{y001y1} & \mathsf{y001y1} & \mathsf{yc1yc1} & \mathsf{101101} & \mathsf{1c11c1} \\ \mathsf{c00c00} & \mathsf{11yy00} & \mathsf{11yy00} & \mathsf{11ccyy} & \mathsf{110110} & \mathsf{11c11c} \end{bmatrix}, \end{aligned} \tag{6.60}$$

$$\begin{aligned} B_{\mathsf{y}} &= C_3([\mathsf{00y}]) \odot C_3([\mathsf{0c1}]) \odot C_3([\mathsf{0c1}]) \odot C_3([\mathsf{cy1}]) \odot C_3([\mathsf{011}]) \odot C_3([\mathsf{y11}]) \\ &= \begin{bmatrix} \mathsf{00y00y} & \mathsf{0c101c} & \mathsf{0c101c} & \mathsf{ycc11y} & \mathsf{011011} & \mathsf{y11y11} \\ \mathsf{0y00y0} & \mathsf{c001c1} & \mathsf{c001c1} & \mathsf{cy1cy1} & \mathsf{101101} & \mathsf{1y11y1} \\ \mathsf{y00y00} & \mathsf{11cc00} & \mathsf{11cc00} & \mathsf{11yycc} & \mathsf{110110} & \mathsf{11y11y} \end{bmatrix}, \end{aligned} \tag{6.61}$$

$$\begin{aligned} B_{\mathsf{g}} &= C_3([\mathsf{0cy}]) \odot C_3([\mathsf{0c1}]) \odot C_3([\mathsf{0y1}]) \odot C_3([\mathsf{001}]) \odot C_3([\mathsf{c11}]) \odot C_3([\mathsf{y11}]) \\ &= \begin{bmatrix} \mathsf{cyc00y} & \mathsf{0c101c} & \mathsf{0y101y} & \mathsf{100100} & \mathsf{c11c11} & \mathsf{y11y11} \\ \mathsf{yc0cy0} & \mathsf{c001c1} & \mathsf{y001y1} & \mathsf{010010} & \mathsf{1c11c1} & \mathsf{1y11y1} \\ \mathsf{00yycc} & \mathsf{11cc00} & \mathsf{11yy00} & \mathsf{001001} & \mathsf{11c11c} & \mathsf{11y11y} \end{bmatrix}. \end{aligned} \tag{6.62}$$

These basis matrices attain that $m = 36$, and $\alpha = \frac{1}{6}$. □

6.3.3 (n, n)-threshold Visual Secret Sharing Schemes

In the previous section, we show that if basis matrices consist of CP matrices, they can easily be derived by solving the simultaneous partial differential equations (6.33) and (6.35). But, it is difficult to obtain the solutions for (6.33) and (6.35) generally. However, in some special cases, we can derive the solution as follows:

For a set of colors $\mathcal{D} = \{\mathsf{d}_1, \mathsf{d}_2, \ldots, \mathsf{d}_J\}$, assume that $\mathsf{d}_j = \mathsf{d}_j^{\langle 1 \rangle} \sqcup \mathsf{d}_j^{\langle 2 \rangle} \sqcup \cdots \sqcup \mathsf{d}_j^{\langle n \rangle}$ where all $\mathsf{d}_j^{\langle i \rangle}$, $1 \le i \le n$, $1 \le j \le J$ are distinct. In this case, (6.33) and (6.35) become

$$\left[F_{\mathsf{d}_j} - \prod_{i=1}^{n} d_j^{\langle i \rangle} \right]_{z=0} = 0, \quad \text{for } 1 \le j \le J, \tag{6.63}$$

$$\Xi F_{\mathsf{d}_1} = \Xi F_{\mathsf{d}_2} = \cdots = \Xi F_{\mathsf{d}_J}, \tag{6.64}$$

respectively, where Ξ is given by

$$\Xi = \sum_{i=1}^{n} \sum_{j=1}^{J} \frac{\partial}{\partial d_j^{\langle i \rangle}} + \frac{\partial}{\partial z}. \tag{6.65}$$

In this case, the following theorem holds:

Theorem 6.13 (Koga et al. [66]) The basis polynomials satisfying (6.63)–(6.65) are given by

$$F_{\mathsf{d}_j} = \sum_{\substack{i=0 \\ i:\text{even}}}^{n-1} s_{j,n-i} z^i + \sum_{\substack{i=1 \\ i:\text{odd}}}^{n-1} \sum_{\substack{\ell=1 \\ \ell \ne j}}^{J} s_{\ell,n-i} z^i, \tag{6.66}$$

where $s_{j,\ell}$ is defined by

$$s_{j,\ell} = \begin{cases} \displaystyle\sum_{\substack{\{V_{i_1},V_{i_2},\ldots,V_{i_\ell}\}\subseteq \\ i_1<i_2<\cdots<i_\ell}} d_j^{\langle i_1\rangle} d_j^{\langle i_2\rangle}\cdots d_j^{\langle i_\ell\rangle}, & \text{if } 1\le \ell \le n, \\ 1, & \text{if } \ell = 0. \end{cases} \tag{6.67}$$

□

Proof of Theorem 6.13 Note that $s_{j,1} = \sum_{i=1}^n d_j^{\langle i\rangle}$ and $s_{j,n} = \prod_{i=1}^n d_j^{\langle i\rangle}$ from (6.67). Hence, since it holds that $[F_{\mathsf{d}_j} - s_{j,n}]_{z=0} = [F_{\mathsf{d}_j} - \prod_{i=1}^n d_j^{\langle i\rangle}]_{z=0} = 0$, F_{d_j} satisfy (6.63) for all $j = 1, 2, \ldots, J$. On the other hand, ΞF_{d_j} can be calculated as follows:

$$\begin{aligned}
&\Xi F_{\mathsf{d}_j} \\
&\overset{\text{(a)}}{=} \sum_{\substack{i=0\\ i:\text{even}}}^{n-1} \left(\sum_{l=1}^n \frac{\partial}{\partial d_j^{\langle l\rangle}} + \frac{\partial}{\partial z}\right) s_{j,n-i} z^i + \sum_{\substack{i=1\\ i:\text{odd}}}^{n-1}\sum_{\substack{\ell=1\\ \ell\neq j}}^{J} \left(\sum_{l=1}^n \frac{\partial}{\partial d_\ell^{\langle l\rangle}} + \frac{\partial}{\partial z}\right) s_{\ell,n-i} z^i \\
&\overset{\text{(b)}}{=} \sum_{\substack{i=0\\ i:\text{even}}}^{n-1} (i+1) s_{j,n-(i+1)} z^i + \sum_{\substack{i=2\\ i:\text{even}}}^{n-1} i s_{j,n-i} z^{i-1} + \sum_{\substack{\ell=1\\ \ell\neq j}}^{J}\sum_{\substack{i=1\\ i:\text{odd}}}^{n-1} (i+1) s_{\ell,n-(i+1)} z^i + \sum_{\substack{\ell=1\\ \ell\neq j}}^{J}\sum_{\substack{i=1\\ i:\text{odd}}}^{n-1} i s_{\ell,n-i} z^{i-1} \\
&= \sum_{\substack{i=1\\ i:\text{odd}}}^{n} i s_{j,n-i} z^{i-1} + \sum_{\substack{i=2\\ i:\text{even}}}^{n-1} i s_{j,n-i} z^{i-1} + \sum_{\substack{\ell=1\\ \ell\neq j}}^{J}\sum_{\substack{i=2\\ i:\text{even}}}^{n} i s_{\ell,n-i} z^{i-1} + \sum_{\substack{\ell=1\\ \ell\neq j}}^{J}\sum_{\substack{i=1\\ i:\text{odd}}}^{n-1} i s_{\ell,n-i} z^{i-1} \\
&= \sum_{i=1}^{n-1}\sum_{\ell=1}^{J} i s_{j,n-i} z^{i-1} + \begin{cases} n(J-1)z^{n-1}, & \text{if } n \text{ even}, \\ nz^{n-1}, & \text{if } n \text{ odd}, \end{cases}
\end{aligned} \tag{6.68}$$

where the marked equalities (a) and (b) hold from that

(a): $s_{j,\ell}$ does not contain $d_{j'}^{\langle i\rangle}$, $j \neq j'$.

(b): $\left(\sum_{l=1}^n \frac{\partial}{\partial d_j^{\langle l\rangle}}\right) s_{j,n-i} = (i+1) s_{j,n-(i+1)}$.

Therefore, it holds that $\Xi F_{\mathsf{d}_1} = \Xi F_{\mathsf{d}_2} = \cdots = \Xi F_{\mathsf{d}_J}$ since ΞF_{d_j} does not depend on j for any d_j. □

Remark 6.14 Note that although the simultaneous partial differential equations (6.63)–(6.65) are a special case of (6.33) and (6.35), the solutions of (6.33) and (6.35) can always be derived from the solutions (6.66) as shown in the following example. □

Example 6.15 In this example, we derive the basis polynomials satisfying (6.47)–(6.50) based on Theorem 6.13. In order to apply Theorem 6.13, we represent the conditions (6.47)–(6.49) as

$$[F_{\mathsf{c}} - a_1 a_2 c_1]_{z=0} = 0, \tag{6.69}$$

$$[F_{\mathsf{y}} - a_3 a_4 y_1]_{z=0} = 0, \tag{6.70}$$

$$[F_{\mathsf{g}} - a_5 c_2 y_2]_{z=0} = 0. \tag{6.71}$$

Then, from (6.66) in Theorem 6.13, we obtain that

$$F_{\mathsf{c}} = a_1a_2c_1 + (a_3a_4 + a_4y_1 + y_1a_3 + a_5c_2 + c_2y_2 + y_2a_5)z + (a_1 + a_2 + c_1)z^2, \quad (6.72)$$
$$F_{\mathsf{y}} = a_3a_4y_1 + (a_1a_2 + a_2c_1 + c_1a_1 + a_5c_2 + c_2y_2 + y_2a_5)z + (a_3 + a_4 + y_1)z^2, \quad (6.73)$$
$$F_{\mathsf{g}} = a_5c_2y_2 + (a_3a_4 + a_4y_1 + y_1a_3 + a_1a_2 + a_2c_1 + c_1a_1)z + (a_5 + c_2 + y_2)z^2. \quad (6.74)$$

By letting $a_1 = a_2 = \cdots = a_5 = a$, $c_1 = c_2 = c$, and $y_1 = y_2 = y$, we obtain

$$F_{\mathsf{c}} = a^2c + (a^2 + 3ay + 2cy)z + (2a + c)z^2, \quad (6.75)$$
$$F_{\mathsf{y}} = a^2y + (a^2 + 3ac + 2cy)z + (2a + y)z^2, \quad (6.76)$$
$$F_{\mathsf{g}} = acy + (2ay + 2ac + 2a^2)z + (a + c + y)z^2. \quad (6.77)$$

Note that (6.75)–(6.77) contain the common term $(a^2 + ac + ay)z + az^2$. From Theorem 6.7, we can delete the common terms from (6.75)–(6.77). Hence, we finally obtain

$$F_{\mathsf{c}} = a^2c + (2ay + cy)z + (a + c)z^2, \quad (6.78)$$
$$F_{\mathsf{y}} = a^2y + (2ac + cy)z + (a + y)z^2, \quad (6.79)$$
$$F_{\mathsf{g}} = acy + (ay + ac + a^2)z + (c + y)z^2, \quad (6.80)$$

which attains that the pixel expansion $m = 36$ and contrast $\alpha = \frac{1}{6}$. □

In the case that basis polynomials have no common terms, they are called *minimal* basis polynomials. We can show in the following theorem that the minimal basis polynomials can be uniquely determined from the simultaneous partial differential equations.

Theorem 6.16 (Koga et al. [66]) The minimal basis polynomials F_{d_j}, $j = 1, 2, \ldots, J$, which satisfy (6.33) and (6.35) are uniquely determined. □

Proof of Theorem 6.16 Suppose there exist another minimal basis polynomials $\tilde{F}_{\mathsf{d}_j}$ that satisfy (6.33) and (6.35), i.e.,

$$\Xi\tilde{F}_{\mathsf{d}_1} = \Xi\tilde{F}_{\mathsf{d}_2} = \cdots = \Xi\tilde{F}_{\mathsf{d}_J}, \quad (6.81)$$

and $[\tilde{F}_{\mathsf{d}_j} - d_j]_{z=0} = 0$ for $j = 1, 2, \ldots, J$. Then, consider the difference homogeneous polynomials f_{d_j}, $j = 1, 2, \ldots, J$, that is defined by

$$f_{\mathsf{d}_j} = F_{\mathsf{d}_j} - \tilde{F}_{\mathsf{d}_j}. \quad (6.82)$$

and the second difference homogeneous polynomial $g = f_{\mathsf{d}_j} - f_{\mathsf{d}_{j'}}$ for some fixed j and $j'(\neq j)$. Since f_{d_j}'s satisfy that

$$f_{\mathsf{d}_j}|_{z=0} = 0, \quad \text{for } j = 1, 2, \ldots, J \quad (6.83)$$
$$\Xi f_{\mathsf{d}_1} = \Xi f_{\mathsf{d}_2} = \cdots = \Xi f_{\mathsf{d}_J}, \quad (6.84)$$

g satisfies that

$$g|_{z=0} = f_{\mathsf{d}_j}|_{z=0} - f_{\mathsf{d}_{j'}}|_{z=0} = 0, \tag{6.85}$$

$$\Xi g = \Xi f_{\mathsf{d}_j} - \Xi f_{\mathsf{d}_{j'}} = 0. \tag{6.86}$$

From (6.86), g can be expressed as

$$g = g_1 z + g_2 z^2 + \cdots + g_{n-1} z^{n-1}, \tag{6.87}$$

where g_i, $i = 1, 2, \ldots, n-1$, are homogeneous polynomials of degree $n-i$ which do not contain z. Then, substituting (6.87) into (6.86), we obtain the following relation.

$$\Xi g = g_1 + \sum_{i=1}^{n-2} \left\{ \tilde{\Xi} g_i + (i+1) g_{i+1} \right\} z^i + \left(\tilde{\Xi} g_{n-1} \right) z^{n-1} = 0, \tag{6.88}$$

where $\tilde{\Xi} \stackrel{\text{def}}{=} \Xi - \frac{\partial}{\partial z}$. Equation (6.88) implies that $g_1 = g_2 = \cdots = g_{n-1} = 0$, and hence, we obtain that $g = 0$.

Since these arguments hold for any j, j', we have

$$f_{\mathsf{d}_1} = f_{\mathsf{d}_2} = \cdots = f_{\mathsf{d}_J} \stackrel{\text{def}}{=} f. \tag{6.89}$$

which does not depend on j. If $f \neq 0$, F_{d_j}'s or $\tilde{F}'_{\mathsf{d}_j}$'s are not minimal from (6.82). Hence, if both F_{d_j}'s and $\tilde{F}_{\mathsf{d}_j}$'s are minimal, it holds that $f = 0$. This means that the minimal basis polynomials are uniquely determined. □

The basis polynomials given by (6.57)–(6.59) and (6.78)–(6.80) in Examples 6.12 and 6.15, respectively, are the same, and they are the minimal basis polynomials. It is clear from Theorem 6.16 that pixel expansion m is also uniquely determined by the simultaneous partial differential equations. However, since the minimal basis polynomials depends on the condition (6.33), the pixel expansion m also depends on the way how each d_j is constructed from the colors in $\mathcal{E}$ as shown in the following example.

Example 6.17 Let us consider the $(3, 3, \mathcal{E}, \mathcal{D})$-VSS scheme with color sets $\mathcal{D} = \{\mathsf{y}, \mathsf{m}, \mathsf{c}, \mathsf{r}, \mathsf{g}, \mathsf{b}\}$. If we use $\mathcal{E} = \{\mathsf{0}, \mathsf{y}, \mathsf{m}, \mathsf{c}, \mathsf{1}\}$ and the conditions

$$\begin{aligned} &[F_{\mathsf{y}} - a^2 y]_{z=0} = 0, [F_{\mathsf{m}} - a^2 m]_{z=0} = 0, [F_{\mathsf{c}} - y a^2 c]_{z=0} = 0, \\ &[F_{\mathsf{r}} - amy]_{z=0} = 0, [F_{\mathsf{g}} - acy]_{z=0} = 0, [F_{\mathsf{b}} - acm]_{z=0} = 0, \end{aligned} \tag{6.90}$$

which means that we use $\mathsf{r} = \mathsf{m} \sqcup \mathsf{y}$, $\mathsf{g} = \mathsf{c} \sqcup \mathsf{y}$, $\mathsf{b} = \mathsf{c} \sqcup \mathsf{m}$, then we obtain the following basis polynomials with $m = 60$ and $\alpha = \frac{1}{10}$:

$$F_{\mathsf{y}} = a^2 y + (2ac + 2am + cm + cy + my) z + (a + y) z^2, \tag{6.91}$$

$$F_{\mathsf{m}} = a^2 m + (2ac + 2ay + cm + cy + my) z + (a + m) z^2, \tag{6.92}$$

$$F_{\mathsf{c}} = a^2 c + (2am + 2ay + cm + cy + my) z + (a + c) z^2, \tag{6.93}$$

$$F_{\mathsf{r}} = amy + (a^2 + 2ac + am + ay + cm + cy) z + (m + y) z^2, \tag{6.94}$$

$$F_{\mathsf{g}} = acy + (a^2 + ac + 2am + ay + cm + my) z + (c + y) z^2, \tag{6.95}$$

$$F_{\mathsf{b}} = acm + (a^2 + ac + am + 2ay + cy + my) z + (c + m) z^2. \tag{6.96}$$

On the other hand, if we use $\mathcal{E} = \{0, \mathsf{y}, \mathsf{m}, \mathsf{c}, \mathsf{r}, \mathsf{g}, \mathsf{b}, 1\}$ and the conditions

$$[F_{\mathsf{y}} - a^2 y]_{z=0} = 0, [F_{\mathsf{m}} - a^2 m]_{z=0} = 0, [F_{\mathsf{c}} - a^2 c]_{z=0} = 0,$$
$$[F_{\mathsf{r}} - a^2 r]_{z=0} = 0, [F_{\mathsf{g}} - a^2 g]_{z=0} = 0, [F_{\mathsf{b}} - a^2 b]_{z=0} = 0, \tag{6.97}$$

we have

$$F_{\mathsf{y}} = a^2 y + 2a(m + c + r + g + b)z + yz^2, \tag{6.98}$$
$$F_{\mathsf{m}} = a^2 m + 2a(y + c + r + g + b)z + mz^2, \tag{6.99}$$
$$F_{\mathsf{c}} = a^2 c + 2a(y + m + r + g + b)z + cz^2, \tag{6.100}$$
$$F_{\mathsf{r}} = a^2 r + 2a(y + m + c + g + b)z + rz^2, \tag{6.101}$$
$$F_{\mathsf{g}} = a^2 g + 2a(y + m + c + r + b)z + gz^2, \tag{6.102}$$
$$F_{\mathsf{b}} = a^2 b + 2a(y + m + c + r + g)z + bz^2, \tag{6.103}$$

which attain $m = 72$ and $\alpha = \frac{1}{12}$. Note that each solution is minimal for each condition. But the attainable pixel expansions are different. □

Example 6.17 implies that we must choose the condition (6.33) adequately in order to attain smaller pixel expansion and higher contrast. However, it is hard to derive the conditions (6.33) that can attain the smallest m and highest α.

6.3.4 (k, n)-threshold Visual Secret Sharing Schemes

In this subsection, we show a method to derive basis matrices for $(k, n, \mathcal{E}, \mathcal{D})$-VSS schemes based on CP matrices. First, let $F^{(k)}_{\mathsf{d}_1}, F^{(k)}_{\mathsf{d}_2}, \ldots, F^{(k)}_{\mathsf{d}_J}$ be basis polynomials for a $(k, k, \mathcal{E}, \mathcal{D})$-VSS scheme, which can be derived by the method in Section 6.3.3. Then, we have the next theorem:

Theorem 6.18 (Koga [63], Koga et al. [66]) Let $F^{(k)}_{\mathsf{d}_j}$, $j = 1, 2, \ldots, J$, be basis polynomials for a $(k, k, \mathcal{E}, \mathcal{D})$-VSS scheme. Then, basis polynomials $F_{\mathsf{d}_1}, F_{\mathsf{d}_2}, \ldots, F_{\mathsf{d}_J}$ defined by

$$F_{\mathsf{d}_j} = z^{n-k} F^{(k)}_{\mathsf{d}_j}, \tag{6.104}$$

are the basis polynomials of the $(k, n, \mathcal{E}, \mathcal{D})$-VSS scheme. □

Proof of Theorem 6.18 In the polynomial representation of VSS schemes, the deletion of arbitrary $n-\ell$ rows from the basis matrices is equivalent to apply the operator Ξ to the corresponding basis polynomials $n - \ell$ times. Therefore, in order to prove this theorem, it is sufficient to show that

$$\left[\Xi^{n-k} F_{\mathsf{d}_j} - C_j d_j\right]_{z=0} = \left[F^{(k)}_{\mathsf{d}_j} - d_j\right]_{z=0} = 0 \quad \text{for any } j = 1, 2, \ldots, J, \tag{6.105}$$
$$\Xi^{n-k+1} F_{\mathsf{d}_1} = \Xi^{n-k+1} F_{\mathsf{d}_2} = \cdots = \Xi^{n-k+1} F_{\mathsf{d}_J}, \tag{6.106}$$

where C_j is a positive integer. Note that (6.105) and (6.106) correspond to Definition 6.2-(i) and (ii), respectively.

First, we show (6.105), which is equivalent to $\left[\Xi^{n-k}F_{\mathsf{d}_j} - C_j F^{(k)}_{\mathsf{d}_j}\right]_{z=0} = 0$ for some positive integer C_j. By calculating $\Xi^{n-k}F_{\mathsf{d}_j}$ for (6.104), we obtain

$$\begin{aligned}\Xi^{n-k}F_{\mathsf{d}_j} &= \sum_{i=0}^{n-k}\binom{n-k}{i}\Xi^{n-k-i}F^{(k)}_{\mathsf{d}_j}\left(\Xi^i z^{n-k}\right)\\ &= \sum_{i=0}^{n-k}\binom{n-k}{i}\frac{(n-k)!}{(n-k-i)!}\left(\Xi^{n-k-i}F^{(k)}_{\mathsf{d}_j}\right)z^{n-k-i}. \end{aligned} \tag{6.107}$$

The last equality in (6.107) holds since $\Xi^{n-k+1}\cdot z^{n-k} = 0$. Substituting $z = 0$ into (6.107), we have $\left[\Xi^{n-k}F_{\mathsf{d}_j} - (n-k)!F^{(k)}_{\mathsf{d}_j}\right]_{z=0} = 0$, and hence, it is satisfied by $C_j = (n-k)!$. Next, we prove (6.106). $\Xi^{n-k+1}F_{\mathsf{d}_j}$ can be calculated as follows:

$$\begin{aligned}\Xi^{n-k+1}F_{\mathsf{d}_j} &= \Xi^{n-k+1}\left(F^{(k)}_{\mathsf{d}_j}z^{n-k}\right)\\ &= \sum_{i=0}^{n-k+1}\binom{n-k+1}{i}\Xi^{n-k+1-i}F^{(k)}_{\mathsf{d}_j}\left(\Xi^i z^{n-k}\right)\\ &= \sum_{i=0}^{n-k}\binom{n-k+1}{i}\frac{(n-k)!}{(n-k-i)!}\left(\Xi^{n-k+1-i}F^{(k)}_{\mathsf{d}_j}\right)z^{n-k-i}. \end{aligned} \tag{6.108}$$

Furthermore, since $F^{(k)}_{\mathsf{d}_j}$'s are the basis polynomials of a $(k,k,\mathcal{E},\mathcal{D})$-VSS scheme, we obtain

$$\Xi^{\ell}F^{(k)}_{\mathsf{d}_1} = \Xi^{\ell}F^{(k)}_{\mathsf{d}_2} = \cdots = \Xi^{\ell}F^{(k)}_{\mathsf{d}_J}, \tag{6.109}$$

for all $\ell \geq 1$. By combining (6.108) and (6.109), (6.106) is established. □

Example 6.19 For the $(2,3,\mathcal{E},\mathcal{D})$-VSS scheme with $\mathcal{E} = \{0,\mathsf{y},\mathsf{c},\mathsf{g},0\}$ and $\mathcal{D} = \{\mathsf{c},\mathsf{y},\mathsf{g}\}$, basis polynomials are given from (6.104) by

$$F_{\mathsf{c}} = z\cdot F^{(2)}_{\mathsf{c}} = acz + yz^2, \tag{6.110}$$
$$F_{\mathsf{y}} = z\cdot F^{(2)}_{\mathsf{y}} = ayz + cz^2, \tag{6.111}$$
$$F_{\mathsf{g}} = z\cdot F^{(2)}_{\mathsf{g}} = cyz + az^2, \tag{6.112}$$

where $F^{(2)}_{\mathsf{c}}, F^{(2)}_{\mathsf{y}}, F^{(2)}_{\mathsf{g}}$ are given by (6.41)–(6.43) in Example 6.11, which are the basis polynomials of the $(2,2,\mathcal{E},\mathcal{D})$-VSS scheme. □

Remark 6.20 The basic idea of CP matrices and their polynomial representations are introduced by Koga [63], and the algebraic construction of VSS schemes are developed in [66]. In this thesis, the algebraic construction is described by using the notion of equivalence class, which is introduced in [52]. Furthermore, it is slightly improved from [66] since the algebraic construction in [66] cannot be applied to the case of $1 \in \mathcal{D}$ as follows.

In [66], the simultaneous partial differential equations for basis polynomials F_{d_j} are given by

$$F_{\mathsf{d}_j}|_{z=0} = \prod_{i=1}^{h_{\mathsf{d}_j}} \left(d_j^{\langle i \rangle}\right)^{u_i}, \tag{6.113}$$

$$\Xi F_{\mathsf{d}_j} = F', \ \text{ for all } \ j, \tag{6.114}$$

which correspond to (6.33) and (6.35), respectively. But, in the case of $\mathsf{d}_j = 1$ for some j, there must exist at least one $d_j^{\langle i \rangle} = z$ in the right hand side of (6.113) although $z = 0$ is assumed in the left hand side of (6.113), which is a contradiction. Hence, it is assumed in [66] that $1 \notin \mathcal{D}$.

On the contrary, it is easy to see that (6.33) is valid even in the case of $1 \in \mathcal{D}$. Hence, we use (6.33) instead of (6.113). □

6.4 Visual Secret Sharing Schemes for General Access Structures

In this section, we describe how to construct a VSS scheme for a given general access structure Γ based on a cumulative map ψ_Γ defined in Chapter 4. Refer Chapter 2 for general access structures.

Let $\Gamma = \{\mathcal{A}_\mathsf{Q}, \mathcal{A}_\mathsf{F}\}$ be a given general access structure for a share set $\boldsymbol{V} = \{V_1, V_2, \ldots, V_n\}$.[8] Then, (k, n)-threshold VSS schemes in Definition 6.2 can be generalized to VSS schemes for general access structure Γ as follows:

Definition 6.21 (Koga et al. [66]) For $\mathcal{D} = \{\mathsf{d}_1, \mathsf{d}_2, \ldots, \mathsf{d}_J\}$ and pixel expansion m, an $n \times m$ matrix B_{d_j} is called a *basis matrix* of d_j for access structure Γ if all B_{d_j}, $j = 1, 2, \ldots, J$ satisfy the following conditions:

(i) For the minimal qualified sets $\mathcal{A}_\mathsf{Q}^-$ of Γ, it holds for any $\boldsymbol{Q} \in \mathcal{A}_\mathsf{Q}^-$ that

$$\eta\left(B_{\mathsf{d}_j}[\![\boldsymbol{Q}]\!]\right) \sim [\, \mathsf{d}_j \, \mathsf{d}_j \, \cdots \, \mathsf{d}_j \ \ 1 \, 1 \cdots 1], \tag{6.115}$$

where the number of d_j is constant. In the case of $\mathsf{d}_j = 1$, the right hand side of (6.115) consists of only $\mathsf{1}$'s.

(ii) For any set $\boldsymbol{F} \in \mathcal{A}_\mathsf{F}$, all $B_{\mathsf{d}_j}[\![\boldsymbol{F}]\!]$, $j = 1, 2, \ldots, J$, belong to the same equivalence class in $\mathcal{E}^{|\ |^m}/\!\sim$.

A VSS scheme for an access structure Γ is called a $(\Gamma, \boldsymbol{V}, \mathcal{E}, \mathcal{D})$-*VSS scheme* if for each color $\mathsf{d}_j \in \mathcal{D}$ each pixel d_j is determined by a matrix randomly selected from $\langle B_{\mathsf{d}_j} \rangle \in \mathcal{E}^{nm}/\!\sim$, where B_{d_j} is the basis matrix of d_j. □

[8] In Part II, we treat only perfect VSS schemes. Hence, for simplicity, notation $\Gamma = \{\mathcal{A}_\mathsf{Q}, \mathcal{A}_\mathsf{F}\}$ is used for an access structure in Part II instead of $\Gamma = \{\mathcal{A}_1, \mathcal{A}_0\}$ defined in Part I, where $\mathcal{A}_\mathsf{Q}$ is the family of qualified sets and $\mathcal{A}_\mathsf{F}$ is the family of forbidden sets.

Note that the contrast can be defined in the same way as Definition 6.3.

Example 6.22 Let $\Gamma_1 = \{\mathcal{A}_{\mathsf{Q}}, \mathcal{A}_{\mathsf{F}}\}$ be an access structure for $\boldsymbol{V} = \{V_1, V_2, V_3, V_4\}$, which is defined as follows:

$$\mathcal{A}_{\mathsf{Q}}^{-} = \{\{V_1, V_2\}, \{V_2, V_3\}, \{V_3, V_4\}\}, \tag{6.116}$$
$$\mathcal{A}_{\mathsf{F}}^{+} = \{\{V_1, V_4\}, \{V_1, V_3\}, \{V_2, V_4\}\}. \tag{6.117}$$

Then, the basis matrices of the $(\Gamma_1, \boldsymbol{V}, \mathcal{E}, \mathcal{D})$-VSS scheme with $\mathcal{E} = \{\mathsf{0}, \mathsf{c}, \mathsf{y}, \mathsf{g}, \mathsf{1}\}$ and $\mathcal{D} = \{\mathsf{c}, \mathsf{y}, \mathsf{g}\}$ are given by

$$B_{\mathsf{c}} = \begin{bmatrix} \mathsf{c00c0011yy0011yy0011ccyy10101c1c} \\ \mathsf{0cc0ccyy1111yy1111gg111111111111} \\ \mathsf{c0cc0c111y1y111y1y11g11g11111111} \\ \mathsf{0c00c0y001y1y001y1yc1yc10101c1c1} \end{bmatrix}, \tag{6.118}$$

$$B_{\mathsf{y}} = \begin{bmatrix} \mathsf{y00y0011cc0011cc0011yycc10101y1y} \\ \mathsf{0yy0yycc1111cc1111gg111111111111} \\ \mathsf{y0yy0y111c1c111c1c11g11g11111111} \\ \mathsf{0y00y0c001c1c001c1cy1cy10101y1y1} \end{bmatrix}, \tag{6.119}$$

$$B_{\mathsf{g}} = \begin{bmatrix} \mathsf{00yycc11cc0011yy000010011c1c1y1y} \\ \mathsf{ggccyycc1111yy111111011011111111} \\ \mathsf{cygycg111c1c111y1y10110111111111} \\ \mathsf{yc0cy0c001c1y001y1010010c1c1y1y1} \end{bmatrix}. \tag{6.120}$$

Then, it holds that $m = 32$, $\alpha = \frac{3}{16}$. □

We note that the multiple assignment map [47] treated in Chapter 4 is suitable for VSS schemes. Let B_{d_j} and $\tilde{B}_{\mathsf{d}_j}$, $j = 1, 2, \ldots, J$, be the basis matrices of $(\Gamma, \boldsymbol{V}, \mathcal{E}, \mathcal{D})$-VSS and $(t, t, \mathcal{E}, \mathcal{D})$-VSS schemes, respectively, where t is the cardinality of $\mathcal{A}_{\mathsf{F}}^{+}$, i.e., $\mathcal{A}_{\mathsf{F}}^{+} = \{\boldsymbol{F}_1, \boldsymbol{F}_2, \ldots, \boldsymbol{F}_t\}$ for $\Gamma = \{\mathcal{A}_{\mathsf{Q}}, \mathcal{A}_{\mathsf{F}}\}$. Letting $\boldsymbol{W}_{(t,t)} = \left\{W_1^{(t)}, W_2^{(t)}, \ldots, W_t^{(t)}\right\}$ be the set of *primitive* shares for the $(t, t, \mathcal{E}, \mathcal{D})$-VSS scheme, the *cumulative map* $\psi_\Gamma : \{1, 2, \ldots, n\} \to 2^{\boldsymbol{W}_{(t,t)}}$ is defined by

$$\psi_\Gamma(i) = \bigcup_{j : V_i \notin \ _j} \left\{W_j^{(t)}\right\}. \tag{6.121}$$

Then, the basis matrices B_{d_j} can be obtained from $\tilde{B}_{\mathsf{d}_j}$ and the cumulative map ψ_Γ as follows:

$$B_{\mathsf{d}_j}[\![\{V_\ell\}]\!] = \eta\left(\tilde{B}_{\mathsf{d}_j}[\![\psi_\Gamma(\ell)]\!]\right). \tag{6.122}$$

It is pointed out (but not proved) in [1] that the basis matrices of VSS schemes with general access structures for BW-binary secret images can be obtained by (6.122). The same arguments hold for a color secret image as shown in the next theorem.

Theorem 6.23 (Koga et al. [66]) Let $\Gamma = \{\mathcal{A}_{\mathsf{Q}}, \mathcal{A}_{\mathsf{F}}\}$ be a given general access structure. Then, the basis matrices of the $(\Gamma, \boldsymbol{V}, \mathcal{E}, \mathcal{D})$-VSS scheme can be obtained from (6.122). □

Proof of Theorem 6.23 From Chapter 4, the cumulative map $\psi_\Gamma(\cdot)$ satisfies following conditions.

$$\Psi_\Gamma(\boldsymbol{A}) \stackrel{\text{def}}{=} \bigcup_{V_i \in \boldsymbol{A}} \psi_\Gamma(i) = \boldsymbol{W}_{(t,t)}, \text{ for all } \boldsymbol{A} \in \mathcal{A}_{\mathsf{Q}}^- \tag{6.123}$$

$$\Psi_\Gamma(\boldsymbol{A}) \stackrel{\text{def}}{=} \bigcup_{V_i \in \boldsymbol{A}} \psi_\Gamma(i) \subsetneq \boldsymbol{W}_{(t,t)}, \text{ for all } \boldsymbol{A} \in \mathcal{A}_{\mathsf{F}}^+ \tag{6.124}$$

Hence, for a qualified set $\boldsymbol{Q} = \{V_{i_1}, V_{i_2}, \cdots, V_{i_p}\}$, we have

$$\begin{aligned}
\eta(B_{\mathsf{d}_j}[\![\boldsymbol{Q}]\!]) &= \eta\left(\tilde{B}_{\mathsf{d}_j}[\![\psi_\Gamma(i_1)]\!]\right) \stackrel{m}{\sqcup} \eta\left(\tilde{B}_{\mathsf{d}_j}[\![\psi_\Gamma(i_2)]\!]\right) \stackrel{m}{\sqcup} \cdots \stackrel{m}{\sqcup} \eta\left(\tilde{B}_{\mathsf{d}_j}[\![\psi_\Gamma(i_p)]\!]\right) \\
&= \eta\left(\tilde{B}_{\mathsf{d}_j}[\![\Psi_\Gamma(\boldsymbol{Q})]\!]\right) \\
&= \eta\left(\tilde{B}_{\mathsf{d}_j}[\![\boldsymbol{W}_{(t,t)}]\!]\right),
\end{aligned} \tag{6.125}$$

which is equivalent to $[\,\mathsf{d}_j\ \mathsf{d}_j \cdots \mathsf{d}_j\ 1\ 1\ \cdots 1]$ from the definition of $\tilde{B}_{\mathsf{d}_j}$.

Next, for a forbidden set $\boldsymbol{F} = \{V_{i_1}, V_{i_2}, \ldots, V_{i_q}\}$, it holds that

$$\tilde{B}_{\mathsf{d}_1}[\![\Psi_\Gamma(\boldsymbol{F})]\!] \sim \tilde{B}_{\mathsf{d}_2}[\![\Psi_\Gamma(\boldsymbol{F})]\!] \sim \cdots \sim \tilde{B}_{\mathsf{d}_J}[\![\Psi_\Gamma(\boldsymbol{F})]\!], \tag{6.126}$$

since $\Psi_\Gamma(\boldsymbol{F}) \subsetneq \boldsymbol{W}_{(t,t)}$ from (6.124). Hence, letting B be a matrix that is equivalent to (6.126), we obtain

$$B_{\mathsf{d}_j}[\![\boldsymbol{F}]\!] = \begin{bmatrix} \eta(\tilde{B}_{\mathsf{d}_j}[\![\psi_\Gamma(i_1)]\!]) \\ \eta(\tilde{B}_{\mathsf{d}_j}[\![\psi_\Gamma(i_2)]\!]) \\ \vdots \\ \eta(\tilde{B}_{\mathsf{d}_j}[\![\psi_\Gamma(i_q)]\!]) \end{bmatrix} \sim \begin{bmatrix} \eta(B[\![\psi_\Gamma(i_1)]\!]) \\ \eta(B[\![\psi_\Gamma(i_2)]\!]) \\ \vdots \\ \eta(B[\![\psi_\Gamma(i_q)]\!]) \end{bmatrix}, \tag{6.127}$$

which does not depend on j. Therefore, Definition 6.21-(ii) holds for all $B_{\mathsf{d}_j}[\![\boldsymbol{F}]\!]$, $j = 1, 2, \ldots, J$. □

Example 6.24 We derive the basis matrices of the $(\Gamma_1, \boldsymbol{V}, \mathcal{E}, \mathcal{D})$-VSS scheme with $\mathcal{E} = \{0, \mathsf{c}, \mathsf{y}, \mathsf{g}, 1\}$, $\mathcal{D} = \{\mathsf{c}, \mathsf{y}, \mathsf{g}\}$, and $\Gamma_1 = \{\mathcal{A}_{\mathsf{Q}}, \mathcal{A}_{\mathsf{F}}\}$ which is the access structure defined by (6.116) and (6.117) in Example 6.22. The cumulative map is given by

$$\psi_\Gamma(1) = \left\{W_3^{(3)}\right\}, \tag{6.128}$$

$$\psi_\Gamma(2) = \left\{W_1^{(3)}, W_2^{(3)}\right\}, \tag{6.129}$$

$$\psi_\Gamma(3) = \left\{W_1^{(3)}, W_3^{(3)}\right\}, \tag{6.130}$$

$$\psi_\Gamma(4) = \left\{W_2^{(3)}\right\}, \tag{6.131}$$

where $W_i^{(3)} \in \boldsymbol{W}_{(3,3)}$. By applying (6.122) to the basis matrices of the $(3, 3, \mathcal{E}, \mathcal{D})$-VSS scheme in (6.60)–(6.62) in Example 6.12, we obtain

$$\hat{B}_{\mathsf{c}} = \begin{bmatrix} \mathsf{c00c0011yy0011yy0011ccyy11011011c11c} \\ \mathsf{0cc0ccyy1111yy1111gg1111111111111111} \\ \mathsf{c0cc0c111y1y111y1y11g11g111111111111} \\ \mathsf{0c00c0y001y1y001y1yc1yc11011011c11c1} \end{bmatrix}, \tag{6.132}$$

$$\hat{B}_{\mathsf{y}} = \begin{bmatrix} \mathsf{y00y0011cc0011cc0011yycc11011011y11y} \\ \mathsf{0yy0yycc1111cc1111gg1111111111111111} \\ \mathsf{y0yy0y111c1c111c1c11g11g111111111111} \\ \mathsf{0y00y0c001c1c001c1cy1cy11011011y11y1} \end{bmatrix}, \tag{6.133}$$

$$\hat{B}_{\mathsf{g}} = \begin{bmatrix} \mathsf{00yycc11cc0011yy0000100111c11c11y11y} \\ \mathsf{ggccyycc1111yy1111110110111111111111} \\ \mathsf{cygycg111c1c111y1y101101111111111111} \\ \mathsf{yc0cy0c001c1y001y10100101c11c11y11y1} \end{bmatrix}. \tag{6.134}$$

For example, the second rows of $\hat{B}_{\mathsf{c}}$, $\hat{B}_{\mathsf{y}}$, $\hat{B}_{\mathsf{g}}$ are obtained by stacking the 1st and 2nd rows of (6.60)–(6.62), respectively.

Finally, from Theorem 6.7, we can delete 4×4 submatrix which consists of all 1 from $\hat{B}_{\mathsf{c}}, \hat{B}_{\mathsf{y}}, \hat{B}_{\mathsf{g}}$, and the basis matrices shown in (6.118)–(6.120) can be obtained. □

Chapter 7

Visual Secret Sharing Schemes for Gray-scale Images

7.1 Introduction

In many studies of VSS schemes, a secret image is usually assumed to be huge letters and/or simple geometrical shapes, e.g., circles, triangles, etc. But, if we can encrypt gray-scale images, a picture, for instance shown in Figure 7.1, can be encrypted as a secret image. In [14], VSS schemes for gray-scale images, for short VSS-GS schemes, are studied, and the necessary and sufficient condition is derived to construct VSS-GS schemes for general access structures. However, concerning VSS-GS scheme, the optimality has not been considered sufficiently, and only the minimum contrast is treated. In this chapter, we consider average contrast and brightness offset in addition to the minimum contrast, and we give the optimal construction of VSS-GS schemes for (n, n)-threshold access structures.

As we showed in Chapter 6, (n, n)-VSS schemes can be constructed algebraically by using polynomials and simultaneous partial differential equations. This method is first derived for color images in [66] and extended to BW-binary images in [72]. In this chapter, we extend this method to gray-scale images. Furthermore, we show that the optimal scheme in all the (n, n)-VSS-GS schemes can be constructed by the proposed method. In this chapter, we consider VSS-GS schemes only for (n, n)-threshold access structures because VSS-GS schemes with (k, n)-threshold or general access structures can be constructed from (t, t)-VSS-GS schemes in the same way as shown in Theorems 6.18 or 6.23, respectively.

This chapter is organized as follows. In Section 7.2, (n, n)-VSS-GS schemes, average and minimum contrasts, and brightness offset are formally defined, and the polynomial representations of (n, n)-VSS-GS schemes are described. Section 7.3 is devoted to show that the optimal (n, n)-VSS-GS scheme, in the viewpoint of resolution, can be constructed by using the polynomial representation. Then, in Section 7.4, we derive tight upper bounds of the average and minimum contrasts. Finally in Section 7.5, we extend gray-scale images to color images with shades.

In Section A.1, we show examples of the VSS-GS-L schemes based on the results obtained

Figure 7.1. Original secret image with 8-depths gray-scale.

in this chapter.

7.2 Preliminaries

7.2.1 Definitions

A secret image is assumed to be a gray-scale image with L depths, $L \geq 2$, which is encrypted to n images called *shares*. Let $\boldsymbol{V} = \{V_1, V_2, \ldots, V_n\}$ be the set of shares. Each pixel on the secret image is expanded to m subpixels. Parameter m is called *pixel expansion*, which should be as small as possible in the viewpoint of resolution for decrypted images. Each subpixel consists of white or black, and a gray depth of a pixel is realized by a composition of white and black subpixels. Hence, we assume that $\mathcal{E} = \{0, 1\}$ and the mixture is expressed by the "*OR*" operation, which is defined as $0 \sqcup 0 = 0$, $1 \sqcup 0 = 0 \sqcup 1 = 1 \sqcup 1 = 1$.

In VSS schemes for gray-scale images with L depths, for short VSS-GS-L schemes, a pixel with the ℓ-th gray depth, $\ell = 1, 2, \ldots, L$, is encrypted into an $n \times m$ matrix $T_{(\ell)}$. The (i, j) element of $T_{(\ell)}$ represents the j-th subpixel of the i-th share, and it takes 0 or 1 when the corresponding subpixel takes white or black, respectively. Then, $(\mathcal{A}_{\mathsf{Q}}, \mathcal{A}_{\mathsf{F}})$-VSS-GS-$L$ schemes are defined as follows:

Definition 7.1 A VSS-GS scheme is called an $(\mathcal{A}_{\mathsf{Q}}, \mathcal{A}_{\mathsf{F}})$-*VSS-GS-$L$ scheme* if each pixel with the ℓ-th gray depth is determined by matrix $T_{(\ell)}$ which is randomly selected for each pixel from the following equivalence class $\langle B_{(\ell)} \rangle$.

(i) For any minimal qualified set $\boldsymbol{Q} \in \mathcal{A}_{\mathsf{Q}}^{-}$ and pixel expansion m, the representatives $B_{(\ell)}$, which are called *basis matrices*, satisfy that

$$m - w(\eta(B_{(1)}[\![\boldsymbol{Q}]\!])) = \delta_{(1)}, \tag{7.1}$$

$$w(\eta(B_{(\ell-1)}[\![\boldsymbol{Q}]\!])) - w(\eta(B_{(\ell)}[\![\boldsymbol{Q}]\!])) = \delta_{(\ell)}, \ \text{ for } \ \ell = 2, 3, \ldots, L, \tag{7.2}$$

where $w(\boldsymbol{v})$ stands for the Hamming weight of $\boldsymbol{v}$, and $\delta_{(\ell)}$ is the *relative difference of brightness* between the $(\ell-1)$-th and ℓ-th gray depths. $\delta_{(\ell)}$ is an integer which satisfies $\delta_{(1)} \geq 0$ and $\delta_{(\ell)} \geq 1$ for $\ell = 2, 3, \ldots, L$.

(ii) For any forbidden set $\boldsymbol{F} \in \mathcal{A}_{\mathsf{F}}$, all $B_{(\ell)}[\![\boldsymbol{F}]\!]$, $\ell = 1, 2, \ldots, L$, belong to the same equivalence class in $\mathcal{E}^{|\ |^m}\!/\!\sim$. □

We note from the above definition that basis matrix $B_{(1)}$ corresponds to the darkest pixel while $B_{(L)}$ expresses the brightest one in the decrypted image. We also note that Definition 7.1 can be considered as the special case of Definition 6.2 such that $\mathcal{E} = \{0, 1\}$ and $\mathsf{d}_j \in \mathcal{D}$ is a gray with the j-th depth.

Next we define *contrasts* and *brightness offset* which guarantee the clearness and the brightness of decrypted images, respectively.

Definition 7.2 Let $B_{(\ell)}$ be the basis matrices of an $(\mathcal{A}_{\mathsf{Q}}, \mathcal{A}_{\mathsf{F}})$-VSS-GS-$L$ scheme. Then, *relative contrasts* are defined as $\alpha_{(\ell)} = \frac{\delta_{(\ell)}}{m}$ for $\ell = 2, 3, \ldots, L$, where m is the pixel expansion. Furthermore, the *minimum contrast*, the *average contrast*, and the *brightness offset* of a decrypted image are defined as

$$\alpha_{\min} = \min_{2 \leq \ell \leq L} \alpha_{(\ell)}, \tag{7.3}$$

$$\alpha_{\mathrm{ave}} = \frac{\sum_{\ell=2}^{L} \alpha_{(\ell)}}{L-1}, \tag{7.4}$$

$$\beta = \frac{\delta_{(1)}}{m}, \tag{7.5}$$

respectively.[1] □

$\alpha_{\min}$ represents the worst clearness in two adjacent gray depths while α_{ave} gives the average clearness of a decrypted image.

In the case of BW-binary images, i.e., $L = 2$, these contrasts $\alpha_{\min}$ and α_{ave} coincide with each other and they are equal to a contrast

$$\alpha_{NS} = \frac{\delta_{(2)}}{m}, \tag{7.6}$$

[1] In [14], $\alpha_{(\ell)} = \frac{\delta_{(\ell)}}{m}$ is called as "relative differences" rather than "relative contrasts".

which is defined by Naor-Shamir [81] for BW-binary secret images. Hence, $\alpha_{\min}$ and α_{ave} can be considered as extensions of α_{NS}. Since α_{NS} does not reflect the effect of brightness offset β, Verheul and Van Tilborg [117] proposed another contrast

$$\alpha_{VV} = \frac{\delta_{(2)}}{m\left(\delta_{(2)} + 2\delta_{(1)}\right)}. \tag{7.7}$$

But it is pointed out in [36] that α_{VV} has a defect such that α_{VV} is always equal to $1/m$ when $\delta_{(1)} = 0$. Instead of α_{VV}, Eisen and Stinson [36] proposed a new contrast

$$\alpha_{ES} = \frac{\delta_{(2)}}{m + \delta_{(1)}} = \frac{\alpha_{NS}}{1+\beta}, \tag{7.8}$$

where two effects of α_{NS} and β are included in the contrast α_{ES}. In [36], [117], it is shown for the BW-binary case that β effects the clearness, and the larger the value of $\delta_{(2)}$ is and the smaller the value of $\delta_{(1)}$ is, the clearer the decrypted image is. In other words, large α_{NS} and small β are desirable. However, such consequences cannot be applied to the case of gray-scale generally.

In the case of VSS-GS schemes, the brightest pixel on a decrypted image cannot become complete white while complete black can be realized. In addition, the darkest pixel on a decrypted image is not always complete black. Hence, even if two VSS-GS schemes have the same relative contrasts $\alpha_{(\ell)}$, the brightness offset β may be different. The larger β is, the brighter the decrypted image is. When $\beta = 0$, i.e., $\delta_{(1)} = 0$, then the darkest pixel is complete black. For instance, Figure 7.2-(a) has $\beta = 0$ and $\alpha_{(\ell)} = \frac{1}{16}$ for $\ell = 2, 3, \ldots, 8$, which means $\alpha_{\min} = \alpha_{\text{ave}} = \frac{1}{16}$. Figure 7.2-(b) has the same relative differences $\alpha_{(\ell)}$ as Figure 7.2-(a), but Figure 7.2-(b) has $\beta = \frac{1}{16}$. In Figure 7.2, (b) is more natural than (a) because the complete black areas on (a) are much more conspicuous than other areas. But if pixel expansion m is smaller, Figure 7.2-(a) may look clearer than (b). These facts mean that it is difficult to determine the optimal value of β because it depends on the size and/or contents of a secret image, and hence β should be treated separately from $\alpha_{\min}$ or α_{ave}. In this paper, we derive the maximum $\alpha_{\min}$ and α_{ave} for a given β.

We note that gray-scale secret images are treated in [14], [67]. But, [67] does not consider the contrast for gray-scale secret images. Although the relative contrasts and the minimum contrast are introduced in [14], the average contrast and the brightness offset are not considered.

Example 7.3 The $(3, 3)$-VSS-GS-3 scheme with $\delta_{(1)} = 1$, $\delta_{(2)} = 2$, and $\delta_{(3)} = 1$ is constructed by the following basis matrices

$$B_{(1)} = \begin{bmatrix} 0001001001111 \\ 0010010010111 \\ 0100100100111 \end{bmatrix}, \tag{7.9}$$

$$B_{(2)} = \begin{bmatrix} 0000011101101 \\ 0000101011011 \\ 0001000110111 \end{bmatrix}, \tag{7.10}$$

$$B_{(3)} = \begin{bmatrix} 0000011011011 \\ 0000101101101 \\ 0000110110110 \end{bmatrix}, \tag{7.11}$$

(a) $\alpha_{(2)} = \alpha_{(3)} = \cdots = \alpha_{(8)} = \frac{1}{16}$, and $\beta = 0$

(b) $\alpha_{(2)} = \alpha_{(3)} = \cdots = \alpha_{(8)} = \frac{1}{16}$, and $\beta = \frac{1}{16}$

Figure 7.2. Comparison between two decrypted images with $\beta = 0$ and $\beta = \frac{1}{16}$.

which have pixel expansion $m = 13$. Since $w(\eta(B_{(1)}[\![\boldsymbol{V}]\!])) = 9$, $w(\eta(B_{(2)}[\![\boldsymbol{V}]\!])) = 10$, and $w(\eta(B_{(3)}[\![\boldsymbol{V}]\!])) = 12$ hold, we note from (7.1) and (7.2) that the basis matrices attain relative differences $\delta_{(1)} = 1$, $\delta_{(2)} = 2$, $\delta_{(3)} = 1$. From Definition 7.2, the contrasts and brightness offset become $\alpha_{(2)} = \frac{1}{13}$, $\alpha_{(3)} = \frac{2}{13}$, $\alpha_{\min} = \frac{1}{13}$, $\alpha_{\text{ave}} = \frac{3}{26}$, and $\beta = \frac{1}{13}$. Since the first and second rows of $B_{(1)}$, $B_{(2)}$, and $B_{(3)}$ satisfy the following equivalence relation

$$\begin{aligned} &B_{(1)}[\![\{V_1, V_2\}]\!] \sim B_{(2)}[\![\{V_1, V_2\}]\!] \sim B_{(3)}[\![\{V_1, V_2\}]\!] \\ &\sim \begin{bmatrix} 0000010101111 \\ 0000101010111 \end{bmatrix} \end{aligned} \tag{7.12}$$

and the similar relation holds for other combinations of two rows, the security condition, i.e., Definition 7.1-(ii) is also satisfied. □

7.2.2 Polynomial Representation of VSS-GS Schemes

In Chapter 6 we showed the algebraic construction of VSS schemes for color images [66]. In this method, basis matrices are corresponded to polynomials, and it is shown that basis matrices are derived algebraically by solving some simultaneous partial differential equations for the polynomials. Kuwakado-Tanaka [72] modified the method to apply to VSS-BW schemes. In this subsection, we extend the method to VSS-GS schemes.

First, for any integer p satisfying $p \leq n$, we define the *constant-column-weight* (CCW) *matrix* $M_{p,n}$ with weight p as the $n \times \binom{n}{p}$ matrix that has all kinds of column vectors with Hamming weight p [72]. For instance, $M_{2,4}$ is given by

$$M_{2,4} \sim \begin{bmatrix} 001110 \\ 011001 \\ 110010 \\ 100101 \end{bmatrix}. \tag{7.13}$$

Note that there are $\binom{n}{p}!$ matrices that are equivalent to $M_{p,n}$. But, by the benefit of the equivalence class, it suffices to consider only the representative, which is any one of the matrices.

Let $M'_{p,n}$ be an $(n-1) \times \binom{n}{p}$ matrix obtained by deleting a row from $M_{p,n}$. Then, it can easily be checked that $M_{p,n}$ and $M'_{p,n}$ satisfy $M'_{p,n} \sim M_{p-1,n-1} \odot M_{p,n-1}$, i.e.,

$$\langle M'_{p,n} \rangle = \langle M_{p-1,n-1} \rangle \odot \langle M_{p,n-1} \rangle \tag{7.14}$$

independently from the deleted row. Now we identify an equivalence class $\langle M_{p,n} \rangle$ with a monomial $\frac{z^p a^{n-p}}{p!(n-p)!}$ where p and $n-p$ represent the numbers of 1 (black) and 0 (white), respectively, in each column of $M_{p,n}$. We also represent formally concatenation operator $\odot$ with plus operator $+$. If we use these representations, $\langle M_{p-1,n-1} \rangle \odot \langle M_{p,n-1} \rangle$ can be identified with homogeneous polynomial $\frac{z^{p-1}a^{n-p}}{(p-1)!(n-p)!} + \frac{z^p a^{n-p-1}}{p!(n-p-1)!}$, which is equal to $(\frac{\partial}{\partial z} + \frac{\partial}{\partial a})\frac{z^p a^{n-p}}{p!(n-p)!}$. This fact means from (7.14) that the partial differential operator $\frac{\partial}{\partial z} + \frac{\partial}{\partial a}$ represents the deletion of an arbitrary row from representative $M_{p,n}$, and hence all matrices in $\langle M_{p,n} \rangle$.

Example 7.4 For $M_{2,4}$ given by (7.13), the polynomial representation of $\langle M_{2,4} \rangle$ is $\frac{z^2a^2}{2!2!}$. If any one row is deleted from $M_{2,4}$, the deleted matrix $M'_{2,4}$ satisfies from (7.13) that

$$M'_{2,4} \sim \begin{bmatrix} 001110 \\ 011001 \\ 110010 \end{bmatrix} \sim \begin{bmatrix} 001110 \\ 010101 \\ 100011 \end{bmatrix} = \begin{bmatrix} 001 \\ 010 \\ 100 \end{bmatrix} \odot \begin{bmatrix} 110 \\ 101 \\ 011 \end{bmatrix}.$$

Hence, by the polynomial representation, $\langle M'_{2,4} \rangle$ can be described as homogeneous polynomial $\frac{z^1a^2}{1!2!} + \frac{z^2a^1}{2!1!}$, which is equal to $(\frac{\partial}{\partial z} + \frac{\partial}{\partial a})\frac{z^2a^2}{2!2!}$. □

In the polynomial representation, there is one-to-one correspondence between all equivalence classes in $\mathcal{E}^{nm}/\sim$, which are generated from finite concatenations of CCW matrices in $\mathcal{E}^{nm}$, and all homogeneous polynomials with degree n. Now, assume that a basis matrix $B_{(\ell)}$ is constructed by the concatenation of CCW matrices as follows.

$$B_{(\ell)} = \bigodot_{p=0}^{n} M_{p,n}^{\left[\mu_{(\ell),p}\right]}, \tag{7.15}$$

where $\mu_{(\ell),p}$ are nonnegative integers and $M^{[u]}$ stands for the u-times concatenation of matrix M, i.e., $\underbrace{M \odot M \odot \cdots \odot M}_{u \text{ times}}$. Then the equivalence class of a basis matrix $B_{(\ell)}$ in (7.15) can be represented by the corresponding homogeneous polynomial $F_{(\ell)}(z, a)$ such as

$$F_{(\ell)}(z, a) = \sum_{p=0}^{n} \mu_{(\ell),p} \frac{z^p a^{n-p}}{p!(n-p)!}, \tag{7.16}$$

which is a *basis polynomial*.

Hence, in the case of (n, n)-threshold access structures, the properties in Definition 7.1 that $(\mathcal{A}_{\mathsf{Q}}, \mathcal{A}_{\mathsf{F}})$-VSS-GS schemes must satisfy can be described by the basis polynomials as follows.

Theorem 7.5 Let $F_{(\ell)}(z, a),\ \ell = 1, 2, \ldots, L$, be basis polynomials which are identified with basis matrices $B_{(\ell)}$ of the (n, n)-VSS-GS-L scheme. Then the construction of the basis matrices satisfying Definition 7.1 is equivalent to solve the following simultaneous partial differential equations.

$$F_{(\ell)}(0, 1) - F_{(\ell-1)}(0, 1) = \frac{\delta_{(\ell)}}{n!}, \tag{7.17}$$

$$\Xi F_{(1)}(z, a) = \Xi F_{(2)}(z, a) = \cdots = \Xi F_{(L)}(z, a), \tag{7.18}$$

where $\Xi = \frac{\partial}{\partial z} + \frac{\partial}{\partial a}$ and $F_{(0)}(0, 1) = 0$. Furthermore, pixel expansion m is given by

$$m = n! F_{(\ell)}(1, 1), \tag{7.19}$$

for any ℓ. □

Proof of Theorem 7.5 In the same way as Theorem 6.10, [66] and [72], it can be checked that (7.17) and (7.18) correspond to Definition 7.1-(i) and (ii), respectively. Equation (7.19) holds because the number of columns in the CCW matrix $M_{p,n}$ is given by $n! \frac{z^p a^{n-p}}{p!(n-p)!}\Big|_{\substack{z=1 \\ a=1}}$. □

7.3 Minimum Pixel Expansion of (n, n)-VSS-GS Schemes

In this section, based on the polynomial representation, we show how to construct the (n, n)-VSS-GS scheme that achieves the minimum pixel expansion for given relative differences. Note that we can easily extend (n, n)-VSS-GS schemes to (k, n)-VSS-GS schemes and to VSS-GS schemes with general access structures by using Theorems 6.18 and 6.23, respectively.

7.3.1 Generality of Polynomial Representation in (n, n)-VSS-GS Schemes

If a basis matrix consists of the concatenation of CCW matrices, it can be represented by the corresponding basis polynomial. But we further show in the next theorem that the basis matrices of any (n, n)-VSS-GS scheme can be represented by the basis polynomials.

Theorem 7.6 For any (n, n)-VSS-GS-L scheme, basis matrices $B_{(1)}, B_{(2)}, \ldots, B_{(L)}$, can be constructed by the concatenations of CCW matrices in the case that all the basis matrices contain no common column vectors except zero column vectors. □

From Theorem 6.7, we can assume that all the basis matrices contain no column vectors except the column zero vector because such common vectors play no role, and hence such common vectors can be removed or changed to the zero vectors to make a pixel bright.

Proof of Theorem 7.6 We first prove that for any column vector $\boldsymbol{v}$ in any $B_{(\ell)}$, $B_{(\ell)}$ must also contain all vectors with the same Hamming weight as $\boldsymbol{v}$.

In the case that $\boldsymbol{v}$ is the zero column vector, Theorem 7.6 holds obviously. Hence, assume that $\boldsymbol{v}$ with $w(\boldsymbol{v}) \geq 1$ is a nonzero column vector of basis matrix $B_{(\ell)}$. Then there is at least one basis matrix $B_{(l)}$, $l \neq \ell$, that does not contain the vector $\boldsymbol{v}$. Although $B_{(l)}$ does not contain $\boldsymbol{v}$, it is possible that $B_{(\ell)}$ and $B_{(l)}$ have the same column vectors. In such cases, $B_{(\ell)}$ and $B_{(l)}$ can be represented as $B_{(\ell)} \sim \hat{B}_{(\ell)} \odot X$, $B_{(l)} \sim \hat{B}_{(l)} \odot X$, where $\hat{B}_{(\ell)}$ and $\hat{B}_{(l)}$ contain no common column vectors. Obviously, $\boldsymbol{v}$ must be contained in $\hat{B}_{(\ell)}$. Since it must satisfy from Definition 7.1 (ii) that any $n-1$ rows in $\hat{B}_{(\ell)}$ are equivalent to the corresponding $n-1$ rows in $\hat{B}_{(l)}$, $\hat{B}_{(l)}$ must contain all n column vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$ that differ one Hamming distance from $\boldsymbol{v}$. On the other hand, for each $\boldsymbol{v}_i$, $i = 1, 2, \ldots, n$, $\hat{B}_{(\ell)}$ also must have all n column vectors that differ one Hamming distance from $\boldsymbol{v}_i$. These facts mean that $\hat{B}_{(\ell)}$ must have all the column vectors that differ even Hamming distances from $\boldsymbol{v}$.

Since the Hamming distance between any two vectors having the same Hamming weight is even, all the vectors with Hamming weight $w(\boldsymbol{v})$ must also be contained in $\hat{B}_{(\ell)}$.

We can also show by the similar argument that if $B_{(\ell)}$ contains the same column vector $\boldsymbol{v}$ s-times, then each vector with Hamming weight $w(\boldsymbol{v})$ is also included in $B_{(\ell)}$ s-times. Hence, in the case of (n, n)-VSS-GS schemes, any basis matrix can be represented by the concatenation of CCW matrices, i.e., the basis polynomials. □

7.3.2 Minimum Pixel Expansion of (n, n)-VSS-GS Schemes

In this subsection, we derive the optimal (n, n)-VSS-GS scheme in the viewpoint of pixel expansion m, in other words resolution, for given relative differences $\delta_{(\ell)},\ \ell = 1, 2, \ldots, L$.

Theorem 7.7 Let m be the pixel expansion of an (n, n)-VSS-GS-L scheme which has relative differences $\delta_{(\ell)},\ \ell = 1, 2, \ldots, L$. Then the minimum pixel expansion m^* is given by

$$m^* = 2^{n-1}\Delta + \delta, \tag{7.20}$$

where $\delta = \delta_{(1)}$ and $\Delta = \sum_{\ell=2}^{L} \delta_{(\ell)}$. The basis matrices that attain m^* are given by

$$B_{(\ell)} = M_{0,n}^{[\delta]} \odot \left[\bigodot_{\substack{p=0 \\ p:\text{even}}}^{n} M_{p,n}^{\left[\Delta_{(\ell)}\right]} \right] \odot \left[\bigodot_{\substack{p=1 \\ p:\text{odd}}}^{n} M_{p,n}^{\left[\Delta-\Delta_{(\ell)}\right]} \right], \tag{7.21}$$

where $\Delta_{(\ell)} = \sum_{l=2}^{\ell} \delta_{(l)}$. □

Proof of Theorem 7.7 From Theorems 7.5 and 7.6, we can use the basis polynomials shown in (7.15) instead of the basis matrices in the construction of (n, n)-VSS-GS schemes. From (7.16) and (7.17), $\mu_{(\ell),0}$ must satisfy that

$$\mu_{(\ell),0} = \sum_{l=1}^{\ell} \delta_{(l)} = \delta + \Delta_{(\ell)}, \tag{7.22}$$

and

$$\delta = \mu_{(1),0} < \mu_{(2),0} < \cdots < \mu_{(L),0} = \delta + \Delta. \tag{7.23}$$

Since it holds that

$$\Xi F_{(\ell)}(z, a) = \sum_{p=0}^{n-1} \left(\mu_{(\ell),p} + \mu_{(\ell),p+1}\right) \frac{z^p a^{n-p-1}}{p!(n-p-1)!} \tag{7.24}$$

and $\Xi F_{(\ell)}(z, a)$ must satisfy (7.18), $\mu_{(\ell),p} + \mu_{(\ell),p+1}$ must be independent of ℓ. Hence, for some nonnegative integers μ_p, $\mu_{(\ell),p}$ must satisfy that for any ℓ

$$\mu_p = \mu_{(\ell),p} + \mu_{(\ell),p+1}. \tag{7.25}$$

Since all μ_p and $\mu_{(\ell),p}$ are nonnegative integers, we have that

$$\mu_p \geq \max_{1 \leq \ell \leq L} \mu_{(\ell),p} \tag{7.26}$$

for any p. Letting $F'(z, a)$ be

$$\begin{aligned} F'(z, a) &= \Xi F_{(1)}(z, a) = \Xi F_{(2)}(z, a) = \cdots = \Xi F_{(L)}(z, a) \\ &= \sum_{p=0}^{n-1} \mu_p \frac{z^p a^{n-p-1}}{p!(n-p-1)!}, \end{aligned} \tag{7.27}$$

pixel expansion m is given from (7.19) as follows.

$$m = (n-1)!\, F'(1,1) = \sum_{p=0}^{n-1} \mu_p \binom{n-1}{p} \tag{7.28}$$

In order to minimize pixel expansion m, we must minimize all μ_p. In the following, we show that such minimization is possible.

Since it holds from (7.23) and (7.26) that $\mu_0 \geq \max_{1\leq \ell \leq L} \mu_{(\ell),0} = \mu_{(L),0} = \delta + \Delta$, μ_0 can be represented as $\mu_0 = \varepsilon_0 + \delta + \Delta$ for some nonnegative parameter $\varepsilon_0 \geq 0$. Substituting μ_0 into (7.25), we have $\mu_{(\ell),1} = \varepsilon_0 + \delta + \Delta - \mu_{(\ell),0}$. Then μ_1 can be represented as $\mu_1 = \varepsilon_0 + \varepsilon_1 + \Delta$ for another nonnegative parameter $\varepsilon_1 \geq 0$ because it is obtained from (7.23) and (7.26) that $\mu_1 \geq \max_{1\leq \ell \leq L} \mu_{(\ell),1} = \varepsilon_0 + \delta + \Delta - \min_{1\leq \ell \leq L} \mu_{(\ell),0} = \varepsilon_0 + \delta + \Delta - \mu_{(1),0} = \varepsilon_0 + \Delta$. Next we have from (7.25) that $\mu_{(\ell),2} = \mu_1 - \mu_{(\ell),1} = \varepsilon_1 - \delta + \mu_{(\ell),0}$. Hence, it is also obtained from (7.22), (7.23) and (7.26) that $\mu_2 \geq \max_{1\leq \ell \leq L} \mu_{(\ell),2} = \varepsilon_1 - \delta + \max_{1\leq \ell \leq L} \mu_{(\ell),0} = \varepsilon_1 - \delta + \mu_{(L),0} = \varepsilon_1 + \Delta$. Repeating the similar procedure, we have that $\mu_0 = \varepsilon_0 + \delta + \Delta$ and for $p = 1, 2, \ldots, n$,

$$\mu_p = \varepsilon_p + \varepsilon_{p-1} + \Delta, \tag{7.29}$$

$$\mu_{(\ell),p} = \varepsilon_{p-1} + \begin{cases} \mu_{(\ell),0} - \delta, & \text{if } p \text{ is even,} \\ \Delta + \delta - \mu_{(\ell),0}, & \text{if } p \text{ is odd,} \end{cases} \tag{7.30}$$

where $\varepsilon_p \geq 0$ are parameters and $\mu_{(\ell),0}$ is given by (7.22). Since μ_p should be as small as possible, the optimal μ_p is obtained by letting $\varepsilon_p = 0$ for all p as follows.

$$\mu_p = \begin{cases} \delta + \Delta, & \text{if } p = 0, \\ \Delta, & \text{if } p \geq 1. \end{cases} \tag{7.31}$$

This optimal case can be attained from (7.22) and (7.30) by

$$\mu_{(\ell),p} = \begin{cases} \Delta_{(\ell)}, & \text{if } p \geq 2 \text{ is even,} \\ \Delta - \Delta_{(\ell)}, & \text{if } p \geq 1 \text{ is odd,} \end{cases} \tag{7.32}$$

and the minimum pixel expansion m^* is obtained from (7.28) and (7.31) by

$$\begin{aligned} m^* &= \mu_0 + \sum_{p=1}^{n-1} \mu_p \binom{n-1}{p} \\ &= \delta + \Delta + \Delta \sum_{p=1}^{n-1} \binom{n-1}{p} \\ &= \delta + \Delta + \Delta(2^{n-1} - 1) \\ &= 2^{n-1}\Delta + \delta. \end{aligned} \tag{7.33}$$

Finally, the optimal basis matrices shown in (7.21) are obtained from (7.15),(7.22) and (7.32). □

We note from the proof of Theorem 7.7 that in case of $m \geq 2^{n-1}\Delta + \delta$, the basis matrices can be constructed by selecting $\varepsilon_p \geq 0$ adequately. Hence we have the following corollary.

Corollary 7.8 The (n, n)-VSS-GS-L scheme with relative differences $\delta_{(\ell)}$ and pixel expansion m can be constructed if and only if it holds that

$$m \geq 2^{n-1}\Delta + \delta. \tag{7.34}$$

□

Theorem 7.7 gives the minimum pixel expansion m^* for given relative differences $\delta_{(\ell)}$. But, when we can select the minimum values of $\delta_{(\ell)}$, i.e., $\delta_{(1)} = 0$, $\delta_{(\ell)} = 1$ for $\ell = 2, 3, \ldots, L$, we have that $\Delta = L - 1$ and $\delta = 0$. This case attains the overall minimum of pixel expansion m^* in all allowable $\delta_{(\ell)}$.

Corollary 7.9 (Naor-Shamir [81], Blundo et al. [14]) The minimum pixel expansion m^* in all the (n, n)-VSS-GS-L schemes is given by $2^{n-1}(L - 1)$. □

This corollary coincides with the results shown in [14] and, in case of $L = 2$, [81].

Remark 7.10 We note that an (n, n)-VSS-GS scheme can be constructed in a different way. We first transform a gray-scale secret image into a BW-binary image with L-depth halftones, e.g., by the dither method [83]. Then we encrypt the binary image by the basis matrices of an (n, n)-VSS-BW scheme. If the differences of the $(\ell - 1)$-th and ℓ-th halftones are $\delta_{(\ell)}$ which are determined by a dither matrix, each pixel must be expanded to at least Δ subpixels in the case of $\delta_{(1)} = 0$. Since 2^{n-1} subpixels are required to realize any (n, n)-VSS-BW scheme, the total pixel expansion becomes $2^{n-1}\Delta$, which coincides with (7.20) in the case of $\delta_{(1)} = 0$. Hence, such construction of (n, n)-VSS-GS-L schemes is also optimal. □

7.4 Maximum Contrasts and Minimum Pixel Expansion

In Section 7.2.1, we pointed out that the optimal brightness offset β may depend on the size or contents of a secret image. However, for a given β, the contrasts should be maximized. Hence, for a given β, we derive the maximum $\alpha_{\min}$ and α_{ave} in Section 7.4.1 and the minimum pixel expansion that attains the maximum average contrast α_{ave} in Section 7.4.2.

7.4.1 Maximum Average Contrast and Minimum Contrast

Blundo et al. [14] showed that a VSS-GS-L scheme with a given access structure Γ exists if and only if it holds that $\sum_{\ell=2}^{L} \alpha_{(\ell)} \leq \alpha_{NS}^*$, where α_{NS}^* is the maximum α_{NS} defined in (7.6) for the VSS-BW schemes with access structure Γ. In the case of (n, n)-VSS-GS schemes, the above inequality becomes

$$\sum_{\ell=2}^{L} \alpha_{(\ell)} \leq 2^{-(n-1)} \tag{7.35}$$

because the maximum contrast α^*_{NS} is given by $\alpha^*_{NS} = 2^{-(n-1)}$ as shown in [81]. This condition given by (7.35) can also be derived directly from Corollary 7.8 by dividing both sides of (7.34) by m and letting $\delta = 0$. Furthermore, we can also obtain the condition in the case of $\delta \neq 0$, i.e., $\beta \neq 0$ from (7.34) as follows.

Corollary 7.11 An (n, n)-VSS-GS-L scheme with relative contrasts $\alpha_{(1)}, \alpha_{(2)}, \ldots, \alpha_{(L-1)}$ and brightness offset β can be constructed if and only if it holds that

$$\sum_{\ell=2}^{L} \alpha_{(\ell)} \leq 2^{-(n-1)}(1-\beta), \tag{7.36}$$

and $\alpha_{(\ell)}$ and β are rational numbers. □

Corollary 7.11 can be derived from Corollary 7.8. But we have from Corollary 7.11 only that

$$m \geq K\left(2^{n-1}\Delta + \delta\right) \tag{7.37}$$

for some integer $K \geq 1$. Hence, Corollary 7.8 cannot be derived directly from Corollary 7.11. In [14], it is described that (7.37) with $(K = 1, \Delta = L-1, \delta = 0)$ is obtained directly from (7.36) with $\beta = 0$ in the (n, n)-threshold case although $K = 2^{n-1}$ is assumed in their proof of [14, Theorem 3.2]. Therefore, their proof for (n, n)-VSS-GS schemes is not rigorous.

Note that the case of $\beta = 0$ does not always give a clear image. Corollary 7.11 gives how the value of β effects the relative contrasts.

Next, from Corollary 7.11 and Theorem 7.7, we derive the maximum $\alpha_{\rm ave}$ and $\alpha_{\rm min}$.

Theorem 7.12 In all the (n, n)-VSS-GS-L schemes, the average and minimum contrasts, $\alpha_{\rm ave}$ and $\alpha_{\rm min}$, are bounded by

$$\alpha_{\rm ave}, \alpha_{\rm min} \overset{\text{(a)}}{\leq} \frac{1-\beta}{2^{n-1}(L-1)} \overset{\text{(b)}}{\leq} \frac{1}{2^{n-1}(L-1)} \tag{7.38}$$

for $L \geq 2$. There always exist the basis matrices that attain the equality of (a), and inequality (b) holds with equality when $\beta = 0$. □

Proof of Theorem 7.12 From Corollary 7.11 and (7.4), it is obvious that inequality (a) holds with respect to $\alpha_{\rm ave}$. On the other hand, for $\alpha_{\rm min}$, inequality (a) follows from that $(L-1)\alpha_{\rm min} \leq \sum_{\ell=2}^{L} \alpha_{(\ell)} \leq 2^{-(n-1)}(1-\beta)$, where the first inequality holds with equality if and only if

$$\delta_{(2)} = \delta_{(3)} = \cdots = \delta_{(L)}. \tag{7.39}$$

Finally, inequality (b) holds because of $0 \leq \beta < 1$. □

We note from the proof of Theorem 7.12 that both $\alpha_{\rm min}$ and $\alpha_{\rm ave}$ can be maximized at the same time in any (n, n)-VSS-GS-L schemes by letting $\delta_{(\ell)}$ satisfy (7.39) and $\delta = 0$. The next example attains the maximum $\alpha_{\rm min}$ and $\alpha_{\rm ave}$ in all the $(3, 3)$-VSS-GS-4 schemes.

Example 7.13 Letting $\delta_{(1)} = 0$ and $\delta_{(2)} = \delta_{(3)} = \delta_{(4)} = 1$, the basis polynomials of the optimal $(3,3)$-VSS-GS scheme with the maximum $\alpha_{\min}$ and α_{ave} is given from (7.16), (7.22) and (7.32) by

$$F_{(1)}(z,a) = 0\frac{z^0a^3}{0!3!} + 3\frac{z^1a^2}{1!2!} + 0\frac{z^2a^1}{2!1!} + 3\frac{z^3a^0}{3!0!}, \tag{7.40}$$

$$F_{(2)}(z,a) = 1\frac{z^0a^3}{0!3!} + 2\frac{z^1a^2}{1!2!} + 1\frac{z^2a^1}{2!1!} + 2\frac{z^3a^0}{3!0!}, \tag{7.41}$$

$$F_{(3)}(z,a) = 2\frac{z^0a^3}{0!3!} + 1\frac{z^1a^2}{1!2!} + 2\frac{z^2a^1}{2!1!} + 1\frac{z^3a^0}{3!0!}, \tag{7.42}$$

$$F_{(4)}(z,a) = 3\frac{z^0a^3}{0!3!} + 0\frac{z^1a^2}{1!2!} + 3\frac{z^2a^1}{2!1!} + 0\frac{z^3a^0}{3!0!}, \tag{7.43}$$

which achieve $\alpha_{\min} = \alpha_{\mathrm{ave}} = \frac{1}{12}$, $\beta = 0$ and $m = 12$. □

7.4.2 Minimum Pixel Expansion with Maximum Average Contrast

In this subsection we consider the minimum pixel expansion that attains the maximum average contrast α_{ave} for a given brightness offset β. From Corollary 7.11, the relative contrast $\alpha_{(\ell)}$ and the brightness offset β must satisfy (7.36), and the equality case in (7.36) maximizes the average contrast α_{ave}. Therefore, we consider such a case.

Theorem 7.14 In an (n,n)-VSS-GS-L scheme, assume that relative contrasts $\alpha_{(2)}, \alpha_{(3)}, \ldots, \alpha_{(L)}$ and brightness offset β satisfy (7.36) with equality, and each $\alpha_{(\ell)}$ and β are given by rational number $\alpha_{(\ell)} = \frac{p_\ell}{q_\ell}$ for $\ell = 2, 3, \ldots, L$ and $\beta = \frac{p_1}{q_1}$, where p_ℓ and q_ℓ are relatively prime. In case of $\beta = 0$, $p_1 = 0$ and $q_1 = 1$. Then, the minimum pixel expansion m^* is given by the least common multiple of $q_1, q_2, \ldots, q_L$. □

Proof of Theorem 7.14 Let λ be the least common multiple of $q_1, q_2, \ldots, q_L$. Then, $\alpha_{(\ell)}$ and β satisfy that

$$\alpha_{(\ell)} = \frac{\delta_{(\ell)}}{m} = \frac{p_\ell}{q_\ell} = \frac{p_\ell \dfrac{\lambda}{q_\ell}}{\lambda}, \tag{7.44}$$

$$\beta = \frac{\delta_{(L)}}{m} = \frac{p_L}{q_L} = \frac{p_L \dfrac{\lambda}{q_L}}{\lambda}. \tag{7.45}$$

Since p_ℓ and q_ℓ are relatively prime, m must be a multiple of q_ℓ for every ℓ, and hence, it cannot become smaller than λ. Since $p_\ell\frac{\lambda}{q_\ell}$ is an integer, we can set $\delta_{(\ell)}$ as $\delta_{(\ell)} = p_\ell\frac{\lambda}{q_\ell}$. In this case, it holds from (7.20) that

$$\begin{aligned} m^* &= 2^{n-1}\sum_{\ell=2}^{L}\delta_{(\ell)} + \delta_{(L)} = 2^{n-1}\lambda\sum_{\ell=2}^{L}\frac{p_\ell}{q_\ell} + p_L\frac{\lambda}{q_L} \\ &= \lambda\left(2^{n-1}\sum_{\ell=2}^{L}\alpha_{(\ell)} + \beta\right) = \lambda, \end{aligned} \tag{7.46}$$

where the last equality follows from the equality case of (7.36). Hence, λ is the minimum pixel expansion. □

We note from the proof of Theorem 7.12 that the minimum pixel expansion m^* given in Theorem 7.14 also attains the maximum $\alpha_{\min}$ if $\alpha_{(\ell)}$ and β satisfy (7.36) with equality and $\alpha_{(2)} = \alpha_{(3)} = \cdots = \alpha_{(L)}$.

Example 7.15 We construct the $(3,3)$-VSS-GS-4 scheme with relative contrasts $\alpha_{(2)} = \frac{1}{16}$, $\alpha_{(3)} = \frac{3}{32}$, $\alpha_{(4)} = \frac{1}{16}$ and brightness offset $\beta = \frac{1}{8}$ which satisfy $\sum_{\ell=2}^{4} \alpha_{(\ell)} = 2^{-(3-1)}(1 - \frac{1}{8})$. Since the least common multiple of denominators of $\alpha_{(\ell)}$ and β is given by $\lambda = 32$, we can attain $m^* = 32$. Actually, we can realize this m^* by letting $\delta_{(\ell)} = \lambda\alpha_{(\ell)}$ and $\delta_{(1)} = \lambda\beta$, i.e., $\delta_{(1)} = 4$, $\delta_{(2)} = 2$, $\delta_{(3)} = 3$, and $\delta_{(4)} = 2$, which derive the following basis polynomials.

$$F_{(1)}(z,a) = 4\frac{z^0a^3}{0!3!} + 7\frac{z^1a^2}{1!2!} + 0\frac{z^2a^1}{2!1!} + 7\frac{z^3a^0}{3!0!}, \tag{7.47}$$

$$F_{(2)}(z,a) = 6\frac{z^0a^3}{0!3!} + 5\frac{z^1a^2}{1!2!} + 2\frac{z^2a^1}{2!1!} + 5\frac{z^3a^0}{3!0!}, \tag{7.48}$$

$$F_{(3)}(z,a) = 9\frac{z^0a^3}{0!3!} + 2\frac{z^1a^2}{1!2!} + 5\frac{z^2a^1}{2!1!} + 2\frac{z^3a^0}{3!0!}, \tag{7.49}$$

$$F_{(4)}(z,a) = 11\frac{z^0a^3}{0!3!} + 0\frac{z^1a^2}{1!2!} + 7\frac{z^2a^1}{2!1!} + 0\frac{z^3a^0}{3!0!}. \tag{7.50}$$

□

Finally we consider the minimum pixel expansion m^* in the case that both $\alpha_{\min}$ and α_{ave} are maximized at the same time for $\beta = 0$. From Theorem 7.12, the maximum of $\alpha_{\min}$ and α_{ave} can be achieved when $\alpha_{(\ell)} = \frac{1}{(L-1)2^{n-1}}$ for all $\ell = 2, 3, \ldots, L$. In this case, the pixel expansion is given by $2^{n-1}(L-1)$ from Theorem 7.14. We note from Corollary 7.9 that this m^* is equal to the minimum pixel expansion in all the (n,n)-VSS-GS-L schemes.

7.5 VSS Schemes for Color Images with Shades

In this section, we give a method to construct the basis matrices of (n,n)-threshold VSS schemes for color images with shades, VSS-CS schemes for short, based on basis polynomials. But, note that VSS-CS schemes with general access structures can easily be derived from (n,n)-VSS-CS schemes by using the cumulative map in the same way as shown in Section 6.4 or [1], [47], [66].

7.5.1 Preliminaries

In this subsection, we extend Definitions 6.21 and 7.1 to the case of VSS-CS schemes with general access structures.

Let $\mathcal{E}$ be the set of colors printed on shares. In order to represent colors with shades, we modify the definition of $\mathcal{D}$ for color images with shades as follows:

We express the colors of pixels with shades in a decrypted secret image DI by capital san-serif fonts $\mathsf{X}_{(\ell)}$, $\ell = 1, 2, \ldots, L_{\mathsf{x}}$. Each $\mathsf{X}_{(\ell)}$, which is composed of x and z, stands for the ℓ-th bright color of x ($\neq \mathsf{z}$). In the case of $\mathsf{x} = \mathsf{0}$, the color with shades becomes gray and we express the gray depth by $\mathsf{A}_{(\ell)}$ for $\ell = 1, 2, \ldots, L_{\mathsf{0}}$. We assume that $\mathsf{X}_{(\ell_1)}$ is brighter than $\mathsf{X}_{(\ell_2)}$, i.e., $\mathsf{X}_{(\ell_1)}$ contains more x than $\mathsf{X}_{(\ell_2)}$ if $\ell_1 > \ell_2$. In the case that all subpixels in a decrypted pixel are $\mathsf{1}$, we represent the pixel color by Z. For the simplicity of notation, we define $\mathsf{X}_{(0)} = \mathsf{Z}$ for any $\mathsf{x} \in \mathcal{E}$. Note that $\mathsf{X}_{(1)} \neq \mathsf{Z}$ for any $\mathsf{x}(\neq \mathsf{1}) \in \mathcal{E}$, and in the case of $\mathsf{x} = \mathsf{0}$, the set $\{\mathsf{A}_{(1)}, \mathsf{A}_{(2)}, \ldots, \mathsf{A}_{(L_0)}\}$ represents the gray scale with L_0 depths discussed in the previous sections [14], [52].

For a set $\{\mathsf{X}_{(0)}(= \mathsf{Z}), \mathsf{X}_{(1)}, \mathsf{X}_{(2)}, \ldots, \mathsf{X}_{(L_{\mathsf{x}})}\}$, let $\delta_{\mathsf{X}_{(\ell)}}$ denote the difference of the numbers of x between $\mathsf{X}_{(\ell-1)}$ and $\mathsf{X}_{(\ell)}$. In case of $\mathsf{x} = \mathsf{1}$, define that $\delta_{\mathsf{Z}} = 0$. Note that $\delta_{\mathsf{X}_{(\ell)}} \geq 1$ for any $\mathsf{x} \neq \mathsf{1}$ and $\ell \geq 1$. Then we assume that the color of each pixel on a secret image SI can be approximated by selecting a color $\mathsf{x} \in \mathcal{E}$ and parameter $\delta_{\mathsf{X}_{(\ell)}}$ adequately, and hence, there exists one-to-one correspondence between the set of colors of SI and that of DI.

Let $\mathcal{D}$ be the set of all the colors with all kinds of brightness included in a decrypted image DI. Then, for $\mathsf{X}_{(\ell)}$ and $\mathsf{Z} \in \mathcal{D}$, we can define a mapping $\gamma : \mathcal{D} \to \mathcal{E}$ that gives a hue $\gamma(\mathsf{X}_{(\ell)}) = \mathsf{x} \in \mathcal{E}$ and $\gamma(\mathsf{Z}) = \mathsf{1}$.

Remark 7.16 The above definition of decrypted pixel colors includes both the definitions for *lattice-based* VSS schemes [43], [66], [67] and *VSS-GS-L* schemes [14], [52]. On the other hand, *meanvalue-color mixing* (MCM) VSS schemes [45], [117] cannot be treated by the above definition because in the MCM-VSS schemes, each pixel on decrypted images is composed of the three primary colors $(\mathsf{r}, \mathsf{g}, \mathsf{b})$ and $\mathsf{1}$. But, since the MCM-VSS schemes requires large pixel expansion, it seems to be hard to realize a VSS scheme for a general access structure with $n \geq 3$. □

Now, we can define VSS schemes for color images with shades for general access structures $\{\mathcal{A}_{\mathsf{Q}}, \mathcal{A}_{\mathsf{F}}\}$ as follows.

Definition 7.17 A VSS scheme for an access structure Γ is called a $(\Gamma, \boldsymbol{V}, \mathcal{E}, \mathcal{D})$-*VSS-CS scheme* if it has color sets $\mathcal{D}$ and $\mathcal{E}$, and for every $\ell \in \{1, 2, \ldots, L_{\mathsf{d}}\}$ each pixel associated with $\mathsf{D}_{(\ell)} \in \mathcal{D}$ is determined by a matrix $T_{\mathsf{D}_{(\ell)}}$ randomly selected from $\langle B_{\mathsf{D}_{(\ell)}} \rangle \in \mathcal{E}^{nm}/\!\sim$, where $B_{\mathsf{D}_{(\ell)}}$ is the basis matrix of $\mathsf{D}_{(\ell)}$ that must satisfy the following conditions:

(i) It holds for any $B_{\mathsf{D}_{(\ell)}}$ and any $\boldsymbol{Q} \in \mathcal{A}_{\mathsf{Q}}^{-}$ that

$$\eta\left(B_{\mathsf{D}_{(\ell)}}[\![\boldsymbol{Q}]\!]\right) \sim \left[\, \gamma\left(\mathsf{D}_{(\ell)}\right) \gamma\left(\mathsf{D}_{(\ell)}\right) \cdots \gamma\left(\mathsf{D}_{(\ell)}\right)\ \mathsf{1}\,\mathsf{1} \cdots \mathsf{1}\right]. \tag{7.51}$$

In the case that $B_{\mathsf{D}_{(\ell)}}[\![\boldsymbol{Q}]\!]$ represents $\mathsf{D}_{(\ell)}$ for some $\ell \geq 1$, $\gamma\left(\mathsf{D}_{(\ell)}\right)$ appears $\sum_{l=1}^{\ell} \delta_{\mathsf{D}_{(l)}}$ times in (7.51) where $\delta_{\mathsf{D}_{(l)}}$, $l = 1, 2, \ldots, \ell$, are positive integers. In the case of $\ell = 0$, the right hand side of (7.51) consists of only $\mathsf{1}$'s.

(ii) For any set $\boldsymbol{F} \subseteq \mathcal{A}_{\mathsf{F}}$, $B_{\mathsf{D}_{(\ell)}}[\![\boldsymbol{F}]\!]$ are equivalent for any $\mathsf{D}_{(\ell)} \in \mathcal{D}$. □

7.5.2 Algebraic Construction of VSS-CS Schemes

In Sections 7.2 and 7.3, we have constructed (n, n)-VSS-GS-L schemes based on CCW matrices. A CCW matrix can be considered as a modified version of CP matrix introduced in Section 6.3.1 for VSS schemes for color images. Hence, the CCW matrices with colors are called *different column permutation* matrices, which are defined formally in the following.

Let $\mathcal{E}$ be the set of colors used in encryption and $\mathcal{D}$ be the set of colors in a decrypted image. First, recall the CP matrix defined in 6.3.1. As an example, a CP matrix is given as follows.

$$C_3\left([\mathsf{cyy}]\right) \sim \begin{bmatrix} \mathsf{cyycyy} \\ \mathsf{ycyycy} \\ \mathsf{yycyyc} \end{bmatrix}. \tag{7.52}$$

Now we assume that a color $\mathsf{x} \in \mathcal{E}$ is obtained by

$$\mathsf{x} = \underbrace{\mathsf{x}^{\langle 1\rangle} \sqcup \cdots \sqcup \mathsf{x}^{\langle 1\rangle}}_{u_1 \text{ times}} \sqcup \underbrace{\mathsf{x}^{\langle 2\rangle} \sqcup \cdots \sqcup \mathsf{x}^{\langle 2\rangle}}_{u_2 \text{ times}} \sqcup \cdots \sqcup \underbrace{\mathsf{x}^{\langle h_\mathsf{x}\rangle} \sqcup \cdots \sqcup \mathsf{x}^{\langle h_\mathsf{x}\rangle}}_{u_{h_\mathsf{x}} \text{ times}}. \tag{7.53}$$

where $\mathsf{x}^{\langle i\rangle} \in \mathcal{E}$ appears u_i times and $\sum_{i=1}^{h_\mathsf{x}} u_i = n$. Note that if $\mathsf{x} \neq 1$, then it must hold from the definition of $\sqcup$ that all $\mathsf{x}^{\langle i\rangle} \neq 1$ for all $i = 1, 2, \ldots, h_\mathsf{x}$. Let $\boldsymbol{v}_\mathsf{x}$ be an n-dimensional row vector given by

$$\begin{aligned} \boldsymbol{v}_\mathsf{x} &= [\underbrace{\mathsf{x}^{\langle 1\rangle} \cdots \mathsf{x}^{\langle 1\rangle}}_{u_1 \text{ times}} \underbrace{\mathsf{x}^{\langle 2\rangle} \cdots \mathsf{x}^{\langle 2\rangle}}_{u_2 \text{ times}} \cdots \underbrace{\mathsf{x}^{\langle h_\mathsf{x}\rangle} \cdots \mathsf{x}^{\langle h_\mathsf{x}\rangle}}_{u_{h_\mathsf{x}} \text{ times}}] \\ &\stackrel{\text{def}}{=} \left[\left(\mathsf{x}^{\langle 1\rangle}\right)^{u_1} \left(\mathsf{x}^{\langle 2\rangle}\right)^{u_2} \cdots \left(\mathsf{x}^{\langle h_\mathsf{x}\rangle}\right)^{u_{h_\mathsf{x}}}\right]. \end{aligned} \tag{7.54}$$

Then the number of different column vectors obtained by the permutations of ${}^t\boldsymbol{v}_\mathsf{x}$ is given by $N(\boldsymbol{v}_\mathsf{x}) \stackrel{\text{def}}{=} \binom{n}{u_1, u_2, \ldots, u_{h_\mathsf{x}}}$. A *different column permutation* (DP) matrix $D_n(\boldsymbol{v}_\mathsf{x})$ is defined as a matrix that consists of such $N(\boldsymbol{v}_\mathsf{x})$ different columns. For example, in the case of $\boldsymbol{v}_\mathsf{g} = [\mathsf{cyy}]$,

$$D_3(\boldsymbol{v}_\mathsf{g}) = D_3\left(\left[\mathsf{c}^1\mathsf{y}^2\right]\right) \sim \begin{bmatrix} \mathsf{cyy} \\ \mathsf{ycy} \\ \mathsf{yyc} \end{bmatrix}. \tag{7.55}$$

We note that any CP matrix can be represented by the concatenations of DP matrices. For instance, $C_3([\mathsf{cyy}])$ and $D_3([\mathsf{c}^1\mathsf{y}^2])$ satisfies from (7.52) and (7.55) that

$$C_3([\mathsf{cyy}]) \sim D_3([\mathsf{c}^1\mathsf{y}^2]) \odot D_3([\mathsf{c}^1\mathsf{y}^2]). \tag{7.56}$$

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

$$D'_3([\mathsf{c}^1\mathsf{y}^2]) \sim \begin{bmatrix} \mathsf{cy} & \mathsf{y} \\ \mathsf{yc} & \mathsf{y} \end{bmatrix} \sim D_2([\mathsf{c}^1\mathsf{y}^1]) \odot D_2([\mathsf{c}^0\mathsf{y}^2]), \tag{7.57}$$

where $[\mathsf{c}^0\mathsf{y}^2] = [\mathsf{y}^2]$. Generally, it holds for $u_i \geq 1$, $i = 1, 2, \ldots, h_{\mathsf{x}}$, that

$$\begin{aligned}\langle D'_n(\boldsymbol{v}_{\mathsf{x}})\rangle &= \left\langle D'_n\left(\left[(\mathsf{x}^{\langle 1\rangle})^{u_1}(\mathsf{x}^{\langle 2\rangle})^{u_2}\cdots(\mathsf{x}^{\langle h_{\mathsf{x}}\rangle})^{u_{h_{\mathsf{x}}}}\right]\right)\right\rangle \\ &= \left\langle D_{n-1}\left(\left[(\mathsf{x}^{\langle 1\rangle})^{u_1-1}\,(\mathsf{x}^{\langle 2\rangle})^{u_2}\cdots(\mathsf{x}^{\langle h_{\mathsf{x}}\rangle})^{u_{h_{\mathsf{x}}}}\right]\right)\right\rangle \\ &\quad \odot \left\langle D_{n-1}\left(\left[(\mathsf{x}^{\langle 1\rangle})^{u_1}\,(\mathsf{x}^{\langle 2\rangle})^{u_2-1}\cdots(\mathsf{x}^{\langle h_{\mathsf{x}}\rangle})^{u_{h_{\mathsf{x}}}}\right]\right)\right\rangle \\ &\quad \odot\cdots\odot \left\langle D_{n-1}\left(\left[(\mathsf{x}^{\langle 1\rangle})^{u_1}\,(\mathsf{x}^{\langle 2\rangle})^{u_2}\cdots(\mathsf{x}^{\langle h_{\mathsf{x}}\rangle})^{u_{h_{\mathsf{x}}}-1}\right]\right)\right\rangle. \end{aligned} \tag{7.58}$$

We now describe the *polynomial representations* of basis matrices which consist of the concatenation of DP matrices. We identify each equivalence class of basis matrices with the corresponding homogeneous polynomial of degree n in the following way.

First, we identify colors $\mathsf{x}^{\langle i\rangle}$ and 1 with variables $x^{\langle i\rangle}$ and z, respectively. We also identify the equivalence class of DP matrices $\langle D_n(\boldsymbol{v}_{\mathsf{x}})\rangle$ and the concatenation operation $\odot$ with a monomial $\prod_{i=1}^{h_{\mathsf{x}}} \frac{(x^{\langle i\rangle})^{u_i}}{u_i!}$ and operation $+$, respectively.

Assume that the equivalence classes of basis matrices $B_{\mathsf{X}_{(\ell)}}$, $0 \leq \ell \leq L_{\mathsf{x}}$, representing colors $\mathsf{X}_{(\ell)} \in \mathcal{D}$ are constructed by the concatenation of equivalence classes of DP matrices $D_n(\boldsymbol{v}_{\mathsf{x}})$ as follows.

$$\langle B_{\mathsf{X}_{(\ell)}}\rangle = \underbrace{\langle D_n(\boldsymbol{v}_{\mathsf{x}})\rangle \odot\cdots\odot \langle D_n(\boldsymbol{v}_{\mathsf{x}})\rangle}_{\sum_{l=1}^{\ell}\delta_{\mathsf{X}_{(l)}}\quad N(\boldsymbol{v}_{\mathsf{x}})\text{ times}} \odot\langle X\rangle, \tag{7.59}$$

where $\sum_{l=1}^{\ell}\delta_{\mathsf{X}_{(l)}}$ is a multiple of $N(\boldsymbol{v}_{\mathsf{x}})$ and X consists of the concatenation of DP matrices that contain at least one 1 in every column.[2] Then, let $F_{\mathsf{X}_{(\ell)}}$ be a *basis polynomials*, which is a homogeneous polynomial of degree n, corresponding to $\langle B_{\mathsf{X}_{(\ell)}}\rangle$.

From the assumption (7.59), the basis polynomial $F_{\mathsf{X}_{(\ell)}}$ must satisfy that

$$\left[F_{\mathsf{X}_{(\ell)}} - \frac{\sum_{l=1}^{\ell}\delta_{\mathsf{X}_{(l)}}}{N(\boldsymbol{v}_{\mathsf{x}})}\prod_{i=1}^{h_{\mathsf{x}}}\frac{(x^{\langle i\rangle})^{u_i}}{u_i!}\right]_{z=0} = 0. \tag{7.60}$$

On the other hand, the polynomial corresponding to the right hand side of (7.58) is given by

$$\sum_{i=1}^{h_{\mathsf{x}}}\left[\frac{(x^{\langle i\rangle})^{u_i-1}}{(u_i-1)!}\prod_{\substack{i'=1\\ i'\neq i}}^{h_{\mathsf{x}}}\frac{(x^{\langle i'\rangle})^{u_{i'}}}{u_{i'}!}\right] = \Xi\prod_{i=1}^{h_{\mathsf{x}}}\frac{(x^{\langle i\rangle})^{u_i}}{u_i!}, \tag{7.61}$$

where $\Xi = \sum_{i=1}^{h_{\mathsf{x}}}\frac{\partial}{\partial x^{\langle i\rangle}}$. Therefore, if any $n-1$ rows of $B_{\mathsf{X}_{(\ell)}}$ are equivalent for any x and ℓ, the basis polynomial $F_{\mathsf{X}_{(\ell)}}$ must satisfy that

$$\Xi F_{\mathsf{X}_{(\ell)}} = F, \tag{7.62}$$

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

Summarizing the above, we have the following theorem.

[2] In the case of $\mathsf{X}_{(0)} = \mathsf{Z}$, $\langle B_{\mathsf{X}_{(0)}}\rangle$ is obtained by letting $\sum_{l=1}^{\ell}\delta_{\mathsf{X}_{(l)}} = 0$.

Theorem 7.18 Suppose that basis matrices $B_{\mathsf{X}_{(\ell)}}$ are obtained by the concatenation of DP matrices as shown in (7.59). Then, the basis polynomials $F_{\mathsf{X}_{(\ell)}}$ corresponding to $B_{\mathsf{X}_{(\ell)}}$ satisfy (7.60) and (7.62). □

In the case that $L_{\mathsf{x}} = 1$ for all x and all the basis matrices consist of CP matrices, the basis polynomials can be obtained by solving simultaneous partial differential equations (7.60) and (7.62) as shown in Section 6.3.2 or [43], [66]. But in general cases, it is difficult to derive the explicit solutions of (7.60) and (7.62). Hence, we consider the case that $h_{\mathsf{x}} = 1$ and $u_1 = n$ for all x. In this case, it holds that $N(\boldsymbol{v}_{\mathsf{x}}) = 1$ for all x, and (7.60) becomes

$$\left[F_{\mathsf{X}_{(\ell)}} - \sum_{l=1}^{\ell} \delta_{\mathsf{X}_{(l)}} \frac{x^n}{n!} \right]_{z=0} = 0. \tag{7.63}$$

Then, the basis polynomials are given by

$$F_{\mathsf{X}_{(\ell)}} = \sum_{l=1}^{\ell} \delta_{\mathsf{X}_{(l)}} f^{\circ}(x) + \sum_{l=\ell+1}^{L_{\mathsf{x}}} \delta_{\mathsf{X}_{(l)}} f^{\bullet}(x) + \sum_{\tilde{\mathsf{x}} \in \zeta(\mathcal{D}) - \{\mathsf{z},\mathsf{x}\}} \sum_{l=1}^{L_{\tilde{\mathsf{x}}}} \delta_{\tilde{\mathsf{X}}_{(l)}} f^{\bullet}(\tilde{x}), \tag{7.64}$$

where $\zeta(\mathcal{D})$ is defined by

$$\zeta(\mathcal{D}) = \left\{ \gamma\left(\mathsf{D}_{(\ell)}\right) : \mathsf{D}_{(\ell)} \in \mathcal{D} \right\}, \tag{7.65}$$

and f° and $f^{\bullet}$ are given by

$$f^{\circ}(x) = \sum_{\substack{t=0 \\ t:\text{even}}}^{n} \frac{z^t}{t!(n-t)!} x^{n-t}, \tag{7.66}$$

$$f^{\bullet}(x) = \sum_{\substack{t=1 \\ t:\text{odd}}}^{n} \frac{z^t}{t!(n-t)!} x^{n-t}. \tag{7.67}$$

Note that $(\frac{\partial}{\partial x} + \frac{\partial}{\partial z}) f^{\circ}(x) = (\frac{\partial}{\partial x} + \frac{\partial}{\partial z}) f^{\bullet}(x)$. (7.66) and (7.67) can easily be obtained from the results shown in [52], [67], [72], and hence we omit the derivation.

Furthermore, it is easy to check that the pixel expansion of $B_{\mathsf{X}_{(\ell)}}$ corresponding to (7.64) is given by

$$m = \sum_{\mathsf{x} \in \zeta(\mathcal{D})} \sum_{l=1}^{L_{\mathsf{x}}} \delta_{\mathsf{X}_{(l)}} \, 2^{n-1}. \tag{7.68}$$

Note that the above construction coincides with the method shown in [67] in the case of (n, n)-threshold access structures.

Example 7.19 Let us consider the $(3, 3, \mathcal{E}, \mathcal{D})$-VSS-CS scheme with $\mathcal{E} = \{\mathsf{g}, \mathsf{y}, 1\}$ and $\mathcal{D} = \{\mathsf{G}_{(1)}, \mathsf{G}_{(2)}, \mathsf{Y}_{(1)}\}$. If we set $\delta_{\mathsf{G}_{(1)}} = \delta_{\mathsf{Y}_{(1)}} = 1$ and $\delta_{\mathsf{G}_{(2)}} = 1$, (7.63) and (7.62) are given by

$$\left[F_{\mathsf{G}_{(1)}} - \frac{g^3}{3!} \right]_{z=0} = 0, \quad \left[F_{\mathsf{G}_{(2)}} - 2\frac{g^3}{3!} \right]_{z=0} = 0, \quad \left[F_{\mathsf{Y}_{(1)}} - \frac{y^3}{3!} \right]_{z=0} = 0, \tag{7.69}$$

$$\Xi F_{\mathsf{G}_{(1)}} = \Xi F_{\mathsf{G}_{(2)}} = \Xi F_{\mathsf{Y}_{(1)}}, \tag{7.70}$$

where $\Xi = \frac{\partial}{\partial z} + \frac{\partial}{\partial g} + \frac{\partial}{\partial y}$. Then, from (7.64), the solutions of (7.69) and (7.70) are given by

$$F_{\mathsf{G}_{(1)}} = f^{\circ}(g) + f^{\bullet}(g) + f^{\bullet}(y), \tag{7.71}$$

$$F_{\mathsf{G}_{(2)}} = 2f^{\circ}(g) + f^{\bullet}(y), \tag{7.72}$$

$$F_{\mathsf{Y}_{(1)}} = f^{\circ}(y) + 2f^{\bullet}(g). \tag{7.73}$$

Since $f^{\circ}(x)$ and $f^{\bullet}(x)$ correspond to

$$D_3([\mathsf{x}^3]) \odot D_3([\mathsf{x}1^2]) = \begin{bmatrix} \mathsf{xx11} \\ \mathsf{x1x1} \\ \mathsf{x11x} \end{bmatrix}, \tag{7.74}$$

$$D_3([1^3]) \odot D_3([\mathsf{x}^2 1]) = \begin{bmatrix} \mathsf{11xx} \\ \mathsf{1x1x} \\ \mathsf{1xx1} \end{bmatrix}, \tag{7.75}$$

respectively, the basis matrices corresponding to $F_{\mathsf{G}_{(1)}}$, $F_{\mathsf{G}_{(2)}}$, $F_{\mathsf{Y}_{(1)}}$ are given as follows:

$$B_{\mathsf{G}_{(1)}} = \begin{bmatrix} \mathsf{gg1111gg11yy} \\ \mathsf{g1g11g1g1y1y} \\ \mathsf{g11g1gg11yy1} \end{bmatrix}, \tag{7.76}$$

$$B_{\mathsf{G}_{(2)}} = \begin{bmatrix} \mathsf{gg11gg1111yy} \\ \mathsf{g1g1g1g11y1y} \\ \mathsf{g11gg11g1yy1} \end{bmatrix}, \tag{7.77}$$

$$B_{\mathsf{Y}_{(1)}} = \begin{bmatrix} \mathsf{yy1111gg11gg} \\ \mathsf{y1y11g1g1g1g} \\ \mathsf{y11y1gg11gg1} \end{bmatrix}. \tag{7.78}$$

Note that from Theorem 6.7, we can eliminate the column ${}^t[111]$ from (7.76)–(7.78). □

7.6 Conclusion

In this chapter, we considered the optimal construction of (n, n)-VSS-GS schemes to minimize the pixel expansion for given relative differences $\delta_{(k)}$, relative contrasts $\alpha_{(k)}$, or to maximize the minimum and average contrasts $\alpha_{\min}$ and α_{ave} for a given brightness offset β.

First we showed that basis polynomials can represent any (n, n)-VSS-GS schemes. Then we derived algebraically the attainable minimum pixel expansion for given relative differences $\delta_{(k)}$ by using the polynomial representation of VSS-GS schemes. Furthermore, we clarified the maximum value of contrasts $\alpha_{\min}$ and α_{ave}, and we derived the minimum pixel expansion for given relative contrasts $\alpha_{(k)}$ and brightness offset β. Finally, we defined the VSS-SH schemes for (n, n) access structures and constructed the basis matrices for such VSS-SH schemes.

Note that (n, n)-VSS-GS schemes can easily be extended to (k, n)-VSS-GS schemes or VSS-GS schemes with general access structures in the same way as shown in Section 6.4 [1], [66]. But it is difficult to derive the optimal (k, n)-VSS-GS scheme in the case of $k < n$. We note that Theorem 7.7 does not hold for the (k, n)-threshold case. For instance, the optimal construction of the $(2, n)$-VSS-BW scheme shown in [12] cannot be represented by any basis polynomials.

Chapter 8

Visual Secret Sharing Schemes for Plural Secret Images

8.1 Introduction

In Chapters 6 and 7, we assumed that a single secret image is encrypted in a VSS scheme, but VSS schemes with two or more secret images are studied in [35], [53], [60], [62], [107]. Kato-Imai [60] proposed a method to reproduce different secret images as the number of shares is increased, and Suga et al.[107] treated VSS schemes for plural secret images and some access structures which can be represented by a graph. Furthermore, Droste [35] showed a method to decrypt different secret images for every subset of n shares, which is improved by Klein-Wessler [62] to attain smaller pixel expansion than Droste's method. However, note that [35], [60], [62], [107] treat only BW-binary secret images, and VSS schemes have not yet been studied for general cases such that secret images are plural color images and their access structures are general.

In this chapter, we propose a method to construct a VSS scheme for q plural images, a VSS-q-PI scheme for short, which can treat color images with shades. In the framework of VSS-q-PI schemes, we assume that each participant holds one share, and usual VSS schemes for one secret image can be treated as VSS-1-PI schemes. Furthermore, VSS schemes with n identification (ID) images [2] can be considered as VSS-$(n+1)$-PI schemes by treating the n ID images as secret images that can be decrypted from a single share.

Note that it is difficult to realize VSS-q-PI schemes, compared with VSS-1-PI schemes, because each pixel of plural secret images must be encoded under the condition that any decrypted images must not leak out any information of the other secret images. In fact, as we will show in Section 8.2.3, the decrypted images of VSS-q-PI schemes treated in [60], [107] leak out some information of the other secret images. But, by defining the correct security conditions of VSS-q-PI schemes, we can establish the construction method of VSS-q-PI schemes that can attain perfectly the security conditions without degenerating the quality of decrypted images compared with the methods in [35], [107].

This chapter is organized as follows. In Section 8.2, the access structures of VSS-q-PI schemes are formally defined, and a color matrix is introduced to describe the colors of plural

secret images. Section 8.3 is devoted to show how to construct VSS-q-PI schemes. Furthermore, in Section 8.4, we discuss an extended construction method by duplicating secret images, which can extend the range of VSS-q-PI schemes that our method can be applied to. Finally, in Section 8.5, we clarify what advantages VSS-q-PI schemes have, compared with q individual VSS-1-PI schemes. The contents of this chapter are published in [53].

Furthermore, some examples of images in VSS schemes with plural secret images are shown in Appendix A.4.

8.2 Definitions

8.2.1 Access Structures

Let $\boldsymbol{V} = \{V_1, V_2, \ldots, V_n\}$ and $2^{\boldsymbol{V}}$ be the set of n shares and the family of all the subsets of $\boldsymbol{V}$, respectively. We suppose that all secret images are encrypted at once into n shares. Each secret image is denoted by $SI^{\langle\langle i \rangle\rangle}$, $i = 1, 2, \ldots, q$, which has the same size. Let $\mathcal{A}_{\mathsf{Q}}^{\langle\langle i \rangle\rangle}$, $i = 1, 2, \ldots, q$, be the family of *qualified sets for the i-th secret image*, and let $\mathcal{A}_{\mathsf{F}}$ be the family of *forbidden sets*. Then, any set in $\mathcal{A}_{\mathsf{Q}}^{\langle\langle i \rangle\rangle}$ can decrypt the i-th secret image $SI^{\langle\langle i \rangle\rangle}$ while any set in $\mathcal{A}_{\mathsf{F}}$ cannot gain any information of any secret image. We call $\Gamma = \left\{ \{\mathcal{A}_{\mathsf{Q}}^{\langle\langle i \rangle\rangle}\}_{i=1}^{q}, \mathcal{A}_{\mathsf{F}} \right\}$ an *access structure for q secret images*.

Note that each $\mathcal{A}_{\mathsf{Q}}^{\langle\langle i \rangle\rangle}$ and $\mathcal{A}_{\mathsf{F}}$ satisfy the following *monotonicity*.

$$\boldsymbol{A} \in \mathcal{A}_{\mathsf{Q}}^{\langle\langle i \rangle\rangle} \Rightarrow \boldsymbol{A}' \in \mathcal{A}_{\mathsf{Q}}^{\langle\langle i \rangle\rangle} \text{ for any } \boldsymbol{A}' \supseteq \boldsymbol{A} \tag{8.1}$$

$$\boldsymbol{A} \in \mathcal{A}_{\mathsf{F}} \Rightarrow \boldsymbol{A}' \in \mathcal{A}_{\mathsf{F}} \quad \text{for any } \boldsymbol{A}' \subseteq \boldsymbol{A} \tag{8.2}$$

Therefore, for each $\mathcal{A}_{\mathsf{Q}}^{\langle\langle i \rangle\rangle}$ and $\mathcal{A}_{\mathsf{F}}$, the *minimal* qualified sets of the i-th secret image $\mathcal{A}_{\mathsf{Q}}^{\langle\langle i \rangle\rangle -}$ and the *maximal* forbidden sets $\mathcal{A}_{\mathsf{F}}^{+}$ can be defined as follows.

$$\mathcal{A}_{\mathsf{Q}}^{\langle\langle i \rangle\rangle -} = \{\boldsymbol{A} \in \mathcal{A}_{\mathsf{Q}}^{\langle\langle i \rangle\rangle} : \boldsymbol{A}' \notin \mathcal{A}_{\mathsf{Q}}^{\langle\langle i \rangle\rangle} \text{ for any } \boldsymbol{A}' \subsetneq \boldsymbol{A}\} \tag{8.3}$$

$$\mathcal{A}_{\mathsf{F}}^{+} = \{\boldsymbol{A} \in \mathcal{A}_{\mathsf{F}} : \boldsymbol{A}' \notin \mathcal{A}_{\mathsf{F}} \text{ for any } \boldsymbol{A}' \supsetneq \boldsymbol{A}\} \tag{8.4}$$

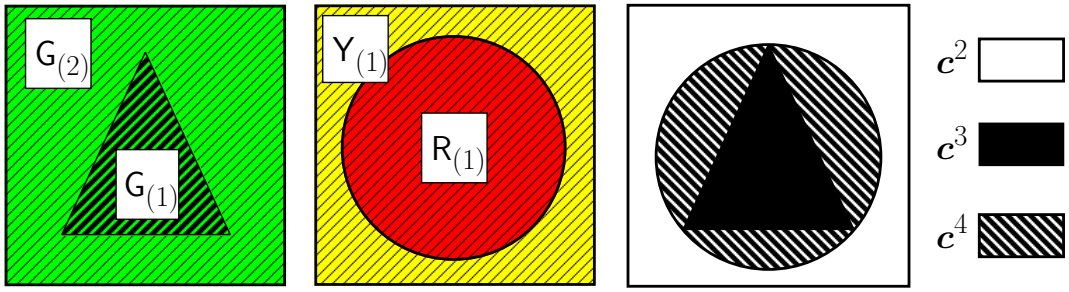
$\mathcal{A}_{\mathsf{Q}}^{\langle\langle i \rangle\rangle -}$ and $\mathcal{A}_{\mathsf{F}}$ are naturally required to satisfy

$$\left\{ \bigcup_{i=1}^{q} \mathcal{A}_{\mathsf{Q}}^{\langle\langle i \rangle\rangle} \right\} \cup \mathcal{A}_{\mathsf{F}} = 2^{\boldsymbol{V}} \quad , \tag{8.5}$$

$$\mathcal{A}_{\mathsf{Q}}^{\langle\langle i \rangle\rangle} \cap \mathcal{A}_{\mathsf{F}} = \emptyset, \tag{8.6}$$

$$\mathcal{A}_{\mathsf{Q}}^{\langle\langle i \rangle\rangle -} \cap \mathcal{A}_{\mathsf{Q}}^{\langle\langle i' \rangle\rangle -} = \emptyset \ \text{ for } i \neq i'. \tag{8.7}$$

The requirement (8.7) comes from the assumption that all the secret images are different. It is worth noting that a VSS-1-PI scheme with an access structure $\{\mathcal{A}_{\mathsf{Q}}^{\langle\langle 1 \rangle\rangle}, \mathcal{A}_{\mathsf{F}}\}$ coincides with a usual VSS scheme with the same access structure for one secret image, which is treated in Chapters 6–7, [1], [10], [14], [66].



(a) $SI^{\langle\langle 1\rangle\rangle}$ (b) $SI^{\langle\langle 2\rangle\rangle}$ (c) Location of shapes in (a) and (b)

Figure 8.1. An example of plural secret images

We also define $\boldsymbol{V}^{\langle\langle i\rangle\rangle}$, the set of *significant* shares for the i-th secret image, as follows.

$$\boldsymbol{V}^{\langle\langle i\rangle\rangle} = \bigcup_{\in \mathcal{A}_{\mathsf{Q}}^{\langle\langle i\rangle\rangle -}} \boldsymbol{A}. \tag{8.8}$$

Example 8.1 Let $\boldsymbol{V} = \{V_1, V_2, V_3, V_4\}$ be the set of shares. Suppose that any two out of three shares $\{V_1, V_2, V_3\}$ can decrypt the secret image $SI^{\langle\langle 1\rangle\rangle}$ shown in Figure 8.1 (a), and set $\{V_3, V_4\}$ can decrypt the secret image $SI^{\langle\langle 2\rangle\rangle}$ shown in Figure 8.1 (b). But, sets $\{V_1, V_4\}$, $\{V_2, V_4\}$ or any one share must not leak out any information of both secret images. This access structure can be represented as follows.

$$\begin{aligned}
\mathcal{A}_{\mathsf{Q}}^{\langle\langle 1\rangle\rangle} &= \{\{V_1, V_2\}, \{V_1, V_3\}, \{V_2, V_3\}, \{V_1, V_2, V_3\}, \\
&\quad \{V_1, V_2, V_4\}, \{V_1, V_3, V_4\}, \{V_2, V_3, V_4\}, \{V_1, V_2, V_3, V_4\}\} && (8.9)\\
\mathcal{A}_{\mathsf{Q}}^{\langle\langle 2\rangle\rangle} &= \{\{V_3, V_4\}, \{V_1, V_3, V_4\}, \{V_2, V_3, V_4\}, \{V_1, V_2, V_3, V_4\}\} && (8.10)\\
\mathcal{A}_{\mathsf{F}} &= \{\{V_1\}, \{V_2\}, \{V_3\}, \{V_4\}, \{V_1, V_4\}, \{V_2, V_4\}\} && (8.11)
\end{aligned}$$

In this case, it holds that $\mathcal{A}_{\mathsf{Q}}^{\langle\langle 1\rangle\rangle -} = \{\{V_1, V_2\}, \{V_1, V_3\}, \{V_2, V_3\}\}$, $\mathcal{A}_{\mathsf{Q}}^{\langle\langle 2\rangle\rangle -} = \{\{V_3, V_4\}\}$, $\mathcal{A}_{\mathsf{F}}^{+} = \{\{V_3\}, \{V_1, V_4\}, \{V_2, V_4\}\}$, $\boldsymbol{V}^{\langle\langle 1\rangle\rangle} = \{V_1, V_2, V_3\}$, $\boldsymbol{V}^{\langle\langle 2\rangle\rangle} = \{V_3, V_4\}$. Note that because of $\{V_1, V_2, V_3\} \notin \mathcal{A}_{\mathsf{Q}}^{\langle\langle 2\rangle\rangle}$, set $\{V_1, V_2, V_3\}$ must not leak out any information of $SI^{\langle\langle 2\rangle\rangle}$ although it can decrypt $SI^{\langle\langle 1\rangle\rangle}$. □

8.2.2 Color Matrix

Let $\mathcal{E}$ be the set of colors used in encryption, and denote by $\mathcal{D}^{\langle\langle i\rangle\rangle}$ the set of colors with shades on decrypted image $DI^{\langle\langle i\rangle\rangle}$, $i = 1, 2, \ldots, q$. We assume that each $\{\mathcal{E}, \mathcal{D}^{\langle\langle i\rangle\rangle}\}$ coincides with $\{\mathcal{E}, \mathcal{D}\}$ defined in Section 7.5. $\mathsf{D}_{(\ell)}^{\langle\langle i\rangle\rangle} \in \mathcal{D}^{\langle\langle i\rangle\rangle}$, $\ell = 1, 2, \ldots, L_{\mathsf{d}^{\langle\langle i\rangle\rangle}}$, stands for a color with hue $\mathsf{d}^{\langle\langle i\rangle\rangle}$ and the ℓ-th depth of shades. Hence, we can define a map $\gamma : \mathcal{D}^{\langle\langle i\rangle\rangle} \to \mathcal{E}$, which gives the hue $\gamma(\mathsf{D}_{(\ell)}) = \mathsf{d}$ for $\mathsf{D}_{(\ell)} \in \mathcal{D}^{\langle\langle i\rangle\rangle}$ and $\gamma(\mathsf{Z}) = 1$ similarly to Section 7.5. Furthermore, let $\delta_{\mathsf{D}_{(\ell)}}^{\langle\langle i\rangle\rangle}$ be the

relative difference of shades, which is defined as the difference of numbers of d between $\mathsf{D}_{(\ell-1)}$ and $\mathsf{D}_{(\ell)}$ in $\mathcal{D}^{\langle\langle i\rangle\rangle}$.

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

$$\begin{aligned}\boldsymbol{D} &= \left[\, \boldsymbol{c}^1\ \boldsymbol{c}^2\ \cdots \boldsymbol{c}^K \,\right] \\ &= \begin{bmatrix} \mathsf{D}^{\langle\langle 1\rangle\rangle,1} & \mathsf{D}^{\langle\langle 1\rangle\rangle,2} & \cdots & \mathsf{D}^{\langle\langle 1\rangle\rangle,K} \\ \mathsf{D}^{\langle\langle 2\rangle\rangle,1} & \mathsf{D}^{\langle\langle 2\rangle\rangle,2} & \cdots & \mathsf{D}^{\langle\langle 2\rangle\rangle,K} \\ \vdots & \vdots & \ddots & \vdots \\ \mathsf{D}^{\langle\langle q\rangle\rangle,1} & \mathsf{D}^{\langle\langle q\rangle\rangle,2} & \cdots & \mathsf{D}^{\langle\langle q\rangle\rangle,K} \end{bmatrix} = \begin{bmatrix} \boldsymbol{r}^{\langle\langle 1\rangle\rangle} \\ \boldsymbol{r}^{\langle\langle 2\rangle\rangle} \\ \vdots \\ \boldsymbol{r}^{\langle\langle q\rangle\rangle} \end{bmatrix}, \end{aligned} \tag{8.12}$$

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

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

Example 8.2 In the case of Example 8.1 with two secret images $SI^{\langle\langle 1\rangle\rangle}$ and $SI^{\langle\langle 2\rangle\rangle}$ shown in Figure 8.1 (a) and (b), $\mathcal{D}^{\langle\langle 1\rangle\rangle}$ and $\mathcal{D}^{\langle\langle 2\rangle\rangle}$ are given by $\mathcal{D}^{\langle\langle 1\rangle\rangle} = \{\mathsf{G}_{(1)}, \mathsf{G}_{(2)}\}$ and $\mathcal{D}^{\langle\langle 2\rangle\rangle} = \{\mathsf{Y}_{(1)}, \mathsf{R}_{(1)}\}$, respectively, and hence the color matrix becomes

$$\boldsymbol{D} = \left[\, \boldsymbol{c}^1\ \boldsymbol{c}^2\ \boldsymbol{c}^3\ \boldsymbol{c}^4 \,\right] = \begin{bmatrix} \mathsf{G}_{(1)}\mathsf{G}_{(2)}\mathsf{G}_{(1)}\mathsf{G}_{(2)} \\ \mathsf{Y}_{(1)}\mathsf{Y}_{(1)}\mathsf{R}_{(1)}\mathsf{R}_{(1)} \end{bmatrix} = \begin{bmatrix} \boldsymbol{r}^{\langle\langle 1\rangle\rangle} \\ \boldsymbol{r}^{\langle\langle 2\rangle\rangle} \end{bmatrix}. \tag{8.13}$$

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

Remark 8.3 Consider the case that the shapes in Figure 8.1 (a) and (b) are located as shown in Figure 8.1 (c). There are three regions in Figure 8.1 (c), which correspond to the column vectors $\boldsymbol{c}^2, \boldsymbol{c}^3$ and $\boldsymbol{c}^4$ in $\boldsymbol{D}$. But the color matrix $\boldsymbol{D}$ should be composed of four column vectors $\boldsymbol{c}^1, \boldsymbol{c}^2, \boldsymbol{c}^3$, and $\boldsymbol{c}^4$ because of $K = 4$. Note that if the public $\boldsymbol{D}$ consists of $\boldsymbol{c}^2, \boldsymbol{c}^3$ and $\boldsymbol{c}^4$, we can know from $DI^{\langle\langle 2\rangle\rangle}$ that the color of the region $\boldsymbol{c}^2$ in Figure 8.1 (c) is $\mathsf{G}_{(2)}$ on $DI^{\langle\langle 1\rangle\rangle}$ because $\mathsf{Y}_{(1)}$ on $DI^{\langle\langle 2\rangle\rangle}$ corresponds only to $\mathsf{G}_{(2)}$ on $DI^{\langle\langle 1\rangle\rangle}$. Therefore, all vectors in $\mathcal{D}$ must be included in $\boldsymbol{D}$ even if some vectors are not appeared in the secret images. □

8.2.3 Definition of VSS-q-PI Schemes

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

If a given set $\boldsymbol{A} \subseteq \boldsymbol{V}$ is included in two or more $\mathcal{A}_{\mathsf{Q}}^{\langle\langle i\rangle\rangle}$, then two or more secret images can be decrypted from $\boldsymbol{A}$. Let $\boldsymbol{I}(\boldsymbol{A})$ be the set of indices of the secret images that can be decrypted from $\boldsymbol{A}$, i.e.,

$$\boldsymbol{I}(\boldsymbol{A}) = \left\{ i : \boldsymbol{A} \in \mathcal{A}_{\mathsf{Q}}^{\langle\langle i\rangle\rangle}, 1 \le i \le q \right\}. \tag{8.14}$$

For instance, $\boldsymbol{I}(\boldsymbol{V}) = \{1, 2, \ldots, q\}$, and $\boldsymbol{I}(\boldsymbol{A}) = \emptyset$ for any $\boldsymbol{A} \in \mathcal{A}_{\mathsf{F}}$.

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

Definition 8.4 For a color matrix $\boldsymbol{D} = [\boldsymbol{c}^1 \boldsymbol{c}^2 \cdots \boldsymbol{c}^J]$, an $n \times m$ matrix B^j is called a basis matrix of a vector $\boldsymbol{c}^j = [\mathsf{D}^{\langle\langle 1\rangle\rangle,j}\ \mathsf{D}^{\langle\langle 2\rangle\rangle,j} \cdots \mathsf{D}^{\langle\langle q\rangle\rangle,j}]$ if B^j satisfies the following conditions:

(i) For every i, j and any $\boldsymbol{A} \in \mathcal{A}_{\mathsf{Q}}^{\langle\langle i\rangle\rangle}$, it holds that

$$\eta\left(B^j[\![\boldsymbol{A}]\!]\right) \sim \left[\, \gamma\left(\mathsf{D}^{\langle\langle i\rangle\rangle,j}\right) \gamma\left(\mathsf{D}^{\langle\langle i\rangle\rangle,j}\right) \cdots \gamma\left(\mathsf{D}^{\langle\langle i\rangle\rangle,j}\right)\ 1\,1 \cdots 1 \right]. \tag{8.15}$$

In the case that $B^j[\![\boldsymbol{A}]\!]$ represents a color $\mathsf{X}_{(\ell)}$ with some $\ell \ge 1$, we have that $\mathsf{D}^{\langle\langle i\rangle\rangle,j} = \mathsf{X}_{(\ell)}$, $\gamma(\mathsf{D}^{\langle\langle i\rangle\rangle,j}) = \mathsf{x}$, and $\gamma\left(\mathsf{D}^{\langle\langle i\rangle\rangle,j}\right)$ appears $\sum_{l=1}^{\ell} \delta_{\mathsf{X}_{(l)}}^{\langle\langle i\rangle\rangle}$ times in (8.15). Note that the positive integer $\delta_{\mathsf{X}_{(\ell)}}^{\langle\langle i\rangle\rangle}$ may depend on $DI^{\langle\langle i\rangle\rangle}$ and $\mathsf{X}_{(\ell)}$, but not on j. In the case of $\ell = 0$, the right hand side of (8.15) consists of only $\mathsf{1}$'s.

(ii) For any set $\boldsymbol{A} \subseteq \boldsymbol{V}$, it holds that $B^j[\![\boldsymbol{A}]\!] \sim B^{j'}[\![\boldsymbol{A}]\!]$ for any j and j' satisfying $\boldsymbol{c}^j[\![\boldsymbol{I}(\boldsymbol{A})]\!] = \boldsymbol{c}^{j'}[\![\boldsymbol{I}(\boldsymbol{A})]\!]$. [1]

A VSS-q-PI scheme for an access structure Γ is called a $(\Gamma, \boldsymbol{V}, \mathcal{E}, \boldsymbol{D})$-*VSS-q-PI scheme* if it has color matrix $\boldsymbol{D}$ for color set $\mathcal{E}$, and for every $j \in \{1, 2, \ldots, K\}$ each pixel associated with $\boldsymbol{c}^j$ is determined by a matrix T^j randomly selected from $\langle B^j \rangle \in \mathcal{E}^{nm}/\!\sim$, where B^j is the basis matrix of $\boldsymbol{c}^j$. □

Example 8.5 In the VSS-2-PI scheme treated in Examples 8.1 and 8.2, basis matrices B^1, B^2, B^3 and B^4 are given by

$$B^1 = \begin{bmatrix} \mathsf{1gg111} \\ \mathsf{g1g111} \\ \mathsf{gg1yr1} \\ \mathsf{111y1r} \end{bmatrix},\ B^2 = \begin{bmatrix} \mathsf{1gg111} \\ \mathsf{1gg111} \\ \mathsf{1ggyr1} \\ \mathsf{111y1r} \end{bmatrix}, B^3 = \begin{bmatrix} \mathsf{1gg111} \\ \mathsf{g1g111} \\ \mathsf{gg1ry1} \\ \mathsf{111r1y} \end{bmatrix},\ B^4 = \begin{bmatrix} \mathsf{1gg111} \\ \mathsf{1gg111} \\ \mathsf{1ggry1} \\ \mathsf{111r1y} \end{bmatrix}. \tag{8.16}$$

It is easy to check that (8.16) satisfies the conditions (i) and (ii) in Definition 8.4. For example, it holds for $\{V_1, V_2\} \in \mathcal{A}_{\mathsf{Q}}^{\langle\langle 1\rangle\rangle -}$ that $\eta\left(B^3[\![\{V_1, V_2\}]\!]\right) \sim [\mathsf{g11111}]$, $\eta\left(B^4[\![\{V_1, V_2\}]\!]\right) \sim [\mathsf{gg1111}]$, $\delta_{\mathsf{G}_{(1)}}^{\langle\langle 1\rangle\rangle} = 1$, and $\delta_{\mathsf{G}_{(2)}}^{\langle\langle 1\rangle\rangle} = 1$. These relations mean that B^3 and B^4 represent $\mathsf{G}_{(1)}$ and $\mathsf{G}_{(2)}$ on $DI^{\langle\langle 1\rangle\rangle}$, respectively. Furthermore, it holds for $\{V_3, V_4\} \in \mathcal{A}_{\mathsf{Q}}^{\langle\langle 2\rangle\rangle -}$ that $\eta\left(B^2[\![\{V_3, V_4\}]\!]\right) \sim [\mathsf{y11111}]$, $\eta\left(B^4[\![\{V_3, V_4\}]\!]\right) \sim [\mathsf{r11111}]$, $\delta_{\mathsf{Y}_{(1)}}^{\langle\langle 2\rangle\rangle} = \delta_{\mathsf{R}_{(1)}}^{\langle\langle 2\rangle\rangle} = 1$, which mean that B^2 and B^4 represent $\mathsf{Y}_{(1)}$ and $\mathsf{R}_{(1)}$ on $DI^{\langle\langle 2\rangle\rangle}$, respectively.

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

It holds that for $\boldsymbol{A}_{123} = \{V_1, V_2, V_3\}$, $B^1[\![\boldsymbol{A}_{123}]\!] \sim B^3[\![\boldsymbol{A}_{123}]\!]$ and $B^2[\![\boldsymbol{A}_{123}]\!] \sim B^4[\![\boldsymbol{A}_{123}]\!]$, i.e., $\boldsymbol{A}_{123}$ does not leak out the colors of pixels on $DI^{\langle\langle 2\rangle\rangle}$. Hence, the basis matrices given by (8.16) attain that both $\boldsymbol{A}_{123} \in \mathcal{A}_{\mathsf{Q}}^{\langle\langle 1\rangle\rangle}$ and $\boldsymbol{A}_{123} \notin \mathcal{A}_{\mathsf{Q}}^{\langle\langle 2\rangle\rangle}$. Furthermore, it can easily be checked that $B^1[\![\boldsymbol{A}]\!] \sim B^2[\![\boldsymbol{A}]\!] \sim B^3[\![\boldsymbol{A}]\!] \sim B^4[\![\boldsymbol{A}]\!]$ for any $\boldsymbol{A} \in \mathcal{A}_{\mathsf{F}}$. □

Remark 8.6 The condition (i) in Definition 8.4 means that any $\boldsymbol{A}^- \in \mathcal{A}_{\mathsf{Q}}^{\langle\langle i\rangle\rangle -}$ can decrypt the secret image $SI^{\langle\langle i\rangle\rangle}$. But, $SI^{\langle\langle i\rangle\rangle}$ cannot always be decrypted by stacking all the shares included in $\boldsymbol{A} \in \mathcal{A}_{\mathsf{Q}}^{\langle\langle i\rangle\rangle}$. For instance, in Example 8.5, $\eta(B^j[\![\boldsymbol{V}]\!]) \sim [111111]$ for all j, which does not satisfy the condition (i) in Definition 8.4, although $\boldsymbol{V} \in \mathcal{A}_{\mathsf{Q}}^{\langle\langle 1\rangle\rangle}$ and $\boldsymbol{V} \in \mathcal{A}_{\mathsf{Q}}^{\langle\langle 2\rangle\rangle}$. We must select a set $\boldsymbol{A}^- \in \mathcal{A}_{\mathsf{Q}}^{\langle\langle i\rangle\rangle -}$ included in $\boldsymbol{A}$ to decrypt $SI^{\langle\langle i\rangle\rangle}$. □

Note that $\boldsymbol{A} \in \mathcal{A}_{\mathsf{F}}$ satisfies the following condition from $\boldsymbol{I}(\boldsymbol{A}) = \emptyset$ and (8.6).

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

In the case of VSS-1-PI schemes, any $\boldsymbol{A}(\subseteq \boldsymbol{V})$ satisfies either $\boldsymbol{A} \in \mathcal{A}_{\mathsf{Q}}^{\langle\langle 1\rangle\rangle}$ or $\boldsymbol{A} \in \mathcal{A}_{\mathsf{F}}$ since the access structures have only two categories $\mathcal{A}_{\mathsf{Q}}^{\langle\langle 1\rangle\rangle}$ and $\mathcal{A}_{\mathsf{F}}$. Hence, in this case, it suffices to consider only the conditions (i) and (ii)′, which coincide with Definition 7.17 (i) and (ii). Based on this consideration, VSS-q-PI schemes are defined by (i) and (ii)′ in [60], [107]. However, the conditions (i) and (ii)′ are not sufficient for $q \geq 2$ because as shown in the following example, the condition (ii)′ does not guarantee that any $\boldsymbol{A} \notin \mathcal{A}_{\mathsf{Q}}^{\langle\langle i\rangle\rangle}$ does not leak out any information of secret image $SI^{\langle\langle i\rangle\rangle}$ even when $\boldsymbol{A} \in \mathcal{A}_{\mathsf{Q}}^{\langle\langle i'\rangle\rangle}$ for some other secret image $SI^{\langle\langle i'\rangle\rangle}$.

Example 8.7 Consider the access structure given by (8.9)–(8.11) in Example 8.1 again. Then, matrices $\tilde{B}^1, \tilde{B}^2, \tilde{B}^3$, and $\tilde{B}^4$ defined by (8.17) satisfy conditions (i) and (ii)′.

$$\tilde{B}^1 = \begin{bmatrix} \mathsf{gg11111} \\ \mathsf{g1g1111} \\ \mathsf{1gg1yr1} \\ \mathsf{1111y1r} \end{bmatrix},\ \tilde{B}^2 = \begin{bmatrix} \mathsf{11gg111} \\ \mathsf{11gg111} \\ \mathsf{11ggyr1} \\ \mathsf{1111y1r} \end{bmatrix},\ \tilde{B}^3 = \begin{bmatrix} \mathsf{11gg111} \\ \mathsf{1g1g111} \\ \mathsf{g11gry1} \\ \mathsf{1111r1y} \end{bmatrix},\ \tilde{B}^4 = \begin{bmatrix} \mathsf{11gg111} \\ \mathsf{11gg111} \\ \mathsf{11ggry1} \\ \mathsf{1111r1y} \end{bmatrix}. \quad (8.17)$$

Note that $\boldsymbol{A}_{12} = \{V_1, V_2\}$, $\boldsymbol{A}_{13} = \{V_1, V_3\}$, $\boldsymbol{A}_{23} = \{V_2, V_3\}$, $\boldsymbol{A}_{123} = \{V_1, V_2, V_3\}$ are not included in $\mathcal{A}_{\mathsf{Q}}^{\langle\langle 2\rangle\rangle}$. The above matrices satisfy that

$$\begin{aligned} &\tilde{B}^1[\![\boldsymbol{A}_{12}]\!] \sim \tilde{B}^3[\![\boldsymbol{A}_{12}]\!],\ \tilde{B}^2[\![\boldsymbol{A}_{12}]\!] \sim \tilde{B}^4[\![\boldsymbol{A}_{12}]\!], \\ &\tilde{B}^1[\![\boldsymbol{A}_{13}]\!] \sim \tilde{B}^3[\![\boldsymbol{A}_{13}]\!],\ \tilde{B}^2[\![\boldsymbol{A}_{13}]\!] \sim \tilde{B}^4[\![\boldsymbol{A}_{13}]\!], \\ &\tilde{B}^1[\![\boldsymbol{A}_{23}]\!] \sim \tilde{B}^3[\![\boldsymbol{A}_{23}]\!],\ \tilde{B}^2[\![\boldsymbol{A}_{23}]\!] \sim \tilde{B}^4[\![\boldsymbol{A}_{23}]\!]. \end{aligned} \quad (8.18)$$

Hence, any one of $\boldsymbol{A}_{12}$, $\boldsymbol{A}_{13}$, $\boldsymbol{A}_{23}$ does not leak out any information about $DI^{\langle\langle 2\rangle\rangle}$. But, it holds that $\tilde{B}^1[\![\boldsymbol{A}_{123}]\!] \not\sim \tilde{B}^3[\![\boldsymbol{A}_{123}]\!]$, $\eta(\tilde{B}^1[\![\boldsymbol{A}_{123}]\!]) \sim [111111]$ and $\eta(\tilde{B}^3[\![\boldsymbol{A}_{123}]\!]) \sim [\mathsf{g}11111]$. This means that from pixels with $\mathsf{G}_{(1)}$ on $DI^{\langle\langle 1\rangle\rangle}$, we can distinguish yellow pixels from red pixels on $DI^{\langle\langle 2\rangle\rangle}$, which correspond to $\tilde{B}^1$ and $\tilde{B}^3$, respectively, by investigating the shares of $\boldsymbol{A}_{123}$. Hence, the matrices given by (8.17) are inadequate as the basis matrices of this access structure. On the contrary, the basis matrices B^1, B^2, B^3 and B^4 given by (8.16) satisfy $B^1[\![\boldsymbol{A}_{123}]\!] \sim B^3[\![\boldsymbol{A}_{123}]\!]$ and $B^2[\![\boldsymbol{A}_{123}]\!] \sim B^4[\![\boldsymbol{A}_{123}]\!]$. □

8.3 Construction Method of VSS-q-PI Scheme

8.3.1 Construction Method

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

First, for a given access structure Γ, define $\tilde{\mathcal{A}}_{\mathsf{Q}}^{\langle\langle i\rangle\rangle}$ and $\tilde{\mathcal{A}}_{\mathsf{F}}^{\langle\langle i\rangle\rangle}$ as follows.

$$\tilde{\mathcal{A}}_{\mathsf{Q}}^{\langle\langle i\rangle\rangle} = \{\boldsymbol{A} \in \mathcal{A}_{\mathsf{Q}}^{\langle\langle i\rangle\rangle} : \boldsymbol{A} \subseteq \boldsymbol{V}^{\langle\langle i\rangle\rangle}\}, \tag{8.19}$$

$$\tilde{\mathcal{A}}_{\mathsf{F}}^{\langle\langle i\rangle\rangle} = \{\boldsymbol{A} \subset \boldsymbol{V}^{\langle\langle i\rangle\rangle} : \boldsymbol{A} \notin \mathcal{A}_{\mathsf{Q}}^{\langle\langle i\rangle\rangle}\}. \tag{8.20}$$

It is easy to check that $\tilde{\mathcal{A}}_{\mathsf{Q}}^{\langle\langle i\rangle\rangle} \cap \tilde{\mathcal{A}}_{\mathsf{F}}^{\langle\langle i\rangle\rangle} = \emptyset$, $\tilde{\mathcal{A}}_{\mathsf{Q}}^{\langle\langle i\rangle\rangle} \cup \tilde{\mathcal{A}}_{\mathsf{F}}^{\langle\langle i\rangle\rangle} = 2^{\langle\langle i\rangle\rangle}$, $\tilde{\mathcal{A}}_{\mathsf{Q}}^{\langle\langle i\rangle\rangle}$ and $\tilde{\mathcal{A}}_{\mathsf{F}}^{\langle\langle i\rangle\rangle}$ have the monotonicity in the same way as $\mathcal{A}_{\mathsf{Q}}^{\langle\langle i\rangle\rangle}$ and $\mathcal{A}_{\mathsf{F}}$, respectively. Therefore, $\Gamma^{\langle\langle i\rangle\rangle} = \{\tilde{\mathcal{A}}_{\mathsf{Q}}^{\langle i\rangle}, \tilde{\mathcal{A}}_{\mathsf{F}}^{\langle\langle i\rangle\rangle}\}$ can be considered as the access structure of the VSS-1-PI scheme with secret image $SI^{\langle\langle i\rangle\rangle}$ for share set $\boldsymbol{V}^{\langle\langle i\rangle\rangle}$. Then, letting $\mathcal{E}^{\langle\langle i\rangle\rangle}$ be the set of colors necessary to encrypt $SI^{\langle\langle i\rangle\rangle}$, the basis matrices of the $(\Gamma^{\langle\langle i\rangle\rangle}, \boldsymbol{V}^{\langle\langle i\rangle\rangle}, \mathcal{E}^{\langle\langle i\rangle\rangle}, \boldsymbol{r}^{\langle\langle i\rangle\rangle})$-VSS-1-PI scheme can be constructed by the method in Section 7.5. Therefore, letting $|\boldsymbol{V}^{\langle\langle i\rangle\rangle}| \times m^{\langle\langle i\rangle\rangle}$ matrices $G^{\langle\langle i\rangle\rangle,j}$, for $j = 1, 2, \ldots, K$, be the basis matrices of the $(\Gamma^{\langle\langle i\rangle\rangle}, \boldsymbol{V}^{\langle\langle i\rangle\rangle}, \mathcal{E}^{\langle\langle i\rangle\rangle}, \boldsymbol{r}^{\langle\langle i\rangle\rangle})$-VSS-1-PI scheme, where $m^{\langle\langle i\rangle\rangle}$ is the pixel expansion for secret image $SI^{\langle\langle i\rangle\rangle}$, then $G^{\langle\langle i\rangle\rangle,j}$ represents a color $\mathsf{D}^{\langle\langle i\rangle\rangle,j}$ and satisfies that $G^{\langle\langle i\rangle\rangle,j} = G^{\langle\langle i\rangle\rangle,j'}$ if $\mathsf{D}^{\langle\langle i\rangle\rangle,j}$ and $\mathsf{D}^{\langle\langle i\rangle\rangle,j'}$ are the same color. Furthermore, basis matrix $G^{\langle\langle i\rangle\rangle,j}$ satisfies conditions (i) and (ii)′, i.e., the number of $\gamma(\mathsf{D}^{\langle\langle i\rangle\rangle,j})$ included in $\eta(G^{\langle\langle i\rangle\rangle,j}[\![\boldsymbol{A}]\!])$, $\sum_{l=0}^{\ell} \delta_{\mathsf{x}_{(l)}}^{\langle\langle i\rangle\rangle}$ where $\mathsf{x} \stackrel{\text{def}}{=} \gamma(\mathsf{D}^{\langle\langle i\rangle\rangle,j})$, is constant for any $\boldsymbol{A} \in \mathcal{A}_{\mathsf{Q}}^{\langle\langle i\rangle\rangle-}$, and it holds that $G^{\langle\langle i\rangle\rangle,1}[\![\boldsymbol{A}]\!] \sim G^{\langle\langle i\rangle\rangle,2}[\![\boldsymbol{A}]\!] \sim \cdots \sim G^{\langle\langle i\rangle\rangle,K}[\![\boldsymbol{A}]\!]$ for any $\boldsymbol{A} \in \mathcal{A}_{\mathsf{F}}^{\langle\langle i\rangle\rangle}$.

Next, we construct an $n \times m^{\langle\langle i\rangle\rangle}$ matrix $H^{\langle\langle i\rangle\rangle,j}$ defined by

$$H^{\langle\langle i\rangle\rangle,j}\left[\!\left[\boldsymbol{V}^{\langle\langle i\rangle\rangle}\right]\!\right] = G^{\langle\langle i\rangle\rangle,j}, \tag{8.21}$$

$$H^{\langle\langle i\rangle\rangle,j}\left[\!\left[\overline{\boldsymbol{V}^{\langle\langle i\rangle\rangle}}\right]\!\right] = J, \tag{8.22}$$

where matrix J consists of only $\mathsf{1}$'s and $\overline{\boldsymbol{V}^{\langle\langle i\rangle\rangle}}$ means the complement set of $\boldsymbol{V}^{\langle\langle i\rangle\rangle}$ on $\boldsymbol{V}$. Then we construct $n \times m$ basis matrices $B^j,\ j = 1, 2, \ldots, K$, by

$$B^j = \bigodot_{i=1}^{q} H^{\langle\langle i\rangle\rangle,j}, \tag{8.23}$$

where $m = \sum_{i=1}^{q} m^{\langle\langle i\rangle\rangle}$.

We now consider two categories Θ_1 and Θ_2 for the access structures of VSS-q-PI schemes.

Definition 8.8

(i) An access structure Γ is in Θ_1 if it satisfies $\boldsymbol{A} \cap \overline{\boldsymbol{V}^{\langle\langle i'\rangle\rangle}} \neq \emptyset$ for any i and i' such that $\boldsymbol{A} \in \mathcal{A}_{\mathsf{Q}}^{\langle\langle i\rangle\rangle-}$ and $i' \in \boldsymbol{I}(\boldsymbol{A}) - \{i\}$.

(ii) An access structure Γ is in Θ_2 if it satisfies that $\boldsymbol{A} \cap \overline{\boldsymbol{V}^{\langle\langle i'\rangle\rangle}} \neq \emptyset$ for any i and $i'(\neq i)$ such that $\boldsymbol{A} \in \mathcal{A}_{\mathsf{Q}}^{\langle\langle i\rangle\rangle-}$. □

Remark 8.9 It is obvious from the above definition that $\Theta_2 \subset \Theta_1$, and it holds generally that $\Theta_2 \subsetneq \Theta_1$. Furthermore, there exist access structures that are not included in Θ_1. □

Example 8.10 Assume that an access structure Γ_{ID} is defined by

$$\mathcal{A}_{\mathsf{F}} = \{\{V_2\}\}, \tag{8.24}$$
$$\mathcal{A}_{\mathsf{Q}}^{\langle\langle 1\rangle\rangle -} = \{\{V_1\}\}, \tag{8.25}$$
$$\mathcal{A}_{\mathsf{Q}}^{\langle\langle 2\rangle\rangle -} = \{\{V_1, V_2\}\}. \tag{8.26}$$

Then, Γ_{ID} does not belong to Θ_1, and hence, nor Θ_2. From (8.25), secret image $SI^{\langle\langle 1\rangle\rangle}$ can be obtained only from V_1. Hence, $SI^{\langle\langle 1\rangle\rangle}$ can be considered as the identification (ID) image of share 1 although $SI^{\langle\langle 2\rangle\rangle}$ is a secret image. The above access structure Γ_{ID} is a modified version of the $(2, 2)$-VSS scheme with two ID images [2], [43], and note that VSS-q-PI schemes include such VSS schemes with ID images as special cases.

Next, consider the access structure Γ_g treated in [107], which is given by

$$\mathcal{A}_{\mathsf{F}} = \{\{V_1\}, \{V_2\}, \{V_3\}, \{V_4\}, \{V_5\}\}, \tag{8.27}$$
$$\mathcal{A}_{\mathsf{Q}}^{\langle\langle 1\rangle\rangle -} = \{\{V_1, V_2\}, \{V_1, V_5\}, \{V_2, V_3\}, \{V_3, V_4\}, \{V_4, V_5\}\}, \tag{8.28}$$
$$\mathcal{A}_{\mathsf{Q}}^{\langle\langle 2\rangle\rangle -} = \{\{V_1, V_3\}, \{V_1, V_4\}, \{V_2, V_4\}, \{V_2, V_5\}, \{V_3, V_5\}\}. \tag{8.29}$$

Then, Γ_g is included in Θ_1 but not in Θ_2. □

Theorem 8.11 B^j, $j = 1, 2, \ldots, K$, given by (8.23) are the basis matrices of the $(\Gamma, \boldsymbol{V}, \mathcal{E}, \boldsymbol{D})$-VSS-$q$-PI scheme, if $|\mathcal{E}| = 2$ and $\Gamma \in \Theta_1$, or if $|\mathcal{E}| \geq 3$ and $\Gamma \in \Theta_2$. □

Example 8.12 We show how the basis matrices given by (8.16) can be derived from Theorem 8.11 for the access structures Γ given by (8.9)–(8.11) in Example 8.1 and the color matrix $\boldsymbol{D}$ given by (8.13) in Example 8.2. Note that the access structure Γ belongs to Θ_2. From (8.19) and (8.20), we have $\tilde{\mathcal{A}}_{\mathsf{F}}^{\langle\langle 1\rangle\rangle} = \{\{V_1\}, \{V_2\}, \{V_3\}\}$ and $\tilde{\mathcal{A}}_{\mathsf{F}}^{\langle\langle 2\rangle\rangle} = \{\{V_3\}, \{V_4\}\}$. Then the basis matrices $G^{\langle\langle i\rangle\rangle, j}$ of the $(\Gamma^{\langle\langle 1\rangle\rangle}, \boldsymbol{V}^{\langle\langle 1\rangle\rangle}, \mathcal{E}^{\langle\langle 1\rangle\rangle}, \boldsymbol{r}^{\langle\langle 1\rangle\rangle})$-VSS-1-PI scheme and the $(\Gamma^{\langle\langle 2\rangle\rangle}, \boldsymbol{V}^{\langle\langle 2\rangle\rangle}, \mathcal{E}^{\langle\langle 2\rangle\rangle}, \boldsymbol{r}^{\langle\langle 2\rangle\rangle})$-VSS-1-PI scheme are given by

$$G^{\langle\langle 1\rangle\rangle,1} = G^{\langle\langle 1\rangle\rangle,3} = \begin{bmatrix} \mathsf{1bb} \\ \mathsf{b1b} \\ \mathsf{bb1} \end{bmatrix}, \; G^{\langle\langle 1\rangle\rangle,2} = G^{\langle\langle 1\rangle\rangle,4} = \begin{bmatrix} \mathsf{1bb} \\ \mathsf{1bb} \\ \mathsf{1bb} \end{bmatrix},$$

and

$$G^{\langle\langle 2\rangle\rangle,1} = G^{\langle\langle 2\rangle\rangle,2} = \begin{bmatrix} \mathsf{y1r} \\ \mathsf{yr1} \end{bmatrix}, \; G^{\langle\langle 2\rangle\rangle,3} = G^{\langle\langle 2\rangle\rangle,4} = \begin{bmatrix} \mathsf{ry1} \\ \mathsf{r1y} \end{bmatrix}, \tag{8.30}$$

respectively. Hence we obtain from (8.21) and (8.22) that

$$H^{\langle\langle 1\rangle\rangle,1} = H^{\langle\langle 1\rangle\rangle,3} = \begin{bmatrix} \mathsf{1bb} \\ \mathsf{1bb} \\ \mathsf{1bb} \\ \mathsf{111} \end{bmatrix}, \; H^{\langle\langle 1\rangle\rangle,2} = H^{\langle\langle 1\rangle\rangle,4} = \begin{bmatrix} \mathsf{1bb} \\ \mathsf{b1b} \\ \mathsf{bb1} \\ \mathsf{111} \end{bmatrix},$$

$$H^{\langle\langle 2\rangle\rangle,1} = H^{\langle\langle 2\rangle\rangle,2} = \begin{bmatrix} \mathsf{111} \\ \mathsf{111} \\ \mathsf{ry1} \\ \mathsf{r1y} \end{bmatrix},\ H^{\langle\langle 2\rangle\rangle,3} = H^{\langle\langle 2\rangle\rangle,4} = \begin{bmatrix} \mathsf{111} \\ \mathsf{111} \\ \mathsf{y1r} \\ \mathsf{yr1} \end{bmatrix}. \tag{8.31}$$

Finally, basis matrices B^1, B^2, B^3 and B^4 are given from (8.23) as follows.

$$\begin{aligned} B^1 &= H^{\langle\langle 1\rangle\rangle,1} \odot H^{\langle\langle 2\rangle\rangle,1},\ B^2 = H^{\langle\langle 1\rangle\rangle,2} \odot H^{\langle\langle 2\rangle\rangle,2}, \\ B^3 &= H^{\langle\langle 1\rangle\rangle,3} \odot H^{\langle\langle 2\rangle\rangle,3},\ B^4 = H^{\langle\langle 1\rangle\rangle,4} \odot H^{\langle\langle 2\rangle\rangle,4}, \end{aligned} \tag{8.32}$$

which are equivalent to (8.16). □

Remark 8.13 In [107], it is shown that the access structure Γ_g given by (8.27)–(8.29) in Example 8.10 can be represented by a graph. In the case of $|\mathcal{E}| = 2$, as treated in [107], (8.23) gives the basis matrices. But in the case of $|\mathcal{E}| \geq 3$, (8.23) does not give the basis matrices for Γ_g generally because Γ_g does not satisfy the condition of Theorem 8.11, i.e., $\Gamma_g \notin \Theta_2$. □

8.3.2 Proof of Theorem 8.11

In this subsection, we prove Theorem 8.11. We first show that matrices $H^{\langle\langle i\rangle\rangle,j}$ given by (8.21) and (8.22) satisfy the next lemma.

Lemma 8.14 For any $i \notin \boldsymbol{I}(\boldsymbol{A})$, it holds that

$$H^{\langle\langle i\rangle\rangle,1}[\![\boldsymbol{A}]\!] \sim H^{\langle\langle i\rangle\rangle,2}[\![\boldsymbol{A}]\!] \sim \cdots \sim H^{\langle\langle i\rangle\rangle,K}[\![\boldsymbol{A}]\!]. \tag{8.33}$$

□

Proof of Lemma 8.14 From (8.14), we note that $\boldsymbol{A} \in \tilde{\mathcal{A}}_{\mathsf{F}}^{\langle\langle i\rangle\rangle}$ if $i \notin \boldsymbol{I}(\boldsymbol{A})$. Hence, from the monotonicity of $\tilde{\mathcal{A}}_{\mathsf{F}}^{\langle\langle i\rangle\rangle}$, it holds that $\boldsymbol{A} \cap \boldsymbol{V}^{\langle\langle i\rangle\rangle} \in \tilde{\mathcal{A}}_{\mathsf{F}}^{\langle\langle i\rangle\rangle}$ for $i \notin \boldsymbol{I}(\boldsymbol{A})$.

$H^{\langle\langle i\rangle\rangle,j}[\![\boldsymbol{A}]\!]$ can be represented as

$$H^{\langle\langle i\rangle\rangle,j}[\![\boldsymbol{A}]\!] = H^{\langle\langle i\rangle\rangle,j}\left[\!\!\left[\left(\boldsymbol{A} \cap \boldsymbol{V}^{\langle\langle i\rangle\rangle}\right) \cup \left(\boldsymbol{A} \cap \overline{\boldsymbol{V}^{\langle\langle i\rangle\rangle}}\right)\right]\!\!\right]. \tag{8.34}$$

In (8.34), it holds for $i \notin \boldsymbol{I}(\boldsymbol{A})$ that $H^{\langle\langle i\rangle\rangle,1}[\![\boldsymbol{A} \cap \boldsymbol{V}^{\langle\langle i\rangle\rangle}]\!] \sim H^{\langle\langle i\rangle\rangle,2}[\![\boldsymbol{A} \cap \boldsymbol{V}^{\langle\langle i\rangle\rangle}]\!] \sim \cdots \sim H^{\langle\langle i\rangle\rangle,K}[\![\boldsymbol{A} \cap \boldsymbol{V}^{\langle\langle i\rangle\rangle}]\!]$ since $H^{\langle\langle i\rangle\rangle,j}[\![\boldsymbol{V}^{\langle\langle i\rangle\rangle}]\!]$ satisfies (8.21) and $\boldsymbol{A} \cap \boldsymbol{V}^{\langle\langle i\rangle\rangle} \in \tilde{\mathcal{A}}_{\mathsf{F}}^{\langle\langle i\rangle\rangle}$. On the other hand, from (8.22), all the elements of $H^{\langle\langle i\rangle\rangle,j}[\![\boldsymbol{A} \cap \overline{\boldsymbol{V}^{\langle\langle i\rangle\rangle}}]\!]$ are 1 for every j. Therefore, (8.33) holds for any $i \notin \boldsymbol{I}(\boldsymbol{A})$. □

Proof of Theorem 8.11 First, we show that B^j given by (8.23) satisfies the condition (i) in Definition 8.4. Substituting (8.23) into $\eta(B^j[\![\boldsymbol{A}]\!])$ for $\boldsymbol{A} \in \mathcal{A}_{\mathsf{Q}}^{\langle\langle i\rangle\rangle^-}$, we have

$$\begin{aligned} \eta\left(B^j[\![\boldsymbol{A}]\!]\right) &= \eta\left(\bigodot_{i'=1}^{q} H^{\langle\langle i'\rangle\rangle,j}[\![\boldsymbol{A}]\!]\right) \\ &\sim \eta(H^{\langle\langle i\rangle\rangle,j}[\![\boldsymbol{A}]\!]) \odot \eta\left(\bigodot_{\substack{i'=1 \\ i' \neq i}}^{q} H^{\langle\langle i'\rangle\rangle,j}[\![\boldsymbol{A}]\!]\right) \\ &\sim \eta(G^{\langle\langle i\rangle\rangle,j}[\![\boldsymbol{A}]\!]) \odot \eta(X^{\langle\langle i\rangle\rangle,j}) \odot \eta(Y^{\langle\langle i\rangle\rangle,j}), \end{aligned} \tag{8.35}$$

where $X^{\langle\langle i\rangle\rangle,j}$ and $Y^{\langle\langle i\rangle\rangle,j}$ are defined as

$$X^{\langle\langle i\rangle\rangle,j} = \bigodot_{i' \in (\ )-\{i\}} H^{\langle\langle i'\rangle\rangle,j}[\![\boldsymbol{A}^{\langle\langle i\rangle\rangle-}]\!], \tag{8.36}$$

$$Y^{\langle\langle i\rangle\rangle,j} = \bigodot_{i' \notin (\ )} H^{\langle\langle i'\rangle\rangle,j}[\![\boldsymbol{A}]\!]. \tag{8.37}$$

Note that since $G^{\langle\langle i\rangle\rangle,j}$ is the basis matrix of the $(\Gamma^{\langle\langle i\rangle\rangle}, \boldsymbol{V}^{\langle\langle i\rangle\rangle}, \mathcal{E}^{\langle\langle i\rangle\rangle}, \boldsymbol{r}^{\langle\langle i\rangle\rangle})$-VSS-1-PI scheme, it satisfies the condition (i) in Definition 8.4 for the $(\Gamma^{\langle\langle i\rangle\rangle}, \boldsymbol{V}^{\langle\langle i\rangle\rangle}, \mathcal{E}^{\langle\langle i\rangle\rangle}, \boldsymbol{r}^{\langle\langle i\rangle\rangle})$-VSS-1-PI scheme. First consider the case of $|\mathcal{E}| = 2$ with $\mathcal{E} = \{1, \mathsf{e}\}$. In this case, $\eta(G^{\langle\langle i\rangle\rangle,j})$, $\eta(X^{\langle\langle i\rangle\rangle,j})$, and $\eta(Y^{\langle\langle i\rangle\rangle,j})$ are vectors with two colors, e and 1. Hence, if for each i, $\eta(X^{\langle\langle i\rangle\rangle,j}) \odot \eta(Y^{\langle\langle i\rangle\rangle,j})$ are equivalent with respect to $\sim$ for any j, (8.15) is satisfied for $\eta(B^j[\![\boldsymbol{A}]\!])$. From Lemma 8.14, we have that

$$H^{\langle\langle i'\rangle\rangle,1}[\![\boldsymbol{A}]\!] \sim H^{\langle\langle i'\rangle\rangle,2}[\![\boldsymbol{A}]\!] \sim \cdots \sim H^{\langle\langle i'\rangle\rangle,K}[\![\boldsymbol{A}]\!] \tag{8.38}$$

for any $i' \notin \boldsymbol{I}(\boldsymbol{A})$. Hence, for each i, $\eta(Y^{\langle\langle i\rangle\rangle,j})$ are equivalent for any j. Furthermore, for any $i' \in \boldsymbol{I}(\boldsymbol{A}) - \{i\}$, $\eta(H^{\langle\langle i'\rangle\rangle,j}[\![\boldsymbol{A}]\!])$ can be represented as

$$\eta(H^{\langle\langle i'\rangle\rangle,j}[\![\boldsymbol{A}]\!]) = \eta\left(H^{\langle\langle i'\rangle\rangle,j}\left[\!\!\left[\left(\boldsymbol{A} \cap \boldsymbol{V}^{\langle\langle i'\rangle\rangle}\right) \cup \left(\boldsymbol{A} \cap \overline{\boldsymbol{V}^{\langle\langle i'\rangle\rangle}}\right)\right]\!\!\right]\right). \tag{8.39}$$

Since (8.22) holds and we have that $\boldsymbol{A} \cap \overline{\boldsymbol{V}^{\langle\langle i'\rangle\rangle}} \neq \emptyset$ for such i' from the assumption $\Gamma \in \Theta_1$ in Theorem 8.11, $\eta(H^{\langle\langle i'\rangle\rangle,j}[\![\boldsymbol{A}]\!])$ consists of only $\mathsf{1}$'s. Hence, all $\eta(X^{\langle\langle i\rangle\rangle,j})$ are also equivalent for any j.

In the case of $|\mathcal{E}| \geq 3$, $\eta(X^{\langle\langle i\rangle\rangle,j})$ and $\eta(Y^{\langle\langle i\rangle\rangle,j})$ may have three or more colors, and hence (8.15) may not be satisfied even if $\eta(X^{\langle\langle i\rangle\rangle,j}) \odot \eta(Y^{\langle\langle i\rangle\rangle,j})$ are equivalent for any j. But, because for any $i' \neq i$, $\boldsymbol{A} \cap \overline{\boldsymbol{V}^{\langle\langle i'\rangle\rangle}} \neq \emptyset$ in (8.39) holds from the assumption $\Gamma \in \Theta_2$ in Theorem 8.11, all elements in $\eta(X^{\langle\langle i\rangle\rangle,j}) \odot \eta(Y^{\langle\langle i\rangle\rangle,j})$ are 1 from (8.22). Hence, (8.15) holds for $\eta(B^j[\![\boldsymbol{A}]\!])$.

Next, let us check that B^j's satisfy the condition (ii) in Definition 8.4. For $\boldsymbol{A} \in \mathcal{A}_{\mathsf{F}}$, $B^j[\![\boldsymbol{A}]\!]$ can be represented as

$$\begin{aligned} B^j[\![\boldsymbol{A}]\!] &= \bigodot_{i=1}^{q} H^{\langle\langle i\rangle\rangle,j}[\![\boldsymbol{A}]\!] \\ &\sim \left[\bigodot_{i \in (\ )} H^{\langle\langle i\rangle\rangle,j}[\![\boldsymbol{A}]\!]\right] \odot \left[\bigodot_{i \notin (\ )} H^{\langle\langle i\rangle\rangle,j}[\![\boldsymbol{A}]\!]\right]. \end{aligned} \tag{8.40}$$

Suppose for the set $\boldsymbol{A} \subseteq \boldsymbol{V}$ that j and $j'(\neq j)$ satisfy $\boldsymbol{c}^j[\![\boldsymbol{I}(\boldsymbol{A})]\!] = \boldsymbol{c}^{j'}[\![\boldsymbol{I}(\boldsymbol{A})]\!]$, which means that $\mathsf{D}^{\langle\langle i\rangle\rangle,j} = \mathsf{D}^{\langle\langle i\rangle\rangle,j'}$ for any $i \in \boldsymbol{I}(\boldsymbol{A})$. Then, it holds that $G^{\langle\langle i\rangle\rangle,j} = G^{\langle\langle i\rangle\rangle,j'}$ from the definition of $G^{\langle\langle i\rangle\rangle,j}$, and hence $H^{\langle\langle i\rangle\rangle,j} = H^{\langle\langle i\rangle\rangle,j'}$ from (8.21) and (8.22). Furthermore, for any $i \notin \boldsymbol{I}(\boldsymbol{A})$, it holds from Lemma 8.14 that $H^{\langle\langle i\rangle\rangle,1}[\![\boldsymbol{A}]\!] \sim H^{\langle\langle i\rangle\rangle,2}[\![\boldsymbol{A}]\!] \sim \cdots \sim H^{\langle\langle i\rangle\rangle,K}[\![\boldsymbol{A}]\!]$. Therefore, it holds that $B^j[\![\boldsymbol{A}]\!] \sim B^{j'}[\![\boldsymbol{A}]\!]$. □

8.4 Construction Method by Duplicating Secret Images

In the previous sections, we have shown how to construct VSS-q-PI schemes for the case that an access structure Γ is included in Θ_1 or Θ_2 for $|\mathcal{E}| = 2$ or $|\mathcal{E}| \geq 3$, respectively. In this section, we treat the case that Γ is not included in Θ_1 nor Θ_2.

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

Suppose that an access structure $\Gamma = \left\{ \{\mathcal{A}_{\mathsf{Q}}^{\langle\langle i \rangle\rangle}\}_{i=1}^{q}, \mathcal{A}_{\mathsf{F}} \right\}$ is given, which may not be included in Θ_1 nor Θ_2. For this Γ, we consider the union of all $\mathcal{A}_{\mathsf{Q}}^{\langle\langle i \rangle\rangle -}$. Let us assume that the union has $\hat{q}$ elements $\boldsymbol{A}_i$, $i = 1, 2, \ldots, \hat{q}$, i.e.,

$$\bigcup_{i=1}^{q} \mathcal{A}_{\mathsf{Q}}^{\langle\langle i \rangle\rangle -} = \{\boldsymbol{A}_1, \boldsymbol{A}_2, \ldots, \boldsymbol{A}_{\hat{q}}\}. \tag{8.41}$$

Then, for each $\boldsymbol{A}_i$, we define $\hat{\mathcal{A}}_{\mathsf{Q}}^{\langle\langle i \rangle\rangle -}$ by

$$\hat{\mathcal{A}}_{\mathsf{Q}}^{\langle\langle i \rangle\rangle -} = \{\boldsymbol{A}_i\} \ \text{ for } \ 1 \leq i \leq \hat{q}. \tag{8.42}$$

For such $\left\{ \hat{\mathcal{A}}_{\mathsf{Q}}^{\langle\langle i \rangle\rangle -} \right\}_{i=1}^{\hat{q}}$, we can define a new access structure $\hat{\Gamma} = \left\{ \{\hat{\mathcal{A}}_{\mathsf{Q}}^{\langle\langle i \rangle\rangle}\}_{i=1}^{\hat{q}}, \mathcal{A}_{\mathsf{F}} \right\}$ for the set of secret images, $\hat{SI}^{\langle\langle i \rangle\rangle}$, $i = 1, 2, \ldots, \hat{q}$, some of which may be the same image. Furthermore, we define the set of significant shares $\hat{\boldsymbol{V}}^{\langle\langle i \rangle\rangle}$ for $\hat{SI}^{\langle\langle i \rangle\rangle}$ like (8.8), the set of colors $\hat{\mathcal{D}}^{\langle\langle i \rangle\rangle}$, and the color matrix $\hat{\boldsymbol{D}}$.

Note that the forbidden sets of $\hat{\Gamma}$ are the same as Γ, and it holds that $\boldsymbol{A}_i = \hat{\boldsymbol{V}}^{\langle\langle i \rangle\rangle}$ for all i. Hence, we have

$$\hat{\mathcal{A}}_{\mathsf{Q}}^{\langle\langle i \rangle\rangle -} = \left\{ \boldsymbol{V}^{\langle\langle i \rangle\rangle} \right\} \ \text{ for } \ 1 \leq i \leq \hat{q}. \tag{8.43}$$

Remark 8.15 In the case of $\mathcal{A}_{\mathsf{F}} = \{\emptyset\}$, $\hat{\Gamma}$ coincides with the access structure proposed in [35] for BW-binary plural secret images. Furthermore, applying (8.41) and (8.42) to the access structure of a VSS-1-PI scheme for a BW-binary secret image, the basis matrix obtained by (8.23) coincides with the basis matrix given in [10]. □

Lemma 8.16 For the access structure $\hat{\Gamma}$, the following two statements hold.

1. For any $i' \in \boldsymbol{I}(\hat{\boldsymbol{V}}^{\langle\langle i \rangle\rangle}) - \{i\}$, it holds that $\hat{\boldsymbol{V}}^{\langle\langle i \rangle\rangle} \cap \overline{\hat{\boldsymbol{V}}^{\langle\langle i' \rangle\rangle}} \neq \emptyset$.
2. If

$$\boldsymbol{I}\left(\hat{\boldsymbol{V}}^{\langle\langle i \rangle\rangle}\right) = \{i\}, \tag{8.44}$$

then it holds that $\hat{\boldsymbol{V}}^{\langle\langle i' \rangle\rangle} \cap \overline{\hat{\boldsymbol{V}}^{\langle\langle i \rangle\rangle}} \neq \emptyset$ for any $i' (\neq i)$. □

Proof of Lemma 8.16 Note from the definition of $\hat{\boldsymbol{V}}^{\langle\langle i\rangle\rangle}$ that $\hat{\boldsymbol{V}}^{\langle\langle i\rangle\rangle} \neq \hat{\boldsymbol{V}}^{\langle\langle i'\rangle\rangle}$ for any $i \neq i'$.

1. For any $i' \in \boldsymbol{I}(\hat{\boldsymbol{V}}^{\langle\langle i\rangle\rangle}) - \{i\}$, it holds that $\hat{\boldsymbol{V}}^{\langle\langle i\rangle\rangle} \supsetneq \hat{\boldsymbol{V}}^{\langle\langle i'\rangle\rangle}$, which means that $\hat{\boldsymbol{V}}^{\langle\langle i\rangle\rangle} \cap \overline{\hat{\boldsymbol{V}}^{\langle\langle i'\rangle\rangle}} \neq \emptyset$.
2. Suppose that $\hat{\boldsymbol{V}}^{\langle\langle i'\rangle\rangle} \cap \overline{\hat{\boldsymbol{V}}^{\langle\langle i\rangle\rangle}} = \emptyset$ for some $i' (\neq i)$. Then we have that $\hat{\boldsymbol{V}}^{\langle\langle i'\rangle\rangle} \subsetneq \hat{\boldsymbol{V}}^{\langle\langle i\rangle\rangle}$, which implies that $i' \in \boldsymbol{I}(\hat{\boldsymbol{V}}^{\langle\langle i\rangle\rangle}) - \{i\}$ and violates (8.44). □

From Lemma 8.16, Theorem 8.11 and (8.43), the next theorem holds for the access structure $\hat{\Gamma}$.

Theorem 8.17 Suppose that the access structure $\hat{\Gamma}$ is constructed by (8.41) and (8.42) from Γ. Then, in the case of $|\mathcal{E}| = 2$, or in the case that $|\mathcal{E}| \geq 3$ and $\hat{\Gamma}$ satisfies (8.44) for all i, the basis matrices of $(\hat{\Gamma}, \boldsymbol{V}, \mathcal{E}, \hat{\boldsymbol{D}})$-VSS-$\hat{q}$-PI scheme can be obtained by (8.23). □

Theorem 8.17 implies that the basis matrices of the VSS-q-PI scheme with the access structure $\hat{\Gamma}$ can always be constructed by (8.23) if $|\mathcal{E}| = 2$. However, in the case of $|\mathcal{E}| \geq 3$, if an access structure requires ID images, we cannot obtain the basis matrices of the access structure from (8.23) because $\hat{\boldsymbol{V}}^{\langle\langle i\rangle\rangle}$ must reproduce the ID image and a secret image, and hence, (8.44) does not hold. The VSS scheme with color ID images is proposed for $|\mathcal{E}| \geq 3$ in [43], where the basis matrices not satisfying (8.15) are used.

Finally, we note that for the construction shown in the above, pixel expansion m is given from (7.68) by

$$m = \sum_{i=1}^{\hat{q}} m^{\langle\langle i\rangle\rangle} = \sum_{i=1}^{\hat{q}} \sum_{\mathsf{x} \in \zeta(\mathcal{D}^{\langle\langle i\rangle\rangle})} \sum_{l=1}^{L_{\mathsf{x}}} \delta_{\mathsf{x}_{(l)}}^{\langle\langle i\rangle\rangle}\, 2^{|\hat{\ }^{\langle\langle i\rangle\rangle}|-1}, \tag{8.45}$$

where $\zeta(\cdot)$ is defined by (7.65), if we construct the basis matrices $H^{\langle\langle i\rangle\rangle,j}$ in (8.23) based on the construction given in Section 7.5.2.

For example, the pixel expansion of the VSS-2-PI scheme with the access structure given by (8.27)–(8.29) for black-white secret images is 12 if the method shown in Section 8.3 is used with the star graph decomposition [107]. But, if we use (8.41) and (8.42), we have $\hat{q} = 10$, and the pixel expansion becomes 20 from (8.45). In general, the pixel expansion attained by the method shown in this section is larger than the method in Section 8.3. However, it is reported that a VSS scheme with 144 $(= 12 \times 12)$ subpixels can be used [45], and hence, it is not hard to use the VSS-2-PI with 20 subpixels in practice.

8.5 Comparison with Trivial Schemes

In the framework of VSS-q-PI schemes, we assume that each participant has one share. But, in some cases each participant may be allowed to have two or more shares. In such cases, VSS schemes for q plural secret images can easily be constructed by using q individual usual VSS schemes, i.e., VSS-1-PI schemes, with access structure $\Gamma^{\langle\langle i\rangle\rangle} = \{\tilde{\mathcal{A}}_{\mathsf{Q}}^{\langle\langle i\rangle\rangle}, \tilde{\mathcal{A}}_{\mathsf{F}}^{\langle\langle i\rangle\rangle}\}$ for each secret

image $SI^{\langle\langle i\rangle\rangle}$. In such trivial VSS schemes, shares $V_1^{\langle\langle i\rangle\rangle}\, V_2^{\langle\langle i\rangle\rangle}, \ldots, V_n^{\langle\langle i\rangle\rangle}$ are constructed for the i-th secret image, and the ℓ-th participant has share set $\{V_\ell^{\langle\langle 1\rangle\rangle}, V_\ell^{\langle\langle 2\rangle\rangle}, \ldots, V_\ell^{\langle\langle q\rangle\rangle}\}$. In this section we compare the VSS-q-PI schemes with such trivial schemes.

The trivial schemes can realize any access structures although the VSS-q-PI schemes cannot realize them if they don't satisfy the conditions described in Theorems 8.11 or 8.17. Furthermore, the pixel expansion of the trivial scheme is less than the VSS-q-PI scheme for the same access structure. This means that the trivial schemes attain higher resolution than the VSS-q-PI schemes in decrypted images. However, in the trivial schemes, each participant must hold securely q plural shares. On the contrary, each participant must hold securely only one share in the VSS-q-PI scheme.

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

1. The VSS scheme with ID images [2], [43], which is considered as a special case of the VSS-q-PI scheme, cannot be realized by the trivial scheme.[2]

2. Consider the case that a lot with *win* and *lose* is made by a VSS scheme, where secret images $SI^{(W)}$ and $SI^{(L)}$ represent *win* and *lose*, respectively.

   In the case of the trivial scheme, letting $\boldsymbol{V}^{(W)} = \{V_1^{(W)}, V_2^{(W)}\}$ and $\boldsymbol{V}^{(L)} = \{V_1^{(L)}, V_2^{(L)}\}$ be the share sets of the $(2,2)$-threshold VSS-1-PI scheme for secret images $SI^{(W)}$ and $SI^{(L)}$, respectively, the lot can be realized if a dealer holds $\{V_1^{(W)}, V_1^{(L)}\}$ and distributes $V_2^{(W)}$ or $V_2^{(L)}$ to people participating in the lot. In this case, two times decryption, i.e., stacking shares, is required to know the result of the lot.

   On the contrary, in the case of the VSS-q-PI scheme, we can use the access structure $\Gamma^{(W,L)}$ with $\mathcal{A}_{\mathsf{Q}}^{(W)-} = \{\{V_1, V_2\}\}$, $\mathcal{A}_{\mathsf{Q}}^{(L)-} = \{\{V_1, V_3\}\}$ and $\mathcal{A}_{\mathsf{F}}^{+} = \{\{V_2, V_3\}\}$. Letting $\{V_1, V_2, V_3\}$ be the share set, a dealer holds V_1 and distributes V_2 or V_3 to the people. In this case, by only once decryption, we can know the result of the lot.[3]

   This advantage of speedy decryption becomes larger as the number of results in the lot becomes larger, and the advantage may be essential in commercial uses.

3. Next, consider the case that a VSS scheme is used as a tally. We have groups X, Y, Z, and Alice, Bob and Carol belong to X and Y, X and Z, Y, respectively. Each of them wants to prove to Peggy which groups he/she belongs to. In the case of the trivial schemes, the tally can be realized by letting $\boldsymbol{V}^{(X)} = \{V_1^{(X)}, V_2^{(X)}\}$, $\boldsymbol{V}^{(Y)} = \{V_1^{(Y)}, V_2^{(Y)}\}$, and $\boldsymbol{V}^{(Z)} = \{V_1^{(Z)}, V_2^{(Z)}\}$ be the sets of shares of the $(2,2)$-threshold VSS-1-PI schemes for secret images $SI^{(X)}, SI^{(Y)}, SI^{(Z)}$, respectively, and distributing $\{V_1^{(X)}, V_1^{(Y)}, V_1^{(Z)}\}$, $\{V_2^{(X)}, V_2^{(Y)}\}$, $\{V_2^{(X)}, V_2^{(Z)}\}$, and $V_2^{(Y)}$, to Peggy, Alice, Bob, and Carol, respectively.

   In the case of the VSS-q-PI scheme, the tally can be realized by letting $\{V_1, V_2, \ldots, V_6\}$ be the share set of the VSS-q-PI scheme for the access structure given by $\mathcal{A}_{\mathsf{Q}}^{(X)-} =$

[2]The VSS schemes with color ID images are treated in [43]. However, the VSS schemes with color ID images cannot be constructed by our method. See the next paragraph of Theorem 8.17.

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

$\{\{V_1, V_4\}, \{V_1, V_5\}\}$, $\mathcal{A}_{\mathsf{Q}}^{(Y)-} = \{\{V_2, V_4\}, \{V_2, V_6\}\}$, and $\mathcal{A}_{\mathsf{Q}}^{(Z)-} = \{\{V_3, V_5\}\}$, and distributing $\{V_1, V_2, V_3\}$, V_4, V_5, V_6 to Peggy, Alice, Bob, and Carol, respectively.

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

(a) If Alice conspires with Bob, Alice can deceive Peggy by showing $\{V_2^{(X)}, V_2^{(Y)}, V_2^{(Z)}\}$ to prove that Alice belongs to all of X, Y, Z. (b) Bob can hide by showing only $V_2^{(Z)}$ that he belongs to X. (c) Assume that an adversary wants to impersonate Alice. Such impersonation attack can be achieved by stealing $V_2^{(X)}$ from Bob and $V_2^{(Y)}$ from Carol besides by stealing $\{V_2^{(X)}, V_2^{(Y)}\}$ from Alice.

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

8.6 Conclusion

In this chapter, we considered methods to construct visual secret sharing schemes for q plural secret images (VSS-q-PI scheme) with general access structures. In the proposed VSS-q-PI schemes, each qualified set of shares can decrypt their own secret images, but it does not leak out any information of the other secret images. Furthermore, the proposed scheme can encode color and/or gray-scale secret images in addition to black-white images. Finally in Section 8.5, we discussed the merits of the VSS-q-PI schemes compared with the trivial schemes.

Chapter 9

Conclusions of Part II

9.1 Summary of Results

In Part II, we proposed new construction methods of VSS schemes for general access structures, which can be applied to any type of plural secret images.

In Chapter 7, the algebraic constructions of VSS schemes for gray-scale images were considered. First, we discussed the contrast of VSS-GS schemes as an extension of BW-binary images in [36], [81], [117]. Then, we gave the modified polynomial representations of VSS-GS schemes [72]. The extended algebraic constructions can attain the optimal (n, n)-VSS-GS schemes in the sense of the minimum pixel expansions for given contrasts. We also constructed the basis polynomials of VSS schemes for color images with shades.

From Chapters 6 and 7, (k, n)-VSS schemes for any kind of secret images can easily be constructed based on the algebraic constructions. Furthermore, as it is shown in Section 6.4, VSS schemes can also be constructed for any general access structures.

Finally in Chapter 8, we proposed VSS schemes with general access structures that can encode plural color secret images with shades. The proposed VSS schemes include most of previous VSS schemes as special cases. Furthermore, the security conditions were defined in the exact way as decrypted images must not leak out any information of the other secret images, which is not satisfied in [35], [107]. We also proposed the construction method of VSS schemes that attain the security condition without degenerating the quality of decrypted images. We showed in Section 8.5, how the proposed VSS schemes have advantages compared with trivial schemes, which consists of several VSS schemes for individual secret images.

9.2 Future Works

In this thesis, we considered the general construction methods of VSS schemes. By the proposed methods, (k, n)-VSS schemes can be constructed systematically, although they may not be the optimal (k, n)-VSS schemes. But, in the construction of VSS schemes, we consider only the original cumulative maps, which is not efficient as shown in Chapter 4. Hence, by using the optimal multiple assignment maps in Chapter 4, it may be possible to construct more efficient

VSS schemes for general access structures. In such cases, the objective functions of integer programming problems may be different from the objective function appeared in Section 4.

In Part II, we only treat *perfect* VSS schemes. But, in order to attain higher quality of decrypted images, *ramp* VSS schemes must be studied, which can be defined similarly to the ramp SS schemes treated in Chapters 3 and 4. In the ramp VSS schemes, there exists a trade-off between the quality of decrypted images and the security. Kato [59] presented a kind of $(3, 2, 3)$-threshold VSS schemes which can decrypt a secret image from three shares although no information of the secret image is obtained from one share. In this case, if we have two shares, some parts of the secret image appears. But, in many cases, we can imagine the secret image correctly from the partially appeared image. Therefore, Kato's ramp VSS schemes is not secure in the sense of ramp VSS schemes. Furthermore, [59] did not give any definition of ramp VSS schemes formally. On the other hand, $(2, 2)$-VSS schemes with ID images such as gray-scale pictures are considered in [25], [78]. In their scheme, the security of a secret image is weakened to attain high quality of ID images and hence their method can also be considered as a kind of ramp VSS schemes with ID images. However, the ramp VSS schemes have not studied theoretically at all, and they are important VSS schemes for future works.

Recently, another definitions of VSS schemes are proposed in [45] and [111] for BW-binary images and color images with shades, respectively.

In [111], VSS schemes are designed under the assumption that in the case of BW-binary secret images, negative images obtained by reversing white and black pixels are equal to their positive images. The optimization of pixel expansion and contrast in such VSS schemes may be interesting problems.

As we pointed out in Remark 7.16, the meanvalue-color mixing (MCM) VSS schemes proposed in [45] can treat color images with shades, although they require large pixel expansion. Hence, the realization of the MCM-VSS schemes with smaller subpixels may also be an important future work.

Appendix A

Examples of Visual Secret Sharing Schemes

In this appendix, we give some examples of shares and decrypted images of VSS schemes treated in this thesis.[1]

A.1 Visual Secret Sharing Schemes for BW-binary Secret Images

Figures A.1–A.3 are the examples of shares for a $(2, 2)$-threshold VSS scheme with a BW-binary image. The basis matrices of shares V_1^{BW} and V_2^{BW} shown in Figures A.1 and A.2, respectively, are given by

$$B_1 = \begin{bmatrix} 01 \\ 10 \end{bmatrix} \text{ and } B_0 = \begin{bmatrix} 01 \\ 01 \end{bmatrix}, \tag{A.1}$$

which are obtained by the method proposed by Naor-Shamir [81]. Figure A.3 is the decrypted image obtained by stacking up V_1^{BW} and V_2^{BW}, and it holds that $\alpha = \frac{1}{2}$ and $m = 2$.

[1] These examples of VSS schemes are constructed by the software program provided by Prof. H. Koga.

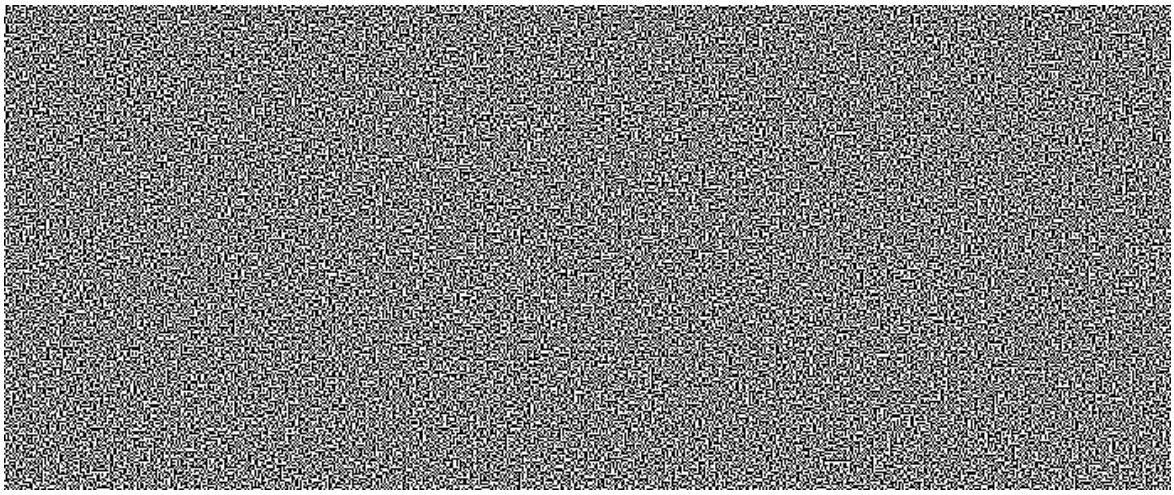


Figure A.1. The first share of a $(2, 2)$-threshold VSS scheme for a BW-binary image: V_1^{BW}

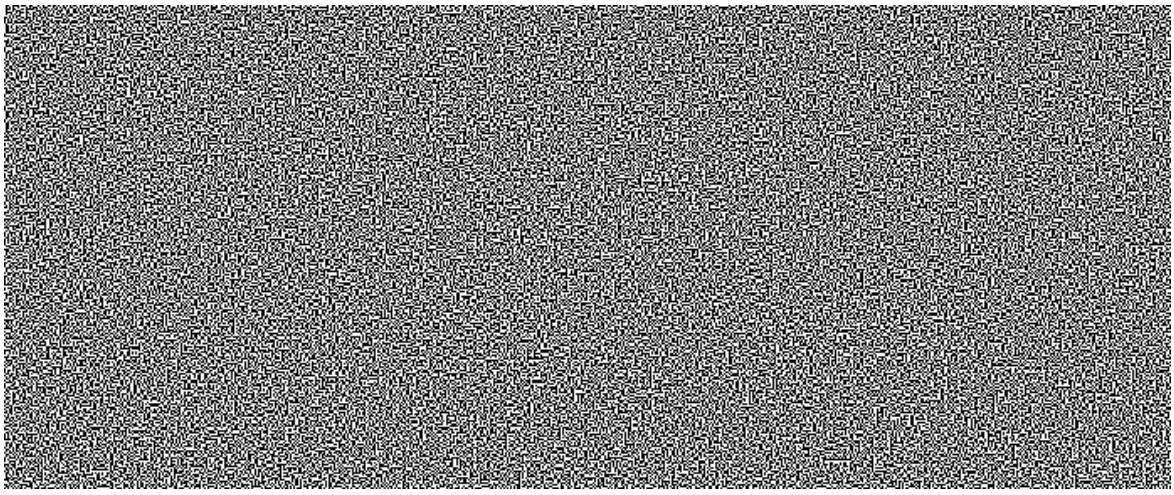


Figure A.2. The second share of a $(2, 2)$-threshold VSS scheme for a BW-binary image: V_2^{BW}

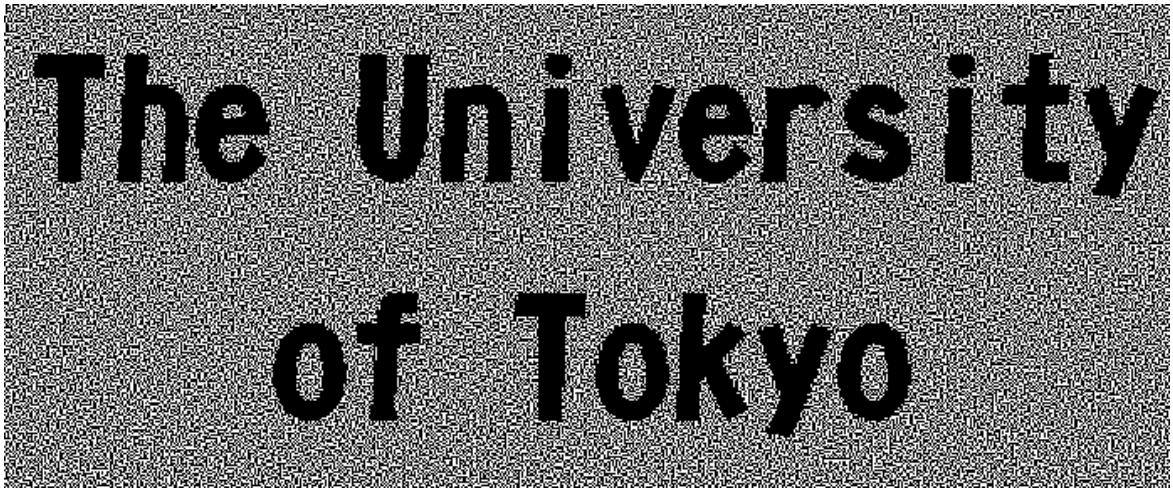


Figure A.3. The decrypted image obtained from V_1^{BW} and V_2^{BW}

A.2 Visual Secret Sharing Schemes for Color Images

In this section, we show three examples of VSS schemes for color images treated in [66], [67] and Chapter 6.

Figures A.4–A.6 are the shares and decrypted images of a $(2, 2)$-threshold VSS scheme with color set $\mathcal{D} = \{0, \mathsf{g}, \mathsf{b}\}$. The basis matrices are given by

$$B_0 = \begin{bmatrix} 01\mathsf{g}b1 \\ 0\mathsf{g}11\mathsf{b} \end{bmatrix}, \quad B_{\mathsf{b}} = \begin{bmatrix} \mathsf{b}1\mathsf{g}01 \\ \mathsf{bg}110 \end{bmatrix} \quad \text{and} \quad B_{\mathsf{g}} = \begin{bmatrix} \mathsf{g}10\mathsf{b}1 \\ \mathsf{g}011\mathsf{b} \end{bmatrix}, \tag{A.2}$$

which have contrast $\alpha = \frac{1}{5}$ and pixel expansion $m = 5$.

Next example is a $(2, 3)$-threshold VSS schemes with color set $\mathcal{D} = \{\mathsf{c}, \mathsf{g}, \mathsf{y}\}$. If we use basis matrices

$$B_{\mathsf{c}} = \begin{bmatrix} 01\mathsf{c}1\mathsf{c}011\mathsf{y}11\mathsf{y} \\ 101\mathsf{c}0\mathsf{c}1\mathsf{y}11\mathsf{y}1 \\ \mathsf{cc}0011\mathsf{y}11\mathsf{y}11 \end{bmatrix}, \quad B_{\mathsf{g}} = \begin{bmatrix} \mathsf{c}1\mathsf{y}1\mathsf{yc}110110 \\ 1\mathsf{c}1\mathsf{ycy}101101 \\ \mathsf{yycc}11011011 \end{bmatrix}, \quad \text{and} \quad B_{\mathsf{y}} = \begin{bmatrix} 01\mathsf{y}1\mathsf{y}011\mathsf{c}11\mathsf{c} \\ 101\mathsf{y}0\mathsf{y}1\mathsf{c}11\mathsf{c}1 \\ \mathsf{yy}0011\mathsf{c}11\mathsf{c}11 \end{bmatrix}, \tag{A.3}$$

then we can obtain shares V_1^{C2}, V_2^{C2}, and V_3^{C2} shown in Figures A.7–A.9, and it holds that $\alpha = \frac{1}{12}$, $m = 12$. The decrypted image from V_1^{C2} and V_2^{C2} is shown in Figure A.10. Note that the same decrypted images can be obtained from the other combinations of 2-out-of-3 shares.

The third example is a VSS scheme with color set $\mathcal{D} = \{\mathsf{c}, \mathsf{y}, \mathsf{g}\}$ for the access structure given by (6.116) and (6.117). If we use the following basis matrices given by (6.118)–(6.120), shares V_1^{C3}, V_2^{C3}, V_3^{C3}, and V_4^{C3} are obtained as shown in Figures A.11–A.14.

$$B_{\mathsf{c}} = \begin{bmatrix} \mathsf{c}00\mathsf{c}0011\mathsf{yy}0011\mathsf{yy}0011\mathsf{ccyy}10101\mathsf{c}1\mathsf{c} \\ 0\mathsf{cc}0\mathsf{ccyy}1111\mathsf{yy}1111\mathsf{gg}111111111111 \\ \mathsf{c}0\mathsf{cc}0\mathsf{c}111\mathsf{y}1\mathsf{y}111\mathsf{y}1\mathsf{y}11\mathsf{g}11\mathsf{g}11111111 \\ 0\mathsf{c}00\mathsf{c}0\mathsf{y}001\mathsf{y}1\mathsf{y}001\mathsf{y}1\mathsf{yc}1\mathsf{yc}10101\mathsf{c}1\mathsf{c}1 \end{bmatrix}, \tag{A.4}$$

$$B_{\mathsf{y}} = \begin{bmatrix} \mathsf{y}00\mathsf{y}0011\mathsf{cc}0011\mathsf{cc}0011\mathsf{yycc}10101\mathsf{y}1\mathsf{y} \\ 0\mathsf{yy}0\mathsf{yycc}1111\mathsf{cc}1111\mathsf{gg}111111111111 \\ \mathsf{y}0\mathsf{yy}0\mathsf{y}111\mathsf{c}1\mathsf{c}111\mathsf{c}1\mathsf{c}11\mathsf{g}11\mathsf{g}11111111 \\ 0\mathsf{y}00\mathsf{y}0\mathsf{c}001\mathsf{c}1\mathsf{c}001\mathsf{c}1\mathsf{cy}1\mathsf{cy}10101\mathsf{y}1\mathsf{y}1 \end{bmatrix}, \tag{A.5}$$

$$B_{\mathsf{g}} = \begin{bmatrix} 00\mathsf{yycc}11\mathsf{cc}0011\mathsf{yy}000010011\mathsf{c}1\mathsf{c}1\mathsf{y}1\mathsf{y} \\ \mathsf{ggccyycc}1111\mathsf{yy}111111011011111111 \\ \mathsf{cygycg}111\mathsf{c}1\mathsf{c}111\mathsf{y}1\mathsf{y}10110111111111 \\ \mathsf{yc}0\mathsf{cy}0\mathsf{c}001\mathsf{c}1\mathsf{y}001\mathsf{y}1010010\mathsf{c}1\mathsf{c}1\mathsf{y}1\mathsf{y}1 \end{bmatrix}. \tag{A.6}$$

Then, it holds that $\alpha = \frac{3}{16}$ and $m = 32$. From a qualified set $\{V_1^{C3}, V_2^{C3}\}$, we can obtain the decrypted image shown in Figure A.15 although no information can be decrypted from a forbidden set $\{V_1^{C3}, V_3^{C3}\}$ as shown in Figure A.16.

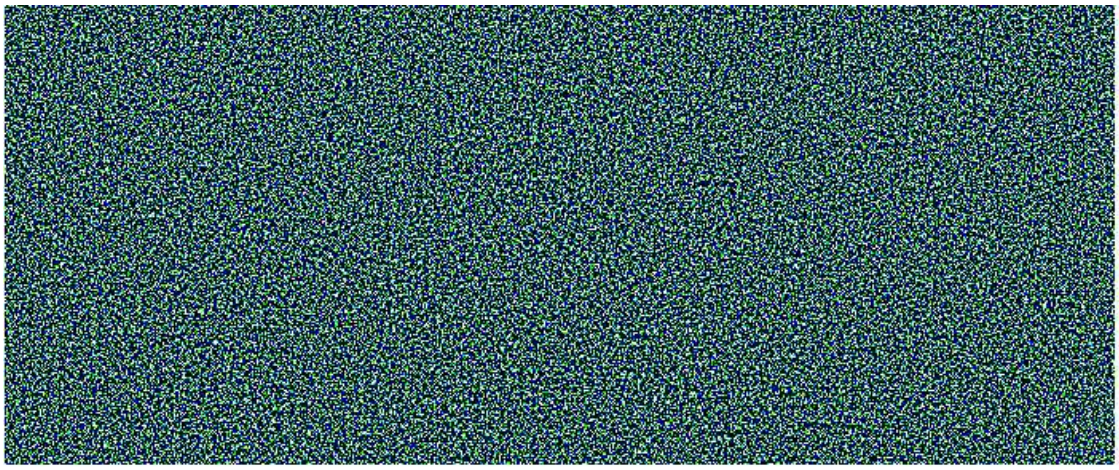


Figure A.4. The first share of a $(2, 2)$-threshold VSS scheme for a color image: V_1^{C1}

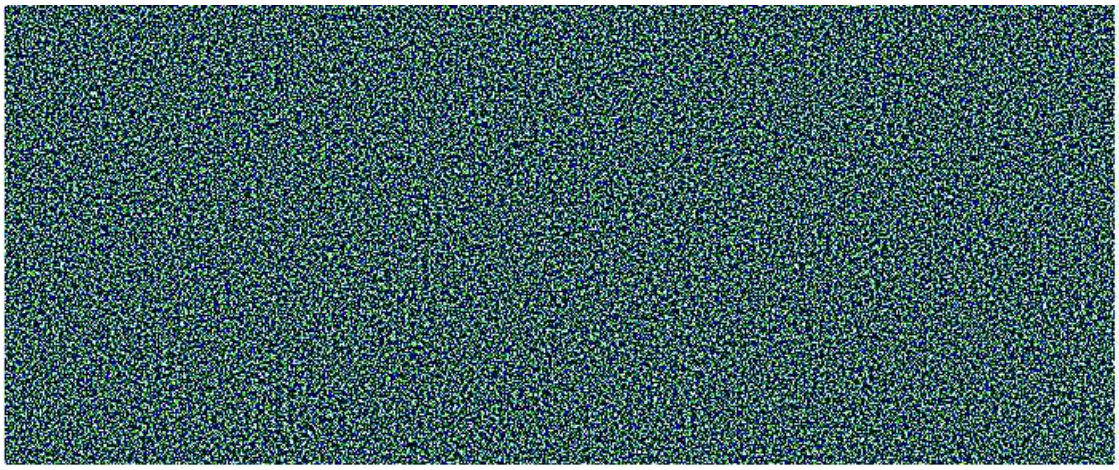


Figure A.5. The second share of a $(2, 2)$-threshold VSS scheme for a color image: V_2^{C1}

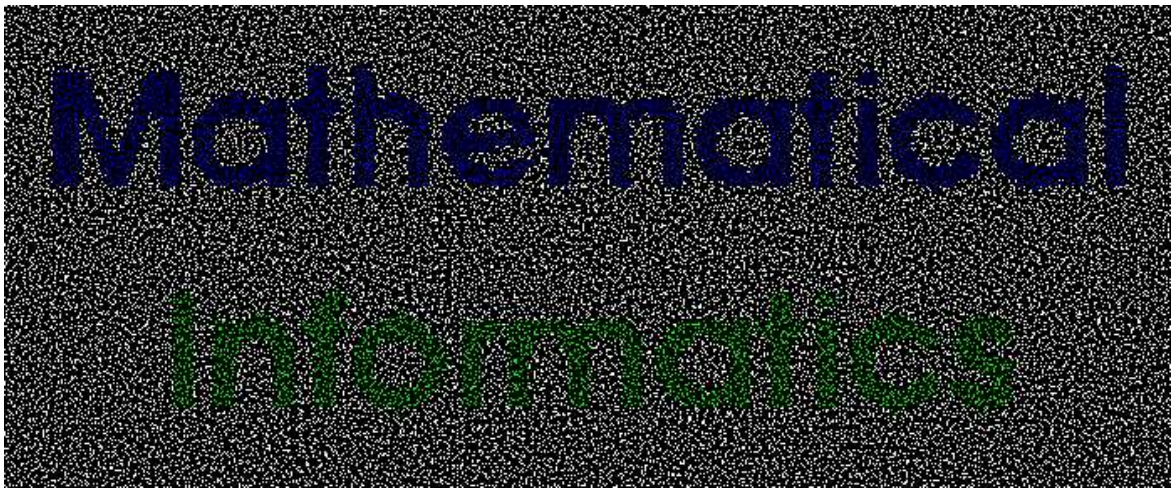


Figure A.6. The decrypted image obtained from V_1^{C1} and V_2^{C1}

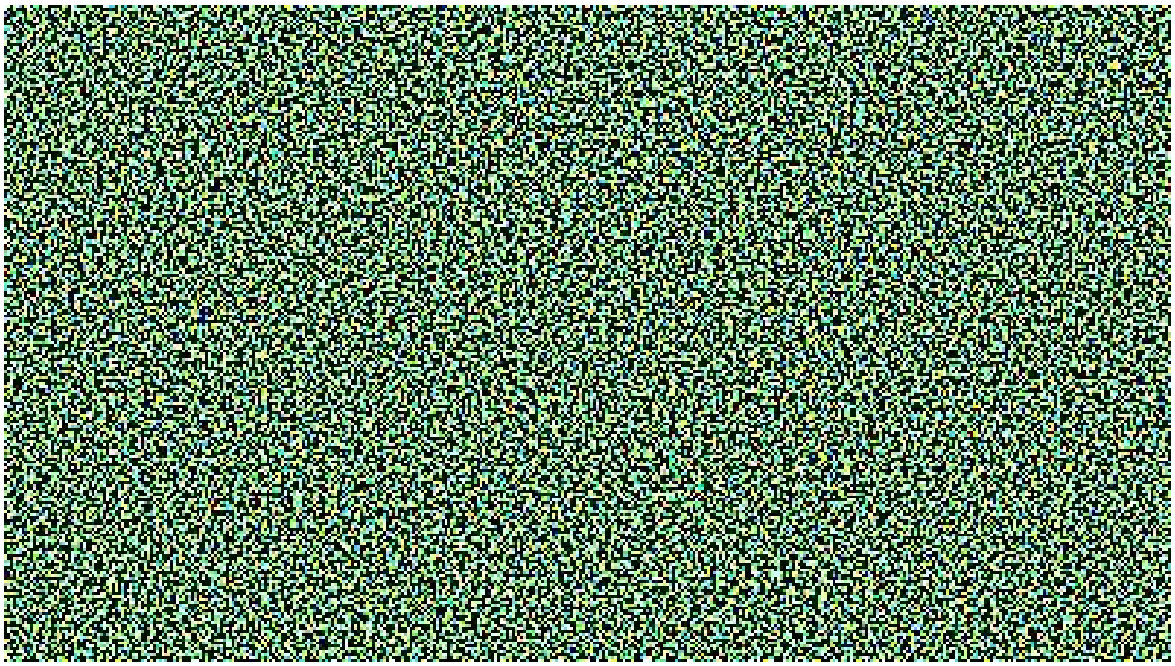


Figure A.7. The first share of a $(2, 3)$-threshold VSS scheme for a color image: V_1^{C2}

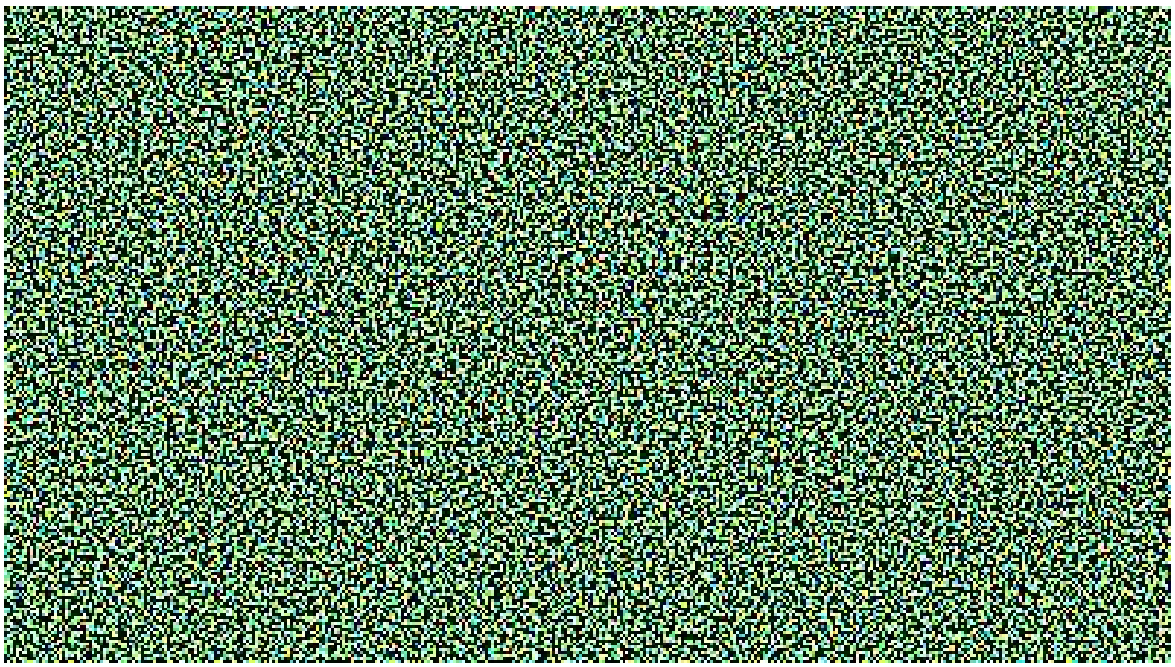


Figure A.8. The second share of a $(2, 3)$-threshold VSS scheme for a color image: V_2^{C2}

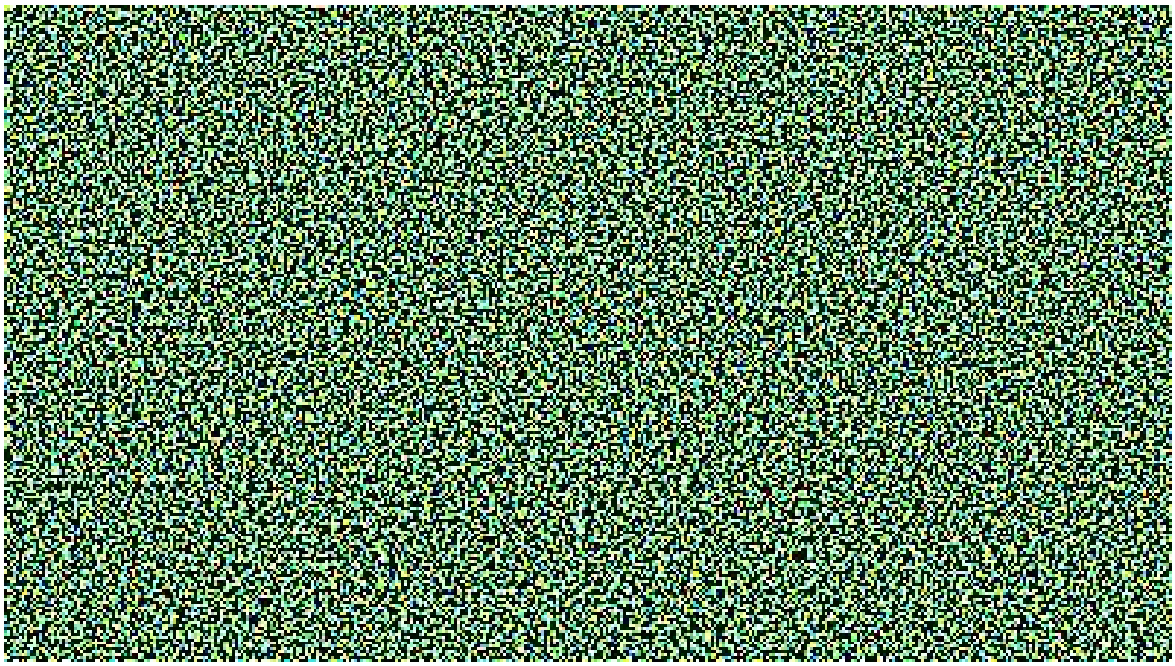


Figure A.9. The third share of a $(2, 3)$-threshold VSS scheme for a color image: V_3^{C2}

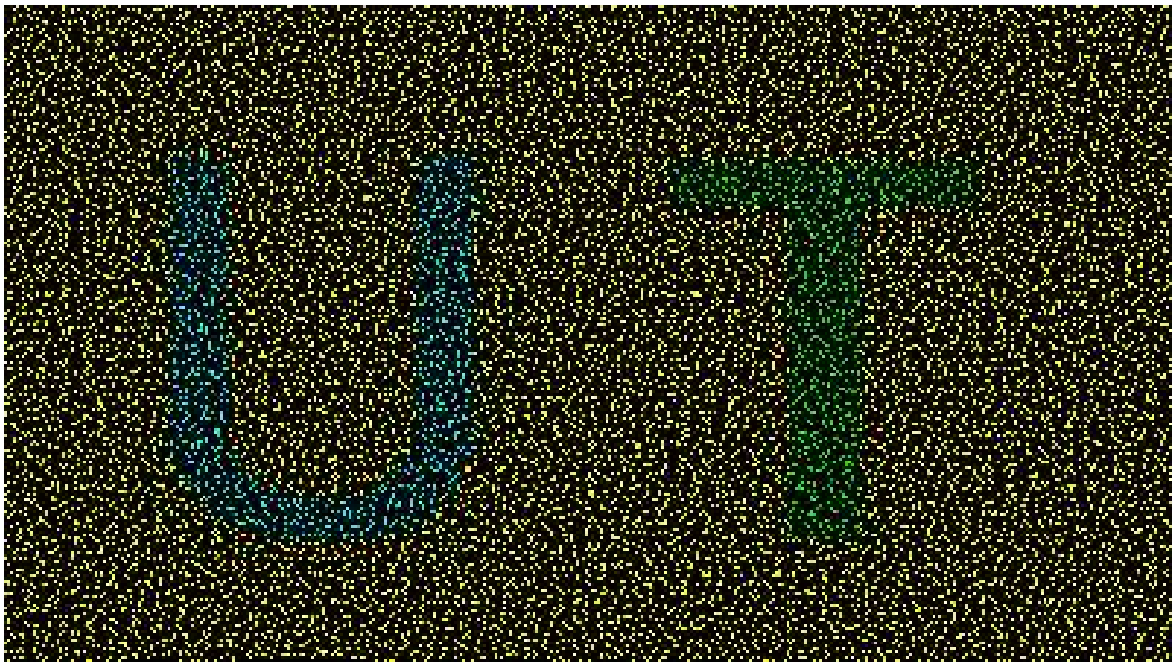


Figure A.10 The decrypted image obtained from V_1^{C2} and V_2^{C2}. ("UT" is the abbreviation of Univ. of Tokyo.)

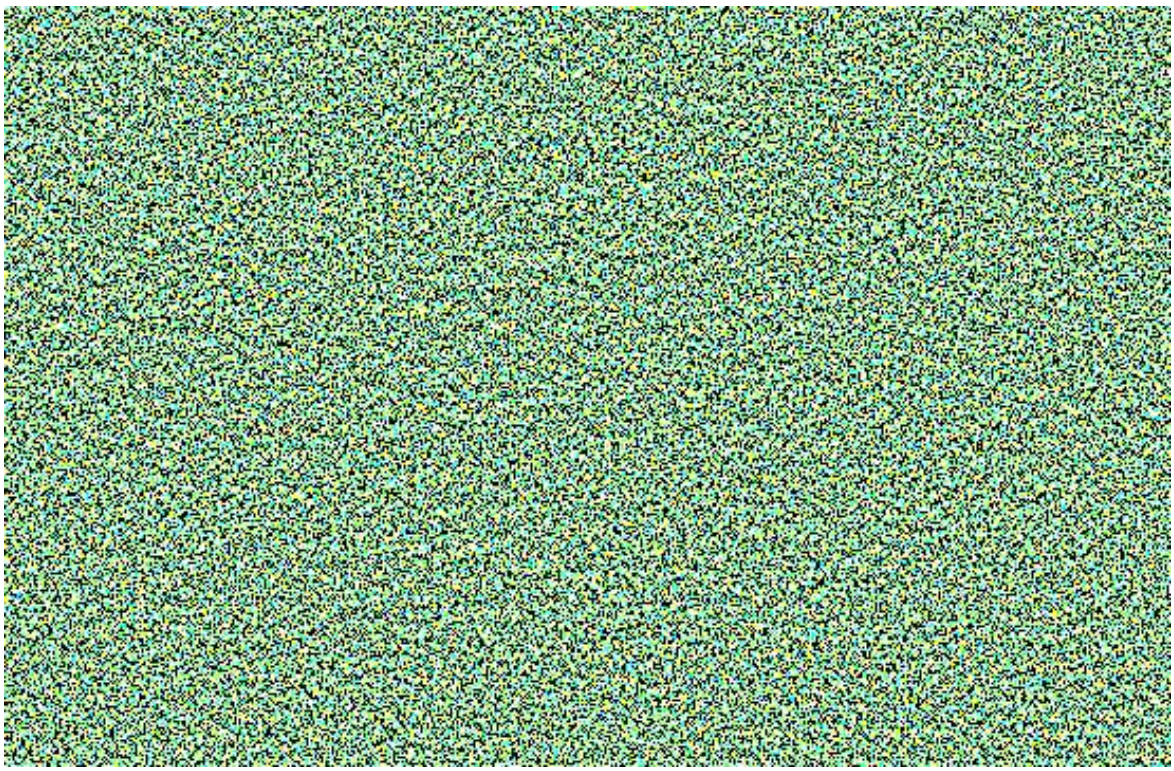


Figure A.11 The first share of a VSS scheme for a color image with the access structure given by (6.116) and (6.117): V_1^{C3}

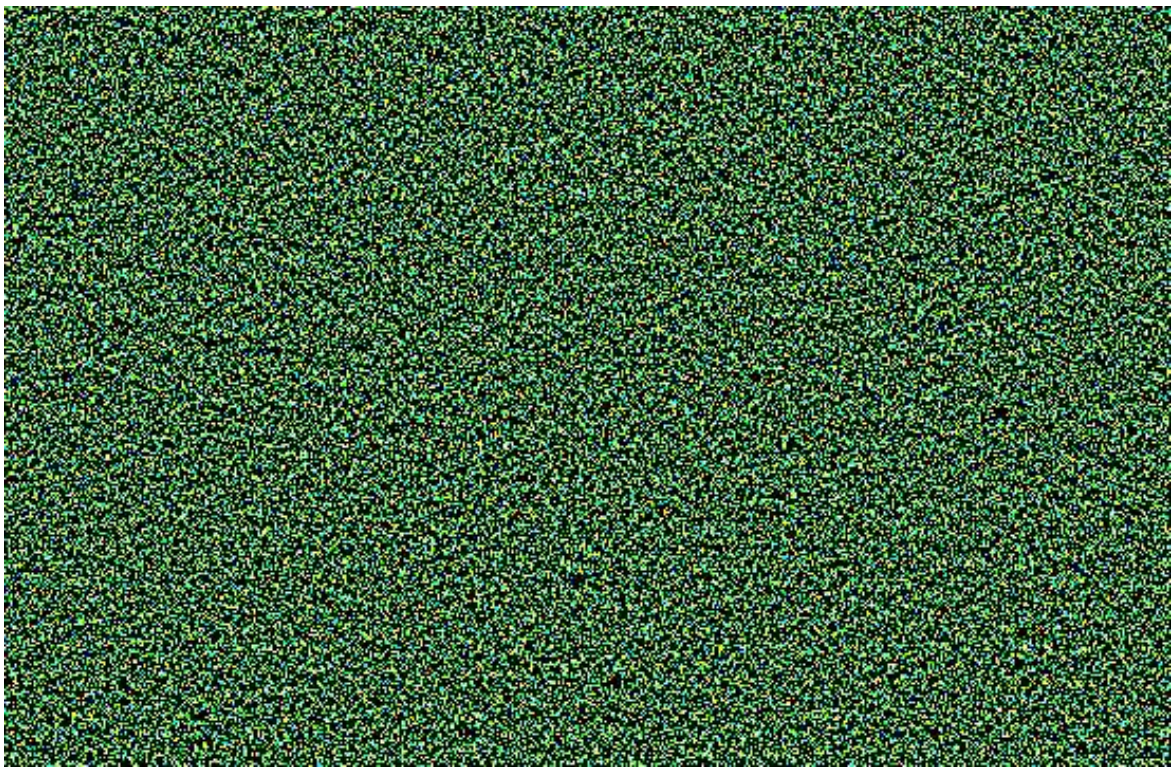


Figure A.12 The second share of a VSS scheme for a color image with the access structure given by (6.116) and (6.117): V_2^{C3}

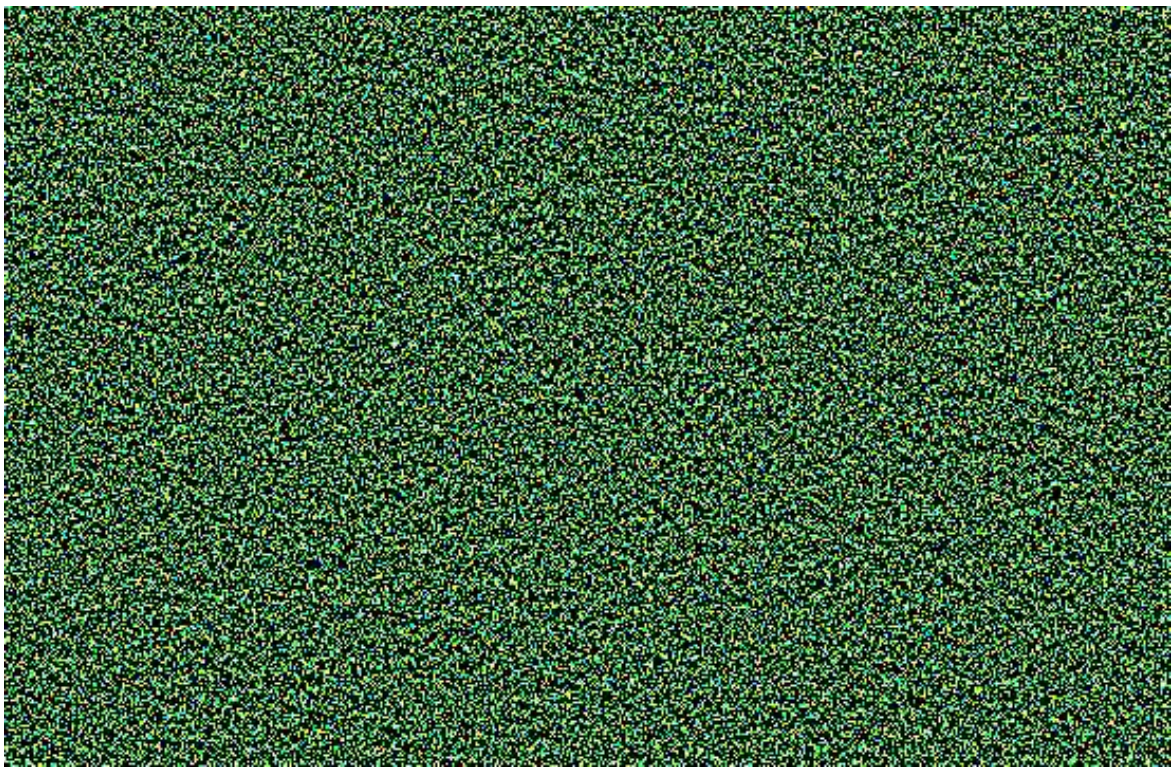


Figure A.13 The third share of a VSS scheme for a color image with the access structure given by (6.116) and (6.117): V_3^{C3}

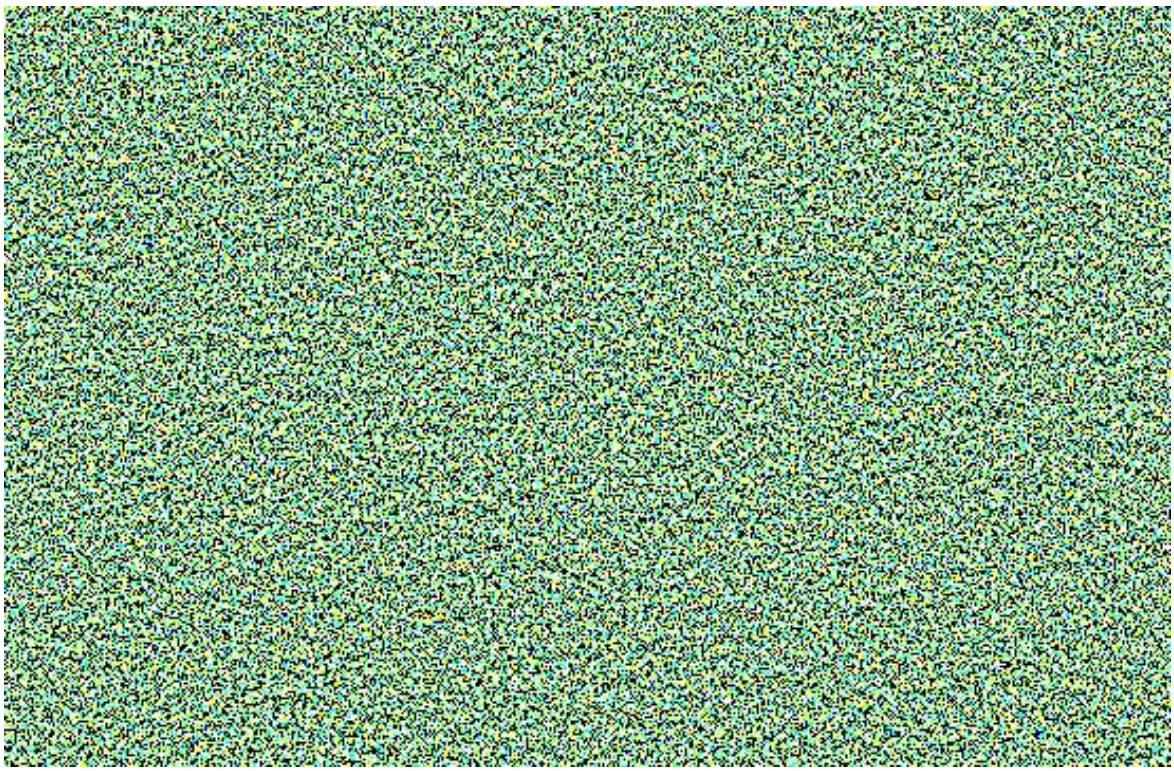


Figure A.14 The fourth share of a VSS scheme for a color image with the access structure given by (6.116) and (6.117): V_4^{C3}

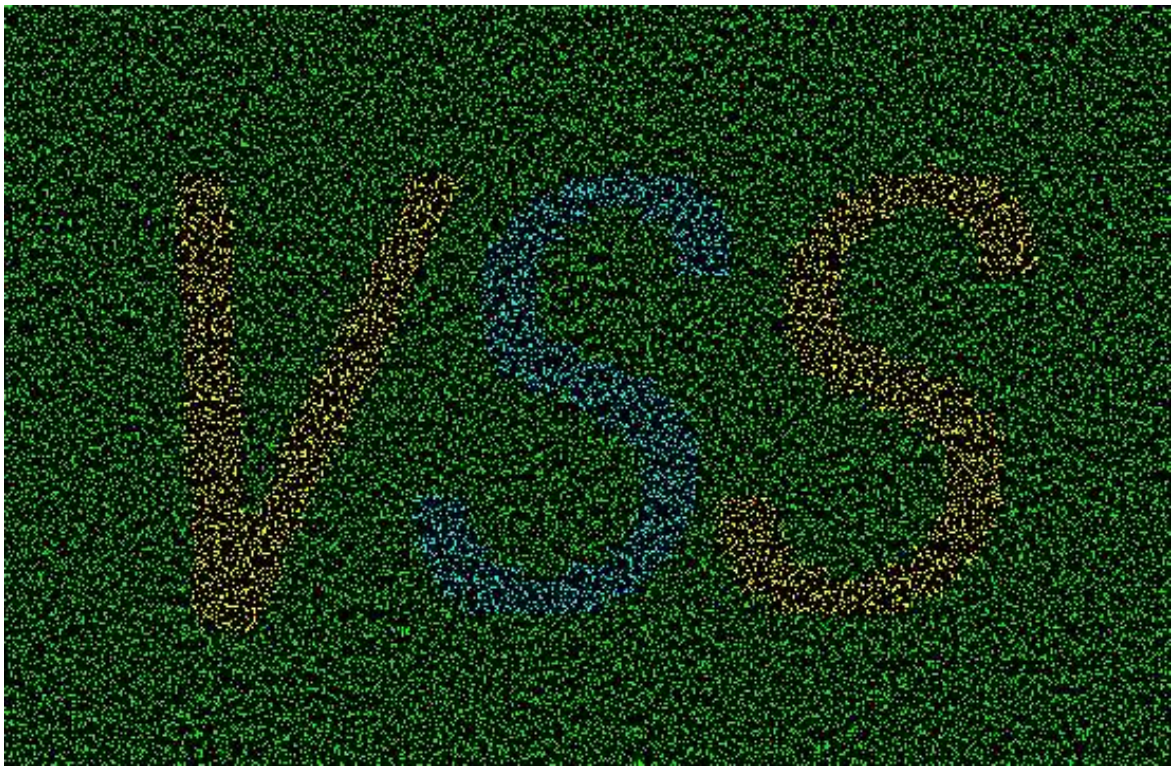


Figure A.15. The decrypted image obtained from V_1^{C3} and V_2^{C3}

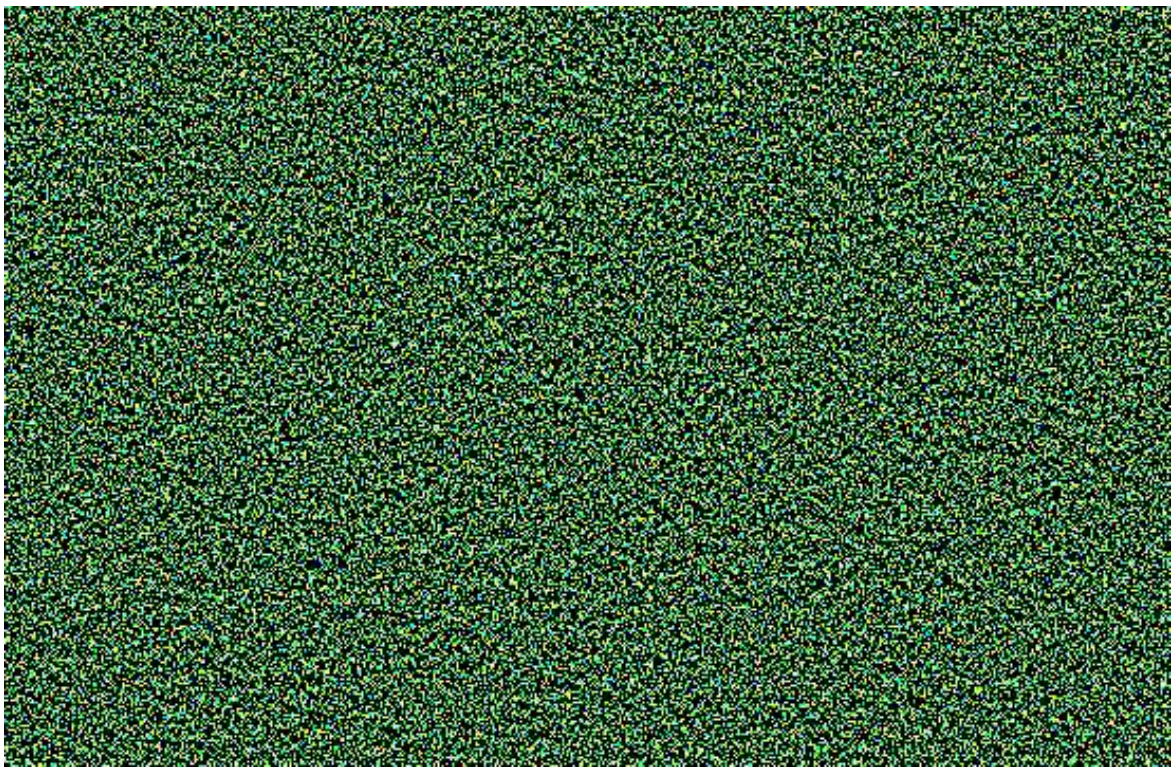


Figure A.16 The image obtained from V_1^{C3} and V_3^{C3} which has no information about the secret image

A.3 Visual Secret Sharing Schemes for Gray-scale Images

In this thesis, we treated the VSS-GS-L schemes in Chapter 8. Here, we show an example of a VSS-GS-8 scheme, which has the following basis matrices. It holds that $m = 15$, $\beta = \frac{1}{15}$, and $\alpha_{(\ell)} = \frac{2}{15}$ for $\ell = 2, 3, \ldots, 8$.

$$B_{(1)} = \begin{bmatrix} 011111110000000 \\ 000000001111111 \end{bmatrix}, \quad B_{(2)} = \begin{bmatrix} 001111110000001 \\ 000000001111111 \end{bmatrix}, \tag{A.7}$$

$$B_{(3)} = \begin{bmatrix} 000111110000011 \\ 000000001111111 \end{bmatrix}, \quad B_{(4)} = \begin{bmatrix} 000011110000111 \\ 000000001111111 \end{bmatrix}, \tag{A.8}$$

$$B_{(5)} = \begin{bmatrix} 000001110001111 \\ 000000001111111 \end{bmatrix}, \quad B_{(6)} = \begin{bmatrix} 000000110011111 \\ 000000001111111 \end{bmatrix}, \tag{A.9}$$

$$B_{(7)} = \begin{bmatrix} 000000010111111 \\ 000000001111111 \end{bmatrix}, \quad B_{(8)} = \begin{bmatrix} 000000001111111 \\ 000000001111111 \end{bmatrix}. \tag{A.10}$$

Figures A.17–A.19 are the two shares and decrypted image of this example.

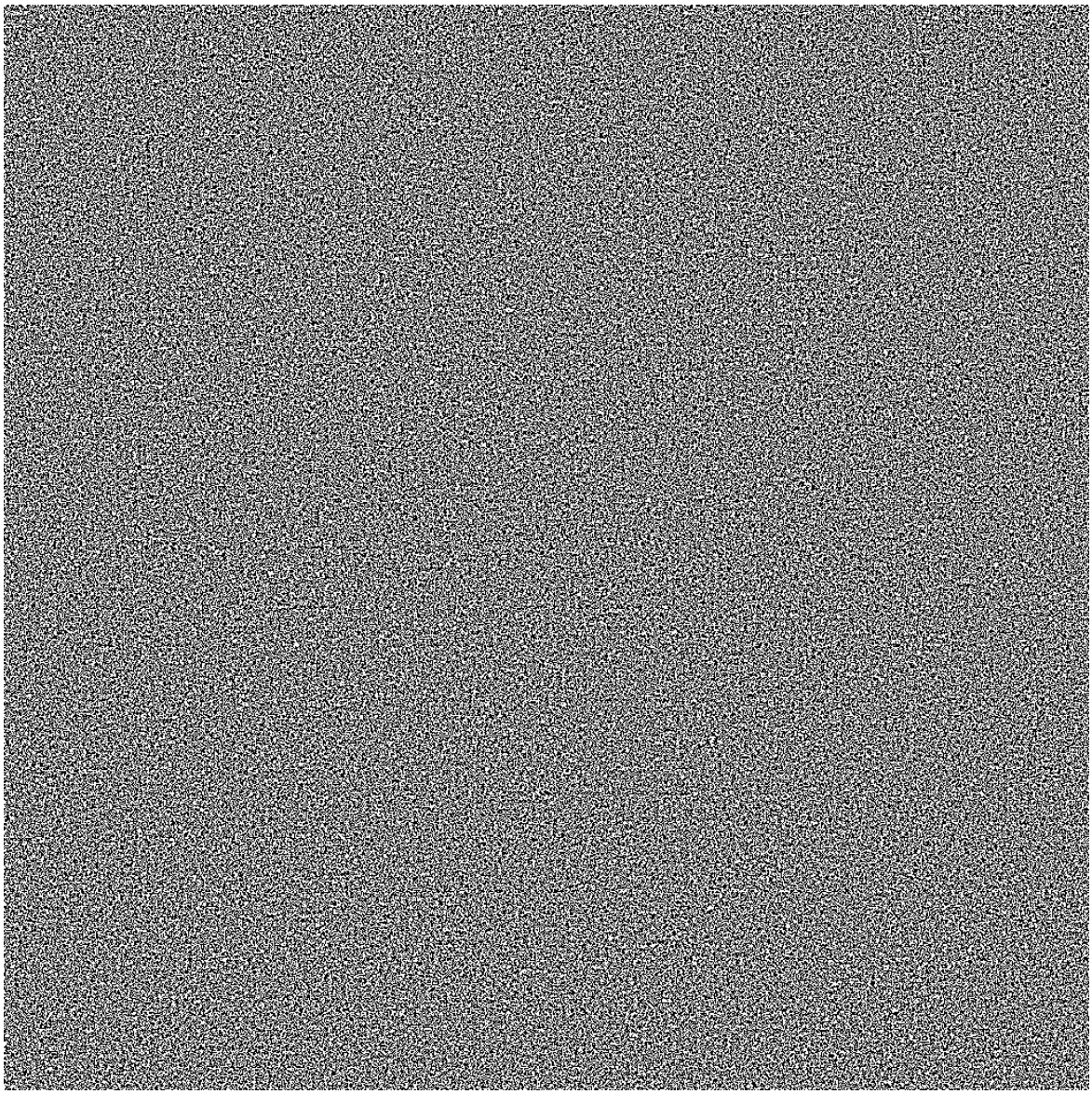


Figure A.17. The first share of a $(2, 2)$-threshold VSS-GS-8 scheme: V_1^{GS}

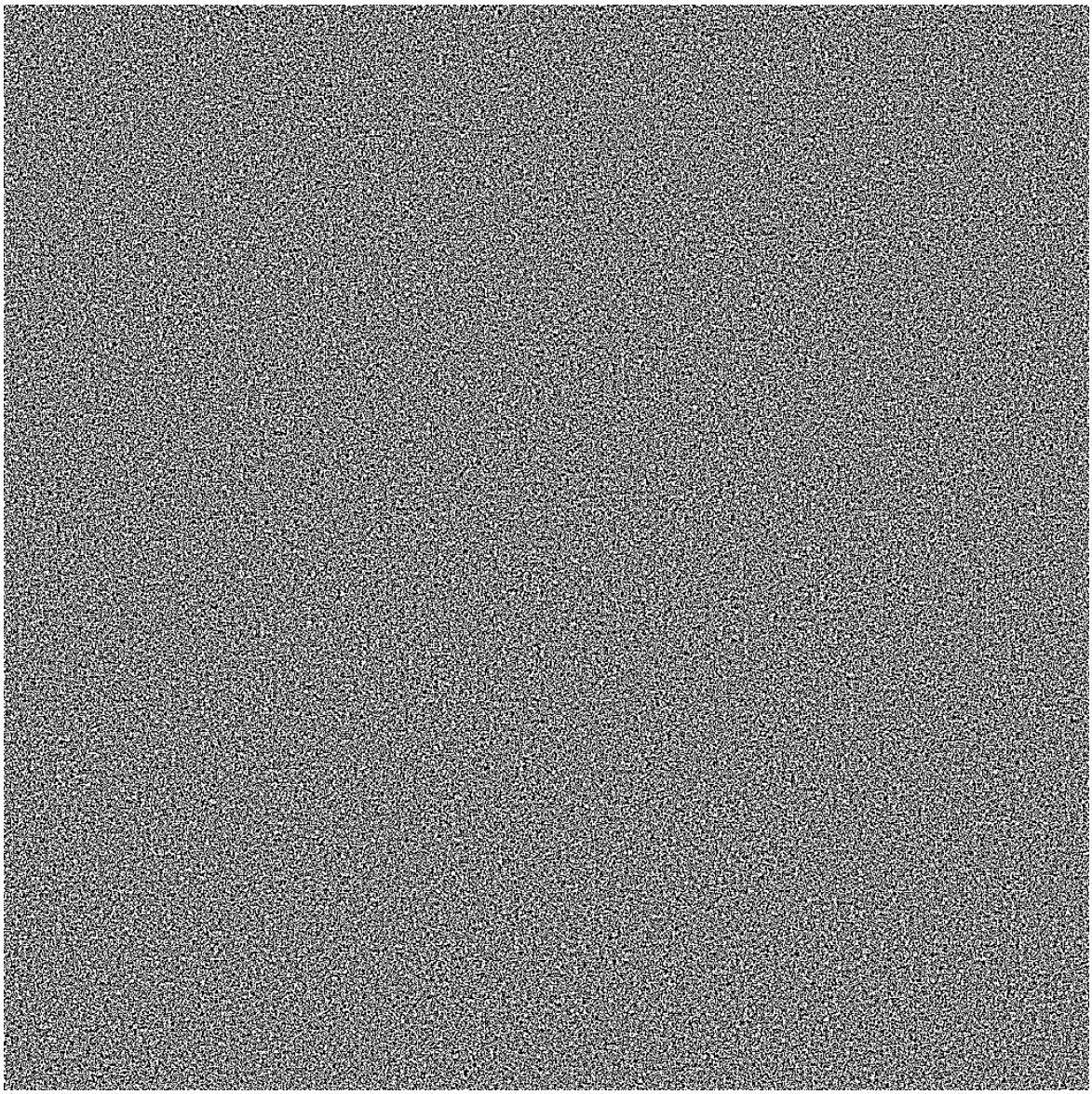


Figure A.18. The second share of a $(2, 2)$-threshold VSS-GS-8 scheme: V_2^{GS}

Figure A.19. The decrypted image obtained from V_1^{GS} and V_2^{GS}

A.4 Visual Secret Sharing Scheme with Plural Secret Images

In this section, we present two examples of VSS-q-PI schemes treated in Chapter 9.

First, we show an example of a $(2,2)$-threshold VSS scheme with ID images which can be considered as a special case of VSS-3-PI schemes. Let $DI^{\langle\langle 1\rangle\rangle}$ and $DI^{\langle\langle 2\rangle\rangle}$ be the ID images for each share V_1^{ID} V_2^{ID} with color sets $\mathcal{D}^{\langle\langle 1\rangle\rangle} = \{0, \mathsf{c}\}$ and $\mathcal{D}^{\langle\langle 2\rangle\rangle} = \{0, \mathsf{g}\}$, respectively, while let $DI^{\langle\langle 3\rangle\rangle}$ be the decrypted images with color set $\mathcal{D}^{\langle\langle 3\rangle\rangle} = \{\mathsf{b}, \mathsf{y}\}$. In this case, the color matrix is represented as follows.

$$\boldsymbol{D}_{ID} = \begin{bmatrix} 0000\mathsf{cccc} \\ 00\mathsf{gg}00\mathsf{gg} \\ \mathsf{bybybyyb} \end{bmatrix} \stackrel{\text{def}}{=} [\, \boldsymbol{c}_{ID}^1\, \boldsymbol{c}_{ID}^2\, \boldsymbol{c}_{ID}^3\, \boldsymbol{c}_{ID}^4\, \boldsymbol{c}_{ID}^5\, \boldsymbol{c}_{ID}^6\, \boldsymbol{c}_{ID}^7\, \boldsymbol{c}_{ID}^8\,], \tag{A.11}$$

Then, the following bases matrices B_{ID}^j, $j = 1, 2, \ldots, 8$, corresponding to each column vector $\boldsymbol{c}_{ID}^j$ can be constructed according to Ishihara-Koga [43].

$$B_{ID}^1 = \begin{bmatrix} \mathsf{b1y01} \\ \mathsf{by110} \end{bmatrix},\ B_{ID}^2 = \begin{bmatrix} \mathsf{y1b01} \\ \mathsf{yb110} \end{bmatrix},\ B_{ID}^3 = \begin{bmatrix} \mathsf{b1y01} \\ \mathsf{by11g} \end{bmatrix},\ B_{ID}^4 = \begin{bmatrix} \mathsf{y1b01} \\ \mathsf{yb11g} \end{bmatrix}, \tag{A.12}$$

$$B_{ID}^5 = \begin{bmatrix} \mathsf{b1yc1} \\ \mathsf{by110} \end{bmatrix},\ B_{ID}^6 = \begin{bmatrix} \mathsf{y1bc1} \\ \mathsf{yb110} \end{bmatrix},\ B_{ID}^7 = \begin{bmatrix} \mathsf{b1yc1} \\ \mathsf{by11g} \end{bmatrix},\ B_{ID}^8 = \begin{bmatrix} \mathsf{y1bc1} \\ \mathsf{yb11g} \end{bmatrix}. \tag{A.13}$$

Figures A.20–A.22 are two shares $V_1^{ID} = DI^{\langle\langle 1\rangle\rangle}$, $V_2^{ID} = DI^{\langle\langle 2\rangle\rangle}$ and decrypted image. In this VSS scheme, note that both ID images, $DI^{\langle\langle 1\rangle\rangle}$ and $DI^{\langle\langle 2\rangle\rangle}$ do not satisfy the condition (i) in Definition 8.4.

Next, let us consider a VSS-3-PI scheme such that three secret images can be decrypted from arbitrary 2-out-of-3 shares, V_1^{PL}, V_2^{PL}, and V_3^{PL}. Assume that three decrypted images $ID^{\langle\langle 1\rangle\rangle}$, $ID^{\langle\langle 2\rangle\rangle}$, and $ID^{\langle\langle 3\rangle\rangle}$ have color sets $\mathcal{D}^{\langle\langle 1\rangle\rangle} = \{\mathsf{r}, \mathsf{y}\}$, $\mathcal{D}^{\langle\langle 2\rangle\rangle} = \{\mathsf{g}, \mathsf{y}\}$, and $\mathcal{D}^{\langle\langle 3\rangle\rangle} = \{\mathsf{b}, \mathsf{y}\}$, and can be decrypted from share set $\{V_1^{PL}, V_2^{PL}\}$, $\{V_2^{PL}, V_3^{PL}\}$, and $\{V_1^{PL}, V_3^{PL}\}$, respectively. Then, the color matrix is represented as follows.

$$\boldsymbol{D}^{PL} = \begin{bmatrix} \mathsf{yyyyrrrr} \\ \mathsf{yyggyygg} \\ \mathsf{bybybyby} \end{bmatrix} \stackrel{\text{def}}{=} [\, \boldsymbol{c}_{PL}^1\, \boldsymbol{c}_{PL}^2\, \boldsymbol{c}_{PL}^3\, \boldsymbol{c}_{PL}^4\, \boldsymbol{c}_{PL}^5\, \boldsymbol{c}_{PL}^6\, \boldsymbol{c}_{PL}^7\, \boldsymbol{c}_{PL}^8\,]. \tag{A.14}$$

Then, we have the following basis matrices based on the method proposed in Chapter 9.

$$B_{PL}^1 = \begin{bmatrix} \mathsf{yym\,1\,1111b1y} \\ \mathsf{yy\,1\,myyc1111} \\ \mathsf{111\ 1yy1cby1} \end{bmatrix},\ B_{PL}^2 = \begin{bmatrix} \mathsf{yym\,1\,1111y1b} \\ \mathsf{yy\,1\,myyc1111} \\ \mathsf{111\ 1yy1cyb1} \end{bmatrix}, \tag{A.15}$$

$$B_{PL}^3 = \begin{bmatrix} \mathsf{yym\,1\,1111b1y} \\ \mathsf{yy\,1\,mcyy1111} \\ \mathsf{111\ 1yc1yby1} \end{bmatrix},\ B_{PL}^4 = \begin{bmatrix} \mathsf{yym\,1\,1111y1b} \\ \mathsf{yy\,1\,mcyy1111} \\ \mathsf{111\ 1yc1yyb1} \end{bmatrix}, \tag{A.16}$$

$$B_{PL}^5 = \begin{bmatrix} \mathsf{m\,y\,y11111b1y} \\ \mathsf{\ y\,m1yyyc1111} \\ \mathsf{1\ 1\,11yy1cby1} \end{bmatrix},\ B_{PL}^6 = \begin{bmatrix} \mathsf{m\,y\,y11111y1b} \\ \mathsf{\ y\,m1yyyc1111} \\ \mathsf{1\ 1\,11yy1cyb1} \end{bmatrix}, \tag{A.17}$$

$$B_{PL}^{7} = \begin{bmatrix} \mathsf{m\,y\,y11111b1y} \\ \mathsf{y\,m1ycyy1111} \\ \mathsf{1\;1\,11yc1yby1} \end{bmatrix}, \quad B_{PL}^{8} = \begin{bmatrix} \mathsf{m\,y\,y11111y1b} \\ \mathsf{y\,m1ycyy1111} \\ \mathsf{1\;1\,11yc1yyb1} \end{bmatrix}. \tag{A.18}$$

Figures A.23–A.25 are the shares of this example, and three decrypted images are shown in Figures A.26-A.28. All the decrypted images have contrast $\alpha = \frac{2}{11}$ and pixel expansion $m = 11$.

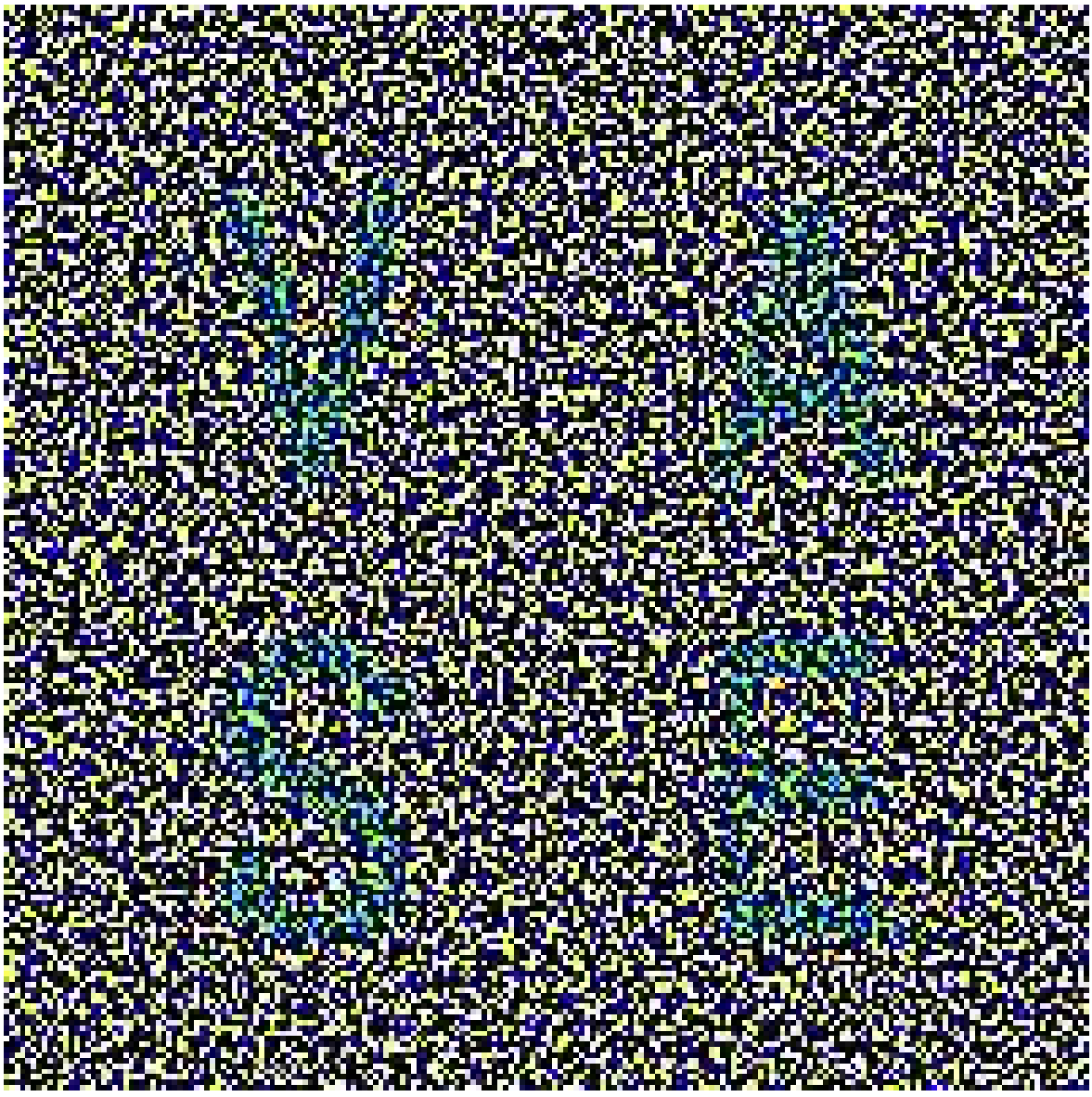


Figure A.20 The first share of a $(2, 2)$-threshold VSS scheme with ID images: V_1^{ID} (The first ID is VASE.)

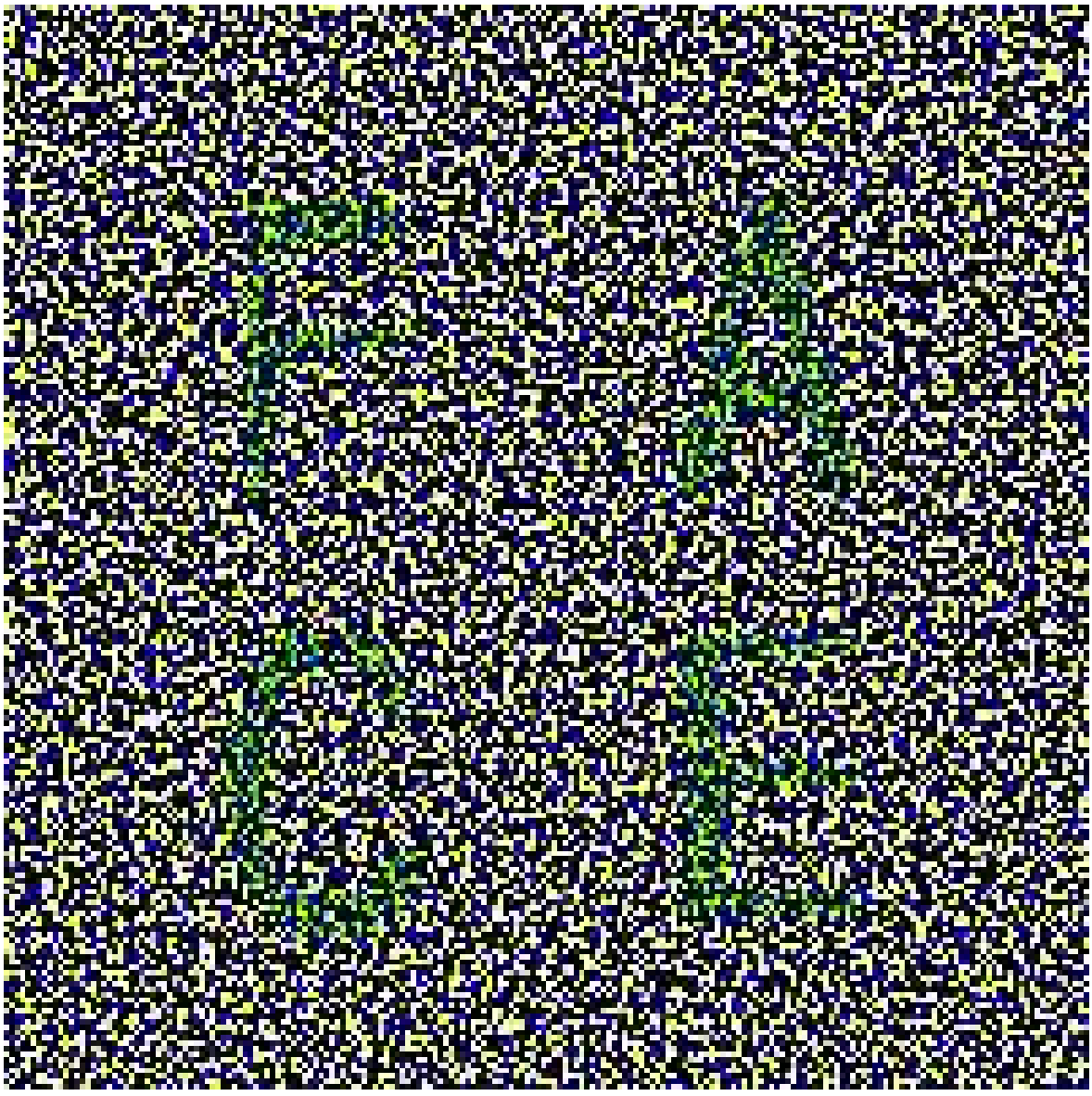


Figure A.21 The second share of a $(2, 2)$-threshold VSS scheme with ID images: V_2^{ID} (The first ID is FACE.)

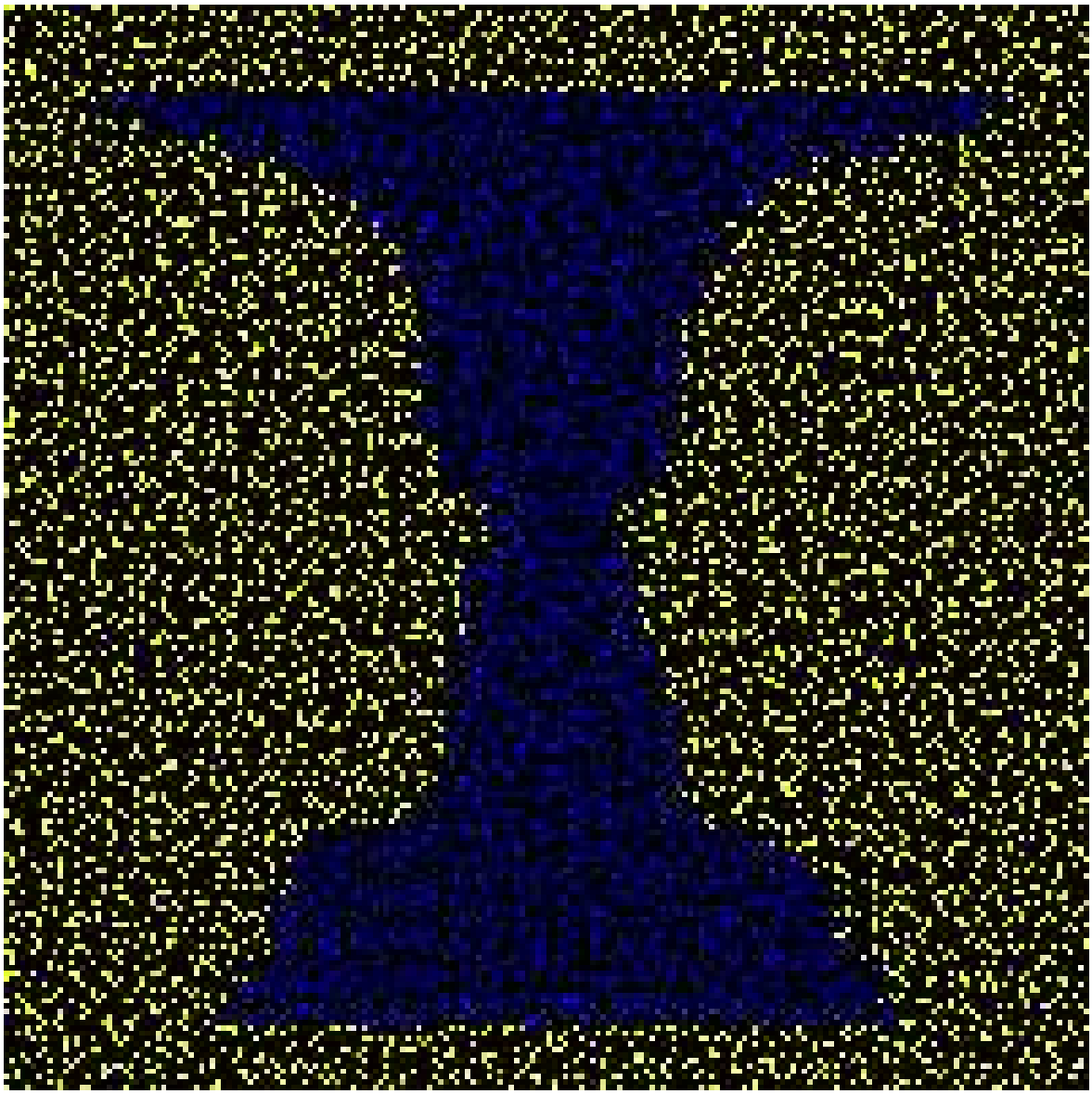


Figure A.22. The decrypted image obtained from V_1^{ID} and V_2^{ID}

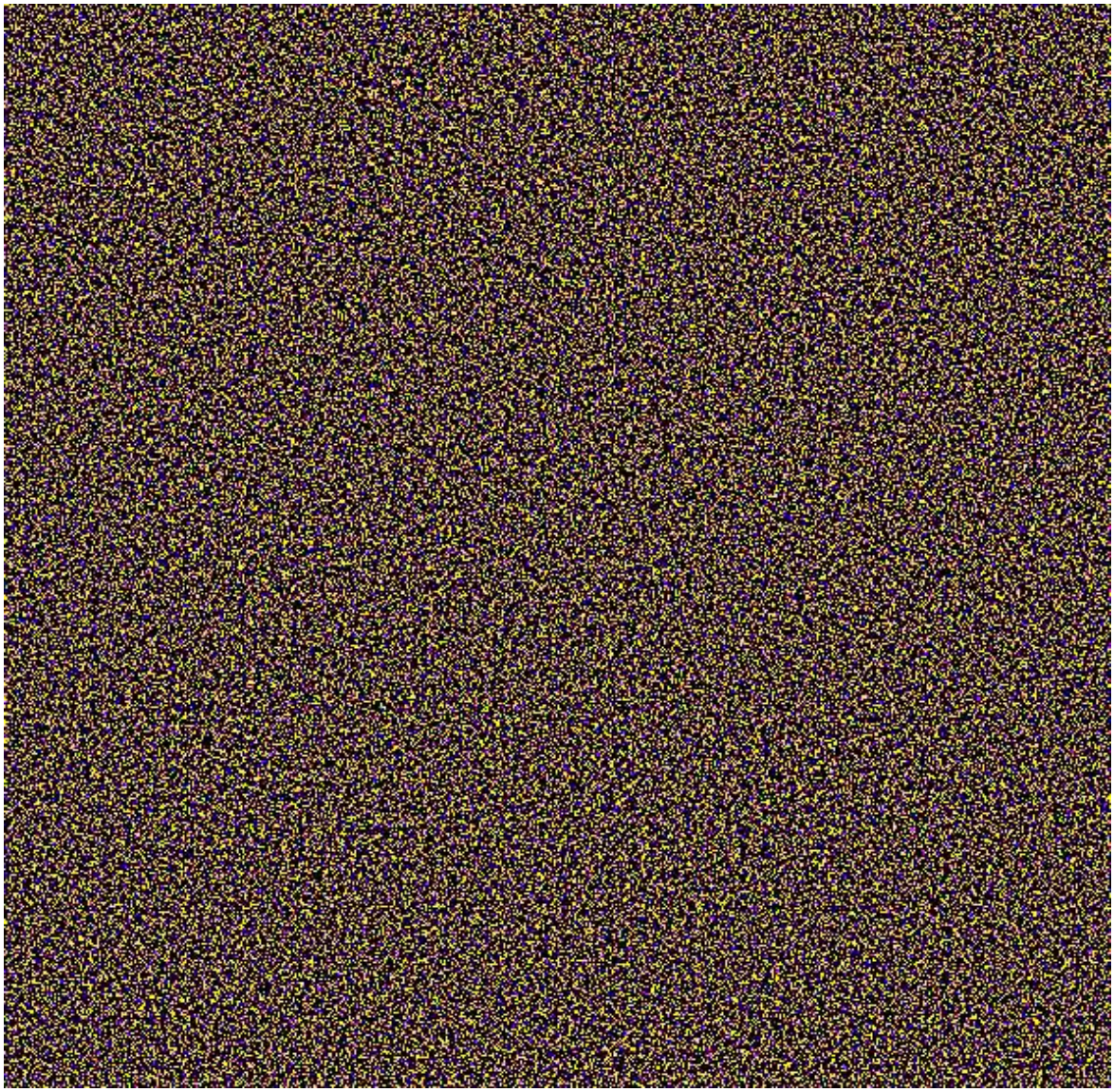


Figure A.23. The first share of a VSS-3-PI scheme: V_1^{PL}

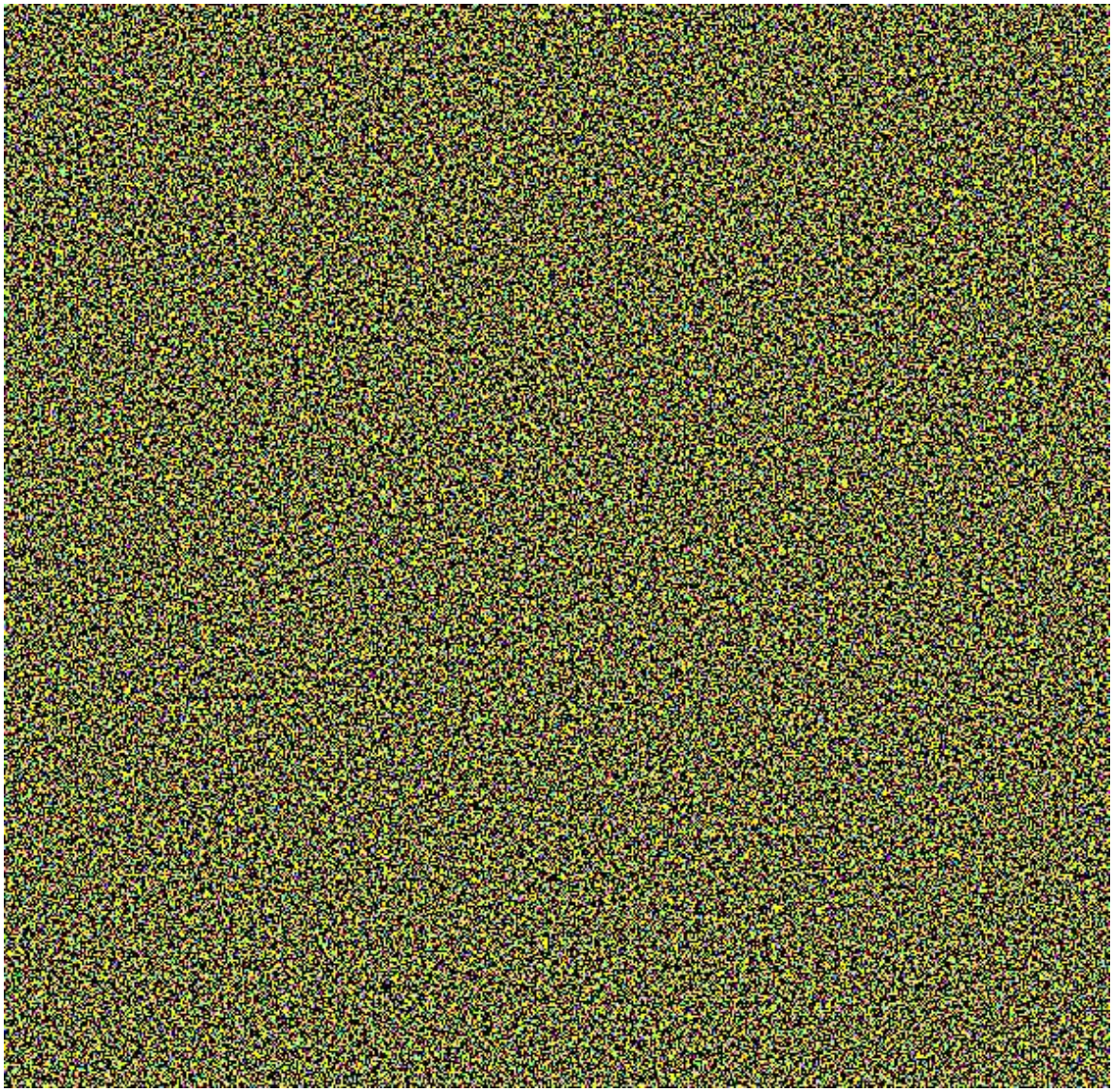


Figure A.24. The second share of a VSS-3-PI scheme: V_2^{PL}

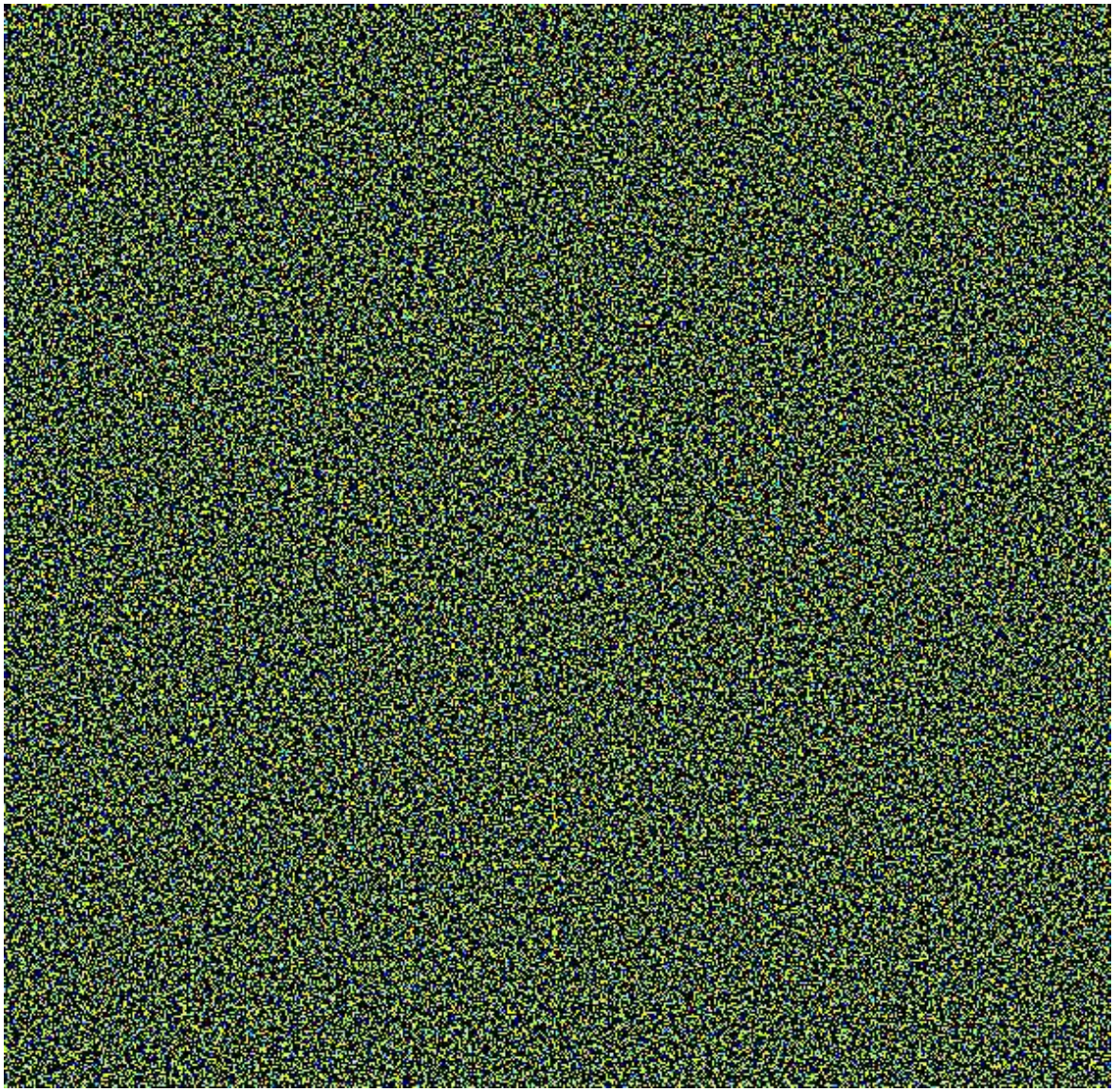


Figure A.25. The third share of a VSS-3-PI scheme: V_3^{PL}

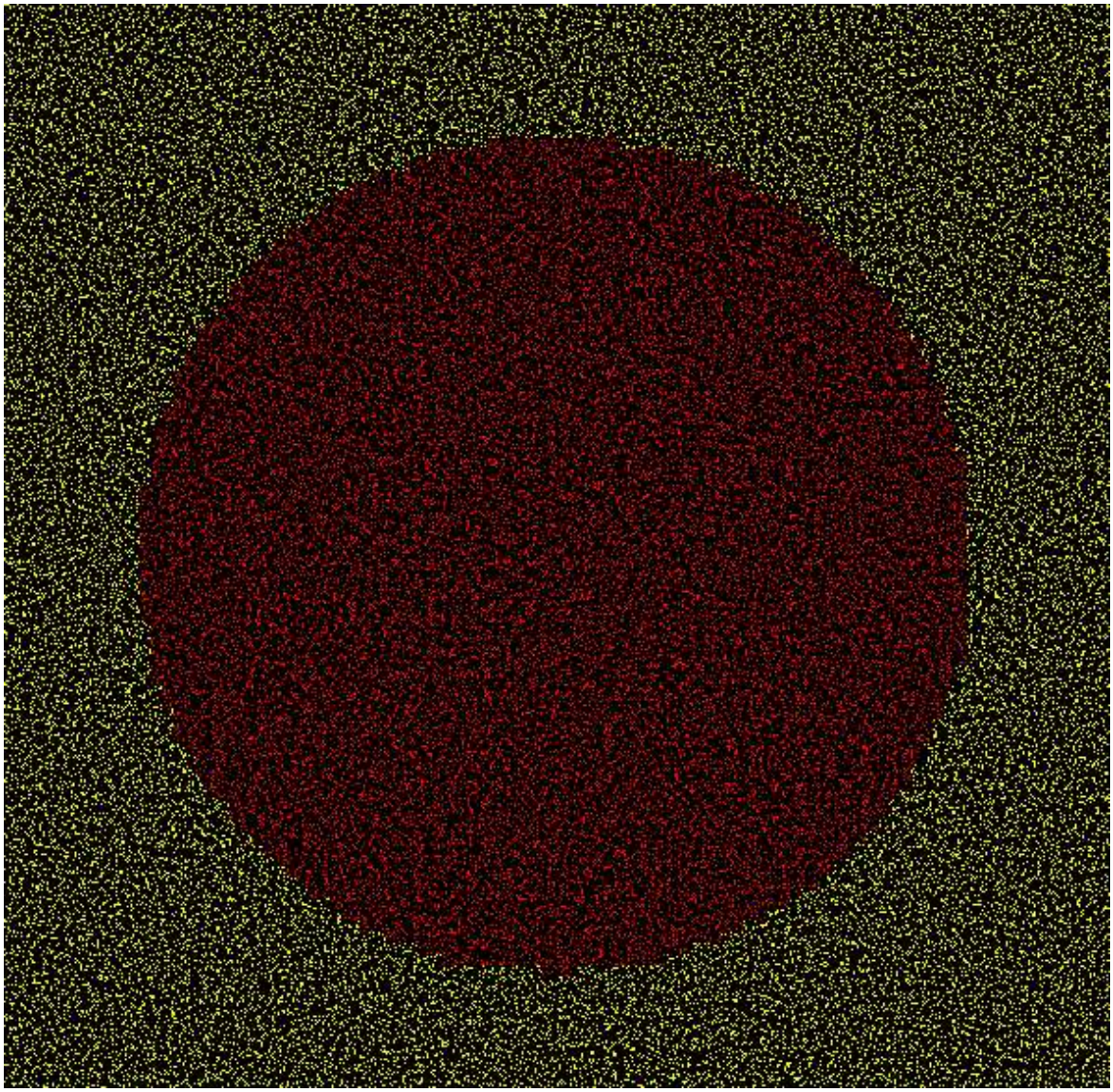


Figure A.26. The decrypted image obtained from V_1^{PL} and V_2^{PL}

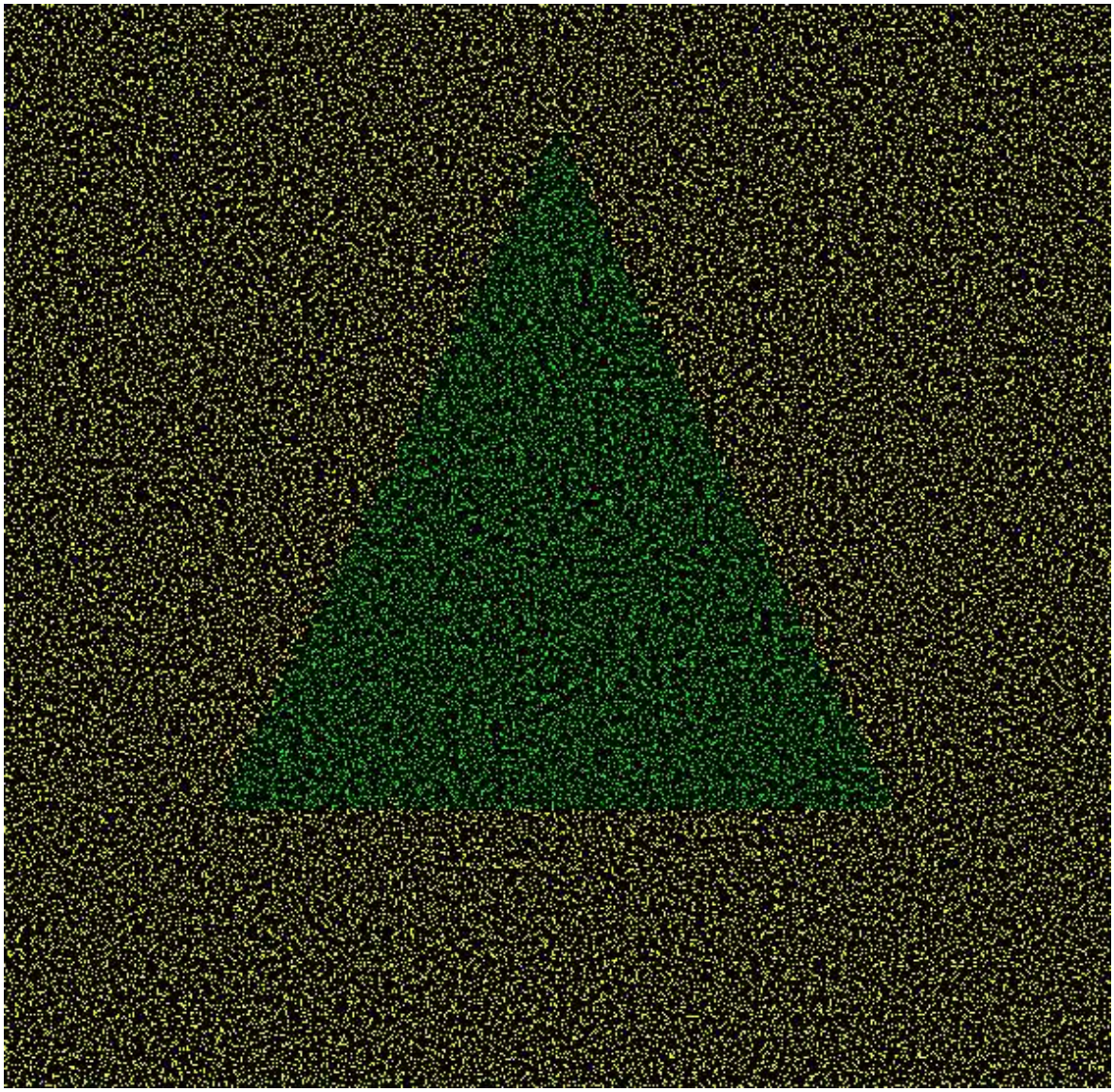


Figure A.27. The decrypted image obtained from V_2^{PL} and V_3^{PL}

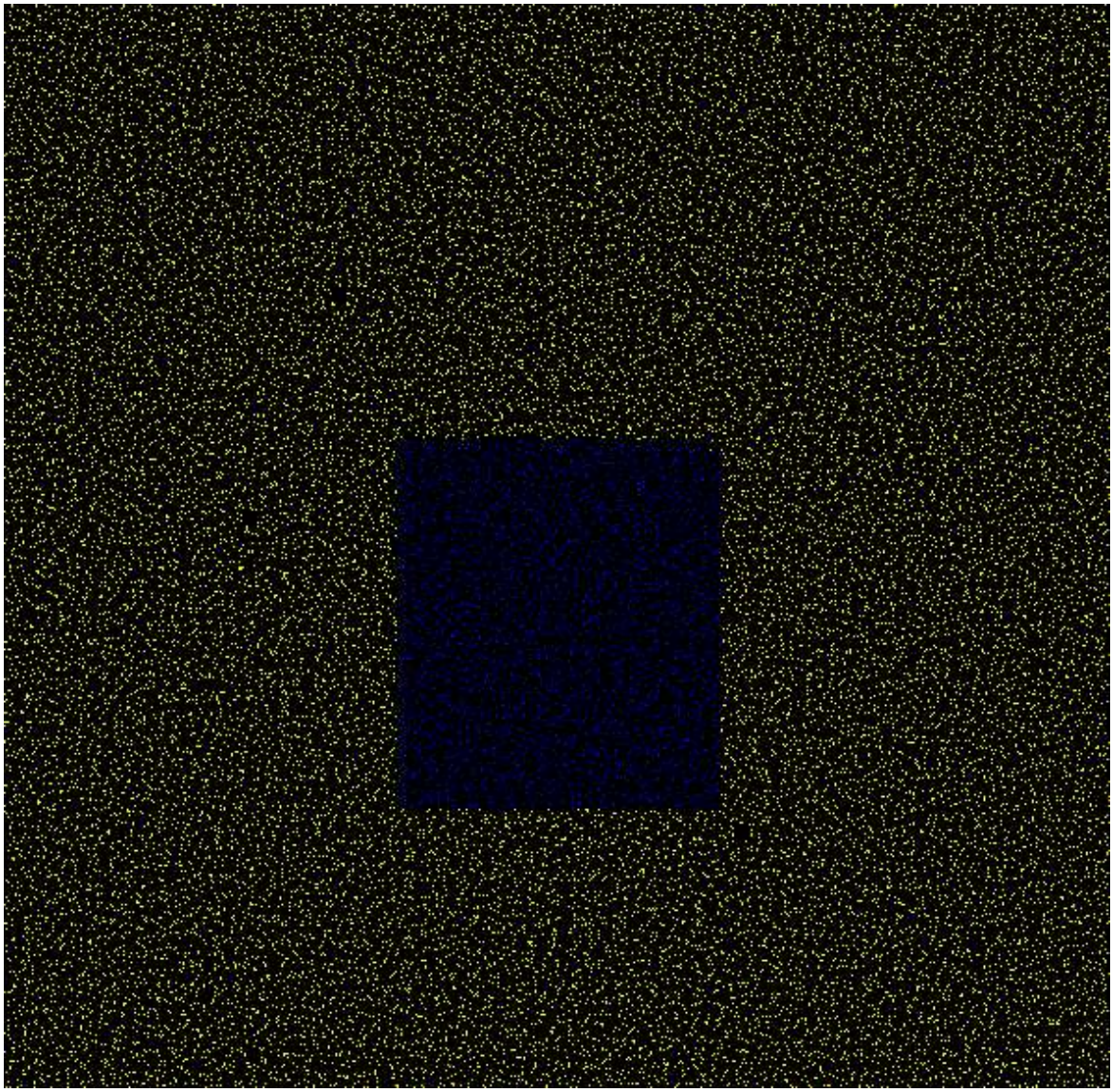


Figure A.28. The decrypted image obtained from V_1^{PL} and V_3^{PL}

Bibliography

[1] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson. Visual cryptography for general access structures. *Information and Computation*, 129, issue 2:86–106, 1996.

[2] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson. Extended capabilities for visual cryptography. *Theoretical Computer Science*, 250(1–2):143–161, 2001.

[3] J. Benaloh. Secret sharing homomorphisms: keeping shares of a secret secret. *Advances in Cryptology-CRYPTO'86,* LNCS 263, Springer-Verlag, pages 251–260, 1986.

[4] J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. *Advances in Cryptology-CRYPTO'88,* LNCS 403, Springer-Verlag, pages 27–35, 1990.

[5] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proc. of IEEE Int. Conf. on Comp. Sys. and Signal Proc.*, pages 175–179, 1984.

[6] I. Biehl and S. Wetzel. Traceable visual cryptography. *Proc. of ICICS'97,* LNCS 1334, Springer-Verlag, pages 63–71, 1997.

[7] B. Blakley, G. R. Blakley, A. H. Chan, and J. Massey. Threshold schemes with disenrollment. *Advances in Cryptology-CRYPTO'92,* LNCS 740, Springer-Verlag, pages 540–548, 1993.

[8] G. R. Blakley. Safeguarding cryptographic keys. *AFIPS 1979 Nat. Computer Conf.*, 48:313–317, 1979.

[9] G. R. Blakley and C. Meadows. Security of ramp schemes. *Advances in Cryptology-CRYPTO'84,* LNCS 196, Springer-Verlag, pages 242–269, 1985.

[10] C. Blundo, A. D. Bonis, and A. De Santis. Improved schemes for visual cryptography. *Designs, Codes and Cryptography*, 24(3):255–278, 2001.

[11] C. Blundo, A. Cresti, A. De Santis, and U Vaccaro. Fully dynamic secret sharing scheme. *Theoretical Computer Science*, 165(2):407–440, 1996.

[12] C. Blundo, P. D'Arco, A. De Santis, and D. R. Stinson. On the contrast in visual cryptography schemes. *J. of Cryptology*, 12, issue 4:261–289, 1999.

[13] C. Blundo, P. D'arco, A. De Santis, and D. R. Stinson. Contrast optimal threshold visual cryptography. *SIAM J. of Discrete Math.*, 16(2):224–261, 2003.

[14] C. Blundo, A. De Santis, and M. Naor. Visual cryptography for gray-level images. *Information Processing Letters*, 75, issue 6:255–259, 2001.

[15] C. Blundo, A. De Santis, R. De Simone, and U. Vaccaro. Tight lower bounds on the information rate of secret sharing schemes. *Design, Codes and Cryptography*, 11:101–122, 1997.

[16] C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro. Graph decomposition and secret sharing schemes. *J. of Cryptology*, 8:39–64, 1995.

[17] C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro. Graph decompositions and secret sharing schemes. *J. of cryptology*, 8:39–64, 1995.

[18] C. Blundo, A. De Santis, and U. Vaccaro. Efficient sharing of many secrets. *Proc. of STACS'93* LNCS 665, Springer-Verlag, pages 692–703, 1993.

[19] C. Blundo, A. De Santis, and U. Vaccaro. On secret sharing schemes. *Information Processing Letters*, 65(1):25–32, 1998.

[20] C. Blundo and D. R. Stinson. Anonymous secret sharing schemes. *Discrete Applied Mathematics*, 77, issue 1:13–28, 1997.

[21] E. F. Brickell and D. M. Davenport. On the classification of ideal secret sharing schemes. *J. of Cryptology*, 4:123–134, 1991.

[22] E. F. Brickell and D. R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. *J .of Cryptology*, 5:153–166, 1992.

[23] C. Cachin. On-line secret sharing. *5th IMA Conference in Cryptography and Coding,* LNCS 1025, Springer-Verlag, pages 190–198, 1995.

[24] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro. On the size of shares for secret sharing schemes. *J. of Cryptology*, 6:157–167, 1993.

[25] C.-C. Chang and T.-X. Yu. Sharing a secret gray image in multiple secret. *Proc. of 1st International Symposium on Cyber Worlds*, pages 1–8, 2002.

[26] S.-Y. Chiou and C.-S. Laih. A tempo-based audio cryptography scheme. *IEICE Trans. Fundamentals*, E86–A(8):2091–2098, 2003.

[27] B. Chor, G. Goldwasser, S. Micali, and B. Awerbuch. Verifiable secret sharing simultaneity in the presence of faults. *Proc. of IEEE 26th Annual Symposium on Foundations of Computer Science*, pages 383–395, 1985.

[28] R. Cleve, D. Gottesman, and H.-K. Lo. How to share a quantum secret. *Physical Review Letters*, 83(3):648–651, 1999.

[29] G. D. Crescenzo. Sharing one secret vs. sharing many secrets. *Theoretical Computer Science*, 295, issue 1–3:123–140, 2003.

[30] L. Csirmaz. The size of a share must be large. *J. of Cryptology*, 10:223–231, 1997.

[31] D. Daeman and V. Rijmen. *The Design of Rijndael: Aes-The Advanced Encryption Standard*. Springer-Verlag, 2002.

[32] Y. Desmedt, S. Hou, and J.-J. Quisquater. Audio and optical cryptography. *Advances in Cryptology-ASIACRYPT'98,* LNCS 1514, Springer-Verlag, pages 392–404, 1998.

[33] Y. Desmedt, S. Hou, and J.-J. Quisquater. Cerebral cryptography. *Proc. of Information Hiding,* LNCS 1525, Springer-Verlag, pages 62–72, 1998.

[34] W. Diffie and M. Hellman. New directions of cryptography. *IEEE Trans. Inform. Theory*, IT–22(6):644–656, 1976.

[35] S. Droste. New results on visual cryptography. *Advances in Cryptology-CRYPTO'96,* LNCS 1109, Springer-Verlag, pages 401–415, 1996.

[36] P. A. Eisen and D. R. Stinson. Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels. *Designs, Codes and Cryptography*, 25(1):15–61, 2002.

[37] P. Feldman. A practical scheme for non-iterative verifiable secret sharing. *Proc. of FOCS'87*, pages 427–437, 1987.

[38] J. D. Golić. On matroid characterization of ideal secret sharing schemes. *J. of Cryptology*, 11:75–86, 1998.

[39] D. Gottesman. Theory of quantum secret sharing. *Physical Review A*, 61(042311), 2000.

[40] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung. Proactive secret sharing or: how to cope with perpetual leakage. *Advances in Cryptology-CRYPTO'95,* LNCS 963, Springer-Verlag, pages 339–352, 1995.

[41] M. Hillery, V. Buzěk, and A. Berthiaume. Quantum secret sharing. *Los Alamos e-print archive*, quant-ph/9806063, 1998.

[42] T. Hofmeister, M. Krause, and H. U. Simmon. Contrast-optimal k out of n secret sharing schemes in visual cryptology. *Theoretical Computer Science*, pages 471–485, 2000. Preliminary version is appeared in *COCOON'97*, LNCS 1276, Springer-Verlag, pp. 176–185, 1997.

[43] T. Ishihara and H. Koga. New constructions of the lattice-based visual secret sharing using mixture of colors. *IEICE Trans. Fundamentals*, E85–A(1):158–166, 2002.

[44] T. Ishihara and H. Koga. On a general formula of the (t, n)-visual secret sharing scheme for color images. *Proc. of SCIS'03*, pages 1077–1082, 2003. (in Japanese).

[45] T. Ishihara and H. Koga. A visual secret sharing scheme for color images based on meanvalue-color mixing. *IEICE Trans. Fundamentals*, E86–A(1):194–197, 2003.

[46] R. Ito, H. Kuwakado, and H. Tanaka. Image size invariant visual cryptography. *IEICE Trans. Fundamentals*, E82–A(10):2172–2176, 1999.

[47] M. Itoh, A. Saito, and T. Nishizeki. Secret sharing scheme realizing general access structure. *IEEE Globecom*, pages 99–102, 1987.

[48] M. Itoh, A. Saito, and T. Nishizeki. Secret sharing scheme realizing general access structure. *IEICE Trans. Fundamentals*, J71–A(8):1592–1598, 1988. (in Japanese).

[49] M. Itoh, A. Saito, and T. Nishizeki. Multiple assignment scheme for sharing secret. *J. of Cryptology*, 6:15–20, 1993.

[50] M. Iwamoto, H.Yamamoto, and H. Ogawa. A general construction method of secret sharing schemes based on (k, n)-threshold schemes using integer programming. *Technical Report of IEICE*, 103(61, ISEC2003-11):63–70, 2003. (in Japanese).

[51] M. Iwamoto and H. Yamamoto. Non-ideal ramp secret sharing schemes for general access structures. *Proc. of Symposium on Information Theory and Its Applications*, pages 227–230, 2002. (in Japanese).

[52] M. Iwamoto and H. Yamamoto. The optimal n-out-of-n visual secret sharing scheme for gray-scale images. *IEICE Trans. Fundamentals*, E85–A(10):2238–2247, 2002.

[53] M. Iwamoto and H. Yamamoto. A construction method of visual secret sharing schemes for plural secret images. *IEICE Trans. Fundamentals*, 86–A(10):2577–2588, 2003.

[54] W.-A. Jackson, K. L. Martin, and C. M. O'Keefe. Ideal secret sharing schemes with multiple secrets. *J. of Cryptology*, 9:233–250, 1996.

[55] W.-A. Jackson, K. M. Martin, and C. M. O'Keefe. Multisecret threshold schemes. *Advances in Cryptology-CRYPTO'93,* LNCS 963, Springer-Verlag, pages 126–135, 1994.

[56] B. Julesz. Binocular depth perception computer-generated patterns. *Bell Tech. J.*, 39:1125–1162, 1960.

[57] A. Karlsson, M. Koashi, and N. Imoto. Quantum entanglement for sharing secret splitting. *Physical Review A*, 59(1):162–168, 1999.

[58] E. D. Karnin, J. W. Greene, and M. E. Hellman. On secret sharing systems. *IEEE Trans. Inform. Theory*, 29(1):35–41, 1983.

[59] T. Kato. *Studies on Visual Secret Sharing Schemes and Their Applications*. PhD thesis, Univ. of Tokyo, 1996. (in Japanese).

[60] T. Kato and H. Imai. An extended construction method of visual secret sharing scheme. *IEICE Trans. Fundamentals*, J79–A(8):1344–1351, 1996. (in Japanese).

[61] Y. Kawamoto and H. Yamamoto. Secret function sharing schemes and their applications to the oblivious transfer. *Proc. of IEEE International Symposium on Information Theory (ISIT)*, page 281, 2003.

[62] A. Klein and M. Wessler. Extended visual cryptography schemes. preprint, 2003.

[63] H. Koga. A simple construction of a (k, n) visual secret sharing scheme using symmetric polynomials. private communications, 1998.

[64] H. Koga. General formula of the (t, n)-threshold visual secret sharing scheme. *Advances in Cryptology-ASIACRYPT'02,* LNCS 2501, Springer-Verlag, pages 328–345, 2002.

[65] H. Koga. Construction of contrast-optimal (t, n)-visual secret sharing scheme for black-white images. *Proc. of 3rd asian-european workshop on information theory*, pages 45–48, 2003.

[66] H. Koga, M. Iwamoto, and H. Yamamoto. An analytic construction of the visual secret sharing scheme for color images. *IEICE Trans. Fundamentals*, E84-A(1):262–272, 2001.

[67] H. Koga and H. Yamamoto. Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images. *IEICE Trans. Fundamentals*, E81–A(6):1262–1269, 1998.

[68] M. Krause and H. U. Simmon. Determining the optimal contrast for secret sharing schemes in visual cryptology. *LATIN'00,* LNCS 1776, Springer-Verlag, pages 280–291, 2000.

[69] H. Krawczyk. Secret sharing made short. *Advances in Cryptology-CRYPTO'93* LNCS 773, Springer-Verlag, pages 136–146, 1994.

[70] K. Kurosawa and K Okada. Combinatorial lower bounds for secret sharing schemes. *Information Processing Letters*, 60:301–304, 1996.

[71] K. Kurosawa, K. Okada, K. Sakano, W. Ogata, and T. Tsujii. Nonperfect secret sharing schemes and matroids. *Advances in Cryptology-EUROCRYPT'93,* LNCS 765, Springer-Verlag, pages 126–141, 1993.

[72] H. Kuwakado and H. Tanaka. Polynomial representation of visual secret sharing scheme and its application. *IEICE Trans. Fundamentals*, E85–A(6):1379–1386, 2002.

[73] C.-S. Laih, L. Harn, J.-Y. Lee, and T. Hwang. Dynamic threshold scheme based on the definition of cross-product in an n-dimensional linear space. *Advances in Cryptology-CRYPTO'89,* LNCS 435, Springer-Verlag, pages 286–298, 1990.

[74] K. M. Martin and J. Nakahara Jr. Weaknesses of protocols for updating the parameters of an established threshold scheme. *IEE Proc.Comput. Digit. Tech.*, 148(1):45–48, 2001.

[75] National Bureau of Standards (U.S.A). *Data Encryption Standard.* Federal Information Processing Standard Publications 46, National Technical Information Services, Springfield, 1977.

[76] R. J. McEliece and D. V. Sarwate. On sharing secrets and Reed-Solomon codes. *Comm. ACM*, 24(9):583–584, 1981.

[77] A. J. Menezes, P. C. Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1997.

[78] M. Nakajima and Y. Yamaguchi. Extended visual cryptography for natural images. *J. of WSCG*, pages 303–310, 2002.

[79] M. Naor and B. Pinkas. Visual authentication and identification. *Advances in Cryptology-CRYPTO'97,* LNCS 1294, Springer-Verlag, pages 322–336, 1997.

[80] M. Naor and B. Pinkas. Distributed oblivious transfer. *Advances in Cryptology-ASIACRYPT2000* LNCS 1976, Springer-Verlag, pages 576–589, 2000.

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

[82] M. Naor and A. Shamir. Visual cryptography II : improving the contrast via the cover base. *Security Protocols,* LNCS–1189, Springer-Verlag, pages 197–202, 1997.

[83] A. N. Netravali and B. G. Haskell. *Digital Pictures: Representation, computation, and standards*. Plenum Press, 2nd. edition, 1994.

[84] S.-L. Ng. A representation of a family of secret sharing matroids. *Designs, Codes and Cryptography*, 30:5–19, 2003.

[85] S.-L. Ng and M. Walker. On the composition of matroids and ideal secret sharing schemes. *Designs, Codes and Cryptography*, 24:49–67, 2001.

[86] W. Ogata and K. Kurosawa. Some basic properties of general nonperfect secret sharing schemes. *J. of Universal Computer Science*, 4(8):690–704, 1998.

[87] T. Ogawa, A. Sasaki, M. Iwamoto, and H. Yamamoto. Coding efficiency and construction of quantum secret sharing schemes. *Proc. of Symposium on Information Theory and Its Applications*, pages 651–654, 2003. (in Japanese).

[88] K. Okada and K. Kurosawa. Lower bound on the size of shares of nonperfect secret sharing schemes. *Advances in Cryptology-ASIACRYPT'94,* LNCS 917, Springer-Verlag, pages 34–41, 1994.

[89] K Okada, W. Ogata, K. Sakano, and K. Kurosawa. Analysis on secret sharing schemes with non-graphical access structures. *IEICE Trans. Fundamentals*, E80–A(1):85–89, 1997.

[90] E. Okamoto and G. R. Blakley. More flexible secret sharing scheme. *Proc. of SCIS'00*, A39, 2000.

[91] T. Okamoto and H. Yamamoto. *Gendai-angou*. Sangyo Tosho, 1997. (in Japanese).

[92] C. Padró and G. Sáez. Secret sharing schemes with bipartite access structure. *IEEE Trans. Inform. Theory*, 46(7):2596–2604, 2000.

[93] T.P̃. Pedersen. Distributed provers with applications to undeniable signatures. *Advances in Cryptology-EUROCRYPT'91,* LNCS 547, Springer-Verlag, pages 221–242, 1992.

[94] T.P̃. Pedersen. Non-interactive and information theoretic secure verifiable secret sharing. *Advances in Cryptology-CRYPTO'91,* LNCS 576, Springer-Verlag, pages 129–140, 1992.

[95] T. Rabin and M. Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority. *Proc. of the 21st Annual ACM Symposium on Theory of Computing*, pages 73–89, 1989.

[96] V. Rijmen and B. Preneel. Efficient color visual encryption or 'shared colors of benetton'. presented at the rump session of *EUROCRYPT'96*, 1996.

[97] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 21(2):120–126, 1978.

[98] P. D. Seymour. On secret-sharing matroids. *J. of Combin. Theory B*, 56:69–73, 1992.

[99] A. Shamir. How to share a secret. *Comm. ACM*, 22(11):612–613, 1979.

[100] C.Ẽ. Shannon. Communication theory of secrecy systems. *Bell Tech. J.*, 28:656–715, Oct. 1949.

[101] G. J. Simmons. *An introduction to shared secret and/or shared control schemes and their applications*, chapter 9, pages 441–497. IEEE Press, 1991.

[102] G. J. Simmons, W.-A. Jackson, and K. Martin. The geometry of shared secret schemes. *Bulletin of the ICA*, 1(2):230–236, 1991.

[103] K. Srinathan, N. T. Rajan, and C. P. Rangan. Non-perfect secret sharing over general access structures. *Progress in Cryptology-INDOCRYPT'02,* LNCS 2551, Springer-Verlag, pages 409–421, 2002.

[104] D. R. Stinson. Decomposition construction for secret-sharing schemes. *IEEE Trans. Inform. Theory*, 40(1):118–125, 1994.

[105] D. R. Stinson. *CRYPTOGRAPHY Theory and Practice*. CRC Press, 1995. (1st. ed.).

[106] D.R. Stinson. An explication of secret sharing schemes. *Designs, Codes and Cryptography*, 2:357–390, 1992.

[107] Y. Suga, K. Iwamura, K. Sakurai, and H. Imai. Extended graph-type visual secret sharing schemes with embedded plural images. *IPSJ J.*, 42(8):2106–2113, 2001. (in Japanese).

[108] Y. Tamura, M. Tada, and E. Okamoto. Update of access structure in Shamir's (k, n) threshold scheme. *Proc. of SCIS'99*, pages 469–474, 1999.

[109] K. Tochikubo. Remarks on the secret sharing scheme for general access structures. *Proc. of Symposium on Cryptography and Information Security*, pages 779–804, 2001. (in Japanese).

[110] M. Tompa and H. Woll. How to share a secret with cheaters. *J. of Cryptology*, 1:133–138, 1988.

[111] W.-G. Tzeng and C.-M. Hu. A new approach for visual cryptography. *Designs, Codes and Cryptography*, 27(3):207–227, 2002.

[112] T. Uehara, T. Nishizeki, E. Okamoto, and K. Nakamura. Secret sharing systems with matroidial schemes. *IECE Trans.*, J69–A(9):1124–1132, 1986. (in Japanese).

[113] M. van Dijk. On the information rate of perfect secret sharing schemes. *Designs, Codes and Cryptography*, 6:143–169, 1995.

[114] M. van Dijk. More information theoretical inequalities to be used in secret sharing? *Information Processing Letters*, 63:41–44, 1997.

[115] M. van Dijk. *Secret key sharing and secret key generation*. PhD thesis, Univ. of Eindhoven, 1997.

[116] M. van Dijk. A general decomposition construction for incomplete secret sharing schemes. *Designs, Codes and Cryptography*, 15:301–321, 1998.

[117] E. R. Verheul and H. C. A. van Tilborg. Constructions and properties of k out of n visual secret sharing scheme,. *Designs, Codes, and Cryptography*, 1(2):179–196, 1997.

[118] H. Yamamoto. Useful codes for secret sharing communication systems. *Technical Reports of IECE*, IT84-8:23–29, 1984. (In Japanese).

[119] H. Yamamoto. On secret sharing systems using (k, L, n) threshold scheme. *IECE. Trans.*, J68–A(9):945–952, 1985. (in Japanese). English translation: Electronics and Communications in Japan, Part I, vol. 69, no. 9, pp. 46–54, Scripta Technica, Inc., 1986.

[120] H. Yamamoto. On secret sharing communication systems with two or three channels. *IEEE Trans. Inform. Theory*, 32(3):387–393, 1986.

[121] H. Yamamoto. Coding theorem for secret sharing communication systems with two noisy channels. *IEEE Trans. Inform. Theory*, 35(3):572–578, 1989.

[122] H. Yamamoto. A coding theorem for secret sharing communication systems with two gaussian wiretap channels. *IEEE Trans. Inform. Theory*, 37(3):634–638, 1991.

[123] C.-N. Yang and C.-S. Laih. New colored visual secret sharing scheme. *Designs, codes, and cryptography*, 20(3):325–335, 2000.

[124] R. W. Yeung. A new outlook on Shannon's information measures. *IEEE Trans. Inform. Theory*, 37(3):466–474, 1991.

List of Publications

Journal and International Symposium

1. H. Koga, M. Iwamoto, and H. Yamamoto. An analytic construction of the visual secret sharing scheme for color images. *IEICE Trans. Fundamentals*, E84-A(1):262–272, 2001. ([66])

2. M. Iwamoto and H. Yamamoto. The optimal n-out-of-n visual secret sharing scheme for gray-scale images. *IEICE Trans. Fundamentals*, E85–A(10):2238–2247, 2002. ([52])

3. M. Iwamoto and H. Yamamoto. Visual secret sharing schemes for plural secret images. *IEEE International Symposium on Information Theory*, p. 283, June–July, 2003.

4. M. Iwamoto and H. Yamamoto. A construction method of visual secret sharing schemes for plural secret images. *IEICE Trans. Fundamentals*, 86–A(10):2577–2588, 2003. ([53])

Domestic Symposium and Technical Meeting

5. M. Iwamoto, H. Koga, and H. Yamamoto. Another constructions of the (k, n) lattice-based visual secret sharing scheme and its application to general access structures. *Proc. of Symposium on Information Theory and Its Applications (SITA99)*, pp. 761–764, Nov.–Dec., 1999. (in Japanese).

6. H. Koga, M. Iwamoto, and H. Yamamoto. An analytic construction of the visual secret sharing scheme for color images. *Proc. of Symposium on Cryptography and Information Security (SCIS2000)*, SCIS2000-B45, Jan., 2000.

7. M. Iwamoto and H. Yamamoto. An optimal n-out-of-n visual secret sharing scheme for gray-scale images. *Proc. of Computer Security Symposium (CSS2001)*, pp. 337–342, Oct., 2001. (in Japanese).

8. M. Iwamoto and H. Yamamoto. A visual secret sharing scheme for plural images. *Proc. of Symposium on Information Theory and Its Applications (SITA2001)*, pp. 565–568, Dec., 2001. (in Japanese).

9. M. Iwamoto and H. Yamamoto. The security condition of visual secret sharing schemes for plural images. *Technical Report of IEICE*, ISEC2001–121, pp. 51–56, March, 2002. (in Japanese).

10. M. Iwamoto and H. Yamamoto. Non-ideal ramp secret sharing schemes for general access structures. *Proc. of Symposium on Information Theory and Its Applications (SITA2002)*, pp. 227–230, Dec., 2002. (in Japanese, [51]).

11. M. Iwamoto, H.Yamamoto, and H. Ogawa. A general construction method of secret sharing schemes based on (k, n)-threshold schemes using integer programming. *Technical Report of IEICE*, 103(61, ISEC2003-11):63–70, 2003. (in Japanese, [50]).

12. T. Ogawa, A. Sasaki, M. Iwamoto, and H. Yamamoto. Coding efficiency and construction of quantum secret sharing schemes. *Proc. of Symposium on Information Theory and Its Applications*, pages 651–654, 2003. (in Japanese, [87]).

Patent

13. 岩本 貢, 山本 博資, 小川博久. 秘密分散法の最適割り当て決定方法及びその方法を実現するコンピュータプログラム. (特願 003-132265, 国際特許分類 G06F 17/60, 申請中), 2003.