

VISUAL CRYPTOGRAPHY WITH CHEATING SHARES

by

Shanfeng Huang

A thesis submitted to the faculty of graduate studies
Lakehead University
in partial fulfillment of the requirements for the degree of
Masters of Science in Computer Science

Department of Computer Science

Lakehead University

April 2006

Copyright © Shanfeng Huang 2006



Library and
Archives Canada

Bibliothèque et
Archives Canada

Published Heritage
Branch

Direction du
Patrimoine de l'édition

395 Wellington Street
Ottawa ON K1A 0N4
Canada

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file *Votre référence*

ISBN: 978-0-494-24057-1

Our file *Notre référence*

ISBN: 978-0-494-24057-1

NOTICE:

The author has granted a non-exclusive license allowing Library and Archives Canada to reproduce, publish, archive, preserve, conserve, communicate to the public by telecommunication or on the Internet, loan, distribute and sell theses worldwide, for commercial or non-commercial purposes, in microform, paper, electronic and/or any other formats.

The author retains copyright ownership and moral rights in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

AVIS:

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque et Archives Canada de reproduire, publier, archiver, sauvegarder, conserver, transmettre au public par télécommunication ou par l'Internet, prêter, distribuer et vendre des thèses partout dans le monde, à des fins commerciales ou autres, sur support microforme, papier, électronique et/ou autres formats.

L'auteur conserve la propriété du droit d'auteur et des droits moraux qui protègent cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

In compliance with the Canadian Privacy Act some supporting forms may have been removed from this thesis.

Conformément à la loi canadienne sur la protection de la vie privée, quelques formulaires secondaires ont été enlevés de cette thèse.

While these forms may be included in the document page count, their removal does not represent any loss of content from the thesis.

Bien que ces formulaires aient inclus dans la pagination, il n'y aura aucun contenu manquant.


Canada

Contents

List of Figures	v
Preface	vi
Acknowledgement	vii
1 Introduction	1
1.1 Statement of Visual Cryptography	1
1.2 Contribution of This Thesis	2
1.3 Outline of The Thesis	3
2 Secret Sharing Scheme	4
2.1 Traditional Secret Sharing scheme	4
2.2 The Comparison with Visual Cryptography	6
3 Naor and Shamir's Scheme	7
3.1 The Model	7
3.2 2 out of 2 Visual Cryptography	9
3.3 The General k out of k Schemes	9
3.4 The General k out of n Schemes	10
4 Improved Contrast Visual Cryptography Schemes	12
4.1 Blundo, D'Acro, Stantis and Stinson's Scheme	12
4.1.1 The Model	12
4.1.2 Basic Matrices	13
4.1.3 Canonical (k,n)-threshold VCS	14
4.1.4 Contrast Optimal (k,n)- threshold VCS	16
4.2 Duong Quang Viet and Kaoru Kurosawa's Scheme	19
4.2.1 Model	20
4.2.2 Basic Idea	21
4.2.3 Proposed Scheme	22
4.2.4 Perfect White VCS	25

5	Colored Visual Cryptography Schemes	27
5.1	Ching-Nung Yang and Chi-Sung Lai's Scheme	27
5.1.1	Basic Colored VCS	27
5.1.2	A Colored k out of n VCS	29
5.2	Young-Chang Hou's Scheme	31
5.2.1	Basic Principles of Colors	31
5.2.2	Three Algorithms for Colored Visual Cryptography	32
6	Implement Visual Cryptography by Other Methods	38
6.1	P.Tuyts, H.D.L.Hollmann, J.H.v.Lint, L.Tolhuizen's Scheme	38
6.1.1	Model	38
6.1.2	Threshold Visual Secret Sharing Schemes	41
6.1.3	General k out of n visual secret sharing schemes	42
7	Visual Cryptography with cheating shares	45
7.1	Attack Statement	45
7.2	Visual Authentication and Identification Application	49
7.2.1	Visual Authentication Scheme	49
7.2.2	The Proposed Method for Visual Authentication Scheme	53
7.2.3	Comparison	55
7.3	Model	56
7.4	Attacks with different levels	57
7.4.1	Partially Successful Attack	57
7.4.2	Completely Successful Attack	59
7.5	Visual Cryptography Scheme Application	59
7.5.1	Definition and Setting	59
7.5.2	Grey Background Method	61
7.6	Attacks on k out of n visual cryptography schemes	63
8	Conclusion	67
	References	69
	Bibliography	69

List of Figures

1.1	A Simple Example of 2 out of 2 Visual Cryptography	2
3.1	subpixels of 2 out of 2 visual cryptography	9
4.1	Proposed (2,2)-VCS(1)	22
4.2	Proposed (2,2)-VCS(2)	23
4.3	Perfect white (2,2)-VCS	26
5.1	the infrastructure of colored subpixel and its OR operation(1)	28
5.2	the infrastructure of colored subpixel and its OR operation(2)	29
5.3	Three colored (3,3)-VCS's subpixels for color 0	30
5.4	Color image printing	33
5.5	Scheme 1 of color cryptography	34
5.6	Scheme 2 of color cryptography	35
5.7	Scheme 3 of color cryptography	36
6.1	Structure and principle of an LC display.	39
6.2	Visual cryptography system by superimposing two LC layers.	40
6.3	Tables for the model	40
7.1	Original text with secret information "EF"	46
7.2	Shares after Encryption	46
7.3	Normal resulting image after Decryption	47
7.4	Share 3 changed from share1 by the traitor	47
7.5	The changed resulting image with different information "FE"	47
7.6	(a)The bounding box depicted on user's transparency (b) The composed image	51
7.7	Many-times visual authentication scheme.	53
7.8	Success Attack with false share	54
7.9	Model	56
7.10	The attacks on the grey pixel	62
7.11	The improved method for Visual Cryptography Scheme	62

Preface

Visual cryptography is a technique that applies the human visual system to decode encrypted information, such as text, image and number, without any sophisticated devices and computing capabilities. Therefore, compared with the traditional cryptography, it is apparent that it saves a large amount of time and money on devices and computations. Also, visual cryptography provides the convenience for humans to carry out decryption with a portal card which is significant to the business application. In the past decade, visual cryptography has been thoroughly researched not only on its contrast and subpixel expansion, but also on its applications.

The main contribution of this thesis is the security of visual cryptography related to the dishonest shareholders. This is the first known work concerning this variety of potentially secure problem. In the previous papers, the shareholders are inherently honest. However, in the real world, it is impossible to guarantee that every shareholder would be honest forever (e.g., because of the interest of business or military, some shareholders might change to be the traitors). Therefore, a new method based on visual authentication[16] is proposed and the improvement is also made. In this thesis, we also review the previous papers on different fields of the visual cryptography.

Acknowledgement

First of all, I really appreciate Dr. Wei who helps me a lot and offers valuable guidance during my graduate study in Lakehead University. It's my pleasure to study and to do the research with him.

Secondly, I would like to deliver my many thanks to all the professors in the department of Mathematics and Computer Science, especially for Dr. Li who provides a lot of advice on this thesis. In fact, as a graduate student and a teaching assistant, I received much help from all these professors.

Last but not least, I would gratefully thank my parents for offering me this great opportunity to study in Canada and supporting me to accomplish my graduate study.

Chapter 1

Introduction

1.1 Statement of Visual Cryptography

Suppose that five thieves have their loot deposited in a numbered Swiss bank account. As the thief, They do not trust each other and they separately escape to different countries. Also, it is assumed that three or more of them do not implement the conspiracy of taking the money out without any authorization and any three of them are able to withdraw the money. Therefore, they divided the secret(bank account number and password) into shares and from any two or less of them cannot get any information about the secret, but from any three shares they can reconstruct the secret. However, there is twist that the thieves do not know any cryptology knowledge and will not have a computer when withdrawing the money, so they would like the decryption to be visually. Obviously, the solution is visual cryptography.

Visual Cryptography is proposed by Naor and Shamir in 1994 [17]. Compared with the traditional cryptography, visual cryptography is a new technique which allows the visual information, such as text, image and number, to be encrypted in a secure way and the decryption is implemented by human visual system, even without any complicated devices and cryptology knowledge. As we all known, the reliable traditional cryptography depends on a number of sophisticated computations and advanced computers. However, in visual cryptography, the encryption is implemented by splitting the secret text into shares so that after stacking these shares printed on the transparencies carefully by shareholders, they are able to reconstruct the secret. The Figure 1.1 clearly shows the process of visual cryptography.

As a matter of fact, visual cryptography that is a special instance of threshold secret sharing scheme[14] is also called visual secret sharing scheme. In k out of n visual cryptography, the secret is broken up into n shares and the decryption can only be done by k or more shareholders after superimposing their transparencies. Moreover, any $k - 1$ or less shareholders can not obtain any information about the secret even with powerful cryptology capabilities. We will elaborate the secret sharing scheme in Chapter 2 as cryptographic background.

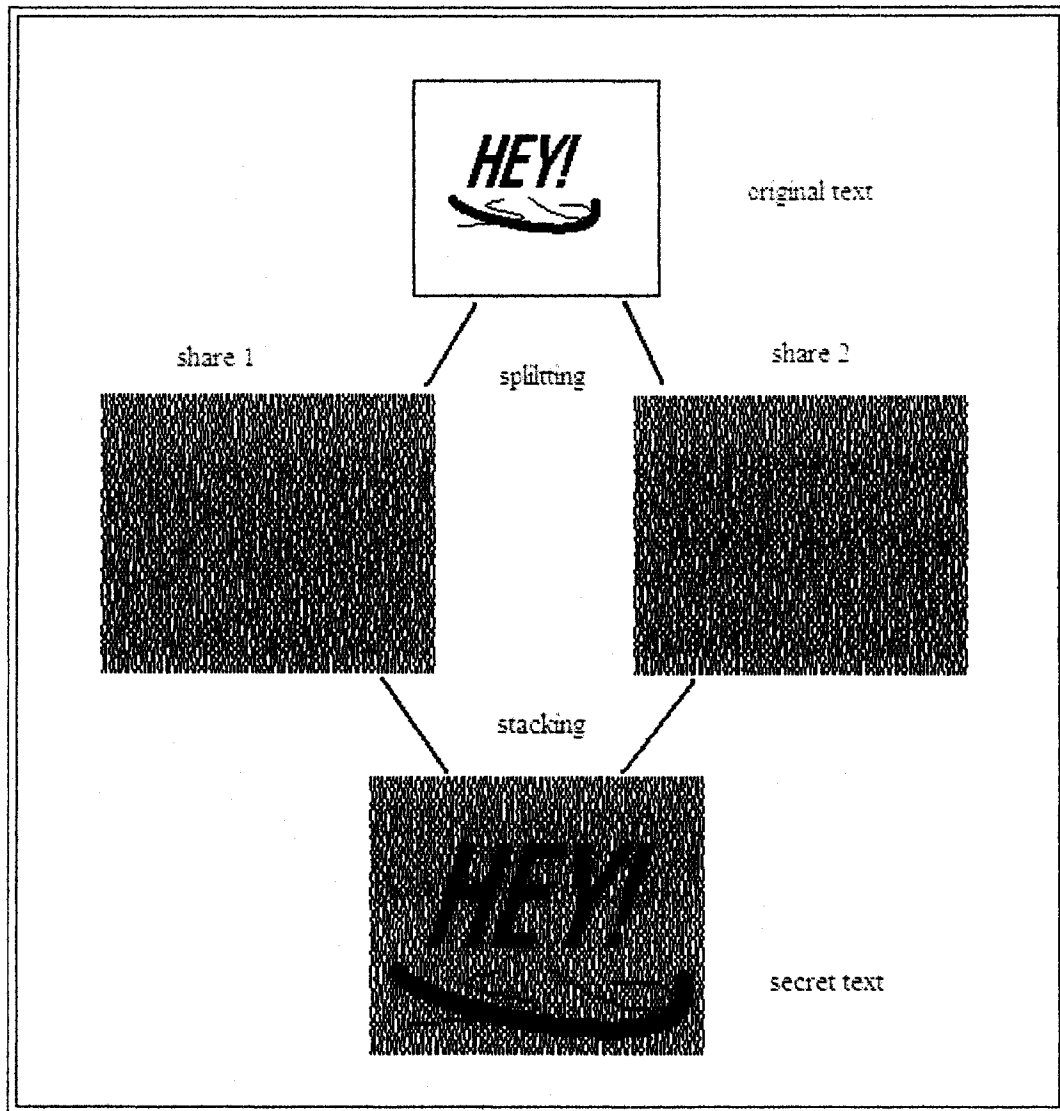


Figure 1.1: A Simple Example of 2 out of 2 Visual Cryptography

1.2 Contribution of This Thesis

In the previous papers, most researchers were concentrated on two directions of visual cryptography: contrast and subpixel expansion which improve the quality of reconstructed image. However, the security of visual cryptography is ignored. The shareholders in the previous literatures are inherently assumed to be honest. Therefore, it would never happen that the shareholders might change from honesty to dishonesty. However, in real world, due to the variety of reasons such as the interest of business and military, the shareholders are unable to keep their loyalty for ever. Thus, we have to take this potential attack into account.

In this thesis, we will focus on the case when some of the shares are changed by

the traitors. For example, the traitors alternate the black pixels to the white ones and vice versa. Then after stacking the qualified number of shares, the resulting image will be naturally considered as the original image though it has been changed. In fact, it is not difficult for traitors to alternate the shares which are printed on the whole transparency. In our thesis, the visual authentication method proposed by Naor and Pinkas [16] is applied to prevent such kind of attacks. Furthermore, we propose a math model to discuss the distinct situations and improve the method in a novel way to reduce the possibilities of successful attacks.

1.3 Outline of The Thesis

The remainder of thesis is organized as follows. In Chapter 2, we present the origins, principles and applications of secret sharing scheme that make us understand visual cryptography better. From Chapter 3 to Chapter 6 we review the previous visual cryptography schemes including the contrast improvement, colored scheme and another method to implement the visual cryptography. In Chapter 7 we propose our method and in Chapter 8 the conclusion is made.

Chapter 2

Secret Sharing Scheme

2.1 Traditional Secret Sharing scheme

Secret sharing scheme is a method which allows a secret to be shared among a finite set of participants in such a way that only qualified subsets of participants can recover it[21]. It is discovered independently by Shamir[1] and Blakley[12] and it aims at establishing a secure key management. Here Blakley's scheme is a probabilistic method based on the linear projective geometry and thus we introduce the Shamir's scheme only. Virtually, in many situations, there exists a key that provides an access to some important files. Therefore, if the key is forgotten by the available person or known by saboteurs, then all the important files become inaccessible or dangerous. In order to avoid this type of danger, the secret sharing scheme is designed based on polynomial interpolation. The basic idea of secret sharing scheme is dividing the secret key into pieces and distributing the pieces to different persons. Moreover, in terms of the previous definition, it is no doubt that secret sharing scheme is called perfect because unqualified group of participants can not obtain any information about the secret.

As a very simple example, consider the following situation that includes a dealer and n participants. Also, the number of the qualified subset of participants is specified by $m(1 \leq m \leq n)$. Then this is a general m out of n secret sharing scheme. In such a scheme, the dealer divides the secret into n parts and deliveries each participant a part so that any m or more participants can put together their shares to recover the secret, but any $m - 1$ or less participants do not suffice to determine the secret. Actually, different choices for the values of m and n reflect the tradeoff between security and reliability. Now let us take a look at Shamir's secret sharing scheme which is perfect just described.

Shamir's secret sharing scheme is a threshold secret sharing scheme that makes use of the arithmetic over the finite field $GF(q)$ and $m - 1$ degree polynomial

$$f(x) = a_0 + a_1x + \dots + a_{m-1}x^{m-1}$$

where a_0 is the secret and other coefficients are random elements in the fields. The field is known to every participants. Each share holds a pair of numbers (x_i, y_i) satisfying

$y_i = f(x_i), x_i \neq 0$. Moreover, any m or more shares can uniquely determine the polynomial and a_0 is able to be computed. However, any $m - 1$ or less shares can not figure out the polynomial uniquely, and hence the secret is any element in the field. Therefore, Shamir's scheme is a perfect secret sharing scheme.

A concrete secret sharing scheme is constructed as follows: We assumed an example of 4 out of 10 threshold scheme on \mathbb{Z}_{31874} with key equals 71. Therefore, the parameters m, n, q, K are 4, 10, 31874, 71 respectively.

- Initialization Phase : The dealer(D) chooses 10 distinct, non-zero elements of \mathbb{Z}_q , denoted $x_i = i, 1 \leq i \leq 10$ (this is where we require $31847 \geq 11$). For $1 \leq i \leq 10$, D gives the value x_i to each participant (P_i) . The values x_i are public.
- Share Distribution: Suppose D want to share a $K = 71$ belongs to \mathbb{Z}_{31847} . D secretly chooses (independently at random) $m - 1 = 3$ elements of \mathbb{Z}_{31847} , $a_1 = 3, a_2 = 5, a_3 = 7$. For $1 \leq i \leq 10$, D computes $y_i = f(x_i)$ in terms of $f(x) = K + a_1x_1 + \dots + a_{m-1}x_{m-1} \pmod{31847}$ as follows:

x_i	$y_i = f(x_i)$
1	86
2	153
3	314
4	611
5	1015
6	1781
7	2738
8	3999
9	5606
10	7601

For $1 \leq i \leq 10$, D gives the share y_i to P_i . So every participants P_i obtains a point (x_i, y_i) on this polynomial.

- Secret Reconstruction: In order to recovery the secret, we should assemble the qualified number of persons. Actually, at least 4 participants is required in the example. Suppose that the participants P_1, P_3, P_4, P_8 want to determine K. They know the pair of numbers (x_i, y_i) where $i \in \{1, 3, 4, 8\}$. Since $f(x)$ has the degree at most 3, $f(x)$ can be written as $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3$ where the coefficients a_0, a_1, a_2, a_3 are the unknown elements and $a_0 = K$ is the key. Obviously, $x_i = i$. So the following equations are obtained.

$$a_0 + a_1 + a_2 + a_3 = 86$$

$$a_0 + 3a_1 + 9a_2 + 27a_3 = 314$$

$$a_0 + 4a_1 + 16a_2 + 64a_3 = 611$$

$$a_0 + 8a_1 + 64a_2 + 512a_3 = 3999$$

This equation system does have a unique solution in the field \mathbb{Z}_{31874} : $a_0 = 71$, $a_1 = 3$, $a_2 = 5$, $a_3 = 7$.

Also, we could verify the perfection of Shamir's secret sharing scheme. Assumed that only 3 participants put their shares together. Proceeding as above, we are able to acquire the following equation systems.

$$a_0 + a_1 + a_2 + a_3 = 86$$

$$a_0 + 3a_1 + 9a_2 + 27a_3 = 314$$

$$a_0 + 4a_1 + 16a_2 + 64a_3 = 611$$

However, we cannot compute the coefficients directly because we finally obtain the equation $a_0 + 12a_3 = 155$. Apparently, a_3 is chosen randomly in the field, and hence the a_0 cannot be computed.

2.2 The Comparison with Visual Cryptography

Although we refer to the traditional secret sharing scheme as the perfect scheme, it sustains a few disadvantages when making the comparisons with the visual cryptography.

- **Convenience:** Generally, in the traditional secret sharing scheme, we require a computer or even more advanced devices to implement the decryption. In visual cryptography, only the transparency is necessary for the participants to take. Therefore, visual cryptography is much more convenient for the shareholders.
- **Popularity:** As we all known, we are not able to decrypt the secret without the good capabilities of cryptographic knowledge and computations in traditional secret sharing scheme. However, the visual cryptography merely ask the shareholders to pool together their shares and recognize the secret by their natural visual system. Undoubtedly, this property strengthen the popularity of visual cryptography.
- **Security:** The shares are usually stored in the computers for traditional secret sharing schemes. It may easily be attacked or destroyed by hackers through the internet. In some sense, it is relatively securer for shareholders to keep the physical shares in visual cryptography.

On the other hand, visual cryptography is of less practical importance than traditional secret sharing scheme. But it is a hot topic in the cryptographic research fields. In next Chapter, we will describe it in details.

Chapter 3

Naor and Shamir's Scheme

Since the discovery of visual cryptography by Shamir and Naor [17] in 1994, it has been developed by a great number of researchers and become a hot topic in the cryptographic researches. In the past decade, the majority of papers were focused on the improvements of visual cryptography which make the resulting text or image more legible for the shareholders. More specifically, in most of the papers regarding the black-and-white image, it depends on the contrast and subpixels expansion. As a matter of fact, these two fields have received more and more attentions and a great progress has been made by the researchers [18, 5, 8, 24, 3, 2].

For color images, due to the complexity of the color pixels, the researchers were trying to find different effective ways to make them well recognizable. However, it is more difficult to establish a perfect visual cryptography scheme for color images. The colored k out of n visual cryptography scheme sharing a colored image is first introduced by Verheul and Van Tilborg [9]. Although some methods of constructions for colored visual cryptography were proposed in the proceeding years, there still exist many drawbacks.

Moreover, the cryptologist began to explore different methods to implement the visual cryptography. The original visual cryptography proposed by Shamir and Naor is based on the the element-wise or-ing of binary matrices. Now, in terms of the principles of lights, a new method succeeds in carrying out the visual cryptography and obtaining a better resulting image.

In this chapter, we will review the Naor and shamir's schemes. From chapter 4 to 6, the schemes will be introduced from the above three directions: Contrast improvement, colored visual cryptography and the novel methods of visual cryptography.

3.1 The Model

At the beginning of [17], Naor and Shamir built up a model consisting of a printed page of ciphertext (which can be sent by mail or faxed) and a printed transparency (which serves as a secret key). Also, they assume that the message consists of a collection of black and white pixels and each pixel is handled separately. Each original pixel

appears in n modified versions (called shares) one for each transparency. Each share is a collection of m black and white subpixels, which are printed in close proximity to each other so that the human visual system averages their individual black/white contributions.

Then the construction is described by an $n \times m$ matrix $S = [S_{ij}]$ where $S_{ij} = 1$ if the j th subpixel in the i th transparency is black. When transparencies i_1, i_2, \dots, i_r are stacked together in a proper way, we can see a combined share whose black subpixels are represented by the Boolean "or" of the rows.

Definition 3.1. Hamming Weight: *the number of non-zero symbols in a symbol sequence. For binary signaling, Hamming weight is the number of 1 bits in the binary sequence.*

According to the definition, the grey level of the combined share is proportional to the Hamming Weight (represented by $H(V)$) of the "or"ed m -vector V . Moreover, it is interpreted by the visual system of the users as black if $H(V) \geq d$ and as white if $H(V) \leq d - \alpha m$ where some fixed threshold $1 \leq d \leq m$ and relative difference $\alpha > 0$.

Definition 3.2. *A solution to the k out of n visual secret sharing scheme consists of two collections of $n \times m$ Boolean matrices C_0 and C_1 . To share a white pixel, the dealer randomly chooses one of the matrices in C_0 , and to share a black pixel, the dealer randomly chooses one of the matrices in 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 C_0 , the or V of any k of the n rows satisfies $H(V) \leq d - \alpha m$.*
2. *For any S in C_1 , the or V of any k of the n rows satisfies $H(V) \geq d$.*
3. *For any subset $\{i_1, i_2, \dots, i_q\}$ of $\{1, 2, \dots, n\}$ with $q < k$, the two collections of $q \times m$ matrices D_t for $t \in \{0, 1\}$ obtained by restricting each $n \times m$ matrix in C_t (where $t = 0, 1$) to rows i_1, i_2, \dots, i_q are indistinguishable in the sense that they contain the same matrices with the same frequencies.*

Condition 3 implies that by inspecting fewer than k shares, even an infinitely powerful cryptanalyst cannot gain any advantage in detecting whether the shared pixel was white or black. In most of their constructions, there is a function f of such that the combined shares from $q < k$ transparencies consist of all the V s with $H(V) = f(q)$ with uniform probability distribution, regardless of whether the matrices were taken from C_0 or C_1 . Such a scheme is called *uniform*. The first two conditions are called *contrast* and the third condition is called *security*.

There are some important parameters in this scheme:

- m : the number of subpixels in a share. This represents the loss in resolution from the original pictures to the shared one. It should be as small as possible.

- α : the relative difference in weight between combined shares that come from a white pixel and a black pixel in the original picture. This represents the loss in contrast. It should be as large as possible.
- r : the size of the collection C_0 and C_1 (they need not be the same size, but in all of our constructions they are). \log_r represents the number of random bits needed to generate the shares and does not effect the quality of the picture.

3.2 2 out of 2 Visual Cryptography

Virtually, 2 out of 2 visual cryptography is a special case of original problem of visual cryptography. In this scheme, one pixel is split into two subpixels. However, in practice this method can distort the aspect ratio of the original image. Therefore, four subpixels are recommended to strengthen it. In 2 out of 2 visual cryptography, four subpixels are arranged in 2×2 array as Figure 3.1 describes.

In Figure 3.1, a white pixel is shared into two identical arrays from the list, and a black pixel is shared into complementary arrays from the list. Obviously, any single pixel is a random choice of two black and two white subpixels that look grey. After stacking the shares together, the result is either grey that represents white or completely black that represents black.

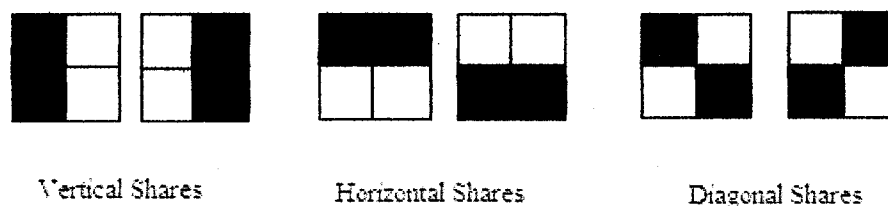


Figure 3.1: subpixels of 2 out of 2 visual cryptography

3.3 The General k out of k Schemes

In this paper, Naor and Shamir proposed two constructions by using subpixels 2^k and 2^{k-1} respectively for a general k out of k scheme.

Construction 3.3. *To define the two collections of matrices, two lists of vectors $J_1^0, J_2^0, \dots, J_k^0$ and $J_1^1, J_2^1, \dots, J_k^1$ are used.*

- Let $J_1^0, J_2^0, \dots, J_k^0$ be vectors of length k over $GF[2]$ with the property that every $k-1$ of them are linearly independent over $GF[2]$, but the set of all k vectors is not independent. For instance, let $J_i^0 = 0^{i-1}10^{k-i}$ for $1 \leq i \leq k$ and $J_k^0 = 1^{k-1}0$.
- Let $J_1^1, J_2^1, \dots, J_k^1$ be vectors of length k over $GF[2]$ with property that they are linearly independent over $GF[2]$.
- Each list defines a $k \times 2^k$ matrix S^t for $t \in \{0, 1\}$ and the collection C_0 and C_1 are obtained by permuting the columns of the corresponding matrix in all possible ways. Index the columns of S^t by vectors of length k over $GF[2]$. For $t \in \{0, 1\}$, let S^t be defined as follows:

$S^t[i, x] = \langle J_i^t, x \rangle$ for any $1 \leq i \leq k$ and any vectors x of length k over $GF[2]$ where $\langle x, y \rangle$ denotes the inner product $GF[2]$.

Lemma 3.4. *The above scheme is a k out of k scheme with parameter $m = 2^k$, $\alpha = \frac{1}{2^k}$, and $r = 2^k!$*

Construction 3.5. *Consider a ground set $W = \{e_1, e_2, \dots, e_k\}$ of k elements and let $\pi_1, \pi_2, \dots, \pi_2^{k-1}$ be a list of all the subsets of W of even cardinality and let $\sigma_1, \sigma_2, \dots, \sigma_2^{k-1}$ be a list of all the subsets of W of odd cardinality (the order is not important).*

Each list defines the following $k \times 2^{k-1}$ 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 $e_i \in \pi_j$ and $S^1[i, j] = 1$ iff $e_i \in \sigma_j$. As in the construction above, the collections C_0 and C_1 are obtained by permuting all the columns of the corresponding matrix.

Lemma 3.6. *The above scheme is a k out of k scheme with parameters $m = 2^{k-1}$, $\alpha = \frac{1}{2^{k-1}}$, and $r = 2^{k-1}!$*

Theorem 3.7. *In any k out of k scheme, $\alpha \leq \frac{1}{2^{k-1}}$ and $m \geq 2^{k-1}$*

3.4 The General k out of n Schemes

The k out of n scheme is derived from the k out of k scheme. Let C be an k out of k visual secret sharing scheme with parameters m, r, α . The scheme consists of two collections of $k \times m$ Boolean matrices $C_0 = T_1^0, T_2^0, \dots, T_r^0$ and $C_1 = T_1^1, T_2^1, \dots, T_r^1$. Furthermore, assume the scheme is uniform, i.e. there is a function $f(q)$ such that for any matrix T_i^t where $t \in \{0, 1\}$ and $1 \leq i \leq r$ and for every $1 \leq q \leq k-1$ rows of T_i^t the Hamming weight of the "or" of the q rows is $f(q)$. Note that all the previous constructions have this property.

Construction 3.8. *Let H be a collection of l functions such that*

1. *Any $h \in H$ satisfies: $\{1 \dots n\} \rightarrow \{1 \dots k\}$*
2. *For all subsets B in $\{1 \dots n\}$ of size k and for all $1 \leq q \leq k$ the probability that a randomly chosen $h \in H$ yields q different values on B is the same. Denote this probability by β_q .*

Constructing from C and H a k out of n scheme C' as follows:

- The ground set is $V = U \times H$ (i.e., it is of size $m \times l$ and consider its elements indexed by a member of U and a member of H).
- Each $1 \leq t \leq r^l$ is indexed by a vector (t_1, t_2, \dots, t_l) where each $1 \leq t_i \leq r$.
- The matrix S_t^b for $t = (t_1, t_2, \dots, t_l)$ where $b \in \{0, 1\}$ is defined as

$$S_t^b[i, (j, h)] = T_t^b[h(i), j]$$

t_h means the h th entry in t , where h is simply interpreted as a number between 1 and l .

Lemma 3.9. *If C is a scheme with parameters m, α, r , then C' is a scheme with parameters $m' = m \cdot l, \alpha' = \alpha \cdot \beta_k, r' = r^l$.*

Theorem 3.10. *For any n and k there exists a visual secret sharing scheme with parameters $m = n^k \cdot 2^{k-1}, \alpha = (2e)^{-k} / \sqrt{2\pi k}$ and $r = n^k(2^{k-1}!)$.*

Chapter 4

Improved Contrast Visual Cryptography Schemes

As previously described, the parameter of contrast called α should be as large as possible. Thus, in [18, 5, 8, 3, 24], the authors present different approaches to improve the contrast of the reconstructed image in visual cryptography. In this section, two of papers will be introduced in details.

4.1 Blundo, D'Acro, Stantis and Stinson's Scheme

In[5], the researchers analyzed the contrast of the resulting image for (k, n) -threshold visual cryptography. They not only defined a canonical form for k out of n visual cryptography but also provided its characterization.

At first, they conclude two parameters which characterize the visual cryptography: *pixel expansion*, which is the number of subpixels each pixel of the original image is encoded into, and the *contrast* which measures the "difference" between the white and black pixels in the resulting image. Then a model is proposed to solve the problem of contrast.

4.1.1 The Model

As a matter of fact, the pre-conditions are the same as the Naor and Shamir's scheme[17]. However, there are some differences between their definitions.

Definition 4.1. Let k and n be two integers such that $k \leq n$ and Let \mathcal{P} be a set of n participants. Two collections(multisets) of $n \times m$ boolean matrices C_0 and C_1 constitute a (k, n) -threshold visual cryptography scheme with pixel expansion m if there exist the value $\alpha(m)$ and the set $\{(X, t_X)\}_{X \subseteq \mathcal{P}: |X|=k}$ satisfying:

1. Any (qualified) set $X = \{i_1, i_2, \dots, i_k\} \subseteq \mathcal{P}$ can recover the shared image by stacking their transparencies. Formally, for any $M \in C_0$, the "or" V of rows

i_1, i_2, \dots, i_k satisfies $H(V) \leq t_X - \alpha(m) \cdot m$; whereas, for any $M \in C_1$ it results that $H(V) \geq t_X$.

2. Any (forbidden) set $X = \{i_1, i_2, \dots, i_p\} \subseteq \mathcal{P}$, with $p < k$, has no information on the shared image. Formally, the two collections of $p \times m$ matrices \mathcal{D}_t , with $t \in \{0, 1\}$, obtained by restricting each $n \times m$ matrix in C_t to rows i_1, i_2, \dots, i_p , are indistinguishable in the sense that they contain the same matrices with the same frequencies.

The value $\alpha(m)$ is called contrast of image and the set $\{(X, t_X)\}_{X \subseteq \mathcal{P}: |X|=k}$ is called the set of thresholds. The slightly different terminology is used in [17] where the contrast is called relative difference and the quantity $\alpha(m) \cdot m$ is referred to as the contrast of the scheme. Therefore, as previous, the product of the contrast times the pixel expansion should be as large as possible and at least one, that is, $\alpha(m) \geq \frac{1}{m}$. Also, in fact, the model is a generalization of the one proposed in [17], since with each set X of size k they associate a (possibly) different threshold t_X . However, in this paper, there is a property that for any $X, X' \subseteq \mathcal{P}$ with $|X| = |X'| \geq k$ so that $t_X = t_{X'}$.

4.1.2 Basic Matrices

In the paper, all the collections of C_0 and C_1 are considered as the same size, that is, $|C_0| = |C_1|$. All the constructions are realized by two $n \times m$ matrices, S^0 and S^1 , called basis matrices satisfying the following definition.

Definition 4.2. *Let k and n be two integers such that $k \leq n$ and let \mathcal{P} be a set of n participants. A (k, n) -threshold Visual Cryptography Scheme with contrast $\alpha(m)$ and set of thresholds $\{(X, t_X)\}_{X \subseteq \mathcal{P}: |X|=k}$ is realized using the two $n \times m$ basis matrices S^0 and S^1 if the following two conditions hold.*

1. If $X = \{i_1, i_2, \dots, i_k\} \subseteq \mathcal{P}$, (i.e., if X is a qualified set), then the "or" V of rows i_1, i_2, \dots, i_k of S^0 satisfies $H(V) \leq t_X - \alpha(m) \cdot m$; whereas, for S^1 it results that $H(V) \geq t_X$.
2. If $X = \{i_1, i_2, \dots, i_p\} \subseteq \mathcal{P}$ and $p < k$ (i.e., if X is a forbidden set), then the two $p \times m$ matrices obtained by restricting S^0 and S^1 to rows i_1, i_2, \dots, i_p are equal up to a column permutation.

The collections C_0 and C_1 are obtained by permuting the columns of the corresponding basis matrix in all possible ways. The algorithm for the visual cryptography scheme based on the previous construction of the collections C_0 and C_1 has small memory requirements (it keeps only the basis matrices S^0 and S^1) and it is efficient (to choose a matrix in C_0 (C_1 , resp.)) it only generates a permutation of the columns of S^0 (S^1 , resp.).

4.1.3 Canonical (k,n) -threshold VCS

In this section, the basic matrices containing all the columns of a given weight each occurring with the same frequency with few additional properties are considered. Moreover, these matrices are referred to as *canonical*. Since the authors are interested in optimizing the contrast without loss of generality.

The notations are set up firstly by authors. Let m be an $n \times m$ matrix and let $X \subseteq \{1, \dots, n\}$ and $Z \subseteq \{1, \dots, m\}$. Let $M[X][Z]$ denote the $|X| \times |Z|$ matrix obtained from M by considering its restriction to rows and columns indexed by X and Z , respectively. Let M be a matrix in the collection $C_0 \cup C_1$ of a (k, n) -threshold VCS on a set of participants \mathcal{P} . For $X \subseteq \mathcal{P}$, let M_X denote the m -vector obtained by considering the *or* of the rows corresponding to participants in X ; whereas $M[X] = M[X][\{1, \dots, m\}]$ denote the $|X| \times m$ matrix obtained from M by considering only the rows corresponding to participants in X . Let M be a matrix and let D be a sub-matrix of M having the same number of rows, with $M \setminus D$ is denoted by the matrix obtained from M by removing all the columns of the matrix D . For sets X and Y and for elements x and y , to avoid the overburdening the notation, x is written for $\{x\}$, xy for $\{x, y\}$, xY for $\{x\} \cup Y$, and XY for $X \cup Y$. Let \mathbf{c} be a boolean vector, with $\bar{\mathbf{c}}$ they denote the vector obtained from \mathbf{c} by complementing all its entries; whereas, given a boolean matrix M with \bar{M} they denote the matrix obtained from M by complementing all its entries. For $i = 0, 1$, with $f_{\mathbf{c},i}$ they denote the multiplicity of the column \mathbf{c} in S^i , that is, $f_{\mathbf{c},i}$ is the number of times the column \mathbf{c} appears in S^i . By abusing of the notation, they write $\mathbf{c} \in M$ to denote the fact that \mathbf{c} is a column of the matrix M .

Definition 4.3. Let (S^0, S^1) be the basic matrices of a (k, n) -threshold VCS. They are in canonical form if, for $i = 0, 1$, the following two properties are satisfied.

1. For any columns \mathbf{c} and \mathbf{c}' such that $H(\mathbf{c}) = H(\mathbf{c}')$, it results that $f_{\mathbf{c},i} = f_{\mathbf{c}',i}$.
2. For any column \mathbf{c} it results that

$$f_{\mathbf{c},i} = \begin{cases} f_{\bar{\mathbf{c}},i} & \text{if } k \text{ is even} \\ f_{\bar{\mathbf{c}},1-i} & \text{if } k \text{ is a odd.} \end{cases} \quad (4.1)$$

A (k, n) -threshold VCS whose basic matrices are in canonical form is referred to as a canonical (k, n) -threshold VCS.

Theorem 4.4. Let S^0 and S^1 be two $n \times m$ boolean matrices. The matrices S^0 and S^1 are basic matrices of a (k, n) -threshold VCS with pixel expansion m and contrast $\alpha(m)$ if and only if for all subsets X consisting of k rows there exist a boolean matrix D^X and integer $z_X \geq \alpha(m) \cdot m$ such that D^X is a sub-matrix of both $S^0[X]$ and $S^1[X]$, all the even columns appear in $S^0[X] \setminus D^X$ with multiplicity z_X , and all the odd columns appear in $S^1[X] \setminus D^X$ with multiplicity z_X .

Lemma 4.5. *Let (S^0, S^1) be the basis matrices of a (k, n) -threshold VCS with pixel expansion m and contrast α . The matrices (B^0, B^1) , defined as*

$$(B^0, B^1) = \begin{cases} (\overline{S^1}, \overline{S^0}) & \text{if } k \text{ is odd} \\ (\overline{S^0}, \overline{S^1}) & \text{if } k \text{ is even,} \end{cases} \quad (4.2)$$

are the basis matrices of a (k, n) -threshold VCS with pixel expansion m and contrast α .

Then, the following Lemma is obtained by the previous Theorem 4.4 and Lemma 4.5.

Lemma 4.6. *Let C_0 and C_1 be the collections of matrices of a (k, n) -threshold VCS with contrast α . Then, there exists a canonical (k, n) -threshold VCS realized by basic matrices (S^0, S^1) having contrast α .*

In any canonical (k, n) -threshold VCS, all the columns of a given weight appear with the same multiplicity. So, $h_{j,i}$ is defined as the multiplicity of a column of weight j in S^i , i.e., $h_{j,i} = f_{c,i}$ if $w(c) = j$. Hence, any canonical (k, n) -threshold VCS can be simply described by the pair of vectors $(h_{0,0}, \dots, h_{n,0})$ and $(h_{0,1}, \dots, h_{n,1})$. Clearly, the pixel expansion m of a canonical (k, n) -threshold VCS is equal to

$$m = \sum_{j=0}^n h_{j,0} \binom{n}{j} = \sum_{j=0}^n h_{j,1} \binom{n}{j} \quad (4.3)$$

Moreover, in a canonical (k, n) -threshold VCS, for any $X, X' \subseteq \mathcal{P}$, with $|X| = |X'| = k$, the $t_X = t_{X'}$ holds as in the original definition by Naor and Shamir[17].

Corollary 4.7. *Let Σ be a (k, n) -threshold VCS in canonical form. If k is odd, then for $j = 0, \dots, n$, it results that $h_{j,0} = h_{n-j,1}$; whereas, if k is even, for $j = 0, \dots, n$, it results that $h_{j,0} = h_{n-j,0}$ and $h_{j,1} = h_{n-j,1}$.*

There is another equality regarding the $h_{i,j}$'s which is based on the security of the (k, n) -threshold VCS.

$$\sum_{i=1}^n h_{i,0} \binom{n-1}{i-1} = \sum_{i=1}^n h_{i,1} \binom{n-1}{i-1} \quad (4.4)$$

Hence, in any canonical (k, n) -threshold VCS all the rows of the basis matrices have the same weight. The next corollary is an immediate consequence of previous observation and of Lemma 4.6.

Corollary 4.8. *The pixel expansion of any canonical (k, n) -threshold VCS is twice the weight of any row of a basic matrix.*

Lemma 4.9. *$S(h_0)$ and $S(h_1)$ are basis matrices of a (k, n) -threshold VCS with pixel expansion m and contrast α if and only if the following properties are satisfied:*

1. $\sum_{j=0}^n \binom{n}{j} h_{j,0} = \sum_{j=0}^n \binom{n}{j} h_{j,1} = m.$
2. $\sum_{j=l'}^{n-l+l'} \binom{n-l}{j-l'} h_{j,0} = \sum_{j=l'}^{n-l+l'} \binom{n-l}{j-l'} h_{j,1},$ for $1 \leq l \leq k-1$ and $0 \leq l' \leq l,$
3. $\sum_{j=0}^{n-k} \binom{n-k}{j} (h_{j,0} - h_{j,1}) = \alpha m.$

Example 4.10. Suppose $k = 2$ and $n = 4$. Let $h_0 = (3, 0, 0, 0, 3)$ and let $h_1 = (0, 0, 1, 0, 0)$. This defines a $(2, 4)$ threshold VCS with $m = 6$ and contrast $\alpha = 1/3$:

$$\sum_{j=0}^4 \binom{4}{j} h_{j,0} = \binom{4}{0} 3 + \binom{4}{4} 3 = 6$$

$$\sum_{j=0}^4 \binom{4}{j} h_{j,1} = \binom{4}{2} 1 = 6$$

$$\sum_{j=0}^3 \binom{3}{j} h_{j,0} = \binom{3}{0} 3 = 3$$

$$\sum_{j=0}^3 \binom{3}{j} h_{j,1} = \binom{3}{2} 1 = 3$$

$$\sum_{j=0}^2 \binom{2}{j} (h_{j,0} - h_{j,1}) = \binom{2}{0} 3 - \binom{2}{2} 1 = 2$$

In view of Lemma 4.6, if we are interested in getting a scheme with a given contrast or bound on the contrast itself, then we can restrict our attention to canonical (k, n) -threshold VCS. Therefore, the following (k, n) -threshold VCS are considered as the canonical (k, n) -threshold VCS unless otherwise specified.

4.1.4 Contrast Optimal (k, n) - threshold VCS

The same column cannot appear in both basic matrices of a contrast optimal (k, n) -threshold VCS. Indeed, if the same column appears in both basic matrices, then by removing it we obtain a new scheme having a better contrast than the one we started with. This property implied the following fact.

Fact 4.11. In any contrast optimal (k, n) -threshold VCS whose basic matrices are in canonical form, for $j = 0, \dots, n$ and $i = 0, 1$, it holds that,

1. If $h_{j,1-i} > 0$, then $h_{j,i} = 0$.
2. If k is even, then $h_{j,i} = h_{n-j,i}$.

3. If k is odd, then $h_{j,i} = h_{n-j,1-i}$.

As a result of above fact and because of the Corollary 4.7, if n is even and k is odd then $h_{n/2,0} = h_{n/2,1} = 0$.

Contrast Optimal $(n-1, n)$ -threshold VCS

In this section, the contrast optimal $(n-1, n)$ -threshold VCS is characterized by the authors.

Lemma 4.12. *Let $n \geq 3$. In any contrast optimal $(n-1, n)$ -threshold VCS whose basis matrices are in canonical form, the $h'_{j,i}$ s satisfy:*

1. $h_{j,0} > 0$ if and only if either $j < n/2$ and j is even or $j > n/2$ and j is odd.
2. $h_{j,1} > 0$ if and only if either $j < n/2$ and j is odd or $j > n/2$ and j is even.

Lemma 4.13. *For any $n \geq 3$ and for any contrast optimal canonical $(n-1, n)$ -threshold VCS the pixel expansion m is given by*

$$m = \begin{cases} \frac{n}{4} \binom{n}{n/2} & \text{if } n \text{ is even} \\ n \binom{n-1}{(n-1)/2} & \text{if } n \text{ is odd.} \end{cases} \quad (4.5)$$

Lemma 4.14. *For any $n \geq 3$ and for any canonical $(n-1, n)$ -threshold VCS the maximum contrast α is given by*

$$\alpha = \begin{cases} \left[\frac{n}{4} \binom{n}{n/2} \right]^{-1} & \text{if } n \text{ is even} \\ \left[\frac{n}{2} \binom{n-1}{(n-1)/2} \right]^{-1} & \text{if } n \text{ is odd.} \end{cases} \quad (4.6)$$

According to the previous lemma one has that in any contrast optimal $(n-1, n)$ -threshold VCS $\alpha = \Theta(2^{-n}n^{-1/2})$. This is lower contrast than an (n, n) -threshold VCS.

Contrast Optimal $(3, n)$ -threshold VCS

For any $n \geq 4$ and any integer $1 \leq g \leq n/2$, consider the visual cryptography scheme whose basic matrices are in canonical form, denoted by $\mathcal{S}(3, n, g)$, described by the following $h_{j,i}$'s.

$$h_{0,0} = h_{n,1} = \binom{n-1}{g} - \binom{n-1}{g-1} \text{ and } h_{n-g,0} = h_{g,1} = 1 \quad (4.7)$$

whereas all the remaining $h_{j,i}$'s are equal to zero. This is a strong $(3, n)$ -threshold VCS as shown by the following theorem.

Theorem 4.15. For any $n \geq 4$ and any integer $1 \leq g \leq n/2$, the scheme $\mathcal{S}(3, n, g)$ described by (4.7) is a strong $(3, n)$ -threshold VCS having pixel expansion and contrast equal to

$$m = 2 \binom{n-1}{g} \text{ and } \alpha = \frac{g(n-2g)}{2(n-1)(n-2)}, \quad (4.8)$$

respectively.

Theorem 4.16. Let $n \geq 4$. In any $(3, n)$ -threshold visual cryptography scheme it holds that

$$\alpha \leq \frac{(n-2 \lfloor \frac{n+1}{4} \rfloor) \lfloor \frac{n+1}{4} \rfloor}{2(n-1)(n-2)}$$

A Canonical $(4, n)$ -threshold VCS

For any even $n \geq 4$ and any integer $1 \leq g < n/2$, consider the visual cryptography scheme whose basic matrices are in canonical form, denoted by $\mathcal{S}(4, n, g)$, described by the following $h_{j,i}$'s

$$h_{0,0} = h_{n,0} = \binom{n-3}{n/2-1} \frac{t_{n,g}(n-1)(n-2g)^2}{ng(n-g)}, \quad (4.9)$$

$$h_{n/2,0} = t_{n,g}, \text{ and } h_{g,1} = h_{n-g,1} = \frac{\binom{n-3}{n/2-1}}{\binom{n-2}{g-1}} \cdot t_{n,g} \quad (4.10)$$

where $t_{n,g} = \binom{n-2}{g-1} / \gcd\{\binom{n-2}{g-1}, \binom{n-3}{n/2-1}\}$ and all the remaining $h_{j,i}$'s are equal to zero. This is a strong $(4, n)$ -threshold VCS as shown by the following theorem.

Theorem 4.17. For any even integer $n \geq 4$ and any integer $1 \leq g \leq n/2$, the scheme $\mathcal{S}(4, n, g)$ is a strong $(4, n)$ -threshold VCS having pixel expansion and contrast equal to

$$m = \frac{2nt_{n,g}(n-1)}{g(n-g)} \binom{n-3}{n/2-1} \text{ and } \alpha = \frac{g(n-g)(n-2g)^2}{4n(n-1)(n-2)(n-3)}, \quad (4.11)$$

respectively.

Remark 4.18. Theorem 4.17 holds only when n is even. If n is odd, then, by applying the technique given in Theorem 4.17, we construct a $(4, n+1)$ -threshold VCS, and then consider only first n rows of the basis matrices of such scheme. Therefore, for any $n \geq 4$ and any integer $1 \leq g < n/2$, there exists a strong $(4, n)$ -threshold VCS having pixel expansion and contrast equal to

$$m = \frac{2nt_{n,g}(n+1)}{g(n+1-g)} \binom{n+1-3}{(n+1)/2-1} \text{ and } \alpha = \frac{g(n+1-g)(n+1-2g)^2}{4n(n+1)(n-1)(n-2)} \quad (4.12)$$

respectively.

A Canonical $(5, n)$ -threshold VCS

For any two integers l and g such that $1 \leq l < g < n/2$, the $(5, n)$ -threshold VCS whose basis matrices are in canonical form, denoted by $\mathcal{S}(5, n, l, g)$, is described by the following $h_{j,i}$'s:

$$h_{g,0} = h_{n-g,1} = t_{(n,l,g)}, \quad h_{n-l,0} = h_{l,1} = s_{(n,l,g)}, \quad h_{0,0} = h_{n,1} = r_{(n,l,g)}, \quad (4.13)$$

where

$$t_{(n,l,g)} = \frac{\binom{n-4}{l-1} - \binom{n-4}{l-3}}{\gcd\left\{\binom{n-4}{l-1} - \binom{n-4}{l-3}, \binom{n-4}{g-1} - \binom{n-4}{g-3}\right\}},$$

$$s_{(n,l,g)} = t_{(n,l,g)} \frac{\left[\binom{n-4}{g-1} - \binom{n-4}{g-3}\right]}{\left[\binom{n-4}{l-1} - \binom{n-4}{l-3}\right]},$$

$$r_{(n,l,g)} = s_{(n,l,g)} \left[\binom{n-4}{l} - \binom{n-4}{l-4}\right] - t_{(n,l,g)} \left[\binom{n-4}{g} - \binom{n-4}{g-4}\right],$$

and all the remaining $h_{j,i}$'s are equal to zero.

Theorem 4.19. *For any two integers l and g such that $1 \leq l < g < n/2$, the scheme $\mathcal{S}(5, n, l, g)$ is a canonical $(5, n)$ -threshold VCS having pixel expansion and contrast equal to*

$$m = s_{(n,l,g)} \left[\binom{n}{l} + \binom{n-4}{l} - \binom{n-4}{l-4}\right] + t_{(n,l,g)} \left[\binom{n}{g} + \binom{n-4}{g-4} - \binom{n-4}{g}\right]$$

and

$$\alpha = \frac{l(g-l)(n-g)(n-2g)(n-2l)}{2(n+2l-2g)(n-1)(n-2)(n-3)(n-4)},$$

respectively.

In this paper, the authors analyzed the contrast of the reconstructed image for (k, n) -threshold VCS. Moreover, they put forward a canonical form for VCS and provide several (k, n) -threshold VCS with $k = 3, 4, 5$ having an optimal contrast.

4.2 Duong Quang Viet and Kaoru Kurosawa's Scheme

At the beginning of this paper[8], the author points out the reason which causes the loss of contrast in visual cryptography. In fact, in the previous VCS, no black sub-pixel can be made into white because transparencies are simply superimposed in the reconstruction phase. This is the essential reason of a much loss of contrast in the

reconstructed image. Consequently, this paper shows a new paradigm of VCS in which the original image is almost perfectly reconstructed.

In the proposed method, a very simple non-cryptographic operation is assumed, reversing the black and white, which many copy machines have these days. All the black region is reversed into white and all the white region is reversed into black by this operation. Namely, it is called a (k, n) -VCS with reversing.

4.2.1 Model

A (k, n) -visual cryptography scheme (VCS) consists of a distribution phase and a reconstruction phase. Let I be a secret image which consists of black and white pixels P .

In the distribution phase, a dealer \mathcal{D} encodes each pixel P into n shares s_1, \dots, s_n , one for each transparency. \mathcal{D} then gives s_i to participants \mathcal{P}_i for $i = 1, \dots, n$.

In the reconstruction phase, any k participants $\mathcal{P}_{i_1}, \dots, \mathcal{P}_{i_k}$ reconstruct I by superimposing their transparencies. That is, the reconstructed pixel is given by

$$\tilde{P} = s_{i_1} + s_{i_2} + \dots + s_{i_k},$$

where $+$ means OR. However, any $k - 1$ participants have no information on I .

Each s_i consists of m sub-pixels, where m is called the *expansion rate*. Hence s_i is described by a Boolean vector of length m

$$v_i = (c_{i,1}, \dots, c_{i,m}),$$

where $c_{i,j} = 1$ if the j -th subpixel is black. Let $C = [c_{i,j}]$ be the $n \times m$ Boolean matrix which consists of v_1, \dots, v_n . That C is the encoding matrix of P .

\tilde{P} is interpreted as black if $w_H(\tilde{P})$ is large, and as white if $w_H(\tilde{P})$ is small, where $w_H(\tilde{P})$ denotes the Hamming weight of \tilde{P} . The grey level of a pixel P is defined as

$$GREY(P) = w_H(\tilde{P})/m,$$

where $P = \text{white}$ or black . $GREY(\text{white})$ should be close to zero and $GREY(\text{black})$ should be close to one. In Naor and Shamir's 2 out of 2 VCS, the grey level of a black pixel and a white pixel are

$$GREY(\text{black}) = 1, GREY(\text{white}) = 1/2.$$

The *contrast* is ideal if

$$GREY(\text{black}) = 1, GREY(\text{white}) = 0.$$

A (k, n) -VCS is perfect black if

$$GREY(\text{black}) = 1 \text{ and } GREY(\text{white}) < 1.$$

The (n, n) -VCS shown by Naor and Shamir [17] is *perfect black*. The expansion rate is $m = 2^{n-1}$ and they showed it is optimum. For any $2 \leq k \leq n$, Blundo et al. showed a perfect black (k, n) -VCS such that

$$GREY(white) = 1 - 1/m$$

for some expansion rate m [2].

4.2.2 Basic Idea

In this section, the authors show a basic idea of their schemes. They present a $(2, 2)$ -VCS with reversing such that $GREY(white) = 1/4$ in addition to $GREY(black) = 1$. So it improves the contrast because $GREY(white) = 1/2$ in [17].

Definition 4.20. *An image I is reversed if all black pixels are reversed into white and all white pixels are reversed into black. Denote by \bar{P} the reversed pixel of P and by \bar{I} the reversed image of I .*

The scheme is described as Figure 4.1 and Figure 4.2.

- (Distribution phase)

1. The dealer \mathcal{D} runs the distribution phase of Naor and Shamir's $(2, 2)$ -VCS twice independently. Let (s_1, s_2) denote the shares of the first run and (s'_1, s'_2) denote the shares of the second run.
2. Now in the scheme, the share of participant \mathcal{P}_1 is (s_1, s'_1) and that of participant \mathcal{P}_2 is (s_2, s'_2)

- (Reconstruction phase)

1. Two participants superimpose s_1, s_2 , and obtain $T = s_1 + s_2$. Similarly, they superimpose s'_1, s'_2 and obtain $T' = s'_1 + s'_2$. They are illustrated in the Figure 4.2.
2. They next reverse T, T' and obtain \bar{T} and \bar{T}' as shown in Figure 4.2.
3. The two participants superimpose \bar{T}, \bar{T}' and obtain $\bar{T} + \bar{T}'$.
4. Finally the two participants reverse $\bar{T} + \bar{T}'$ and obtain $\overline{\bar{T} + \bar{T}'}$. The $\overline{\bar{T} + \bar{T}'}$ is the reconstructed image of the scheme.

Now as we can see from Figure 4.2, we obtain that $GREY(black) = 1$ and

$$E[GREY(white)] = (1/2) \times 0 + (1/2) \times (1/2) = 1/4.$$

The reasons are listed as follows. Suppose that a pixel P is white. Then

1. T and T' are always black as shown in Figure 4.1.

pixel P		s_1	s_2	$T = s_1 + s_2$
□	$\mu = .5$			
	$\mu = .5$			
■	$\mu = .5$			
	$\mu = .5$			

pixel P		s'_1	s'_2	$T' = s'_1 + s'_2$
□	$\mu = .5$			
	$\mu = .5$			
■	$\mu = .5$			
	$\mu = .5$			

Figure 4.1: Proposed (2,2)-VCS(1)

2. Therefore, \overline{T} and $\overline{T'}$ are always white as shown in Figure 4.2.
3. Therefore, $\overline{T} + \overline{T'}$ is always white.
4. Hence $\overline{\overline{T} + \overline{T'}}$ is always black.

On the other hand, suppose that a pixel P is a white. Then

1. As shown in Figure 4.1, T and T' are grey such that a half region is black and the other half is white in each one of the four cases.
2. Therefore, \overline{T} and $\overline{T'}$ are grey such that a half region is white and the other half is black in each one of the four cases as shown in Figure 4.2.
3. Therefore, $\overline{T} + \overline{T'}$ is black with probability 1/2 and grey(half black and half white) with probability 1/2. This is because (s_1, s_2) and (s'_1, s'_2) are generated independently and randomly.
4. Hence $\overline{\overline{T} + \overline{T'}}$ is all white with probability 1/2 and it is grey(half black and half white) with probability 1/2.

4.2.3 Proposed Scheme

In this section, they show their (k, n) -VCS with reversing. The reconstruction of black region is perfect and the reconstruction of white region is almost perfect. The cost is the size of shares. If the size of shares is c times larger, then the grey level of white region converges to zero exponentially.

Pixel P		T	\bar{T}	\bar{T}	$\overline{\bar{T} \setminus \bar{T}}$
□	$p = .25$				
	$p = .25$				
	$p = .25$				
	$p = .25$				
■	$p = 1$				

Figure 4.2: Proposed (2,2)-VCS(2)

c-Run (k, n)-VCS with Reversing

Suppose that there exists a perfect black (k, n)-VCS. Then construct a "c-run (k, n)-VCS with reversing" as follows in which the underlying (k, n)-VCS is run c times independently.

Let P be a secret pixel to be distributed.

(Distribution phase)

1. The dealer \mathcal{D} runs the distribution phase of the underlying perfect black (k, n)-VCS c times independently. Let $(s_{1,i}, \dots, s_{n,i})$ be the set of shares in the i-th run for $i = 1, \dots, c$.
2. In the scheme, the share of participant \mathcal{P}_j is $(s_{j,1}, \dots, s_{j,c})$.

(Reconstruction phase) Any k participants, say $\mathcal{P}_{j_1}, \dots, \mathcal{P}_{j_k}$, reconstruct P as follows.

1. For $i = 1, \dots, c$, they superimpose their shares and obtain

$$T_i = s_{j_1,i}, \dots, s_{j_k,i}$$

2. They reverse T_i and obtain \bar{T}_i for $i = 1, \dots, c$.
3. They superimpose $\bar{T}_1, \dots, \bar{T}_c$ and obtain $U = \bar{T}_1 + \dots + \bar{T}_c$.
4. Reverse U and obtain \tilde{P} , where

$$\tilde{P} = \bar{U} = \overline{\bar{T}_1 + \dots + \bar{T}_c}$$

Obviously, any k - 1 participants have no information on P from the property of the original (k, n)-VCS.

Contrast

It is easy to see that $\mathbf{GREY}(\text{black}) = 1$ because the original VCS is perfect black. Now we show that both $\mathbf{E}[\mathbf{GREY}(\text{white})]$ and $\mathbf{Var}[\mathbf{GREY}(\text{white})]$ converge to zero.

Theorem 4.21. *Suppose that $\mathbf{GREY}(\text{white}) = q < 1$ in the original perfect black VCS. Then in our c -run VCS with reversing.*

- (1) $\mathbf{E}[\mathbf{GREY}(\text{white})] = q^c.$
- (2) $\mathbf{Var}[\mathbf{GREY}(\text{white})] \leq q^c(1 - q^c)$

Corollary 4.22. *There exists a perfect black $(2, 2)$ -VCS with reversing such that*

$$\mathbf{E}[\mathbf{GREY}(\text{white})] = (1/2)^c$$

$$\mathbf{Var}[\mathbf{GREY}(\text{white})] \leq (1/2)^c \{1 - (1/2)^c\}$$

with the expansion rate $m = 2$, where c is any positive integer.

For general (k, n) -VCS, they obtain the following corollary from [2].

Corollary 4.23. *For any $2 \leq k \leq n$, there exists a perfect black (k, n) -VCS with reversing such that*

$$\mathbf{E}[\mathbf{GREY}(\text{white})] = (1 - 1/m)^c$$

$$\mathbf{Var}[\mathbf{GREY}(\text{white})] \leq (1 - 1/m)^c \{1 - (1 - 1/m)^c\}$$

for any positive integer c , where m is the expansion rate given by [2].

Example 4.24. *As an example, we present a 3-Run $(2, 2)$ -VCS.*

(Distribution phase) *The Dealer \mathcal{D} runs the distribution phase of $(2, 2)$ -VCS in [17] three times independently. Let (s_1, s_2) be the shares of the first run, (s'_1, s'_2) be the shares of the second run and (s''_1, s''_2) be the set of shares of the third run.*

Then the share of participant \mathcal{P}_1 is (s_1, s'_1, s''_1) and that of participant \mathcal{P}_2 is (s_2, s'_2, s''_2) .

(Reconstruction phase)

1. We superimpose s_1 and s_2 , and then obtain $T = s_1 + s_2$. Similarly, we obtain $T' = s'_1 + s'_2$ and $T'' = s''_1 + s''_2$.
2. we reverse T , T' and T'' , and obtain \bar{T} , \bar{T}' and \bar{T}'' .
3. we superimpose \bar{T} , \bar{T}' , \bar{T}'' and obtain $U = \bar{T} + \bar{T}' + \bar{T}''$.
4. We reverse U and obtain \tilde{P} .

(Contrast): *We can then see that $\mathbf{GREY}(\text{black}) = 1$ and*

$$\mathbf{E}[\mathbf{GREY}(\text{white})] = (1/4) \times (1/2) + (3/4) \times 0 = 1/8$$

4.2.4 Perfect White VCS

Conversion from Perfect Black VCS

A (k, n) -VCS is *perfect white* if

$$\text{GREY}(\text{white}) = 0 \text{ and } \text{GREY}(\text{black}) > 0$$

In usual pictures, the white region is much larger than the black region. Therefore, perfect white VCSs are much preferable than perfect black VCSs. However, no perfect white VCS has been known. In this section, we show that a perfect white (k, n) -VCS with reversing is easily obtained from a perfect black (k, n) -VCS (with reversing).

Theorem 4.25. *Suppose that there exists a perfect black (k, n) -VCS with reversing such that $E[\text{GREY}(\text{white})] = p$. Then there exists a perfect white (k, n) -VCS with reversing such that $E[\text{GREY}(\text{black})] = 1-p$.*

Almost Ideal Contrast with Perfect White

We can obtain a perfect white (k, n) -VCS with reversing such that

$$E[\text{GREY}(\text{black})] \rightarrow 1$$

by applying Theorem 4.25 to our construction shown in section 4.2.3.

In this case, we can reduce the number of reversing from $c + 1$ to c by terminating at step 3 of the reconstruction phase. The U of step 3 is the reconstructed image.



















pixel P		s_1	s_2	$s_1 \uparrow s_2$	$s_1 \times s_2$
	$p = \bar{s}$				
	$p = \bar{s}$				
	$p = \bar{s}$				
	$p = \bar{s}$				

Figure 4.3: Perfect white $(2,2)$ -VCS

Example 4.26. *As an example, we show how to convert the perfect black $(2, 2)$ -VCS into a perfect white $(2, 2)$ -VCS with reversing.*

(Distribution phase):

CHAPTER 4. IMPROVED CONTRAST VISUAL CRYPTOGRAPHY SCHEMES 26

1. the dealer \mathcal{D} first reverses the original image I . Hence each white pixel is reversed into black and each black pixel is reversed into white.
2. \mathcal{D} then applied the distribution phase of the perfect black $(2, 2)$ -VCS. Participant \mathcal{P}_1 obtains a share s_1 and participants \mathcal{P}_2 obtains a share s_2 .

(Reconstruction phase):

1. the two participants superimposes s_1 and s_2 and obtains $s_1 + s_2$.
2. They finally reverse $s_1 + s_2$ and obtains $\overline{s_1 + s_2}$

From Figure 4.3, we see that a perfect white $(2, 2)$ -VCS is obtained such that **GREY**(black) = $1/2$.

In this paper, the authors make use of the non-cryptographic operation to obtain the almost ideal contrast. It will be a further work to find another simple and similar method for improving the contrast.

Chapter 5

Colored Visual Cryptography Schemes

In the previous researches, the majority of literatures was focused on the black-and-white secret image. However, it did not satisfy the requirement of the real world. Although the colored secret image has caught the attention of many researchers, there are not many papers regarding the colored image yet. In this chapter, we will introduce two of [9, 4, 27, 26, 23] which involve different methods to carry out the colored (k, n) -VCS.

Verheul and Van Tilborg [9] proposed a general construction, making use of the concept of *arcs*, for a colored VCS scheme so that the participants are able to share the colored secret image.

In the following sections, two colored schemes will be elaborated. One is put forward by the C. N. Yang and C.S. Lai, and Y.C.Hou established another.

5.1 Ching-Nung Yang and Chi-Sung Lai's Scheme

In this paper, the authors define a different structure of the colored subpixels so that the previous black-and-white VCS can be easily modified and extended to construct the colored VCS.

5.1.1 Basic Colored VCS

If the smallest graphic unit in a colored picture is called pixel, the key concept of VCS is to transform the pixel to b sub pixels of color $0, 1, \dots, c - 1$. The infrastructure of colored sub pixels is shown in Figure 5.1.

A circle subpixel with a sector of angle $2\pi/c$ is called a color i subpixel where the sector has color i and the other part in the circle is black. Although the color black might be one of the c colors, it is always distinguishable from the c colors. Figure 5.1(b) shows that "OR" of elements equals color i , if all elements are color i , otherwise it equals color black. For a colored (k, n) VCS, the dealer produces n transparencies

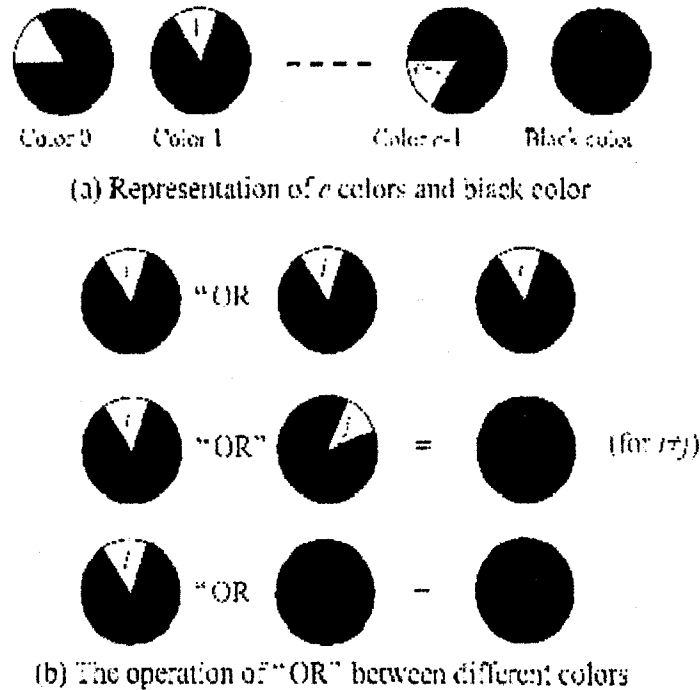


Figure 5.1: the infrastructure of colored subpixel and its OR operation(1)

and each pixel in transparency contains b subpixels. The color of one pixel in stacked transparencies is dependent on the interrelation between the stacked("OR") subpixels. If all subpixels are of color i , then one sees color i , otherwise one sees black color.

Definition 5.1. A k out of n c -color VSS scheme $S = (C_0, C_1, \dots, C_{c-1})$, consists of c collections of $n \times b$ q -ary matrices, in which the c colors are elements of the Galois field $GF(q)$. To share a pixel of color i , the dealer randomly chooses one of the matrices in C_i . The chosen matrix defines the color of the b sub pixels in each one of the transparencies. The solution is considered valid if the following three conditions are met for all $0 \leq i \leq c - 1$:

1. For any S in C_i , the OR v of any k of the n rows satisfies $z_i(v) \geq h$, where v is a vector with coordinates in c colors and black color, and $z_i(v)$ denotes the number of coordinates in v equal to color i .
2. For any S in C_i , the OR v of any k of the n rows satisfies $z_i(v) \leq l$, for $j \neq i$.
3. For any $i_1 < i_2 < \dots < i_s$ in $\{1, 2, \dots, n\}$ with $s < k$, the collections of $s \times b$ matrices D_j , for $j \in \{0, 1, \dots, c - 1\}$ obtained by restricting each $n \times b$ matrix in C_j to rows i_1, i_2, \dots, i_s are indistinguishable in the sense that they contain the same matrices with the same frequencies.

Note that $h > l$ and b is the block length of a colored VCS. The cardinalities of the C_i are denoted as r and must coincide. The first two conditions can be called *color* ensuring that stacking k transparencies will reveal the original color of the pixel. The last condition is called *security* implying that $k - 1$ or fewer transparencies give absolutely no information about the shared secret. The value of h and l determines how good the revealed secret image is, and the value of b determines the resolution of the original picture.

5.1.2 A Colored k out of n VCS

Actually, the color i circle subpixel with a sector or color i and the other sector of black color cannot be directly used in the *image editing package*. The infrastructure of the modified color subpixels is shown in Figure 5.2.

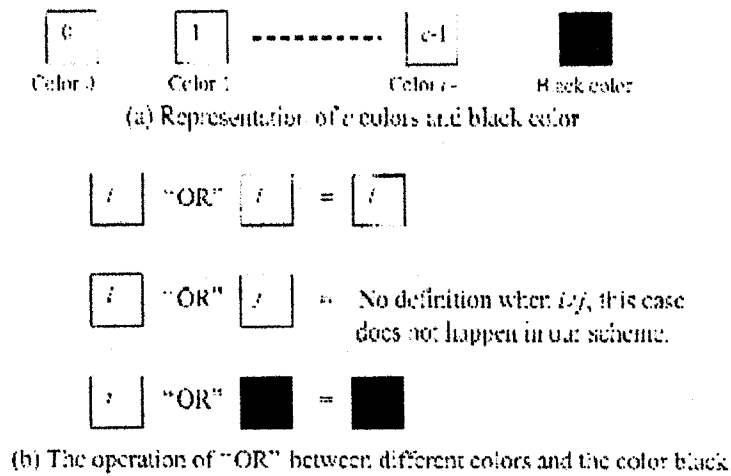


Figure 5.2: the infrastructure of colored subpixel and its OR operation(2)

Now we describe the construction based on the new infrastructure of colored subpixels. In the scheme, the block length $b = m \times c$, where c is the number of colors and m is the share size of the used black-and-white (k, n) -VCS.

Construction 5.2. Let B_0 and B_1 be the two $n \times m$ Boolean white and black matrices, respectively, as defined in conventional black-and-white (k, n) -VCS. The parameters are the share size m , the Hamming weight of any k of the n rows in black share matrix h' , the Hamming weight of any k of the n rows in white share matrix l' , and $h' > l'$. Then, a colored (k, n) -VCS with c colors has the $n \times (c \times m)$ matrices C_i , $i \in \{0, 1, \dots, c - 1\}$ and $C_i = \{ \text{all the matrices obtained by permuting the columns of } [B_0^{(0 \rightarrow i; 1 \rightarrow *)} | B_1^{(0 \rightarrow j_1; 1 \rightarrow *)} | \dots | B_1^{(0 \rightarrow j_2; 1 \rightarrow *)} | \dots | B_1^{(0 \rightarrow j_{c-1}; 1 \rightarrow *)}] \}$, where $j_1 \sim j_{c-1} \in \{\{0, 1, \dots, c-1\} - \{i\}\}$. The subscript $(0 \rightarrow i; 1 \rightarrow *)$ means that the elements 0 and 1 in B_0 or B_1 are replaced by i and $*$, respectively. The $*$ denotes the black color.

Theorem 5.3. *The scheme from Construction 5.2 is a colored (k, n) -VCS with "c" colors and the parameters are $b = c \times m$, $h = m - l'$, $l = m - h'$.*

Note that we can delete all the * columns to improve the block length so that we will have teh slightly better results. This improvement is shown in the following Lemma.

Lemma 5.4. *The scheme from Construction 5.2 can be improved with the parameters $b = ctimesm - \{the\ number\ of\ all-1\ columnss\ in\ B_0\} - (c - 1) \times \{the\ number\ of\ all-1\ columns\ in\ B_1\}$*

A colored (k, k) -VCS is just a particular case of Construction 5.1. Here, we will use the optimal construction of a black-and-white (k, k) -VCS to construct a colored (k, k) -VCS. The colored VCS will have the block length $b = c \times 2^{k-1}$, where c is the number of colors.

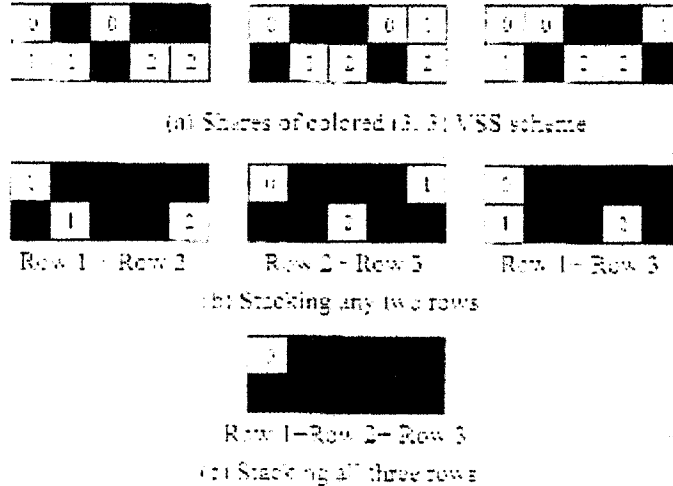


Figure 5.3: Three colored $(3,3)$ -VCS's subpixels for color 0

Example 5.5. *The three 3×10 matrices C_0, C_1 and be constructed as follows. First, review the B_0 and B_1 in optimal black-and-white $(3,3)$ -VCS as follows:*

$$B_0 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \quad B_1 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Since

$$[B_0^{(0 \rightarrow 0; 1 \rightarrow *)} | B_1^{(0 \rightarrow 1; 1 \rightarrow *)} | B_1^{(0 \rightarrow 2; 1 \rightarrow *)}] = \begin{pmatrix} 0 * 0 * * 1 1 * * 2 2 * \\ 0 * * 0 1 * 1 * 2 * 2 * \\ 0 0 * * 1 1 * * 2 2 * * \end{pmatrix}$$

then we delete all-* columns Finally, we get

$$C_0 = \text{by permuting the columns of } \begin{pmatrix} 0 * 0 * * 11 * 22 \\ 0 * * 01 * 12 * 2 \\ 00 * * 11 * 22* \end{pmatrix}$$

$$C_1 = \text{by permuting the columns of } \begin{pmatrix} 1 * 1 * * 00 * 22 \\ 1 * * 10 * 02 * 2 \\ 11 * * 00 * 22* \end{pmatrix}$$

$$C_2 = \text{by permuting the columns of } \begin{pmatrix} 2 * 2 * * 00 * 11 \\ 2 * * 20 * 01 * 1 \\ 22 * * 00 * 11* \end{pmatrix}$$

The share of a colored (3,3) VCS with three colors are further described in Figure 5.3. A pixel color 0 share by three shadows is divided into 10 subpixels as shown in Figure 5.3(a). Figure 5.3(b) and (c) show the results of stacking any two rows and all three rows, respectively.

5.2 Young-Chang Hou's Scheme

In [26], the researchers combined the previous results in [27] which involves the color decomposition principle and halftone technology to develop the algorithms of visual cryptography for colored secret image.

5.2.1 Basic Principles of Colors

First the author review the basic principles of colors: The additive and subtractive models are commonly used to describe the constitutions of colors. In additive system, the primaries are red, green and blue(RGB), with desired colors being obtained by mixing different RGB components. By controlling the intensity of red (green or blue) component, we can modulate the amount of red (green or blue) in the compound light. The more the mixed colored-lights, the more is the brightness of the light. When mixing all red, green and blue components with equal intensity, white color will result. The computer monitor is a good example of the additive model.

In the subtractive model, color is represented by applying the combinations of colored-lights reflected from the surface of an object (because most objects do not radiate by themselves). Take an apple under the natural light for example. The surface of the apple absorbs green and blue part of the natural light and reflects the red light to human eyes, so it becomes a red apple. By mixing cyan (C) with magenta (M) and yellow (Y) pigments, we can produce a wide range of colors. The more the pigment we add, the lower is the intensity of the light, and thus the darker is the light. This is why it is called the subtractive model. C, M and Y are the three primitive colors of pigment, which cannot be composed from other colors. The color printer is a typical application of the subtractive model.

In computer systems, Application Interfaces (APIs) provided by most image processing software as well as the Windows operating system are based on the RGB model. This is mainly because they use monitors as the primary output media. Monitors themselves generate color images by sending out RGB light into humans retina. In true color systems, R, G, B are each represented by 8 bits, and therefore each single color of R, G, B can represent 0 – 255 variations of scale, resulting in 16.77 million possible colors. When using (R, G, B) to describe a color pixel, (0;0;0) represents full black and (255; 255; 255) represents full white.

In visual cryptography, we use sharing images as the decryption tool; that is, the final outputs are transparencies. Because the subtractive model is more suitable for printing colors on transparencies, we will use the CMY model to represent colors in what follows. Because (R, G, B) and (C, M, Y) are complementary colors, in the true color model, (R, G, B) and (C, M, Y) possess the following relationships: $C = 255 - R$, $M = 255 - G$, $Y = 255 - B$. Thus, in the (C, M, Y) representation, (0;0;0) represents full white and (255; 255; 255) represents full black.

Because most color printers use C, M, Y ink to display color, a color image must be processed by the color-decomposed procedure before printing. Color decomposition mainly is to separate C, M, and Y colors from colors within every pixel of the image. These three components form three monochromatic images. These monochromatic images are like gray-level images in which every pixel has its own color level and has to be transformed into a halftone image before printing. The three monochromatic halftone images will be (cyan, white), (magenta, white) and (yellow, white) binary images, respectively. After stacking these images, all kinds of the colors in the original image can be displayed. Figure 5.4 illustrates the procedure of printing color images.

We can see from the figure that every pixel P_{ij} of the composed color image P is obtained by combining the corresponding pixels C_{ij}, M_{ij}, Y_{ij} in the three C, M, and Y separating halftone images, where C, M, and Y images are all binary. For any pixel, C_{ij}, M_{ij} or Y_{ij} , there are only two possible values: blank or not blank, where 0 denotes blank, and 1 denotes the corresponding color. Hence P_{ij} has the following possible combinations: (0;0;0), (1;0;0), (0;1;0), (0;0;1), (1;1;0), (1;0;1), (0;1;1), and (1;1;1), where $P_{ij}(0;0;0)$ denotes a white pixel, and (1;1;1) denotes a black pixel. Because C, M, and Y are primitive colors in the subtractive model, they retain the usual characteristics that C (M or Y) plus C (M or Y) is C (M or Y), C (M or Y) plus white is C (M or Y), and white plus white is white, when stacking them on transparent media. In the following sections, we will introduce our three methods for color visual cryptography.

5.2.2 Three Algorithms for Colored Visual Cryptography

In this section, three methods will be introduced. For simplicity, the schemes and algorithms are shown as follows.

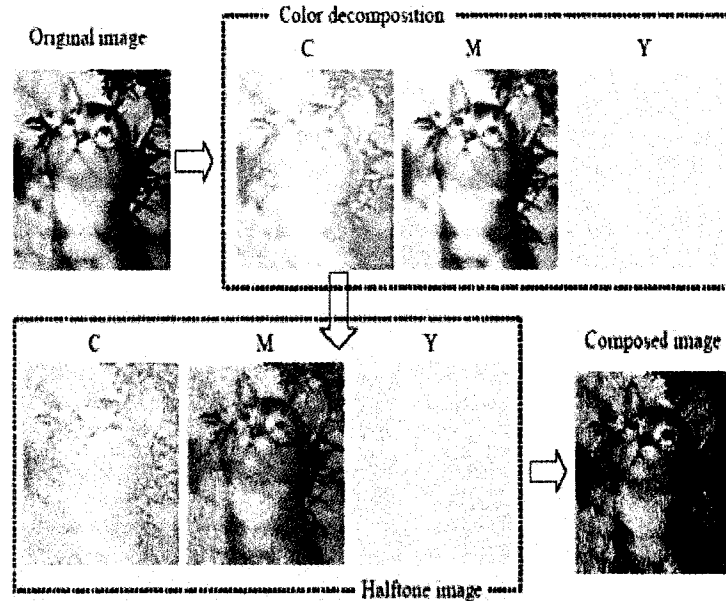


Figure 5.4: Color image printing

Method 1

The method uses the procedure illustrated in Figure 5.4 to transform a color secret image into three C, M, and Y halftone images. Then, every pixel of the halftone images is expanded into a 2×2 block. Every block of the sharing images therefore includes two transparent (white) pixels and two color pixels so that the entropy reaches its maximum to conceal the content of the secret image. Furthermore, we design a half black-and-white mask to shade unexpected colors on the stacked sharing images so that only the expected colors show up.

Take Figure 5.5 for example. If pixel P_{ij} of the composed image is $(0; 0; 0)$, the distribution of the color pixels in the three sharing images is assigned as the first row in Figure 5.5. After stacked by the mask image, all the color pixels on the three sharing images are shaded by black pixels and only the white pixels can reveal, thus showing a white-like color. If pixel P_{ij} is $(1; 1; 0)$, only the C and M components are revealed, with the Y component being covered by the black mask. The distribution of the color pixels in the three sharing images is as the fifth row in Figure 5.5, thus showing a blue-liked (cyan plus magenta) color. If pixel P_{ij} is $(1; 1; 1)$, the C, M, and Y parts can all be revealed, thus showing a black color. The distribution of the color pixels in the three sharing images is as the eighth row in Figure 5.5. The eight combinations of the three primary colors of the composed image under this method are illustrated in Figure 5.5.

Algorithm 5.6. 1. Transform the color image into three halftone images: C, M,

Mask	Revealed color (C,M,Y)	Share1(C)	Share2(M)	Share3(Y)	Stacked image	Revealed color quantity (C,M,Y)
	(0, 0, 0)					(1/2, 1/2, 1/2)
	(1, 0, 0)					(1, 1/2, 1/2)
	(0, 1, 0)					(1/2, 1, 1/2)
	(0, 0, 1)					(1/2, 1/2, 1)
	(1, 1, 0)					(1, 1, 1/2)
	(0, 1, 1)					(1/2, 1, 1)
	(1, 0, 1)					(1, 1/2, 1)
	(1, 1, 1)					(1, 1, 1)

Figure 5.5: Scheme 1 of color cryptography

and Y .

2. For each pixel P_{ij} with color components $(C_{ij}, M_{ij}$ or $Y_{ij})$ of the composed image P , do the following:
 - Select a black mask with a size of 2×2 , and assign a black pixel randomly to two of these four positions and leave the rest positions blank (transparent or white). This step will make the black mask a half black-and-white block.
 - After selecting a mask, determine the positions of the cyan pixels in the block of the corresponding sharing images. This is done according to the positions of the black pixels in the mask and the value of C_{ij} .
 If $C_{ij} = 1$ (the cyan component will be revealed), fill the positions corresponding to the positions of the white pixels in the mask with a cyan pixel and leave the rest positions blank.
 If $C_{ij} = 0$ (the cyan component will be hidden), fill the colors in the opposite way. That is, fill the positions corresponding to the positions of the black pixels in the mask with a cyan pixel and leave the rest positions blank.
 Finally, add the block to the corresponding position of Share 1.
 - In accord with the above step, determine the positions of magenta pixels of the block in Share 2 with the value of M_{ij} and those in Share 3 with the value of Y_{ij} .
3. Repeat Step 2 until every pixel of the composed image is decomposed, hence obtaining four transparencies (cyan, magenta, yellow and black) of visual cryptography to share the secret image.

4. After stacking the four sharing images, the secret image can be decrypted by human eyes.

Method 2

Algorithm 5.7. 1. Transform the color image into three halftone images: C , M , and Y .

2. For each pixel P_{ij} of the composed image, do the following:

- Expand a 2×2 block in Share 1 and fill the block with cyan, magenta, yellow, and transparent randomly.
- Generate a 2×2 block in Share 2 according to the permutation of the four colors of the block in Share 1 and the values of C_{ij} , M_{ij} , Y_{ij} , and determine the color distribution of the corresponding block in Share 2 as illustrated in Figure 5.6.

3. Repeat Step 2 until every pixel of the composed image is decomposed, hence obtaining two visual cryptography transparencies to share the secret image.

4. After stacking two sharing images, the secret image can be decrypted by human eyes.

Revealed color (C,M,Y)	Share 1	Share 2	Stacked image	Method	Resultant result	Revealed color quantity (C,M,Y)
(0, 0, 0)				Share 1 and Share 2 with the same permutation		(1/4, 1/4, 1/4)
(1, 0, 0)				Swap the position of cyan and transparent		(1/2, 1/4, 1/4)
(0, 1, 0)				Swap the position of magenta and transparent		(1/4, 1/2, 1/4)
(0, 0, 1)				Swap the position of yellow and transparent		(1/4, 1/4, 1/2)
(1, 1, 0)				Swap the position of cyan and magenta		(1/2, 1/2, 1/4)
(0, 1, 1)				Swap the position of yellow and magenta		(1/4, 1/2, 1/2)
(1, 0, 1)				Swap the position of cyan and yellow		(1/2, 1/4, 1/2)
(1, 1, 1)				Swap two positions in pair		(1/2, 1/2, 1/2)

Figure 5.6: Scheme 2 of color cryptography

Method 3

In order to alleviate the inconvenience of Method 1, which needs four sharing images, and the loss of image contrast under Method 2, the third method is established.

This method needs only two sharing images and does not sacrifice too much contrast for color visual cryptography. It transforms a color secret image into three halftone images C , M , and Y and exploits the technique of gray-level visual cryptography to generate six temporary sharing images C_1, C_2, M_1, M_2, Y_1 , and Y_2 . Each of these sharing images will have two white pixels and two color pixels in every 2×2 block; i.e. all the color quantities are $2/4$.

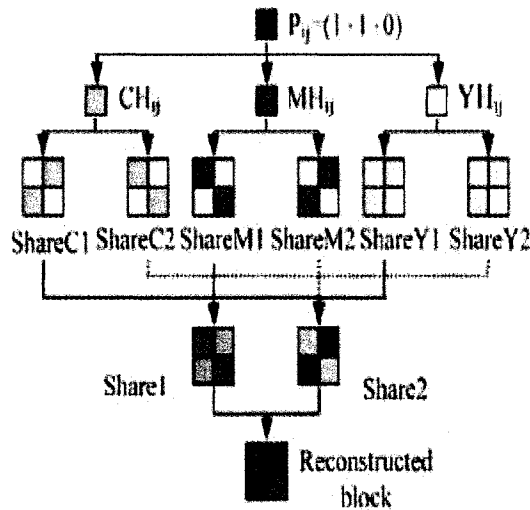


Figure 5.7: Scheme 3 of color cryptography

Algorithm 5.8. 1. Transform the color image into three halftone images: C , M , and Y .

2. For each pixel P_{ij} of the composed image, do the following:

- According to the traditional method of black-and-white visual cryptography, expand C_{ij}, M_{ij} and Y_{ij} into six 2×2 blocks, $C1_{ij}, C2_{ij}; M1_{ij}, M2_{ij}$ and $Y1_{ij}, Y2_{ij}$.
- Combine the blocks $C1_{ij}, M1_{ij}$ and $Y1_{ij}$ and fill the combined block corresponding to P_{ij} in Share 1.
- Combine the blocks $C2_{ij}, M2_{ij}$ and $Y2_{ij}$ and fill the combined block corresponding to P_{ij} in Share 2.

3. Repeat Step 2 until every pixel of the composed image is decomposed, hence obtaining two visual cryptography transparencies to share the secret image.

4. *After stacking the two sharing images, the secret image can be decrypted by human eyes.*

Although this paper only involves the $(2,2)$ or simple VCS, it can also be easily applied to the k out of n VCS and the extended schemes for visual cryptography.

From the previous literatures about the colored visual cryptography, we can find that there will be much more further work deserved to research.

Chapter 6

Implement Visual Cryptography by Other Methods

The conventional visual cryptography proposed by Naor and Shamir is based on the "OR" operation of the columns of the basic matrices. However, it is not the unique way to implement the visual cryptography because some researchers found other effective and efficient approaches.

In [22], the authors present an optical method for visual cryptography using phase masks and an interferometer. Moreover, in [25], neural networks is used in the novel approach for implementing the visual cryptography. Here, another new method will be described in details in following sections.

6.1 P.Tuyls, H.D.L.Hollmann, J.H.v.Lint, L.Tolhuizen's Scheme

The new visual cryptography system proposed by these authors in this paper uses the polarization of light and has good color, contrast, and resolution properties.

This method is based on two well-known physical principles: 1) Polarizers only transmit light whose polarization is aligned with the one of the polarizer (sunglasses) and 2) Liquid Crystal(LC) cells can be used to rotate the polarization direction of incoming light.

At first, the authors set up a model for the visual cryptography system.

6.1.1 Model

In order to introduce the model, they explain the physics of an LC display with black-light. An LC display consists mainly of four layers (Figure 6.1). The first one has the black light. The second layer consists of a polarizer, the third one is the LC layer and the fourth one consists again of a polarizer. The black emits circularly polarized light. The first polarization layer projects the polarization of the incident light on its

polarization direction. Depending on the voltage that is applied to a LC cell, this LC cell will rotate the polarization of the light that enters it over a certain angle. If the polarization direction of the light leaving the LC-layer matches that of the final polarizer, light comes out of the display. If on the other hand the polarization of the light coming out of the LC is perpendicular to the polarization direction of the final polarizer, no light comes out. By applying voltages to the LC-cell such that the polarization direction of the outgoing light makes an angle $\phi \leq \pi/2$ with the polarization direction of the second polarizer, gray scales can be generated.

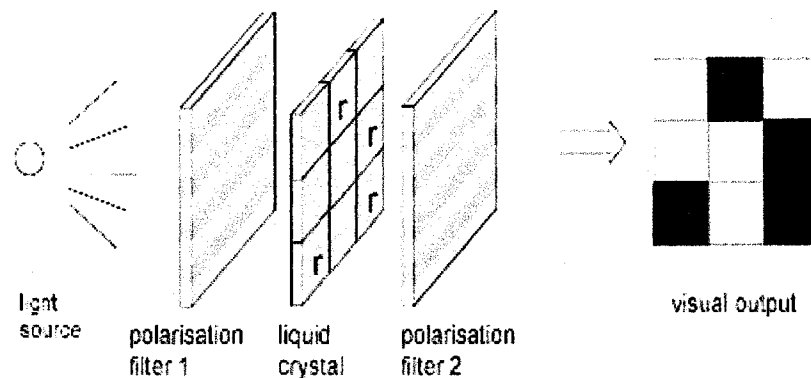


Figure 6.1: Structure and principle of an LC display.

In Figure 6.1, the symbol r in a cell means that this LC cell rotates the polarization of the incoming light. In order to build a visual cryptography system based on LC displays they proceed as follows (Figure 6.2). There are two displays consisting of an LC layer which have a polarizer at one side and no polarizer at the other side. Also, assume that the first LC has the backlight and the second has not. The second display has to be considered as a dedicated trusted device that a user is carrying with him. The shares of both users are then the two (or more) LC layers on which the dealer writes a certain pattern in terms of the angle of rotation of the various LC cells.

Assume that the direction of the first polarizer equals that of the second polarizer and is horizontal. Furthermore, assumed that two voltages can be applied to LC cells V_1 and V_2 . When the voltage V_1 is applied, the LC cell will not rotate the polarization direction of the incoming light, while when the voltage V_2 is applied, the polarization direction is rotated over an angle of 90 degrees. When an LC consists of N pixels (LC cells), one share will basically consist of N voltages (corresponding to the angle of rotation of the different cells). In Figure 6.3, Table 1 summarizes the physics for one pixel. It follows from Table 1 that when two superimposed LC cells apply the same rotation, this generates a white pixel and when they rotate the polarization over a different angle this generates a black pixel.

If an LC does not rotate the polarization of the incoming light, then we will denote this by a 0. If on the other hand the polarization is rotated over 90 degrees by the

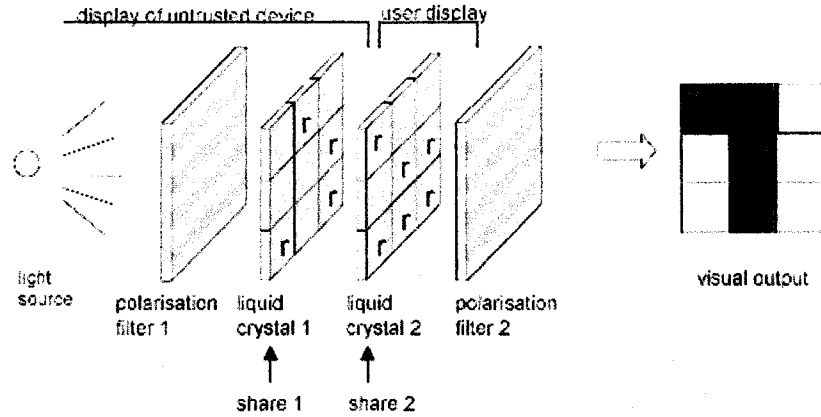


Figure 6.2: Visual cryptography system by superimposing two LC layers.

Pol filter 1	→	→	→	→
LC1			○	○
LC2		○		○
Pol filter 2	→	→	→	→
Color	white	black	black	white

Table 1: This table summarizes the physics of a polarisation based visual crypto system. The arrows → indicate that the polariser projects the polarisation direction of the incoming light on the horizontal. The symbols | and ○ stand for LC cells that do not and do rotate the polarisation direction of the light respectively.

LC1	0	0	1	1
LC2	0	1	0	1
Color	0	1	1	0

Table 2: Mathematical model of Table 1.

Figure 6.3: Tables for the model

LC cell, this will be denoted by a 1. This means that the mathematical structure of the system is that of binary addition as follows from Table 2 in Figure 6.3. The visual encryption scheme corresponds then to the physic implementation on LC layers of the One Time Pad based on an XOR operation. As LC layers can be driven electronically (as in LCD's), the key can be easily updated(using pseudo random number generators), which leads to a practical updating mechanism.

6.1.2 Threshold Visual Secret Sharing Schemes

In this section, the threshold visual secret sharing scheme based on the polarization rotation technique as explained in section 6.1.1 will be constructed. Here, only the black-and-white images are considered.

Following from the definition of the conventional visual cryptography, for a vector $v \in GF(2)^b$, we denote by $z(v)$ the number of zero entries in the vector v (note that $z(v) + w(v) = b$, where $w(v)$ denotes the Hamming weight of the vector v). A k out of n threshold visual secret sharing scheme (TVSS) $S = (C_0, C_1)$ consists of two collections of $n \times b$ binary share matrices C_0 and C_1 .

Definition 6.1. Let k, n, b, h, l be positive integers satisfying $1 \leq k \leq n$ and $b \geq h > l$. A $[(k, n); b, h, l]$ TVSS scheme consists of two collections of $n \times b$ boolean matrices C_0 and C_1 such that:

1. For any $s \in C_0$, the XOR v of any k of the n rows of s satisfies $z(v) \geq h$.
2. For any $s \in C_1$, the XOR v of any k of the n rows of s satisfies $z(v) \leq l$.
3. For any $i_1 < i_2 < \dots < i_t$ in $\{1, 2, \dots, n\}$ with $t < k$ the two collections of $t \times b$ matrices \mathcal{D}_j for $j \in \{0, 1\}$, obtained by restricting each $n \times b$ matrix in C_j , for $j = 0, 1$, to rows i_1, i_2, \dots, i_t are indistinguishable in the sense that they contain the same matrices with the same frequencies.

h is called the white level of the system and l is called the black level. The parameter b is called the block length and determines the resolution of the scheme.

Proposition 6.2. Let $S = (C_0, C_1)$ be a $[(k, n); b, h, l]$ TVSS scheme with k odd and let \hat{C}_i be obtained from C_i by replacing zeros by ones and vice versa. Then, the scheme $\hat{S} = (\hat{C}_0, \hat{C}_1)$ is a $[(k, n); b, b - l, b - h]$ scheme with contrast \hat{c} ,

$$\hat{c} = (h - l) / (2b - l - h).$$

It follows that $\hat{c} > c$ whenever $l + h > b$.

Proposition 6.3. Let $S = (C_0, C_1)$ be a $[(k, n); b, h, l]$ TVSS scheme with $k \geq 3$ and let c_1 and c_2 be two rows of a share matrix in C_0 and hence also two rows of a share matrix in C_1 . Then,

$$d(c_1, c_2) \leq \min\{2l, 2(b - h)\}$$

where $d(\cdot, \cdot)$ denotes the Hamming distance.

n out of n visual secret sharing

In this section, we can show that (n, n) TVSS schemes can have maximal contrast ($c = 1$) with minimal block length ($b = 1$).

Proposition 6.4. *Let C_0 and C_1 be two sets of $n \times 1$ matrices defined as follows.*

$$C_0 = \{s \in (GF(2))^n \mid \bigoplus_{i=1}^n s_i = 0\}, C_1 = \{s \in (GF(2))^n \mid \bigoplus_{i=1}^n s_i = 1\}.$$

Then, the scheme $S = (C_0, C_1)$ is a $[(n, n); 1, 1, 0]$ TVSS scheme.

Hence, in this set-up there exist visual encryption schemes with good contrast and resolution properties. This stands in sharp contrast with OR-based visual cryptography systems where maximal contrast schemes can only exist if $b > 1$.

(2,n) TVSS Schemes

A general construction for $(2, n)$ TVSS schemes is given by the following theorem. It shows that $(2, n)$ TVSS schemes are equivalent to binary codes. By a (b, n, d) code, we mean a binary code of length b , n words and minimum Hamming distance d .

Theorem 6.5. *Let b, l be natural numbers with $b > 1$ and $0 \leq l \leq b$. A $[(2, n); b, b, l]$ TVSS scheme exists if and only if there exists a binary $(b, n, b - l)$ code C .*

Corollary 6.6. *The contrast of a $[(2, n); b, b, l]$ TVSS scheme is at most*

$$(b - \log_2 n + 1) / (b + \log_2 n - 1)$$

6.1.3 General k out of n visual secret sharing schemes

In this section, two constructions of (k, n) TVSS scheme for all $3 \leq k \leq n - 1$. The first construction is recursive, the second one is a direct construction and based on so-called MDS codes known from algebraic coding theory.

Construction 1

Firstly we emphasize that in all of the following constructions we produce two classes of share matrices consisting of n rows called C_0 and C_1 . In each step of the construction we will let the permutation group S_n act on the n rows of the share matrices in C_0 and C_1 . The appropriate permutation group S will act on the columns of the share matrices C_0 and C_1 . This ensures the indistinguishability property according to Definition 6.1 for the sets C_0 and C_1 . In all constructions, assumed that this is done without mentioning this.

The idea of the construction is the following. Denote by a_i the weight of the sum of any $1 \leq i \leq k$ rows of a matrix $A \in C_0$ and similarly we use the notation b_i for the weight any i rows for $B \in C_1$. The construction will guarantee that $a_i = b_i$ as long as $i < k$ and that $a_k \neq b_k$ as required by the indistinguishability property.

(3, n) TVSS scheme Let $B \in M^{n \times (2n-2)}$ be a matrix defined as follows,

$$B = (I_n J_{n,n-2}),$$

where I_n stands for the $n \times n$ identity matrix and $J_{n,n-2}$ is the all one matrix with n rows and $n-2$ columns. The matrix $A \in M^{n \times (2n-2)}$ is defined as the complement of B . We build the sets of share matrices C_0 and C_1 by letting the appropriate permutation groups act on the rows and the columns of the matrices A and B respectively, as the previous section described.

Proposition 6.7. *The scheme $S = (C_0, C_1)$ as defined in the previous paragraph is a $[(3, n); 2n-2, n+1, n-3]$ TVSS scheme with contrast $c = 4/(2n-2)$.*

Construction 2

In this section, assumed that $2 < k < n$. In order to construct (k, n) TVSS schemes we make use of MDS codes over $\text{GF}(q)$, the finite field with q elements. Because an $[n, k, n-k+1]$ MDS code over $\text{GF}(q)$ exists if $q+1 \geq n$, we choose $q \geq n-1$.

We start by constructing the set C_1 . Let A be a $n \times q^k$ matrix over $\text{GF}(q)$. The columns of A consists of q^k words of an $[n, k, n-k+1]$ code \mathcal{C} over $\text{GF}(q)$.

Lemma 6.8. *Denote by A^s the restriction of the matrix A to the first s rows. The columns of the matrix A^k contain each vector of the vector space $\text{GF}(q)^k$ exactly once. Moreover, the restriction A^{k-1} contains each vector of $\text{GF}(q)^{k-1}$ exactly q times.*

Lemma 6.8 holds for the restriction of A to any k rows, as one sees by inspection of its proof. We derive a binary matrix $\hat{A} \in M^{n \times q^k}$ from the matrix A by replacing all non-zero entries of A by the element 1.

Lemma 6.9. *Let A^{i_1, \dots, i_k} denote the restriction of the matrix A to the rows i_1, \dots, i_k and denote by $v_{i_1, \dots, i_k}^\oplus \in \text{GF}(2)^{q^k}$ the sum of the k rows of the associated binary matrix $\hat{A}^{i_1, \dots, i_k}$. Then,*

$$z(v_{i_1, \dots, i_k}^\oplus) = \frac{q^k + (2-q)^k}{2}$$

Since the number $z(v_{i_1, \dots, i_k}^\oplus)$ does not depend on the rows i_1, \dots, i_k , we will further denote this number simply by $z(v_b^\oplus)$. Put $A_1 = \hat{A}$ and define the set C_1 as the set of share matrices obtained by letting the permutation group S_{q^k} act on the columns of the matrix \hat{A} .

Next, we describe the construction of the set C_0 . Denote by B_0 an $n \times q^{k-1}$ matrix over $\text{GF}(q)$ whose columns are the words of an $[n, k-1, n-k+2]$ (MDS) code over $\text{GF}(q)$ (this code exists since $n \leq q+1$). The matrix B consists of q copies of the matrix B_0 and is hence an $n \times q^k$ matrix over $\text{GF}(q)$.

Lemma 6.10. *Denote by B^{i_1, \dots, i_k} the restriction of the matrix B to the rows i_1, \dots, i_k . Then, the columns of the matrix B^{i_1, \dots, i_k} contain each vector of $\text{GF}(q)^k$ either zero or q times. The columns of the matrix $B^{i_1, \dots, i_{k-1}}$ contain each vector of the space $\text{GF}(q)^{k-1}$ exactly q times.*

We define the binary matrix \hat{B} be replacing in the matrix B each non-zero entry by one. Put $A_0 = \hat{B}$.

Lemma 6.11. *Let $A_0^{i_1, \dots, i_k}$ denote the restriction of the matrix A_0 to the rows i_1, \dots, i_k . Then, the number of zeroes in the sum vector $v_{i_1, \dots, i_k}^\oplus$ is given by*

$$z(v_{i_1, \dots, i_k}^\oplus) = z(v_b^\oplus) + (q - 1)2^{k-1}.$$

Again, we remark that the number $z(v_{i_1, \dots, i_k}^\oplus)$ does not depend on the rows i_1, \dots, i_k . Therefore, we denote this number by $z(v_w^\oplus)$. The set C_0 is then defined by letting the permutation group S_{q^k} act on the columns of A_0 .

Construction 2 of a general (k, n) schemes

1. Choose q (power of a prime) with $q \geq n - 1$.
2. Define the sets of share matrices C_0 and C_1 as earlier in this section.
3. Define the scheme $S = (C_0, C_1)$.

Theorem 6.12. *The scheme $S = (C_0, C_1)$ as defined in construction 2, is a $[(k, n); q^k, z(v_w^\oplus), z(v_b^\oplus)]$ TVSS scheme.*

Finally, note that the contrast c of $[(k, n); b, h, l]$ schemes in construction 2 is given by

$$c = ((q - 1)2^{k-1}) / (q^k + (-1)^k(q - 2)^k + (q - 1)2^{k-1}).$$

Chapter 7

Visual Cryptography with cheating shares

In the past decade, the researchers were mainly concentrated on the improvement of the contrast and subpixel expansion. Consequently, a lot of papers with regard to these two directions are published. However, in these conventional visual cryptography schemes, there is an assumption that all the shareholders are inherently honest which means they do not take the people who may have effect on the security into account. Therefore, it is no doubt that this assumption can cause a fatal security problem of visual cryptography.

In [14], the authors present one of the traitor's cases: In (k, n) visual cryptography scheme, if $k - 1$ of shareholders become the traitors and then they pool their shares together and publish the resulting image, any other shareholders are able to obtain the secret image after stacking their own shares with the published one. Obviously, this traitorous behavior may collapse the visual cryptography system and it is prohibited.

Here, we will describe another possible attack by the cheating shares and the method proposed by Naor and Pinkas [16] will be used to solve the problem.

7.1 Attack Statement

In the conventional visual cryptography, the shares distributed to the shareholders are printed on the *whole* transparency. Thus, after stacking their transparencies, the secret image is displayed. However, this process also provides a possible attack by the cheating shares.

Now, we consider the following situation: some shares are modified by the shareholders, so that other people might obtain wrong information when they reveal the image. This problem was discussed by Naor and Pinkas when they considered visual authentication and identification scheme in [16]. In fact, if some shareholders alternate some pixels of their own shares (e.g., changing the white pixels to the black ones.), then overlaying the shares including the alternated ones will be accepted as the original one because none of the shareholders knows the secret image. Since every share is printed

on the whole transparency, it is not difficult to change pixels of shares by a shareholder. We will call a shareholder traitor when he/she modified his/her share.

In terms of 2 out of 2 visual cryptography, there are two types of changes defined as follows[16].

- Traitors can change the position of the two black subpixels in the squares in the image. This change cannot be noticed by the recipient.
- Traitors can put more than or less than two black subpixels in a square. This produces an illegal share. However, this deviation will probably go unnoticed by recipient unless it is done in too many pixels.

Here, we first take a look at a simple example: The dealer encrypts the secret image with information “EF” (Figure 7.1) to share 1 (Figure 7.2(a)) and share 2 (Figure 7.2(b)).



Figure 7.1: Original text with secret information “EF”

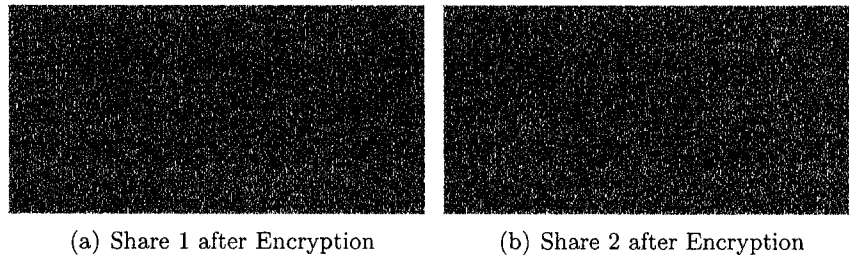


Figure 7.2: Shares after Encryption

If we stacked them carefully, the correct secret image (Figure 7.3) will be acquired.

However, when the shareholder who holds the share 1 change to be a traitor, he changed his share1 to share3 by alternating some pixels (Figure 7.4). It is obvious from Figure 7.4 that we have no idea whether the share has been changed or not. Therefore, after overlaying share2 and share3, the wrong information “FE” will be accepted as the original image and then the attack is successful.

In our proposed scheme, we consider four situations of that kind of attacks based on the destructive effect on cheating shares:

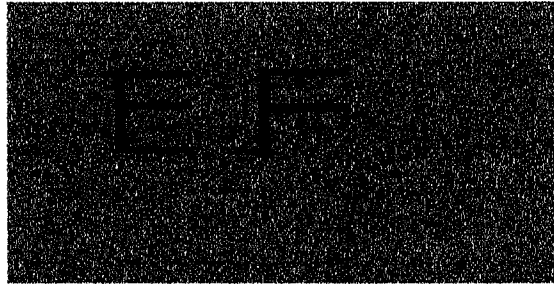


Figure 7.3: Normal resulting image after Decryption

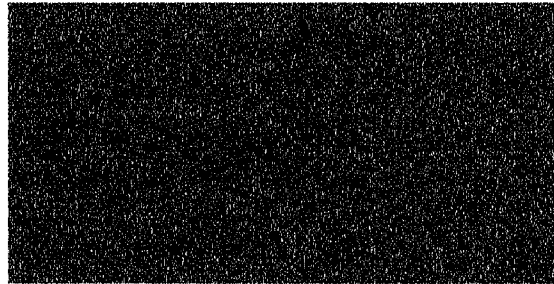


Figure 7.4: Share 3 changed from share1 by the traitor



Figure 7.5: The changed resulting image with different information "FE"

- Complete Success: The secret image is changed to a different meaning and honest shareholders cannot find the change, while the traitor can find out the correct original image.
- Success: The secret image is changed. The honest shareholders are aware of the change, but do not know the original image. The traitor can find out the original image.
- Partial Success: The secret image is changed. All the people are aware of the change but no one knows the original image.
- Failure: The secret image is changed. All the people are aware of the change but

they can still find out the original image.

As the traitors, the higher-level attack they implement, the more success they will achieve.

For simplicity, we will first consider the 2-out-of-2 visual secret sharing scheme of [17]. In this scheme an image is represented as a collection of pixels. Each pixel is represented by a square of 2×2 real pixels that are called subpixels. For the pixels on the plaintext, each of them is split into two shares with four subpixels such that two of subpixels are black and the others are white in each share. As Figure 3.1 illustrated, there are three types of arrangements of these black and white subpixels: vertical, horizontal and diagonal. Suppose that in first share one of the horizontal types is chosen in such a way that the two upper subpixels are black and the lower are white. If in the other share, the complementary type of horizontal shares is chosen in which the lower subpixels are black and the upper subpixels are white, then stacking the two shares yields an image in which all four subpixels are black. If on the other hand the upper subpixels are black and the lower subpixels are white in the second share, then stacking the shares composes an image in which only two subpixels are black. Moreover, if different types of subpixels are chosen (e.g., the first share is vertical and the second share is horizontal), then after stacking the shares the resulting pixel with three black subpixels which is also considered as white will be obtained. In Figure 3.1, for each pixel, the first share is randomly chosen from one of the six options. If the pixel is black, the second share will contain complementary subpixels and if the pixel is white, the second share will be the same as the first share or different types of subpixels .

Following the definition of visual cryptography, we will consider images containing black and white pixels only. In fact, we will mainly consider text images. The reason is that all the known visual cryptographic schemes will reduce the contrast of a image and therefore the useful real applications perhaps are for text images only.

There are three phases in our scheme.

1. **Share creation:** To create shares, a dealer randomly chooses a matrix from C_0 for a white pixel and a matrix from C_1 for a black pixel (In addition, a matrix from C_2 defined later in our method for a grey pixel). The chosen matrices define the color of the m sub-pixels in each of the n shares. After this phase the dealer is no longer exits.
2. **Share holding:** There are n shareholders in the scheme, each of them keeps a share. During this phase, there are no computing limitations for shareholders. The shareholders are able to analyze and modify the shares they possessed.
3. **Image recovering:** k of the n shareholders put their shares together to recover the original image. In this phase, the shareholders have very limited computing abilities. Basically, they only can align the shares and recognize the image by vision.

In our scheme, there is a dealer \mathcal{D} who will distribute the shares to the shareholders. We assume that the dealer is always honest and after share distribution, the dealer will be out of the scheme.

The shareholders have unlimited computation abilities during their share holding time. When the shareholders pool their shares together to reveal the visual information, their computation abilities are limited. However, sometimes we will assume they have some certain computation capacities (they have sharp eyes, as we explained later).

In this paper, we will use some techniques from [16]. Their scheme can be described as follows.

7.2 Visual Authentication and Identification Application

7.2.1 Visual Authentication Scheme

In order to carry out the visual authentication application for the smart card system, Naor and Pinkas [16] put forward three methods which function as one-time pad authentication. One of them that we will make advantage of is “ Position on Screen ” method. Now we are going to describe it in details. At first, let us review some definitions of the visual authentication scheme.

Definition 7.1. (*visual authentication scenario*) *There are three entities in the visual authentication scenario: H (Harry), P (Peggy) and S (Sally). H is human and has human visual capabilities. For each protocol the capabilities that are required from H must be stated. These capabilities must include the ability to identify an image resulting from the composition of two shares of a 2-out-of-2 visual secret sharing. Other capabilities might be the ability to verify that a certain area is black, the ability to check whether two images are similar, etc.*

There is a security parameter n , such that the storage capacities and computing power of S and P are polynomial in n .

In the initialization phase S produces a random string r , and creates a transparency T_r and some auxiliary information A_r as function of r . Their size is polynomial in the security parameter n . S send T_r and A_r to H through an off-line initialization private channel to which P has no access (this is the only time this private channel is used). S also sends to H a set of instructions that H should perform in the protocol (e.g. checking at a certain point in time whether a certain area in the image is black, comparing two areas, etc). These instructions are public and might get known to P , but she is unable to change them.

Following the initialization phase all the communication between H and S is done through a channel controlled by P , who might change the transferred messages.

Definition 7.2. (*visual authentication protocol*) *S wishes to communicate to H an information piece m , the content of which is known to P .*

- S sends a message c to H , which is a function of m and r .
- P might change the message c before H receives it.
- Upon receiving a message c' H outputs either *FAIL* or $\langle \text{ACCEPT}, m' \rangle$ as a function of c' and his secret information T_r and A_r . When he outputs *ACCEPT* he also outputs m' , what he thinks to be the information sent to him from S .

Next, the definition of security requirements from visual authentication systems is presented.

Definition 7.3. (*visual authentication system*) Assume that H has the capabilities required from him for the protocol, that he acts according to the instructions given in the protocol, and that the visual authentication system has the property that when P is faithful then H always outputs $\langle \text{ACCEPT}, m \rangle$. we call the system

- $(1 - p)$ -**authentic** if for any message m communicated from S to H the probability that H outputs $\langle \text{ACCEPT}, m' \rangle$ is at most p (where m' is of course different from m).
- $(1 - p)$ -**single-transformation-secure** ($(1 - p)$ -sts) if for any message m communicated from S to H and any $m' \neq m$ (which was determined a-prior) the probability that H outputs $\langle \text{ACCEPT}, m' \rangle$ is at most p .

Here the $(1 - p)$ -authentic system is more securer than $(1 - p)$ -sts visual authentication system because $(1 - p)$ -sts visual authentication system only guarantee that it is hard to change the secret information to a specified message which was predefined.

Based on the definitions, we keep reviewing the “ Position on Screen ” method proposed in [16]. There are two essential elements of “ Position on Screen ” method which also provide the basic idea for our method.

- **Bounding Box:** In the initialization phase, the authors establish some assumptions: The image is composed of $r \times c$ pixels. A “bounding box” of size $r' \times c'$ pixels is drawn with a thin line at a random location on the transparency that is given to the shareholders. During the authentication communication, the combination of the transparency and the communicated share should have the confidential message displayed inside the bounding box, in white on a black background which covers all pixels inside and outside the bounding box. The Figure 7.6 illustrates a transparency with a *marked* bounding box and a composed image with message in the bounding box.

Obviously, the bounding box is very useful for us to prevent the attack mentioned in previous section. Due to random position of bounding box, even the traitor has a powerful cryptanalytic ability, it is a low possibility that he can obtain the right position of share on the transparency. Therefore, alternating the color of pixels in other areas of transparency will make no sense to the real share. If the traitor alternates the pixels in a large area of the transparency, he also fails to

implement a successful or higher level attack because the shareholder will find out the share is changed by someone. So this property of bounding box prevent the high level attacks effectively.

- **Previously Known Position:** As the Figure 7.6 illustrated, the position of bounding box is marked on transparency and hence the shareholder previously knows the position of share on the transparency. Also, the message should be displayed in white on a black ground after stacking the shares. These two properties are good enough to prevent two types of attacks. If the traitor change pixels of areas besides the valuable message on the transparency, it is easy to be noticed and it also warns the shareholder of being more careful with her own share next time. Moreover, if the traitor carry out another successful attack in which a false share is also put on the transparency to make the consumer confused, the shareholder can recognize the real one because of previously known position of bounding box. However, this property is not applicable to our method and thus we modify it to satisfy our scheme (we will explain it later).

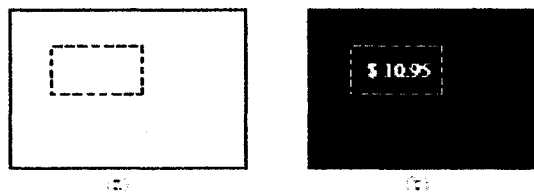


Figure 7.6: (a) The bounding box depicted on user's transparency (b) The composed image

Moreover, the authors considered two situations of the shareholders. One of them is **Sharp Eyed user**. In this case, the shareholder are assumed to be having two abilities:

- The shareholder is able to detect the difference between the displayed image and the specific message m' that the adversary would like to display even a single pixel located in the bounding box. (e.g., the shareholder sees an incomprehensible image or considers the displayed image as the original one different from the m')
- The shareholder has the capability to notice the image having a pixel in which the number of black subpixels is not exactly two.

Therefore, the adversary has to change the pixels in the proper area of the transparency. If the width and height of bounding box are r' and c' respectively, there are $(r-r')(c-c')$ equally likely different sets of pixels to be reversed. Then if the adversary chooses the wrong set of pixels, she failed. The probability of success is therefore at most $\frac{1}{(r-r')(c-c')}$.

Another situation is a **not so Sharp Eyed** which is more useful for ordinary users. The authors assume that the shareholder has the capability to detect differences of t pixels or more between the displayed message and the image with the m' in the correct bounding box (actually, t might depend on the m'). If the number of different pixels is at least t , then the adversary fails. Also, another type of attack can be detected if more than t' pixels has more than or less than two black subpixels. Based on the analysis and a series of Claims in section 3.2.2 of [16], the following theorem (Theorem 9 of [16]) is obtained.

Theorem 7.4. *Let r be the number of rows of the image, and let c be the number of columns. Let r' and c' be these values regarding the bounding box. Let m be the message and let m' be a semantically different message. Assume that the human recipient has the following capabilities: any image with hamming distance greater than t from m' is not captured by recipient as being m' , and recipient notices if more than t' pixels in the image displayed to him have more than or less than two black subpixels. Then, in authentication system we described the adversary can convince the user to identify the message as m' with probability at most $\frac{4(t+t')}{(r-r')(c-c')}$.*

In the previous paragraphs, we discussed the properties of “Position on the screen” method. Obviously, the method is one-time pad which means it is only for single authentication because the location of the bounding box is previously known by the shareholders. In order to make the method secure for several authentications, a straightforward approach is constructed. They store the several copies of the previous method in different areas of a single transparency, where each copy depend on the security parameters which define the size of the area that is used by each copy, and on the size of the transparency.

Following the construction, the authors define the many-times security and demonstrate how to construct an efficient many-times authentication from the “Position on screen” method. We will first review the definition of many-times security.

Definition 7.5. (*n-times security*) *A visual authentication system is n-times(1 - p)-single-transformation-secure(n-times(1 - p)-sts) if the following is true for any n messages $\langle m_1, m_2, \dots, m_n \rangle$. For any message $m_i (1 \leq i \leq n)$ communicated from S to H , and any message m' different from m_i , the probability that H outputs $\langle ACCEPT, m' \rangle$ is at most p . If P is faithful then H should always output $\langle ACCEPT, m \rangle$.*

The settings are established as follows. Let the message that should be authenticated be of size $r' \times c'$ pixels. The parameters r_0, c_0 are the security parameters. Let the size of transparency be $r \times c$, where $r = r_0 + n_r r'$ and $c = c_0 + n_c c'$. The transparency is used for $n = n_r n_c$ authentications. The Figure 7.7 illustrates the process of the many-times authentications.

In the initialization phase, A random start point (i_0, j_0) is chosen where $1 \leq i_0 \leq r_0$, $1 \leq j_0 \leq c_0$. A grid of $n_r n_c$ areas which are composed of $r' c'$ pixels, is drawn starting from the location (i_0, j_0) . The i -th area is defined as the area in the intersection of row $\lceil i/n_c \rceil$ and column $(i \bmod n_c) + 1$. Thus, the i -th authentication is easily implement

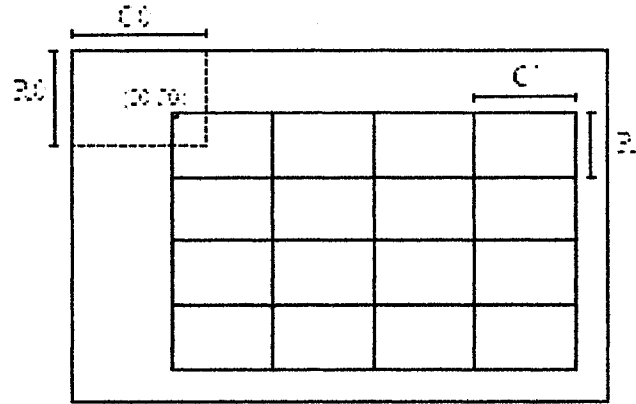


Figure 7.7: Many-times visual authentication scheme

in terms of the previous description. When the dealer sends her share of the message m_i in the i -th area of the grid, and in other pixels on the transparency have and only have two black subpixels, the recipient would verify that the message after stacking his share on the i -th area.

Moreover, the authors also figure out the probability of being attack in the case of many-times authentications (Theorem 12 of [16]).

Theorem 7.6. *Assume that if the hamming distance between the displayed image and an image m' is greater than t then the human recipient does not perceive the displayed image as m' . Also assume that the user notices if in more than t' pixels the number of black subpixels is not two. Then a transparency of size $(r_0 + n_r r') \times (c_0 + n_c c')$ pixels can be used to get an $n_r n_c$ -times $(1-p)$ -single-transformation-secure visual authentication system, where each message is of size $r' \times c'$ pixels, and where $p = \frac{4(t+t')}{r_0 c_0}$.*

In this paper, we will propose our method to reduce the possibility of attacks. Also, we will make use of the basic idea of this authentication method to improve the security of visual cryptography when facing the cheating shares created by traitors. Furthermore, a modification will be made in the proposed method which is not only better for preventing the cheating shares but also applicable to visual authentication scheme.

7.2.2 The Proposed Method for Visual Authentication Scheme

In “Position on Screen” method, the usage of bounding box has an effect on preventing the attack by the traitor. When the traitor receives the share from the dealer and then implements the attack, the changes alternated outside the bounding box will make no sense to the recognition of original image by honest shareholder. It is obvious that only the low-level attack can be obtained. In addition, as we mentioned in the previous section, the random position of bounding box can also reduce the possibility of being attacked by traitors.

As a matter of fact, there exist some differences between the visual cryptography and visual authentication schemes. The main difference is that the position can not be previously known by the shareholder who might become the traitor. Otherwise, the existence of bounding box is out of use because the traitor can change the original image without difficulty. Therefore, the difference cause the “Position on screen” method not completely applicable to the visual cryptography and we have to modify it to satisfy the our scheme.

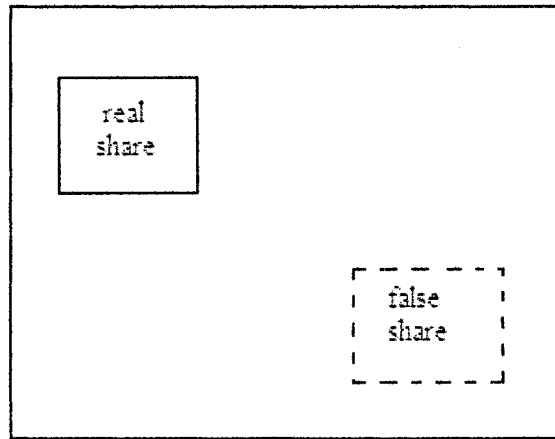


Figure 7.8: Success Attack with false share

In our proposed method, the location of share on the transparency is random every time and more importantly it should be hidden to the shareholders. However, we have to note that the visual cryptography will go through a successful attack under this condition. Although the traitors did not know the location of the share, he can make a similar share and put it on an appropriate position. Then after overlaying the transparencies, two resulting shares will be shown on the superimposed transparencies. Obviously, the traitor definitely knows the real secret image but the honest shareholder cannot differentiate it(Figure 7.8). In terms of the definition we described before, we consider this type of attack as the successful attack. In fact, this attack is not only the reason why we make the position of share random on the transparency to enlarge the possibility of the intersection between the real and false shares, but also the reason why we modify the method to be applicable for the 2-out-of-2 visual cryptography scheme(We will explain it later).

Although the proposed method we present is possibly attacked by the successful attack, it is good enough for the visual authentication scheme in smart card system. Generally, we assume that if the consumer sees both true and false shares on his transparency in the transaction, he will refuse to make the payment and ask the merchant to show the price again. Due to the random position of the share every time, the merchant cannot deduce the position and implement the completely successful attack.

However, in many-times authentications, the merchant is able to deduce the position of the i -th authentication based on the previous transactions.

Therefore, our method outweighs the previous authentication method. Next we will compare these two methods at length.

7.2.3 Comparison

Now, we will compute the possibilities of being attacked by traitors and demonstrate our proposed method is better than many-times "Position on screen" method of visual authentication scheme.

Although many-times method has made a great progress compared to the one-time method, the probability that the adversary implements a successful attack is larger than that of our method. Following from Figure 7.7 and Theorem 7, this probability is $\frac{4(t+t')}{r_0c_0}$ and we can figure out the probability of our method given the same conditions.

The start points of bounding boxes are defined as (i_0, j_0) and they are chosen from the area of $r_0 \times c_0$ as Figure 7.7 illustrated. For our method, due to the unknown position of the share on transparency, the traitors need to guess it every time. Consequently, every left upper point of bounding box is the possible start point and the start points are chosen from the area with the size of $(r - r') \times (c - c')$. Then the probability of being attacked successfully in our method is $\frac{4(t+t')}{(r-r') \times (c-c')}$.

Next, we will discuss about the relationship between r_0c_0 and $(r - r')(c - c')$. Given a fixed size of transparency, if the r_0c_0 is set to be larger, the corresponding times of authentications will be reduced because they are satisfied the equations $r = r_0 + n_r r'$ and $c = c_0 + n_c c'$. When $r - r' = r_0$ and $c - c' = c_0$, only one authentication can be carried out (where $n_r = 1, n_c = 1$). Therefore, r_0c_0 is much smaller than $(r - r')(c - c')$ and hence the probability that traitors implement the successful attack in our method is much smaller than that of visual authentication scheme.

Furthermore, it is easy to find out that this probability of our method is the same as that of the one-time "Position on screen" method for preventing the attack. However, in the "Position on screen" method, if the consumer is careless and the marked position of her share is noticed by cheating merchant, then the cheating merchant can implement the completely successful attack on the right position. For example, in the smart card system mentioned in [16], the cheater can ask the consumer to pay the amount of money more than the real price because he has the capability of carrying out the completely attack. Supposed that the cheater who is responsible not only for communicating with the bank but also displaying the amount of money should be paid by consumer plays a role as merchant. She can tell the consumer that he has to pay her \$1 but demands \$10 from the smart card. She will know that the information that the smart card will send to consumer contains \$10 and thus when she gets the share that the smart card asks her to display she can deduce the content of the transparency. Then she can alternate the image which will result in the message containing \$1. Also, the consumer cannot be aware of the cheating behavior. Then the cheater can obtain the authentication from consumer and meanwhile modify the real price when

communicating with banks. This is the reason why the visual cryptography can not be directly used for authentication mentioned in [16]. However, in our method, the unmarked bounding box on the transparency is more securer because we do not have to worry about the cheating merchant peeks the position of the share on transparency.

As a whole, we can make a conclusion that for smart card system, our proposed method is better than the “Position on screen” method in visual authentication scheme because of the unknown position of share on the transparency that results in the small possibilities of being attacked.

7.3 Model

In fact, the main difference between the previous visual authentication method and our proposed method is whether the position of the share is previously known. In our case, if the location of the share on the transparency is known by shareholders in advance, the protection fails. Therefore, only the dealer who implements the encryption and distributes the shares can know the location of the share and after encryption, he will be out of the scheme. Based on this assumption, we will discuss about the security parameters and the relationship between the size of shares and transparencies. At first, we will set up a model for the following discussion.

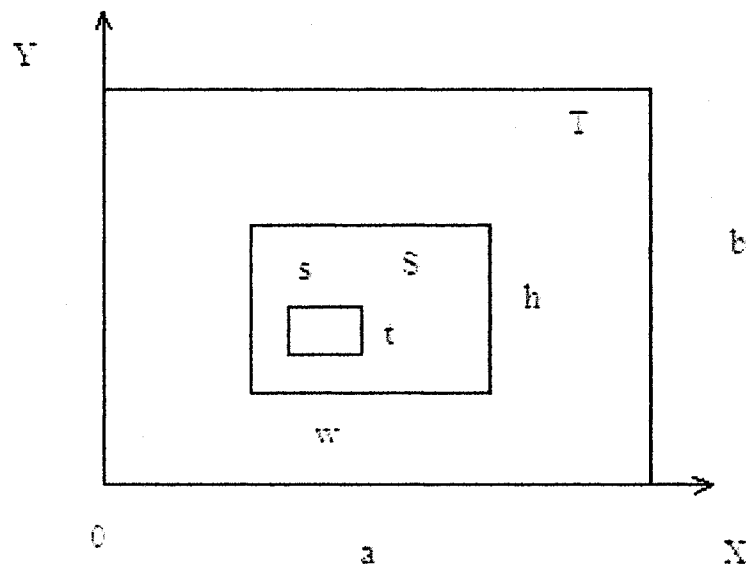


Figure 7.9: Model

We refer to all the elements in Figure 7.9 as follows. S is the symbol of the-middle-

size rectangle that represents the share. T is the symbol of the biggest rectangle that stands for the transparency. A is the symbol of changed area. Denote a, b by the width and height of T and denote w, h by the width and height of S . The width and height of A are s and t respectively. Let (U, V) be the central point of the S , then (U, V) is two-dimensional random vector having uniform distribution in T . Let (X, Y) be the central point of changed area and it satisfies the same condition of (U, V) .

In next section, different attacks will be described in terms of the model and some results relate to the security will be obtained.

7.4 Attacks with different levels

We have defined four-level attacks in section 7.1. Now, we are going to find the better proportion between the size of transparency and share to reduce the possibility of attacks.

7.4.1 Partially Successful Attack

For partial success, the shareholders and the traitors are aware of the change, but nobody can recognize the secret image. Here, we assume that if the changed area has the intersection, even a single pixel, with the share, then attack is partially successful.

Therefore, to calculate the possibility of the attack has been transformed to calculate the possibility of the intersection between the S and changed area. Then the following conditions should be satisfied:

$$\{(U, V, X, Y) : \frac{w}{2} < U < a - \frac{w}{2}, \frac{h}{2} < V < b - \frac{h}{2}, \quad (7.1)$$

$$\frac{s}{2} < X < a - \frac{s}{2}, \frac{t}{2} < Y < b - \frac{t}{2}, \quad (7.2)$$

$$\left\{ |U - X| < \frac{w + s}{2}, |Y - V| < \frac{h + t}{2} \right\} \quad (7.3)$$

This four-dimensional space can be computed by the following method: we first consider the s, t and their distribution, and then we can work out the possibilities of intersection between the share and the changed area if the distribution of s and t is known. The formula of computing the possibilities is listed as follows:

$$P(S \cap A \neq \emptyset) = \int_0^a \int_0^b P(S \cap A \neq \emptyset | s, t) f(s, t) ds dt \quad (7.4)$$

Where $f(s, t)$ is the probability density function of random variables (s, t) . As a matter of fact, the random variables s, t can be set to the different distributions. Now, in our

method, we consider the uniform distribution of s and t .

$$P(S \cap A \neq \emptyset | s, t) = \begin{cases} 1 & \text{if } s > a - w, t > b - h \\ 1 - \frac{(a-s-w)^2}{(a-w)(a-s)} & \text{if } s < a - w, t > b - h \\ 1 - \frac{(b-t-h)^2}{(b-h)(b-t)} & \text{if } s > a - w, t < b - h \\ (1 - \frac{(a-s-w)^2}{(a-w)(a-s)}) \times (1 - \frac{(b-t-h)^2}{(b-h)(b-t)}) & \text{if } s < a - w, t < b - h \end{cases} \quad (7.5)$$

Obviously, when $a > s + w$ and $b > h + t$, the smallest possibility of partially successful attack would be achieved. The value of $P(S \cap A \neq \emptyset | s, t)$ is applicable to the possibility formula in which $f(s, t) = \frac{1}{ab}$ satisfies the uniform distribution.

$$P(S \cap A \neq \emptyset) = \int_0^a \int_0^b P(S \cap A \neq \emptyset | s, t) f(s, t) ds dt \quad (7.6)$$

$$= \int_0^a \int_0^b (1 - \frac{(a-s-w)^2}{(a-w)(a-s)}) \cdot (1 - \frac{(b-t-h)^2}{(b-h)(b-t)}) \cdot \frac{1}{ab} ds dt \quad (7.7)$$

Now we will consider the specific case when the share is uniformly distributed on the transparency. To be a good traitor, everything he needs to do is magnify the possibility of the attack as large as he can. Therefore, he would try to find the best ways to implement the attack with full possibility.

Theorem 7.7. *If Share is uniformly distributed on the transparency, The best way to attack the share is also uniformly distributed.*

Proof: Following from the previous model, to find the distribution of the best attack, we have to figure out the possibility of the attack given the distribution of the central point (X, Y) of changed area. Then we get deduce the inequality which the central point satisfy.

$$\{(U, V, X, Y) : \frac{w}{2} < U < a - \frac{w}{2}, \frac{h}{2} < V < b - \frac{h}{2}, \quad (7.8)$$

$$|U - X| < \frac{w+s}{2}, |Y - V| < \frac{h+t}{2}\} \quad (7.9)$$

Suppose that the distribution of central point is uniform, then it satisfies the

$$A = \begin{cases} \frac{1}{(a-w)(b-h)} & a > w, b > h \\ 0 & \text{otherwise} \end{cases} \quad (7.10)$$

In fact, based on these conditions, we can list sixteen different cases when discussing about the relationships among them. For example, when $X - \frac{w+s}{2} \geq \frac{w}{2}$, $X + \frac{w+s}{2} \leq a - \frac{w}{2}$, $Y - \frac{h+t}{2} \geq \frac{h}{2}$, $Y + \frac{h+t}{2} \leq b - \frac{h}{2}$ are satisfied, the possibility $h(x, y)$ is computed as follows.

$$h(x, y) = \int_{X - \frac{w+s}{2}}^{X + \frac{w+s}{2}} \int_{Y - \frac{h+t}{2}}^{Y + \frac{h+t}{2}} A du dv = \frac{(w+s)(h+t)}{(a-w)(b-h)}$$

where $w \leq \frac{a-s}{2}$, $h \leq \frac{b-t}{2}$. Especially when $w = \frac{a-s}{2}$ and $h = \frac{b-t}{2}$, $h(x, y) = 1$.

Obviously, the central point (X, Y) that satisfies the uniform distribution is the best way of implementing the attack.

7.4.2 Completely Successful Attack

As the traitors, the goal is to implement the completely successful attack. In our method, we assume that if the changed area is included in the share, the attack will be considered as the complete success. Consequently, $s < w$, $t < h$ is predefined. we also define two parameters which depend on the requirement of the secret image : $\varepsilon(0 < \varepsilon < 1)$, security parameter and $\theta(0 < \theta < 1)$, the percentage of changeable area in shares.

According to the requirement of security, ε can be classified into three levels: low(0.1), medium(0.01) and high(0.001). Because different images and texts have distinct changeable area, then only the dealer can determine the size of changeable area for every secret visual information. Therefore, the θ is set up for the dealer. According to the previous description, the following conditions should be satisfied:

$$\{(U, V, X, Y) : s < w, t < h, |U - X| < \frac{w - s}{2}, |Y - V| < \frac{h - t}{2}, \quad (7.11)$$

$$\frac{s}{2} < X < a - \frac{s}{2}, \frac{t}{2} < Y < b - \frac{t}{2}, \quad (7.12)$$

$$\left. \frac{w}{2} < U < a - \frac{w}{2}, \frac{h}{2} < V < b - \frac{h}{2} \right\} \quad (7.13)$$

To reduce the possibility of attacks, the following possibility is chosen.

$$P(S \cap A \neq \emptyset) = \left(1 - \frac{a - w}{a - s}\right) \left(1 - \frac{b - h}{b - t}\right) \quad (7.14)$$

Now we will have an example given the specified security parameters. Suppose the security level is defined as medium ($\varepsilon = 0.01$), and the convertible area is $\frac{1}{9}$ (For example, $s = \frac{1}{3}w, t = \frac{1}{3}h$) of the share.

$$P(S \cap A \neq \emptyset) = \left(1 - \frac{a - w}{a - s}\right) \left(1 - \frac{b - h}{b - t}\right) \quad (7.15)$$

$$= \left(1 - \frac{a - w}{a - \frac{1}{3}w}\right) \left(1 - \frac{b - h}{b - \frac{1}{3}h}\right) < 0.01 \quad (7.16)$$

Then we can compute the results: $a > 7w, b > 7h$. According to this result, the dealer can design the size of the share and transparency. In fact, when processing different secret information, the dealer can work out this value depending on requirements of security parameters of the information. Then it is certain that he is able to reduce the attack possibility in terms of this value.

7.5 Visual Cryptography Scheme Application

7.5.1 Definition and Setting

As we mentioned before, our proposed method may go through the successful attack by using the false share in the visual cryptography scheme (Figure 7.8). For 2-out-of-2

visual cryptography scheme, the honest shareholder is unable to determine which share is real but the traitor can differentiate them. In order to prevent this kind of attacks, we will improve the proposed method as follows.

We previously used the 2-out-of-2 visual cryptography scheme defined by Naor and Shamir in which all four subpixels of a black pixel are black, whereas a white pixel has two or three black subpixels. Now we will modify the definition: a black pixel has four black subpixels, a white pixel has two black subpixels, and we define a pixel having three black subpixels as *grey*.

Following from the definition of visual cryptography, we add the grey pixels to our method more specifically. C_0 and C_1 are previously defined as the matrices of white and black pixels respectively. Let the matrices of grey pixels be denoted as C_2 . Then we list the C_0 , C_1 , C_2 of 2-out-of-2 visual cryptography scheme as follows.

$$C_0 = \left\{ \left\{ \begin{matrix} 0011 \\ 0011 \end{matrix} \right\} \left\{ \begin{matrix} 0101 \\ 0101 \end{matrix} \right\} \left\{ \begin{matrix} 1010 \\ 1010 \end{matrix} \right\} \left\{ \begin{matrix} 1100 \\ 1100 \end{matrix} \right\} \left\{ \begin{matrix} 1001 \\ 1001 \end{matrix} \right\} \left\{ \begin{matrix} 0110 \\ 0110 \end{matrix} \right\} \right\} \quad (7.17)$$

$$C_1 = \left\{ \left\{ \begin{matrix} 0110 \\ 1001 \end{matrix} \right\} \left\{ \begin{matrix} 0011 \\ 1100 \end{matrix} \right\} \left\{ \begin{matrix} 1010 \\ 0101 \end{matrix} \right\} \left\{ \begin{matrix} 1001 \\ 0110 \end{matrix} \right\} \left\{ \begin{matrix} 1100 \\ 0011 \end{matrix} \right\} \left\{ \begin{matrix} 0101 \\ 1010 \end{matrix} \right\} \right\} \quad (7.18)$$

$$C_2 = \left\{ \left\{ \begin{matrix} 0110 \\ 1010 \\ 0011 \\ 1010 \\ 1100 \\ 1010 \\ 1010 \\ 0011 \\ 0101 \\ 0011 \\ 1001 \\ 0011 \end{matrix} \right\} \left\{ \begin{matrix} 0110 \\ 0101 \\ 0011 \\ 0101 \\ 1100 \\ 0101 \\ 1010 \\ 1100 \\ 0101 \\ 1100 \\ 1001 \\ 1100 \end{matrix} \right\} \left\{ \begin{matrix} 0110 \\ 1100 \\ 0011 \\ 1001 \\ 1010 \\ 1010 \\ 1001 \\ 0101 \\ 1001 \\ 1001 \\ 1001 \\ 1010 \end{matrix} \right\} \left\{ \begin{matrix} 0110 \\ 0011 \\ 0110 \\ 0110 \\ 1100 \\ 0110 \\ 0110 \\ 0101 \\ 0110 \\ 1001 \\ 0101 \end{matrix} \right\} \right\} \quad (7.19)$$

Obviously, for a white pixel, there are 6 different permutations of matrices as well as for a black pixel. When the black(white) pixel is selected, the dealer can choose one of the options from $C_1(C_0)$. Also, there are 24 elements in the matrices of grey pixels and if the grey pixels is selected, the dealer will choose one of them from C_2 .

Next, we will discuss the changes among white, black, and grey pixels to verify that grey pixels have more advantages.

original color	possibly changed color	Method
white	black	switch the positions of the black and white subpixels
	grey	change the position of one black subpixel
black	white	switch the positions of the black and white subpixels
	grey	change the position of one black subpixel
grey	black	move a right black subpixel to a proper position
	white	move a right black subpixel to a proper position
	grey	move the black subpixels in all ways except above two

From the table, we find the fact that it is not difficult for traitor to change the pixel from black to white or grey as well as to change the pixel from white to black or grey. However, for changing the pixel from grey to white or black, it is hard to choose the right black subpixel and then move it to a proper position. Actually the traitor must know he will fail to change the grey color if he chooses the complement of his current subpixels arrangement and hence this case will not be considered by the traitor. After the movement of one subpixel, if the changed subpixels are arranged the same as the other share, it must be alternated to a white pixel and if the changed subpixels compose the complement of the other share, it must be alternated to a black pixel. Then we compare the possibility between changing the pixel from grey to white or black and keeping its original color. When the traitor change the pixel from grey to white or black, the possibility that the traitor perform a successful attack are only $\frac{1}{4}$, $\frac{1}{4}$ respectively and hence the possibility that the grey pixels do not change the color is $\frac{1}{2}$. (Figure 7.10). Apparently, it is more likely that the traitor cannot change grey pixel to other two colors.

7.5.2 Grey Background Method

In terms of the analysis and facts, we found that the grey pixels are more difficult to be changed than black and white pixels. Thus, we apply this property of grey pixels to our "Grey Background" method. First, the previously proposed method in which the share with black letters in white background is printed on the transparency randomly is also adopted. Additionally, in order to prevent the previous method from being attacked by the false share, the transparency except the real share are assumed to be composed of grey pixels(Figure 7.11).

Now we are going to demonstrate the advantages of the "Grey Background" method. As we described before, after the traitor finished a successful attack by a false share, the honest shareholder will be confused by differentiating a real share and a false share but the traitor will certainly know the real share. As a traitor, he is supposed to deduce an appropriate position of transparency and then alternate the color of some pixels in the area to display the content that he wishes. In fact, it is not difficult for the traitor to alternate pixels from white to black and vice versa in our previous method. Thus, the traitor can easily implemented this kind of successful attack.

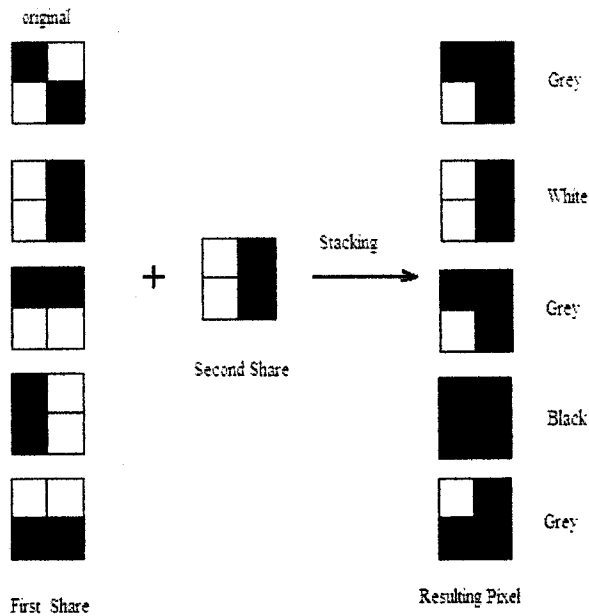


Figure 7.10: The attacks on the grey pixel

However, Due to the application of grey pixels in the “ Grey Background ” method, even if the traitor knows the background is grey, it is not easy for him to carry out an attack successfully. Note that we follow the assumption from the visual authentication scheme that the shareholder has sharp eyes so that he can identify the pixel that has more or less than two subpixels on the transparency. Accordingly, the honest shareholder will consider a pixel without having two subpixels as a invalid pixel.

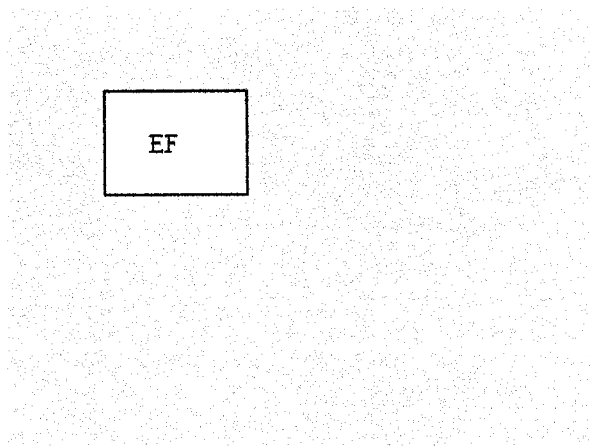


Figure 7.11: The improved method for Visual Cryptography Scheme

The assumption limits the traitor not only to consider how to change the pixel from

grey to the color that he wishes to display but also to consider how to balance each pixel to have two subpixels. For example, if he would like to change the grey pixels to the black ones which represent the content of the share as we defined, he can only obtain a quarter successful possibility for each pixel. Supposed that the content of the false share is composed of n black pixels, then the possibility that the traitor can display the content correctly is $(\frac{1}{4})^n$. By such a small possibility, it is obviously difficult for the traitor to implement an attack by use of the false share.

Although “Grey Background” method has been verified to be effective to prevent visual cryptography scheme from being attacked by traitors, there still exist some drawbacks. According to the definition of grey pixel for 2-out-of-2 visual cryptography scheme, it is obvious that the hamming distance between the grey pixels and white or black pixels is 1. So the main drawback of this method is that it reduces the contrast of the displayed image. Note that our method is designed for 2-out-of-2 visual cryptography scheme and actually it is more complex for the traitor to change the color of pixels in k out of n visual cryptography. We will discuss the attacks in the following section.

7.6 Attacks on k out of n visual cryptography schemes

In the previous sections, we focused on the 2 out of 2 visual cryptography to simplify the descriptions of our method. Actually, all the k out of n can be attacked by the traitors. Therefore, we would verify the fact and explain how to attack these visual cryptography schemes in details based on the constructions of Naor and Shamir’s schemes.

For 2 out of n visual cryptography, the only change we need to make is switching the positions of 1 and 0 in one row (share) of C_0 and C_1 respectively. Then after overlaying the shares, the white pixels are changed into black and the black pixels are changed into white.

In 3 out of 3 visual cryptography, each pixel is split into 4 subpixels (two white subpixels and two black subpixels) for each share. No matter what the pixel is white or black, if we switch the position of all the black and white subpixels in any one of the rows of C_0 or C_1 , the attack is also successfully carried out.

Similarly, if all the 1’s are changed into 0’s and all the 0’s are changed into 1’s in one of the rows of C_0 or C_1 , the 4 out of 4 visual cryptography can also be attacked by changing the black(white) pixels to the white(black).

Thus, for all the k out of k visual cryptography scheme, the Hamming weight of black pixels is one more than that of white pixels in the resulting image. It also can be seen from the matrices C_0 and C_1 that one of columns are all 0’s in C_0 and at least one 1 in each column of C_1 . Then after switching the equal and enough number of black and white subpixels in one of the rows of C_0 or C_1 , traitors can reverse the color of pixels. Note that this attack can be finished by only one traitor.

Moreover, the k out of n visual cryptography is more complicated than k out of k visual cryptography. For example, in 3 out of n visual cryptography scheme [17], let B be the black $n \times (n - 2)$ matrix which contains only 1’s, and let I be the identity

$n \times n$ matrix which contains 1's on the diagonal and 0's elsewhere. Let BI denote the $n \times (2n - 2)$ matrix obtained by concatenating B and I , and let $c(BI)$ be the Boolean complement of the matrix BI . Then

$C_0 = \{ \text{all the matrices obtained by permuting the columns of } c(BI) \}$

$C_1 = \{ \text{all the matrices obtained by permuting the columns of } BI \}$ has the properties: Any single share (row) contains an arbitrary collection of $n - 1$ black and $n - 1$ white subpixels; any pair of shares have n black subpixels composed of two individual black and $n - 2$ black subpixels; any stacked triplet of shares from C_0 has n black subpixels, whereas any stacked triplet of shares from C_1 has $n + 1$ black subpixels.

More specifically, one element of the C_0 and C_1 are

$$C_0 = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & 1 & \dots & 1 \\ 0 & 0 & \dots & 0 & 1 & 0 & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 1 & 1 & \dots & 0 \end{pmatrix}$$

$$C_1 = \begin{pmatrix} 1 & 1 & \dots & 1 & 1 & 0 & \dots & 0 \\ 1 & 1 & \dots & 1 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & \dots & 1 & 0 & 0 & \dots & 1 \end{pmatrix}$$

respectively.

From the above two matrices, it is clear that if the traitor would like to change the white pixel into the black, he can switch the positions between two black subpixels and two white subpixels. Then we can find Hamming weight of the stacked triplet of shares from C_0 has become $n + 1$. However, the change of the black pixel from C_1 is difficult for one traitor to make. To change the pixel from black to white, the traitor has to decide which 1 exists the specific column which has only a 1. The probability that the traitor can choose the right 1 is $\frac{1}{n-1}$. Thus, this attack by only one traitor is the event with low probability if n is large enough.

Now we consider the situation that two of shareholders are traitors. When these traitors contact with each other and pull together their shares, they can implement the attack by the following method. From one of matrices C_1 described above, two stacked shares cannot reveal any information because the black pixels cannot be distinguishable from the white ones. However, the traitor can detect the subpixels of their shares by computers. They will not change the subpixels if they find two subpixels are black in the same column, whereas if they find the color of two subpixels is different in the same column, they will switch the position between the black subpixel in one of these columns and the white subpixel in one of the other similar columns in one of the shares. Then the Hamming weight of the stacked shares is reduced to n and the black pixel is changed into white.

Although the change from black pixels to white is not easy for one traitor, it is not hard for two traitors to implement. Thus, in k out of n visual cryptography scheme, the method of changing the pixels from white to black is the same as the k out of k visual cryptography schemes. Furthermore, if any $k - 1$ or less shareholders become

traitors, the change of pixels from black to white is also easy. Here we are not going to analyze the different cases of k out of n visual cryptography schemes.

Based on the previous descriptions, the k out of n visual cryptography can be attacked if the shares are printed on the whole transparencies. In fact, in order to avoid distorting the aspect ratio of image and improve the contrast in 2-out-of-2 visual cryptography scheme, the number of subpixels had been changed from 2 to 4. Then the Hamming weight distance between black and white pixels is also changed from 1 to 2. However, for other k out of k visual cryptography schemes in [17], there is only one Hamming weight distance between the black and white pixels. Therefore, "Grey Background" method seems not applicable to these schemes. As a matter of fact, the contrast of resulting image has been improved by the researchers in the past[18, 5, 8, 3, 24]. According to the previous literatures regarding the contrast improvement, we are able to apply the "Grey Background" method in which although the contrast of visual cryptography scheme is reduced again by adding the definition of grey pixels, it guarantees the security of visual cryptography.

For example, in the original definition of 3-out-of-3 visual cryptography scheme, the black and white pixels are chosen from the following C_1 and C_0 .

$$C_0 = \left\{ \text{all the matrices obtained by permuting the columns of } \begin{pmatrix} 0011 \\ 0101 \\ 0110 \end{pmatrix} \right\}$$

$$C_1 = \left\{ \text{all the matrices obtained by permuting the columns of } \begin{pmatrix} 1100 \\ 1010 \\ 1001 \end{pmatrix} \right\}$$

Obviously, the superimposition of three transparencies from C_0 is 3/4 black, whereas the superimposition of three transparencies from C_1 is completely black. Therefore, the grey pixels can not be added because only one Hamming weight distance between the white and black pixels. We have to find another solution for the contrast of 3-out-of-3 visual cryptography scheme so that we are able to make use of the grey pixels to protect the visual cryptography from the attacks. In order to increase the Hamming weight distance between white and black pixels, we enlarge the size of subpixel expansion m to obtain a better contrast. Then the novel matrices of white (C_0) and black (C_1) pixels are defined as follows.

$$C_0 = \left\{ \text{all the matrices obtained by permuting the columns of } \begin{pmatrix} 0011 & 0011 \\ 0101 & 0101 \\ 0110 & 0110 \end{pmatrix} \right\}$$

$$C_1 = \left\{ \text{all the matrices obtained by permuting the columns of } \begin{pmatrix} 1100 & 1100 \\ 1010 & 1010 \\ 1001 & 1001 \end{pmatrix} \right\}$$

From the above definition, we can obtain the fact that the stack of three transparencies from C_0 is 6/8 black and the stack of three transparencies from C_1 is completely black. It is obvious that there exist two Hamming weight distances between white and black pixels. Therefore, we are able to apply the grey pixels having 7/8 black subpixels that can be distinguished from white and black pixels to 3-out-of-3 visual cryptography

scheme. Based on the previous analysis, it is difficult for traitors to change the color of grey pixels and the protection of visual cryptography by “Grey Background” method is available again.

In the case of the application of “Grey Background” method, the honest shareholders can discover some areas of the transparency have been changed with meaningless content which may be composed of black, white or grey pixels. Also, the similar attack and protection will take place in k out of n visual cryptography schemes because it is more complex for traitors to alternate the pixel from grey to other colors.

Chapter 8

Conclusion

Visual cryptography may not be as much of great practical importance as other research fields in cryptography although the idea of visual authentication schemes might be of practical value. However, visual cryptography is a hot topic for teaching purpose, and introducing the cryptographic ideas to a wide audience. Besides, it's a lot of fun [7]. Moreover, visual cryptography has been applied to practice [15, 13].

In this thesis, we described the secret sharing scheme which is the basic idea of visual cryptography firstly. Then we reviewed the previous literatures on visual cryptography from three different fields: Contrast improvement, colored visual cryptography and implementing visual cryptography by other methods. Among these fields, contrast improvement is the hottest topic and has caught a lot of attention from the researchers. It involves improving the quality of resulting images to makes them more recognizable. Another field is extending the black-and-white visual cryptography scheme to the colored one. Obviously, the colored visual cryptography scheme is more complicated. Thus, until now, the researchers still cannot find a good solution to carry out it. Moreover, the researchers try to find the novel ways which are different from the Naor and Shamir's for visual cryptography. In fact, a few approaches have been found but they also seem not good enough. Although we have made a progress on visual cryptography schemes, it still left a lot of problems that deserve further work.

However, in the previous literatures, none of them was concerned about the security of visual cryptography. The shareholders in their schemes are inherently assumed to be honest and hence they did not take the human cheating behavior into account. My thesis is the first paper which proposes the possible attack by the cheating shareholder called traitor (e.g. the traitor alternate the pixels of his own share and then damage the secret image).

To prevent this potential attack, we make advantage of the method in visual authentication scheme [16]. The "Position on screen" method in [16] provides the essential idea of our method. We also improve this method to make it applicable to visual cryptography scheme. Then we compare the possibilities of being attacked by traitors between these two methods and we find that our method is much better than many-times "Position on screen" method when considering the possibility of being attacked. Thus,

our method is also able to be applied to the visual authentication scheme to reduce the possibility of attacks. However, we found that the proposed method may go through a successful attack by using a false share in visual cryptography scheme. Then “Grey Background” method is put forward in which we add the definition of grey pixels and verify that the grey pixels can prevent such a successful attack effectively.

Furthermore, we establish a mathematical model to compute the possibility of attacks given different situations: Partial success and success. From the results of these mathematical analysis, some facts are also obtained and they are beneficial for our research.

For simplicity, we only make use of 2-out-of-2 visual cryptography to discuss our method at first. In section 7.6, we extend the discussion to k out of n scheme for more general cases.

In our method, there are some open questions left. In fact, we consider that if the 2-out-of-2 visual cryptography scheme is composed of the black and white pixels, it can probably be attacked by the traitor. We left this question to be demonstrated in the future research. Moreover, the contrast of displayed image is required to be improved.

References

- [1] A. Shamir, How to share a secret, *Communications of the ACM* 22 (1979), 612-613.
- [2] C.Blundo, A.D.Bonis and A.D.Santis, "Improved schemes for visual cryptography", in: *Designs, Codes, and Cryptography*, vol.24, pp.255-278(2001).
- [3] C. Blundo, A. D. Santis, D.R. Stinson, On the contrast in visual cryptography schemes, *J. Cryptology* 12 (4) (1999) 261-289.
- [4] C. N. Yang and C.S. Laih, "New colored visual secret sharing schemes, *Designs Codes and Cryptography*, Volume 20, Issue 3, pp.325-336, July, 2000
- [5] C.Blundo, P.D'Arco, A.D.Santis, and D.R.Stinson. Contrast Optimal Threshold Visual Cryptography Schemes, *SIAM J. on Discrete Math.* 16 (2003), 224-261
- [6] D.R.Stinson. *Cryptography: Theory and Practice, Second Edition*, CRC Press, Inc., Boca Raton, 2002, 339 pp.
- [7] D.R.Stinson, An introduction to visual cryptography, presented at Public Key Solution97, Toronto, Canada, April28-30,1997.
- [8] D.Q.Vie and K.Kurosawa. Almost ideal contrast visual cryptography with reversing, in: *Proc. of Topics in Cryptology—CT-RSA 2004, The Cryptographers' Track at the RSA Conference 2004, San Francisco, CA, USA, 23-27 February, 2004*, in: *Lecture Notes in Comput. Sci.*, vol. 2964, Springer, Berlin, 2004, pp. 353-365.
- [9] E.R.Verheul and H.C.A.Van Tilborg, Constructions and properties of k out of n visual secret sharing schemes, *Designs, Codes and Cryptography*, Vol. 11, No. 2 (1997) pp. 179-196.
- [10] G.J.Simmons, How to (really) share a secret, in "Advances in Cryptology – CRYPTO '88", S. Goldwasser, ed., *Lecture Notes in Computer Science* 403 (1989), 390-448.
- [11] G.J.Simmons, An introduction to shared secret and/or shared control schemes and their application, in "Contemporary Cryptology, The Science of Information Integrity", G. J. Simmons, ed., IEEE Press, 1992, 441-497.

- [12] G.R.Blakley, Safeguarding cryptographic keys, AFIPS Conference Proceedings 48 (1979), 313-317.
- [13] H.Yamamoto, Y.Hayasaki, and N.Nishida. Securing Information display by use of visual cryptography. OPTICS LETTERS, Vol. 28, No. 17, September 1, 2003
- [14] Biehl.I and Wetzel.S, Traceable Visual Cryptography. Proceedings of the First International Conference on Information and Communication Security (ICICS'97), LNCS 1334, Springer, 1997.
- [15] L.W.Hawkes, A.Yasinsac, C.Cline. An application of Visual Cryptography to Financial Document. Available website: <http://www.cs.fsu.edu/research/reports/TR-001001.pdf>
- [16] M.Naor, B.Pinkas. Visual Authentication and Identification, CRYPTO97. 1997.
- [17] M.Naor and A.Shamir, Visual Cryptography, Eurocrypt'94, Springer-Verlag LNCS Vol.950.Springer-Verlag,1995,1-12.
- [18] M.Naor and A.Shamir, Visual Cryptography II: Improving the Contrast Via the Cover Base, Security in Communication Networks, September 16-17. 1996.
- [19] P.Busse, Visual Encryptor, Available website: <http://compsci.snc.edu/cs460-archive/2003/busspr/index.html>
- [20] P.Tuyls, H.D.L.Hollmann, J.H.v.Lint, L.Tolhuizen A polarisation based Visual Crypto System and its Secret Sharing Schemes. available website <http://eprint.iacr.org/2002/194.ps>
- [21] S.P.Shieh and H.M.Sun, On constructing secret sharing schemes, in "Infocom '94 Proceedings", IEEE Press, 1994, 1288-1292.
- [22] S.S.Lee, J.C.Na, S.W.Sohn, C.Park, D.H.Seo, and S.J.Kim, Visual Cryptography Based on an Interferometric Encryption Technique. ETRI Journal, vol.24, no.5, Oct. 2002, pp.373-380.
- [23] S.Cimato, R.D.Prisco, A.D.Santis. Optimal Colored Threshold Visual Cryptography Schemes. Des. Codes Cryptography 35(3): 311-335 (2005)
- [24] T.Hofmeister, M.Krause, H.U.Simon, Contrast-optimal k out of n secret sharing schemes in visual cryptography, Theoretical Computer Science, v.240 n.2, p.471-485, June 17, 2000
- [25] T.W.Yue, S.Chiang. A Neural Network Approach for Visual Cryptography. IJCNN (5) 2000: 494-502
- [26] Y.C.Hou, Visual cryptography for color images, Pattern Recognition 36(7)(2003)1619-129.

- [27] Y.C.Hou, C.Y.Chang, F.Lin, Visual Cryptography for color images based on color decomposition, Proceedings of the Fifth Conference on Information Management., Taipei, November 1999