M. Tech (Computer Science) Dissertation Series

Constructions of Visual Cryptography Schemes

A dissertation submitted in partial fulfilment of the
requirements for the M. Tech (Computer Science)
degree of the Indian Statistical Institute

By

Somnath Sikdar

under the supervision of

Prof. Bimal Roy

INDIAN STATISTICAL INSTITUTE
203, Barrackpore Trunk Road
Kolkata-700 108

Certificate of Approval

This is to certify that the work reported in this thesis entitled "Constructions of Visual Cryptography Schemes" by Somnath Sikdar has been done under my guidance and supervision. This work is worthy of the M. Tech degree in Computer Science.

Supervisor

Acknowledgements

This work has been possible due to a number of people. Firstly, I would like to thank my supervisor Prof. Bimal Roy for his guidance and assistance throughout the course of this work. He lent much of his time to review this work and helped me on a number of points. Many thanks to Mr. Trideb Kr. Dutta with whom we had had a number of useful discussions. I would also like to thank my teachers Prof. Rana Barua, Prof. Palash Sarkar, and Dr. Subhomoy Maitra for their excellent courses. Dr. Maitra reviewed portions of Chapter 4 and suggested a number of changes to improve the presentation.

Thanks to my friends Avishek Adhikari, M. Prem Laxman Das, Shantanu Das, and Madhusudan Karan. The work in Chapter 4 was in collaboration with Avishek. Prem reviewed Chapter 4 and made some valuable suggestions. Shantanu and Madhu helped us implement some of the cryptography schemes.

Finally, thanks to my parents for their support and encouragement.

Abstract

Visual cryptography is a secret sharing scheme in which the secret is an image. The image could be a page of printed text, a photograph, a picture, etc. A visual cryptography scheme enables an image to be split into a number of shares that are printed on transparencies, so that when certain subsets of these transparencies are stacked together, one can see the original image. By examining other subsets of transparencies, one obtains no information about the secret image.

In this thesis, we review three classes of visual cryptography schemes– those that are applicable to black/white, grey-level, and color images. We also present a new $(2, n)$ visual cryptography scheme for color images. In such a scheme, the dealer provides a transparency to each one of n users; any two of them can see the image by stacking their transparencies, but no one of them can gain any information about it. Finally, we present some open problems in color visual cryptography.

Contents

Chapter 1

Visual Cryptography: An Introduction

The fundamental objective of cryptography is to enable secure communication over an insecure channel. A person A wants to send B a secret message over a communication channel that may be tapped by an opponent C. The basic problem is enable such communication without the opponent discovering what the message is.

The solution to this problem is to *encrypt* the secret message (also known as the *plaintext*) using a predetermined key and then transmit the resulting *ciphertext* over the channel. On receiving the ciphertext, B, who knows the encryption key can recover the plaintext; the line-tapper C, on the other hand, cannot determine what the plaintext was.

In contrast to this, is a model that deals with sharing a secret among a set of people with the objective of protecting its privacy. This model consists of a person D, known as the *dealer*, and a set $\mathcal{P}$ of *participants*. We assume that $D \notin \mathcal{P}$. When D wants to share a secret among the participants in $\mathcal{P}$, he gives each participant some partial information called a *share*. The shares should be distributed secretly, so no participant knows the share given to another participant. At a later time, a subset $X \subseteq \mathcal{P}$ of participants will pool their shares in an attempt to recover the secret. The method used to share the secret is called a *secret sharing scheme*.

Visual cryptography is a recent secret sharing scheme introduced by Naor and Shamir in 1994 [11]. The setup of a visual cryptography scheme consists of a set $\mathcal{P}$ of participants, where some subsets of participants are defined to be *qualified* whereas other subsets are defined to be *forbidden*. A secret image SI is shared among the participants such that

1. each participant receives exactly one share

2. only qualified subsets of participants can "visually" recover the secret image, and

3. no forbidden subset of participants can reconstruct the secret image.

Each share consists of what appears to be a random collection of pixels printed on a transparency and a "visual" recover for a set $X \subseteq \mathcal{P}$ consists of stacking the transparencies distributed among the participants in X. What makes visual cryptography different from other cryptography schemes is that the secret image is reconstructed directly by the human visual system and no computations are involved during reconstruction. Because of its simplicity it can be used even by people with no knowledge of cryptography.

Naor and Shamir analyzed k out of n visual cryptography schemes. In such a scheme, any subset of k or more participants is a qualified subset and the remaining subsets are forbidden. Therefore, the secret image is visible if and only if any set of k or more transparencies are stacked together. One possible application of these schemes is the following. The 2 out of 2 visual cryptography scheme can be thought of as a private key cryptosystem. We encode the secret image into two randomly looking transparencies and send one of them by mail or fax. This constitutes the ciphertext whereas the other transparency serves as a secret key. The original image is revealed by stacking the transparencies together. This system is similar to the one-time pad as each page of ciphertext is decoded using a different key with the difference being that no computations are involved, the decoding being done by the human visual system.

The secret images dealt with by Naor and Shamir consisted of a collection of black and white pixels. While these images are sufficient to represent data such as printed text, they cannot be used for grey-scale and color images. In order to apply visual cryptography schemes to such images one would have to generalize the existing schemes for black and white images. Visual cryptography schemes for grey-scale images have been proposed in [5] and color images in [7, 8, 9, 12]. We will look at these schemes later. Generalizations in other directions have also been considered.

1. In one generalization of visual cryptography known as *extended visual cryptography*, the shares given to participants do not look like a random bunch of pixels, but like innocent looking images such as that of a house, an animal, a tree etc. A solution to this problem is given in [1].

2. In another generalization, more than one secret image is shared among a set of participants. In such a scheme, stacking different sets of transparencies reveal different secret images. A method for doing this can be found in [6].

In this thesis, we propose a 2 out of n visual cryptography scheme for color images. Our scheme is more efficient than existing 2 out of n schemes for color images for a number of reasons that we will explain later. At this point, we will just mention that existing $(2,n)$ schemes (and also (k,n) schemes) suffer from the defect that they are unfeasible to implement if either the number of colors or the number of participants is large; the quality of the recovered image also deteriorates as these numbers increase. Our scheme alleviates this problem to an extent.

We have organized this thesis as follows. Chapter 2 discusses visual cryptography schemes that are applicable to black and white images. It also discusses a number of theoretical results on the quality of the recovered image. Chapter 3 discusses existing schemes for grey level and color images. In Chapter 4, we propose our 2 out of n scheme. Finally, in Chapter 5 we discuss some open problems in the area of color visual cryptography.

Chapter 2

Black and White VCS

In this chapter, we will look at visual cryptography schemes for black and white images—images composed of just two types of pixels: black and white. We begin by describing the model used in black and white visual cryptography. We then look at constructions of visual cryptography schemes, first for threshold access structures and then for general access structures. We also present some theoretical results regarding the quality of the recovered image. The material in this chapter is based on references [2, 4, 10, 11].

2.1 The Model

The model that we describe here is taken nearly verbatim from Blundo, De Santis, and Stinson [4]. Let $\mathcal{P} = \{1, 2, \ldots, n\}$ be a set of elements called *participants*, and let $2^{\mathcal{P}}$ denote the set of all subsets of $\mathcal{P}$. Let $\Gamma_{Qual} \subseteq 2^{\mathcal{P}}$ and $\Gamma_{Forb} \subseteq 2^{\mathcal{P}}$, where $\Gamma_{Qual} \cap \Gamma_{Forb} = \emptyset$. We refer to members of Γ_{Qual} as *qualified sets* and we call members of Γ_{Forb} as *forbidden sets*. The pair $(\Gamma_{Qual}, \Gamma_{Forb})$ is called an *access structure* for $\mathcal{P}$.

For $A \subseteq 2^{\mathcal{P}}$, we say that A is *monotone increasing* if for any $B \in A$ and any $C \subseteq \mathcal{P}$ such that $B \cap C = \emptyset$, we have $B \cup C \in A$. A is said to be *monotone decreasing* if for any $B \in A$ and any $C \subseteq B$, $B - C \in A$. If $\Gamma_{Qual} \cup \Gamma_{Forb} = 2^{\mathcal{P}}$ and if Γ_{Qual} is monotone increasing then Γ_{Forb} is monotone decreasing. In such a case, we say that the access structure is *strong*. We define Γ_0 to consist of all the minimal qualified subsets.

$$\Gamma_0 = \{A \in \Gamma_{Qual} : A' \notin \Gamma_{Qual} \text{ for all } A' \subset A\}$$

In a strong access structure, Γ_0 is called the *basis* and Γ_{Qual} is called the *closure* of Γ_0.

We also need to define essential and nonessential participants. A participant $i \in \mathcal{P}$ is *essential* if there exists a set $X \subseteq \mathcal{P}$ such that $X \notin \Gamma_{Qual}$ but $X \cup \{i\} \in \Gamma_{Qual}$. We also say that i is *strongly essential* if $X \in \Gamma_{Forb}$ and $X \cup \{i\} \in \Gamma_{Qual}$. A participant i is *nonessential* if there does not exists a set X such that $X \notin \Gamma_{Qual}$ but $X \cup \{i\} \in \Gamma_{Qual}$. If a participant is nonessential then we can construct a visual cryptography scheme giving him/her nothing as his/her share. In fact, a nonessential participant need not participate "actively" in the reconstruction of the image, since the information he/she has is not needed by any subset of $\mathcal{P}$ in order to recover the shared image. Therefore, we assume that all participants are essential.

We assume that the secret image consists of a collection of black and white pixels, each pixel being encrypted separately. To understand the encryption process consider the case where the secret image consists of just a single black or white pixel. On encryption, this pixel appears in the n shares distributed to the participants. However, in each share the pixel is subdivided into m *subpixels*, each of which is either black or white. It is important to note that the shares are printed on transparencies, and that a "white" subpixel is actually an area where nothing is printed, and therefore left transparent. We assume that the subpixels are sufficiently small and close enough so that the eye averages them to some shade of grey. We can represent this with an $n \times m$ boolean matrix $S[i, j]$, where $S[i, j] = 1$ if and only if the jth subpixel in the ith share is black. When the shares are stacked together, the perceived grey level is proportional to the number of 1's in the boolean OR of the $m-$vectors representing the shares of each participant. When the secret image consists of more than one pixel, we encrypt each pixel separately. The shares then consist of a collection of blocks of m subpixels, each block of m subpixels representing a single pixel of the original secret image.

In order that the recovered image is clearly discernible, it is important that the grey level of a black pixel be darker than that of a white pixel. Informally, the difference in the grey levels of the two pixel types is called *contrast*. We want the contrast to be as large as possible. Three variables control the perception of black and white regions in the recovered image: a threshold value, a relative difference, and the number of subpixels (also known as *pixel expansion*) [10]. We use:

- t to denote the threshold value;
- α to denote the relative difference;
- m to denote the pixel expansion.

The *threshold value* is a numeric value that represents a grey level that is perceived by the human eye as the color black. The value $\alpha \cdot m$ is the contrast, which we want to be as large as possible. We require that $\alpha \cdot m \geq 1$ to ensure that black and white areas will be distinguishable.

We give the following definition of a visual cryptography scheme for a general access structure. The phrasing is taken directly from Atienese, Blundo, De Santis, and Stinson [2]. We use $OR\ V$ to denote the boolean operation OR of a set of vectors with result V. The *Hamming weight* $w(V)$ is the number of 1's in the boolean vector V.

Definition 2.1 *Let* $(\Gamma_{Qual}, \Gamma_{Forb})$ *be an access structure on a set* $\mathcal{P}$ *of* n *participants. Two collections (multisets) of* $n \times m$ *boolean matrices* C_0 *and* C_1 *constitute a visual cryptography scheme* $(\Gamma_{Qual}, \Gamma_{Forb}, m)-VCS$ *if there exist values* $\alpha(m)$ *and* $\{t_X\}_{X \in \Gamma_{Qual}}$ *satisfying the following conditions:*

1. *For any* $M \in C_0$ *and any* $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Qual}$, *the* $OR\ V$ *of rows* $i_1, i_2, \ldots, i_p$ *satisfies*

$$w(V) \leq t_X - \alpha(m) \cdot m;$$

whereas, for any $M \in C_1$ *it results that* $w(V) \geq t_X$.

2. *For any* $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Forb}$, *the two collections of* $p \times m$ *matrices* $\mathcal{D}_t$ ($t \in \{0,1\}$), *obtained by restricting each* $n \times m$ *matrix in* $\mathcal{C}_t$ ($t \in \{0,1\}$) *to rows* $i_1, i_2, \ldots, i_p$ *are indistinguishable in the sense that they contain the same matrices with the same frequencies.*

Each pixel of the original image will be encrypted into n pixels, each of which consist of m subpixels. To share a white (resp. black) pixel, the dealer randomly chooses one of the matrices in $\mathcal{C}_0$ (resp. $\mathcal{C}_1$), and distributes row i to participant i. Thus the chosen matrix defines the m subpixels in each of the n transparencies. Note that in the definition above we allow a matrix to appear more than once in $\mathcal{C}_0$ ($\mathcal{C}_1$). Finally, note that the size of the collections $\mathcal{C}_0$ and $\mathcal{C}_1$ need not be the same.

The first property in the definition above is related to the contrast of the image. It says that when a qualified set of participants stack their transparencies, the grey level of a black pixel in the recovered image is greater than or equal to some predefined threshold value and that the difference in the grey levels of a black and white pixel is at least $\alpha(m) \cdot m$. The second property is related to *security*, since it implies that even by inspecting all their shares, a forbidden set of participants cannot gain any information about whether the shared pixel was white or black.

2.1.1 Basis Matrices

Instead of working with the collections $\mathcal{C}_0$ and $\mathcal{C}_1$, it is convenient (in terms of memory requirements) to consider only two $n \times m$ boolean matrices, S^0 and S^1 called *basis matrices* which satisfy the following definition.

Definition 2.2 *Let* $(\Gamma_{Qual}, \Gamma_{Forb})$ *be an access structure on a set* $\mathcal{P}$ *of* n *participants. A* $(\Gamma_{Qual}, \Gamma_{Forb}, m)-VCS$ *with relative difference* $\alpha(m)$ *and a set of thresholds* $\{t_X\}_{X \in \Gamma_{Qual}}$ *is realized using the* $n \times m$ *basis matrices* S^0 *and* S^1 *if the following two conditions hold:*

1. *If* $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Qual}$, *then the* OR V *of the rows* $i_1, i_2, \ldots, i_p$ *of* S^0 *satisfies*

$$w(V) \leq t_X - \alpha(m) \cdot m;$$

   whereas, for S^1 *it results that* $w(V) \geq t_X$.

2. *If* $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Forb}$, *the two* $p \times m$ *matrices obtained by restricting* S^0 *and* S^1 *to rows* $i_1, i_2, \ldots, i_p$ *are equal up to a column permutation.*

The collections $\mathcal{C}_0$ and $\mathcal{C}_1$ are obtained by permuting the columns of the corresponding basis matrix (S^0 for $\mathcal{C}_0$ and S^1 for $\mathcal{C}_1$) in all possible ways. Note that, in this case, the sizes of the collections $\mathcal{C}_0$ and $\mathcal{C}_1$ are the same.

2.1.2 Share Distribution Algorithm

Now that we will be working with the basis matrices S^0 and S^1, we need to modify the encryption process slightly as described below.

For each pixel P, do the following:

1. Generate a random permutation π of the set $\{1, 2, \ldots, m\}$.

2. If P is a black pixel, then apply π to the columns of S^0; else apply π to the columns of S^1. Call the resulting matrix T.

3. For $1 \leq i \leq n$, row i of T comprises the m subpixels of P in the ith share.

2.2 Threshold Schemes

A $(k, n)-$threshold structure is any access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ in which

$$\Gamma_0 = \{B \subseteq \mathcal{P} : |B| = k\}$$

and

$$\Gamma_{Forb} = \{B \subseteq \mathcal{P} : |B| \leq k - 1\}.$$

In any $(k, n)-$threshold VCS, the image is visible if any k of the n participants stack their transparencies, but totally invisible if fewer than k transparencies are stacked together or analyzed by any other method. In a strong $(k, n)-$threshold VCS, the image remains visible if more than k participants stack their transparencies.

We now examine some constructions of threshold VCS proposed by Naor and Shamir [11] and Blundo, De Santis and Stinson [4].

2.2.1 $(2, n)-$threshold VCS

The 2 out of n visual secret sharing problem can be solved by using the following $n \times n$ matrices as basis matrices [11].

$$S^0 = \begin{bmatrix} 1 & 0 & 0 & \ldots & 0 \\ 1 & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \ldots & 0 \end{bmatrix}$$

$$S^1 = \begin{bmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{bmatrix}$$

S^0 is a boolean matrix whose first column comprises of 1's and whose remaining entries are 0's. S^1 is simply the identity matrix of dimension n.

When we encrypt a white pixel, we apply a random permutation to the columns of S^0 to obtain matrix T. We then distribute row i of T to participant i. To encrypt a black pixel, we apply the permutation to S^1. A single share of a black or white pixel consists of a randomly placed black subpixel and $(n-1)$ white subpixels. Two shares of a white pixel have a combined Hamming weight of 1, whereas any two shares of a black pixel have a combined Hamming

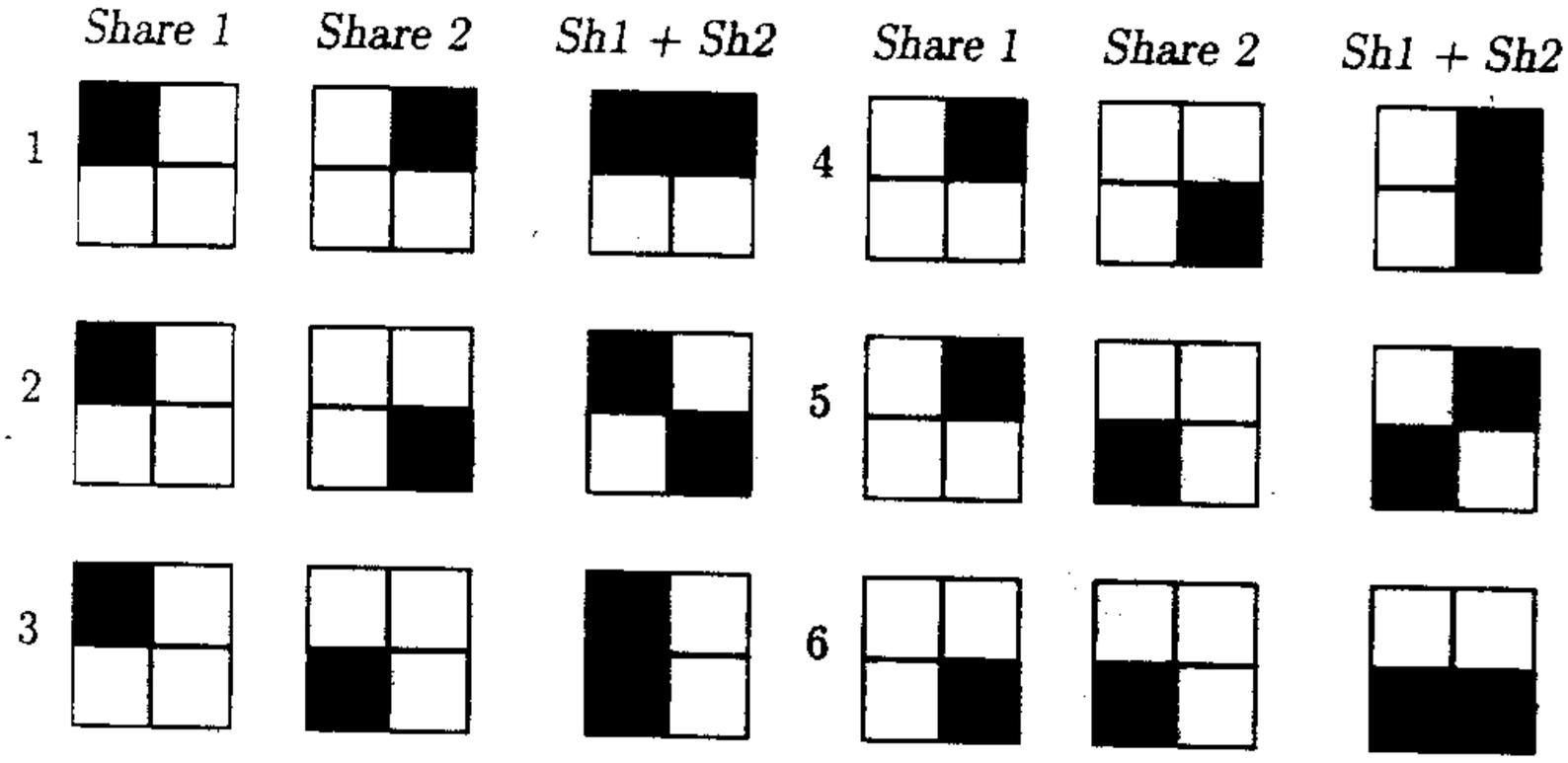

Figure 2.1: The shares of a black pixel

weight of 2, which looks darker. The visual difference between the two cases becomes clearer as we stack additional transparencies.

To exemplify this discussion, let us take a concrete example of a (2,4) VCS. The basis matrices S^0 and S^1 in this case are given by:

$$S^0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

$$S^1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

A black pixel can be shared in any one of the six ways shown in Figure 2.1. A white pixel can be shared in four possible ways as shown in Figure 2.2.

If one examines just a single share then it is impossible to determine whether it represents a share of a black or a white pixel since single shares, whether black or white, look alike. If two shares of a black pixel are combined together, we obtain two black and two white subpixels. Combining the shares of a white pixel yields only one black and three white subpixels. Therefore, on stacking two shares, a black pixel will look darker than a white pixel.

It is intuitively clear that as the value of n increases, it will become progressively difficult to discriminate a black from a white pixel in the recovered image. This is because, as n increases, the grey level produced by 1 black and $(n-1)$ white subpixels is approximately equal to that produced by 2 black and $(n-2)$ white subpixels. This can be also seen from the

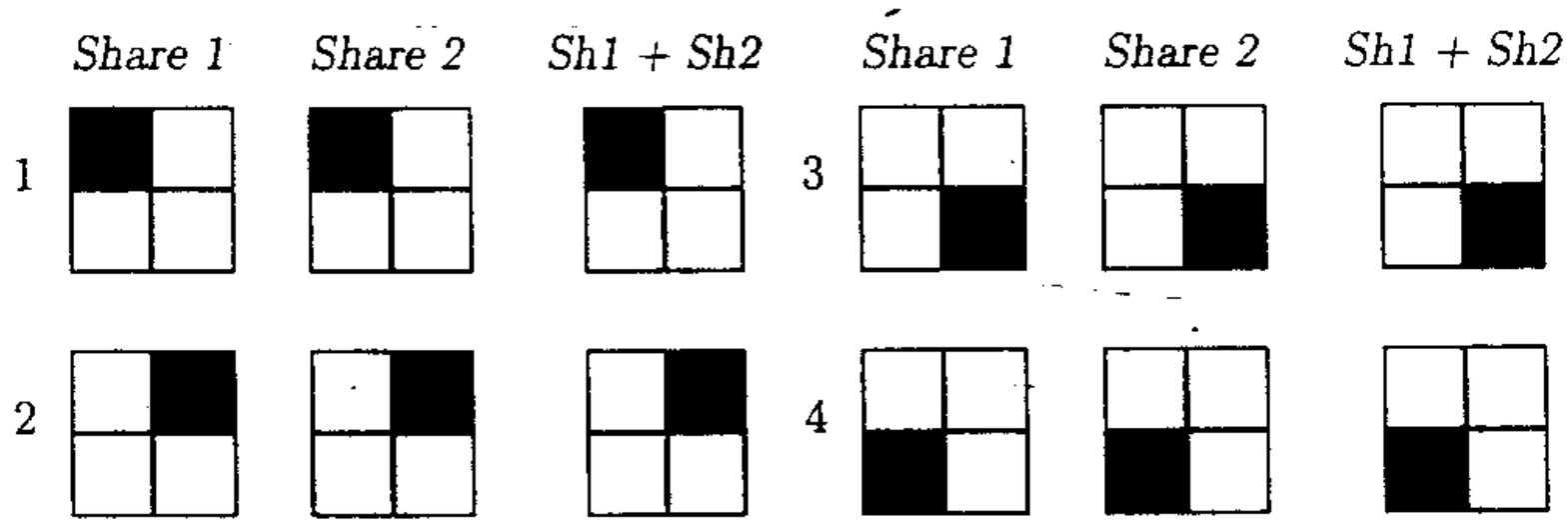

Figure 2.2: The shares of a white pixel

fact that the relative difference α is $1/n$. The relative difference measures the difference in contrast between black and white pixels. As n increases, this quantity goes to 0. Therefore, this construction is viable only if n is small.

2.2.2 A $(2, n)$−threshold VCS with optimal contrast

We now present a $(2, n)$−threshold VCS due to Blundo, De Santis, and Stinson [4] in which the relative difference is optimal.

The $n \times m$ basis matrices S^0 and S^1 are constructed as follows: The columns of S^1 consist of all binary n−vectors of weight $\lfloor n/2 \rfloor$. Hence, $m = \binom{n}{\lfloor n/2 \rfloor}$ and any row in S^1 has weight equal to $\binom{n-1}{\lfloor n/2 \rfloor - 1}$. S^0 is constructed from n identical row vectors of length m, and of weight $\binom{n-1}{\lfloor n/2 \rfloor - 1}$. Before we prove that these matrices indeed satisfy the definition of basis matrices let us record some of the properties of S^0 and S^1.

Property 1. *S^0 and S^1 have $m = \binom{n}{\lfloor n/2 \rfloor}$ columns, and any row in either matrix has weight $\binom{n-1}{\lfloor n/2 \rfloor - 1}$.*

Proof: Follows directly from the definition. ■

Property 2. *Let $X = \{i_1, i_2, \ldots, i_q\}$ be a set of any $q \geq 2$ distinct rows. Then $w(S^0_X) = \binom{n-1}{\lfloor n/2 \rfloor - 1}$, where $w(S^0_X)$ represents the Hamming weight of the OR of the rows $i_1, i_2, \ldots, i_q$ of S^0.*

Proof: Follows directly from the definition of S^0.

■

Property 3. *For $q > n - \lfloor n/2 \rfloor = \lceil n/2 \rceil$, we have that $w(S^1_X) = m$.*
Proof: Since the number of 1's in any column of S^1 is $\lfloor n/2 \rfloor$, the submatrix S^1_X formed by restricting S^1 to a set X of $q > \lceil n/2 \rceil$ rows will have at least one 1 in each of its columns. The Hamming weight of the OR of the rows of S^1_X must therefore be m.

■

Property 4. *For $2 \leq q \leq \lceil n/2 \rceil$,*

$$w(S^1_X) = \left(\begin{array}{c} n \\ \lfloor n/2 \rfloor \end{array} \right) - \left(\begin{array}{c} n-q \\ \lfloor n/2 \rfloor \end{array} \right).$$

Proof: $w(S^1_X)$, in this case, is m minus the number of all zero columns in the submatrix S^1_X. The number of such columns is equal to the number of columns of S^1 in which all the $\lfloor n/2 \rfloor$ 1's are restricted to the $n-q$ rows of submatrix $S^1_{\{1,2,\ldots,n\}-X}$. This number is

$$\left(\begin{array}{c} n-q \\ \lfloor n/2 \rfloor \end{array} \right).$$

■

We now show that S^0 and S^1 are indeed basis matrices. Property 2 of definition 2.2 is obviously satisfied. To prove Property 1, we compute the difference $w(S^1_X) - w(S^0_X)$ (X is a set of q rows $i_1, i_2, \ldots, i_q$). From Properties (3) and (4) above and the identity

$$\left(\begin{array}{c} n \\ k \end{array} \right) = \left(\begin{array}{c} n-1 \\ k-1 \end{array} \right) + \left(\begin{array}{c} n-1 \\ k \end{array} \right)$$

where $1 \leq k \leq n$, we obtain that:

$$w(S^1_X) - w(S^0_X) = \begin{cases} \left(\begin{array}{c} n-1 \\ \lfloor n/2 \rfloor \end{array} \right) - \left(\begin{array}{c} n-q \\ \lfloor n/2 \rfloor \end{array} \right) & \text{if } 2 \leq q \leq \lceil n/2 \rceil \\ \left(\begin{array}{c} n-1 \\ \lfloor n/2 \rfloor \end{array} \right) & \text{if } \lceil n/2 \rceil < q \leq n \end{cases}$$

As can be seen, the quantity $w(S^1_X) - w(S^0_X)$ does not depend on the actual set X but only on its size. Let $\beta(q) = w(S^1_X) - w(S^0_X)$. The quantity $\beta(q)$ is nondecreasing and is minimum at $q = 2$. Define $\alpha(m) = \beta(2)/m$. Hence,

$$\begin{aligned} \alpha(m) \cdot m &= \left(\begin{array}{c} n-1 \\ \lfloor n/2 \rfloor \end{array} \right) - \left(\begin{array}{c} n-2 \\ \lfloor n/2 \rfloor \end{array} \right) \\ &= \left(\begin{array}{c} n-2 \\ \lfloor n/2 \rfloor - 1 \end{array} \right) \end{aligned}$$

Since $m = \binom{n}{\lfloor n/2 \rfloor}$, we get

$$\alpha(m) = \frac{\binom{n-2}{\lfloor n/2 \rfloor - 1}}{\binom{n}{\lfloor n/2 \rfloor}} = \frac{\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)}$$

Let us define $\alpha^*(n) = \frac{\lfloor n/2 \rfloor \lceil n/2 \rceil}{n(n-1)}$. Note that we can express $\alpha^*(n)$ in the following manner:

$$\alpha^*(n) = \begin{cases} \frac{n}{4n(n-1)} & \text{if } n \text{ is even} \\ \frac{n+1}{4n} & \text{if } n \text{ is even} \end{cases}$$

For any set X of at least two participants, if we set $t_X = w(S^1_X)$ and $\alpha(m) = \alpha^*(n)$, then Property 2 of definition 2.2 is satisfied.

Since $\beta(q)$ is nondecreasing, it is obvious that by stacking more than two transparencies, the image recovered becomes more discernible. When we stack $\lfloor n/2 \rfloor < q \leq n$ transparencies we have that

$$\beta(q) = \binom{n-1}{\lfloor n/2 \rfloor}.$$

Since $m = \binom{n}{\lfloor n/2 \rfloor}$, the relative difference in this case is equal to

$$\frac{\beta(q)}{m} = 1 - \left\lfloor \frac{n}{2} \right\rfloor = \begin{cases} \frac{1}{2} & \text{if } n \text{ is even} \\ \frac{1}{2} + \frac{1}{2n} & \text{if } n \text{ is odd} \end{cases}$$

We summarize the above discussion in the following theorem.

Theorem 2.1 *For any $n \geq 2$, there exists a strong $(2, n)-$threshold VCS with pixel expansion $m = \binom{n}{\lfloor n/2 \rfloor}$ and $\alpha(m) = \alpha^*(n)$.*

Example 2.1 Let $n = 4$. Then, the two basis matrices are:

$$S^0 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \qquad S^1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

■

Blundo, De Santis, and Stinson have proved that this scheme achieves an optimal relative difference (see Theorem 4.2 in [4]). We state this theorem without proof.

Theorem 2.2 *Let $n \geq 2$. In any $(2, n)-$threshold VCS with pixel expansion m, it holds that $\alpha(m) \leq \alpha^*(n)$.*

We end this subsection with another theorem by Blundo, De Santis, and Stinson [4] that establishes lower bounds on the pixel expansion m, as a function of n (see Theorem 4.9 in [4]).

Theorem 2.3 *Suppose there exists a $(2, n)-$threshold VCS with pixel expansion m and (optimal) relative difference $\alpha(m) = \alpha^*(n)$. Then*

$$m \geq \begin{cases} 2n-2 & \text{if } n \text{ is even} \\ n & \text{if } n \equiv 3 \bmod 4 \\ 2n & \text{if } n \equiv 1 \bmod 4 \end{cases}$$

2.2.3 $(k, k)-$threshold VCS

The k out of k VCS proposed by Naor and Shamir is optimal with respect to pixel expansion m and relative difference α. The construction is as follows:

Consider a ground set $W = \{1, 2, \ldots, k\}$ of k elements and let $\pi_1, \pi_2, \ldots, \pi_{2^{k-1}}$ be a list of all subsets of W of even cardinality and let $\sigma_1, \sigma_2, \ldots, \sigma_{2^{k-1}}$ be a list of all subsets of W of odd cardinality. Each list defines the following $k \times 2^{k-1}$ boolean matrices S^0 and S^1. For $1 \leq i \leq k$ and $1 \leq j \leq 2^{k-1}$ let $S^0[i, j] = 1$ iff $i \in \pi_j$ and $S^1[i, j] = 1$ iff $i \in \sigma_j$. One can show that these two matrices indeed satisfy the definition of basis matrices for k out of k schemes. We provide a proof of this fact below. The first part of this proof, which deals with contrast, is reproduced verbatim from [11]. The second part deals with security where we have put forward our own argument.

Lemma 2.1 *The above scheme is a k out of k scheme with parameters $m = 2^{k-1}$ and $\alpha = 1/2^{k-1}$.*

Proof: In order to show contrast, note that in the matrix S_0 there is one column that is all 0, the one indexed by the empty set. On the other hand, in S^1 there is no column that is all 0. Therefore, in any permutation of S^0 the OR of the k rows yields only $2^{k-1} - 1$ ones, whereas in any permutation of S^1 the OR of the k rows yields 2^{k-1} ones.

To prove security, consider the matrices T^0 and T^1 obtained by deleting the ith row from S^0 and S^1. We need to show that T^0 and T^1 are identical up to a column permutation. First note that both T^0 and T^1 are $(k-1) \times 2^{k-1}$ matrices. We claim that the columns of T^0 (T^1) describe the set of all subsets of $Y = \{1, \ldots, i-1, i+1, \ldots, k\}$. Recall that the columns of S^0 describe all subsets of $\{1, 2, \ldots, k\}$ of even cardinality. Since T^0 is obtained by deleting the ith row of S^0, each subset of Y of even cardinality is represented by some column in T^0. Let $X \subseteq Y$ be a set of odd cardinality. Then $X \cup \{i\}$ is of even cardinality and is represented by a unique column c in S^0. This column c then represents the set X in the matrix T^0. Hence, every subset of Y is represented by some column in T^0. Since T^0 has 2^{k-1} columns and the cardinality of the power set of Y is also 2^{k-1}, we have actually shown that every subset of Y is represented by a unique column in T^0.

We can repeat this argument for S^1 also. This proves that both T^0 and T^1 have the same structure and one can be obtained from the other by a column permutation. ■

Naor and Shamir go on to prove the optimality of this scheme (see Theorem 4.3 in [11]). We state this theorem without proof.

Theorem 2.4 *In any k out of k scheme $\alpha \leq 1/2^{k-1}$ and $m \geq 2^{k-1}$.*

2.2.4 (k, n)−threshold VCS

The following construction is due to Blundo, De Santis. and Stinson [4] and it makes use of an *initial matrix* which is defined as follows:

Definition 2.3 *Let n, l, k be integers such that $k|n$. An initial matrix $IM(n, l, k)$ is an $n \times l$ matrix whose entries are elements of the ground set $A = \{a_1, a_2, \ldots, a_k\}$, in which the set of columns is equal to the set of vectors in which each element of A appears n/k times.*

The number of columns, l, of an initial matrix $IM(n, l, k)$ is equal to the number of distinct permutations of the word:

$$\underbrace{a_1 \ldots a_1}_{n/k \text{ times}} \cdots \underbrace{a_i \ldots a_i}_{n/k \text{ times}} \cdots \underbrace{a_k \ldots a_k}_{n/k \text{ times}}$$

that is,

$$l = \frac{n!}{\{(n/k)!\}^k}$$

Given an initial matrix $IM(n, l, k)$ we can construct a (k, n)−threshold VCS as follows: The $n \times (l \cdot 2^{k-1})$ basis matrices S^0 and S^1 are constructed by replacing the symbols $a_1, a_2, \ldots, a_k$, respectively with the 1st, ..., kth rows of the corresponding basis matrices of the (k, k)−threshold VCS described in the last subsection (Subsection 2.2.3). The next theorem, which has been quoted from Blundo, De Santis, and Stinson [4], proves that the scheme just described is a (k, n)−threshold VCS. We omit the proof.

Theorem 2.5 *Let n and k be integers such that $2 \leq k \leq n$ and $k|n$. Then the scheme described above is a strong (k, n)−threshold VCS with*

$$m = \frac{n!}{\{(n/k)!\}^k} \cdot 2^{k-1} \quad \text{and} \quad \alpha(m) = \frac{(n/k)^k}{\binom{n}{k} \cdot 2^{k-1}}$$

The previous theorem provides a construction for (k, n)−threshold VCS when $k|n$. To realize a (k, n)−threshold VCS for any values of k and n we can construct, using the above technique, a (k, n_0)−threshold VCS, where $n_0 > n$ and $k|n_0$, and then consider only the first n rows of the basis matrices of this scheme. The resulting scheme has the same parameters as the (k, n_0)−threshold VCS. The next theorem states the existence of (k, n)−threshold VCS for any values of k and n.

Theorem 2.6 *Let k and n be integers such that $2 \leq k \leq n$. Then there exists a strong (k, n)−threshold VCS with*

$$m = \frac{n_0!}{\{(n_0/k)!\}^k} \cdot 2^{k-1} \text{ and } \alpha(m) = \frac{(n_0/k)^k}{\binom{n_0}{k} \cdot 2^{k-1}}$$

where $n_0 = \lceil \frac{n}{k} \rceil \cdot k$.

We end this subsection with a result due to Blundo, De Santis, and Stinson [4] that places bounds on the relative difference and the pixel expansion in any $(k, n)-$threshold scheme realized using basis matrices (see Theorem 6.3 and Corollary 6.6 in [4]).

Theorem 2.7 *For any $(k, n)-$threshold VCS realized using basis matrices, the relative difference $\alpha(m)$ satisfies*

$$\alpha(m) \leq \frac{1}{2^k} + \epsilon$$

where

$$\epsilon = \begin{cases} \frac{1}{2^k(n-k+1)} & \text{if } n-k \text{ is even} \\ \frac{1}{2^k(n-k+2)} & \text{if } n-k \text{ is odd} \end{cases}$$

The pixel expansion m satisfies

$$m = 2^{k-2} \cdot \log(n-k+2).$$

2.3 VCS for General Access Structures

We now present a construction for general access structures based on the ***cumulative array*** method [2]. Let $\Gamma = (\Gamma_{Qual}, \Gamma_{Forb})$ be a strong access structure on the set of participants $\mathcal{P} = \{1, 2, \ldots, n\}$. Recall that in a strong access structure

- Γ_{Qual} is monotone increasing
- Γ_{Forb} is monotone decreasing
- $\Gamma_{Qual} \cup \Gamma_{Qual} = 2^{\mathcal{P}}$

Let Z_M denote the collection of the maximal forbidden sets of Γ:

$$Z_M = \{B \in \Gamma_{Forb} : B \cup \{i\} \in \Gamma_{Qual} \text{ for all } i \in \mathcal{P} - B\}$$

Note that any set $X \in \Gamma_{Forb}$ is a subset of some $B \in Z_M$. A *cumulative map* (β, T) for Γ_{Qual} is a finite set T along with a mapping $\beta : \mathcal{P} \rightarrow 2^T$ such that for $Q \subseteq \mathcal{P}$ we have that

$$\bigcup_{i \in Q} \beta(i) = T \text{ iff } Q \in \Gamma_{Qual}$$

We can construct a cumulative map (β, T) for any Γ_{Qual} by using the collection of maximal forbidden sets $Z_M = \{F_1, F_2, \ldots, F_t\}$ as follows. Let $T = \{T_1, T_2, \ldots, T_t\}$ and for any $i \in \mathcal{P}$ define

$$\beta(i) = \{T_j : i \notin F_j, 1 \leq j \leq t\}.$$

Then if $X \in \Gamma_{Qual}$ we must have $\bigcup_{i \in X} \beta(i) = T$. For if $T_j \notin \bigcup_{i \in X} \beta(i)$ for some $1 \leq j \leq t$, then $X \subseteq F_j$. Since Γ is a strong access structure, this means that $F_j \in \Gamma_{Qual}$ contradicting the fact that $F_j \in \Gamma_{Forb}$. If $X \in \Gamma_{Forb}$, then $X \subseteq T_j$ for some $1 \leq j \leq t$ and so $\bigcup_{i \in X} \beta(i)$ cannot be the whole of T.

From the cumulative mapping for Γ_{Qual} defined above, we can obtain a *cumulative array* for Γ_{Qual}, as follows. A cumulative array is a $|\mathcal{P}| \times |T|$ boolean matrix, denoted by CA, such that $CA(i,j) = 1$ iff $i \notin F_j$.

Example 2.2 Let $\mathcal{P} = \{1,2,3,4\}$, $\Gamma_0 = \{\{1,2\},\{2,3\},\{3,4\}\}$, $Z_M = \{\{1,4\},\{1,3\},\{2,4\}\}$, and let $F_1 = \{1,4\}$, $F_2 = \{1,3\}$, and $F_3 = \{2,4\}$. Therefore, $|T| = 3$. The cumulative array for Γ_{Qual} is the following:

$$CA = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

■

Using the cumulative array we can realize a visual cryptography scheme for any strong access structure. For this, we need to consider the $(k,k)-$threshold VCS of Section 2.2.3. Let Z_M be the set of maximal forbidden sets and let $t = |Z_M|$. Let CA be the cumulative array for Γ_{Qual} obtained using the cumulative map. Let $\widehat{S}^0$ and $\widehat{S}^1$ be the basis matrices for a $(t,t)-$threshold VCS. The basis matrices S^0 and S^1 for a VCS for the access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ is constructed as follows. For any fixed row i of CA, let $j_1, \ldots, j_p$ be the integers j such that $CA(i,j) = 1$. The i-th row of S^0 (S^1 resp.) consists of the OR of the rows $j_1, \ldots, j_p$ of $\widehat{S}^0$ ($\widehat{S}^1$ resp.). An example will illustrate the technique.

Example 2.3 Let $\mathcal{P} = \{1,2,3,4\}$, $\Gamma_0 = \{\{1,2\},\{2,3\},\{3,4\}\}$, $Z_M = \{\{1,4\},\{1,3\},\{2,4\}\}$, and let $F_1 = \{1,4\}$, $F_2 = \{1,3\}$, and $F_3 = \{2,4\}$. Hence, $|T| = 3$. Let $\widehat{S}^0$ and $\widehat{S}^1$ be

$$\widehat{S}^0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \qquad \widehat{S}^1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

The basis matrices S^0 and S^1 in a VCS realizing the strong access structure with basis Γ_0 are:

$$S^0 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \qquad S^1 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

The second row of S^0 is the OR of the rows 1 and 2 of $\widehat{S}^0$, that is,

$$[0,1,1,1] = [0,1,1,0]\ OR\ [0,1,0,1],$$

and the third row of S^0 is the OR of rows 1 and 3 of $\widehat{S}^0$. The first and fourth rows of S^0 are equal to rows 3 and 2 of $\widehat{S}^0$, respectively, and similarly for $\widehat{S}^1$.

■

The next theorem summarizes the above discussion (see Theorem 4.2 in [2]).

Theorem 2.8 *Let $\Gamma = (\Gamma_{Qual}, \Gamma_{Forb})$ be a strong access structure on the set of participants $\mathcal{P} = \{1,2,\ldots,n\}$, and let Z_M be the family of the maximal forbidden sets in Γ_{Forb}. Then there exists a $(\Gamma_{Qual}, \Gamma_{Forb}, m)-VCS$ with $m = 2^{|Z_M|-1}$ and $t_X = m$ for any $X \in \Gamma_{Qual}$.*

Chapter 3

Grey Level and Color VCS

3.1 Grey Level VCS

In this section we present constructions for grey-level visual cryptography schemes due to Blundo, De Santis, and Naor [5]. A survey of existing results on grey-level visual cryptography schemes is provided by MacPherson [10]. The material in this section is based on these references.

3.1.1 The Model

We begin by defining what we mean by a visual cryptography scheme with g grey levels.

Definition 3.1 *Let $(\Gamma_{Qual}, \Gamma_{Forb})$ be an access structure on n participants and let $g \geq 2$ be an integer. The g collections of $n \times m$ boolean matrices $C_0, C_1, \ldots, C_{g-1}$ form a visual cryptography scheme with g grey levels and pixel expansion m if there exist values $\alpha_0, \ldots, \alpha_{g-2}$ and sets $\{X, t_{i,X}\}_{X \in \Gamma_{Qual}}$ for $0 \leq i \leq g-2$ satisfying the following conditions:*

1. *Any $X = \{j_1, \ldots, j_p\} \in \Gamma_{Qual}$ can recover the shared image by combining their shares. Formally, for $i = 0, \ldots, g-2$ for any $M \in C_i$ and any $N \in C_{i+1}$ the OR V of rows $j_1, \ldots, j_p$ satisfies:*

$$w(V_M) \leq t_{i,X} - \alpha_i \cdot m \quad \text{and} \quad w(V_N) \geq t_{i,X}$$

2. *Any $X = \{j_1, \ldots, j_p\} \in \Gamma_{Forb}$ has no information on the shared image. Formally, the g collections of $p \times m$ matrices D_i, $0 \leq i \leq g-1$, obtained by restricting each $n \times m$ matrix in C_i to rows $j_1, \ldots, j_p$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.*

Note that for each pair of adjacent grey levels i and $i+1$, $0 \leq i \leq g-2$, we have a set of thresholds $\{t_X\}$ and a relative difference. The first property ensures that the participants will be able to distinguish the g grey levels. The quantity $\alpha_i \cdot m$ is known as the contrast for grey level i $(0 \leq i \leq g-2)$. We require that $\alpha_i \cdot m \geq 1$, $0 \leq i \leq g-2$ to ensure that the participants can distinguish all the grey levels.

The second property ensures the security of the scheme. Even by inspecting all their shares, a forbidden set of participants cannot gain any information on the secret image.

We rewrite the above definition in terms of basis matrices.

Definition 3.2 *Let $(\Gamma_{Qual}, \Gamma_{Forb})$ be an access structure on n participants and let $g \geq 2$ be an integer. The g $n \times m$ boolean matrices $G_0, G_1, \ldots, G_{g-1}$ form a visual cryptography scheme with g grey levels and pixel expansion m if there exist values $\alpha_0, \ldots, \alpha_{g-2}$ and sets $\{X, t_{i,X}\}_{X \in \Gamma_{Qual}}$ for $0 \leq i \leq g-2$ satisfying the following conditions:*

1. *If $X = \{j_1, \ldots, j_p\} \in \Gamma_{Qual}$ then for $0 \leq i \leq g-2$, the OR V of rows $j_1, \ldots, j_p$ of G_i satisfies $w(V) \leq t_{i,X} - \alpha_i \cdot m$; whereas for G_{i+1} we have that $w(V) \geq t_{i,X}$.*
2. *If $X = \{j_1, \ldots, j_p\} \in \Gamma_{Forb}$ then the g $p \times m$ matrices $G'_0, \ldots, G'_{g-1}$ obtained by restricting them to rows $j_1, \ldots, j_p$ are equal up to a column permutation.*

The collections of matrices C_i in Definition 3.1 may be obtained by generating all column permutations of the basis matrices G_i.

Blundo, De Santis, and Stinson [5] also prove the following result that establishes the optimal pixel expansion for any (k, k) threshold scheme. In what follows, a $(k, n)-$GVCS with pixel expansion m and g grey levels is denoted by $(k, n, m, g)-$GVCS.

Lemma 3.1 *In any $(k, k, m, g)-GVCS$ with relative differences $\alpha_0, \ldots, \alpha_{g-2}$, we have*

$$\min\{\alpha_0, \ldots, \alpha_{g-2}\} \leq 1/(g-2) \cdot 2^{k-1}$$

and

$$m \geq (g-1) \cdot 2^{k-1}$$

3.1.2 An optimal (k, k) threshold construction

We can use the optimal $(k, k)-$VCS from Naor and Shamir [11] to create a GVCS with pixel expansion $m = (g-1) \cdot 2^{k-1}$. For each grey level i, we assume that a pixel with grey level i is a union of i black subpixels and $g-i-1$ white subpixels. We begin with an optimal $(k, k)-$VCS which has the basis matrices S_0 and S_1 and pixel expansion $m' = 2^{k-1}$. The basis matrices G_i are simply the concatenation of $g-i-1$ copies of S_0 and i copies of S_1.

$$G_i = \underbrace{S_0 \circ \ldots \circ S_0}_{g-i-1} \circ \underbrace{S_1 \circ \ldots \circ S_1}_{i}$$

We define the set of threshold values $\{t_{i,X}\}$ to be $t_{i,X} = (g-1) \cdot m' - g + i + 1$ and relative differences $\alpha_i = 1/m$. Since we are concatenating $g-1$ matrices, the pixel expansion is $m = (g-1) \cdot 2^{k-1}$, which is optimal.

Theorem 3.1 *The construction described above is a $(k, k, g, m)-GVCS$ with pixel expansion $m = (g-1) \cdot 2^{k-1}$ with the set of thresholds $t_i = m - g + i + 2$ and relative difference $\alpha_i = 1/m$.*

Proof: For $0 \leq i \leq g-1$, the weight of the OR V of all k rows of G_i is

$$\begin{aligned} w(V) &= (g-i-1) \cdot (m'-1) + i \cdot m' \\ &= (g-1) \cdot m' - g + i + 1 \\ &= m - g + i + 1 \end{aligned}$$

Since for $0 \leq i \leq g-2$, $t_{i,X} = m - g + i + 2$ and $\alpha_i \cdot m = 1$, we have that

$$t_{i,X} - \alpha_i \cdot m = m - g + i + 1$$

Therefore, we have $w(V) \leq t_{i,X} - \alpha_i \cdot m$ as required. If we compute the OR V of all k rows on the matrix G_{i+1}, we have

$$w(V) = m - g + (i+1) + 1 = m - g + i + 2$$

Therefore, $w(V) \geq t_{i,X}$, and Property 1 of Definition 3.2 is satisfied.

To prove Property 2, we consider each adjacent pair of basis matrices G_i, G_{i+1} for $0 \leq i \leq g-2$. Let $X \subset \mathcal{P}$, where $|X| < k$. Then G_i contains $g-i-1$ copies of S_0 and i copies of S_1, and G_{i+1} contains $g-i-2$ copies of S_0 and $i+1$ copies of S_1. Since each contains $g-i-2$ copies of S_0 and i copies of S_1, these columns are clearly equal for any choice of participants X. The remaining columns of G_i are equal to S_0 and those of G_{i+1} are equal to S_1. But $S_0[X] = S_1[X]$ up to a column permutation, and therefore $G_i[X] = G_{i+1}[X]$ up to a column permutation. Since this is true for any $0 \leq i \leq g-2$, we have that all $G_i[X]$ are equal up to a column permutation for $0 \leq i \leq g-1$. This proves Property 2, and therefore, the construction is a valid GVCS.

■

3.1.3 A (k, n) threshold construction

The $(k, n)-$threshold construction described here makes use of *starting matrices*, which we define below.

Definition 3.3 *A starting matrix $SM(n, l, k)$ is an $n \times l$ matrix whose entries are elements of the ground set $G = \{a_1, \ldots, a_k\}$, with the property that for any subset $X = \{i_1, \ldots, i_k\}$ of k rows, the submatrix $SM[X]$ has at least one column whose entries are all distinct.*

Given a starting matrix $SM(n, l, k)$, we can construct a $(k, n)-$threshold GVCS as follows: the $n \times (l \cdot (g-1) \cdot 2^{k-1})$ basis matrices $G_0, \ldots, G_{g-1}$ are constructed by replacing the symbols $a_1, \ldots, a_k$ with the 1st, ..., k-th rows of the corresponding basis matrices of the optimal $(k, k)-$GVCS, respectively described in the last section.

Theorem 3.2 *Given a starting matrix $SM(n, l, k)$, there exist basis matrices for a (k, n, g, m) $-$threshold GVCS with pixel expansion $m = l \cdot (g-1) \cdot 2^{k-1}$.*

Proof: Let $G_0^k, \ldots, G_{g-1}^k$ be the basis matrices of an optimal $(k, k)-$GVCS and let $SM(n, l, k)$ be a starting matrix whose entries are elements of a ground set $\{a_1, \ldots, a_k\}$. Let $G_0, \ldots, G_{g-1}$ be $n \times (l \cdot (g-1) \cdot 2^{k-1})$ matrices constructed by replacing the symbols $\{a_1, \ldots, a_k\}$ with the 1st, ..., k-th rows of $G_0^k, \ldots, G_{g-1}^k$, respectively.

To prove Property 1 of Definition 3.2, we consider the basic block $B_{i,j}$ which is the $n \times ((g-1) \cdot 2^{k-1})$ matrix obtained by expanding column j of the starting matrix using G_i^k. Choose any adjacent pair of basic blocks $B_{i,j}, B_{i+1,j}$ (from adjacent matrices G_i and G_{i+1}). Consider any $d \geq k$ rows of the basic blocks. There are two cases: Either these d rows include all the rows of G_i^k (G_{i+1}^k resp.), where a row may appear more than once; or the d rows contain

at most $(k-1)$ distinct rows. In the first case, the OR of the rows has weight $t_i - 1$ (t_i resp.): in the second case, the OR of the rows has the same weight in both basic blocks. Since the first situation will be true for at least one j for any choice of $d \geq k$ rows, Property 1 of Definition 3.2 is satisfied.

To prove Property 2, we need to show that for any $X \subseteq \{1, \ldots, n\}$ with $|X| < k$, we have that $G_0[X] = \ldots = G_{g-1}[X]$ up to a column permutation. This is true since $B_{0,j} = \ldots = B_{g-1,j}$ up to a column permutation for all $1 \leq j \leq l$.

■

3.2 Color VCS

Until recently, most of the research on visual cryptography concentrated on black and white visual cryptography schemes. Lately, there have been some papers on grey-level visual cryptography schemes, but research on color schemes has been very limited with only a few papers available on the subject (see [7, 8, 9]). Color visual cryptography is inherently more complicated than black and white visual cryptography for a number of reasons.

Firstly, the rules of color combination, which are so simple for black and white images, are considerably more complex for color images. Secondly, if one tries to construct basis matrices for a color visual cryptography scheme keeping the security property intact, then one finds that the pixel expansion necessarily becomes very large. This situation is compounded by the fact that in the recovered image, only a small proportion of the subpixels retain the color of the original shared pixel. Together, these two effects serve to diminish the brightness of the recovered image. This is not a problem in black and white or grey-level visual cryptography schemes, but it becomes painfully obvious when the image is colored. Hence although (k, n) schemes have been proposed for color images, none of them are efficient in terms of producing a clean reconstructed image.

In this section, we review color VCS proposed in [7]. The model proposed in this paper (and also in [8, 9]) are based on a finite lattice (see the next section for a definition of a finite lattice). But first, we introduce a parameter called the *color ratio* which we will use to measure the brightness of the recovered image in a color VCS.

Definition 3.4 *Let us assume that we have a $(k, n)-$threshold VCS for color images with the color set $C = \{c_1, \ldots, c_K\}$. The color ratio of this VCS is the set $\{R_{c_i}\}_{i=1}^{K}$ where for $1 \leq i \leq K$,*

$$R_{c_i} = \frac{\textit{the number of subpixels that have the color } c_i}{\textit{the pixel expansion } m}.$$

This ratio is evaluated for a pixel of color c_i in the reconstructed image.

In comparing two color VCS with the same color set C, we could use the minimum value of the set $\{R_{c_i}\}_{i=1}^{K}$ as a benchmark in deciding which scheme is better. We will denote $\min_{1 \leq i \leq K}\{R_{c_i}\}$ by R. Note that R denotes the lower bound on the color ratio of any color c_i that the scheme supports.

We next describe the rules of color combination. There are two ways to interpret and produce color. We may add together light sources, each of which produces light with its own distribution of frequencies. This method of producing color is called *additive color* and is how

Additive Colors	*Subtractive Colors*
Red	Cyan
Green	Yellow
Blue	Magenta
Red + Green = Yellow	Cyan + Yellow = Green
Red + Blue = Magenta	Cyan + Magenta = Blue
Green + Blue = Cyan	Yellow + Magenta = Red
Red + Green + Blue = White	Cyan + Yellow + Magenta = Black

Figure 3.1: Table showing additive and subtractive colors

color is produced by a CRT, for example. In the additive case, there are three primary colors- red, green, and blue. The combination of these colors produces the colors shown in the first column of the table in Figure 3.1.

The second way to produce color is to start with a source of white light (which contains all the visible frequencies), and then remove colors by filters. This method of producing colors, called *subtractive color*, is the way colors are produced by natural phenomena. For example, grass is green because it absorbs other frequencies but reflects frequencies in the green range. In subtractive systems, the complimentary colors of cyan, magenta, and yellow are considered to be primaries and the rules of color combination are as in the second column of the table in Figure 3.1. In visual cryptography, color is produced by the subtractive process and so, from now on, our primary colors will be cyan, magenta, and yellow.

3.2.1 Lattice-based $(k, n)-$VCS

We begin with a few definitions. A *partial ordering* of a set L is a binary relation $\leq$ on L which satisfies the following properties for all a_1, a_2, and a_3 in L:

1. $a_1 \leq a_2$ (reflexive).

2. If $a_1 \leq a_2$ and $a_2 \leq a_3$, then $a_1 \leq a_3$ (transitive).

3. If $a_1 \leq a_2$ and $a_2 \leq a_1$, then $a_1 = a_2$ (anti-symmetric).

A set L equipped with such a relation is called a partially ordered set (or a poset).

If A is a subset of a poset L, then an *upper bound* for A is an element $b \in L$ such that $a \leq b$ for all $a \in A$. A *least upper bound* (l.u.b) of A is an upper bound b_0 of A such that $b_0 \leq b$ for every other upper bound b of A. The notions of a lower bound and greatest lower bound (g.l.b) may be defined similarly.

A poset $(L, \leq)$ is called a *lattice* if for all $a, b \in L$, the set $\{a, b\}$ has both a l.u.b and a g.l.b. A poset $(L, \leq)$ is called an *upper semi-lattice* if for all $a, b \in L$ the set $\{a, b\}$ has a l.u.b. If $(L, \leq)$ is an upper semi-lattice then the *join* (denoted by $\sqcup$) of L is a binary operation on L defined as follows: For $x, y \in L$,

$$x \sqcup y = \text{least upper bound of } \{x, y\}.$$

An upper semi-lattice is said to be *bounded* if it contains the least element 0 and the greatest element 1 such that

$$x \sqcup 0 = x \quad \text{and} \quad x \sqcup 1 = 1$$

for all $x \in L$. It is easy to see that if L is a bounded upper semi-lattice and m an integer ≥ 1, then the m-th Cartesian product L^m is also a bounded upper semi-lattice if the join $\sqcup_m$ of L^m is defined as

$$(x_1, \ldots x_m) \sqcup_m (y_1, \ldots, y_m) = (x_1 \sqcup y_1, \ldots, x_m \sqcup y_m).$$

The least and greatest elements of L^m are

$$\underbrace{(0 \ldots, 0)}_{m \text{ copies}} \quad \text{and} \quad \underbrace{1, \ldots, 1}_{m \text{ copies}},$$

respectively.

We associate the elements of a bounded upper semi-lattice L, with a set of colors. The physical operation of mixing two colors $c_1, c_2 \in L$, in the sense of taking two transparencies of colors c_1 and c_2 and stacking them on top of one another, corresponds to finding the least upper bound of $\{c_1, c_2\}$. We use a bounded semi-lattice since in practice, if we mix any color with black (1) we get black; mixing any color with white (0) gives us back our original color. A bounded upper semi-lattice takes into account these two situations.

We are now ready to define a lattice-based $(k, n)-$VCS. Let L be a bounded upper semi-lattice of colors and let $m \geq 2$ be an integer. Define $\mathcal{C} = \{c_1, \ldots, c_K\} \subseteq L$ to be the set of colors that the secret image contains. This subset need not be a sublattice of L. Let $\mathcal{P}$ be a set of n participants. We can view an element of $(L^m)^n$ as an $n \times m$ matrix S whose entries are elements of L. For $1 \leq p \leq n$ and $A = \{i_1, \ldots, i_p\} \subseteq \mathcal{P}$ define $S[A]$ to be the $p \times m$ matrix obtained by restricting S to rows $i_1, \ldots, i_p$. For such a p and A define the mapping $h : (L^m)^n \to L^m$ as

$$h(S[A]) = \bar{s}_{i_1} \sqcup_m s_{i_2} \sqcup_m \ldots \sqcup_m s_{i_p}$$

where $\bar{s}_{i_j}$ denotes the i_j-th row of matrix S and $\sqcup_m$ denotes the join of L^m defined previously. Note that h describes the physical operation of stacking the shares of the i_1th, $\ldots . i_p$th participants.

A lattice-based visual cryptography scheme for an access structure Γ is defined as follows:

Definition 3.5 *Let $\Gamma = (\Gamma_{Qual}, \Gamma_{Forb})$ be an access structure on a set $\mathcal{P}$ of participants. Let L be a bounded upper semi-lattice of colors and $\mathcal{C} = \{c_1, \ldots, c_K\}$ a subset of L. Let $\mathcal{X}_{c_i}$ $(1 \leq i \leq K)$ denote a collection of $n \times m$ matrices with elements from L. The set $\{\mathcal{X}_{c_i}\}_{i=1}^{K}$ is called a lattice-based visual cryptography scheme for the access structure Γ with colors $\mathcal{C}$ and pixel expansion m if the following two properties hold:*

1. *For each $1 \leq i \leq K$, if $A \in \Gamma^*_{Qual}$ and $S \in \mathcal{X}_{c_i}$, then $h(S[A]) \in L^m$ contains only 1s and at least one c_i. Γ^*_{Qual} is a minimum qualified set of Γ_{Qual}.*

2. *If $A \in \Gamma^*_{Forb}$, then the sets $\mathcal{X}_{c_i}[A]$ $(1 \leq i \leq K)$ are indistinguishable in the sense that they contain the same elements with the same frequencies. $\mathcal{X}_{c_i}[A]$ is defined as*

$$\mathcal{X}_{c_i}[A] = \{S[A] : S \in \mathcal{X}_{c_i}\}.$$

Γ^*_{Forb} refers to the maximal forbidden sets of Γ_{Forb}.

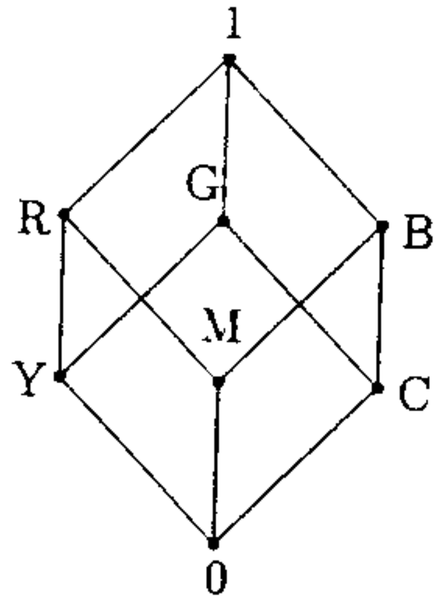

Figure 3.2: Hasse diagram of the bounded upper semi-lattice L_{color}

Property 1 of the above definition simply says that any subset of qualified participants can recover the shared image. Property 2 deals with security and ensures that no forbidden set of participants can gain any information about the shared image.

To encrypt a secret image into n shares we do the following: for each pixel P (of color, say, c_j) in the secret image, we choose an $S \in \mathcal{X}_{c_j}$ at random. The rows of S describe the shares distributed to the n participants. We repeat this step until all the pixels in the secret image are encrypted.

3.2.2 An (n, n) construction

In order to construct a lattice-based (n, n)–VCS for the color set $\mathcal{C} = \{c_1, \ldots, c_K\}$, it is necessary to choose a finite lattice L such that $\mathcal{C} \subseteq L$, and the collections of $n \times m$ matrices $\{\mathcal{X}_{c_i}\}_{i=1}^{K}$ appropriately. At this point, we will introduce the finite lattice L_{color} shown in Figure 3.2. L_{color} has the following colors as its elements: 0 (white), Y (yellow), M (magenta), C (cyan), R (red), G (green), B (blue), and 1 (black). The Hasse diagram shows that Y⊔M = R, Y⊔C = G, M⊔C = B, and R⊔C = G⊔M = B⊔Y = 1. In this section, we will use L_{color} and its sublattices in the constructions.

A simple (2,2) construction

Let L_{YCG} denote the sublattice of L_{color} composed of the elements $\{0, Y, C, G, 1\}$. We let $L = L_{YCG}$, $m = 4$ and $\mathcal{C} = \{Y, C, G\}$. The elements of $\mathcal{X}_Y$, $\mathcal{X}_C$, and $\mathcal{X}_G$ can be obtained by permuting the columns of the basis matrices S_Y, S_C, and S_G, respectively, given below:

$$S_Y = \begin{bmatrix} Y & 0 & 1 & C \\ 0 & Y & C & 1 \end{bmatrix}, \qquad S_C = \begin{bmatrix} C & 0 & 1 & Y \\ 0 & C & Y & 1 \end{bmatrix},$$

$$S_G = \begin{bmatrix} Y & C & 1 & 0 \\ C & Y & 0 & 1 \end{bmatrix}.$$

When we stack two shares together, only two out of a total of four subpixels have the color of the original shared pixel; the remaining two are black. The color ratios R_Y, R_C, and R_G are therefore each equal to $2/4 = 1/2$.

If we let $L = L_{color}$, $C = \{0, Y, C, M, R, G, B, 1\}$, and $m = 8$, the sets $\mathcal{X}_{c_i}$ ($c_i \in C$) can be realized by considering all possible column permutations of the basis matrices S_{c_i} defined below:

$$S_0 = \begin{bmatrix} 0 & Y & M & C & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & Y & M & C & 1 \end{bmatrix},$$

$$S_Y = \begin{bmatrix} Y & 0 & M & C & 1 & 1 & 1 & 1 \\ 0 & Y & 1 & 1 & M & C & 1 & 1 \end{bmatrix},$$

$$S_M = \begin{bmatrix} M & 0 & C & Y & 1 & 1 & 1 & 1 \\ 0 & M & 1 & 1 & C & Y & 1 & 1 \end{bmatrix},$$

$$S_C = \begin{bmatrix} C & 0 & Y & M & 1 & 1 & 1 & 1 \\ 0 & C & 1 & 1 & Y & M & 1 & 1 \end{bmatrix},$$

$$S_R = \begin{bmatrix} Y & M & C & 0 & 1 & 1 & 1 & 1 \\ M & Y & 1 & 1 & C & 0 & 1 & 1 \end{bmatrix},$$

$$S_G = \begin{bmatrix} C & Y & M & 0 & 1 & 1 & 1 & 1 \\ Y & C & 1 & 1 & M & 0 & 1 & 1 \end{bmatrix},$$

$$S_B = \begin{bmatrix} M & C & Y & 0 & 1 & 1 & 1 & 1 \\ C & M & 1 & 1 & Y & 0 & 1 & 1 \end{bmatrix},$$

$$S_1 = \begin{bmatrix} Y & M & C & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & Y & M & C & 0 \end{bmatrix}.$$

In this case, if we stack two shares of a pixel of color c_i ($c_i \in \{Y, M, C, R, G, B\}$), only two subpixels out of a total of 8 have the color of the original shared pixel. The color ratios R_{c_i}'s ($c_i \in \{Y, M, C, R, G, B\}$) are therefore each equal to $2/8 = 1/4$. Clearly, $R_0 = 1/8$ and $R_1 = 1$.

A simple (n, n) construction

The construction we now describe uses the basis matrices of the (n, n)−threshold scheme proposed by Naor and Shamir [11]. See Chapter 2 Section 2.2.3 for an explanation of this scheme. We will illustrate the technique used to construct the basis matrices of the (n, n) lattice-based scheme with an example.

Let $n = 3$. Then the basis matrices S_0 and S_1 of Naor and Shamir's (n, n) scheme are:

$$S_0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \qquad S_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

Define $S_0(x)$ and $S_1(x)$ by

$$S_0(x) = \begin{bmatrix} x & x & 1 & 1 \\ x & 1 & x & 1 \\ x & 1 & 1 & x \end{bmatrix} \qquad S_1(x) = \begin{bmatrix} 1 & x & x \\ x & 1 & x \\ x & x & 1 \end{bmatrix}$$

$S_0(x)$ is obtained by replacing 0's by x's; $S_1(x)$ is obtained in a similar fashion but by deleting the all 1 column. Let $L = L_{YCG}$ and $C = \{Y, C, G\}$. The basis matrices S_Y, S_C, and S_G are as defined below:

$$\begin{aligned} S_Y &= S_0(Y) \circ S_1(C) \circ S_1(G) \\ S_C &= S_0(C) \circ S_1(Y) \circ S_1(G) \\ S_G &= S_0(G) \circ S_1(C) \circ S_1(Y) \end{aligned}$$

Here $\circ$ denotes concatenation of matrices.

If n is even, the all 1 column appears in S_0 and in forming $S_0(x)$ we would have to drop this column from S_0 and then replace 0's by x's. When $|C| = K$, the pixel expansion of the scheme is:

$$m = \begin{cases} K \cdot 2^{n-1} - 1, & \text{if } n \text{ is even} \\ K \cdot 2^{n-1} - (K-1), & \text{if } n \text{ is odd} \end{cases}$$

The color ratio $R = 1/m$.

3.2.3 A (k, n) construction

We now present a lattice-based $(k, n)-$VCS due to Koga and Yamamoto [7]. This construction uses two matrices $A(x)$ and $D(x)$ which play the same role as $S_0(x)$ and $S_1(x)$, respectively, where $S_0(x)$ and $S_1(x)$ are the matrices introduced in last section. If the color set $C = \{Y, C\}$, then the basis matrices S_Y and S_C are defined as:

$$\begin{aligned} S_Y &= A(Y) \circ D(C) \\ S_C &= A(C) \circ D(Y) \end{aligned}$$

$A(x)$ and $D(x)$ are designed so that the l.u.b of any k rows of $A(x)$ consists of only x's and 1's while that of $D(x)$ consists of only 1's. Any collection of $(k-1)$ rows of $A(Y) \circ D(C)$ and $A(C) \circ D(Y)$ are identical in the sense that one can be obtained from the other by a sequence of column transpositions. If the color set is $C = \{c_1, \ldots, c_K\}$, the basis matrices S_{c_i} ($c_i \in \{c_1, \ldots, c_K\}$) are defined as follows:

$$S_{c_i} = A(c_i) \circ D(c_1) \circ \ldots \circ D(c_{i-1}) \circ D(c_{i+1}) \circ \ldots \circ D(c_K)$$

Before we describe the construction, let us set up our notation. For $j = 1, 2, \ldots, n$, define $M_{n,n-j}(x)$ as the matrix obtained by permuting a column containing one x, $n-j$ 0's, and $j-1$ 1's in all possible ways. As an example, for $n = 3$, $M_{3,2}(x)$, $M_{3,1}(x)$, and $M_{3,0}(x)$ can be written as:

$$M_{3,2}(x) = \begin{bmatrix} x & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x \end{bmatrix}$$

$$M_{3,1}(x) = \begin{bmatrix} x & x & 0 & 1 & 0 & 1 \\ 0 & 1 & x & x & 1 & 0 \\ 1 & 0 & 1 & 0 & x & x \end{bmatrix}$$

$$M_{3,0}(x) = \begin{bmatrix} x & 1 & 1 \\ 1 & x & 1 \\ 1 & 1 & x \end{bmatrix}$$

Clearly. $M_{n,n-j}(x)$ has l columns where

$$\begin{aligned} l &= \frac{n!}{(n-j)!\,(j-1)!} \\ &= j \cdot \binom{n}{j} \end{aligned}$$

If M is a matrix and $\alpha \geq 1$ an integer, $M^{[\alpha]}$ denotes the matrix obtained by concatenating M with itself α times.

$$M^{[\alpha]} = \underbrace{M \circ M \circ \ldots \circ M}_{\alpha \text{ times}}.$$

We state without proof how $A(x)$ and $D(x)$ can be defined under various situations. In each case, we assume the color set to be $\mathcal{C} = \{Y, C\}$.

The (n, n) case

For n odd,

$$\begin{aligned} A(x) &= M_{n,n-1}(x) \circ M_{n,n-3}(x) \circ \ldots \circ M_{n,0}(x), \\ D(x) &= M_{n,n-2}(x) \circ M_{n,n-4}(x) \circ \ldots \circ M_{n,1}(x). \end{aligned}$$

For n even,

$$\begin{aligned} A(x) &= M_{n,n-1}(x) \circ M_{n,n-3}(x) \circ \ldots \circ M_{n,1}(x), \\ D(x) &= M_{n,n-2}(x) \circ M_{n,n-4}(x) \circ \ldots \circ M_{n,0}(x). \end{aligned}$$

The number of columns in $A(x)$ is

$$\binom{n}{1} + 3\binom{n}{3} + 5\binom{n}{5} + \ldots$$

The number of columns in $D(x)$ is

$$2\binom{n}{2} + 4\binom{n}{4} + 6\binom{n}{6} + \ldots$$

To count the number of columns in $A(x)$ and $D(x)$ we need a few identities involving binomial coefficients. First note that

$$n\binom{n-1}{k} = (k+1)\binom{n}{k+1}$$

Expanding $n \cdot (1+b)^{n-1}$ by the binomial theorem and using the above identity we obtain:

$$\begin{aligned} n(1+b)^{n-1} &= n\left\{\binom{n-1}{0} b^0 + \binom{n-1}{1} b^1 + \ldots + \binom{n-1}{n-1} b^{n-1}\right\} \\ &= 1\binom{n-1}{k} b^0 + 2\binom{n-1}{k} b^1 + \ldots + n\binom{n-1}{k} b^{n-1} \end{aligned}$$

If we let $b = 1$, we obtain the identity:

$$\binom{n}{1} + 2\binom{n}{2} + \ldots - n\binom{n}{n} = n \cdot 2^{n-1}$$

On the other hand if we let $b = -1$, we obtain the identity:

$$\begin{aligned}\binom{n}{1} + 3\binom{n}{3} + \ldots &= 2\binom{n}{2} + 4\binom{n}{4} + \ldots \\ &= n \cdot 2^{n-2}\end{aligned}$$

Now it is easy to see that:

1. The number of columns in $A(x)$ $(D(x))$ is $n \cdot 2^{n-2}$ and that in $A(x) \circ D(x)$ is $n \cdot 2^{n-1}$.
2. The l.u.b of n rows of $A(x) \circ D(x)$ contains n x's.
3. The color ratio of this scheme is $R = n/n \cdot 2^{n-1} = 1/2^{n-1}$.

The $(n-1, n)$ case

For n odd,

$$\begin{aligned}A(x) &= M_{n,n-2}(x) \circ M^{[3]}_{n,n-4}(x) \circ \ldots \circ M^{[n-2]}_{n,1}(x), \\ D(x) &= M^{[2]}_{n,n-3}(x) \circ M^{[4]}_{n,n-5}(x) \circ \ldots \circ M^{n-1}_{n,0}(x).\end{aligned}$$

For n even,

$$\begin{aligned}A(x) &= M_{n,n-2}(x) \circ M^{[3]}_{n,n-4}(x) \circ \ldots \circ M^{[n-1]}_{n,0}(x), \\ D(x) &= M^{[2]}_{n,n-3}(x) \circ M^{[4]}_{n,n-5}(x) \circ \ldots \circ M^{n-2}_{n,1}(x).\end{aligned}$$

The number of columns of $A(x) \circ D(x)$ is $n(n-1)2^{n-2}$, while the l.u.b of any set of $(n-1)$ rows contains $(n-1)$ x's. The color ratio R is therefore $1/n \cdot 2^{n-2}$.

The $(2, n)$ case

In this case,

$$\begin{aligned}A(x) &= M_{n,1}(x) \\ D(x) &= M^{[n-1]}_{n,0}(x)\end{aligned}$$

$A(x)$ and $D(x)$ each have $n(n-1)$ columns. The l.u.b of two arbitrary rows contains two x's. The color ratio R is $1/n(n-1)$.

The (k, n) case

For $3 \leq k \leq n-2$, Koga and Yamamoto have shown the existence of a sequence of integers $\{\alpha_i\}_{i=1}^{K}$ which can be used to define $A(x)$ and $D(x)$ in the manner shown below:

$$\begin{aligned} A(x) &= M_{n,k-1}^{[\alpha_1]}(x) \circ M_{n,k-3}^{[\alpha_3]}(x) \circ \ldots \circ M_{n,1}^{[\alpha_{k-1}]}(x), \\ D(x) &= M_{n,k-2}^{[\alpha_2]}(x) \circ M_{n,n-4}^{[\alpha_4]}(x) \circ \ldots \circ M_{n,0}^{\alpha_k}(x). \end{aligned}$$

Here we have assumed k to be even. For k even, there is a similar construction.

What Koga and Yamamoto have been unable to show is the positiveness of the sequence $\{\alpha_i\}_{i=1}^{k}$. However, they note that it is not necessary for each α_i to be positive. For if $A(x)$ includes $M_{n,k-j}^{[\alpha_j]}(x)$ with $\alpha_i < 0$, one should remove $M_{n,k-j}^{[\alpha_j]}(x)$ from $A(x)$ and concatenate it with $D(x)$. If $\alpha_i = 0$, $M_{n,k-j}^{[\alpha_j]}(x)$ need not be concatenated with $A(x)$ in the first place. The same operation should be applied to $D(x)$ if it includes $M_{n,k-j}^{[\alpha_j]}(x)$ with $\alpha_i \leq 0$.

Chapter 4

A New $(2, n)-$Threshold VCS for Color Images

In this chapter, we propose a $(2, n)-$ threshold VCS for color images. Our scheme has the following advantages:

1. Our scheme provides a lower bound on the color ratio. For instance, if the secret image is composed of the colors cyan, yellow and green, then the color ratio of our scheme is lower bounded by 1/4. This lower bound depends only on the number of colors in the secret image and is *independent* of the number of shares. Other schemes dealing with color images can provide no such lower bound (see [8], [9]).

2. The color ratio of our scheme is very high compared to what other schemes can provide. The result is that our images are brighter. If the secret image has the colors $\mathcal{C} = \{c_1, c_2, \ldots, c_k\}$ such that no two colors c_i and $c_j \in \mathcal{C}$ can be combined to produce a third color $c_k \in \mathcal{C}$, then the color ratio of our scheme is lower bounded by $1/2k$. Compare this with the color ratio $2/k \cdot n(n-1)$, which is what the scheme proposed by Koga ([7]) achieves. The scheme proposed by Koga in 2001, ([9]), achieves a color ratio of $1/k \cdot 2^{n-2} \cdot \binom{n}{t}$.

3. The pixel expansion of our scheme is reasonably good. If the secret image consists of colors cyan, yellow and green, then the pixel expansion is $4m$ where

$$m = \binom{n}{\lfloor n/2 \rfloor}.$$

In case, the secret image is composed of the colors red, green, blue, cyan, magenta and green. the pixel expansion is $6m$. Compare this with the pixel expansion given in [9], which for these same two color sets is $3 \cdot 2^{n-1} \cdot n!$ and $6 \cdot 2^{n-1} \cdot n!$ respectively. It can be easily seen that:

$$3 \cdot 2^{n-1} \cdot n! > 4m \quad \text{and} \quad 6 \cdot 2^{n-1} \cdot n! > 6m.$$

In what follows, we describe our scheme for the color sets $\mathcal{C}_1 = \{Y, C, G\}$ and $\mathcal{C}_2 = \{Y, C, M, R, G, B\}$. We also show how our scheme can be extended to support an arbitrary number of colors.

4.1 The construction with three base colors

Let us assume that the secret image is composed of the three colors Cyan (C), Yellow (Y) and Green (G). We will first construct a $(2,2)$–VCS with the color set $\mathcal{C} = \{C, Y, G\}$. The basis matrices S_C, S_Y, S_G of this scheme are given below:

$$S_C = \begin{bmatrix} C & 0 & Y & 1 \\ 0 & C & 1 & Y \end{bmatrix}$$

$$S_Y = \begin{bmatrix} Y & 0 & C & 1 \\ 0 & Y & 1 & C \end{bmatrix}$$

$$S_G = \begin{bmatrix} C & Y & 1 & 0 \\ Y & C & 0 & 1 \end{bmatrix}$$

To generalize this scheme to a $(2,n)$–color VCS ($n \geq 3$), we consider the basis matrix S^1 of the $(2,n)$–VCS for black and white images described in [4]. S^1 is an $n \times m$ Boolean matrix which is realized by considering all binary n–vectors of weight $\lfloor n/2 \rfloor$, where

$$m = \binom{n}{\lfloor n/2 \rfloor}$$

We will use the basis matrices of the (2,2) scheme as templates in the construction of the basis matrices of the $(2,n)$ scheme. From here on, we will denote the basis matrix S_{col} of the (2,2) scheme by X_{col}. Therefore, S_C, S_Y, S_G defined above will be denoted as X_C, X_Y, and X_G respectively. S_C, S_Y and S_G, the basis matrices for the $(2,n)$ scheme, are constructed as follows: S_C is an $n \times 4m$ matrix obtained by replacing the 0's in S^1 by the first row of X_C and the 1's in S^1 by the second row of X_C. S_Y and S_G are constructed in a similar fashion. One can verify that the ith rows ($1 \leq i \leq n$) of the matrices S_C, S_Y and S_G thus obtained are identical up to a column permutation, thereby satisfying the security requirement of basis matrices.

Example 4.1 Let us construct a $(2,3)$–VCS with the color set $\mathcal{C} = \{Y, C, G\}$. S^1, in this case, is a $3 \times \binom{3}{1}$ matrix whose columns are obtained by permuting a binary vector consisting of $\lfloor 3/2 \rfloor$ 1's and $3 - \lfloor 3/2 \rfloor$ 0's. The matrix S^1 is shown below.

$$S^1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Since

$$X_C = \begin{bmatrix} C & 0 & Y & 1 \\ 0 & C & 1 & Y \end{bmatrix}$$

$$X_Y = \begin{bmatrix} Y & 0 & C & 1 \\ 0 & Y & 1 & C \end{bmatrix}$$

$$X_G = \begin{bmatrix} C & Y & 1 & 0 \\ Y & C & 0 & 1 \end{bmatrix}$$

we have

$$S_C = \begin{bmatrix} 0 & C & 1 & Y & C & 0 & Y & 1 & C & 0 & Y & 1 \\ C & 0 & Y & 1 & 0 & C & 1 & Y & C & 0 & Y & 1 \\ C & 0 & Y & 1 & C & 0 & Y & 1 & 0 & C & 1 & Y \end{bmatrix}$$

$$S_Y = \begin{bmatrix} 0 & Y & 1 & C & Y & 0 & C & 1 & Y & 0 & C & 1 \\ Y & 0 & C & 1 & 0 & Y & 1 & C & Y & 0 & C & 1 \\ Y & 0 & C & 1 & Y & 0 & C & 1 & 0 & Y & 1 & C \end{bmatrix}$$

$$S_G = \begin{bmatrix} Y & C & 0 & 1 & C & Y & 1 & 0 & C & Y & 1 & 0 \\ C & Y & 1 & 0 & Y & C & 0 & 1 & C & Y & 1 & 0 \\ C & Y & 1 & 0 & C & Y & 1 & 0 & Y & C & 0 & 1 \end{bmatrix}$$

Note that S_C is constructed by replacing the 0's of S^1 by the first row of X_C and the 1's by the second row of X_C. S_Y is constructed by replacing the 0's of S^1 by the first row of X_Y and the 1's by the second row of X_Y. S_G is constructed in a similar fashion. Here $R_C = 5/12$, $R_Y = 5/12$ and $R_G = 4/12$.

■

4.1.1 Share distribution algorithm

We use the following algorithm to encode the secret image.

For each pixel P in the secret image do the following:

1. Generate a random permutation π of the set $\{1, 2, \ldots, 4m\}$.
2. If P has color c_i ($c_i \in \{Y, C, G\}$), apply π to the columns of S_{c_i}. Call the resulting matrix T_{c_i}.
3. For $1 \leq j \leq n$, row j of T_{c_i}, describes the color distribution among the $4m$ subpixels of the jth share.

If $n = 2$, we apply the column permutations to the matrices X_{c_i} of the (2,2) scheme.

We next show that the color ratio attained by this encryption scheme is bounded below by 1/4. To prove this result we need the following lemmas:

Lemma 4.1 *For any distinct $i, j = 1, 2, \ldots, n$ let $S^1\{i, j\}$ denote the $2 \times m$ matrix obtained by restricting S^1 to rows i and j. Then the submatrix $S^1\{i, j\}$ has an equal number of patterns of the forms*

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

and this number is equal to $m \cdot \alpha(m)$. Also the total number of patterns of the forms

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix} \text{ and } \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

is given by $m - 2 \cdot m \cdot \alpha(m)$. Here $\alpha(m)$ is given by

$$\alpha(m) = \begin{cases} 1/4 + 1/4(n-1), & \text{if } n \text{ is even} \\ 1/4 + 1/4n. & \text{if } n \text{ is odd} \end{cases}$$

Proof: The fact that for any distinct $i, j = 1, 2, \ldots, n$ the submatrix $S^1\{i, j\}$ has an equal number of patterns of the forms

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

and that this number is equal to $m \cdot \alpha(m)$ has been proved by Blundo, De Santis, and Stinson in [4]. Since S^1 has a total of m columns, the total number of patterns of the forms

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix} \text{ and } \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

is given by $m - 2 \cdot m \cdot \alpha(m)$.

■

Note. From here on whenever we use the term $\alpha(m)$, we will use it as defined above in Lemma 4.1. To see how $\alpha(m)$ is obtained, consult reference [4].

Lemma 4.2 *For each cyan (or yellow) pixel in the original image, the total number of cyan (or yellow) colored subpixels in a superimposed image is given by* $m[1 + 2 \cdot \alpha(m)]$. *For each green pixel in the original image, the total number of green colored subpixels in a superimposed image is given by* $4m \cdot \alpha(m)$.

Proof: Recall that we defined X_C as follows:

$$X_C = \begin{bmatrix} C & 0 & Y & 1 \\ 0 & C & 1 & Y \end{bmatrix}.$$

First note that each of the patterns

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

contributes two C's in S_C. Each of the patterns

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

contributes one C in S_C. So for each cyan colored pixel in the secret image, the total number of cyan colored subpixels in a superimposed image is given by (using Lemma 4.1)

$$2m \cdot \alpha(m) + 2m \cdot \alpha(m) + m - 2m \cdot \alpha(m)$$

which simplifies to

$$m[1 + 2 \cdot \alpha(m)]$$

One can verify that this result also holds for a yellow pixel.

Next we will work this out for a green pixel. Recall that we defined X_G as follows

$$X_G = \begin{bmatrix} C & Y & 1 & 0 \\ Y & C & 0 & 1 \end{bmatrix}$$

Note that each of the patterns

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

contributes two G's in S_G. The patterns

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix} \text{ and } \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

contribute no G's in S_G. Thus for each green pixel in the original image, the total number of green colored subpixels in a superimposed image is given by (using Lemma 4.1)

$$2m \cdot \alpha(m) + 2m \cdot \alpha(m) + 0 + 0 = 4m \cdot \alpha(m).$$

■

Now we come to the main theorem.

Theorem 4.1 *For any $n \geq 3$, there exists a $(2, n)-$color VCS with base colors Cyan (C), Yellow(Y), and Green (G) with pixel expansion $4m$ and color ratios*

$$R_C = \begin{cases} 3/8 + 1/8(n-1), & \text{if } n \text{ is even} \\ 3/8 + 1/8n, & \text{if } n \text{ is odd} \end{cases}$$

$$R_Y = \begin{cases} 3/8 + 1/8(n-1), & \text{if } n \text{ is even} \\ 3/8 + 1/8n, & \text{if } n \text{ is odd} \end{cases}$$

$$R_G = \begin{cases} 1/4 + 1/4(n-1), & \text{if } n \text{ is even} \\ 1/4 + 1/4n, & \text{if } n \text{ is odd} \end{cases}$$

For $n = 2$, the color ratio of the $(2, n)-$color VCS is 1/2 and the pixel expansion is 4.

Proof: That for $n = 2$, the color ratio is 1/2 and the pixel expansion is 4 can be seen by examining the basis matrices of the (2,2) scheme.

Therefore, consider the case when $n \geq 3$. The number of columns in S_{c_i}, $c_i \in \{C, Y, G\}$ is $4m$. By using Lemma 4.2, the color ratio R_C is given by

$$R_C = [m \cdot (2 \cdot \alpha(m) + 1)]/4m = 1/4 + \alpha(m)/2$$

From (4), we know that $\alpha(m)$ is given by,

$$\alpha(m) = \begin{cases} 1/4 + 1/4(n-1), & \text{if } n \text{ is even} \\ 1/4 + 1/4n, & \text{if } n \text{ is odd} \end{cases}$$

Therefore, R_C can be written as:

$$R_C = \begin{cases} 3/8 + 1/8(n-1), & \text{if } n \text{ is even} \\ 3/8 + 1/8n. & \text{if } n \text{ is odd} \end{cases}$$

R_Y can be derived in a similar fashion. One can verify that R_Y is given by:

$$R_Y = \begin{cases} 3/8 + 1/8(n-1), & \text{if } n \text{ is even} \\ 3/8 + 1/8n. & \text{if } n \text{ is odd} \end{cases}$$

Again by Lemma 4.2, R_G is given by

$$R_G = 4m \cdot \alpha(m)/4m = \alpha(m) = \begin{cases} 1/4 + 1/4(n-1), & \text{if } n \text{ is even} \\ 1/4 + 1/4n, & \text{if } n \text{ is odd} \end{cases}$$

■

Remark

Note that each share contains the three base colors C, Y, and G together with the colors white (0) and black (1). If the encoded pixel is cyan colored, then on superimposing any two shares, the resulting reconstructed pixel has subpixels of colors cyan, yellow, black, and white. Here the color yellow is an unwanted color since it hinders the human visual system from discerning the true color of the pixel. We will call such unwanted colors *nuisance* colors. Suppose that the true color of a pixel is c_i, and on superimposing two arbitrary shares, we find some subpixels with the color c_j ($c_j \neq$ black, white). Then c_j is a nuisance color for c_i and any subpixel with color c_j in a pixel for c_i will be denoted by $N_{c_i}^{c_j}$. In this case, yellow is a nuisance color for cyan and we denote yellow colored subpixels in a cyan pixel by N_C^y. For a yellow colored pixel, the nuisance color is cyan and we denote those subpixels by N_Y^c. Finally, a green colored pixel has the nuisance colors cyan and yellow and we denote those colored subpixels by N_G^c and N_G^y respectively.

We now count the number of $N_{c_i}^t$ subpixels in a superimposed image for a pixel of color c_i, where $c_i \in \{C, Y, G\}$ and $t \in \{C, Y\}$. Note that in the (2,2) color VCS with color set $\{C, Y, G\}$ there are no nuisance colors. Let the pixel in the original image be a cyan colored one. When shares of the i-th and j-th participants are superimposed, the nuisance color yellow appears due to the patterns $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ in $S^1\{i, j\}$. Each of these patterns contributes one Y in the superimposed image. Recall that the total number of such patterns is given by $m - 2 \cdot m \cdot \alpha(m)$. Hence the total number of yellow colored subpixels N_C^y is given by

$$m - 2 \cdot m \cdot \alpha(m) = \begin{cases} m[\frac{1}{2} - \frac{1}{2(n-1)}], & \text{if } n \text{ is even} \\ m[\frac{1}{2} - \frac{1}{2n}], & \text{if } n \text{ is odd} \end{cases}$$

Note that this number is less than $m/2$. One can show that $N_Y^c < m/2$. For each green pixel in the original image, the number of cyan and yellow colored subpixels are each less than $m/2$. Hence their sum is less than m. Although, the reconstructed image has nuisance colors, they do not affect the quality of the reconstructed image significantly. Nuisance colors do not produce any diminution of brightness, as the overwhelming majority of black subpixels do in the schemes described in [7] and [9].

4.2 The construction with six base colors

Let us now assume that the secret image is made up of the six colors Red (R), Green (G), Blue (B), Cyan (C), Yellow (Y), and Magenta (M). To construct our $(2, n)$–color VCS for

this color set. we first construct the basis matrices of the corresponding $(2, 2)$ scheme. These are shown below.

$$X_Y = \begin{bmatrix} Y & 0 & C & M & 1 & 1 \\ 0 & Y & 1 & 1 & C & M \end{bmatrix}$$

$$X_C = \begin{bmatrix} C & 0 & M & Y & 1 & 1 \\ 0 & C & 1 & 1 & M & Y \end{bmatrix}$$

$$X_M = \begin{bmatrix} M & 0 & Y & C & 1 & 1 \\ 0 & M & 1 & 1 & Y & C \end{bmatrix}$$

$$X_R = \begin{bmatrix} Y & M & C & 1 & 1 & 0 \\ M & Y & 1 & C & 0 & 1 \end{bmatrix}$$

$$X_G = \begin{bmatrix} Y & C & M & 1 & 1 & 0 \\ C & Y & 1 & M & 0 & 1 \end{bmatrix}$$

$$X_B = \begin{bmatrix} M & C & Y & 1 & 1 & 0 \\ C & M & 1 & Y & 0 & 1 \end{bmatrix}$$

Note that C + Y = G, C + M = B and Y + M = R. The basis matrix S_{c_i} ($c_i \in \{Y, C, M, R, G, B\}$) is obtained by replacing the 0's of the $n \times \binom{n}{\lfloor n/2 \rfloor}$ matrix S^1 by the first row of X_{c_i} and the 1's of S^1 by the second row of X_{c_i}. S_{c_i} defined in this manner is an $n \times 6m$ matrix, where $m = \binom{n}{\lfloor n/2 \rfloor}$. Note that the ith rows of the matrices S_R, S_G, S_B, S_C, S_Y, and S_M thus obtained are identical up to a column permutation.

Theorem 4.2 *For any $n \geq 3$, there exists a $(2, n)$–color VCS with base colors Red (R), Green (G), Blue (B), Cyan (C), Yellow (Y), and Magenta (M) with pixel expansion 6m and color ratios*

$$R_Y = \begin{cases} 1/4 + 1/12(n-1), & \text{if } n \text{ is even} \\ 1/4 + 1/12n, & \text{if } n \text{ is odd} \end{cases}$$

$$R_C = \begin{cases} 1/4 + 1/12(n-1), & \text{if } n \text{ is even} \\ 1/4 + 1/12n, & \text{if } n \text{ is odd} \end{cases}$$

$$R_M = \begin{cases} 1/4 + 1/12(n-1), & \text{if } n \text{ is even} \\ 1/4 + 1/12n, & \text{if } n \text{ is odd} \end{cases}$$

$$R_R = \begin{cases} 1/6 + 1/6(n-1), & \text{if } n \text{ is even} \\ 1/6 + 1/6n, & \text{if } n \text{ is odd} \end{cases}$$

$$R_G = \begin{cases} 1/6 + 1/6(n-1), & \text{if } n \text{ is even} \\ 1/6 + 1/6n. & \text{if } n \text{ is odd} \end{cases}$$

$$R_B = \begin{cases} 1/6 + 1/6(n-1), & \text{if } n \text{ is even} \\ 1/6 + 1/6n. & \text{if } n \text{ is odd} \end{cases}$$

If $n = 2$, then the pixel expansion is 6 and the color ratio of the scheme is 1/3.

Proof: The proof is similar to the proof of Theorem 4.1.

■

4.3 Extension to an arbitrary number of colors

Our scheme can be generalized to an arbitrary number of colors. If the secret image has the colors $\mathcal{C} = \{c_1, c_2, \ldots, c_k\}$ such that no two colors c_i and $c_j \in \mathcal{C}$ can be combined to produce a third color $c_k \in \mathcal{C}$, then for each color $c_i \in \mathcal{C}$ we define matrix X_{c_i} as follows :

$$X_{c_i} = \begin{bmatrix} c_i & 0 & c_1 & \ldots & c_{i-1} & c_{i+1} & \ldots & c_k & 1 & \ldots & 1 & 1 & \ldots & 1 \\ 0 & c_i & 1 & \ldots & 1 & 1 & \ldots & 1 & c_1 & \ldots & c_{i-1} & c_{i+1} & \ldots & c_k \end{bmatrix}$$

The color ratio can be shown to be

$$\frac{1}{2k} + \frac{\alpha(m)}{k}.$$

This lower bound is independent of the number of shares and depends only on the number of colors in the secret image. In case colors can be combined, we will get a better lower bound for the color ratio.

Chapter 5

Conclusions and Open Problems

In this thesis, we have reviewed constructions for black and white, grey-level, and color visual cryptography schemes. In the black and white case, we presented constructions for $(2,n)$, (k,k), and (k,n) threshold schemes. We also presented a cumulative array construction for strong access structures. For the $(2,n)$ case, the construction given is optimal with respect to the relative difference. The (k,k) construction is optimal with respect to both the relative difference and the pixel expansion.

For grey-level VCS, we presented an optimal (k,k) scheme. We also showed how this can be generalized to a (k,n) scheme using starting matrices. For color VCS, we reviewed constructions of $(2,n)$, (k,k), and (k,n) lattice-based schemes.

Finally, we presented our $(2,n)$ scheme for color images. For the color set $C_1 = \{Y,C,G\}$, our scheme achieves a color ratio that is lower bounded by $1/4$; for the second color set $C_2 = \{Y,C,M,R,G,B\}$, the lower bound on the color ratio is $1/6$. The color ratio that we obtain is also much higher than those obtained in the schemes proposed in [7] and [9]. The pixel expansion is quite good, and is certainly better than the one in [9]. We have also shown that our scheme can be extended to support an arbitrary number of colors and that the pixel expansion of our scheme does not depend on the number of shares but only on the number of base colors. An open problem is to extend this scheme to a $(k,n)-$threshold scheme.

An important open problem in color visual cryptography is the following: What is the optimal lower bound on the pixel expansion of a $(k,n)-$threshold scheme (a scheme for a general access structure) for color images with base colors $\{c_1,\ldots,c_J\}$? What are the optimal upper bounds on the color ratios $\{R_{c_i}\}_{i=1}^{J}$ for such a scheme?

If we specialize to the case $k=n$, we know from [11] that the pixel expansion is at least 2^{n-1}. None of the existing (n,n) color schemes achieve this pixel expansion. The best known result (see [7]) has a pixel expansion of $J\cdot n\cdot 2^{n-2}$, where J denotes the number of base colors in the secret image. We do not know whether this is indeed the optimal pixel expansion of an (n,n) scheme with J colors.

For $k=2$, Blundo, De Santis, and Stinson [4] have established lower bounds on the pixel expansion, as a function of n, for black and white VCS with optimal relative difference. The lower bounds obtained by them are all linear in n. No existing $(2,n)-$threshold VCS for color images achieves a pixel expansion that is linear in n. The pixel expansion of the $(2,n)$ scheme described in [7] is $J\cdot n\cdot(n-1)$, which is quadratic in n. Again, it is not known if this is optimal.

For an arbitrary $(k, n)-$threshold scheme realized using basis matrices Blundo, De Santis, and Stinson [4] have shown that the lower bound on the pixel expansion is $2^{k-2} \cdot \log(n-k+2)$. Existing $(k, n)-$threshold color schemes have a much larger pixel expansion. For example, [9] gives a (k, n) scheme where $m = J \cdot 2^{n-2} \cdot n!$.

In addition to providing lower bounds for the pixel expansion, we need to upper bound the color ratios. The color ratios determine the brightness of the reconstructed image and the upper bounds will give us an idea as to what the best possible reconstructed image will look like. Finally, having obtained lower and upper bounds, we would also want a method of constructing visual cryptography schemes that achieve these optimal bounds.

Bibliography

[1] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, *Extended Capabilities for Visual Cryptography*, Theoretical Computer Science, vol. 250, nos.1-2. pp. 143-161, 2001.

[2] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, *Visual Cryptography for General Access Structures*, Information and Computation, vol. 129, pp. 86-106, 1996.

[3] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, *Constructions and Bounds for Visual Cryptography*, in "23rd International Colloquium on Automata, Languages and Programming" (ICALP '96), F.M. auf der Heide and B. Monien Eds., Vol. 1099 of "Lecture Notes in Computer Science", Springer-Verlag, Berlin, pp. 416-428,1996.

[4] C. Blundo, A.De Santis, and D.R. Stinson, *On the Contrast in Visual Cryptography Schemes*, J. Cryptology, vol. 12, no. 4, pp. 261-289, 1999.

[5] C. Blundo, A. De Santis and M. Naor, *Visual Cryptography for gray Level Images*, Inf. Process. Lett., Vol. 75, Issue. 6, pp. 255-259, 2001.

[6] S. Droste, *New Results on Visual Cryptography*, Advance in Cryptography- CRYPT'96. Lecture Notes in Computer Science, 1109, pp. 401-415, Springer-Verlag, 1996.

[7] H. Koga and H. Yamamoto, *Proposal of a Lattice-Based Visual Secret Sharing Sceme for Color and Gray-Scale Images*, IEEE Trans. Fundamentals, Vol. E81-A, No. 6 June 1998.

[8] H. Koga and T. Ishihara, *New Constructions of the Lattice-Based Visual Secret Sharing Scheme Using Mixture of Colors*, IEICE Trans. Fundamentals, Vol. E85-A, No. 1 January 2002.

[9] H. Koga, M. Iwamoto and H. Yamamoto, *An Analytic Construction of the Visual Secret Scheme for Color Images*, IECIE Trans. Fundamentals, Vol. E84-A, No. 1 January 2001.

[10] L.A. MacPhérson *Grey Level Visual Cryptography for General Access Structures*, Master's Thesis, University of Waterloo, 2002.

[11] M. Naor and A. Shamir, *Visual Cryptography*, Advance in Cryptography, Eurocrypt'94. Lecture Notes in Computer Science 950, pp. 1-12, Springer-Verlag, 1994.

[12] V. Rijmen and B. Preneel, *Efficient Color Visual Encryption or "Shared Colors of Benetton"*, presented at EUROCRYPT '96 Rump Session. Available at

`http://www.iacr.org/conferences/ec96/rump/preneel.ps`.