



Run Run Shaw Library

香港城市大學  
City University of Hong Kong

### **Copyright Warning**

Use of this thesis/dissertation/project is for the purpose of private study or scholarly research only. ***Users must comply with the Copyright Ordinance.***

Anyone who consults this thesis/dissertation/project is understood to recognise that its copyright rests with its author and that no part of it may be reproduced without the author's prior written consent.

CITY UNIVERSITY OF HONG KONG  
香港城市大學

(Extended) Visual Cryptography Scheme  
for Color Images with No Pixel Expansion  
一種(擴充型)像素不擴展的  
彩色視覺密碼方案

Submitted to  
Department of Computer Science  
電腦科學系  
in Partial Fulfillment of the Requirements  
for the Degree of Master of Philosophy  
哲學碩士學位

by

Wu Xiaoyu  
吳曉宇

September 2010  
二零一零年九月

## Abstract

In 1994, Naor and Shamir introduced the notion of Visual Cryptography Scheme (VCS), which is the secret sharing of digitized images. A  $k$ -out-of- $n$  VCS splits an image into  $n$  secret shares which are indistinguishable from random noise. These shares are then printed on transparencies. From any  $k - 1$  or less shares, no information about the original image (other than the size of it) will be revealed. The image can only be recovered by superimposing  $k$  or more shares. This recovery process does not involve any computation. It makes use of the human vision system to perform the pixel-wise OR logical operation on the superimposed pixels of the shares. When the pixels are small enough and packed in high density, the human vision system will average out the colors of surrounding pixels and produce a smoothed mental image in a human's mind.

Early VCS schemes mainly focused on black-and-white secret images. If the original image is not black-and-white, for example, a gray-scale image, dithering is employed to preprocess the original image. However, this technique would degrade the image quality. Another issue that is common to most of the previous work is pixel expansion, which means that the size of each secret share is several times larger than that of the original image. Two important parameters which govern the quality of reconstructed images are  $m$  (pixel expansion rate which represents the loss in resolution from the original image to the shares) and  $\alpha$  (the relative difference in weight between the superimposed shares that come from one color level (e.g. black) and another color level (e.g. white)). For image integrity, a good VCS should make the value of  $m$  close to one (i.e. no pixel expansion) and  $\alpha$  as large as possible.

It is unknown if there is a scheme which satisfies all the following four commonly

desired properties: (1) supporting images of arbitrary number of colors; (2) no pixel expansion; (3) supporting  $k$ -out-of- $n$  threshold setting; and (4) a ‘tunable’ number of color levels in the secret share creation process. We answer this question affirmatively by proposing a  $k$ -out-of- $n$  threshold visual cryptography scheme which satisfies all these properties. In particular, our scheme utilizes a probabilistic technique for achieving no pixel expansion and generically converts any  $k$ -out-of- $n$  threshold visual cryptography scheme for black-and-white images into one that supports color images.

Furthermore, we propose an extension of our VCS called Extended Visual Cryptography Scheme (EVCS). In this EVCS, the  $n$  shares which are generated from the secret image also carry  $n$  meaningful and independently chosen images. To the best of our knowledge, our EVCS is the first scheme for color images that supports the general  $k$ -out-of- $n$  secret sharing while having no pixel expansion.



## Acknowledgements

First of all, I would like to express my gratitude to my supervisor Prof. Li Qing and co-supervisor Dr. Duncan S. Wong. I gratefully acknowledge Prof. Li for his constant support to my plans and ideas, which makes me more self-confident. His advice made me more open-minded and helped me broaden my horizon. My deepest gratitude also goes to Dr. Duncan S. Wong for his guidance and encouragement during my study and research in City University of Hong Kong. His kindness, patience and wisdom helped me overcome the obstacles in my research work. Thanks to their valuable comments, I have developed my own research methodology in design, implementing and summarizing.

My thanks also go to my former colleague Bert Leung, who shared with me his ideas on visual cryptography and helped me solve problems in my research. I am fortunate to work with such a talented friend. And I would like to give my thanks to the members of our cryptography group: Qiong Huang, Xiaokang Xiong, Roman Schlegel, Cora Chang, Chung Ki Li, Haimin Jin and Yuan Wang. Group studies and discussions helped me deeper understand the theories and applications of cryptography. I learned from them the latest ideas relating to cryptography and these ideas inspired me many new thoughts.

Last but not least, my thanks go to my beloved family and friend: my dear Mom, Dad and Amos Chan for their continuous consideration and support. Without their encouragement, I can not possibly achieve my work.

# Contents

<b>Abstract</b>	<b>i</b>
<b>Acknowledgements</b>	<b>iii</b>
<b>List of Tables</b>	<b>vi</b>
<b>List of Figures</b>	<b>vii</b>
<b>1 Introduction</b>	<b>1</b>
<b>2 Related Work</b>	<b>7</b>
2.1 VCS Schemes for Black-and-White Images . . . . .	7
2.1.1 Naor-Shamir Black-and-White VCS . . . . .	8
2.1.2 Other Black-and-White VCS Schemes . . . . .	9
2.2 VCS Schemes for Gray-scale Images . . . . .	10
2.2.1 Some Gray-Scale VCS Schemes . . . . .	10
2.2.2 Chen et al. Gray-Scale VCS with No Pixel Expansion . . . . .	12
2.3 VCS Schemes for Color Images . . . . .	13
2.3.1 Hou Colored VCS Schemes . . . . .	14
2.3.2 Yang-Chen Colored VCS . . . . .	18
2.3.3 Other Colored VCS Schemes . . . . .	20
2.4 Extended Visual Cryptography Schemes . . . . .	20
2.4.1 Ateniese et al. Black-and-White EVCS . . . . .	21
2.4.2 Other EVCS Schemes . . . . .	23
<b>3 A New <math>k</math>-out-of-<math>n</math> Colored VCS</b>	<b>24</b>

3.1	Preliminaries . . . . .	24
3.2	Our Scheme . . . . .	27
3.2.1	Histogram Generation . . . . .	27
3.2.2	Color Quality Determination . . . . .	28
3.2.3	Grouping . . . . .	29
3.2.4	Share Creation . . . . .	30
3.3	Security Analysis . . . . .	33
3.4	Summary . . . . .	35
<b>4</b>	<b>A New <math>k</math>-out-of-<math>n</math> Colored EVCS</b>	<b>38</b>
4.1	Our Scheme . . . . .	38
4.1.1	Histogram Generation . . . . .	39
4.1.2	Color Quality Determination . . . . .	39
4.1.3	Grouping . . . . .	40
4.1.4	Share Creation . . . . .	41
4.2	Example . . . . .	45
4.3	Security Analysis . . . . .	48
4.4	Summary . . . . .	53
<b>5</b>	<b>Determining the Number of Color Levels and Grouping Method</b>	<b>54</b>
5.1	Color Level Determination . . . . .	54
5.2	Grouping Method . . . . .	59
<b>6</b>	<b>Comparison</b>	<b>62</b>
6.1	VCS Schemes . . . . .	62
6.2	EVCS Schemes . . . . .	66
<b>7</b>	<b>Conclusion and Future Work</b>	<b>69</b>
	<b>List of Publications</b>	<b>71</b>
	<b>Bibliography</b>	<b>72</b>

# List of Tables

3.1	The chance of using $B^0$ or $B^1$ for individual group during Share Creation	32
3.2	The chance of using each column of $B^0$ or $B^1$ for individual group during Share Creation . . . . .	37
4.1	The chance of picking the columns of $B^0 \circ A^{c_1, c_2, c_3}$ or $B^1 \circ A^{c_1, c_2, c_3}$ with respect to $X$ during Share Creation ( $X \in \{R, G, B\}$ ). . . . .	50
6.1	Comparison of VCS schemes . . . . .	63
6.2	Comparison of EVCS schemes . . . . .	66

# List of Figures

1.1	The Original Dithered Black-and-White Lena Image . . . . .	4
1.2	Two Shares and Their Superimposed Image of Lena . . . . .	4
1.3	The Dithered Black-and-White Meaningful Images: Sailboat and Peppers	5
1.4	Two Shares and Their Superimposed Image . . . . .	5
2.1	The Six Arrays of Four Subpixels . . . . .	8
2.2	The Original Image of Text and The Superimposed Image . . . . .	9
2.3	Three Shares and Their Superimposed Image . . . . .	11
2.4	Scheme 1 of Hou Colored VCS Schemes . . . . .	15
2.5	Scheme 2 of Hou Colored VCS Schemes . . . . .	17
3.1	The Original Lena Image . . . . .	28
3.2	The RGB Component Images of Lena . . . . .	28
3.3	Histograms of the RGB Component Images . . . . .	29
3.4	Histograms Illustrating the $4 \times 4 \times 4$ Color Levels . . . . .	30
3.5	The Two Shares of the Original Lena Image . . . . .	33
3.6	The Superimposed Image of the Two Shares . . . . .	33
4.1	The Images of Mandrill, Sailboat, Peppers . . . . .	46
4.2	Histograms of the RGB Components of Mandrill . . . . .	46
4.3	Histograms of the RGB Components of Sailboat . . . . .	47
4.4	Histograms of the RGB Components of Peppers . . . . .	47
4.5	Histograms Illustrating the $4 \times 4 \times 4$ Groupings of Mandrill . . . . .	48

4.6	Histograms Illustrating the $4 \times 4 \times 4$ Groupings of Sailboat . . . . .	48
4.7	Histograms Illustrating the $4 \times 4 \times 4$ Groupings of Peppers . . . . .	49
4.8	Three Shares Corresponding to Mandrill, Sailboat and Peppers Images .	49
4.9	The Superimposed Images of the First and the Second Shares, the First and the Third Shares and the Second and the Third Shares . . . . .	51
4.10	The Superimposed Image of the Three Shares . . . . .	51
5.1	The Image of Mac Logo . . . . .	55
5.2	The Image of Text . . . . .	56
5.3	The Original Image of Alice . . . . .	57
5.4	The Reconstructed Images of Alice with $2 \times 2 \times 2$ , $4 \times 4 \times 4$ , $N \times N \times N$ Levels . . . . .	57
5.5	The Reconstructed Images of Lena with $2 \times 2 \times 2$ , $4 \times 4 \times 4$ , $N \times N \times N$ Levels . . . . .	57
5.6	The Original Image of F22-raptor . . . . .	58
5.7	The Reconstructed Images of F22-raptor with $2 \times 2 \times 2$ , $4 \times 4 \times 4$ , $N \times N \times N$ Levels . . . . .	58
5.8	The Original Image of Gray(21-level) . . . . .	59
5.9	The Reconstructed Images of Gray(21-level) with 4 and $N$ Levels . . .	59
5.10	The Two Shares Corresponding to Sailboat and Peppers. . . . .	59
5.11	The Superimposed Image of the Two Shares Corresponding to Sailboat and Peppers. . . . .	60
5.12	Histogram with $4 \times 4 \times 4$ by the Candidate Method . . . . .	61
6.1	The Image of Lena (Gray) . . . . .	65
6.2	The Superimposed Image of Lena (Gray) . . . . .	65

# Chapter 1

## Introduction

In the recent decades, it is undoubted that the widespread use of the Internet has changed the lifestyle of human being. On the one hand, people enjoy great convenience brought by the Internet in communication, business trade and other services. On the other hand, people face more insecure factors, e.g., worms and viruses, while surfing the Internet. Cryptography, which is the study and practice of hiding information, becomes a significant tool to maintain the security of the Internet.

Cryptography probably began in or around 2000 B.C. in Egypt. On the tombs of deceased kings, hieroglyphics, which are intentionally cryptic, were used to tell their life stories and achievements. Cryptography was once used to make the text more regal and important. Classic cryptography means only secret writing (converting a meaningful message into an incomprehensible one). There are two techniques most commonly used in the classic cryptography, i.e. transposition and substitution. Transposition means that the order of the plaintext is rearranged according to a specified rule (e.g. “cityuofhk” becomes “uckoyfht” in a simple rearrangement scheme). Substitution means that the

original letter or group of letters are replaced by other letter or group of letters (e.g. “cityuofhk” becomes “djuzvpgil” by replacing each letter with the one following it in alphabetical order). Classic ciphers were used historically in transporting secret messages, e.g. Caesar cipher (a type of substitution cipher), which was used by Julius Caesar to communicate with his generals. However, almost all types of classic ciphers are vulnerable to statistical analysis since they always reveal statistical information about the original message. Now people still use these classic ciphers, but mainly as puzzles.

The modern field of cryptography has been expanded to more topics, e.g., secret sharing schemes, authentication codes, identification schemes and key distribution. There are two classes of encryption algorithms for modern cryptography, i.e., symmetric-key cryptography and public-key cryptography. In symmetric-key cryptography, the sender and the receiver share the same key to encrypt or decrypt a message. This algorithm leads to the difficulty in key management since the number of keys grows quickly with the increase of the communication groups. Public-key cryptography can solve the problem of key management by providing a public key and a private key. The two keys are mathematically related, but without the secret information, no one can get one key from the other. Typically, the public key is freely distributed and used to encrypt a message, while the private key is kept secret and used to decrypt a message.

One of the topics of modern cryptography is secret sharing. Secret sharing [22] is a cryptographic technique which can improve the reliability and robustness of secure key management. Consider the following situation: if the only key that provides access to some important data is lost, then the data will become inaccessible. The problem can be resolved by dividing the key into pieces and then distributing them to different persons so that any pre-specified set of persons can recover the key jointly. Formally, in a  $k$ -out-



of- $n$  threshold secret sharing scheme, a dealer gives a secret to  $n$  players in such a way that any group of  $k$  (for threshold) or more players can jointly reconstruct the secret but no group of fewer than  $k$  players can. As an example, Shamir's scheme [29] is one of the first threshold secret sharing schemes.

Based on the idea of threshold secret sharing, in 1994, Naor and Shamir [27] introduced Visual Cryptography, which is the secret sharing of digitized images. It solves the problem of encrypting images in a secure way so that the decryption process can be done by a person purely using his/her visual system without any computation. A  $k$ -out-of- $n$  Visual Cryptography Scheme (VCS) splits an image into  $n$  secret shares which are then printed on transparencies. These shares when separated will reveal no information about the original image (other than the size of it). The image can only be recovered by superimposing  $k$  or more shares. This recovery process does not involve any computation. It makes use of the human vision system to perform the pixel-wise OR logical operation on the superimposed pixels of the shares. When the pixels are small enough and packed in high density, the human vision system will average out the colors of surrounding pixels and produce a smoothed mental image in a human's mind. Fig. 1.1 shows a dithered black-and-white Lena image. Fig. 1.2 shows the two secret shares which are created using Naor-Shamir 2-out-of-2 VCS, and the superimposed image of them. From any one of the shares, no information about the secret image is revealed. The secret image can be recovered only by superimposing the shares. Note the size of the shares and the reconstructed image is expanded by a factor of 4.

An extension of VCS called Extended Visual Cryptography Scheme (EVCS) was also introduced in [27]. In an EVCS, the  $n$  shares, which are generated from a secret image, also carry  $n$  meaningful and independently chosen images. To generate these



Figure 1.1: The Original Dithered Black-and-White Lena Image

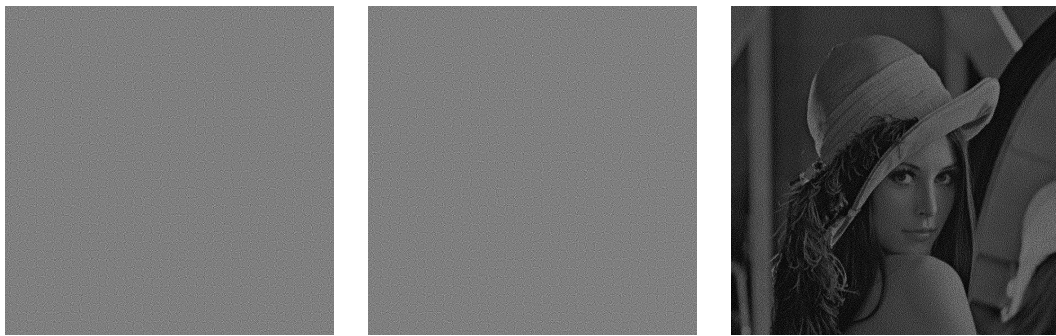


Figure 1.2: Two Shares and Their Superimposed Image of Lena

shares, a user arbitrarily chooses  $n$  meaningful images which have the same size as the secret image. Then the user splits the secret image and embeds the secret information into the  $n$  meaningful images in such a way that these  $n$  meaningful images are still visible. In addition, the threshold property is maintained, namely, given any  $k-1$  or less shares, no information about the secret image can be obtained, while given any  $k$  or more shares, the secret image will be revealed when the shares are superimposed. Fig. 1.3 shows two meaningful images (Sailboat and Peppers) which are to be used for embedding secret shares of Lena (Fig. 1.1). Fig. 1.4 are the two shares and the superimposed image by applying Ateniese et al.'s 2-out-of-2 EVCS scheme [3]. Each share carries a meaningful image. From any one of the shares, no information about the secret image is revealed. The secret image can be recovered only by superimposing the shares. Note the size of the shares and the reconstructed image is also expanded by a

factor of 4.

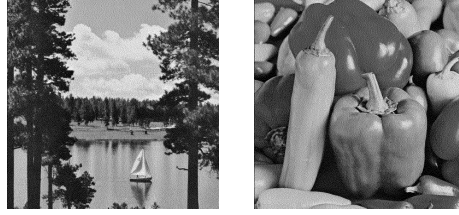


Figure 1.3: The Dithered Black-and-White Meaningful Images: Sailboat and Peppers

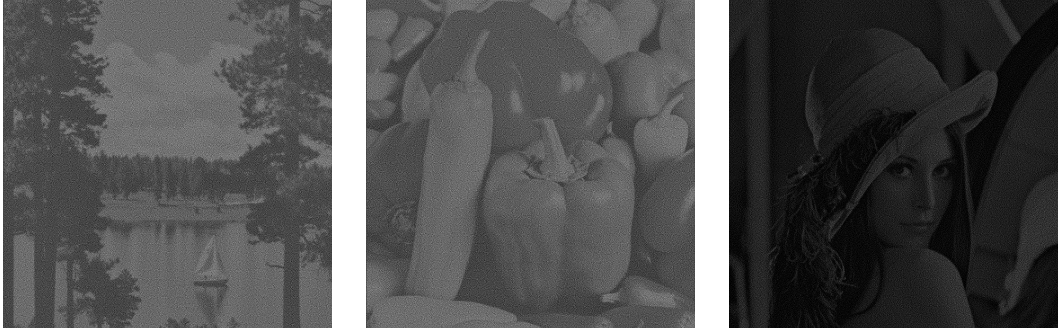


Figure 1.4: Two Shares and Their Superimposed Image

Early VCS and EVCS schemes [1, 3–9, 13, 14, 27, 28, 33, 34, 38] mainly focused on black-and-white or gray-scale secret images. Additionally, pixel expansion is common to most of the previous work. This means that the size of each secret share is several times larger than that of the original image and the resulting superimposed image is also several times larger than the original secret image.

In this thesis, we propose a new VCS scheme for color images and further extend it to an EVCS for color images as well. In our construction of VCS scheme, we generically transform any  $k$ -out-of- $n$  threshold VCS scheme for black-and-white images to color images. We utilize a probabilistic technique for achieving no pixel expansion. In addition, we allow the user to choose the number of color levels for each primary color

(i.e. Red, Green and Blue) that the reconstructed image could have. The reconstructed image refers to the image obtained by superimposing  $k$  or more share images. We find that this “tunable” feature is very useful (in practice), as the user is able to employ it for maximizing the quality of the reconstructed image, given that different types of images may better appear with different color levels (more details will be given in the later part of the paper). Our VCS scheme is the first scheme supporting the four desirable properties which are summarized as follows.

- 1) Supporting images of arbitrary number of colors;
- 2) No pixel expansion;
- 3) Supporting  $k$ -out-of- $n$  threshold setting;
- 4) Supporting a “tunable” number of color levels in the secret sharing process.

To extend our work, we also propose a new EVCS scheme which supports the four properties described above. Users of EVCS can also choose the number of color levels for the reconstructed and share images independently.

The rest of the thesis is organized as follows. In Chap. 2, we review some of the related results in VCS and EVCS. In Chap. 3 and Chap. 4, we propose new  $k$ -out-of- $n$  colored VCS and EVCS schemes respectively. Discussions on determining the number of color levels and grouping method are in Chap. 5. In Chap. 6, we provide quality comparisons between our schemes and other related schemes. Finally, we conclude our schemes in Chap. 7.

# Chapter 2

## Related Work

In this chapter, we briefly review the related work on black-and-white VCS schemes, colored VCS schemes and EVCS schemes. By reviewing these schemes, we find several commonly desirable properties which should be supported by VCS schemes.

### 2.1 VCS Schemes for Black-and-White Images

In this section, we firstly review Naor-Shamir black-and-white VCS [27]. They introduced the concept of VCS and proposed a general  $k$ -out-of- $n$  threshold VCS for black-and-white images. Their scheme acts as the building block of other VCS schemes. We also summarize the features of several other black-and-white VCS schemes proposed after Naor-shamir's and show their merits and demerits.

### 2.1.1 Naor-Shamir Black-and-White VCS

In [27], Naor and Shamir introduced Visual Cryptography. It solves the problem of encrypting written material (printed text, handwritten notes, etc.) in a secure way so that the decryption process only needs the human visual system without any computation. The written material only consists of black and white pixels. The original encryption problem can be considered as a 2-out-of-2 secret sharing. The solution of the 2-out-of-2 black-and-white VCS scheme can be either dividing one pixel in the original secret image into two subpixels or four subpixels in the two shares. In order not to distort the aspect ratio of the original image, in practice, we usually use four subpixels (two black subpixels and two white ones) arranged in a  $2 \times 2$  array in shares to represent one pixel in the secret image. So the size of the superimposed image is expanded by a factor of 4. Fig. 2.1 shows all the possible arrays of the four subpixels. They deal with the secret



Figure 2.1: The Six Arrays of Four Subpixels

image pixel by pixel. For a pixel in the secret image, they randomly choose an array from Fig. 2.1 as the first share. If the original pixel is white, the second share is identical with the first one; if the original pixel is black, the second share is complementary with the first one. When the two shares are superimposed, the white color is recovered as medium gray and the black is recovered as completely black. Fig. 2.2 shows the original image of text which only contains black and white pixels and the superimposed image.

They proposed several constructions in [27], where the generic one supports  $k$ -out-

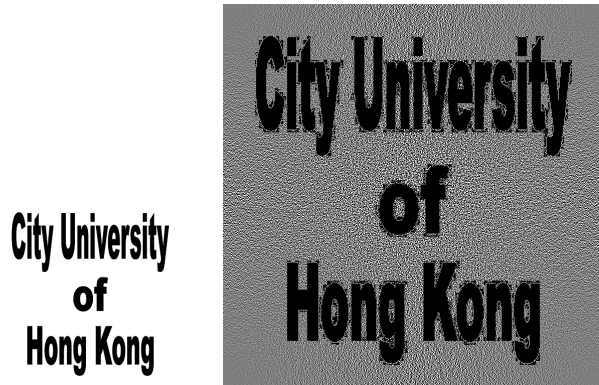


Figure 2.2: The Original Image of Text and The Superimposed Image

of- $n$  threshold setting for black-and-white images. These constructions are provably secure and the pixel expansion rate is getting larger when the values of  $k$  and  $n$  grow. Moreover, the scheme does not support images of arbitrary number of colors.

### 2.1.2 Other Black-and-White VCS Schemes

Since the introduction of VCS, there have been many other schemes proposed [1, 3–9, 13–15, 21, 28, 31, 33, 34, 38, 41]. In 2003, by removing the same column which appears in both Basic Matrices, Blundo et al. [7] proposed VCS schemes with optimal contrast. In [7], they improved the contrast of  $(n - 1)$ -out-of- $n$  (where  $n > 3$ ) and 3-out-of- $n$  schemes. They also conjectured that the  $k$ -out-of- $n$  scheme, where  $k=4$  or 5, had an optimal contrast. In 2004, Adhikari et al. [1] proposed a VCS which achieved a better result from the pixel expansion's point of view than [27]. They compared Naor-Shamir  $k$ -out-of- $n$  VCS scheme with the  $k$ -out-of- $n$  VCS scheme obtained from their method and showed that their pixel expansion was less in almost all cases. In [38], Yang proposed another one which achieved no pixel expansion by using the frequency of white pixels to show the contrast of the recovered image. Yang's scheme can be easily

implemented on the black-and-white VCS with pixel expansion. All the above schemes only support black-and-white images.

## 2.2 VCS Schemes for Gray-scale Images

Due to the limitation on applicability of the black-and-white VCS schemes, in 1997, Verheul and van Tilborg [35] proposed the  $k$ -out-of- $n$  VCS for gray-scale images. In this section, we give a review on their scheme and also raise several problems about it. Several VCS schemes for gray-scale images were proposed to resolve these problems, e.g., [10, 11, 20]. In the following, we further discuss these schemes.

### 2.2.1 Some Gray-Scale VCS Schemes

In 1997, Verheul and van Tilborg [35] introduced a general method for  $k$ -out-of- $n$  VCS for gray-scale images. For an image of  $c$  gray levels,  $c$   $n \times q$  matrices are constructed to represent the secret sharing process for each gray level. The elements of these matrices are in  $\{0, 1, \dots, c-1\}$ . And they use  $i$  ( $i \in \{0, 1, \dots, c-1\}$ ) to represent the gray level. The superimposed color is  $i$  if all the corresponding subpixels of all shares are  $i$ , otherwise, the superimposed color is black. To encrypt a pixel with the gray level  $i$  (where  $0 \leq i \leq c-1$ ), they choose the matrix which represents the gray level  $i$ . The  $n$  rows of the matrix correspond to the  $n$  shares and the  $q$  columns correspond to the gray levels of the  $q$  subpixels of each share. In this scheme, the pixel expansion rate has to be at least  $c^{(k-1)}$ . As an example, below are the three matrices of a 3-out-of-3 scheme for a



3 gray-level (namely, 0, 1, 2) image.

$$B^0 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 \end{bmatrix}$$

$$B^1 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 2 & 0 & 1 & 0 & 1 & 2 & 1 & 2 & 0 \end{bmatrix}$$

$$B^2 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 1 & 2 & 0 & 2 & 0 & 1 & 0 & 1 & 2 \end{bmatrix}$$

Fig. 2.3 shows the three shares and the superimposed image of them by using Verheul and van Tilborg's 3-out-of-3 VCS when the gray level of the original pixel is 1.

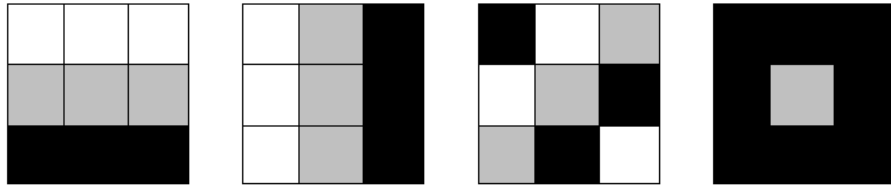


Figure 2.3: Three Shares and Their Superimposed Image

Lin and Tsai [20] proposed another VCS scheme for gray-scale images by applying dithering techniques in 2003. The gray-scale image is first converted into a binary image with the same size by dithering and then Naor-Shamir's VCS for black-and-white images is employed. This scheme improved the pixel expansion of Verheul and van Tilborg's VCS so that the pixel expansion rate is the same as Naor-Shamir's black-and-white VCS. Furthermore, only two collections of matrices are needed for any number of

gray levels. In 2004, a gray-scale VCS without pixel expansion was proposed by Chan et al. [10]. The scheme needs preprocessing by dithering and adjusting the gray level of the original image. The general  $k$ -out-of- $n$  threshold setting is not supported.

### 2.2.2 Chen et al. Gray-Scale VCS with No Pixel Expansion

In 2007, Chen et al. [11] extended the results of [38] to gray-scale images and proposed a gray-scale VCS. Chen et al.'s VCS maps a block in a secret image to one corresponding equal-sized block in each share image without image size expansion. For a secret block, this method generates the corresponding share blocks containing multiple levels rather than two levels based on the density of black pixels on the block. It uses two types of techniques, namely, histogram width-equalization and histogram depth-equalization. Chen et al.'s VCS scheme can reach the goal of no pixel expansion. However, their scheme does not support colored images and only supports  $k$ -out-of- $k$  threshold setting. Besides, before secret sharing, it needs to do preprocessing on the original images (block averaging). The details of the algorithm will be described in the following.

In the  $k$ -out-of- $k$  scheme where each secret block contains  $s$  pixels, the algorithm *BASIS MATRIX*( $k, s, l$ ) is designed to randomly generate a Boolean Basis Matrix for a secret block. Here,  $s$  is the block size and  $l$  ( $0 \leq l \leq s/2$ ) is the gray-scale intensity level.

Algorithm: *BASIS MATRIX*( $k, s, l$ )

1. Randomly select  $s/2 + l$  positions  $p_1, p_2, \dots, p_{s/2+l}$  from the  $s$  positions.
2. For  $i = 1$  to  $k-1$ , randomly select  $s/2$  positions from  $p_1, p_2, \dots, p_{s/2+l}$ ; Let  $R_i$  be

a variable consisting of  $s$  bits and set the bits located at the  $s/2$  selected positions in  $R_i$  as 1-bits and others as 0-bits.

**3.**  $R = R_1$  or  $R_i$  or  $\dots$  or  $R_{k-1}$ ;

**4.** Let  $p'_1, p'_2, \dots, p'_h$  be the positions of all the 0-bits which are located at positions  $p_1, p_2, \dots, p_{s/2+l}$  in  $R$ .

**5.** Set the bits located at  $p'_1, p'_2, \dots, p'_h$  of  $R_k$  as 1-bits; Set the  $s/2$ -h bits by randomly selecting from the bits located at  $p_1, p_2, \dots, p_{s/2+l}$  from  $R_k$ , except the positions  $p'_1, p'_2, \dots, p'_h$ , as 1-bits, and set the other bits as 0-bits. Regard each member of  $R_1, R_2, \dots, R_k$  as one row of the basic matrix.

This algorithm adopts block-to-block mapping as a key measure in its implementation. It makes significant progress in the aspect of pixel expansion since it is the first scheme which achieves no pixel expansion. However, the authors did not provide a general solution for the  $k$ -out-of- $n$  scheme. And there was no solution for colored images in their scheme as well. Besides, it needs to preprocess the original image before doing secret sharing (block averaging). This process reduces the quality of reconstructed image.

## 2.3 VCS Schemes for Color Images

The requirement of encrypting natural image makes researchers focus on the VCS schemes for color images. In [16], Hou firstly proposed three methods for encrypting color images. In this section, we describe Hou's scheme in detail and review Yang-Chen colored VCS [40] for its no pixel expansion property. Moreover, we discuss some other colored

VCS schemes proposed recently to show the development of colored VCS.

### 2.3.1 Hou Colored VCS Schemes

For color VCS schemes, [2, 12, 16–18, 23–25, 30, 37, 39, 40], Hou’s schemes [16] are believed to be the first set of color VCS schemes. In his paper, he proposed three methods for gray-scale and color images based on the previous studies in black-and-white visual cryptography, halftone technology, and color decomposition method. His methods have the backward compatibility with the previous results in black-and-white visual cryptography and can be easily applied to gray-scale and color images. Subtractive model is used in all the methods.

**Hou’s Method 1:** The first method produces four shares, namely *black mask*, *C* share, *M* share and *Y* share. By superimposing these shares, it shows the best reconstructed quality among Hou’s three methods. In the following, this method is described step by step.

**Step 1.** The original colored image is firstly be decomposed into three primary-color images under the subtractive model, namely, *C* (Cyan), *M* (Magenta) and *Y* (Yellow). The size of the three images is equal to that of the original one.

**Step 2.** Then each primary-color image is dithered so that each image will have two color levels. Dithering is a technique used to create an illusion of color depth in images with limited color palette. The principle is to pack pixels in higher density for representing darker colors and distribute the pixels sparsely for representing lighter colors. As a result, the superimposed image has 1-bit depth for each of the three primary-

color images. In other words, it has 3-bit depth.

**Step 3.** A *black mask* with double size of width and height of the original secret image is randomly generated in this step. Each pixel is mapped to a  $2 \times 2$  block which consists of two black pixels and two white pixels. Since the *black mask* is randomly generated, for each block, there are six possible patterns in total.

**Step 4.** Three other shares are generated at last. To generate the  $C$ ,  $Y$  and  $M$  shares, the dithered  $C$ ,  $M$  and  $Y$  primary-color images of the original secret image are scanned pixel by pixel. We use 0 and 1 to represent the two conditions of a primary color. 0 represents absence of the primary color while 1 represents the opposite condition. Fig. 2.4 summarizes this method by giving an example in which a random block of the black mask is chosen and shown in the first column. The second column shows the eight possible combinations of the original (dithered)  $C$ ,  $M$ ,  $Y$  pixel values. The following three columns show the encoding of the blocks in the corresponding shares of  $C$ ,  $M$ ,  $Y$ . The last column illustrates the superimposed image of  $C$ ,  $M$ ,  $Y$  shares with the *black mask*.


































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 2.4: Scheme 1 of Hou Colored VCS Schemes

**Hou's Method 2:** The second method expands every pixel of a halftone image into a  $2 \times 2$  block on two sharing images and fills the block with cyan, magenta, yellow and transparent, respectively. Using these four colors, two stacked images can generate various colors through different permutations. The details of this method are described in the following.

**Step 1.** Transform the color image into three halftone images:  $C$ ,  $M$ , and  $Y$ .

**Step 2.** For each pixel of the secret image, a  $2 \times 2$  block, which is randomly filled with cyan, magenta, yellow, and transparent, is chosen as Share 1. According to the values of  $C$ ,  $M$ ,  $Y$  and Share 1, they generate a  $2 \times 2$  block as Share 2. The block in Share 2 is the permutation of the four colors of the block in Share 1. Fig. 2.5 shows the color distribution of the block in Share 2 when the block in Share 1 is chosen. Repeat this step until every pixel of the decomposed image is dealt with. Hence, two visual cryptography transparencies to share the secret image are obtained.

**Hou's Method 3:** This method needs 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 generates 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  $2 \times 2$  block. The method then combines  $C_1$ ,  $M_1$ , and  $Y_1$  to form a colored halftone Share 1 and  $C_2$ ,  $M_2$ , and  $Y_2$  to form Share 2. This method is described step by step in the following.

**Step 1.** Transform the color image into three halftone images:  $C$ ,  $M$ , and  $Y$ .

**Step 2.** For each pixel of the decomposed image, do the following: according to the traditional method of black-and-white visual cryptography, expand  $C$ ,  $M$ , and  $Y$  into

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 2.5: Scheme 2 of Hou Colored VCS Schemes

six  $2 \times 2$  blocks,  $C_1$ ,  $C_2$ ,  $M_1$ ,  $M_2$  and  $Y_1$ ,  $Y_2$ .

**Step 3.** Combine the blocks of  $C_1$ ,  $M_1$  and  $Y_1$  and fill the combined block corresponding to pixels in Share 1. Combine the blocks  $C_2$ ,  $M_2$  and  $Y_2$  and fill the combined block corresponding to pixels in Share 2. Repeat this step until every pixel of the decomposed image is handled. Hence, two visual cryptography transparencies to share the secret image are obtained.

Hou's three methods for encrypting colored images are considered to be the first colored schemes. Since Hou did not provide any security analysis on these methods, we can not guarantee the security of them. The first method has been proved to be insecure recently by Leung et al. [19]. The second one is secure, whereas the quality

of reconstructed image is not satisfying. The third one is considered to be secure with better quality of reconstructed image.

However, the three methods have several common drawbacks. First, the pixel expansion rates of these methods are all 4 which makes the reconstructed image four times larger than the original one. Second, they have limitation on the color levels of original images, so dithering is needed before secret sharing. Third, no general  $k$ -out-of- $n$  solution was proposed, since the first method is for 4-out-of-4 and the last two are for 2-out-of-2. Finally, no security analysis for these methods was provided

### 2.3.2 Yang-Chen Colored VCS

In all the previous methods, a secret pixel is represented by several color subpixels and the number of these subpixels is referred to as the pixel expansion. Generally, they require a larger pixel expansion to produce more colors. In [40], Yang and Chen use additive color mixing in a probabilistic way so that the pixel expansion is fixed on 3 regardless of the number of colors in the reconstructed images. They use the appearance frequencies of  $R$ ,  $G$  and  $B$  to simulate a secret color. The drawback of the scheme is that to improve the color contrast of the reconstructed images, the only way is to modify the original images. The details of the scheme are discussed in the following.

A secret pixel is divided into three colored subpixels ( $R$ ,  $G$ ,  $B$ ) where the first  $R$ -colored subpixel has the appearance probability  $p_R^i$ , i.e., this subpixel may be  $R$  color with probability  $p_R^i$  and null color with probability  $(1 - p_R^i)$ . Accordingly, the other two subpixels ( $G$ -color and  $B$ -color) have the appearance probabilities  $p_G^j$  and  $p_B^k$ , respectively.



**Step 1.** Calculate  $L_R$ ,  $L_G$  and  $L_B$  which represent the number of colors on the three primary colors of the original image respectively.

**Step 2.** Construct the primary color sets:  $C_R^i$  (R-colored sets),  $C_G^j$  (G-colored sets) and  $C_B^k$  (B-colored sets). Suppose the basic matrices of black-and-white scheme are  $n \times l$  boolean matrices, then the primary color sets are  $n \times l \cdot L_X$  matrices ( $X \in R, G, B$ ).

$$C_R^{(255 \times r)/(L_R-1)} = \underbrace{C_W \cup \dots \cup C_W}_{L_R-1-r} \cup \underbrace{C_B \cup \dots \cup C_B}_r \xrightarrow{1 \rightarrow R; 0 \rightarrow N}$$

$r \in [0, L_R-1]$  and  $L_R$  is the number of colors on the primary color red. And  $C_W$  and  $C_B$  are the basic matrices of black-and-white scheme. The constructions of  $C_G^j$  (G-colored sets) and  $C_B^k$  are similar with  $C_R^i$ .

**Step 3.** Scan each pixel of the original image and apply the corresponding matrices in Step 2 by randomly choosing a column of each of the three *Basis Matrices*. Consider this column as an  $n$ -bit vector. For the first bit, assign the corresponding pixel black color (i.e. 0 color intensity) if the bit is 1, otherwise we assign it  $X$  ( $X \in \{R, G, B\}$ ) color (i.e. 255 color intensity). Continue this process until the corresponding color in each of the  $n$  shares is assigned a color value. There are 3 subpixels for each pixel in the original image so the pixel expansion is 3.

It is quite a new idea for its using probabilistic method to make sure the pixel expansion maintains 3. And it doesn't limit the number of colors in the original image. Besides, they provided a general  $k$ -out-of- $n$  scheme. It can deal with colored image and is provably secure. The quality of the reconstructed image is good when the size of the original image is large. However, it still needs preprocessing, since the only way of improving the color contrast is to modify the number of colors in the original image.

### 2.3.3 Other Colored VCS Schemes

Lukac and Plataniotis [24] proposed a colored VCS scheme in 2005, which only supports 2-out-of-2 threshold setting and has pixel expansion. Shyu [30] proposed a colored VCS scheme in 2006. Shyu's scheme applies any  $k$ -out-of- $n$  black-and-white VCS on decomposed images of the original secret image so that it supports the general  $k$ -out-of- $n$  threshold setting. The scheme has less pixel expansion compared with previous ones while it has relatively good quality of superimposed image. Hou and Tu's colored VCS [17] supports  $k$ -out-of- $n$  threshold setting with no pixel expansion. Dithering is required for preprocessing the original image before secret sharing and the number of colors supported is fixed on 8. Cimato et al.'s scheme [12], at the cost of large pixel expansion, solves the problem that superimposing many pixels of the same color results in a dark version of the color. By reducing the contrast quality to certain level, Yang and Chen [40] proposed a colored VCS scheme, which has fixed pixel expansion rate of 3.

## 2.4 Extended Visual Cryptography Schemes

A  $k$ -out-of- $n$  EVCS is an extension of the  $k$ -out-of- $n$  VCS. It encodes  $n$  independently chosen meaningful images into  $n$  meaningful shares so that by superimposing any  $k$  or more shares, the original secret image, which is embedded in these shares, will be recovered. Any  $k - 1$  or less shares are with no trace of the secret image. An example of a 2-out-of-2 EVCS is shown in Chap. 1. Fig. 1.3 shows the two meaningful images (Sailboat and Peppers) which are to be used for embedding secret shares of Lena (Fig. 1.1). Fig. 1.4 shows the two shares and the superimposed image by applying Ateniese et al.'s 2-out-of-2 EVCS scheme [3]. Each share carries a meaningful image. From any one of

the shares, no information about the secret image is revealed. The secret image can be recovered only by superimposing the shares.

### 2.4.1 Ateniese et al. Black-and-White EVCS

In [3], Ateniese et al. proposed the first  $k$ -out-of- $n$  EVCS for black-and-white images by using the hypergraph coloring method. The scheme constructs two sets of  $2^n$   $n \times m$  matrices, namely,  $T_0^{c_1, \dots, c_n}$  and  $T_1^{c_1, \dots, c_n}$  where  $c_1, \dots, c_n \in \{b, w\}$  ( $b$  represents black and  $w$  represents white). The solution of a  $k$ -out-of- $n$  black-and-white EVCS is considered valid if the following three conditions are met [36]:

1. For any  $c_1, \dots, c_n \in \{b, w\}$ , the “OR”ed value  $V$  of any  $k$  of the  $n$  rows satisfies

$$H(V) \leq \alpha_F \times m \text{ for any } S \in T_w^{c_1, \dots, c_n}; H(V) \geq d \text{ for any } S \in T_b^{c_1, \dots, c_n}.$$

2. For any  $c_1, \dots, c_n \in \{b, w\}$  and for any subset  $\{i_1, \dots, i_q\}$  of  $\{1, \dots, n\}$  with  $q < k$ , the two collections of  $q \times m$  matrices  $D_t^{c_1, \dots, c_n}$  with  $t \in \{b, w\}$  obtained by restricting each  $n \times m$  matrix in  $T_t^{c_1, \dots, c_n}$  to rows  $\{i_1, \dots, i_q\}$  are indistinguishable in the sense that they contain the same matrices with the same frequencies.

3. For any  $i \in \{1, \dots, n\}$  and any  $c_1, \dots, c_{i-1}, c_{i+1}, \dots, c_n \in \{b, w\}$ ,

$$\min H(S_i) (S_i \in \mu_b) - \max H(S_i) (S_i \in \mu_w) \geq \alpha_S \times m$$

$$\text{where } \mu_b = \bigcup T_w^{c_1, \dots, c_{i-1}, b, c_{i+1}, \dots, c_n} \text{ and } \mu_w = \bigcup T_b^{c_1, \dots, c_{i-1}, w, c_{i+1}, \dots, c_n}$$

The values  $\alpha_F$  and  $\alpha_S$  are referred to as relative differences of the reconstructed image and the shares, respectively. The first condition states that by superimposing any  $q$  ( $q \geq k$ ) shares, the secret image can be correctly recovered. The second condition implies

that no information of the secret image is gained if less than  $k$  shares are obtained. The third condition implies after being coded into shares, the meaningful images are still recognizable.

To encrypt a pixel in the secret image, if the pixel is white (resp. black) and the colors of the corresponding pixels of the  $n$  meaningful images are  $c_1, \dots, c_n \in \{b, w\}$ , then  $T_0^{c_1, \dots, c_n}$  (resp.  $T_1^{c_1, \dots, c_n}$ ) is used for creating the  $n$  share images. For the  $i$ -th share ( $1 \leq i \leq n$ ), a collection of black-and-white subpixels are printed in close proximity to each other according to the bit values of the  $i$ -th row of  $T_0^{c_1, \dots, c_n}$  (resp.  $T_1^{c_1, \dots, c_n}$ ), but in a randomly permuted order. This step is similar to randomly choosing a matrix from  $C_0$  (resp.  $C_1$ ) in the  $k$ -out-of- $n$  black-and-white VCS. The pixel expansion rate for this black-and-white EVCS is  $m > 1$ . This scheme is only for black-and-white images and has pixel expansion though it supports the general  $k$ -out-of- $n$  threshold setting.

The following is an example of a 2-out-of-2 EVCS which is used to create the two shares in Fig. 1.3. The Basic Matrices are  $T_c^{c_1, c_2}$  ( $c, c_1, c_2 \in \{w, b\}$ ) where  $c$  represents the color of the pixel in the secret image and  $c_i$  ( $i \in \{1, 2\}$ ) represents the color of the pixel in the  $i$ -th meaningful image:

$$\begin{aligned} T_w^{ww} &= \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}, T_w^{wb} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}, T_w^{bw} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}, T_w^{bb} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}, \\ T_b^{ww} &= \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, T_b^{wb} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}, T_b^{bw} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, T_b^{bb} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \end{aligned}$$

In this example,  $\alpha_F = 1/4$  and  $\alpha_S = 1/4$ .

### 2.4.2 Other EVCS Schemes

In [26], Nakajima and Yamaguchi presented a system which takes three images as inputs and outputs two share images corresponding to the two of the input images. By superimposing the two share images, the third image can be recovered. Since previous schemes mainly focused on binary images, this scheme extended them to support gray-scale and color images. In their scheme, one pixel in a gray-scale image is halftoned into several subpixels. Encryption method is then applied to the quantized image pixel by pixel. The scheme is restricted to 2-out-of-2 secret sharing. In [32], Sirhindi et al. proposed another EVCS for color images with fixed pixel expansion rate of 9. The scheme splits an color images into red (R) , green (G) and blue (B) components. A pixel from each color component is then divided into two  $3 \times 3$  subpixel blocks. Each block is filled with the component color or white (transparent). The two shares of the scheme are formed by superimposing the corresponding share of the RGB components. This scheme achieves the lossless recovery of secret image at the cost of an additional recovery algorithm. But it does not support the general  $k$ -out-of- $n$  threshold setting. In [36], Wang et al. proposed a  $k$ -out-of- $n$  EVCS for black-and-white images and also EVCS schemes for gray-scale and color images. The Basic Matrices of their scheme are constructed by concatenating the Basic Matrices of a black-and-white VCS with  $2^n$  extended matrices. The major contribution of Wang et al.'s scheme is the construction of the extended matrices. All of the schemes have pixel expansion.

For a more comprehensive comparison among these schemes and the ones we propose in this paper, we refer reader to Table 6.1 and Table 6.2 in Sec. 6 (page 62).

## Chapter 3

### A New $k$ -out-of- $n$ Colored VCS

In this chapter, we firstly introduce the notations which will be used in the following of the paper. Then we propose a  $k$ -out-of- $n$  color VCS which satisfies the four commonly desirable properties listed in Chap. 1. Finally, we prove that our VCS for color images is secure by providing a security analysis.

#### 3.1 Preliminaries

The  $k$ -out-of- $n$  threshold color VCS proposed in this paper supports original images of any number of color levels. Without loss of generality, we herewith assume that the color of the original image is represented by the conventional 24-bit primary colors of  $R$  (red),  $G$  (green) and  $B$  (blue), each having 256 levels (i.e. 8-bits), that is, for each pixel of the original image, the color quality is represented by three bytes of values and each byte specifies the intensity of the corresponding primary color. In the following, we present some notations which will be used in the rest of the paper.

For a generic  $k$ -out-of- $n$  threshold VCS for black-and-white images (e.g. [27]), we use an  $n \times l$  Boolean Matrix  $S$  (below) to denote the secret sharing process where  $l$  is the pixel expansion rate. The  $n$  rows of the matrix correspond to the  $n$  shares and the  $l$  columns correspond to the “colors” (1 for black; 0 for white/transparent) of the  $l$  pixels of each share.

$$S = \begin{bmatrix} S_{0,0} & S_{0,1} & \dots & S_{0,l-1} \\ \vdots & & & \\ S_{n-1,0} & S_{n-1,1} & \dots & S_{n-1,l-1} \end{bmatrix}$$

where  $S_{i,j} \in \{0, 1\}$ . Depending on different black-and-white VCS schemes applied, the pixel expansion rate  $l$  varies.

A  $k$ -out-of- $n$  black-and-white VCS typically consists of two  $n \times l$  Boolean Matrices  $B^0$  and  $B^1$ , which correspond to the white and black pixels in the original image, respectively. Let

$$C_b = \{\text{matrices obtained by permuting the columns of } B^b\}$$

where  $b = 0, 1$ . The secret sharing of the original image is performed pixel by pixel. For each pixel in the original image, if the color is white (resp. black), one  $n \times l$  Boolean Matrix in  $C_0$  (resp.  $C_1$ ) is randomly picked and used for creating the  $n$  shares.

The solution is considered valid if the following three conditions are met:

1. For any  $S$  in  $C_0$ , the “or” value of any  $k$  of the  $n$  rows satisfies  $H(V) \leq d - \alpha l$ .
2. For any  $S$  in  $C_1$ , the “or” value of any  $k$  of the  $n$  rows satisfies  $H(V) \geq d$ .
3. For the subset  $i_1, i_2, \dots, i_q$  with  $q < k$ , the two collections of  $q \times l$  matrices  $D_b$  (where  $b \in \{0, 1\}$ ) obtained by restricting each  $n \times l$  matrix in  $C_b$  (where  $b \in \{0, 1\}$ )

to rows  $i_1, i_2, \dots, i_q$  are indistinguishable in the sense that they contain the same matrices with the same frequencies.

The important parameters of a scheme are:

- $l$ , the number of pixels in a share. This represents the loss in resolution from the original picture to the shared one. We would like  $l$  to be as small as possible.
- $\alpha$ , 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. We would like  $\alpha$  to be as large as possible.
- $r$ , the size of the collection  $C_0$  and  $C_1$ ,  $\log r$  represents the number of random bits needed to generate the shares.

For general  $k$  and  $n$ , Naor and Shamir constructed a scheme with  $l = \log_n \cdot 2^{O(k \cdot \log_k)}$  and  $\alpha = \frac{1}{2^{\Omega(k)}}$ .

For 3-out-of-4 black-and-white VCS, below is an example of the Basic Matrices:

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

Here, the pixel expansion is 6. In our scheme described in the next section, we will see how to convert this scheme to a threshold color VCS with no pixel expansion (i.e. pixel expansion rate is 1).

The  $H(V)$  of any 3 or 4 rows of  $B^0$  is 4 while the  $H(V)$  of any 3 or 4 rows of  $B^1$  is



5 or 6. The  $H(V)$  of any 2 rows of both  $B^0$  and  $B^1$  is 4 and the  $H(V)$  of any one row of both  $B^0$  and  $B^1$  is 3. So it satisfies the three conditions of a valid VCS with  $d=5$ ,  $\alpha=1/6$  and  $l = 6$ .

## 3.2 Our Scheme

We now describe the VCS which supports all the four properties listed in Chap. 1. Along with the scheme description, we use Lena image (Fig. 3.1) for illustration. Our VCS scheme consists of the following steps.

1. Histogram Generation
2. Color Quality Determination
3. Grouping
4. Share Creation

These steps are elaborated as follows.

### 3.2.1 Histogram Generation

For the secret image, we first generate three primary-color (i.e.  $R$ ,  $G$ ,  $B$ ) component images and then create a histogram for each primary-color component image. To do so, we can group all the pixels in a easy and effective way. As an example, suppose that the secret image is the Lena image which is encoded in 24-bit RGB (Fig. 3.1). Fig. 3.2 shows the three RGB primary-color component images of Lena. In each component

image, there are 256 levels of intensity of the corresponding primary color. Fig. 3.3 shows the three histograms generated in this step. In the histogram of  $R$  (resp.  $G$  and  $B$ ), the horizontal axis represents the intensity of  $R$  (resp.  $G$  and  $B$ ) ranging from 0 to 255 and the vertical axis represents the number of pixels in the  $R$  (resp.  $G$  and  $B$ ) component image that have the intensity value.

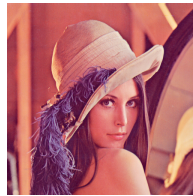


Figure 3.1: The Original Lena Image

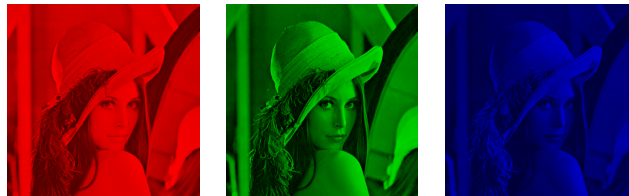


Figure 3.2: The RGB Component Images of Lena

### 3.2.2 Color Quality Determination

In this step, the user is to choose the number of intensity levels that the reconstructed image will have when at least  $k$  share images are superimposed. The number of intensity levels directly affect the quality of reconstructed image. First, the user is to determine the number of intensity levels for maximizing the quality of the reconstructed image. Let  $N$  be the number of intensity levels that the reconstructed image will have. As the reconstructed image has three primary-color components, we set  $N = N_R \times N_G \times N_B$ ,

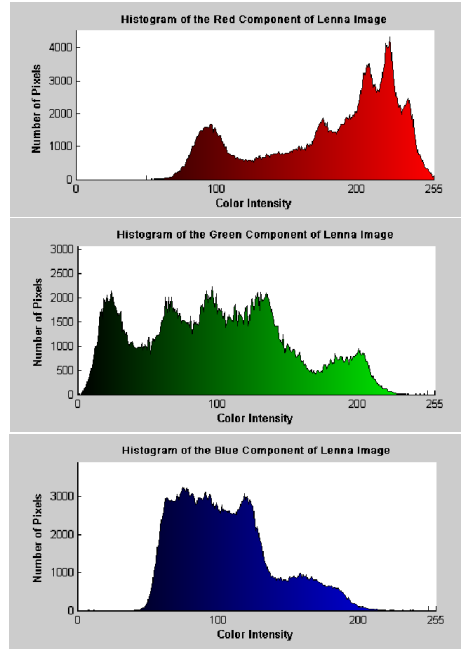


Figure 3.3: Histograms of the RGB Component Images

where  $N_X$  denotes the number of the intensity levels of  $X \in \{R, G, B\}$  primary-color component of the reconstructed image. Suppose that we would like to have a 64-color reconstructed image, we may set  $N_X$ ,  $X \in \{R, G, B\}$ , as follows:  $64(N) = 4(N_R) \times 4(N_G) \times 4(N_B)$ . Note that  $N_R$ ,  $N_G$  and  $N_B$  do not need to be the same. In Sec. 5.1, we provide more discussions on how to choose the number of color levels.

### 3.2.3 Grouping

In this step, we partition all pixels into different groups. Original pixels which are in different group will show difference in the reconstructed image. For each primary color  $X \in \{R, G, B\}$ , we partition the histogram of  $X$  of the secret image into  $N_X$  groups so that each group has the same area as other groups on the histogram, where  $N_X$  is the number of color intensities for the  $X$  component of the (to-be)-reconstructed secret

image determined in the previous step. By the same area on a histogram, it implies that there will be an equal number of pixels in each of the  $N_X$  groups on the histogram. Fig. 3.4 shows the histograms of the RGB primary-color component images of Lena after grouping where  $N_X = 4$  for all  $X \in \{R, G, B\}$ . In the figure, we use different color intensities to represent different groups. There are also other partition methods. In Sec. 5.1, we introduce another partition method and further discuss the reasons behind choosing this approach for grouping.

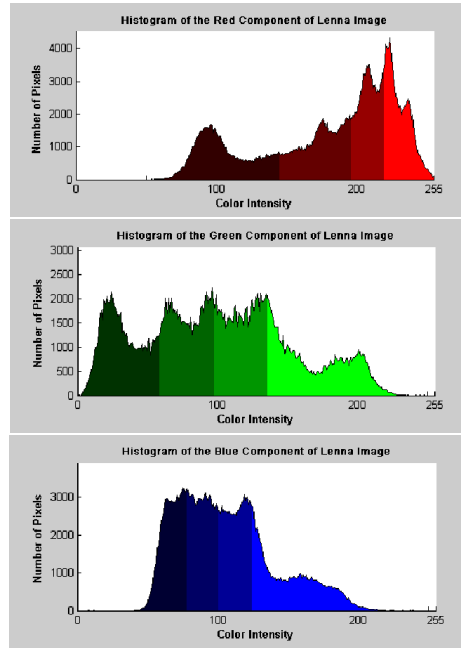


Figure 3.4: Histograms Illustrating the  $4 \times 4 \times 4$  Color Levels

### 3.2.4 Share Creation

We now apply the following method to each of the primary color independently. For general  $k$ -out-of- $n$  scheme, we employ techniques from the VCS by Naor and Shamir.

First of all, we change the representation of  $B^0$  (resp.  $B^1$ ) to the following:

$B^0 = \begin{bmatrix} B_0^0, B_1^0, \dots, B_{l-1}^0 \end{bmatrix}$  and  $B^1 = \begin{bmatrix} B_0^1, B_1^1, \dots, B_{l-1}^1 \end{bmatrix}$  where  $B_i^0$  and  $B_i^1$  ( $0 \leq i \leq l-1$ ) represent the  $(i+1)$ -th column of the matrix basis of  $C_0$  and  $C_1$  respectively.

This step is carried out pixel by pixel for the secret image. For each primary color  $X \in \{R, G, B\}$  of a pixel in the secret image, we carry out the following steps:

1. On the  $X$  histogram of the secret image, suppose that the color intensity of the pixel with respect to primary color  $X$  is in the  $(k+1)$ -th group (where  $0 \leq k \leq N_X - 1$ ). We compute a probability value  $P_X = k/(N_X - 1)$  which determines the likelihood of going through one of the following steps.
2. With the probability  $P_X$ , we carry out the following two steps:
  - We look into  $B^0$  and randomly pick a column, for example,  $B_j^0$  where  $0 \leq j \leq l-1$ .
  - We consider this column as an  $n$ -bit vector. For the first bit, we assign the black color (i.e. 0 color intensity) if the bit is 1, otherwise we assign  $X$  color (i.e. 255 color intensity). This continues until we have assigned colors to this pixel for all the  $n$  shares.
3. With the probability  $1-P_X$ , we carry out similar steps to that in step 2 above, but the set of matrices are now referring to  $B^1$ .

Determined by the value of  $P_X$ , in Table 3.1, we summarize the probability distribution of  $B^0$  and  $B^1$  for individual group.

Table 3.1: The chance of using  $B^0$  or  $B^1$  for individual group during Share Creation

	Group 0	Group $k$	Group $(N_X - 1)$
probability of using $B^0$	0	$k/(N_X - 1)$	1
probability of using $B^1$	1	$1-k/(N_X - 1)$	0

Finally, we superimpose the  $i$ -th  $R$  share with the  $i$ -th  $G$  share as well as the  $i$ -th  $B$  share, for  $i=1, \dots, n$ , to form the final  $i$ -th share which consists of the corresponding  $R, G, B$  components.

**Example** Suppose we want to create a 64-level set of secret shares so that each color component has four groups. After dividing the  $R, G, B$  components of the original image into four groups (i.e. Grouping) respectively, we carry out the Share Creation by adopting the 3-out-of-4 scheme in Sec. 3.1. The probability distribution of the individual column of  $B^0$  and  $B^1$  is shown in Table 3.2.

Table 3.2 shows when doing secret sharing based on 3-out-of-4 scheme, the probability of choosing one column of  $B^0$  or  $B^1$  in different groups. Column 2 shows the color of the four shares when choosing the different column of  $B^0$  or  $B^1$  (0 represents the primary color with color intensity 255 and 1 represents the black color). Column 3 to 6 is the probability of choosing the corresponding column of  $B^0$  or  $B^1$  if the original color of the pixel is in one of the four groups. Since the columns in  $B^0$  (resp.  $B^1$ ) are uniformly distributed, when doing the secret sharing, the dealer just randomly chooses one column in  $B^0$  (resp.  $B^1$ ) with the possibility of  $\frac{k/(N_X-1)}{l}$  (resp.  $\frac{1-k/(N_X-1)}{l}$ ). Based on the description above, in Fig. 3.5, we illustrate the two shares created from the Lena

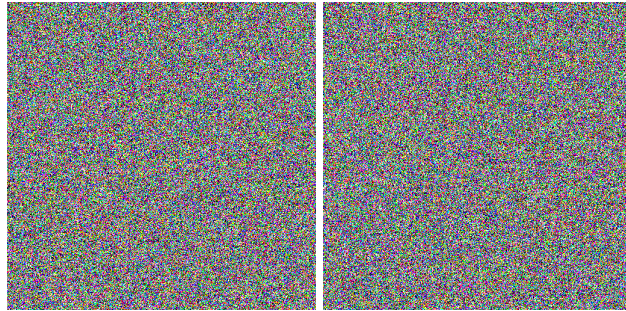


Figure 3.5: The Two Shares of the Original Lena Image

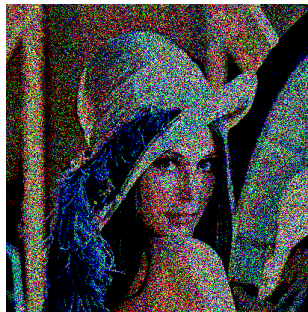


Figure 3.6: The Superimposed Image of the Two Shares

image (Fig. 3.1). Fig. 3.6 is the superimposed image of the two shares.

### 3.3 Security Analysis

Let  $B^0$  and  $B^1$  be the two Basic Matrices of a  $k$ -out-of- $n$  black-and-white VCS [27]. We refer readers to Sec. 3.1 for the details of the security definition of a secure  $k$ -out-of- $n$  black-and-white VCS. Without loss of generality, suppose  $B^0$  and  $B^1$  are  $n \times l$  boolean matrices. Let  $N$  be the number of color intensity levels that the reconstructed image in our VCS scheme will have, where  $N = N_R \times N_G \times N_B$ .  $N_X$  denotes the number of intensity levels of the  $X \in \{R, G, B\}$  primary color that the reconstructed image will have. The following description is applied to each of the primary color  $X$  in  $\{R, G, B\}$ .

Let  $D_j(q)$  be the “OR”ed value of any  $q$  ( $1 \leq q \leq n$ ) elements in the  $j$ -th column ( $1 \leq j \leq 2l$ ) of  $B^0 \circ B^1$ . Let  $P_j(r)$  be the probability of choosing the  $j$ -th column of  $B^0 \circ B^1$  if the pixel in the original secret image that has the color intensity with respect to primary color  $X$  falls in the Group  $r$  ( $0 \leq r \leq N_X - 1$ ). Let  $CI_{VCS}(q, r) = \sum_{j=1}^{2l} P_j(r) \times D_j(q)$  be the weighted intensity corresponding to primary color  $X$  when the pixels from any  $q$  shares corresponding to the pixel in the original secret image are superimposed, given the pixel in the original secret image that has the color intensity with respect to primary color  $X$  falls in the Group  $r$  ( $0 \leq r \leq N_X - 1$ ).

**Definition** A  $k$ -out-of- $n$  VCS for color images is secure if the following conditions are met:

1. For any  $q$  shares such that  $q \geq k$  and for any two pixels of the original secret image in different intensity group with respect to a primary color  $X \in \{R, G, B\}$ , namely  $r$  and  $r'$  such that  $0 \leq r, r' \leq N_X - 1$  and  $r \neq r'$ , we have  $|CI_{VCS}(q, r) - CI_{VCS}(q, r')| \geq \alpha_F$  where  $\alpha_F > 0$ .
2. For any  $q$  shares such that  $q < k$  and for any two pixels of the original secret image in different intensity group with respect to a primary color  $X \in \{R, G, B\}$ , namely  $r$  and  $r'$  such that  $0 \leq r, r' \leq N_X - 1$  and  $r \neq r'$ , we have  $|CI_{VCS}(q, r) - CI_{VCS}(q, r')| = 0$ .

$\alpha_F$  is the relative difference between combined shares that come from two pixels in different groups in the original image. The first condition states that by superimposing any  $q$  ( $q \geq k$ ) shares, the secret image can be correctly recovered. The second condition implies that no information of the secret image is gained if less than  $k$  shares are obtained.



**Theorem 3.3.1** *Our  $k$ -out-of- $n$  VCS is a valid scheme with  $\alpha_F = \alpha/(N_X - 1)$  ( $\alpha$  is the contrast parameter of a  $k$ -out-of- $n$  black-and-white VCS).*

**Proof** From the definition of a valid black-and-white VCS in Sec. 3.1, the Basic Matrices of a  $k$ -out-of- $n$  black-and-white VCS  $B^0$  and  $B^1$  should meet the following conditions:

- For  $B^0$ , the bitwise OR result denoted by  $V_0$  of any  $k$  of the  $n$  rows satisfies that  $H(V_0) \leq d - \alpha l$ , for some  $1 \leq d \leq l$  and  $\alpha > 0$ ;
- For  $B^1$ , the bitwise OR result denoted by  $V_1$  of any  $k$  of the  $n$  rows satisfies that  $H(V_1) \geq d$ ;
- The bitwise OR result denoted by  $V$  of any less than  $k$  of the  $n$  rows satisfies that  $H(V)$  is the same for both  $B^0$  and  $B^1$ .

Therefore,  $CI_{VCS}(k, r) = r/(N_X - 1) \times H(V_0)/l + (1 - r/(N_X - 1)) \times H(V_1)/l$ .

$$|CI_{VCS}(k, r) - CI_{VCS}(k, r')| = |(r - r') \times \alpha/(N_X - 1)| \geq \alpha/(N_X - 1) > 0.$$

$$|CI_{VCS}(q, r) - CI_{VCS}(q, r')| = 0 \quad (q < k).$$

### 3.4 Summary

In this chapter, we have proposed a  $k$ -out-of- $n$  VCS for color images. Our scheme generically converts any  $k$ -out-of- $n$  threshold visual cryptography scheme for black-and-white images into one that supports color images. We elaborated the four steps,

namely, Histogram Generation, Color Quality Determination, Group and Share Creation in detail along with an example. We also defined a valid  $k$ -out-of- $n$  VCS for color images and prove our scheme is a valid one. In the next Chapter, we will extend our colored VCS to colored EVCS which also has no pixel expansion.

Table 3.2: The chance of using each column of  $B^0$  or  $B^1$  for individual group during Share Creation

The possibility of choosing the $N$ th column of matrix $X$	Shares	Group 0	Group 1	Group 2	Group 3
$N=1, X=B^0$	0000	0	1/18	1/9	1/6
$N=2, X=B^0$	0000	0	1/18	1/9	1/6
$N=3, X=B^0$	1110	0	1/18	1/9	1/6
$N=4, X=B^0$	1101	0	1/18	1/9	1/6
$N=5, X=B^0$	1011	0	1/18	1/9	1/6
$N=6, X=B^0$	0111	0	1/18	1/9	1/6
$N=1, X=B^1$	1000	1/6	1/9	1/18	0
$N=2, X=B^1$	0100	1/6	1/9	1/18	0
$N=3, X=B^1$	0010	1/6	1/9	1/18	0
$N=4, X=B^1$	0001	1/6	1/9	1/18	0
$N=5, X=B^1$	1111	1/6	1/9	1/18	0
$N=6, X=B^1$	1111	1/6	1/9	1/18	0

## Chapter 4

### A New $k$ -out-of- $n$ Colored EVCS

In this chapter, we propose a  $k$ -out-of- $n$  EVCS for color images which has no pixel expansion. The notations, which are used to describe our scheme in this chapter, were introduced in Sec. 3.1.

#### 4.1 Our Scheme

We now propose a  $k$ -out-of- $n$  EVCS for color images. The scheme is the first EVCS for color images with *no* pixel expansion. For a color secret image, suppose that  $n$  meaningful images have already been chosen. These images are color images chosen arbitrarily and will be used for generating  $n$  share images. Also, the choosing processing is totally independent as long as the image size is the same as that of the secret image since our scheme does not have any pixel expansion. Our scheme consists of the following steps.

1. Histogram Generation

2. Color Quality Determination
3. Grouping
4. Share Creation

These steps are elaborated as follows.

#### **4.1.1 Histogram Generation**

For the secret image and each of the  $n$  images which will be used to create share images, we first generate three primary-color (i.e.  $R$ ,  $G$ ,  $B$ ) component images for each of them and then create a histogram for each primary-color component image. To do so, we can group all the pixels in a easy and effective way. As an example, suppose that the secret image is the Lena image which is encoded in 24-bit RGB (Fig. 3.1). Fig. 3.2 shows the three RGB primary-color component images of Lena. In each component image, there are 256 levels of intensity of the corresponding primary color. Fig. 3.3 shows the three histograms generated in this step. In the histogram of  $R$  (resp.  $G$  and  $B$ ), the horizontal axis represents the intensity of  $R$  (resp.  $G$  and  $B$ ) ranging from 0 to 255 and the vertical axis represents the number of pixels in the  $R$  (resp.  $G$  and  $B$ ) component image that have the intensity value.

#### **4.1.2 Color Quality Determination**

In this step, the user is to choose the number of intensity levels that the reconstructed image will have when at least  $k$  share images are superimposed and the number of

intensity levels of each share image. The number of intensity levels directly affect the quality of reconstructed image. First, the user is to determine the number of intensity levels for maximizing the quality of the reconstructed image or the share images. Let  $N$  be the number of intensity levels that the reconstructed image will have. As the reconstructed image has three primary-color components, we set  $N = N_R \times N_G \times N_B$ , where  $N_X$  denotes the number of the intensity levels of  $X \in \{R, G, B\}$  primary-color component of the reconstructed image. For the  $n$  share images, let  $M_i$  be the number of intensity levels of the  $i$ -th share image (for  $i = 1, \dots, n$ ), where  $M_i = M_{i_R} \times M_{i_G} \times M_{i_B}$ , where  $M_{i_X}$  denotes the number of intensity levels of  $X \in \{R, G, B\}$  component of the  $i$ -th share. Suppose that we would like to have a 64-color reconstructed image, we may set  $N_X$ ,  $X \in \{R, G, B\}$ , as follows:  $64(N) = 4(N_R) \times 4(N_G) \times 4(N_B)$ . Note that  $N_R, N_G$  and  $N_B$  do not need to be the same.  $M_{i_X}$  and  $N_X$ ,  $X \in \{R, G, B\}$ ,  $1 \leq i \leq n$ , can also be different. In Sec. 5.1, we provide more discussions on how to choose the number of color levels.

### 4.1.3 Grouping

In this step, we partition all pixels into different groups. Original pixels which are in different group will show difference in the reconstructed image. As of the previous step, this step is carried out on each of the  $n$  meaningful images as well as the secret image. In the following, we use the secret image as an example to describe how the grouping works. For each primary color  $X \in \{R, G, B\}$ , we partition the histogram of  $X$  of the secret image into  $N_X$  groups so that each group has the same area as other groups on the histogram, where  $N_X$  is the number of color intensities for the  $X$  component of the (to-be)-reconstructed secret image determined in the previous step. By the same area

on a histogram, it implies that there will be an equal number of pixels in each of the  $N_X$  groups on the histogram. Fig. 3.4 shows the histograms of the RGB primary-color component images of Lena after grouping where  $N_X = 4$  for all  $X \in \{R, G, B\}$ . In the figure, we use different color intensities to represent different groups.

#### 4.1.4 Share Creation

The final step of the scheme is to create the  $n$  shares. To create these shares, we start with by creating  $n$  shares for each primary color. After creating all the shares of the three primary colors, we then superimpose the three shares corresponding to the three primary colors of the  $i$ -th share,  $1 \leq i \leq n$ , for forming the  $n$  final shares. In the following, we describe how the  $n$  shares of each primary color  $X \in \{R, G, B\}$  are created. In the description, we will employ the Basic Matrices  $B^0$  and  $B^1$  of the  $k$ -out-of- $n$  black-and-white VCS reviewed in Sec. 3.1. Note that the two Basic Matrices have the dimension of  $n \times l$ .

1. We first construct a  $k$ -out-of- $n$  black-and-white EVCS. The construction can be viewed as an extension of the  $k$ -out-of- $n$  black-and-white VCS reviewed in Sec. 3.1. The extension is similar to the method due to Wang, Yi and Li [36].
  - (a) Take a  $k$ -out-of- $n$  black-and-white VCS which satisfies the conditions in Sec. 3.1. Let the Basic Matrices  $B^0$  and  $B^1$  are of dimension  $n \times l$ . For example, the following is the  $B^0$  and  $B^1$  for a 2-out-of-3 black-and-white VCS where  $n = l = 3$ .

$$B^0 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \text{ and } B^1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

- (b) Then, we construct  $2^n$  boolean matrices denoted by  $A^{c_1, \dots, c_n}$  ( $A_c$  is short for  $A^{c_1, \dots, c_n}$ ) for  $c_1, \dots, c_n \in \{b, w\}$ , where  $b$  stands for *black* and  $w$  stands for *white*. Each of  $A^{c_1, \dots, c_n}$  will be  $n \times t$  for some integer  $t \geq \lceil \frac{n}{k-1} \rceil$ . In each row of  $A^{c_1, \dots, c_n}$ , for example, the  $i$ -th row ( $1 \leq i \leq n$ ), all the  $t$  bits but one must be 1. The remaining bit is 1 if  $c_i = b$  and is 0 if  $c_i = w$ . We denote this bit as  $*$  in the following. In other words, each row of  $A^{c_1, \dots, c_n}$  has only one  $*$ . Besides, the number of  $*$  in each column of  $A^{c_1, \dots, c_n}$  should be at most  $k-1$ . Below is an example for  $n = 3$  and  $k = 2$ , i.e. the case of 2-out-of-3 black-and-white VCS. For any  $(c_1, c_2, c_3) \in \{b, w\}^3$ ,  $A^{c_1, c_2, c_3}$  is of the form below where  $t = 3$ .

$$A^{c_1, c_2, c_3} = \begin{bmatrix} * & 1 & 1 \\ 1 & * & 1 \\ 1 & 1 & * \end{bmatrix}, \quad * \in \{0, 1\}. \quad (4.1)$$

These eight  $A^{c_1, c_2, c_3}$ ,  $c_1, c_2, c_3 \in \{b, w\}$  are as follows.

$$\begin{aligned} A^{www} &= \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}, & A^{wwb} &= \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \\ A^{wbw} &= \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}, & A^{wbb} &= \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \end{aligned}$$



$$\begin{aligned}
A^{bww} &= \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}, & A^{bwb} &= \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \\
A^{bbw} &= \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}, & A^{bbb} &= \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.
\end{aligned}$$

(c) The  $k$ -out-of- $n$  black-and-white EVCS is defined as the following Basic Matrices:

$T_0^{c_1, \dots, c_n} = B^0 \circ A^{c_1, \dots, c_n}$  and  $T_1^{c_1, \dots, c_n} = B^1 \circ A^{c_1, \dots, c_n}$  for  $c_1, \dots, c_n \in \{b, w\}$ . Therefore, there are altogether  $2^{n+1}$  Basic Matrices and they can be considered as two *sets* of Basic Matrices, that is,  $\{T_0^{c_1, \dots, c_n}\}_{c_1, \dots, c_n \in \{b, w\}}$  and  $\{T_1^{c_1, \dots, c_n}\}_{c_1, \dots, c_n \in \{b, w\}}$ , each set has  $2^n$  Basic Matrices. Since  $B^0$  and  $B^1$  are  $n \times l$  and  $A^{c_1, \dots, c_n}$  are  $n \times t$ , these matrices are  $n \times m$  where  $m = l + t$ .

For example, we can construct a 2-out-of-3 black-and-white EVCS by defining two sets of Basic Matrices as  $T_0^{c_1, c_2, c_3}$  and  $T_1^{c_1, c_2, c_3}$ , for  $c_1, c_2, c_3 \in \{b, w\}$ , by concatenating the Basic Matrices of a 2-out-of-3 black-and-white VCS ( $B^0$  or  $B^1$ ) and the eight  $A^{c_1, c_2, c_3}$  shown as above.

This  $k$ -out-of- $n$  black-and-white EVCS works as follows. For each pixel in the secret image, if the pixel is white (resp. black) and the colors of the corresponding pixels of the  $n$  meaningful images are  $c_1, \dots, c_n \in \{b, w\}$ , then  $T_0^{c_1, \dots, c_n}$  (resp.  $T_1^{c_1, \dots, c_n}$ ) is used for creating the  $n$  share images. For the  $i$ -th share, a collection of black and white subpixels are printed in close proximity to each other according to the bit values of the  $i$ -th row of  $T_0^{c_1, \dots, c_n}$  (resp.  $T_1^{c_1, \dots, c_n}$ ), but in a randomly permuted order. This step is similar to randomly choosing a matrix from  $C_0$  (resp.  $C_1$ ) in the  $k$ -out-of- $n$  black-and-

white VCS. As a result, the pixel expansion rate for this black-and-white EVCS is  $m > 1$  (since  $l \geq 1$  and  $t \geq 1$ ).

In the next step, we use the Basic Matrices  $T_0^{c_1, c_2, \dots, c_n}$  and  $T_1^{c_1, c_2, \dots, c_n}$  in a *probabilistic* way on each RGB primary-color component image so that the share images created will have the same size as the original secret image (i.e. no pixel expansion or having the optimal pixel expansion rate of 1).

2. This step is carried out pixel by pixel for the secret image. For each primary color  $X \in \{R, G, B\}$  of a pixel in the secret image, we carry out the following steps:

(a) On the  $X$  histogram of the secret image, suppose that the color intensity of the pixel with respect to primary color  $X$  is in Group  $k$  group (where  $0 \leq k \leq N_X - 1$ ). We compute a probability value  $P_X = k/(N_X - 1)$  which determines the likelihood of going through one of the following steps.

(b) With probability  $P_X$ , we carry out the following two steps:

- We look into  $n \times l$  Basic Matrix  $B^0$  of the  $k$ -out-of- $n$  black-and-white VCS and the general form  $A^{c_1, \dots, c_n}$  as of equation (4.1).

- With probability  $P_1$ , which is determined by the user as follows, we randomly pick a column from  $B^0$ ; The trade-off between the quality of share images and the reconstructed image is the result of adjusting the value of  $P_1$ . The greater (less) the  $P_1$  is, the higher (lower) the quality of the reconstructed image would be and the lower (higher) the quality of the share images would be.

- With probability  $1 - P_1$ , suppose the color intensity of the  $X$  primary-color component of the corresponding pixel in the  $i$ -th meaningful image is in Group  $k_{i_X}$  (where  $0 \leq k_{i_X} \leq M_{i_X} - 1$  and  $1 \leq i \leq n$ ),

we compute a probability value  $Q_{i_X} = k_{i_X} / (M_{i_X} - 1)$ . We then set the  $*$  in the  $i$ -th row of the general form  $A^{c_1, \dots, c_n}$  to 0 with the probability  $Q_{i_X}$  and to 1 with the probability  $1 - Q_{i_X}$  and randomly choose a column from it.

- Consider the column chosen as an  $n$ -bit vector. For the first bit, we assign the black color (i.e. 0 color intensity) if the bit is 1, otherwise we assign  $X$  primary color (i.e. 255 color intensity) to the corresponding pixel in the first share image. This continues until we have assigned colors to the corresponding pixel on all the  $n$  share images.

(c) With the probability  $1 - P_X$ , we carry out similar steps to the above, but change  $B^0$  to  $B^1$ .

3. Finally, we superimpose the  $i$ -th  $R$  share with the  $i$ -th  $G$  share and the  $i$ -th  $B$  share, for  $i = 1, \dots, n$ , to form the final  $i$ -th color share image.

## 4.2 Example

We now give an example which is a 2-out-of-3 EVCS for 24-bit RGB color images. Suppose that the secret image is Lena (Fig. 3.1) and the three meaningful images have already been chosen, which are Mandrill, Sailboat and Peppers (Fig. 4.1).

First, we generate 4 sets of histograms corresponding to the 4 images and each set contains the  $R$ ,  $G$  and  $B$  histograms of the corresponding image. Fig. 3.3, Fig. 4.2, Fig. 4.3 and Fig. 4.4 are the histograms of Lena, Mandrill, Sailboat and Peppers generated in this step.

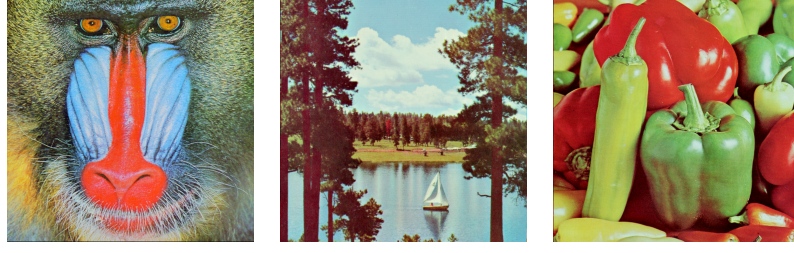


Figure 4.1: The Images of Mandrill, Sailboat, Peppers

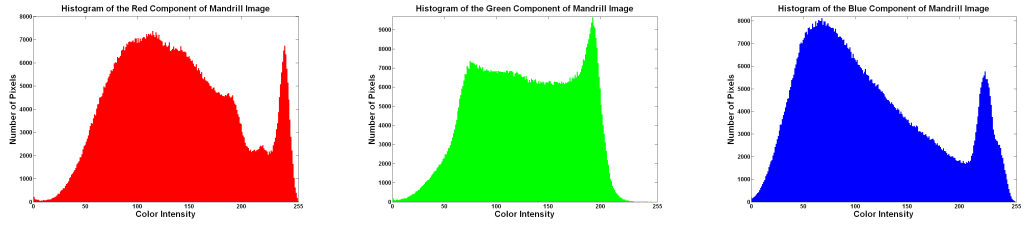


Figure 4.2: Histograms of the RGB Components of Mandrill

Then we set  $N = M_i = 64$ ,  $N_R = N_G = N_B = 4$  and  $M_{i_R} = M_{i_G} = M_{i_B} = 4$  (where  $1 \leq i \leq 3$ ) and do the grouping on each of the 4 images. Fig. 3.4, Fig. 4.5, Fig. 4.6 and Fig. 4.7 show the grouping (using different color intensities) on the histograms of Lena, Mandrill, Sailboat and Peppers.

Finally, we create 3 shares as follows.

1. Suppose we use the Basic Matrices  $B^0$  and  $B^1$  for the 2-out-of-3 black-and-white EVCS shown in the example of Share Creation (Sec. 4.1.3). We also use the general form  $A^{c_1, c_2, c_3}$  in equation (4.1).
2. We now go through the secret image pixel by pixel, for each pixel and for each primary color  $X \in \{R, G, B\}$ , we choose one column from  $B^0 \circ A^{c_1, c_2, c_3}$  or  $B^1 \circ A^{c_1, c_2, c_3}$ , depending on  $P_X$  computed. In Table 4.1, we summarize the probability distribution among the columns of  $B^0 \circ A^{c_1, c_2, c_3}$  and  $B^1 \circ A^{c_1, c_2, c_3}$  when  $P_1$  is

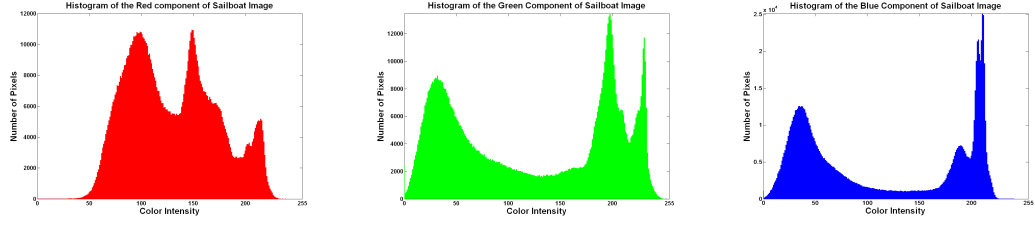


Figure 4.3: Histograms of the RGB Components of Sailboat

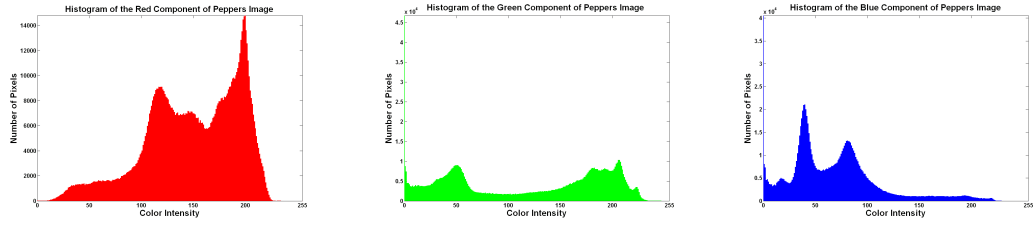


Figure 4.4: Histograms of the RGB Components of Peppers

chosen as 0.5 ( $Q_{i_X} = k_{i_X}/3$  for  $0 \leq k_{i_X} \leq 3$  and  $1 \leq i \leq 3$ ). Column 2 in Table 4.1 specifies the pixel color of the three shares when the  $j$ -th ( $1 \leq j \leq 6$ ) column of  $B^0 \circ A^{c_1, c_2, c_3}$  or  $B^1 \circ A^{c_1, c_2, c_3}$  is chosen (0 represents the primary color; 1 represents the black color). Column 3 to 6 indicate the probabilities of choosing the  $j$ -th ( $1 \leq j \leq 6$ ) column. Since the columns in  $B^0 \circ A^{c_1, c_2, c_3}$  (resp.  $B^1 \circ A^{c_1, c_2, c_3}$ ) are uniformly distributed, when doing the secret sharing, the dealer just randomly chooses one column in  $B^0 \circ A^{c_1, c_2, c_3}$  (resp.  $B^1 \circ A^{c_1, c_2, c_3}$ ) with the possibility of  $\frac{k/(N_X-1)}{(l+t)}$  (resp.  $\frac{1-k/(N_X-1)}{(l+t)}$ ).

3. Consider the chosen column as a 3-bit vector. For the first bit, we assign the black color (i.e. 0 color intensity) if the bit is 1, otherwise we assign primary color  $X$  (i.e. 255 color intensity). This continues until we have assigned colors to this pixel for all the 3 shares. Then we superimpose the  $i$ -th  $R$  share with the  $i$ -th  $G$  share as well as the  $i$ -th  $B$  share, for  $i = 1, 2, 3$ , to form the final  $i$ -th share which

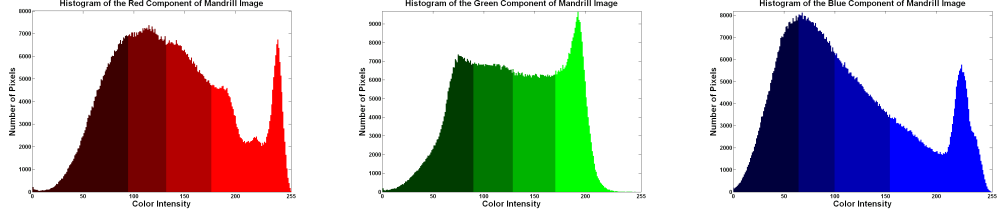


Figure 4.5: Histograms Illustrating the  $4 \times 4 \times 4$  Groupings of Mandrill

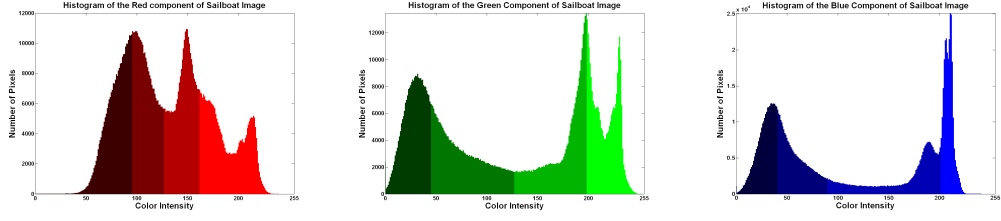


Figure 4.6: Histograms Illustrating the  $4 \times 4 \times 4$  Groupings of Sailboat

consists of the corresponding RGB components. Fig. 4.8 shows the share images corresponding to Mandrill, Sailboat and Peppers. Fig. 4.9 and Fig. 4.10 are the superimposed images of any two of the shares and the three shares, respectively.

### 4.3 Security Analysis

Let  $B^0$  and  $B^1$  be the two Basic Matrices of a  $k$ -out-of- $n$  black-and-white VCS [27]. We refer readers to Sec. 3.1 for the details of the security definition of a secure  $k$ -out-of- $n$  black-and-white VCS. As specified in Sec. 3.1, suppose that each of  $B^0$  and  $B^1$  is a  $n \times l$  boolean matrix. Let a  $n \times t$  ( $t \geq \lceil \frac{n}{k-1} \rceil$ ) boolean matrix  $A_c$  be the Extended Matrix for constructing the Basis Matrices of our  $k$ -out-of- $n$  EVCS. Let  $N$  be the number of color intensity levels that the reconstructed image in our EVCS scheme will have, where  $N = N_R \times N_G \times N_B$ .  $N_X$  denotes the number of intensity levels of

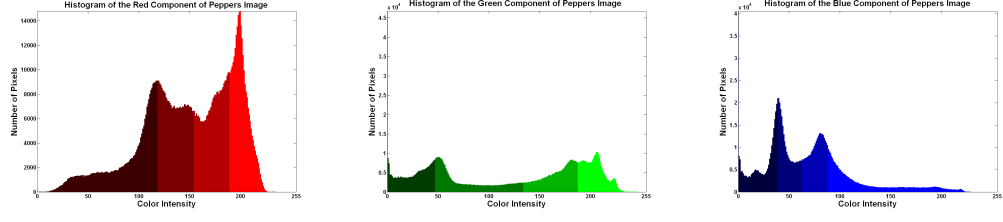


Figure 4.7: Histograms Illustrating the  $4 \times 4 \times 4$  Groupings of Peppers

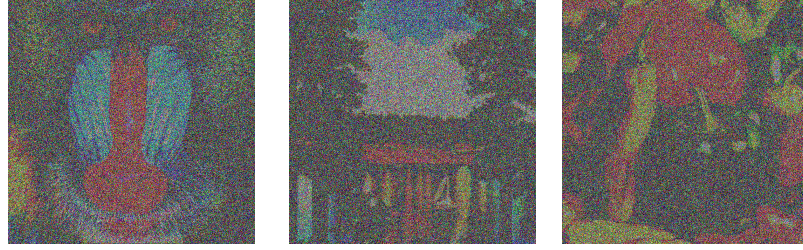


Figure 4.8: Three Shares Corresponding to Mandrill, Sailboat and Peppers Images

the  $X \in \{R, G, B\}$  primary color that the reconstructed image will have. Let  $M_i$  be the number of color intensity levels that the  $i$ -th share in our EVCS scheme will have, where  $M_i = M_{i_R} \times M_{i_G} \times M_{i_B}$ .  $M_{i_X}$  denotes the number of intensity levels of the  $X \in \{R, G, B\}$  primary color that the  $i$ -th share ( $1 \leq i \leq n$ ) will have. The following description applies to each of the primary color  $X$  in  $\{R, G, B\}$ .

Let  $D'_j(q)$  be the “OR”ed value of any  $q$  ( $1 \leq q \leq n$ ) elements in the  $j$ -th column ( $1 \leq j \leq 2(l+t)$ ) of  $B^0 \circ A_c \circ B^1 \circ A_c$ . Let  $P'_j(r)$  be the probability of choosing the  $j$ -th column of  $B^0 \circ A_c \circ B^1 \circ A_c$  if the the pixel in the original secret image that has the color intensity with respect to primary color  $X$  falls in the Group  $r$  ( $0 \leq r \leq N_X - 1$ ). Let  $CI_{EVCS}(q, r) = \sum_{j=1}^{2(l+t)} P'_j(r) \times D'_j(q)$  be the weighted intensity corresponding to primary color  $X$  when the pixels from any  $q$  shares corresponding to the pixel in the original secret image are superimposed, given the the pixel in the original secret image has the color intensity with respect to primary color  $X$  falls in the Group  $r$  ( $0 \leq r \leq$

Table 4.1: The chance of picking the columns of  $B^0 \circ A^{c_1, c_2, c_3}$  or  $B^1 \circ A^{c_1, c_2, c_3}$  with respect to  $X$  during Share Creation ( $X \in \{R, G, B\}$ ).

The case of choosing the $j$ th column of $B \circ A^{c_1, c_2, c_3}$	Shares	Group 0	Group 1	Group 2	Group 3
$j = 1, B=B^0$	111	0	1/18	1/9	1/6
$j = 2, B=B^0$	000	0	1/18	1/9	1/6
$j = 3, B=B^0$	000	0	1/18	1/9	1/6
$j = 4, B=B^0$	011	0	$1/18 \times Q_{1_X}$	$1/9 \times Q_{1_X}$	$1/6 \times Q_{1_X}$
	111	0	$1/18 \times (1 - Q_{1_X})$	$1/9 \times (1 - Q_{1_X})$	$1/6 \times (1 - Q_{1_X})$
$j = 5, B = B^0$	101	0	$1/18 \times Q_{2_X}$	$1/9 \times Q_{2_X}$	$1/6 \times Q_{2_X}$
	111	0	$1/18 \times (1 - Q_{2_X})$	$1/9 \times (1 - Q_{2_X})$	$1/6 \times (1 - Q_{2_X})$
$j = 6, B = B^0$	110	0	$1/18 \times Q_{3_X}$	$1/9 \times Q_{3_X}$	$1/6 \times Q_{3_X}$
	111	0	$1/18 \times (1 - Q_{3_X})$	$1/9 \times (1 - Q_{3_X})$	$1/6 \times (1 - Q_{3_X})$
$j = 1, B = B^1$	100	1/6	1/9	1/18	0
$j = 2, B = B^1$	010	1/6	1/9	1/18	0
$j = 3, B = B^1$	001	1/6	1/9	1/18	0
$j = 4, B = B^1$	011	$1/6 \times Q_{1_X}$	$1/9 \times Q_{1_X}$	$1/18 \times Q_{1_X}$	0
	111	$1/6 \times (1 - Q_{1_X})$	$1/9 \times (1 - Q_{1_X})$	$1/18 \times (1 - Q_{1_X})$	0
$j = 5, B = B^1$	101	$1/6 \times Q_{2_X}$	$1/9 \times Q_{2_X}$	$1/18 \times Q_{2_X}$	0
	111	$1/6 \times (1 - Q_{2_X})$	$1/9 \times (1 - Q_{2_X})$	$1/18 \times (1 - Q_{2_X})$	0
$j = 6, B = B^1$	110	$1/6 \times Q_{3_X}$	$1/9 \times Q_{3_X}$	$1/18 \times Q_{3_X}$	0
	111	$1/6 \times (1 - Q_{3_X})$	$1/9 \times (1 - Q_{3_X})$	$1/18 \times (1 - Q_{3_X})$	0

$N_X - 1$ ). For the  $i$ -th row of  $B^0 \circ A_c \circ B^1 \circ A_c$  where  $1 \leq i \leq n$ , suppose the only  $*$  in this row is in the  $d$ -th column ( $1 \leq d \leq 2(l+t)$ ), let  $S_{i,d}$  be the weighted value of  $*$ .  $S_{i,d} = P_w(r_i) \times 1 + P_b(r_i) \times 0$ , where  $P_w(r_i)$  (resp.  $P_b(r_i)$ ) is the probability of setting the value of  $*$  to 1 (resp. 0) if the pixel in the  $i$ -th meaningful image that has the color intensity with respect to primary color  $X$  falls in Group  $r_i$  ( $0 \leq r_i \leq M_{i_X} - 1$ ). Note that  $P_w(r_i) + P_b(r_i) = 1$ . Let  $S_{i,j}$  be the value of the  $j$ -th ( $1 \leq j \leq 2(l+t)$ ) element in the  $i$ -th row of  $B^0 \circ A_c \circ B^1 \circ A_c$  where  $j \neq d$ . Let  $CI_{EVCS}(r_i) = \sum_{j=1}^{d-1} P'_j(r) \times S_{i,j} + P'_d(r) \times$



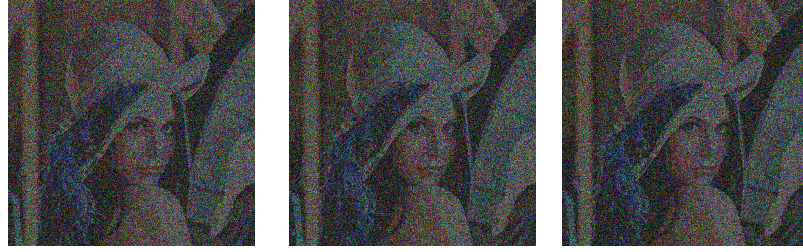


Figure 4.9: The Superimposed Images of the First and the Second Shares, the First and the Third Shares and the Second and the Third Shares

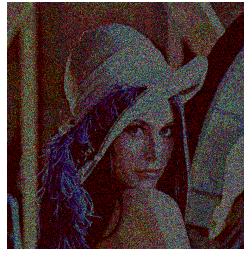


Figure 4.10: The Superimposed Image of the Three Shares

$S_{i,d} + \sum_{j=d}^{2(l+t)} P'_j(r) \times S_{i,j}$  be the weighted intensity corresponding to primary color  $X$  when the pixel is from the  $i$ -th share, given the pixel in the  $i$ -th meaningful image that has the color intensity with respect to primary color  $X$  falls in the Group  $r_i$ .

**Definition** A  $k$ -out-of- $n$  EVCS for color images is secure if the following conditions are met:

1. For any  $q$  shares such that  $q \geq k$  and for any two pixels of the original secret image in different intensity group with respect to a primary color  $X \in \{R, G, B\}$ , namely  $r$  and  $r'$  such that  $0 \leq r, r' \leq N_X - 1$  and  $r \neq r'$ , we have  $|CI_{EVCS}(q, r) - CI_{EVCS}(q, r')| \geq \alpha_F$  where  $\alpha_F > 0$ .
2. For any  $q$  shares such that  $q < k$  and for any two pixels of the original secret image in different intensity group with respect to a primary color  $X \in \{R, G, B\}$ ,

namely  $r$  and  $r'$  such that  $0 \leq r, r' \leq N_X - 1$  and  $r \neq r'$ , we have  $|CI_{EVCS}(q, r) - CI_{EVCS}(q, r')| = 0$ .

3. For any two pixels of the  $i$ -th ( $1 \leq i \leq n$ ) share in different intensity group with respect to a primary color  $X \in \{R, G, B\}$ , namely  $r_i$  and  $r'_i$  such that  $0 \leq r_i, r'_i \leq M_{i_X} - 1$  and  $r \neq r'$ , we have  $|CI_{EVCS}(r_i) - CI_{EVCS}(r'_i)| \geq \alpha_S$  where  $\alpha_S > 0$ .

The values  $\alpha_F$  and  $\alpha_S$  are referred to as relative differences of the reconstructed image and the shares, respectively. The first condition states that by superimposing any  $q$  ( $q \geq k$ ) shares, the secret image can be correctly recovered. The second condition implies that no information of the secret image is gained if less than  $k$  shares are obtained. The third condition of implies after coding the meaningful images into shares, they are still recognizable.

**Theorem 4.3.1** *Our  $k$ -out-of- $n$  EVCS is a valid scheme with  $\alpha_F = \alpha \times P_1 / (N_X - 1)$  and  $\alpha_S = (1 - P_1) / (t \times (M_{i_X} - 1))$  where  $P_1$  is the trade-off probability and  $0 \leq P_1 \leq 1$  ( $\alpha$  is the contrast parameter of a  $k$ -out-of- $n$  black-and-white VCS).*

**Proof** From the definition of a valid black-and-white VCS, the Basic Matrices of a  $k$ -out-of- $n$  black-and-white VCS  $B^0$  and  $B^1$  should meet the following conditions:

- For  $B^0$ , the bitwise OR result denoted by  $V_0$  of any  $k$  of the  $n$  rows satisfies that  $H(V_0) \leq d - \alpha l$ , for some  $1 \leq d \leq l$  and  $\alpha > 0$ ;
- For  $B^1$ , the bitwise OR result denoted by  $V_1$  of any  $k$  of the  $n$  rows satisfies that  $H(V_1) \geq d$ ;

- The bitwise OR result denoted by  $V$  of any less than  $k$  of the  $n$  rows satisfies that  $H(V)$  is the same for both  $B^0$  and  $B^1$ .

For the first condition: let the bitwise OR result of any  $k$  of the  $n$  rows of  $A_c$  denoted by  $H(A_c)$ ,

$$CI_{EVCS}(k, r) = P_1/l \times \frac{r}{N_X-1} \times H(V_0) + (1 - P_1)/t \times \frac{r}{N_X-1} \times H(A_c) \\ + P_1/l \times (1 - \frac{r}{N_X-1}) \times H(V_1) + (1 - P_1)/t \times (1 - \frac{r}{N_X-1}) \times H(A_c). \\ |CI_{EVCS}(k, r) - CI_{EVCS}(k, r')| = |\alpha \times P_1 \times (r' - r)/(N_X - 1)| > 0. |r' - r| \geq 1, \text{ thus} \\ \alpha_F = \alpha \times P_1/(N_X - 1).$$

For the second condition: according to the third condition of  $k$ -out-of- $n$  black-and-white VCS,

$$|CI_{EVCS}(q, r) - CI_{EVCS}(q, r')| = |(H(V) - H(V))/l \times P_1 \times (r' - r)/(N_X - 1)| = 0 \\ (q < k).$$

For the third condition: Since each row of  $A_c$  has only one \*, we have

$$|CI_{EVCS}(r_i) - CI_{EVCS}(r'_i)| = |(1 - P_1)/t \times (r'_i - r_i)/(M_{i_X} - 1)| > 0. |r'_i - r_i| \geq 1, \text{ thus } \alpha_S = (1 - P_1)/(t \times (M_{i_X} - 1)).$$

## 4.4 Summary

In this chapter, we have proposed a  $k$ -out-of- $n$  EVCS for color images which satisfies the four properties listed in Chap. 1. We elaborated the four steps, namely, Histogram Generation, Color Quality Determination, Group and Share Creation, along with an example. We also defined a valid  $k$ -out-of- $n$  EVCS for color images and prove our scheme is a valid one.

## Chapter 5

# Determining the Number of Color Levels and Grouping Method

In Sec. 3.2.2 and Sec. 4.1.2, we let the user determine the number of color levels for reconstructed image and share images. In Sec. 5.1, we provide more discussions on how to choose the number of color levels. Additionally, we introduce another grouping method which can be applied to our VCS and EVCS. We further discuss the reason why we choose the grouping method used in Sec. 3.2.3 and Sec. 4.1.3 in our schemes.

### 5.1 Color Level Determination

In this section, we discuss how to choose the number of color levels (i.e.  $N = N_R \times N_G \times N_B$ ) in the reconstructed secret image or the share images. As the schemes allow a user to arbitrarily choose the number of color levels, we observe that the number of color levels has a significant impact on the quality of images. The number of color

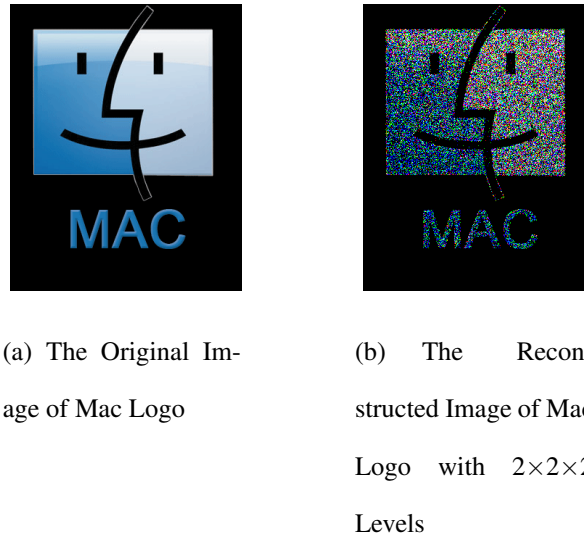


Figure 5.1: The Image of Mac Logo

levels should be chosen depending on the number of colors of the original images.

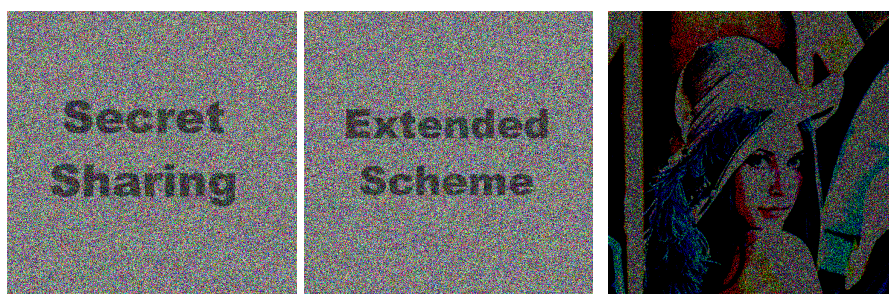
In order to get good quality of an image, when doing the secret sharing on each primary color of the image, we classify them into two categories by the number of levels on the primary color. In category 1, the number of levels on the primary color is less than 4. In category 2, the number of levels on the primary color is more than or equal to 4.

For the images with the primary color in category 1, our scheme with  $N$  levels can be directly used. Since the number of levels on the primary color of original image is small, there is no need to try our scheme with different levels any more. Text and logos might be in this category. Fig. 5.1 shows the original image and reconstructed image of Mac Logo by using our VCS scheme with  $2 \times 2 \times 2$  levels. Fig. 5.2(a) shows the meaningful images (text), the corresponding shares and the reconstructed image by using our EVCS scheme with  $2 \times 2 \times 2$  levels (the secret image is Lena).

For the images with the primary color in category 2, we suggest the user try our

## **Secret**      **Extended** **Sharing**    **Scheme**

(a) The Original Images of Text



(b) The Corresponding Shares of Text with  $2 \times 2 \times 2$  levels

(c) The Reconstructed Image of the Two Shares of Text

Figure 5.2: The Image of Text

scheme with  $2 \times 2 \times 2$  levels,  $4 \times 4 \times 4$  levels and  $N$  levels respectively. Then based on the results, user could choose one scheme with optimal quality of reconstructed image or share image. Photos of portrait, landscape or cartoons might be in this category.



Figure 5.3: The Original Image of Alice

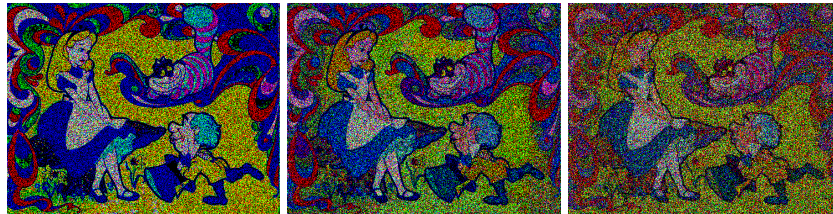


Figure 5.4: The Reconstructed Images of Alice with  $2 \times 2 \times 2$ ,  $4 \times 4 \times 4$ ,  $N \times N \times N$  Levels

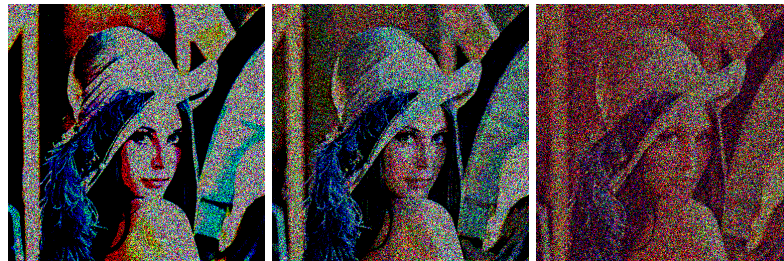


Figure 5.5: The Reconstructed Images of Lena with  $2 \times 2 \times 2$ ,  $4 \times 4 \times 4$ ,  $N \times N \times N$  Levels

In Fig. 5.4 we can see that the reconstructed image of “Alice in the Wonderland” (Fig. 5.3) with  $2 \times 2 \times 2$  levels has the sharpest image but limited number of colors, while the  $N_R \times N_G \times N_B$  (where in “Alice in the Wonderland”,  $N_R=256$ ,  $N_G=255$ ,  $N_B=256$ )





Figure 5.6: The Original Image of F22-raptor

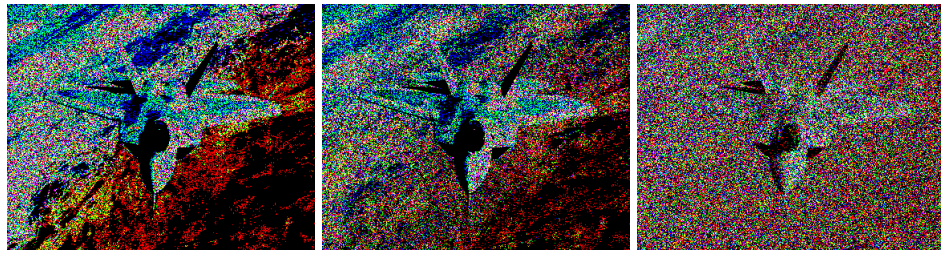


Figure 5.7: The Reconstructed Images of F22-raptor with  $2 \times 2 \times 2$ ,  $4 \times 4 \times 4$ ,  $N \times N \times N$  Levels

level image has the same number of colors as the original one but looks blurry. The image with  $4 \times 4 \times 4$  shows relatively better quality with abundant colors and clear figure. Fig. 5.5 and Fig. 5.7 show similar results with Fig. 5.4. Fig. 5.10 shows the two shares (Sailboat and Peppers) of a 2-out-of-2 EVCS and Fig. 5.11 is the reconstructed image (Lena),  $N_R=N_G=N_B=M_{i_R}=M_{i_G}=M_{i_B}=4$  (where  $1 \leq i \leq 2$ ).

Fig. 5.9 shows the reconstructed image of Gray (21-level) (Fig. 5.8) by applying our scheme with 4 levels and  $N_X$  levels respectively (Note that in this case, the value of  $RGB$  components are the same on every pixel, so the scheme with level number  $N_R \times N_G \times N_B$  is actually the scheme with the level number  $N_X$ ). The user can observe the gradual change of the color by choosing the  $N_X$  level scheme so that the reconstructed image is closest to the original one. Gray (21-level) image with  $N_X$  levels gives the details of gradual change while Gray (21-level) image with 4 levels doesn't.



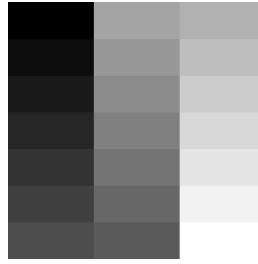


Figure 5.8: The Original Image of Gray(21-level)

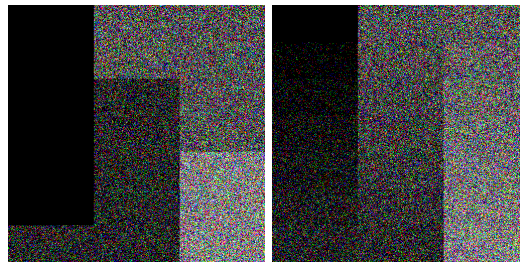


Figure 5.9: The Reconstructed Images of Gray(21-level) with 4 and  $N$  Levels



Figure 5.10: The Two Shares Corresponding to Sailboat and Peppers.

## 5.2 Grouping Method

In Chap. 3 and Chap. 4, we group pixels of image by making sure each group contains the same number of pixels. In this section, we emphatically discuss another grouping method which can be used in our VCS and EVCS schemes. In the following, we use grouping pixels in the secret image as an example to illustrate this method.

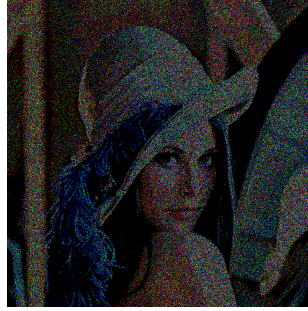


Figure 5.11: The Superimposed Image of the Two Shares Corresponding to Sailboat and Peppers.

In this method, for each primary color  $X \in \{R, G, B\}$ , the horizontal coordinate of the histogram of  $X$  is equally partitioned, namely, each pixel is in one of the following groups:  $[0, 255/N_X)$ ,  $[255/N_X, 255 \times 2/N_X)$ ,  $\dots$ ,  $[255 \times (N_X - 1)/N_X, 255]$ . Fig. 5.12 shows the histograms of  $R$ ,  $G$  and  $B$  of Lena after grouping the pixels into four groups by using this grouping method. We use different color intensities to distinguish different groups. Normally, the number of pixels in each group is different.

This method does not need to scan the color intensities for the RGB components of each pixel in the original image. Differing from the grouping method we described in Sec. 3.2.3 and Sec. 4.1.3, the color intensity distribution of the original image has nothing to do with how we group pixels. From Fig. 5.12, we can see that most of the pixels of Lena on the primary color blue are grouped into the second group. These pixels will show no difference in the reconstructed image with respect to  $B$  component.

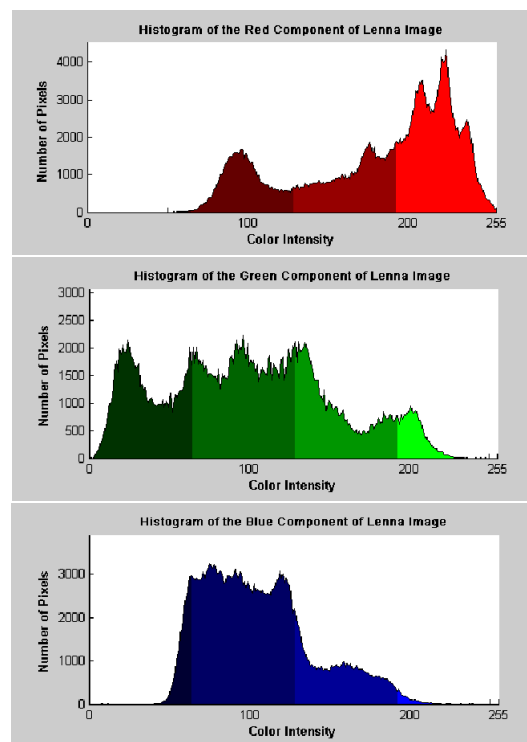


Figure 5.12: Histogram with  $4 \times 4 \times 4$  by the Candidate Method

# Chapter 6

## Comparison

In this chapter, we compare our VCS with other VCS schemes (namely, Naor-Shamir [27], Hou [16], Yang [38], Chan [10], Hou and Tu [17], Shyu [30], Chen et al. [11] and Yang-chen [40] VCS schemes) in five aspects and compare our EVCS with other EVCS schemes (namely, Ateniese et al. [4], Nakajima and Yamaguchi [26], Sirhindi et al. [32] and Wang et al. [36] EVCS schemes) in six aspects.

### 6.1 VCS Schemes

In this section, we compare our VCS with other eight schemes which are Naor-Shamir [27] (the first VCS), Hou [16] (the first colored scheme), Yang [38] (using probabilistic method for gray images), Chan [10] (no pixel expansion for gray images), Hou and Tu [17] (no pixel expansion for colored images), Shyu [30] (supporting  $k$ -out-of- $n$  threshold setting), Chen et al. [11] (multiple-level and with no pixel expansion for gray images) and Yang-Chen [40] (using probabilistic method for colored images) visual

cryptography schemes in five aspects showed in the first row. Table. 6.1 summarizes the

Table 6.1: Comparison of VCS schemes

	Colored	Expansion rate	General	Level	Tunable
NS [27]	B/W	$m_1$	✓	2 levels	
Hou [16]	✓	4	k=n	8 levels	
Yang [38]	B/W	1	✓	2 levels	
Chan [10]	Gray	1	k=n=2	2 levels	
HT [17]	✓	1	✓	2 levels	
Shyu [30]	✓	$\log_2 C \cdot l$	✓	multi	
Chen [11]	Gray	1	k=n	multi	
YC [40]	✓	3	✓	multi	
Our scheme	✓	1	✓	multi	✓

nine VCS schemes ( $C$  is the number of colors;  $l$  is the pixel expansion rate of a black-and-white VCS; and  $m_1 > 1$ ). The first row of the table is the five objectives of VCS (dealing with colored images, no pixel expansion, proposed general  $k$ -out-of- $n$  scheme, no color level limitation of original image and tunable).

Compared with other visual cryptography schemes, our new scheme allows user to deal with colored image and determine the color number of reconstructed image according to the expected quality of it. Besides, our scheme does not need to do the dithering, which would degrade the quality of reconstructed image, but still has no pixel expansion. In the following, we mainly compare our scheme with Chen's [11] and Yang-

Chen's [40] schemes since the former meets the requirement of no pixel expansion and the latter employs a probabilistic method which is also used in our scheme.

Chen's scheme, which can only deal with gray level image, maps a block in a secret image to one corresponding equal-sized block in each share image so that there is no image size expansion. In this case, a block of pixels, instead of one pixel, are encrypted each time. They do secret sharing based on the average color intensity of the block. And the number of levels depends on the size of a block. The larger the block is, the more levels the reconstructed image has. However, more levels also means they do secret sharing based on the average color intensity of more pixels. It makes the quality of the original image degrade. For example, 3-level scheme requires the block size of 4 ( $2 \times 2$ ) and 9-level scheme requires the block size of 16 ( $4 \times 4$ ). In a word, the block size grows as the number of levels grows. In our new scheme, we do secret sharing pixel by pixel so no average value of color intensity is required. Consequently, our scheme improves the quality of reconstructed image. Fig. 6.1 shows the original image of Lena (gray) image and the image of which the original block ( $4 \times 4$ ) is replaced by an equal-sized block and the color of each pixel is set to the average color intensity of the original block. Fig. 6.2 shows the 9-level superimposed image of Lena by Chen's scheme and our scheme .

Yang's scheme [40] for color images also uses the probabilistic method and it encrypts one pixel each time. Besides, this method has a fixed number of pixel expansion (3) which has nothing to do with the values of  $k$  and  $n$ . Compared with our scheme, Yang's scheme can not improve the color contrast of reconstructed image by determining its levels but can by modifying the number of levels of original image. In our scheme, the original image does not need to be modified before doing secret sharing, so it is more convenient and flexible.

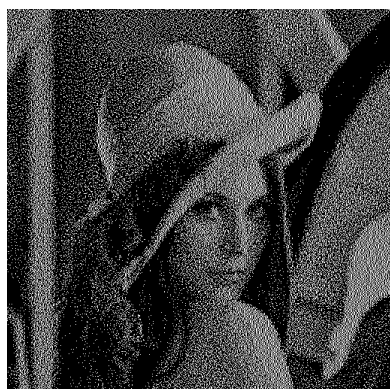


(a) The Original Image of Lena (Gray)

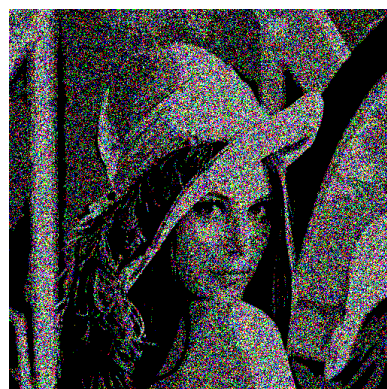


(b) Lena (Gray) Image After Block Averaging with Block Size 16

Figure 6.1: The Image of Lena (Gray)



(a) The Superimposed Image of Lena (Gray) by Chen's(9-level)



(b) The Superimposed Image of Lena (Gray) by Our Schemes with  $4 \times 4 \times 4$  Levels

Figure 6.2: The Superimposed Image of Lena (Gray)

## 6.2 EVCS Schemes

In this section, we compare our  $k$ -out-of- $n$  color EVCS with four other EVCS schemes: Ateniese et al. [4] (the first EVCS), Nakajima and Yamaguchi [26] (EVCS for color images), Sirhindi et al. [32] (pixel expansion rate = 9) and Wang et al. [36]. Table 6.2 shows the comparison with respect to six properties: supporting color images, without pixel expansion, supporting general  $k$ -out-of- $n$  threshold setting, no limitation on the number of color levels of the original image, a trade-off between the shares and the reconstructed image in terms of quality and tunable (which means users can determine the number of colors of the shares and the reconstructed image). To the best of our knowledge, the EVCS proposed in this paper is the only one that satisfies all the six properties.

Table 6.2: Comparison of EVCS schemes

	Colored	No Expansion	General	Level	Trade-off	Tunable
Ateniese [4]	B/W	×	✓	2 levels	✓	×
NY [26]	✓	×	$k = n = 2$	8 levels	×	×
Sirhindi [32]	✓	×	$k = n = 2$	multi	×	×
Wang [36]	✓	×	✓	multi	×	×
Our scheme	✓	✓	✓	multi	✓	✓

In the following, we further compare our scheme with Ateniese et al.'s [4], Nakajima and Yamaguchi's [26], Sirhindi et al.'s [32] and Wang et al.'s [36].



Ateniese et al. [4] proposed the first EVCS scheme for black-and-white images in 1996. A  $q$ -coloring of the hypergraph is used to construct an  $n \times q$  matrix  $D$  which is then concatenated with the  $n \times l$  Basic Matrices of a black-and-white VCS scheme. The pixel expansion is  $l + \lceil \frac{n}{k-1} \rceil$  where  $l$  is the pixel expansion of a black-and-white VCS scheme. The problem of pixel expansion will become prominent, if  $n$  is much greater than  $k$ . For example, if  $k=2$  and  $n=10$ , the pixel expansion rate of the 2-out-of-10 EVCS scheme is  $l + \lceil \frac{n}{k-1} \rceil = 10 + 10 = 20$  (suppose they use Naor-Shmair black-and-white VCS).

Nakajima and Yamaguchi [26] extended Ateniese et al. EVCS so that it can encrypt natural images. They applied halftoning techniques to transform a pixel in grayscale image to several black-and-white subpixels. Then the Basic Matrices for 2-out-of-2 threshold setting are constructed. Their EVCS scheme is one of the first sets of EVCS schemes that can deal with grayscale and color images. Besides the pixel expansion, it has the limitation of not supporting the general  $k$ -out-of- $n$  construction.

Sirhindi et al. EVCS scheme [32] improves the pixel expansion factor compared to other colored EVCS schemes. In [32], the pixel expansion factor is fixed on 9 for a color space as large as comprising  $2^{24}$  colors. However, in order to achieve losslessness, the reconstructed image should not be obtained by only superimposing the shares. An extra recovery technique is required. In addition, it only provided the solution of 2-out-of-2 EVCS scheme.

Wang et al. [36] proposed EVCS schemes for black-and-white, grayscale and colored images. Their EVCS scheme for black-and-white images uses a different method for constructing the Basic Matrices from Ateniese et al.'s, but has the same result. All the proposed EVCS schemes have pixel expansion.

Compared with other EVCS schemes, ours supports the general  $k$ -out-of- $n$  threshold setting and has no pixel expansion. Moreover, our EVCS scheme allows user to handle colored images. And according to the expected quality of them, users can also determine the color number of reconstructed image and shares.

## Chapter 7

### Conclusion and Future Work

In this thesis, we have a brief overview of the development and the applications of cryptography in Chap. 1. We also describe one branch of cryptography - secret sharing. Based on secret sharing, the  $k$ -out-of- $n$  threshold VCS and EVCS are introduced. We then take several examples to discuss how VCS and EVCS work and list four commonly desirable properties which should be satisfied by VCS and EVCS. In Chap. 2, we review the related literature on black-and-white VCS, gray-scale VCS, colored VCS and EVCS schemes. Through the discussion of their features, we present the merits and demerits of them.

In Chap. 3 and Chap. 4, we propose a new  $k$ -out-of- $n$  color VCS and a new  $k$ -out-of- $n$  color EVCS without pixel expansion and provide the security analysis for them. Our new VCS and EVCS schemes satisfy the following properties:

- (1) supporting images of arbitrary number of colors;
- (2) no pixel expansion;

- (3) supporting  $k$ -out-of- $n$  threshold setting;
- (4) a “tunable” number of color levels in the secret share creation process.

According to our experimental results, we demonstrate that our schemes are the first ones that achieve all these desirable properties. And they can provide one of the best reconstructed images and share images in quality due to the “tunable” feature in the secret share creation step. We discuss how to determine the number of color levels in Chap. 5. Another grouping method is also introduced in this Chapter. By comparing this grouping method with the one in our VCS and EVCS, we show that ours is better. In Chap. 6, we compare our VCS with eight other schemes in five aspects and compare our EVCS with four EVCS schemes in six aspects. The results show that our schemes are optimal.

To improve the contrast of the reconstructed image or meaningful shares, we let the user determine the number of color levels of them. One scheme with certain levels is chosen depending on the quality of the reconstructed image or meaningful shares. This procedure relies on visual inspection of human. Our future work is to derive a numerical measure that accurately measures the quality of images. Our scheme with certain levels can be automatically chosen without the determination of users.

## **List of Publications**

1. Xiaoyu Wu, Duncan S. Wong and Qing Li, Extended visual cryptography scheme for color images with no pixel expansion, International Conference on Security and Cryptography, Athens, Greece, July 26 - 28, 2010.
2. Xiaoyu Wu, Duncan S. Wong and Qing Li, Threshold visual cryptography scheme for color images with no pixel expansion, International Symposium on Computer Science and Computational Technology , pp. 310 - 315, Huangshan, China, Dec 26 - 28, 2009.

# Bibliography

- [1] A. Adhikari, T. K. Dutta, and B. Roy. A new black and white visual cryptographic scheme for general access structures. In *Progress in Cryptology - INDOCRYPT 2004*, pages 399–413, 2004. Lecture Notes in Computer Science, Vol. 3348.
- [2] G. Alvarez, L. H. Encina, and A. M. del Rey. A multisecret sharing scheme for color images based on cellular automata. *Information Sciences*, 178:4382–4395, 2008.
- [3] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson. Visual cryptography for general access structures. *Inf. Comput.*, 129(2):86–106, 1996.
- [4] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson. Extended capabilities for visual cryptography. *Theor. Comput. Sci.*, 250(1-2):143–161, 2001.
- [5] I. Biehl and S. Wetzel. Traceable visual cryptography. *Information and Communications Security*, pages 61–71, 1997.
- [6] C. Blundo, A. D. Bonis, and A. D. Stantis. Improved schemes for visual cryptography. *Designs, Codes and Cryptography*, 24(3):255–278, 2001.
- [7] C. Blundo, P. D’Arco, A. D. Santis, and D. R. Stinson. Contrast optimal threshold visual cryptography schemes. *SIAM J. Discrete Math.*, 16(2):224–261, 2003.

- [8] C. Blundo and A. D. Santis. Visual cryptography schemes with perfect reconstruction of black pixels. *Computers and Graphics*, 22(4):449–455, August 1998.
- [9] C. Blundo, A. D. Santis, and D. R. Stinson. On the contrast in visual cryptography schemes. *J. Cryptology*, 12(4):261–289, 1999.
- [10] C. S. Chan, Y.-W. Liao, and J.-C. Chuang. Visual secret sharing techniques for gray-level image without pixel expansion technology. *Journal of Information, Technology and Society*, 95(1), 2004.
- [11] Y.-F. Chen, Y.-K. Chan, C.-C. Huang, M.-H. Tsai, and Y.-P. Chu. A multiple-level visual secret-sharing scheme without image size expansion. *Information Sciences*, 177(21):4696–4710, November 2007.
- [12] S. Cimato, R. D. Prisco, and A. D. Santis. Colored visual cryptography without color darkening. *Theoretical Computer Science*, 374:261–276, 2007.
- [13] S. Cimato, A. D. Santis, A. L. Ferrara, and B. Masucci. Ideal contrast visual cryptography schemes with reversing. *Information Processing Letters*, 93(4):199 – 206, February 2005.
- [14] P. A. Eisen and D. R. Stinson. Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels. *Des. Codes Cryptography*, 25(1):15–61, 2002.
- [15] J. Feng, H. Wu, C. Tsai, Y. Chang, and Y. Chu. Visual secret sharing for multiple secrets. *Pattern Recognition*, 41:3572–3581, 2008.
- [16] Y. C. Hou. Visual cryptography for color images. *Pattern Recognition*, 36:1619–1629, 2003.

- [17] Y. C. Hou and S. F. Tu. A visual cryptographic technique for chromatic images using multi-pixel encoding method. *Journal of Research and Practice in Information Technology*, 37(2):179–191, May 2005.
- [18] D. Jin, W. Yan, and M. S. Kankanhalli. Progressive color visual cryptography. *Journal of Electronic Imaging*, 14(3):033019–1–033019–13, 2005.
- [19] B. W. Leung, F. Y. Ng, and D. S. Wong. On the security of a visual cryptography scheme for color images. *Pattern Recognition*, 42(5):929–940, May 2009.
- [20] C.-C. Lin and W.-H. Tsai. Visual cryptography for gray-level images by dithering techniques. *Pattern Recognition Letters*, 24(1-3):349–358, 2003.
- [21] P. Lin, J. Lee, and C. Chang. Distortion-free secret image sharing mechanism using modulus operator. *Pattern Recognition*, 42:886–895, 2009.
- [22] C. L. Liu. *The Introduction to Combinatorial Mathematics*. Mcgraw-Hill, 1968.
- [23] R. Lukac and K. N. Plataniotis. Bit-level based secret sharing for image encryption. *Pattern Recognition*, 35(5):767–772, 2005.
- [24] R. Lukac and K. N. Plataniotis. A cost-effective encryption scheme for color images. *Real-Time Imaging*, 11:454–464, 2005.
- [25] R. Lukac, K. N. Plataniotis, B. Smolka, and A. N. Venetsanopoulos. A new approach to color image secret sharing. In *European Signal Processing Conference (EUSIPCO 2004)*, pages 1493–1496, 2004.
- [26] M. Nakajima and Y. Yamaguchi. Extended visual cryptography for natural images. *Journal of WSCG*, 10(2):303–310, 2002.



- [27] M. Naor and A. Shamir. Visual cryptography. In *Advances in Cryptology - EUROCRYPT '94*, pages 1–12, 1994. Lecture Notes in Computer Science, Vol. 950.
- [28] M. Naor and A. Shamir. Visual cryptography II: Improving the contrast via the cover base. In *International Workshop on Security Protocols*, pages 197–202, 1996. Lecture Notes in Computer Science, Vol. 1189.
- [29] A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, Nov. 1979.
- [30] S. J. Shyu. Efficient visual secret sharing scheme for color images. *Pattern Recognition*, 39(5):866–880, 2006.
- [31] S. J. Shyu, S.-Y. Huang, Y.-K. Lee, R.-Z. Wang, and K. Chen. Sharing multiple secrets in visual cryptography. *Pattern Recognition*, 40:3633–3651, 2007.
- [32] R. Sirhindi, M. Afzal, and S. Murtaza. An extended secret sharing scheme for colour images with fixed pixel expansion. *International Journal of Electronic Security and Digital Forensics*, 2(1):58–67, 2009.
- [33] W. Tzeng and C. Hu. A new approach for visual cryptography. *Designs, Codes and Cryptography*, 27(3):207–227, 2002.
- [34] M. Uno and M. Kano. Visual secret sharing schemes with cyclic access structure for many images. In *Information Security and Cryptology (ICISC 2008)*, pages 84–97, 2009. Lecture Notes in Computer Science, Vol. 5461.
- [35] E. Verheul and H. van Tilborg. Construction and properties of  $k$  out of  $n$  visual secret sharing schemes. *Designs Codes Cryptogr.*, (11):179–196, 1997.

- [36] D. Wang, F. Yi, and X. Li. On general construction for extended visual cryptography schemes. *Pattern Recognition*, 42(11):3071–3082, 2009.
- [37] C. Yang and C. Lai. New colored visual secret sharing schemes. *Designs, Codes and Cryptography*, 20(3):325–336, 2000.
- [38] C. N. Yang. New visual secret sharing schemes using probabilistic method. *Pattern Recognition Letters*, 25(4):481–494, March 2004.
- [39] C. N. Yang and T. S. Chen. Reduce shadow size in aspect ratio invariant visual secret sharing schemes using a square block-wise operation. *Pattern Recognition*, 39(7):1300–1314, 2006.
- [40] C. N. Yang and T. S. Chen. Colored visual cryptography scheme based on additive color mixing. *Pattern Recognition*, 41(10):3114–3129, 2008.
- [41] R. Zhao, J. Zhao, F. Dai, and F. Zhao. A new image secret sharing scheme to identify cheaters. *Computer Standards and Interfaces*, 31:252–257, 2009.