2006

Simultaneous Visual Cryptography

Oliver Kikic

Simultaneous Visual Cryptography

Oliver Kikic (oxk2361@cs.rit.edu)
Masters Thesis

Rochester Institute of Technology
Rochester, NY

Advisor: Chris Homan (cmh@cs.rit.edu)
Reader: Stanislaw Radziszowski (spr@cs.rit.edu)
Observer: Edith Hemaspaandra (eh@cs.rit.edu)

May 25, 2006

Rochester Institute of Technology
Computer Science Department

Simultaneous Visual Cryptography

by
Oliver Kikic

A thesis, submitted to
The Faculty of the Department of Computer Science,
in partial fulfillment of the requirements for the degree of
Master of Science in Computer Science.

Approved by:

Christopher Homan
Prof. Christopher Homan

Stanislaw Radziszowski
Prof. Stanislaw Radziszowski

Edith Hemaspaandra
Prof. Edith Hemaspaandra

May 25, 2006

Thesis/Dissertation Author Permission Statement

Title of thesis or dissertation: SIMULTANEOUS VISUAL CRYPTOGRAPHY

Name of author: OLIVER KIKIC
Degree: M.S.
Program: COMPUTER SCIENCE
College: GCCIS

I understand that I must submit a print copy of my thesis or dissertation to the RIT Archives, per current RIT guidelines for the completion of my degree. I hereby grant to the Rochester Institute of Technology and its agents the non-exclusive license to archive and make accessible my thesis or dissertation in whole or in part in all forms of media in perpetuity. I retain all other ownership rights to the copyright of the thesis or dissertation. I also retain the right to use in future works (such as articles or books) all or part of this thesis or dissertation.

Print Reproduction Permission Granted:

I, Oliver Kikic, hereby **grant permission** to the Rochester Institute Technology to reproduce my print thesis or dissertation in whole or in part. Any reproduction will not be for commercial use or profit.

Signature of Author: Oliver Kikic Date: _____

Print Reproduction Permission Denied:

I, _____, hereby **deny permission** to the RIT Library of the Rochester Institute of Technology to reproduce my print thesis or dissertation in whole or in part.

Signature of Author: _____ Date: _____

Inclusion in the RIT Digital Media Library Electronic Thesis & Dissertation (ETD) Archive

I, Oliver Kikic, additionally grant to the Rochester Institute of Technology Digital Media Library (RIT DML) the non-exclusive license to archive and provide electronic access to my thesis or dissertation in whole or in part in all forms of media in perpetuity.

I understand that my work, in addition to its bibliographic record and abstract, will be available to the world-wide community of scholars and researchers through the RIT DML. I retain all other ownership rights to the copyright of the thesis or dissertation. I also retain the right to use in future works (such as articles or books) all or part of this thesis or dissertation. I am aware that the Rochester Institute of Technology does not require registration of copyright for ETDs.

I hereby certify that, if appropriate, I have obtained and attached written permission statements from the owners of each third party copyrighted matter to be included in my thesis or dissertation. I certify that the version I submitted is the same as that approved by my committee.

Signature of Author: Oliver Kikic Date: _____

Abstract

A visual cryptography scheme (VCS), as proposed by M. Naor and A. Shamir, encodes a secret image into n different shares. The scheme ensures that only certain designated combinations of shares can recover the original image, while other combinations yield, in probabilistic sense, no information about the secret image. In this thesis, we show that there exist simultaneous visual cryptography schemes (SVCS), i.e. cryptographic schemes that allow for multiple secret images to be encoded across a set of n shares. The essential part of this research is to derive a set of formal definitions used to construct a valid SVCS and to design and examine different approaches for establishing valid SVCS constructions. In particular, we describe an SVCS that allows encoding $n - 1$ distinct secret images across a set of n shares, and include a program that demonstrates the successful use of this SVCS in the appendix.

Contents

1 Introduction 2

2 Basic Visual Cryptography Schemes 6

3 Simultaneous Visual Cryptography Schemes 16
- 3.1 A Very Simple SVCS System 18
- 3.2 An $n-1$ out of n SVCS 21

4 Conclusion and Considerations for Further Research 28

A SVCS Example 31
- A.1 Share Images 32
- A.2 Superposition of Share Images 33

Chapter 1

Introduction

Suppose that a group of n pirates decides to bury a treasure and distribute a map among them that marks its location. The pirates wish to come back to this location and uncover it some number of years down the line. However, they are not sure if all the pirates will be present when they recover the treasure, in which case vital parts of the treasure map might be missing. There is also a concern that single portions of the treasure map might disclose the general area where the treasure has been hidden. In the worst case, the exact location of the treasure might be revealed. Clearly, cutting the treasure map into n pieces and distributing those among all participants does not fully address the concerns of the pirates. They need a solution which will recover the map by using k out of n map pieces, and they also need to ensure that combinations of less than k map pieces do not reveal any information regarding the treasure map. Visual cryptography provides the pirates with techniques that will allow them to encode their map in this manner.

The concept of visual cryptography schemes (VCS) was developed by Naor and Shamir in 1994 [1]. It provides users with a method for encoding a secret image into a collection of equally sized images called *shares*. It is common in visual cryptography to refer to all shares as *transparencies*, because one retrieves the original secret image by stacking qualifying shares on top of each other. Since all shares have equal dimensions, the decoding procedure ordinarily consists of printing shares onto transparent material. Thus, the secret image recovery process is typically performed visually. In its basic form, the VCS design requires all shares in the system in order to decode the secret image, but in its more sophisticated forms, the users have some power to designate certain combinations of shares to reconstruct the

secret image and other combinations to not reveal any information at all about the secret image.

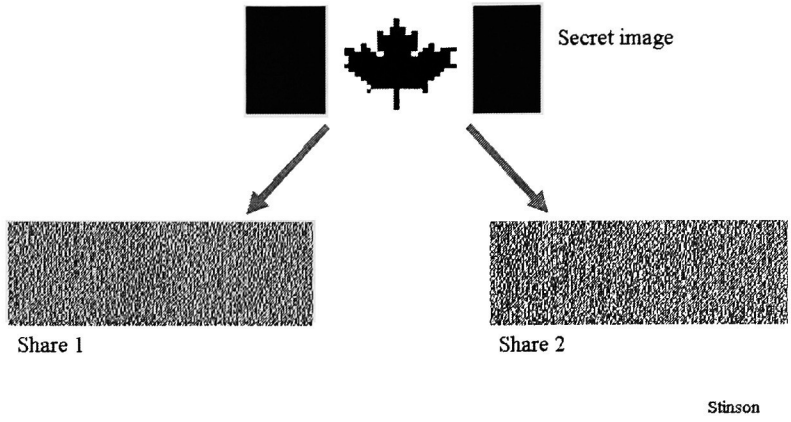

Figure 1.1: An example of a VCS. The secret image of the Canadian flag is encoded into two share images (transparencies).

The images in Fig. 1.1 and 1.2 provide an example of a simple VCS, which has the capability to encode a black and white image into two shares. Fig. 1.1 contains the secret image, which in this case is a Canadian flag, and the two share images that are the result of the VCS encoding process. On the other hand, Fig. 1.2 demonstrates the VCS decoding process by showing the result obtained through the superposition of the two share images. The resulting image matches the original secret image of the Canadian flag, although there is also a noticeable loss of contrast.

Aside from defining VCS's in their paper [1], Shamir and Naor provide a number of practical implementations for the basic model. Furthermore, the authors devote a portion of their research to prove bounds for VCS parameters. There are a number of inherent problems that exist within the VCS concept and are addressed by the authors. Most noticeably, the results produced by any visual cryptography scheme contain a substantial loss of contrast, as already demonstrated by the example in Fig 1.2.

A simultaneous visual cryptography scheme (SVCS) utilizes the image sharing techniques used in VCS's to build a powerful extension of the VCS system. Instead of sharing only one secret image across a set of participating shares, the user now has the ability to share multiple secret images. When

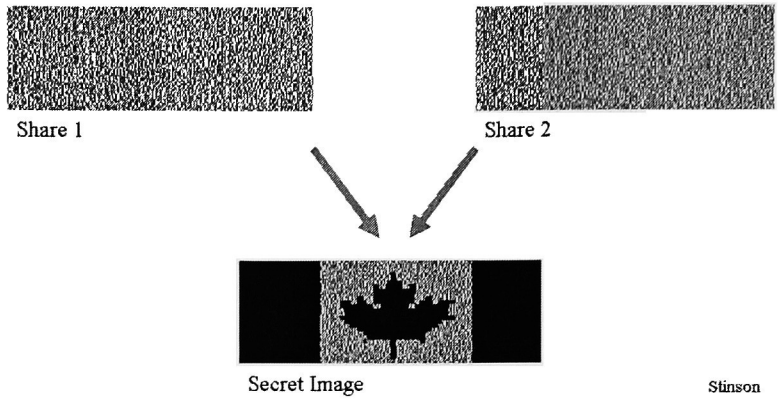

Figure 1.2: An example of VCS secret image decoding. The superposition of the two share images retrieves the secret Canadian flag image.

dealing with a conventional VCS, it is, to decode the secret image, sufficient that the attacker recovers any comprehensible result with a combination of shares. However, if we encode, using an SVCS, the secret image with other images, the attacker is not guaranteed to recover the secret image. Moreover, there is a chance that she might mistake one of the other images for the secret image. Using the treasure map analogy from above, suppose that the pirates decide to use SVCS in order to encode their original treasure map. Aside from creating an image of the original map, they also create a number of false maps that are the result of other combinations of shares. When recovered by an unknowing rival group interested in finding the treasure, the false maps will throw them off by giving out false information. The attackers must recover all shares in the systems and exhaustively stack combinations of share images until they recover all secret images in the system. More importantly, in terms of the number of shares needed, a SVCS allows users to more effectively encode a set of secret images. Given n secret images that we wish to encode across at least $n-1$ shares, it would require n different VCS's, where each VCS contains $n-1$ different share images. On the other hand, we can achieve the same goal by utilizing one SVCS with n share images.

In this thesis, we first formalize the notion and present two main definitions regarding VCS systems. Alongside of the VCS definitions, we explain

the encoding process for each secret image pixel. In order to further demonstrate various possibilities presented by the concepts of VCS, we include a brief explanation of extended visual cryptography scheme (EVCS), as proposed by Stinson, et. al. [3]. Following the EVCS description, the focus shifts to a formal representation of SVCS's, in which contains the formal SVCS definition. A portion of the discourse that follows the SVCS definition consists of examples of different SVCS's. The first example presented in this thesis is very simple but it sets the foundation used in developing a powerful SVCS, which can encode secret image for any $n - 1$ out of n shares in its system. We present such system at the end of this thesis.

Chapter 2

Basic Visual Cryptography Schemes

Visual cryptography schemes (VCS's) were first proposed by Naor and Shamir [1]. Given integers n and k such that $1 < k \leq n$ and a black and white secret image, a VCS creates n transparencies, called *shares*, in such a way that one can reconstruct the secret image by stacking together any k distinct shares, but by stacking together fewer than k shares one gets no information about the secret image. Shares are created one secret pixel at a time, independently of every other secret pixel, based on the following procedure.

Create two collections of "rules", $\mathcal{C}_0$ and $\mathcal{C}_1$ (we discuss below how to create the rules).
for all pixels p in the secret image **do**
  if p is black, choose at random a rule from $\mathcal{C}_1$
  if p is white, choose at random a rule from $\mathcal{C}_0$
  use the chosen rule to share p
end for

In sharing a secret image pixel, the procedure first breaks it into a collection of m *subpixels* printed so closely together that they appear to form a single lightness value. Each "rule" in $\mathcal{C}_0$ and $\mathcal{C}_1$ dictates the color of each subpixel. We represent each rule by an $n \times m$ Boolean matrix, where each row of the matrix corresponds to one of the n shares in the VCS, and the columns represent the subpixels assigned to each share. Black subpixels are depicted by 1's and white pixels by 0's. A collection $\mathcal{C}_i$, where $i \in \{0, 1\}$, of

r matrices, is often generated by taking one $n \times m$ Boolean matrix, called a *basis matrix*, that meets the requirements for encoding a black (white) pixel, and including in the collection every possible column permutation on said matrix. Matrices M in Fig. 2.2 and Fig. 2.3 help visualize this notion. We emulate the above-mentioned superposition of k shares of a single pixel by extracting the corresponding rows of the appropriate $n \times m$ Boolean matrix M, performing a Boolean OR operation on the columns of these k rows, and obtaining a vector V of length m (Fig. 2.2 and Fig. 2.3). In order to differentiate between black and white pixels, we calculate the Hamming weight $H(V)$ of the vector. Parameter d is a fixed threshold, where $1 \leq d \leq m$ and $\alpha > 0$. We call the value α the *relative difference* and it describes the difference in weight between vectors V that result from encoding a white and a black pixel in the secret image. In case where $H(V) \geq d$, we interpret the gray level of the vector V as black, as demonstarted by the example in Fig. 2.2. Similarly, Fig. 2.3 shows that if $H(V) \leq d - \alpha m$, then the gray level of vector V describes a white pixel.

The table in Fig. 2.1 explains the encoding and decoding processes illustrated in Fig. 1.1 and 1.2. For each pixel of the secret image, the shares are assigned a collection of two subpixels, one of which is white and the other is black. Thus, the collection $\mathcal{C}_0$ contains the matrices

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

and

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

The collection $\mathcal{C}_1$ contains the matrices

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

and

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

We say that collections $\mathcal{C}_0$ and $\mathcal{C}_1$ constitute a VCS if the following conditions are met.

Definition 2.1. [1, *Definition* 2.1] *A solution to the k out of n VCS consists of two collections of $n \times m$ Boolean matrices $\mathcal{C}_0$ and $\mathcal{C}_1$. To share a white*

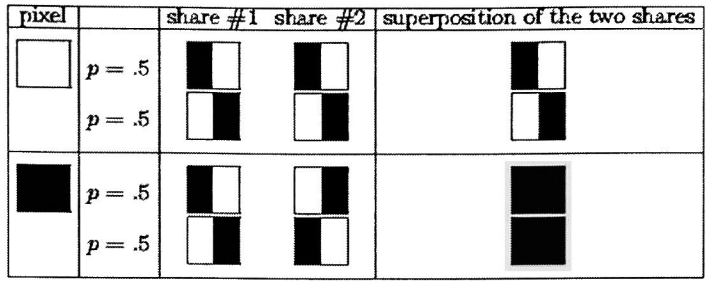

Figure 2.1: VCS encoding and decoding on the pixel level. The table contains all possible combinations of subpixels for a white or black secret image pixel and the results of their superposition.

pixel, the user randomly chooses one of the matrices in $\mathcal{C}_0$, and to share a black pixel, the user randomly chooses one of the matrices in $\mathcal{C}_1$. The chosen matrix defines the color of the m subpixels in each one of the n transparencies. The solution is considered valid if the following three conditions are met:

1. *For any S in $\mathcal{C}_0$, the "or" V of any k out of n rows satisfies $H(V) \leq d - \alpha m$.*

2. *For any S in $\mathcal{C}_1$, the "or" V of any k out of n rows satisfies $H(V) \geq d$.*

3. *For any subset $\{i_1, i_2, \ldots, i_q\}$ of $\{1, 2, \ldots, n\}$ with $q < k$, the two collections of $q \times n$ matrices $\mathcal{D}_t$ for $t \in \{0, 1\}$ obtained by restricting each $n \times m$ matrix in $\mathcal{C}_t$ to rows $i_1, i_2, \ldots, i_q$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.*

The superposition of the shares from the example in Fig. 2.1 can be used to reconstruct the secret image pixel, due to the fact that $H(V) = 1$ for all $M \in \mathcal{C}_0$ and $H(V) = 2$ for all $M \in \mathcal{C}_1$. Furthermore, it is evident that restricting all matrices in collections $\mathcal{C}_0$ and $\mathcal{C}_1$ to a single row, results in two collections that are indistinguishable in the sense that they contain the same matrices with the same frequencies because they will always contain matrices [1 0] and [0 1]. The collections $\mathcal{C}_0$ and $\mathcal{C}_1$ used in the Canadian flag example meet the conditions of Definition 2.1 and therefore constitute a valid VCS.

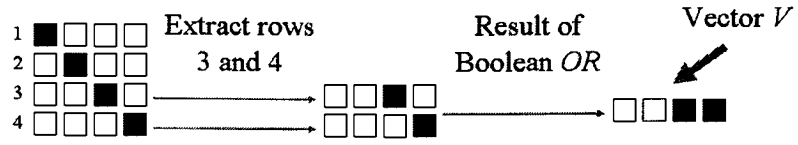

Figure 2.2: An example of black pixel encoding in a 2 out of 4 VCS. The first step of the encoding process entails extracting any two rows of the matrix $M \in C_1$, and this example uses rows 3 and 4. Vector V is the result of a Boolean "OR" operation performed on the two extracted rows and its Hamming weight is 2. Using any other two rows of the matrix yields the same result.

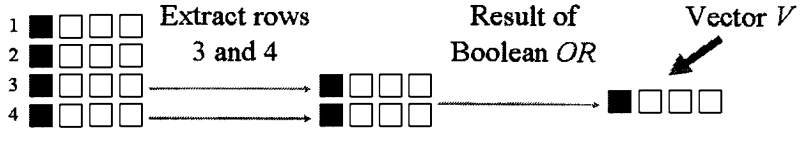

Figure 2.3: An example of white pixel encoding in a 2 out of 4 VCS. Extracting any two rows from the depicted matrix $M \in C_0$ produces a vector V whose Hamming weight is 1. As in the previous example, the rows used for the encoding are 3 and 4.

Naor and Shamir present two different general n out of n VCS constructions. The first VCS has the parameters $m = 2^n$, $\alpha = 1/2^n$, and $r = 2^n!$ [1, Lemma 4.1], and the second has parameters $m = 2^{n-1}$, $\alpha = 1/2^{n-1}$, and $r = 2^{n-1}!$ [1, Lemma 4.2]. Furthermore, the authors show that the parameters α and m of the second VCS are optimal for all n out of n VCS's.

Theorem 2.2. [1, *Theorem* 4.3] *In any n out of n scheme* $\alpha \leq 1/2^{n-1}$ *and* $m \geq 2^{n-1}$

Noar and Shamir use their general construction of a n out of n VCS, and apply those results in the general construction of a k out of n VCS. The authors describe the steps necessary to perform this transformation, and prove the following theorem in order to provide optimal bounding values for a k out of n VCS.

Theorem 2.3. [1, *Theorem* 5.2] *For any n and k there exists a VCS with parameters* $m = n^k \cdot 2^{k-1}$, $\alpha = (2e)^{-k}/\sqrt{2\pi k}$, *and* $r = n^k(2^{k-1}!)$.

Stinson et al. extend Naor and Shamir's model [1] to general access structures, where an access structure is an explicit specification of all forbidden and qualified subsets of share images [3]. The authors define a VCS over a 3-tuple (Γ_Q, Γ_F, m), where the pair (Γ_Q, Γ_F) is called the *access structure* [2]. Γ_Q and Γ_F are subsets of the powerset over some set $P = \{1, \ldots, n\}$ of shares. The set Γ_Q is called the *qualifying set* and Γ_F is called the *forbidden set.* Each element of Γ_Q represents a subset of P that can recover the secret image, and each element of Γ_F represents a subset of P that cannot reconstruct the secret image. If Γ_F is monotone decreasing, Γ_Q monotone increasing, and $\Gamma_Q \cup \Gamma_F = 2^P$, then (Γ_Q, Γ_F) is said to be *strong* [3, p.3]. In this case, "monotone decreasing" means that subsets of all members in Γ_F are themselves included in Γ_F, and "monotone increasing" means that supersets of all members in Γ_Q are themselves included in Γ_Q.

Stinson et al. also differentiate between weak and strong VCS models. The main difference between the two models is found in the requirements for the security condition of the sharing scheme. A weak VCS guarantees that the participants in a forbidden set of the scheme cannot retrieve any information on the secret image by examining their shares and the original images associated with them. A strong VCS requires that by inspecting the shares associated with any of the original n images of any non-qualifying subset of shares one gains no information about the secret image.

Stinson et al. use the term $w(M_X)$ to express the Hamming weight of a vector given by the Boolean 'OR' of some rows in matrix M. More precisely, for any $n \times m$ Boolean matrix

$$M = \begin{bmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & . & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{bmatrix}$$

and $X = \{i_1, \ldots, i_p\} \subseteq \{1, . \quad , n\}$ they define M_X as

$$\begin{bmatrix} a_{i_1,1} & \cdots & a_{i_1,m} \\ \vdots & . & \vdots \\ a_{i_p,1} & \cdots & a_{i_p,m} \end{bmatrix}$$

and $w(M)$ as $m - \sum_{j=1}^{m} \prod_{i=1}^{n} (1 - a_{ij})$.

Given the concepts presented by Naor and Shamir and the notion of access structures presented by Stinson et al., we would like to use them in order to define VCS's more rigorously. For example, we distinguish the Boolean matrices in each C_i by an index value, and we use $w(M)$ instead of $H(V)$. The following definition will prove useful in creating simultaneous visual cryptography schemes (SVCS), which we describe in the next chapter.

Definition 2.4. *For $n \in \mathbb{N}$, let (Γ_Q, Γ_F) be an access structure on the set $\mathcal{P} = \{1, \ldots, n\}$, where $\Gamma_Q, \Gamma_F \subseteq 2^P$ For $r \in \mathbb{N}$ and $i \in \{0, 1\}$, let C_i be a collection of $n \times m$ Boolean matrices $C_i = \{M^{i,1}, \ldots, M^{i,r}\}$. We obtain a $((\Gamma_Q, \Gamma_F, m)$-VCS) if, for each $X \in \Gamma_Q$, there exist $\alpha \in \mathbb{R}$ and $t_X \in \mathbb{N}$ satisfying both of the following.*

1. Any qualified set $X = \{i_1, \ldots, i_p\} \in \Gamma_Q$ can recover the shared image i by stacking their transparencies.
   Formally, for any $k \in \{1, \ldots, r\}$ it holds that $w(M_X^{0,k}) \leq t_X - \alpha \cdot m$ and $w(M_X^{1,k}) \geq t_X$.

2. Any forbidden set $X \in \Gamma_F$ has no information on any of the shared images.
   Formally, for any $X \in \Gamma_F$ there exists a permutation π on the set $\{1, \ldots, r\}$ such that for any $k \in \{1, \ldots, r\}$ it holds that $M_X^{1,k} = M_X^{0,\pi(k)}$

Essentially, Definition 2.6 defines the requirements for basis matrices for all VCS's. Instead of explicitly defining a series of basis matrix definitions for individual VCS's, we would like to refer to a single definition for all systems. As discussed previously in this chapter, we can construct any $\mathcal{C}_s$ in a VCS by finding a matrix $M \in \mathcal{C}_s$, and including all possible column permutations of M in $\mathcal{C}_s$. The same principle applies for extended VCS's and SVCS's, because they also use Boolean matrix collections $\mathcal{C}_s$. Given that it is possible for $\mathcal{C}_s$ to contain multiple instances of a Boolean matrix M, we define it as a collection instead of a set for all SVCS's. This property is essential in preserving isomorphism between all defined $\mathcal{C}_s$ in a SVCS. Extended VCS's are discussed later in this chapter, and the next chapter of this thesis contains a detailed discussion of SVCS's. We now formally define VCS basis matrices as follows.

Definition 2.5. *Let P_π be a $m \times m$ matrix, such that $P_\pi = \begin{bmatrix} e_{\pi(1)} \\ \vdots \\ e_{\pi(m)} \end{bmatrix}$, where π is a permutation of $\{1, \ldots, m\}$ and e_i is the i^{th} vector in the identity matrix I_m. Then P_π is referred to as* permutation matrix.

Definition 2.6. *Let $p, n, m \in \mathbb{N}$ and $i \in \{1, \ldots, p\}$. Given a VCS, we call the collections $\mathcal{C}_i$ used to share secret image pixel* share collections. *Furthermore, let $S_1, \ldots, S_p$ be $n \times m$ Boolean matrices and let Σ_i be a collection of $n \times m$ Boolean matrices, such that $S_i P_\pi, S_i \in \Sigma_i$, where $i \in \{1, \ldots, p\}$. $S_1, \ldots, S_p$ are the basis matrices of the VCS, if $\mathcal{C}_i = \{M | M \in \Sigma_i\}$.*

Naor and Shamir discuss various possible extensions of VCS, such as: the possibility of concealing the existence of the secret image and the problem of visual encryption of a continuous tone image. By "continuous tone image", the authors mean an image whose pixels' gray levels range from 0 to 255. Thus, the VCS framework defined by Naor and Shamir in [1] does not directly apply to such images. Assuming that the secret image is broken up into two separate shares, the authors propose a solution that does not require the pixels of the secret image to be broken up into collections of subpixels. In their solution, each pixel of the secret image is, for each share image, encoded as a rotated half circle:

> When the two half circles (with rotation angles a and b) are carefully aligned, the superposition of the two half circles can

range in color from medium grey (representing white) to completely black (representing black) depending on the relative angle $a - b$ between the two rotated circles. If we choose for each pixel in each share a random absolute rotation angle (with the desired relative rotation angle between them), then each transparency will look uniformly grey and will reveal absolutely no information, but the superposition of the two transparencies will be a darker version of the original continuous tone image.

Secret images in a VCS are shared as images that appear to be nothing but randomly chosen black and white pixels. Stinson et al. study visual cryptography schemes, where each shared image can be anything the encoder chooses [2]. In our treasure map analogy, this would translate into the pirates encoding the secret map into, say, pictures of other, false maps or innocent pictures of disparate objects. Essentially, we are left with a method that, for some $n \in \mathbb{N}^+$, allows a secret image to be encoded into n completely unrelated and misleading images. The authors call a VCS that facilitates this capability an extended visual cryptography scheme (EVCS).

In this chapter we will only consider the construction of the weak EVCS model. The weak EVCS model is realized by starting out, for some $n \in N$ such that $n \geq 2$, with a collection of $n+1$ images: n images, each corresponding to a share, and the secret image. The main difference between the VCS and EVCS models lies in the construction of the collection of matrices used in pixel encoding. Rather than having two collections C_0 and C_1 for creating shares, as in the VCS model, we now have 2^n pairs, ${C_0}^{c_1,\ldots,c_n}, {C_1}^{c_1,\ldots,c_n}$, where $c_1, \ldots, c_n \in \{0,1\}$, of matrix collections. We use the matrix collections as follows: Let 0 denote a white pixel, and 1 denote a black pixel. To encode a pixel in the secret image, we choose a matrix from ${C_c}^{c_1,\ldots,c_n}$, where $c \in \{0,1\}$ is the color of the secret pixel, and for each $i \in \{1,\ldots,n\}$, $c_i \in \{0,1\}$ is the color of the corresponding pixel in share i.

Stinson et al. define an EVCS for an access structure Γ as follows:

Definition 2.7. [3, *Definition* 3.1] *Let* (Γ_Q, Γ_F) *be an access structure on a set of* n *participants and* $m, n, r \in \mathbb{N}$. *A family of* 2^n *pairs of share collections of* $n \times m$ *Boolean matrices* $\{{C_0}^{c_1,\ldots,c_n}, {C_1}^{c_1,\ldots,c_n}, \}$ *where* ${C_i}^{c_1,\ldots,c_n} = \{M^{i,1}, \ldots, M^{i,r}\}$, $c_1, \ldots, c_n \in \{0,1\}$, *and* $i \in \{0,1\}$, *constitutes a weak* $((\Gamma_Q, \Gamma_F, m)$*-EVCS), if there exist values* $\alpha \in \mathbb{R}$ *and* $t_X \in \mathbb{N}$ *satisfying the following conditions.*

1. Any qualified set $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_Q$ can recover the shared image.
   Formally, for any $X \in \Gamma_Q$ *and for any* $\{c_1, \ldots, c_n \in \{0,1\}\}$ *the threshold* t_X *and relative difference* α *are such that for any* $M \in {C_0}^{c_1,\ldots,c_n}$ *we have that* $w(M_X) \leq t_X - \alpha \cdot m$*; whereas, for any* $M \in {C_1}^{c_1,\ldots,c_n}$ *it results that* $w(M_X) \geq t_X$.

2. Any (forbidden) set $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_F$ has no information on any of the shared images.
   Formally, for any $c_{i_1}, \ldots, c_{i_p} \in \{0,1\}$*, any* $i \in \{0,1\}$*, and for any* $X \in \Gamma_F$*, there exists a permutation* π *on the set* $\{1, \ldots, r\}$*, such that for any* $k \in \{1, \ldots, r\}$ *it holds that* $(M^{1,k})_X = (M^{0,\pi(k)})_X$*, where* $M \in {C_i}^{c_1,\ldots,c_n}$

3. After encoding, the original innocent-looking images are still meaningful, that is, any user will recognize the image on her transparency.
   Formally, for any $j \in \{1, \ldots, n\}$*,* $X = j$ *and any* $\{c_1, \ldots, c_{j-1}, c_{j+1}, \ldots, c_n\} \in \{0,1\}$ *it results that* $w(M_X) > w(M'_X)$*, where* $M \in {C_1}^{c_1,\ldots,c_{j-1}1c_{j+1},\ldots,c_n}$ *and* $M' \in {C_0}^{c_1,\ldots,c_{j-1}0c_{j+1},\ldots,c_n}$.

The first part of the EVCS definition ensures that a set of qualified shares (i.e. a member of Γ_Q), has the ability to correctly reconstruct the secret image by stacking the corresponding transperencies together. The second condition ensures the security of the system by stating that by inspecting each share individually or by stacking together transparencies that belong to a non-qualified set in Γ_F, one gains no insight into the construction of the secret image. The last condition mandates that the original images will still be recognized after they are encoded within the EVCS. In other words, after the n shares are encoded using the 2^n collections ${C_1}^{c_1,\ldots,c_n}, {C_0}^{c_1,\ldots,c_n}$, users will still be able to easily identify the original images on their respective transparencies.

The discussion in this chapter provides information about research efforts in the field of visual cryptography that is for the most part limited to two papers: Shamir and Naor's initial first publication about visual cryptography and the discussion of EVCS's by Stinson et al. We believe that supplying this information is vital in generating a necessary foundation for a discussion of our research results. However, it must be noted that there exist several other important contributions on the subject that we elected not to discuss in detail. A significant part of the research papers in the visual cryptography

field focus on the contrast problem that is inherent in VCS's and all VCS based schemes.

Chapter 3

Simultaneous Visual Cryptography Schemes

This section defines and shows how to construct simultaneous visual cryptography schemes (SVCS). An SVCS enables the user to encode an arbitrary number of secret images across a single set of shared images. As in our discussion of VCS's and EVCS's, we assume that there are no *isolated* participating shares. In other words, no single share will contain an entire secret image.

As is with a VCS, with a SVCS we start out with a set P of n participating shares. Recall that in an access-structure-based VCS one may place a subset of P in a qualifying or forbidden set, depending on whether one wishes for the subject to recover the image or to not be able to recover anything about the image. Since a SVCS contains multiple secret images, we require each secret image to have its own qualifying set. A single forbidden set, in which belonging to the forbidden set means the shares gain nothing about any secret image, will suffice. Within this forbidden set we store all share combinations that do not decode any of the secret images.

Definition 3.1. *Let $q, n, m \in \mathbb{N}$ and $\mathcal{P} = \{1, \ldots, n\}$. Let $\Gamma_F \subseteq 2^{\mathcal{P}}$ and, for all $i \in \{1, \ldots, q\}$, let $\Gamma_{Q_i} \subseteq 2^{\mathcal{P}}$ such that $\Gamma_{Q_i} \cap \Gamma_F = \emptyset$. Then, we refer to the $(q+1)$-tuple $(\Gamma_{Q_1}, \ldots, \Gamma_{Q_q}, \Gamma_F)$ as a simultaneous access structure.*

In order to prevent a set of attackers from one qualifying set from gaining information about the secret image associated with some other qualifying set, the SVCS definition adds to the security requirements of a VCS one additional requirement. The following definition formally states the requirements

for a SVCS on a simultaneous access strucure.

Definition 3.2. *For $n, q \in \mathbb{N}$, let $(\Gamma_{Q_1}, \ldots, \Gamma_{Q_q}, \Gamma_F)$ be a simultaneous access structure on the set $\mathcal{P} = \{1, \ldots, n\}$. For each $s \in \{0,1\}^n$, let $\mathcal{C}_s = (M^{s,1}, \ldots, M^{s,r})$, be a collection of $n \times m$ Boolean matrices. A* simultaneous visual cryptography scheme $(\Gamma_{Q_1}, \ldots, \Gamma_{Q_q}, \Gamma_F, m) - SVCS$ *exists if there are values $\alpha \in \mathbb{R}$ and $t_X \in \mathbb{N}$, where $X \in \Gamma_{Q_i}$ and $i \in \{1, \ldots, q\}$, that satisfy the following conditions:*

1. For any $i \in \{1, \ldots, q\}$, any qualified set $X \in \Gamma_{Q_i}$ can recover the shared image i by stacking their transparencies.
   Formally, there exists $t_X \in \mathbb{N}$ such that, for any $s \in \{0,1\}^{i-1}0\{0,1\}^{q-i-1}$ and $k \in \{1, \ldots, r\}$ it holds that $w(M_X^{s,k}) \leq t_X - \alpha \cdot m$, and for any $s \in \{0,1\}^{i-1}1\{0,1\}^{q-i-1}$ and $k \in \{1, \ldots, r\}$ it holds that $w(M_X^{s,k}) \geq t_X$.

2. Each forbidden set $X \in \Gamma_F$ has no information on any of the shared images.
   Formally, for any $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_F$ and any $s, s' \in \{0,1\}^q$, there exists a permutation π on set $\{1, \ldots, r\}$ for any $k \in \{1, \ldots, r\}$ such that $M_X^{s,k} = M_X^{s',\pi(k)}$

3. Any qualifying set $X \in \Gamma_{Q_i}$ (where $i \in \{1, \ldots, q\}$) has no information on any other shared image.
   Formally, for any $i \in \{1, \ldots, q\}$, any $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Q_i}$, and any $s \neq s'$, $s, s' \in \{0,1\}^{i-1}\{0\}\{0,1\}^{q-i-1}$ (respectively, $\{0,1\}^{i-1}\{1\}\{0,1\}^{q-i-1}$), there exists a permutation π on $\{1, \ldots, r\}$ such that for any $k \in \{1, \ldots, r\}$ $M_X^{s,k} = M_X^{s',\pi(k)}$.

The first property of the definition deals with the contrast of the image. Instead of having only two r-tuples of matrices to choose from, as in a VCS, in an SVCS with n shared images there are 2^n r-tuples of Boolean matrices. As mentioned previously and in a manner analogous to the security requirements of the VCS, members of the forbidden set provide no information, in a probabilistic sense, about any of the secret images. Thus, by the definition of an SVCS, given any pair of distinct r-tuples of $n \times m$ Boolean matrices $\mathcal{C}_s$ and $\mathcal{C}_{s'}$, where $s, s' \in \{0,1\}^n$, restricting all matrices in $\mathcal{C}_s$ and $\mathcal{C}_{s'}$ to rows corresponding to any forbidden set $X \in \Gamma_F$ will result in a pair of tuples of matrices that are permutations of each other. The

third requirement strengthens the overall security of the system. It states that for any $i \in \{1, \ldots, n\}$ and all distinct tuples of matrices $\mathcal{C}_s, \mathcal{C}'_s$, where $s, s' \in \{0,1\}^{i-1}\{0\}\{0,1\}^{n-i-1}$ (respectively, $s, s' \in \{0,1\}^{i-1}\{1\}\{0,1\}^{n-i-1}$), will produce matrices indistinguishable up to a column permutation when restriced to rows corresponding to any $X \in \Gamma_{Q_i}$. By ensuring that such values are used to represent each white (black, respectively) pixel of a secret image shared by the SVCS, we attain uniformity in the encoding process, which prohibits us from accidently giving away information about the secret image in question.

With the SVCS definition in place, we now focus on explicit constructions of SVCS's. We will first consider a simple SVCS that contains two distinct secret images and is created by *merging together* two VCS's. Then we will present another way of realizing a more efficient and powerful $n-1$ *out of* n SVCS.

3.1 A Very Simple SVCS System

The SVCS in this example is created by using two distinct VCS's whose shares are composed of members of an identical set of shares. Given a VCS that contains two disjoint qualifying sets, we show how to construct an SVCS with two different secret images. We present our construction in Theorem 3.4 and prove its correctness. Theorem 3.4 uses Lemma 3.3, which we state and prove below.

Lemma 3.3. *Let $n, m, k \in \mathbb{N}$ and let M and N be Boolean matrices of size $n \times m$ such that $M \neq N$. Let M and N be indistinguishable up to a column permutation, so that there exists a permutation matrix P_π such that $MP_\pi = N$. Then after inserting the exact same k rows, each containing either only zeros or only ones, into M and N, we obtain matrices N' and M' of size $(n+k) \times m$ such that $M'P_\pi = N'$.*

Proof. Matrices M and N are modified in the same manner, such that the same k rows are added to the matrices in the same positions. Multiplying a vector V of length m that contains all the same elements with P_π yields vector V as the result. Therefore all changes to matrix M' will be reflected in N'. □

The formal definition of the SVCS is presented in the theorem below,

which is followed by an extensive proof that ensures the validity of the proposed system in accordance to Definition 3.2.

Theorem 3.4. *Let Γ_{Q_1} and Γ_{Q_2} be subsets of $2^{\mathcal{P}}$ such that, for all $X_1 \in \Gamma_{Q_1}$ and $X_2 \in \Gamma_{Q_2}$, $X_1 \cap X_2 = \emptyset$, and let $\Gamma_{R_i} = \{Z \mid (\exists\, X_i \in \Gamma_{Q_1} \cup \Gamma_{Q_2})\ [Z \cap X_i \neq \emptyset]\}$. Let $\Gamma_{F_1} = 2^{\mathcal{P}} - \{X \supseteq Y | Y \in \Gamma_{Q_1}\} - \Gamma_{R_1}$ and $\Gamma_{F_2} = 2^{\mathcal{P}} - \{X \supseteq Y | Y \in \Gamma_{Q_2}\} - \Gamma_{R_2}$. If there exists a $(\Gamma_{Q_1}, \Gamma_{F_1}, m)$-VCS and a $(\Gamma_{Q_2}, \Gamma_{F_2}, m)$-VCS, then there exists a $(\Gamma_{Q_1}, \Gamma_{Q_2}. \Gamma_{F_2} \cap \Gamma_{F_1})$-SVCS.*

Proof. Without loss of generality, let $\mathcal{C}_{0,l}$ denote the Boolean matrix collection $\mathcal{C}_0$ of a $(\Gamma_{Q_l}, \Gamma_{F_l}, m)$ VCS, where $l \in \{1, 2\}$. Furthermore, let $\alpha = \min\{\alpha_1, \alpha_2\}$, where, for $l \in \{1, 2\}$, α_l is the relative difference of the $(\Gamma_{Q_l}, \Gamma_{F_l}, m)$ VCS. We construct basis matrices S^{ij}, where $i, j \in \{0, 1\}$, for the $(\Gamma_{Q_1}, \Gamma_{Q_2}, \Gamma_{F_2} \cap \Gamma_{F_1})$-SVCS. Since the members of Γ_{Q_1} and Γ_{Q_2} do not share common elements, we can build S^{ij} in the following manner:

> For $i, j \in \{0, 1\}$, Choose some $M \in \mathcal{C}_{i,1}$ and, for all $X \in \Gamma_{Q_1}$ and $v \in X$, let the v^{th} row of S^{ij} be the v^{th} row of M so that $S^{ij}_X = M_X$. Choose $M \in \mathcal{C}_{j,2}$ and, for all $X \in \Gamma_{Q_2}$ and $v \in X$, let the v^{th} row of S^{ij} be the v^{th} row of M so that $S^{ij}_X = M_X$. Let each remaining row of S^{ij} contain only zeros.

We construct Boolean matrix collections $\mathcal{C}_{ij}$ by using $S^{ij} \in \mathcal{C}_{ij}$ as a SVCS basis matrix in accordance to Definition 2.6, so that we obtain an r-tuple of Boolean matrices $\mathcal{C}_{ij} = (M^{ij,1}, \ldots, M^{ij,r})$

We will now prove that the above construction meets the requirements imposed by Definition 3.2 and that S^{ij} represents a valid SVCS basis matrix. Below, for each of the three requirements of the SVCS, we justify this claim.

1. Considering the construction of this SVCS and the definitions 2.6 and 3.2, we know that for any $X \in \Gamma_{Q_l}$ and any $M \in \mathcal{C}_{0,l}$, where $l \in \{1, 2\}$, we get $w(M_X) \leq t_X - \alpha \cdot m$, and for any $M \in \mathcal{C}_{1,l}$ it holds that $w(M_X) \geq t_X$, so that also for all $M \in \mathcal{C}_{0j}$ and $k \in \{1, \ldots, r\}$, it holds that $w(M^{0j,k}_X) \leq t_X - \alpha \cdot m$, and for all $M \in \mathcal{C}_{1j}$, it holds that $w(M^{1j,k}_X) \geq t_X$. Thus, X meets the first requirement of Definition 3.2.

2. For this requirement choose $X \in \Gamma_{F_1} \cap \Gamma_{F_2}$. We have to consider three possible cases for members of the forbidden set:

(a) Suppose that for any $Y \in \Gamma_{Q_1} \cup \Gamma_{Q_2}$ it holds that $X \cap Y = \emptyset$. By the SVCS construction, for all $M^{s,k} \in \mathcal{C}_s$ and $M^{s',k'} \in \mathcal{C}_{s'}$, there exists a permutation matrix P_π such that $M_X^{s,k} P_\pi = M_X^{s',k'}$, where $s, s' \in \{i,j\}^2$ and $k, k' \in \{1,\ldots,r\}$. Thus, X satisfies the second condition of Definition 3.2.

(b) Suppose that for some $Y \in \Gamma_{Q_1} \cup \Gamma_{Q_2}$, we have $X \subsetneq Y$, and suppose WLOG that $Y \in \Gamma_{Q_1}$. By the SVCS construction and Definition 2.4, it holds that $M_X^{ij,k} = M_X^i$, for any $i \in \{0,1\}$ where $M^i \in \mathcal{C}_{i,1}$, so that there exists a permutation matrix P_π such that for matrices $M^{s,k} \in \mathcal{C}_s$ and $M^{s',k'} \in \mathcal{C}_{s'}$ it holds that $M_X^{s,k} P_\pi = M_X^{s',k'}$, where $s, s' \in \{i,j\}^2$ and $k, k' \in \{1,\ldots,r\}$. Thus, X satisfies the second condition of Definition 3.2.

(c) Suppose that for any $Y \in \Gamma_{Q_1} \cup \Gamma_{Q_2}$, $X \cap Y \neq \emptyset$, $Y \neq X$ and $Y \nsubseteq X$. In other words, X can contain combinations of a strict subset of any member of a qualifying set and shares that are strictly in the forbidden set. Let $J \subseteq X$, where $J \cap Y = \emptyset$, and let $K \subseteq X$, where $K \subsetneq Y$ and $J \cup K = X$. We know that there exist permutation matrices P_π, such that for matrices $M^{s,k} \in \mathcal{C}_s$ and $M^{s',k'} \in \mathcal{C}_{s'}$ it holds that $M_J^{s,k} P_\pi = M_J^{s',k'}$ and $M_K^{s,k} P_\pi = M_K^{s',k'}$, where $s, s' \in \{i,j\}^2$ and $k, k' \in \{1,\ldots,r\}$. Considering Lemma 3.3 and the construction of the SVCS, we know that there exists a permutation matrix P_π such that for matrices $M^{s,k} \in \mathcal{C}_s$ and $M^{s',k'} \in \mathcal{C}_{s'}$ it holds that $M_X^{s,k} P_\pi = M_X^{s',k'}$, where $s, s' \in \{i,j\}^2$ and $k, k' \in \{1,\ldots,r\}$. Thus, X satisfies the second condition of Definition 3.2.

3. By the SVCS construction and WLOG, for all possible $M^{0j,k} \in \mathcal{C}_{0j}$, let $M \in \mathcal{C}_{0,1}$ and it holds that $M_X^{0j,k} = M_X$, where $j \in \{0,1\}$, $k \in \{1,\ldots,r\}$, $X \in \Gamma_{Q_1}$. Thus, X satisfies the third condition of Definition 3.2.

□

Although we have proved it to be valid and functional, the simple SVCS system described in this section contains severe restrictions in its definition. A major limitation of the system is obvious: The conditions imposed on the

construction of the forbidden sets Γ_{F_1} and Γ_{F_2}, whose intersection makes up the forbidden set for the entire SVCS system, are severe. The system assumes no solution for sets of shares that are supersets of members of either qualifying set, as well as sets that partially contain members of both qualifying sets Γ_{Q_1} and Γ_{Q_2}. Therefore, the SVCS is only secure if attackers examine sets of shares that are subsets of any member of one of the qualifying sets, are not found in any member-set of a qualifying set, or both. We would like an SVCS system whose definition includes less restrictive requirements for the forbidden set.

3.2 An $n-1$ out of n SVCS

In this section we describe a $n-1$ out of n SVCS, where n represents the total number of shares. The design of the system enables every possible combination of $n-1$ shares to represent a pixel in its respective secret image. Since there are n possible combinations of $n-1$ shares and each can reconstruct either a black or a white pixel of one secret image, the SVCS must provide 2^n different collections $\mathcal{C}_s$, where $s = \{0,1\}^n$

The description of regular VCS's has already shown, by distinguishing between strong and weak VCS systems, that there exist valid sharing schemes that include combinations of shares whose results are not necessarily included in the forbidden or qualifying set. In comparison to the above-described basic SVCS, the SVCS presented in this section is more powerful in regard to security and the restrictions imposed on forbidden and qualifying sets. However, we increase the number of subpixels per share in order to facilitate these improvements.

The basic underlying principle utilized in the construction of this SVCS system is to horizontally concatenate basis matrices of VCS systems in order to create basis matrices for the resulting SVCS. Before we discuss the general construction of $n-1$ out of n SVCS's, we prove a second lemma, which is about properties of horizontal concatenation. This lemma contains an operation that is extensively used in this SVCS construction. We also formally define the notion of horizontal concatenation of matrices in Definition 3.5.

Definition 3.5. *Let A and B be $n \times m$ Boolean matrices such that*

$$A = \begin{bmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{bmatrix}$$

and

$$B = \begin{bmatrix} b_{1,1} & \cdots & b_{1,m} \\ \vdots & . & \vdots \\ b_{n,1} & \cdots & b_{n,m} \end{bmatrix}$$

Furthermore, let C be a $n \times 2m$ Boolean matrix that is the result of a horizontal concatenation of matrices A and B such that $C = A|B$ and

$$C = \begin{bmatrix} a_{1,1} & \cdots & a_{1,m} & b_{1,1} & \cdots & b_{1,m} \\ \vdots & . & \vdots & \vdots & & \vdots \\ a_{n,1} & \ldots & a_{n,m} & b_{n,1} & \ldots & b_{n,m} \end{bmatrix}$$

Lemma 3.6. *Let M_1, M_2, N_1, and N_2 be $n \times m$ Boolean matrices such that, for $m \times m$ permutation matrices P_{π_1} and P_{π_2} it holds that $M_1 P_{\pi_1} = M_2$ and $N_1 P_{\pi_2} = N_2$. Then there exists a $2m \times 2m$ permutation matrix P_{π_3} such that $(M_1|N_1)P_{\pi_3} = (M_2|N_2)$.*

Proof. Given the above construction and without loss of generality, if $P_{\pi_3} = \begin{bmatrix} P_{\pi_1} & \mathbf{0} \\ \mathbf{0} & P_{\pi_2} \end{bmatrix}$, then $(M_1|N_1)P_{\pi_3} = (M_2|N_2)$.

□

In the following definition, we formally define the requirements for the k out of n SVCS.

Definition 3.7. *For $n, k, q \in \mathbb{N}$, a k out of n SVCS is a $(\Gamma_{Q_1}, \ldots, \Gamma_{Q_q}, \Gamma_F, m) - SVCS$, where $q = \binom{n}{k}$, for each $X \subseteq \mathcal{P}$ such that $|X| = k$ there is an $i \in \{1, \ldots, q\}$ such that $\Gamma_{Q_i} = \{X\}$, and $\Gamma_F = \{X \subseteq \mathcal{P} \mid |X| < k\}$.*

The following theorem contains a formal construction of a $n-1$ out of n SVCS and is directly followed by a proof of its validity.

Theorem 3.8. *Given an* $(n-1)$ *out of* $(n-1)$ *VCS with Boolean matrix collections* $\mathcal{C}_0$ *and* $\mathcal{C}_1$*, choose for each* $i \in \{0,1\}$ *a matrix* $B_i \in \mathcal{C}_i$*. For each* $j \in \{1,\ldots,n\}$ *let* $D_{i,j}$ *be the unique matrix satisfying* $(D_{i,j})_{\{1,\ldots,n\}-\{j\}} = B_i$ *and* $w((D_{i,j})_{\{j\}} = 0)$*. For each* $c_1,\ldots,c_n \in \{0,1\}$*, let* $s = c_1 \cdots c_n$ *and let* $M^s = D_{c_1,1}|D_{c_2,2}|\cdots|D_{c_n,n}$*. Let* $M \in \mathcal{C}_s$ *and form the Boolean matrix share collection* $\mathcal{C}_s = (M^{s,1}\ldots,M^{s,r})$ *by using* M *as the basis matrix in accordance to Definitions 2.6 and 3.2. Then the collections* $\{\mathcal{C}_s = s \in \{0,1\}^n\}$ *form an n-1 out of n SVCS.*

Proof. We prove that the above theorem provides an SVCS construction that meets all the requirements imposed by Definitions 3.2, 3.7 and 2.6, and thus is a valid $n-1$ out of n SVCS.

Let $s = \{c_1 \cdots c_n\}$ and $k \in \{1,\ldots,r\}$, where $c_j \in \{0,1\}$ and $f,g,h,j \in \{1,\ldots,n\}$.

1. For all $M^{s,k} \in \mathcal{C}_s$ and $X \in \Gamma_{Q_j}$, it results that $M^{s,k}_X$ is the equivalent of n horizontal concatenations of matrices $(D_{c_1,1})_X|\cdots|(D_{c_f,f})_X|\cdots|(D_{c_n,n})_X$. Given the SVCS construction, we know that, for any $X \in \Gamma_{Q_j}$, we obtain $(D_{c_j,j})_X = B_{c_j}$. Thus, it holds that $w((D_{c_j,j})_X) \leq t_X - \alpha \cdot m$, if $c_j = 0$, and $w((D_{c_j,j})_X) \geq t_X$, if $c_j = 1$. For all other $(D_{c_g,g})_X$ and $(D_{c_h,h})_X$, where $j \neq g$, $j \neq h$ and $h \neq g$, it holds that there exist $J, J' \in X$, $|J| = |J'| = 1$ such that $(D_{c_g,g})_J = (D_{c_h,h})_{J'} = R$. Furthermore, it holds that, for $Y = \{X\} - \{J\}$ and $Y' = \{X\} - \{J'\}$, there exists a permutation matrix P_π such that $(D_{c_g,g})_Y P_\pi = (D_{c_h,h})_{Y'}$. Thus, we obtain $w((D_{c_g,g})_X) = w((D_{c_h,h})_X)$, and we know that for any $X \in \Gamma_{Q_j}$, it results that $w(M^{s,k}_X) \leq t_X - \alpha \cdot m$ and $w(M^{s,k}_X) \geq t_X$, if $c_j = 0$, $c_j = 1$ respectively. Therefore, X meets the first requirement of Definition 3.2.

2. For all $M^{s,k} \in \mathcal{C}_s$ and all $X \in \Gamma_F$, it results that $M^{s,k}_X$ is the equivalent of n horizontal concatenations of matrices $(D_{c_1,1})_X|\cdots|(D_{c_f,f})_X|\cdots|(D_{c_n,n})_X$. For all $|X| = z$, where $1 < z < n-1$, it holds that for z matrices $(D_{c_f,f})_X$ we obtain $(D_{c_f,f})_X = (B_i)_X$. By Definition 2.4 we know that there exists a permutation matrix P_π such that $(B_{c_j})_X P_\pi = (B_{c_g})_X$, where $j \neq g$. Given Lemma 3.3, we know that for the remaining $n-z$ matrices $(D_{c_f,f})_X$ it holds that there exists a permutation matrix P_π such that $(D_{c_j,j})_X P_\pi = (D_{c_g,g})_X$ if $(D_{c_j,j})_J = (D_{c_g,g})_J = R$, for some $J \in X$, $|J| = 1$. Thus, it holds that

there exist matrices $M_X^{s,k} = M_X^{s',k}$, where $M^{s',k} \in \mathcal{C}_{s'}$ and $s \neq s$, and X meets the second requirement of Definition 3.2.

3. For all $M^{s,k} \in \mathcal{C}_s$ and $X \in \Gamma_{Q_j}$, it results that $M_X^{s,k}$ is the equivalent of n horizontal concatenations of matrices $(D_{c_1,1})_X | \cdots | (D_{c_f,f})_X | \cdots | (D_{c_n,n})_X$. Let WLOG $s, s' \in \{0,1\}^{i-1}\{0\}\{0,1\}^{n-i-1}$, and $M^{s',k} \in \mathcal{C}_{s'}$, so that $M_X^{s,k}$ is the equivalent of n horizontal concatenations of matrices $(D'_{c_1,1})_X | \cdots | (D'_{c_f,f})_X | \cdots | (D'_{c_n,n})_X$. Referring to the SVCS construction, we know that $(D_{c_j,j})_X = B_{c_j} = (D'_{c_j,j})_X$. Furthermore, given Lemma 3.3, we know that for all other $(D_{c_f,f})_X$ and $(D'_{c_f,f})_X$ it holds that $(D_{c_f,f})_X P_\pi = (D'_{c_f,f})_X$. Thus, X meets the third requirement of Definition 3.2.

4. Given that for all $X \in \Gamma_F$ it holds that $1 < |X| < n-1$, and for all $Y \in \Gamma_{Q_j}$ it holds that $|Y| = n-1$, there are $q = \binom{n}{n-1} = n$ qualifying sets Γ_{Q_j}. Thus, the SVCS is a valid $n-1$ out of n in accordance to Definition 3.7.

□

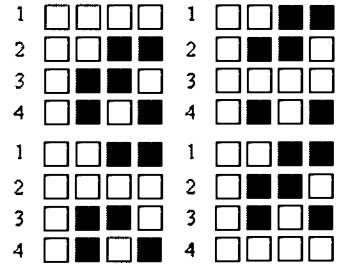

Figure 3.1: Example of four $(D_{0,j})$ matrices for a 3 out of 4 SVCS. The matrix in the top left corner is $(D_{0,1})$. Its first row contains only white subpixel, and the remaining three rows comprise matrix B_0. The matrix in the bottom left corner is $(D_{0,2})$, and matrices $(D_{0,3})$ and $(D_{0,4})$ are depicted on the right side of the figure.

Fig. 3.1 and 3.2 show visual examples of a $(D_{0,j})$ Boolean matrix, respectively $(D_{1,j})$, in a 3 out of 4 SVCS, in order to further help demonstrate

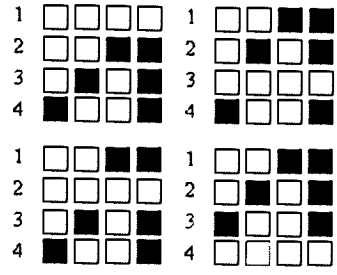

Figure 3.2: Example of four $(D_{1,j})$ Matrices for a 3 out of 4 SVCS. The matrix in the top left corner is $(D_{1,1})$. Its first row contains only white subpixel, and the remaining three rows comprise matrix B_1. The matrix in the bottom left corner is $(D_{1,2})$, and matrices $(D_{1,3})$ and $(D_{1,4})$ are depicted on the right side of the figure.

how to construct basis matrices for a $n-1$ out of n SVCS. For both Fig. 3.1 and 3.2, it holds that each of the four pictured matrices contains one row R that contains only white elements, represening zeros in a Boolean matrix. Furthermore, we see that for Fig. 3.1, Fig. 3.2 respectively, row R is located in different row for each of the pictured four matrices.

In Fig. 3.3, we see that matrix S^{0000} is the result of a horizontal concatenation of four matrices pictured in Fig. 3.1. Similarly, matrix S^{1111} is the result of concatenating the four matrices pictured in Fig. 3.2. It is highly important to note that for each matrix S in Fig. 3.3, each of the four matrices D that are used for the horizontal concatenation operation must contain a row R, but it must not be at the same position, as demonstrated by the matrices in Fig. 3.1 and 3.2.

Referring to Fig. 3.4, we observe the difference in results after performing a Boolean OR on rows $\{1,2,3\}$ and $\{2,3,4\}$, respectively, thus proving that it is possible to establish a difference in contrast between combinations of shares representing a white pixel and combinations representing a black pixel of a secret image.

In the above-described SVCS, we assume that the system contains n secret images and that each secret image requires a combination of $n-1$ shares for its decoding process. Given its construction and the lack of restrictions imposed on the forbidden set Γ_F of the $n-1$ out of n SVCS, it becomes evident that we have reached the goal of developing a more secure and powerful SVCS than

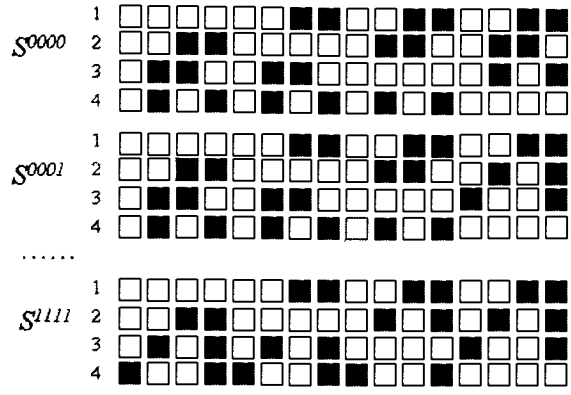

Figure 3.3: The resulting basis matrices for a 3 out of 4 SVCS. Matrix S^{0000} consists of a horizontal concatenation of matrices $(D_{0,1})$, $(D_{0,2})$, $(D_{0,3})$, and $(D_{0,4})$, and matrix S^{0001} of $(D_{0,1})$, $(D_{0,2})$, $(D_{0,3})$, and $(D_{1,4})$. Following the same pattern, the matrix S^{1111} is represented by the concatenation of matrices $(D_{1,1})$, $(D_{1,2})$, $(D_{1,3})$, and $(D_{1,4})$.

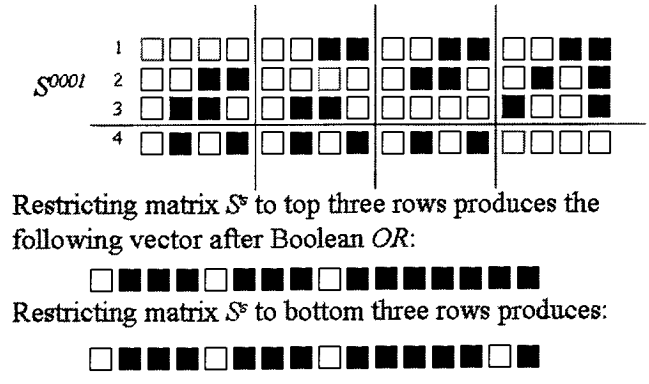

Figure 3.4: Example of resulting vectors V for a basis matrix S^{0001} of a 3 out of 4 SVCS. The Hamming weight of the vector obtained by extracting the top three rows from the matrix is greater than the Hamming weight of the vector obtained by a combination of any other three rows.

the system introduced in Theorem 3.4. Thus, we conclude our discussion of SVCS's.

Chapter 4

Conclusion and Considerations for Further Research

In this thesis, we first presented a general discussion of VCS's, by introducing the notions of pixel encoding and secret image decoding, then we discussed the formal VCS definition provided by Naor and Shamir [1]. We also included a number of theorems from Naor and Shamir's work, specifically theorems defining bounds on values for VCS parameters. We introduces two new definitions. First, we introduced a new, more rigorous VCS definition that features new notation and better suits our research efforts, and then we introduced a definition that lists the formal requirements for all basis matrices. We concluded the general discussion of VCS's by discussing proposed VCS extensions, which also included a brief discussion of EVCS's. With the discussion of VCS's as our basis, we utilized these results to formally define SVCS's and its parameters, as well as develop security measures to ensure their stability. Furthermore, we introduced two general SVCS constructions in the thesis. The first SVCS entailed a very simple and restricted scheme, whereas the discussion of the $n - 1$ out of n SVCS demonstrated how to construct a more complicated and powerful system.

With the formal definition of SVCS's in place, there exists an immediate need to formally define the bounding values for SVCS parameters. In particular, we believe that the next step in this research would focus on finding the bounding values for the pixel extension value m for an $n - 1$ out of n SVCS. Other possible extensions of this thesis include developing a k out of n SVCS, where $1 < k < n$, and defining the bounding values for its parameters.

Bibliography

[1] Naor, M., & Shamir, A. (1995). Visual Cryptography. *Lecture Notes in Computer Science, 950,* 1-12.

[2] Stinson, D., Ateniese, G., Blundo, C., & De Santis, A. (1996). Visual Cryptography for General Access Structures. *Information and Computation, 129.2,* 86-106.

[3] Stinson, D., Ateniese, G., Blundo, C., & De Santis, A. (2001). Extended Capabilities for Visual Cryptography. *Theoretical Computer Science, 250.1-2,* 143-161.

[4] Stinson, D., Ateniese, G., Blundo, C., & De Santis, A. (1999). Visual Cryptography and Threshold Schemes. *IEEE Potentials, 18,* 13-16.

[5] Stinson, D., Ateniese, G., Blundo, C., & De Santis, A. (1996). Constructions and Bounds for Visual Cryptography. *Lecture Notes in Computer Science, 1099,* 416-428.

[6] Stinson, D., & Blundo, C. (1999). On the Contrast in Visual Cryptography Schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research, 12.4,* 261-289.

[7] Stinson, D., & Eisen, P. A., (2002). Threshold Visual Cryptography Schemes With Specified Whiteness Levels of Reconstructed Pixels. *Designs, Codes and Cryptography, 25,* 15-61.

[8] Stinson, D., Blundo, C., De Santis, A., & D'Arco, P. (2003). Contrast Optimal Threshold Visual Cryptography Schemes. *SIAM Journal on Discrete Mathematics, 16,* 224-261.

[9] Hofmeister, T., Krause, M., & Simon, H., (2000). Contrast-Optimal k out of n Secret Sharing Schemes in Visual Cryptography. *Theoretical Computer Science, 240,* 471-485.

[10] Rosen., K. H. (1999). *Discrete Mathematics and Its Applications.* Boston: WCB/McGraw-Hill.

[11] Trappe, W., & Washington, L. C., (2002). *Introduction to Cryptography with Coding Theory.* Upper Saddle River, NJ: Prentice Hall.

[12] Naor, M., & Shamir, A. (1996). Visual Cryptography II: Improving the Contrast Via the Cover Base. *Lecture Notes in Computer Science, 1189,* 197-202.

[13] Paul, N., Evans, D., & Rubin, A., (2003). Authentication for Remote Voting. *ACM Workshop on Human-Computer Interaction and Security Systems.*

[14] Thompson. T. (2000). *RIT Master's Project: Visual Cryptography.* Retrieved Feb 20, 2006, from `http://citeseer.ifi.unizh.ch/thompson00rit.html`.

Appendix A

SVCS Example

Below we present an example of a 2 out of 3 SVCS, which we generated by developing a small application. We wrote this simple SVCS application in Java and partially based it on code from the EVCK system developed by Dario Fiore. The EVCK code is available from Dario Fiore's website (`http://www.scoutweb.it/dariofiore/evck.html`), and if you wish to obtain the SVCS code, please send an e-mail to `oxk2361@cs.rit.edu`.

The simple SVCS example presented below consists of 3 shares and decodes 3 secret images. Each of the three combinations of 2 shares produces a secret image. The user is required to provide the secret images and initial share images, which must all have identical dimensions and formats or the program will halt. All image files must be in `.PNG` format. The program generates the share images by analyzing the provided secret images and overwrites the initial share images provided by the user. Furthermore, the user can view all resulting share images and the results of the superposition of any two share images in a GUI environment.

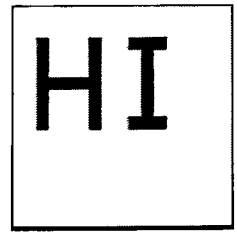

Figure A.1: Secret Image 1

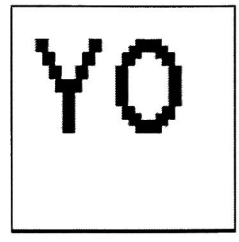

Figure A.2: Secret Image 2

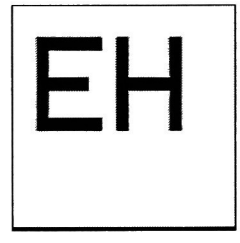

Figure A.3: Secret Image 3

A.1 Share Images

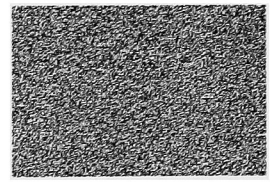

Figure A.4: Share Image 1

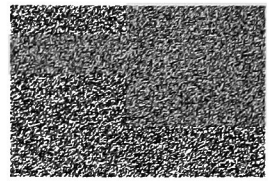

Figure A.5: Share Image 2

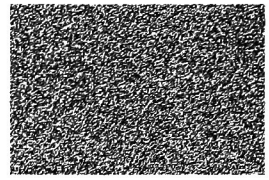

Figure A.6: Share Image 3

A.2 Superposition of Share Images

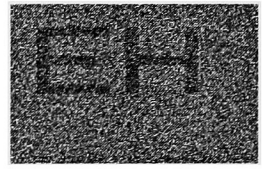

Figure A.7: Superposition of Share Image 1 and Share Image 2

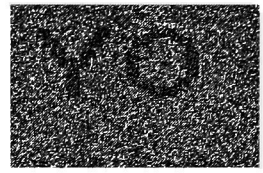

Figure A.8: Superposition of Share Image 1 and Share Image 3

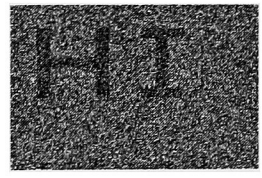

Figure A.9: Superposition of Share Image 2 and Share Image 3