

Improved Visual Cryptography Schemes Without Image Size Expansion

by

©Nazanin Askari

A Thesis submitted to the
School of Graduate Studies
in partial fulfillment of the
requirements for the degree of

Master of Engineering

Faculty of Engineering and Applied Science

Memorial University of Newfoundland

September, 2012

St. John's

Newfoundland

Abstract

Over the past few years, increasing concern about the privacy of information shared in computer systems has increased interest in data security. Visual cryptography is a secure secret sharing scheme that divides secret images into shares which on their own reveal no information of the original secret. Recovery of the secret image can be performed by superimposing the shares using transparencies. Hence, the process does not require any special software or hardware for cryptographic computations and the decoding process is done by human visual system.

In the application of visual cryptography, pixel expansion and contrast are two primary issues. Pixel expansion can result in many problems such as the problem of image distortion and the requirement of more storage space. In addition to the problem of pixel expansion, loss of contrast is also a problem for visual cryptography. Since the secret is recovered visually, making a good visual effect is as important as keeping the image size invariant. A few studies pay attention to solving the problem of pixel expansion; however, such schemes may not be suitable because the visual effect of the recovered image is poor.

In this research, we propose a novel visual secret sharing scheme for sharing one secret image. The purpose of the proposed method is to solve a problem of pixel expansion and generate a recovered image such that its visual quality is very similar to the original secret image. Our proposed non-expansion scheme is perfectly secure

and experimental results show that it provides better contrast and visual quality of the recovered image in comparison with previous non-expansion visual cryptography schemes.

Furthermore, we extend our research to find a solution to deal with the problem of pixel expansion and the visual quality of the recovered images for advanced schemes such as multiple image visual cryptography and extended visual cryptography. This is done by using algorithms that process the original secret image prior to applying the visual cryptography schemes. The resulting recovered images in a multiple image visual cryptography scheme and the share images in an extended visual cryptography scheme are significantly visually improved over other approaches. The improvement in visual quality is particularly critical for halftoned images which are derived originally from grayscale images. Three novel methods are proposed to improve the visual quality of the recovered share images when using grayscale secret images.

Acknowledgements

First of all, I would like to express my sincere gratitude to my supervisors, Prof. Howard Heys and Prof. Cecilia Moloney, for their financial support and guidance from the very early stage of this research. Their positive attitude, encouragement and scientific reviewing made me more confident to carry out my research successfully. I am really grateful to them.

I would like to thank to all the members of the Computer Engineering Research Lab (CERL) at Memorial University. Moreover, I would like to thank my friends Hanif Sedighnejad and Nima Khakzad for their kind help and suggestions.

Finally, my deepest gratitude goes to my family for their unflagging love, support and encourage throughout my whole life. This work would not have been completed without them; I dedicate this thesis to my mother.

Table of Contents

Abstract	ii
Acknowledgments	iv
Table of Contents	vii
List of Tables	viii
List of Figures	xii
1 Introduction	1
1.1 Background	1
1.2 Motivation	3
1.3 Purpose	7
1.4 Outline of Thesis	8
2 Review of Visual Cryptography Schemes	10
2.1 Introduction	10
2.2 Basic Definitions	10
2.3 (2, 2) Visual Cryptography Scheme	11
2.4 Multiple Image Visual Cryptography	17
2.5 Extended Visual Cryptography	19

2.6	Visual Cryptography Schemes Without Pixel Expansion	23
2.6.1	Introduction	23
2.6.2	Probabilistic scheme	23
2.6.3	Chou's Non-Expansion VCS	25
2.6.4	MLVSS Scheme Without Image Size Expansion	27
2.7	Grayscale Images and Halftoning	28
2.8	Conclusion	30
3	Visual Cryptography Without Image Size Expansion	31
3.1	Introduction	31
3.2	A Novel (2, 2) Visual Cryptography Scheme Without Image Size Expansion	32
3.2.1	Description of the Scheme	33
3.2.2	Example	38
3.3	Security and Contrast Analysis	40
3.4	Numerical Experiment Results	42
3.5	Visual Experimental Results and Discussion	45
3.6	Conclusion	55
4	Processing Grayscale Secret Images for Use in Visual Cryptography	57
4.1	Introduction	57
4.2	Chou's Non-expansion Method	58
4.3	Random Conversion Method	61
4.4	Clustering and Thresholding Method	64
4.4.1	Void-and-Cluster Halftoning Method	65
4.4.2	Clustering and Constant Threshold Method	66
4.4.2.1	CCT Method	66

4.4.2.2	Example	67
4.4.2.3	Experimental Results	69
4.4.3	Clustering and Variable Threshold Method	71
4.4.3.1	CVT Method	71
4.4.3.2	Example	73
4.4.3.3	Experimental Results	73
4.5	Conclusion	76
5	Multiple Image VCS and Extended VCS Without Image Size Expansion	78
5.1	Introduction	78
5.2	Multiple Image Visual Cryptography Without Image Size Expansion	80
5.2.1	A New Scheme	80
5.2.2	Visual Experimental Results and Discussion	81
5.3	Extended Visual Cryptography Without Image Size Expansion	84
5.3.1	A New EVC Scheme	89
5.3.2	Visual Experimental Results and Discussion	89
5.4	Conclusion	90
6	Conclusions and Future Work	96
6.1	Conclusions	96
6.2	Future Work	98
	Bibliography	99

List of Tables

2.1	Illustration of a 2-out-of-2 secret image sharing scheme with 2 subpixels	12
2.2	Illustration of a (2, 2)-VCS with 4 subpixels	16
2.3	Illustration of multiple image VCS (Chen and Wu)	18
2.4	Illustration of probabilistic (2, 2)-VCS	25
2.5	Classification of Chou's scheme	27
2.6	A part of the MLVSS scheme without pixel expansion	28
3.1	Block models of the image	33
3.2	Mapping process	34
3.3	Proposed encoding process	35
3.3	Proposed encoding process	36
3.3	Proposed encoding process	37
3.3	Proposed encoding process	38
3.4	Comparison of secret block distributions (In number of 2×2 blocks)	42
3.5	Comparison of recovered image characteristics for halftoned Lena . .	44
3.6	Comparison of recovered image characteristics for binary fingerprint .	44
4.1	The block replacement process proposed by Chou	59
4.2	The block replacement process in random conversion method	62
5.1	Illustration of the (2, 2) multiple image VCS	82

List of Figures

1.1	Example of an application of visual secret sharing to biometric data .	4
2.1	(2, 2)-VCS with 2 subpixels: (a) secret Dancers image; (b) reconstructed Dancers image; (c) first share; (d) second share	14
2.2	Example of a (2, 2)-VCS with 4 subpixels:(a) secret Dancers image; (b) reconstructed Dancers image; (c) first share; (d) second share	17
2.3	Example of four possible patterns to be assigned in multiple secret sharing scheme for first share	18
2.4	Example of four possible patterns to be assigned in multiple secret sharing scheme for second share	18
2.5	Example of a multi-image VCS: (a) first secret image; (b) second secret image; (c) share A; (d) share B; (e) share C; (f) reconstructed secret 1; (g) reconstructed secret 2	20
2.6	Example of (2, 2)- extended visual cryptography scheme: (a) first cover image; (b) second cover image; (c) secret image; (d) extended share 1; (e) extended share 2; (f) recovered secret image	22
2.7	Example of probabilistic (2, 2)-VCS; (a) original secret image; (b) recovered image; (c) share 1; (d) share 2	26
2.8	Error filter	30

2.9	Image halftoning with Floyd-Steinberg method: (a) gray scale Lena; (b) halftoned Lena	30
3.1	Example of block selection	39
3.2	Example of mapping process	39
3.3	Secret images: (a) gray scale Lena; (b) halftoned Lena; (c) binary fingerprint	41
3.4	Probabilistic (2, 2) experimental results: (a) binary fingerprint; (b) recovered image; (c) share 1; (d) share 2	48
3.5	Probabilistic (2, 2) experimental results: (a) halftone Lena; (b) recov- ered image; (c) share 1; (d) share 2	49
3.6	Chou's (2, 2) experimental results: (a) binary fingerprint; (b) recovered image; (c) share 1; (d) share 2	50
3.7	Chou's (2, 2) experimental results: (a) halftone Lena; (b) recovered image; (c) share 1; (d) share 2	51
3.8	MLVSS (2, 2) experimental results: (a) halftone fingerprint; (b) recov- ered image; (c) share 1; (d) share 2	52
3.9	MLVSS (2, 2) experimental results: (a) halftone Lena; (b) recovered image; (c) share 1; (d) share 2	53
3.10	Proposed (2, 2) scheme experimental results: (a) binary fingerprint; (b) recovered image; (c) share 1; (d) share 2	54
3.11	Proposed (2, 2) scheme experimental results: (a) halftone Lena; (b) recovered image; (c) share 1; (d) share 2	55
4.1	Block replacement process in Chou's method: (a) halftoned Lena; (b) processed Lena; (c) halftoned baboon; (d) processed baboon	60

4.2	Block replacement process in random conversion method: (a) halftoned Lena; (b) processed Lena; (c) halftoned baboon; (d) processed baboon	64
4.3	Example of the block replacement process in CCT method	68
4.4	Block replacement process in CCT method: (a) halftoned Lena; (b) processed Lena; (c) halftoned baboon; (d) processed baboon	70
4.5	Example of the block replacement process in CVT method	75
4.6	Block replacement process in CVT method: (a) halftoned Lena; (b) processed Lena; (c) halfroned baboon; (d) processed baboon	76
5.1	Sample encoding/decoding process for multi-image VCS	83
5.2	Experimental results of multi-image VCS with Chou's method; (a) halftoned baboon; (b) halftoned Lena; (c) processed baboon; (d) processed Lena; (e) reconstructed baboon; (f) reconstructed Lena	85
5.3	Experimental results of multi-image VCS with random conversion block replacement method: (a) halftoned baboon; (b) halftoned Lena; (c) processed baboon; (d) processed Lena; (e) reconstructed baboon; (f) reconstructed Lena	86
5.4	Experimental results of multi-image VCS with CCT block replacement method: (a) halftoned baboon; (b) halftoned Lena; (c) processed baboon; (d) processed Lena; (e) reconstructed baboon; (f) reconstructed Lena	87
5.5	Experimental results of multi-image VCS with CVT block replacement method: (a) halftoned baboon; (b) halftoned Lena; (c) processed baboon; (d) processed Lena; (e) reconstructed baboon; (f) reconstructed Lena	88
5.6	Images used for EVCS: (a) halftoned boat; (b) halftoned baboon; (c) halftoned Lena	91

5.7	Experimental results of EVCS with Chou's method: (a) processed boat; (b) processed baboon; (c) processed Lena; (d) reconstructed Lena; (e) first cover image; (f) second cover image	92
5.8	Experimental results of EVCS with random conversion block replacement method: (a) processed boat; (b) processed baboon; (c) processed Lena; (d) reconstructed Lena; (e) first cover image; (f) second cover image	93
5.9	Experimental results of EVCS with CCT block replacement method: (a) processed boat; (b) processed baboon; (c) processed Lena; (d) reconstructed Lena; (e) first cover image; (f) second cover image	94
5.10	Experimental results of EVCS with CVT block replacement method: (a) processed boat; (b) processed baboon; (c) processed Lena; (d) reconstructed Lena; (e) first cover image; (f) second cover image	95

Chapter 1

Introduction

1.1 Background

Increasing access to the Internet and information resources has a great impact on our everyday lives and is making humans more dependent on computer systems and networks. However, this dependency has brought many threats to stored data and transmitted information. Therefore, information security has become one of the most important technologies and much research has been done to protect secret information and data in a computer systems.

Cryptography is a well-known approach to protect data by writing it in secret codes and transmitting it in a secure way. Historically, cryptography was used only for transmitting confidential messages. For example, the Caesar cipher is one of the oldest ciphers which replaces each original letter in the message by a letter which is three positions down alphabetically to encrypt the message [1]. This makes the secret message meaningless. The decryption process can be simply done by replacing the letters in reverse [1]. In all ciphers, there is a key that provides access to the secret information; thus, the key needs to be protected from being lost or destroyed. Over

the past few years, different cryptographic technologies have been introduced and the goal of all these cryptographic methods is to provide unbreakable algorithms with a secure key that can protect a secret from eavesdropping or other threats.

Secret sharing is a cryptographic method introduced by Blakley [2] and Shamir [3], which distributes secret information between several participants. The concept of a secret sharing scheme is to divide secret information into several pieces called shares, each of these shares having no information on its own of the secret. However, combining the qualified shares reveals the secret. For example, when the owner of the secret information does not trust any single person to transmit a secret, secret-sharing methods are a secure technique for transmitting secret data.

In 1994, visual cryptography was introduced by Naor and Shamir [4]. Visual cryptography is a type of secret sharing scheme that encodes secret messages in a format of black and white (or binary) secret images. A binary image can be divided into shares such that, while the shares are meaningless images, the secret image can be recovered visually by superimposing the share images together. Recently, visual cryptography and its applications have become an interesting research topic for two main reasons. The first is that visual cryptography provides perfect security [4]. Thus, it is impossible to get any information about the secret unless all the qualified shares are stacked together to reveal the secret. The other notable feature is its decoding process. This decoding process does not require any special software or hardware for cryptographic computations and it uses only the human visual system to identify the secret from the reconstructed image [5]. Based on these two characteristics, visual cryptography is a very secure and convenient way to protect and transmit secret information.

Visual cryptography also has application in biometrics. For example, biometric authentication systems are widely accepted in various applications such as in iden-

tification based systems and access control, ID cards, banking, etc. Therefore data accuracy and confidentiality in such applications should be guaranteed [6]. Biometrics is a science that uses unique physical characteristics (such as fingerprints, iris, retina, face and hand geometry) or behavioural characteristics (such as voice, signatures, and keystrokes) for the purpose of identification and authentication [7]. Using biometric methods has significant advantages over traditional password authentication systems [8][9]. For example, passwords can be forgotten, stolen or shared. Also simple passwords are easy to guess and complex passwords are hard to remember. Hence biometric traits can be more reliable. In addition, it is difficult to forge biometrics because the presence of an eligible user is required for authentication. But, there are some difficulties in biometric authentication. Biometric data is not secret and often this data can be changed according to the physical or emotional conditions of an owner at the time of authentication [7].

Visual cryptography is a suitable method that can be used in order to increase the level of information security and user authentication. Figure 1.1 provides an example of an application of visual cryptography. For example, biometric data such as a fingerprint image, a face image or a signature can be divided into several share images. To enhance security, each of the shares are distributed individually and the secret information is revealed after stacking the corresponding shares together.

1.2 Motivation

The basic model of a visual cryptography scheme (VCS), known as traditional visual cryptography, can be described by the basic 2-out-of-2 visual cryptography scheme [10]. In this scheme, Naor and Shamir assumed that the secret message (image) is a collection of binary 1's and 0's displayed as black and white pixels, re-

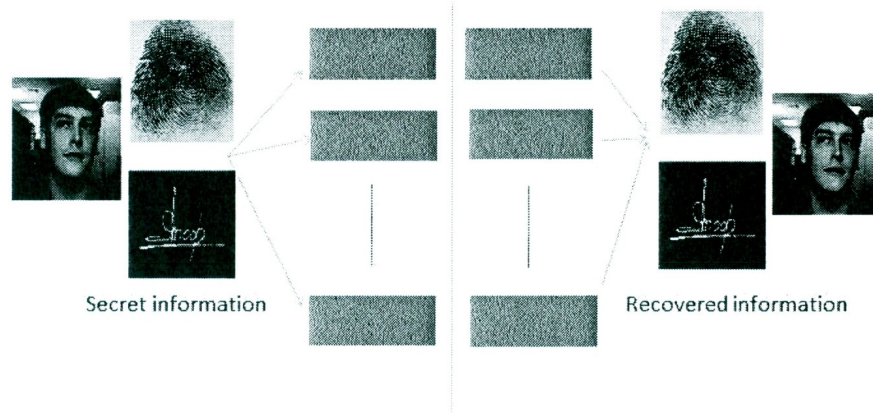


Figure 1.1: Example of an application of visual secret sharing to biometric data

spectively. The image splits into two share images which are individually meaningless. Recovery of the secret image can be performed by superimposing the two shares, while inspecting only one share cannot reveal any information. The basic model is extended to a k out of n secret sharing problem, called a (k, n) visual cryptography scheme. According to this algorithm, the secret image is processed into n shares and that the secret is revealed if any k of the shares are stacked together [10]. The image remains hidden if fewer than k shares are stacked together.

Image contrast and the number of subpixels of the shares are two main parameters in visual cryptography schemes [10]. The number of subpixels represents expansion of the image and should be as small as possible. In Naor and Shamir's visual cryptography scheme (traditional VCS), each pixel in the secret image is mapped into a block of m pixels in each share. Hence one shortcoming of traditional VCS is that the shares and the recovered secret image are m times larger than the original secret image. Moreover, the recovered image is poor in contrast since only black pixels are perfectly reconstructed. In this thesis, this effect is called loss in contrast. Image size expansion and the loss in contrast are serious problems in any visual cryptogra-

phy scheme. Since the secret image is decoded by human visual system, the visual quality of the recovered image is important and the poor visual quality can make the secret image hard to interpret. Moreover, when the size of each secret share and reconstructed image is several times larger than the original image, it can cause some problems such as image distortion and inefficiencies in storage space and transmission time.

During the past few years, many studies have been performed to improve traditional visual cryptography to make it more effective and applicable in different environments. In traditional visual cryptography, only one secret image can be concealed at a time. Some schemes have been proposed in order to share multiple secrets simultaneously [11]. Such schemes are referred to as multiple image VCS. Moreover, some methods have been proposed to solve the problem of meaningless, noise-like shares in traditional visual cryptography. The resulting creation of shares representing meaningful images is referred to as extended visual cryptography [12][13]. As well, studies also have been performed on applying visual cryptography to support grayscale and color images [14][15][16]. Further, a limited amount of research has been focused on visual cryptography schemes without image size expansion [17][18][19][20]. However, to the best of our knowledge, there is no effective non-expansion scheme related to mitigate the problem of contrast degradation and poor visual quality of the reconstructed images for both binary and grayscale images.

While visual cryptography is a very powerful secret sharing technology, it would be more practical and can be broadly applied to many authentication applications only if it can provide perfect security and good visual quality of the recovered images without size expansion. As an example application combining biometrics and data hiding, consider an ID card containing a biometric template VC share. The fingerprint is the most common human biometric characteristic that has been used

for personal identification [7]. Thus fingerprint images are considered as a biometric sample and an entrance security system in a company is considered as a case study for this approach. The fingerprint of each eligible person is collected by the system administrator and made available to the visual cryptography system. Random shares are created from the fingerprint images by a visual cryptography algorithm. One of the shares is stored in the database and the other share is given to the eligible person in the form of a unique ID card [21]. For verification, the user should insert the ID card into the security system. The corresponding share which is stored in the database is found and stacked with the other random share that is embedded in the ID card. After verification, the system should identify the participant. Hence, the system requests new fingerprints from the participants to compare with the minutiae extracted from secret fingerprint images obtained from the visual cryptography algorithm. Authentication is accepted if the matching process succeeds. Entrance will be allowed if the comparison and matching of the newly provided fingerprints stored as the secret images with the physically obtained fingerprints are close together [22]. As the matching process is based on the minutiae details, it is difficult to extract the minutiae points accurately when the reconstructed fingerprint image is of low quality. Also, the speed of the authentication and matching process would be slow if the size of the shares and the reconstructed image is larger than the original secret image.

Thus, in this thesis, we have the motivation to present a visual cryptography scheme which is not only perfectly secure, but also provides improved visual quality without expansion of the reconstructed image.

1.3 Purpose

In this research, we address two major problems of traditional visual cryptography scheme and propose solutions to overcome the drawbacks. As noted before, traditional VC is not an efficient method to be applied on sensitive security and authentication systems, due to its size expansion and the poor visual quality of the images it produces. Therefore, the first purpose of our study is to design and implement a novel visual cryptography scheme that solves the issue of size expansion and also improves the contrast and quality of the recovered image, along with providing perfect security of the scheme. Unlike traditional VC, our novel scheme preserves the arrangement of a black and white pixels in the secret image as much as possible. In other words, the pattern we have designed for generating the shares is able to recover the secret pixels with the minimum difference from the original pixels. As a result, the reconstructed image obtained by this scheme is very similar to the original secret and is easy to visually distinguish. Also, this scheme ensures the security of the secret image and can be applied on both halftoned and binary images.

The visual cryptography scheme proposed in [4] can only deal with binary images and grayscale images such as photographs cannot be handled in such a scheme. Hence, methods such as halftoning techniques are used to convert the grayscale images to binary images and prepare the images for visual cryptography schemes [23]. However, recovered halftoned images can have loss of contrast and poor visual quality. Thus, human visual system may have difficulty to identify the secret information from the recovered image. Therefore, we attempt to improve the visual quality of the halftoned images by introducing three methods. In this research, a random conversion method, a clustering and constant threshold (CCT) method, and clustering and variable threshold (CVT) method are proposed to prevent pixel expansion while maintaining good visual quality of the recovered images when grayscale images are

utilized as secret images in different visual cryptography schemes.

The other purpose of this research is to generate a visual cryptography scheme without pixel expansion and apply it to multiple-image VCS and extended VCS. Multiple image visual cryptography, proposed by Chen and Wu [11], uses share rotation to conceal more than one secret image, and extended VCS creates meaningful shares instead of noise-like shares. Both these schemes are well-known and important as they are very useful for application in biometric authentication systems. However, these approaches suffer from the pixel expansion problem and a loss in contrast. Multiple image visual cryptography and extended visual cryptography without image size expansion and with good resolution of the resulting images could have useful applications to authentication systems. The random conversion method, CCT method and the CVT method are practical solutions for overcoming the problems of pixel expansion and poor visual quality of the recovered images in multiple image VCS and extended VCS.

1.4 Outline of Thesis

This thesis is composed of six chapters and organized as follows:

In Chapter 2, related literature on the main visual cryptography schemes are reviewed. Experimental results for each scheme are also depicted and discussed in this chapter. As well, digital halftoning is introduced and one of its techniques is described at the end of this chapter.

In Chapter 3, a novel visual secret sharing scheme for sharing a single image is proposed in order to improve the contrast and avoid pixel expansion. Moreover, to evaluate the performance of our proposed scheme and compare it with other non-expansion schemes, numerical and visual experimental results are discussed in this

chapter.

In Chapter 4, we extend Chou's non-expansion model and propose three novel methods to deal with the problem of pixel expansion and to improve the contrast and visual quality of the reconstructed secret images.

In Chapter 5, the proposed algorithms in Chapter 4 are applied to multiple image VCS and extended VCS. Also, simulation results are shown and discussed in this chapter.

Finally, conclusions and future work are presented in Chapter 6.

Chapter 2

Review of Visual Cryptography Schemes

2.1 Introduction

A visual cryptography scheme (VCS) is a type of secret sharing scheme where the secret is an image. The creation of shares does not need complicated computation and the recovery of the secret is done by the human visual system. Since the introduction of visual cryptography, this secure and unique cryptographic method has attracted the effort of many researchers. In this section, we introduce the concept of visual cryptography and review some constructions of visual cryptography schemes.

2.2 Basic Definitions

Visual cryptography is a type of secret sharing scheme introduced by Naor and Shamir in 1994 [4]. The initial visual cryptography scheme can be generally referred to as a k out of n visual cryptography scheme and abbreviated as a (k, n) -VCS. The secret to be hidden is a black and white image consisting of a collection of binary 1s















and 0s displayed as black and white pixels. This scheme splits the secret image into n share images. Each pixel of the binary image is encoded into m black and white subpixels in each of the n shares. The secret is recovered when any k or more of the shares are stacked together. However, the secret remains hidden if the number of shares stacked is less than k . When stacking shares, it is assumed that a white pixel in a share is transparent and a black pixel is opaque. The scheme introduced by Naor and Shamir is perfectly secure; as it is noted in [4], the security in VCS is similar to one time pad, so it is impossible to get any information about the secret image from shares individually. Another advantage of VCS is that, unlike other cryptography techniques, the secret recovery does not need difficult computations. The secret information can easily be recovered with enough shares and as the name suggests, it can be done by human vision instead of special software or hardware.

Security in the VCS and the contrast of the reconstructed image are two important conditions in every VC scheme. In VCS, contrast is defined as the difference measure between a black and a white pixel in the reconstructed image and good contrast reflects the clear distinguishing of regions of white and black in an image [10]. The parameter m is the number of subpixels in each share and represents the expansion ratio of the image. It should be as small as possible; ideally $m=1$ for no pixel expansion.

2.3 (2, 2) Visual Cryptography Scheme

The basic idea of visual cryptography can be illustrated with the traditional 2-out-of-2 scheme [10]. A black and white image is split into two individually meaningless share images called share 1 and share 2. Each share images is distributed individually and the secret image is only revealed when the two shares are stacked together. The secret recovery does not require any complex algorithm or devices; moreover,

Table 2.1: Illustration of a 2-out-of-2 secret image sharing scheme with 2 subpixels

Pixel	Probability	Share1	Share2	After Stacking
	1/2			
White	1/2			
	1/2			
Black	1/2			

observing only one share does not reveal any information about the secret image.

Every pixel from the secret image is turned into two subpixels in each share. Table 2.1 shows the pixel pattern generation for 2-out-of-2 VCS with 2-subpixel layout, that is, $m=2$. According to the table, if the pixel in the secret image is white, one row from the first two rows is selected randomly to encode a white pixel into two shares. Similarly, if the pixel in the secret image is black, one row from the second two rows is selected randomly to encode a black pixel into two shares. The share generation process can be mathematically represented using binary matrices. In this work, we represent black and white pixels by binary "1" and "0", respectively. S_0 and S_1 are the basic matrices in the (2, 2)-VCS and are designed as follows:

$$S_0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad S_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

For encrypting a white pixel, a random permutation should be applied to the columns of S_0 , and to encrypt a black pixel, we apply a permutation on S_1 . Based on this definition, C_0 and C_1 are the two sets of matrices obtained by permuting the columns of S_0 and S_1 and used to randomly select a share scheme to encode a white or black pixel from the original image:

$$C_0 = \left\{ \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \right\},$$

$$C_1 = \left\{ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$$

As illustrated in Table 2.1, the shares can be generated in the following manner: one of the matrices in C_0 is selected randomly (with the same probability) to encode the white pixel into two shares in a way that the first row of the selected matrix is considered as the first share and the second row is used for the second share. Likewise, for encoding the black pixel, one of the two matrices from C_1 is selected and the encoding process uses the rows to represent the shares. As each share contains one black and one white subpixel, observing only one share does not reveal information about the original secret image.

Secret image recovery or the decoding process can be performed by superimposing the shares together with the binary OR operation. If the secret pixel is black, the recovered pixel contains two black subpixels and when the original pixel is white, the superposition results in one white and one black subpixel. This fact will lead to a problem which is a distortion of the aspect ratio in the shares and the reconstructed image.

Figure 2.1 shows an example of applying the (2, 2)-VCS with a two subpixel layout. Figure 2.1(a) is an original secret image named binary Dancers. As is expected from the algorithm, black regions in the reconstructed image shown in Figure 2.1(b), are

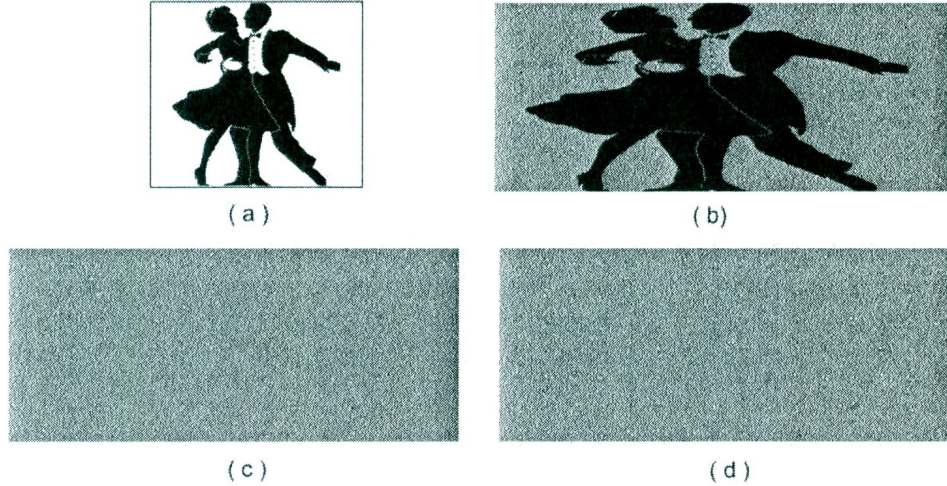


Figure 2.1: (2, 2)-VCS with 2 subpixels: (a) secret Dancers image; (b) reconstructed Dancers image; (c) first share; (d) second share

fully recovered while the white area in the background of this image appear as half black and half white. This fact reduces the visual quality of the recovered image and is known as a loss in contrast or contrast degradation. The first and second share images are depicted in Figures 2.1 (c) and (d), respectively. Observing the shares does not reveal any detail about the Dancers image. Also, results obtained by this scheme illustrate the horizontal distortion of the shares and the reconstructed image as the size of the secret image is 200×200 while the size of each share and recovered image is 200×400 .




























To avoid image distortion, Naor and Shamir introduced the (2, 2)-VCS with 4 subpixels [4]. We can easily construct a (2, 2)-VCS with 4 subpixels by the following collection of matrices:

$$C_0 = \left\{ \text{all matrices derived by permuting the columns of } \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} \right\}$$

$$C_1 = \{\text{all matrices derived by permuting the columns of } \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}\}.$$

In this scheme, 4 subpixels are generated from each pixel of the secret image in a way that 2 subpixels are white and 2 are black. The subpixels for each share are selected randomly. When a pixel from the original image is white, one of the matrices in C_0 is randomly selected to encode the pixel into 2 shares with each row of the selected matrix representing the subpixel pattern in the share. Table 2.2 demonstrates a share generation process of (2, 2)-VCS with four subpixels. As can be seen, the first and the second shares in the table represent all the matrices in C_0 and C_1 , in a way that the first row of the matrix maps to the first share subpixels and the second row of the same matrix maps to the second share subpixels (from left to right and top to bottom). It is easy to see that knowing only one share value does not reveal the other share nor any information of the secret image pixel as each pixel in the secret image is encoded into a 4-subpixel layout with 2 black and 2 white subpixels. However superimposing both shares with the OR operation reveals the corresponding binary secret image. Thus, this method provides perfect security. Figure 2.2 shows an example of applying the (2, 2)-VCS with 4-subpixels layout, where the share images are 2 times larger than the original secret image in each dimension. That is, the share uses 4 subpixels for the original pixel. As illustrated in Figure 2.2, (a) is the secret image, (c) and (d) are two random shares, and (b) shows the reconstructed image from superimposing the two shares. In this example, as expected, the size of the shares and the recovered image are 4 times larger than the size of the secret image. Although in the 4 subpixel layout scheme there is no distortion in the reconstructed image, the scheme has the problems of pixel expansion and contrast degradation.

Table 2.2: Illustration of a (2, 2)-VCS with 4 subpixels

Pixel	Probability	Share 1	Share 2	After Stacking
<div> <div></div> <div>White</div> </div>	1/6			
	1/6			
	1/6			
	1/6			
	1/6			
	1/6			
	1/6			
<div> <div></div> <div>Black</div> </div>	1/6			
	1/6			
	1/6			
	1/6			
	1/6			
	1/6			
	1/6			

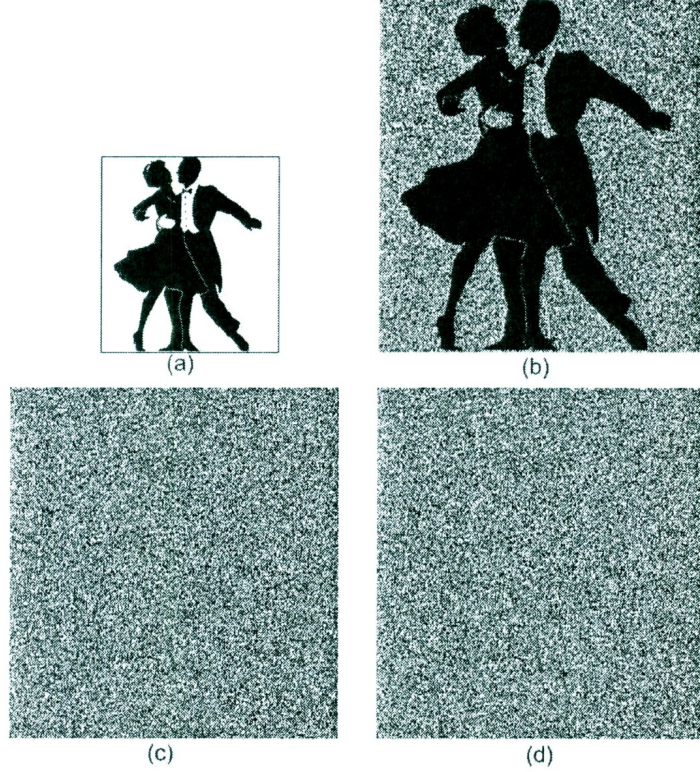


Figure 2.2: Example of a $(2, 2)$ -VCS with 4 subpixels: (a) secret Dancers image; (b) reconstructed Dancers image; (c) first share; (d) second share

2.4 Multiple Image Visual Cryptography

Following the research of Naor and Shamir that could embed only one secret image, in 1998, Chen and Wu [11] developed a $(2, 2)$ -VCS and proposed a multiple secret image scheme. Multiple image visual cryptography scheme or multi-image VCS has the advantage of concealing two secrets at the same time by using a rotation technique in a way that binary images divide into two random, meaningless shares, according to the encoding process. The first secret image becomes visible by stacking the first and second shares and the second secret is revealed by rotating counterclockwise the pixel groups of the first share by θ , where θ is 90° , 180° or 270° , and stacking it with the

Table 2.3: Illustration of multiple image VCS (Chen and Wu)

Pixel of the first secret image	W	W	B	B	W	W	B	B	W	W	B	B	W	W	B	B
Pixel of the second secret image	W	B	B	W	W	B	B	W	W	B	B	W	W	B	B	W
s1																
s2																
s3																
s1 stack s2																
s3 stack s2																

second share. Like the traditional VCS, recovered secret images are 4 times larger than the original secret images or expanded by a factor of 2 in each dimension. Wu and Chen's encoding scheme for visual two-secret sharing in two shares is summarized in Table 2.3. In the table, s1, s2 and s3 represent share 1, share 2 and share 3, respectively, and the rotation angle is assumed to be 90° counterclockwise in this method.

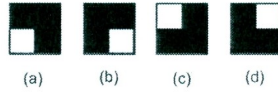


Figure 2.3: Example of four possible patterns to be assigned in multiple secret sharing scheme for first share

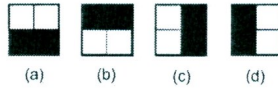


Figure 2.4: Example of four possible patterns to be assigned in multiple secret sharing scheme for second share

As an example, assume that a pixel of the first and a pixel of a second secret image are

both black. Four patterns can be assigned to create the first share (s1). If the selected pattern is randomly selected for the patterns depicted in Figure 2.3, the second share (s2) should be selected in a way that black can be revealed by the stacking of s1 and s3, where s3 is s1 rotated counterclockwise by 90° . Consequently, four different patterns shown in Figure 2.4 could satisfy this condition depending on which pattern is selected for s1. If Figure 2.3(a) is selected for s1, then Figure 2.3(b) represents s3 and the pattern shown in Figure 2.4(a) must be used for s2 so that stacking this pattern with what is shown in Figure 2.3(a) and(b), will reveal the black subpixels.

Results after applying Chen and Wu's scheme are illustrated in Figure 2.5. Two text images are used as secret images in this example and are shown in (a) and (b). The size of each of the secret images is 100×300 pixels. As is shown in Figure 2.5, the images are encrypted into three shares, each with the size of 200×600 pixels. For decryption, share image A and share image B are stacked together and the first secret image is restored. The second secret image is revealed by rotating the pixel groups of share A counterclockwise by 90° (share image C in Figure 2.5) and superimposing it on share B. Besides the problem of pixel expansion, this approach is limited in the rotation angles required for revealing the secret to 90° , 180° or 270° , and also the number of secret images that can be hidden is limited to two. To overcome these shortcomings, multiple image visual cryptography methods using circular shares [24][25] have been proposed that have various values for the rotation angle.

2.5 Extended Visual Cryptography

As indicated in the previous subsections, both traditional and multiple image visual cryptography schemes produce noise-like shares that have no visual meaning. Due to the value of having shares which are meaningful images, in 1996 Ateniese et al. [12]

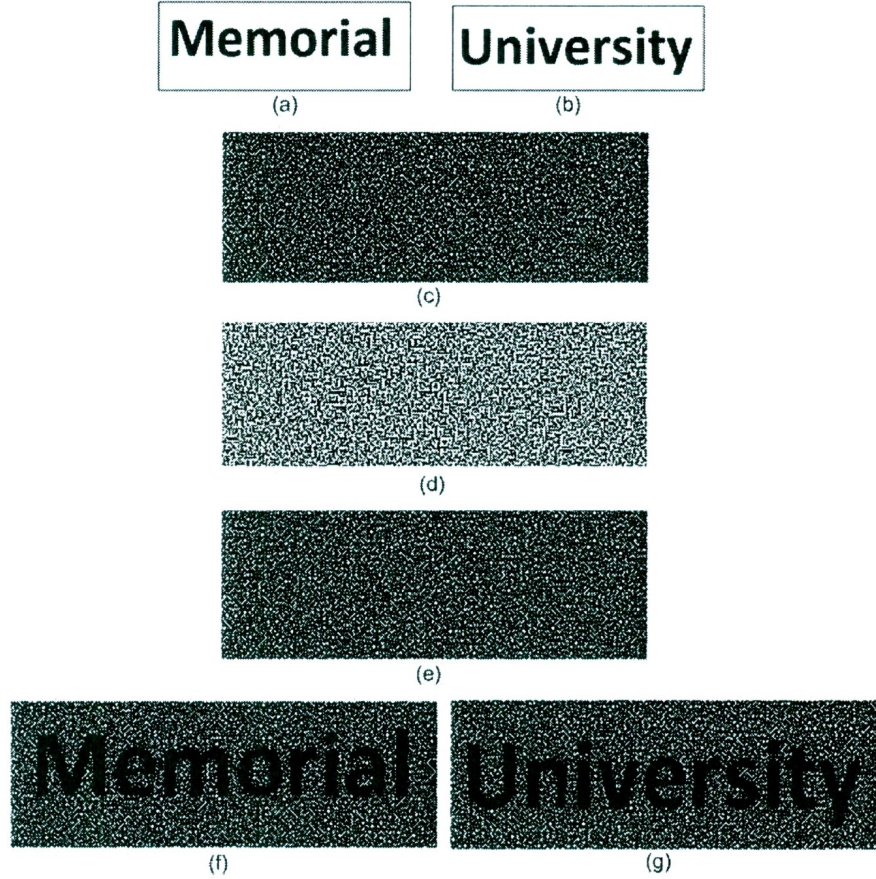


Figure 2.5: Example of a multi-image VCS: (a) first secret image; (b) second secret image; (c) share A; (d) share B; (e) share C; (f) reconstructed secret 1; (g) reconstructed secret 2

introduced a type of visual cryptography method named extended visual cryptography scheme (EVCS) that reconstructs the binary secret image by stacking meaningful images (shares) together. The (k, n) -EVCS takes $n+1$ images as input and generates the first n images as a meaningful shares referred to as cover images. The secret image is the $n+1$ -th image that is recovered after the sets of meaningful cover images are superimposed. For implementing EVCS, the tone of each pixel (black or white) in the secret image and cover images should be determined. Therefore a collection of

matrices are determined for encoding the secret image to cover images. This is denoted by $C_c^{c_1, c_2}$, for $(2, 2)$ -EVCS where c, c_1 and $c_2 \subseteq \{b, w\}$. Shares can be determined by choosing a matrix from the collection of matrices, where c_1 and c_2 are the tone of the first and second cover image, respectively, and c is the tone of the secret image. The collections $C_c^{c_1, c_2}$ are obtained by permuting the columns of the following matrices where superscripts and subscripts are defined above.

$$\begin{aligned}
S_w^{ww} &= \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} & \text{and } S_b^{ww} &= \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \\
S_w^{wb} &= \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} & \text{and } S_b^{wb} &= \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}, \\
S_w^{bw} &= \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} & \text{and } S_b^{bw} &= \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \\
S_w^{bb} &= \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} & \text{and } S_b^{bb} &= \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}
\end{aligned}$$

As an example, if a pixel tone of the secret image is white and the pixel tone of the first and second cover image are also white, the first row of matrix S_w^{ww} is considered as the first meaningful share image and the second row is used for the second share image. Figure 2.6 provides an example of applying the $(2, 2)$ -EVCS on three images. As can be seen from the figure, two meaningful shares are generated from the cover images. During the share generation, the secret image is encoded between the two shares, but after superimposing the extended shares together, the cover images on the shares disappear and the secret message reveals. In 2002, extended visual cryptography for natural images (such as grayscale or colour images) was proposed in [26].

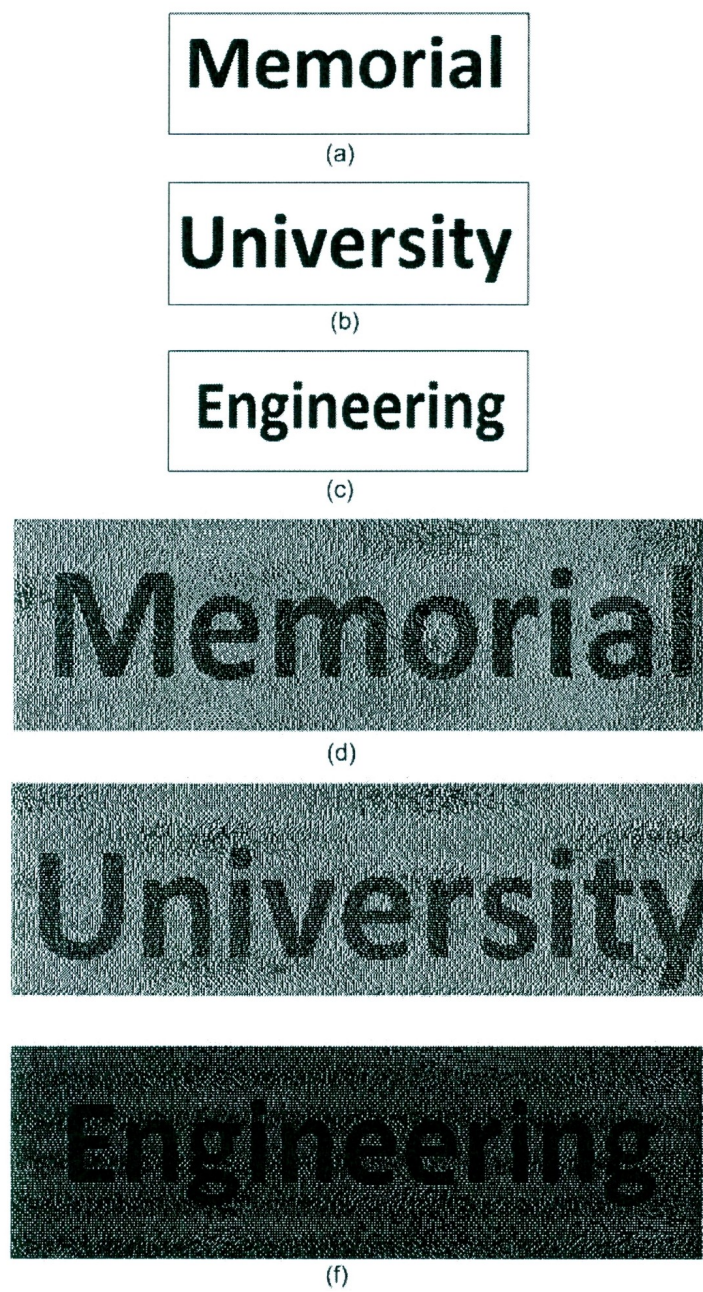


Figure 2.6: Example of $(2, 2)$ - extended visual cryptography scheme: (a) first cover image; (b) second cover image; (c) secret image; (d) extended share 1; (e) extended share 2; (f) recovered secret image

2.6 Visual Cryptography Schemes Without Pixel Expansion

2.6.1 Introduction

Since most visual cryptography schemes result in pixel expansion, the reconstructed images obtained by these schemes are expanded, potentially by different factors in the two dimensions, causing problems such as image distortion and consumption of more storage space. Therefore, a few visual cryptography schemes have been developed to cope with the problem of pixel expansion. In this section, 3 non-expansion VCS are reviewed.

2.6.2 Probabilistic scheme

In 1999, Ito et al. [17] proposed a (k, n) -VCS without expanding the number of pixels, that is, the secret image and the shares all have the same size. Their scheme employed a probabilistic concept to solve the problem of pixel expansion. Like traditional VCS, this method is based on the two boolean basis matrices S_0 and S_1 . Each pixel in the secret image is presented as a black or white pixel in the share images. To encode a black (resp. white) pixel, one of the column vectors in S_1 (resp. S_0) is selected randomly and the i -th row of the randomly chosen column is assigned to the i -th share. To reconstruct the secret, traditional ORing is applied to the pixels in each vector. As an example for this scheme, the $(2, 2)$ visual cryptography scheme with $m=1$ is constructed by boolean matrices S_0 and S_1 defined in traditional $(2, 2)$ -VCS. To share a white (resp. black) pixel, one of the columns in S_0 (resp. S_1) should be selected randomly. As an example, we suppose that the second column

vector from S_0 is selected to encode a white pixel:

$$V = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

The chosen column vector defines the tone of each pixel in the corresponding share image. So, the first and second shares are assigned as black pixel. For sharing a black pixel, assume that the first column vector from S_1 is selected:

$$V = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$















Therefore, a white pixel is assigned to the first share image, and black to the second share image. This process is repeated for all pixels in the secret image resulting in the final set of shares.

Like other cryptographic schemes, contrast and security are the main parameters in this scheme. According to the probabilistic method in [17], their scheme is just as secure as the traditional visual cryptography. The contrast of the reconstructed image for this scheme is defined as follows:

$$\beta = |p_0 - p_1|$$

where parameter β represent the contrast and p_0 (p_1) represents the probabilities that a white (resp. black) secret pixel is encrypted as a black pixel on the recovered image. In the above example, the probability that a white secret pixel is encrypted as a black pixel on the secret image is 0.5 and the probability that a black pixel is encrypted as

Table 2.4: Illustration of probabilistic (2, 2)-VCS

Pixel	Probability	Share1	Share2	After Stacking
	1/2			
White	1/2			
	1/2			
Black	1/2			

a black pixel is 1.0. Therefore the contrast of the reconstructed image is $\beta = 0.5$.

Table 2.4 illustrates probabilistic (2, 2)-VCS, and Figure 2.7 shows experimental results obtained after applying the probabilistic method. In this experiment, binary Dancers with size 200×200 is used as a secret image. As is expected, the share images and the reconstructed secret image have the same size as original secret image. However, the resulting secret image has a poor visual quality as the white pixels are not fully recovered. More analysis of this scheme and experimental results are discussed in Chapter 3.

2.6.3 Chou's Non-Expansion VCS

In contrast to pixel-wise schemes, in 2002, Chou [20] presented another scheme without pixel expansion which uses a block-wise operation. Unlike the other visual cryptography schemes, this scheme divides a secret image into non-overlapping 2×2 blocks of four pixels. Based on Chou's method, a block of four pixels is classified in a way that if a block has 2 to 4 black pixels, it is seen as a black block and if it contains 0 to 1 black pixels, it is known as white block, as shown in Table 2.5. The encoding process for this scheme is exactly the same as the (2, 2) traditional

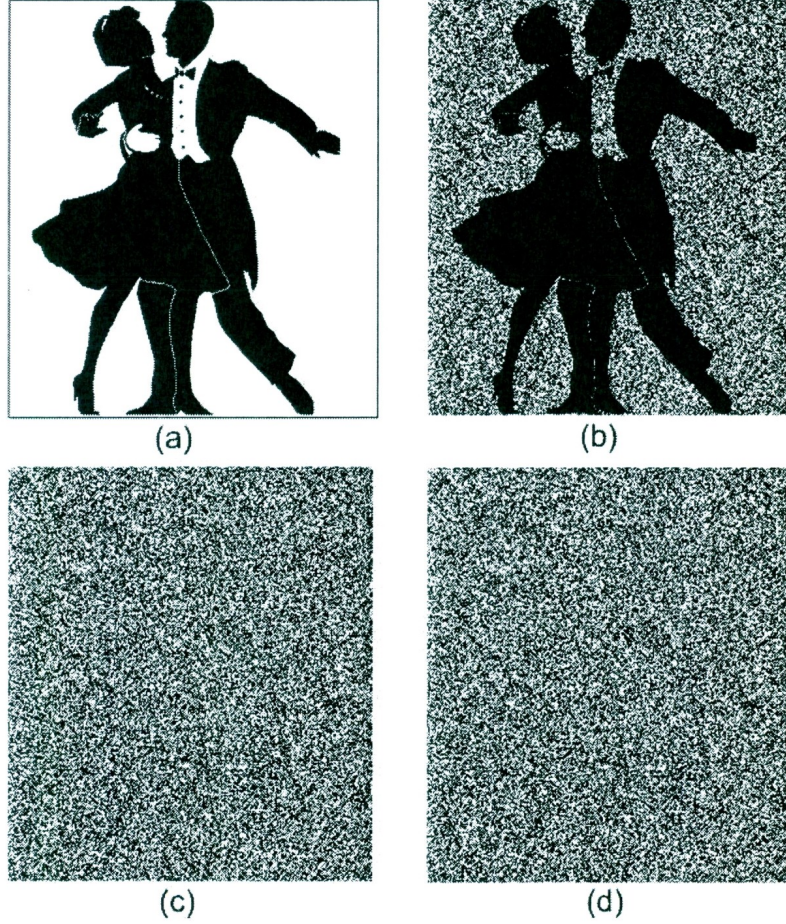



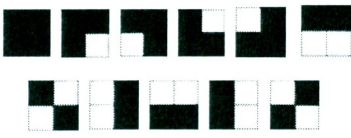


Figure 2.7: Example of probabilistic $(2, 2)$ -VCS; (a) original secret image; (b) recovered image; (c) share 1; (d) share 2

visual cryptography scheme with 4 subpixel layout; therefore, one of the first six rows in Table 2.2 is selected to encode a white block into two shares. Likewise, to encrypt a black block, we randomly choose one of the last six rows in Table 2.2 to split the block into two random shares. Although this is a non-expansion method with perfect security, the results obtained by this scheme shows poor visual quality in the reconstructed image. More analysis of this scheme and experimental results are discussed in Chapter 3.













Table 2.5: Classification of Chou's scheme

After classification	All blocks before classification
 White	
 Black	

2.6.4 MLVSS Scheme Without Image Size Expansion

In order to improve the quality of the reconstructed secret image, in 2007, Chen et al. [27] proposed a multiple-level visual secret sharing (MLVSS) scheme without image size expansion. This scheme divides a secret image into several blocks and then arranges the secret blocks according to the density of black pixels in each block. Based on the number of black pixels, each secret block belongs to a specific group, symbolized by G1, G2 and G3. According to the grouping rule proposed in the scheme, every block that has 4, 3 and 2 white pixels, belongs to the G1. All the secret blocks containing 3 black pixels are classified into G2 and blocks with 4 black pixels are belongs to G3. For each group, secret blocks are generated into 2 shares in a way that each share contains 2 white and 2 black subpixels in share blocks and superimposing the share blocks with the OR operation, reconstructs the corresponding secret block. Table 2.6 shows an example of the encoding and decoding process proposed in this method. As an example, if the secret block contains 4 black pixels, it belong to G3 and there are 6 possible combination of share blocks with 2 black and 2 white pixels which recover the secret black block. According to the encoding process of

Table 2.6: A part of the MLVSS scheme without pixel expansion

Group	Secret Block	Share1	Share2	After Stacking
G1				
G2				
G3				

MLVSS, this scheme is not perfectly secure and has a problem of leakage of the secret information as share selection is not a random selection from the share blocks with the same probability. More analysis about this scheme and experimental results are discussed in Chapter 3.

2.7 Grayscale Images and Halftoning

Visual cryptography can be used to encode natural images, where natural images may be in the form of a grayscale image. Digital halftoning is a technique that transforms a grayscale image to a black and white images and makes them more suitable for printing, especially in laser and ink jet printers [28]. The halftoning process creates the visual illusion of the shade of gray by varying the density of black and white dots in an image. So the varying intensities of the black dots produce a simulation of a continuous-tone image. The ordered dither array and error diffusion algorithm are two well known halftoning techniques that are widely used for transforming gray level images to binary images. When the image is halftoned by the dither array technique, every pixel in the image is compared with an element from the dither array or threshold. If the pixel is darker than threshold, the output pixel represents as black

and if the corresponding pixel is brighter than the threshold, the output pixel turns to white [29]. This is a basic and simple method for transforming grayscale to binary images known as a traditional halftoning technique.

Error diffusion is another type of halftoning technique introduced by Floyd and Steinberg in 1975 [30] in which neighbouring pixel values are taken into account to determine the output of any particular pixel value. Error diffusion compares the current tone of the pixel with its neighbour's tone and takes the difference between them. This difference is known as the error filter and it is distributed amongst neighbouring pixels. This approach produced halftoned images with high quality in comparison to the ordered dithering method. However, error diffusion halftoning technique requires more computation and memory due to its neighbouring operation and thresholding [31]. Figure 2.8 describes the error filter proposed by Floyd and Steinberg. According to the algorithm, firstly, each pixel of the image should be processed for a binary thresholding, and then the error between output and modified input values is computed. Then, the error is dispersed into the error diffusion filter as it is shown in Figure 2.8 and, finally the value of each pixel is updated with the errors from its neighbour pixels. We use Floyd-Steinberg error diffusion algorithm in our thesis due to its good quality and high resolution. Figure 2.9 (a) shows a gray-level image and (b) illustrates the halftone image after applying the error diffusion algorithm. Since the gray-level image has transformed to a binary image by the halftoning technique, now we can use this binary image in visual cryptography schemes.

	Pixel	7/16
3/16	5/16	1/16

Figure 2.8: Error filter



Figure 2.9: Image halftoning with Floyd-Steinberg method: (a) gray scale Lena; (b) halftoned Lena

2.8 Conclusion

In this chapter we have reviewed a number of important visual cryptography schemes and evaluated their performance on security, number of secret images, pixel expansion and contrast. In the upcoming chapters we will improve on previously proposed methods by proposing secure, non-expansion methods, for both original binary image and halftoned grayscale images, that result in good visual quality of the recovered secret after applying different VC schemes.

Chapter 3

Visual Cryptography Without Image Size Expansion

3.1 Introduction

As described before, traditional visual cryptography schemes will result in shares and a reconstructed image with their size expanded beyond that of the original image, which will cause problems such as image distortion and consumption of more storage space and bandwidth. In addition to the pixel expansion, contrast of the recovered image is one of the important characteristics in visual cryptography. According to the results obtained by applying the traditional visual cryptography schemes, contrast degradation causes poor visual quality of the reconstructed image. Therefore, some research has focused on mitigating image size expansion and contrast degradation.

















Ito et al.[17] introduced a (k, n) -VCS which prevented size expansion by a probabilistic method. These represent each pixel in the secret image as a black or white pixel in the share images and the secret image can be revealed by stacking the shares together. In 2004, Yang et al. [18] proposed a similar probabilistic method called

ProbVSS for binary and grayscale images. In [19], the authors presented a multiple image secret sharing scheme without pixel expansion based on Chou’s method [20]. In this scheme a block of four pixels are designed in a way that if a block has 2 to 4 black pixels, it is seen as a black block and if it contains 0 to 1 black pixels, it is known as white block. Chen et al. [27] proposed a multiple level visual secret sharing scheme (MLVSS). This scheme divides a secret image into several blocks called secret blocks and generates share blocks according to the density of the black pixels in a secret block. Although these earlier works succeed in preventing size expansion, they still have significant problems such as leakage of the secret information and poor quality of the reconstructed secret image.

3.2 A Novel (2, 2) Visual Cryptography Scheme Without Image Size Expansion

In this section, we propose a solution to overcome the problem of pixel expansion and mitigate contrast degradation for visual cryptography with one secret image. Our scheme, which is a novel visual secret sharing scheme without pixel expansion, is constructed as a (2, 2) scheme. Hence, the secret image is encoded into two share images and, when the two shares are stacked together, the secret information can be revealed. This scheme first divides a secret image into several blocks, each containing 4 pixels in 2×2 block arrangement. These blocks of 4 pixels are encoded into a block of 4 pixels for each share. Hence, the original secret image, the reconstructed secret image, and each share image all have the same size. But the most unique feature of our method is that the encoding rules have the advantage of recovering the secret pixels closely to the original secret pixels based on binary XOR operation. Due to this feature of our scheme, the recovered secret image clearly restores details of the

Table 3.1: Block models of the image

bbbb	bbbw	bbwb	wbbb	bwbb	bbww	bwbw	wbwb
							
							
wwbb	bwbb	wbbw	wwbw	wwwb	bwww	wbww	wwww

original image. Therefore, our novel scheme is very suitable for application to both binary and halftoned images.

3.2.1 Description of the Scheme

The block selection, mapping process and encoding process are the three main steps in the scheme and are described as follows:

Algorithm : Encoding

Inputs:(1) A grayscale secret image

or

(2) A binary secret image size $2x \times 2y$, (i.e. size of input image must be even in both dimensions).

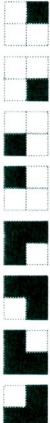
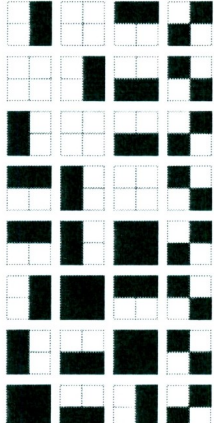
Output: share 1 and share 2 each sized $2x \times 2y$

Step 1: If grayscale input image, transform it into halftone image HS of size $2x \times 2y$.

Step 2 : The HS or binary image is divided into a number of blocks with 2×2 pixels. We call the block in the secret image a secret block, and the block in the share image a share block.

Step 3 : All the secret blocks are labeled according to the distribution of the black and white pixels. In Table 3.1, we present the name of each block model with each block model composed of four pixels in 2×2 pixel arrangement.

Table 3.2: Mapping process

Secret Blocks	Candidate Blocks
	

Step 4 : In the mapping process, secret blocks are categorized according to the following decision rule:

If the secret block contains 1 black pixel (3 white pixels) or 3 black pixels (1 white pixel), they are randomly mapped to one of the 4 secret block candidates illustrated in Table 3.2. Otherwise, no mapping process is required.

Step 5 : Shares are created by randomly selecting one of the 8 possible share blocks for each secret block as is illustrated in Table 3.3.

Step 6 : Repeat Steps 2 to 5 until all secret blocks of the secret image are encoded. The reconstructed secret image is obtained by stacking the first and the second share together using the XOR operation. In this logic operation, XORing two pixels with same colour results in a black pixel and XORing two pixels when one pixel is white and the other is black results in a white pixel. In this scheme, for the purpose of the XOR operation, black is assumed to be "0" and white is assumed to be "1".

Table 3.3: Proposed encoding process




Secret Block	Probability	Share1	Share2	After Stacking
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
Continued on next page				

Table 3.3: Proposed encoding process











Secret Block	Probability	Share1	Share2	After Stacking
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
Continued on next page				

Table 3.3: Proposed encoding process




























































Secret Block	Probability	Share1	Share2	After Stacking
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
		1/8		
1/8				
1/8				
1/8				
1/8				
1/8				
1/8				
Continued on next page				

Table 3.3: Proposed encoding process

Secret Block	Probability	Share1	Share2	After Stacking
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			
	1/8			

3.2.2 Example

To explain more, we describe the proposed scheme with an example. A grayscale image (Lena) is assumed to be a secret image in this example. For the first step, a secret image is transformed to a binary image with the Floyd-Steinberg halftoning algorithm. After the image is divided into blocks of 2×2 pixels, we assume that the *bbw* case from Table 3.1 is selected as the first secret block. Figure 3.1 depicts step 2 and step 3 of this example for the grayscale image which is converted to the halftoned image.

According to Step 4, as this block has 3 black pixels and one white pixel, one of

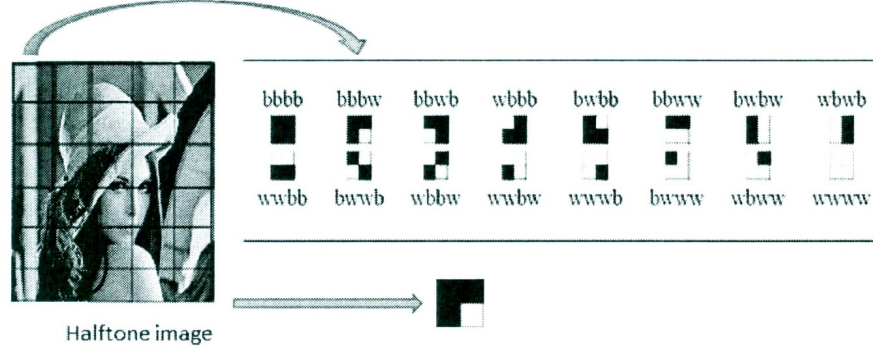


Figure 3.1: Example of block selection

the *bbww*, *bbbb*, *bwbw* and *wbbw* models should be randomly selected from Table 3.2. As is illustrated in Figure 3.2, *bbww* is selected as a secret block for the encoding process. According to Table 3.3, 8 possible combinations of share blocks exist for share 1 and share 2 to produce the recovered secret blocks. One of the patterns will be selected randomly to create the shares for the secret block. As is indicated in Table 3.3, stacking the two shared blocks with the XOR operation results in the recovered secret block which is a *bbww* block.

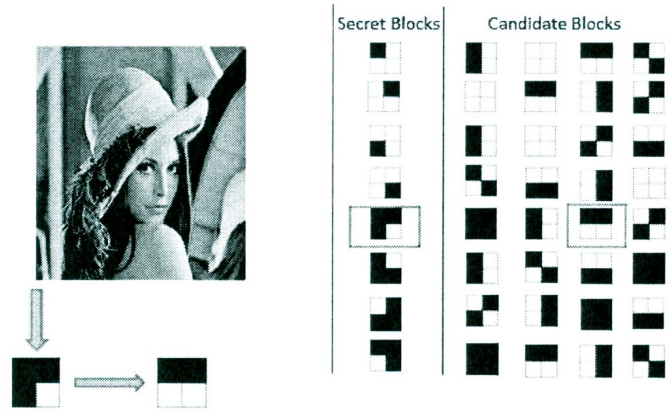


Figure 3.2: Example of mapping process

3.3 Security and Contrast Analysis

Security is the primary issue in visual secret sharing schemes. As shown in [4], the traditional $(2, 2)$ scheme is perfectly secure since a forbidden set of participants cannot gain any information about the original secret image by inspecting one of the shares. Hence, share images should be indistinguishable in the sense that they contain the same share blocks with the same probability regardless of the distribution of pixels in the original secret image. To ensure the security of our proposed scheme, we should guarantee that all the share blocks have the same probability distribution of all possible patterns on the shares. Therefore, no one can get any secret information by analyzing these shares. In the encoding process of our proposed VCS, each block of the secret image is randomly encoded into one of 8 pairs of share blocks. All the 8 pairs of share blocks contains 4 vertical share blocks (where the black and white pixels align vertically), 4 horizontal share blocks, 4 diagonal share blocks and 4 solid white or solid black share blocks. Since each share contains a random selection between the pairs and also each share block is equally likely to occur for any original secret image block, no information of the secret image can be gained by examining only one share. Hence, our proposed scheme is perfectly secure [32].

Another important characteristic of VCS is contrast [33]. Contrast represents the difference between the gray-levels of the black and white regions in the image, and good contrast reflects the clear distinguishing of regions of white and black in an image. For all the visual cryptography schemes that were described in Chapter 1, the contrast of the reconstructed image was lower than the original image. Traditional VCS, for example, is known to have poor contrast since white pixels become blocks of subpixels that are only 50% white while being 50% black. As a result, the relative contrast for this scheme is $\beta = 1/2$ and the loss of contrast is 50% which is a high loss of contrast and has negative affects on the reconstructed image quality.

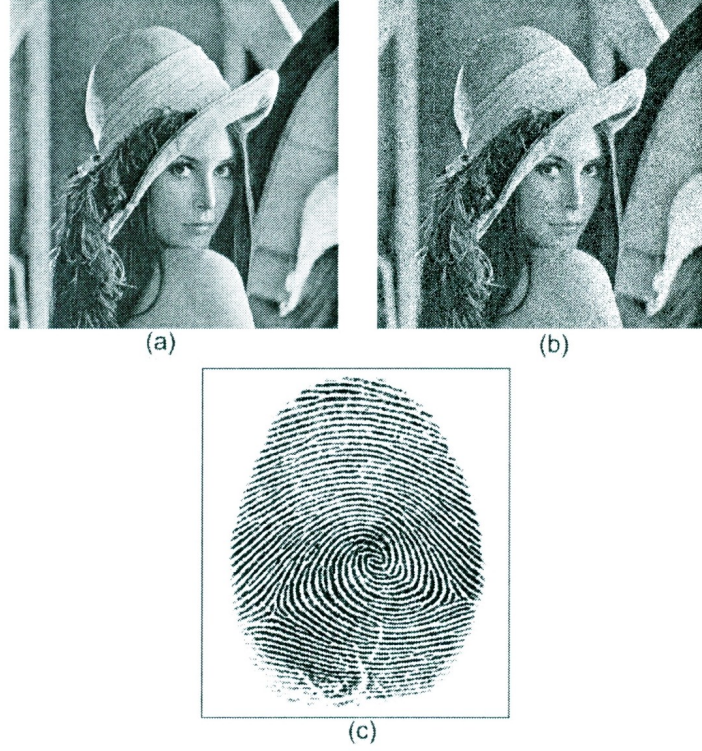


Figure 3.3: Secret images: (a) gray scale Lena; (b) halftoned Lena; (c) binary fingerprint

According to the encoding process of our proposed scheme, all blocks of pixels in the original secret image which are all white, all black, or 50% white / 50% black are all perfectly recovered when the shares are stacked with XOR operation, resulting in the preservation of the contrast in the original secret image. But in some cases as described in the example of Section 3.2.1, where blocks with one black or one white pixel are the secret blocks, they are mapped to blocks with 2 black and 2 white pixels or 4 black and 4 pixels. Hence, the mapping process can degrade the contrast for these secret blocks since one of the 4 subpixels in the recovered block will be in error when compared to the original secret image, but the remaining 3 subpixels remain correct. As there are 16 block models available, the total number of pixels across all

Table 3.4: Comparison of secret block distributions (In number of 2×2 blocks)

Secret images	4 white	4 black	3 white	3 black	2 white (black)
Binary Fingerprint	149559	50040	7137	6908	8228
Halftone Lena	1527	2801	15112	16646	29450

models is 64. Hence, if we assume each model is equally likely to be selected, based on the mapping process, only 8/64 of pixels are in error while 56/64 of pixels appear the same as the original secret block. Therefore, in our scheme, assuming randomly distributed pixels blocks in the original secret image, as estimated 12.5% of the pixels in the recovered image are in error.

3.4 Numerical Experiment Results

In order to explore the issues of contrast and pixel errors, an experiment is conducted on four different visual cryptography schemes. In Chapter 2, we reviewed three different visual cryptography schemes that prevented image size expansion: a probabilistic scheme [17], Chou’s scheme [20] and MLVSS scheme [27]. In this section, we compare these earlier schemes with our proposed schemes based on numerical experiment. In this experiment and the following experimental results in this chapter, two different images are considered as a secret image: one halftoned grayscale image known as Lena and a binary image of a fingerprint, with the size of 512×512 pixels and 784×1132 pixels, respectively. Figure 3.3 illustrates the Lena and fingerprint images. Grayscale images are different from binary images. Grayscale is a range of shades of gray and the varying intensity of black and white pixels produce a gray tone to the

human visual system while binary image is only black and white. In order to check the feasibility of our proposed scheme on different images, we have selected halftoned Lena and fingerprint images due to the variety of the distribution of black and white pixels and more importantly, the variety of secret blocks they present. Observing the two images, it is clear that the fingerprint image has more secret blocks with 4 white pixels and less blocks with 2 white and 2 black pixels while the halftoned Lena is likely to have fewer secret blocks with 4 white pixels but more blocks with 2 white and 2 black pixels. As described in our algorithm, the encoding process and mapping is based on the density of black and white pixels in each secret block, therefore it is important to apply our experiments on images which have different distributions of block models. To compare the distribution of black and white pixels in secret blocks of two images, we have computed the number of secret blocks with 4 white, 4 black, 2 white (and 2 black), 3 white and 3 black pixels for each image. Results are indicated in Table 3.4. The number of secret blocks in each image support the visual observation, but in more detail. In the numerical experiment, we have computed the number of black and white pixels for two secret images. As well, we have computed the number of black and white pixels for the reconstructed images after applying different visual cryptography schemes and compared the results. Results of this experiment are shown in Tables 3.5 and 3.6. In these tables, the fraction of black represents the number of pixels of the reconstructed secret images that appear as black divided by the total number of pixels in the images. The pixel error calculates the percentage of all the recovered black and white pixels in the reconstructed images that are different from the black and white pixels in original secret image.

Table 3.5: Comparison of recovered image characteristics for halftoned Lena

Halftone Lena	Total pixels	Fraction of black	Pixel error
Secret image	262144	0.5212	-
Probabilistic scheme	262144	0.758	35.31%
MLVSS scheme	262144	0.4044	19.94%
Chou's scheme	262144	0.8730	41.45%
Proposed scheme	262144	0.5065	13.86%

Table 3.6: Comparison of recovered image characteristics for binary fingerprint

Binary Fingerprint	Total pixels	Fraction of black	Pixel error
Secret image	887488	0.275	-
Probabilistic scheme	887488	0.637	36.21%
MLVSS scheme	887488	0.613	36.35%
Chou's scheme	887488	0.646	37.96%
Proposed scheme	887488	0.274	1.72%

In this experiment, the size of the halftoned Lena is 512×512 for total of 262144 black and white pixels while the binary fingerprint with size 784×1132 contains 887488 black and white pixels. According to the total pixels obtained after applying different VCS for both images, we know that the size of the reconstructed image in all the schemes is the same as the original secret image. Also, observing the fraction of black pixels, we can see that the fraction of black pixels is substantially different from the original image for all schemes except in our proposed scheme, indicating the recovered image obtained by these schemes are visually darker than the original secret image which is the reason of significant degradations in contrast for these schemes. Likewise, the fraction of pixels in error in the recovered secret images is smallest for our proposed scheme. This indicates that about 13% of the total pixels from original halftoned Lena are incorrectly recovered and only 1 % of the pixels in the fingerprint

image are in error. While the number of pixels in error for halftoned Lena and fingerprint image of 41% and 38% after applying Chou's scheme, and 35% and 36% after applying the probabilistic method. The difference in the number of pixels in error can be easily explained based on the mapping process of our proposed scheme and the distribution of the black and white pixels in the secret blocks in the halftoned images in comparison with the binary images. Results illustrated in Tables 3.5 and 3.6 support the argument that the recovered image after applying our proposed scheme has low noise and good visual quality compared to other schemes.

3.5 Visual Experimental Results and Discussion

In order to check the feasibility of the proposed scheme and also compare the results of our approach with previous approaches, in this section, we have obtained the images from the probabilistic scheme [17], MLVSS scheme [27], Chou's scheme [20] and our proposed scheme. To demonstrate that our method is suitable for both binary and halftone images, two images are used as secret images in our experiment, grayscale Lena and binary fingerprint. In this experiment a grayscale image is converted to the binary image with Floyd-Steinberg halftoning method [30].

Figures 3.4 and 3.5 are the results obtained by applying the probabilistic method on these two secret images. As is expected, the visual quality of the recovered images are poor. In their method, as we described before, one of the columns of basic matrices are chosen to encode a pixel. According to Table 2.4, the black secret pixels are fully recovered while the probability that a white secret pixel is encrypted as a black pixel on the secret image is $1/2$. Since the white pixels are not fully recovered, the superimposed images look darker and are covered by random noise like a mist that

affects the image quality.

Figures 3.6 and 3.7 demonstrate the results of Chou's visual secret sharing scheme. Although this is a secure non-expansion scheme, compared to the original images, the quality of the recovered images is poor due to the low contrast between black and white pixels causing a darkening effect. As explained in Chapter 2, all the blocks of four pixels containing 2 to 4 black pixels turn into blocks of four black pixels, while secret blocks with 0 and 1 black pixels turn into a block of four white pixels. This means that the pixels which appeared black on the shares outnumber the white ones and the recovered secret image shows more blackness.

The third set of results are obtained after applying the MLVSS scheme and shown in Figures 3.8 and 3.9. In this approach, since each secret block that consists of 3 or 4 white pixels appears as half white and half black secret blocks, some information may be lost in the reconstructed secret images. Observing the results shown in Figures 3.8 and 3.9 and also according to results in numerical experiment, the visual quality of the results obtained by this method is better than the two other reviewed approaches. The reason is that the secret blocks containing two black and two white pixels appear the same in the reconstructed image and this can enhance the image quality. But, examining the shares illustrated in Figures 3.8 and 3.9, we have discovered this scheme reveals secret information on shares. The leakage of information was expected by the encoding process of Chen's scheme; while the encoding process for some secret blocks is not random and there is only one pattern existing for recovering those secret blocks. As we discussed earlier, security is one of the most important parameters in every visual cryptography scheme. Although the above scheme succeeded in preventing size expansion, it still has a significant problem of leakage of the secret information.

The last experiment is applied using our novel visual secret sharing scheme without size expansion as seen in Figure 3.10 and 3.11. As we have described at the begin-

ing of this chapter, the security of our method is the same as the traditional visual cryptography scheme and examining the shares ensures the security of this approach as the share images are random and do not reveal any information about the secret image. The reconstructed images in Figure 3.10 and 3.11 demonstrate the effects of this approach. There is a significant improvement in the reconstructed image quality compared to the other 3 non-expansion schemes. Both the reconstructed Lena and fingerprint images have the most similarity to the original images. Details including eyes, hat, edges, background and fingerprint minutia of the images are recovered more clearly by our construction. Details are preserved in our scheme because all the secret blocks except the ones that have 1 white or 1 black pixel are fully recovered. Hence, the proposed scheme does not break the arrangement between black and white pixels too much in an image which enhances the contrast and provides better image quality. The fraction of pixel errors indicated in Table 3.5 and 3.6 is clear evidence for the improved pixel recovery of our proposed scheme in comparison with the other 3 non-expansion visual cryptography schemes. About 99% and 87% of the pixels in fingerprint image and halftoned Lena have been properly recovered respectively.

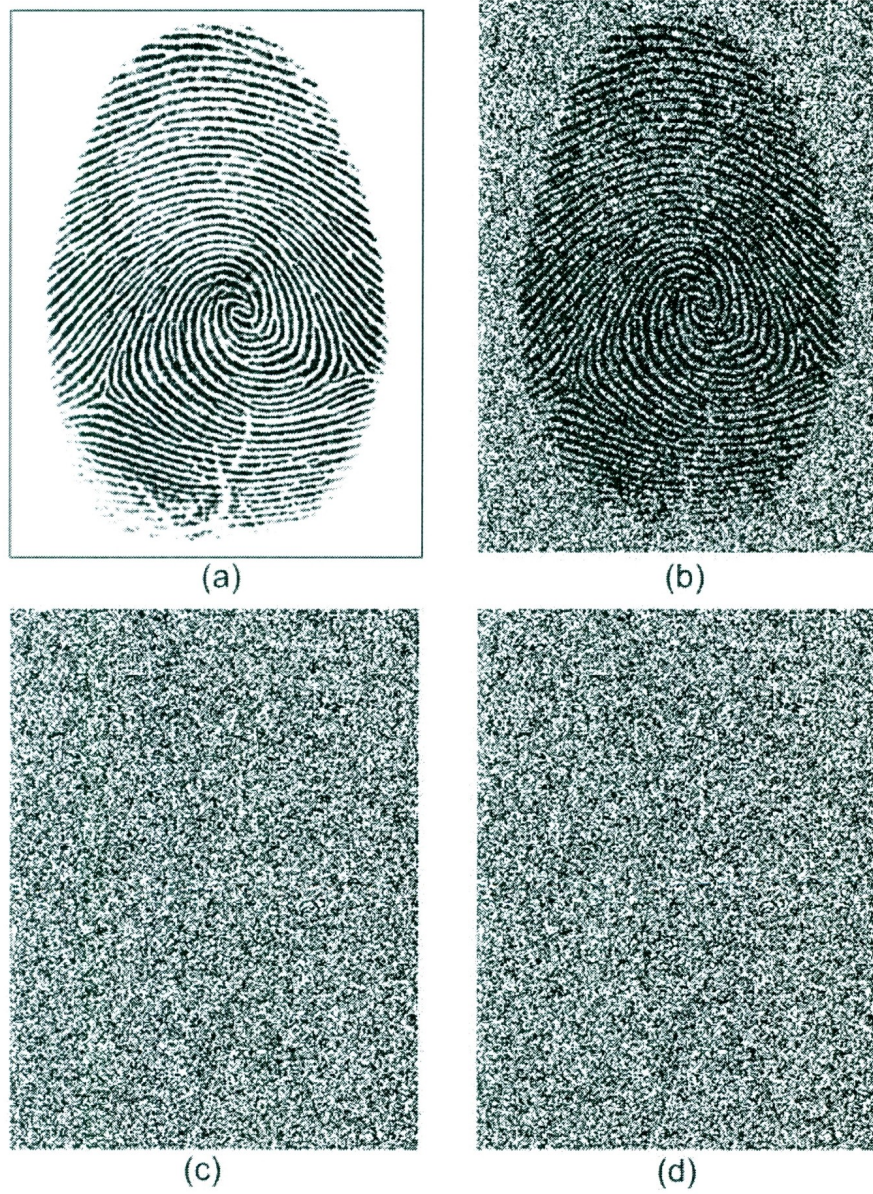


Figure 3.4: Probabilistic $(2, 2)$ experimental results: (a) binary fingerprint; (b) recovered image; (c) share 1; (d) share 2

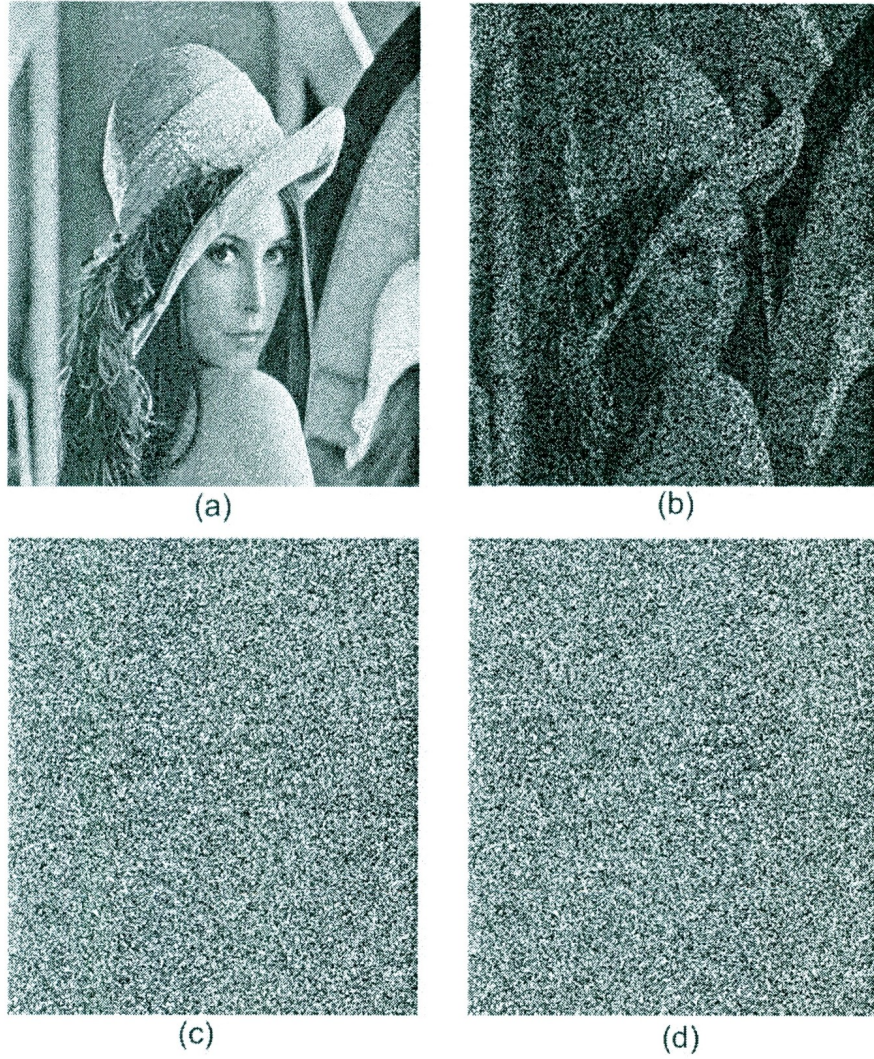


Figure 3.5: Probabilistic $(2, 2)$ experimental results: (a) halftone Lena; (b) recovered image; (c) share 1; (d) share 2

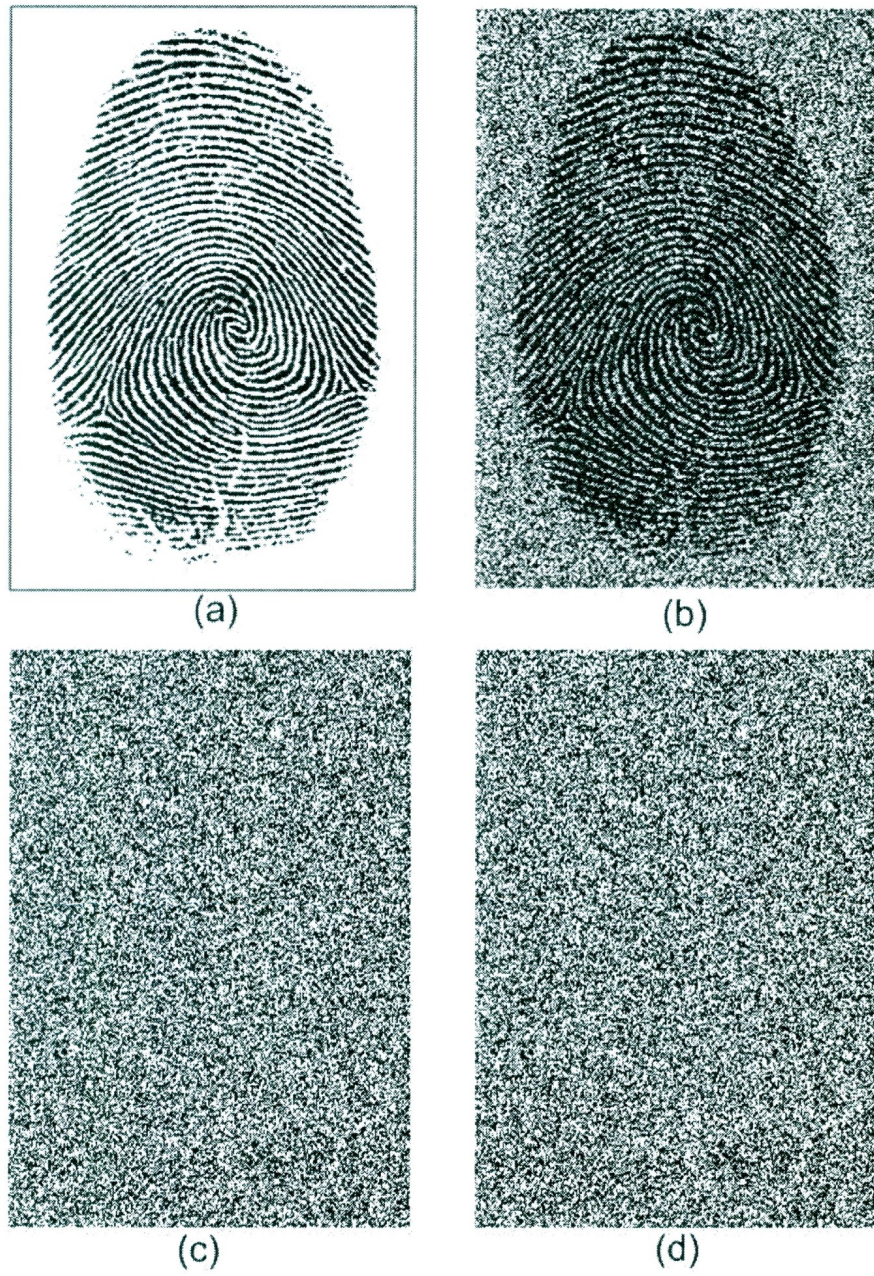


Figure 3.6: Chou's (2, 2) experimental results: (a) binary fingerprint; (b) recovered image; (c) share 1; (d) share 2

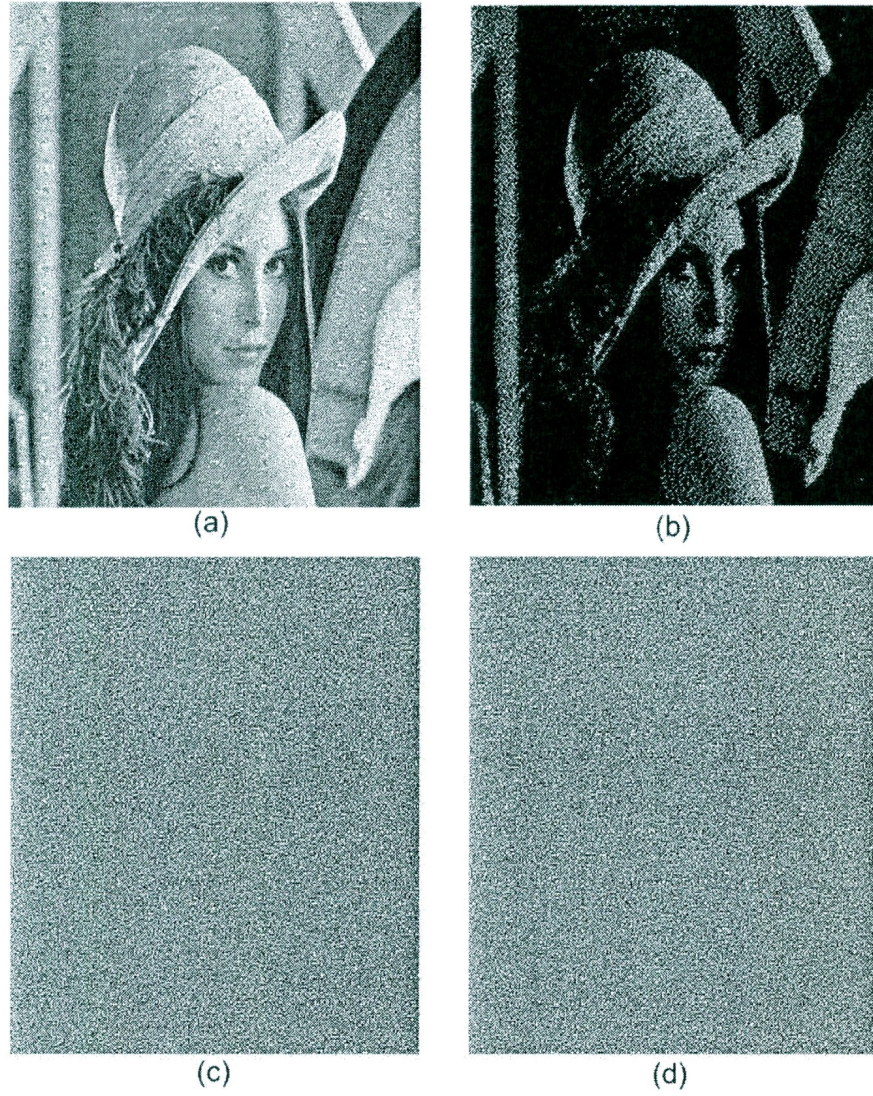


Figure 3.7: Chou's (2, 2) experimental results: (a) halftone Lena; (b) recovered image; (c) share 1; (d) share 2

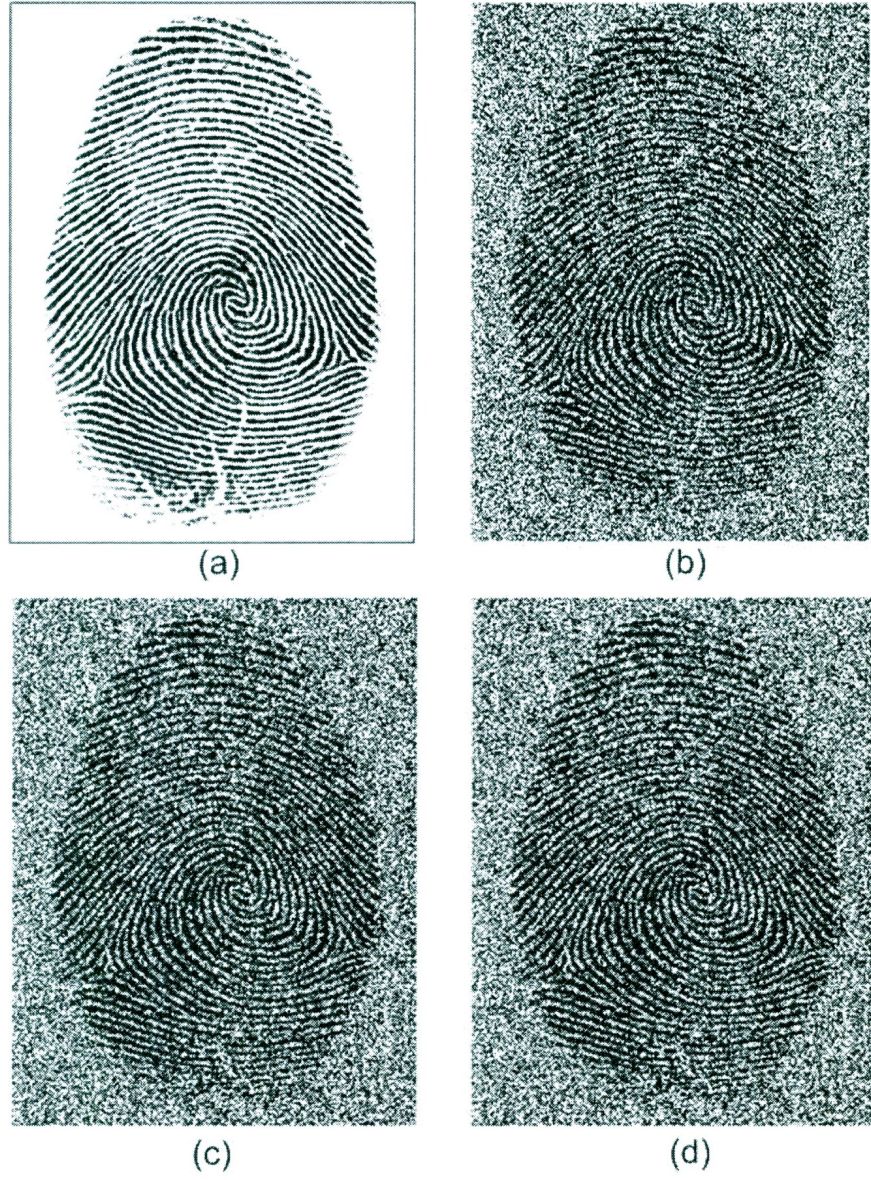


Figure 3.8: MLVSS (2, 2) experimental results: (a) halftone fingerprint; (b) recovered image; (c) share 1; (d) share 2

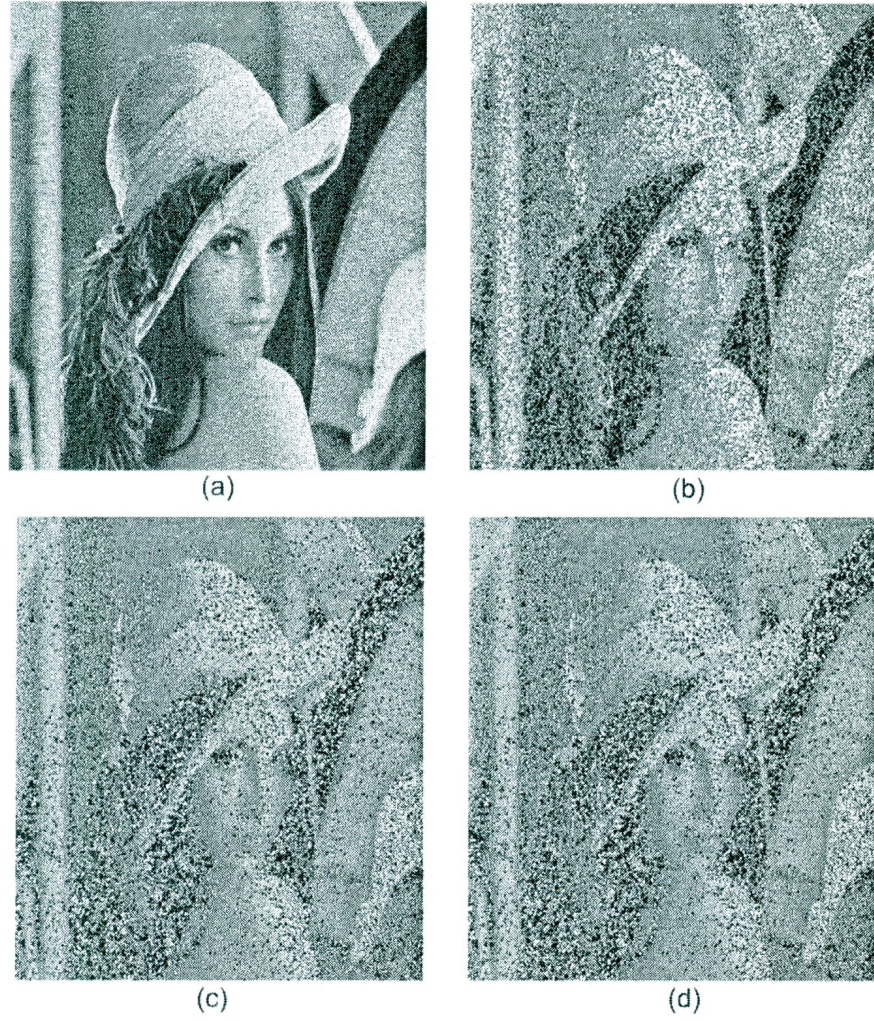


Figure 3.9: MLVSS (2, 2) experimental results: (a) halftone Lena; (b) recovered image; (c) share 1; (d) share 2

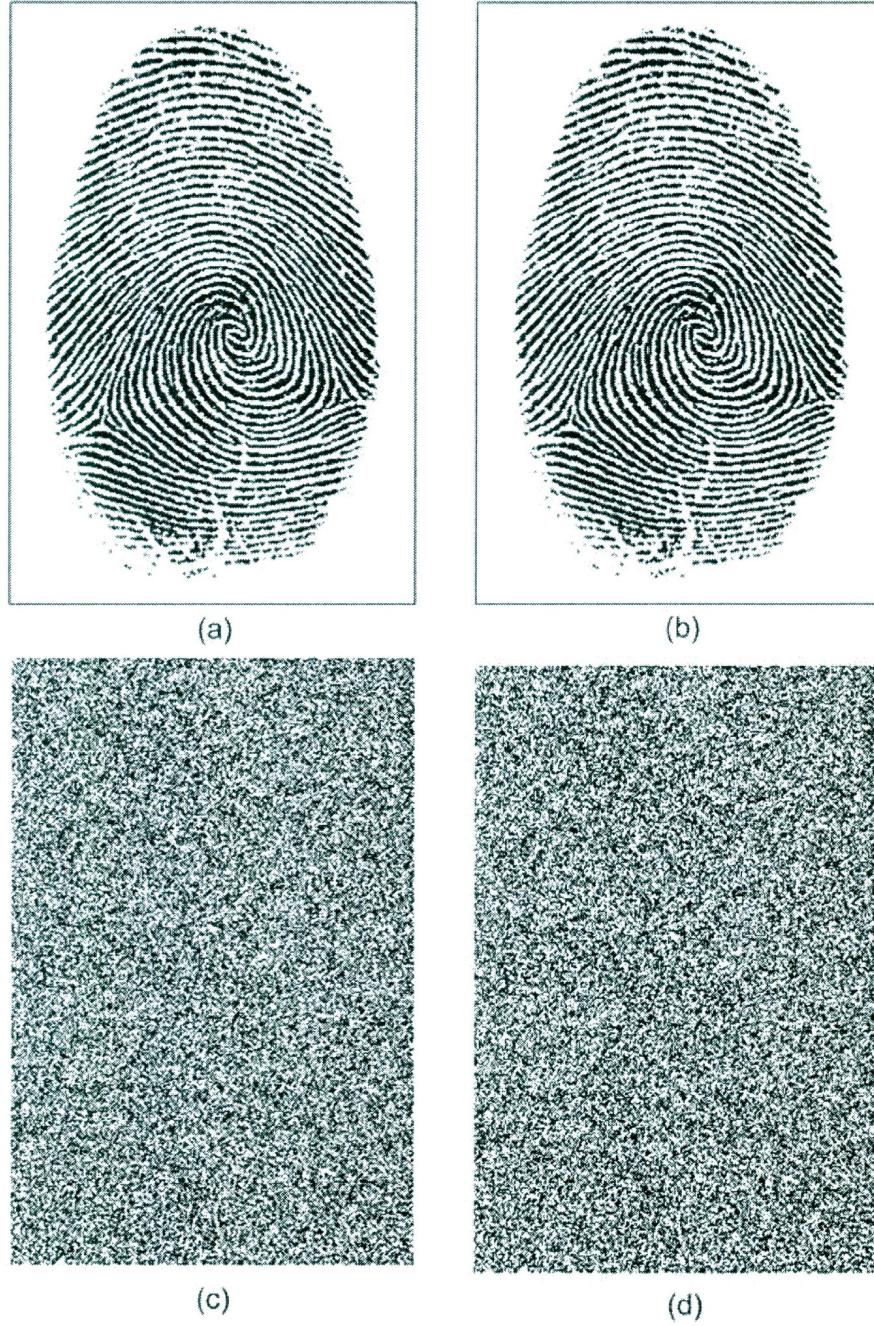


Figure 3.10: Proposed $(2, 2)$ scheme experimental results: (a) binary fingerprint; (b) recovered image; (c) share 1; (d) share 2

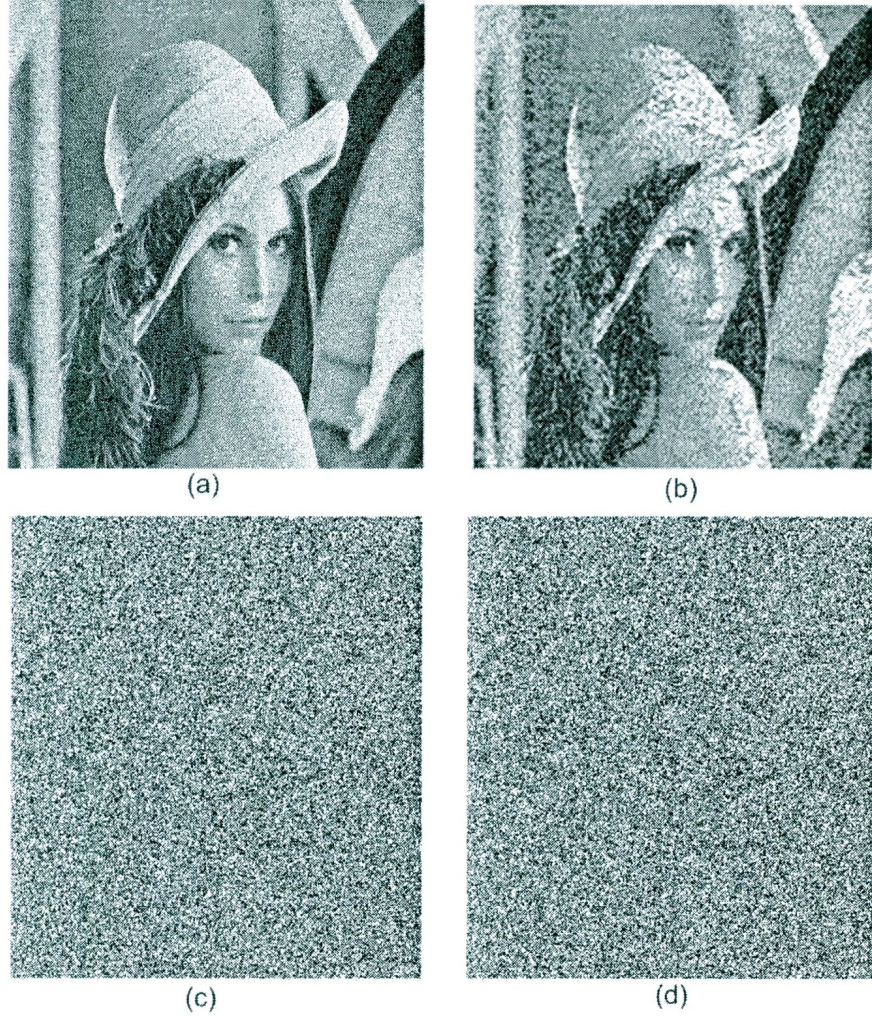


Figure 3.11: Proposed $(2, 2)$ scheme experimental results: (a)halftone Lena; (b) recovered image; (c) share 1; (d) share 2

3.6 Conclusion

The traditional visual cryptography scheme is a perfectly secure method that encodes a secret image into random shares and recovers the image by superimposing the

shares. However, this scheme leads to the degradation in the quality of the recovered images and in image size expansion. In this chapter, we have modified traditional visual cryptography by introducing a novel $(2, 2)$ visual cryptography scheme without size expansion. The principle of this scheme is to divide a secret image into blocks of four pixels named secret blocks. According to our encoding rules, we encode each secret block one at a time, and create two noise-like random shares. The encoding process is based on the number and distribution of black and white pixels, thereby allowing the secret image to be clearly restored by using the XOR operation. Our novel scheme can be applied on both binary and halftone images and does not increase the number of pixels required to represent the shares or the recovered image. The proposed scheme also differs from other non-expansion methods in a way that it recovers the pixels of the original secret image with the minimum error. Since the scheme preserves the arrangement of a black and white pixels, the reconstructed image is similar to the original image and can easily be interpreted by human vision. In this chapter, we present two experiments with results to show the applicability of our scheme to the problem of image expansion and the loss in contrast in comparison with the other non-expansion schemes. Our scheme presents the best image quality of the recovered image, while ensuring no image expansion and guaranteeing the perfect security of traditional VCS.

Chapter 4

Processing Grayscale Secret Images for Use in Visual Cryptography

4.1 Introduction


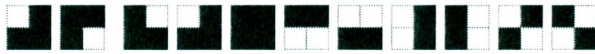

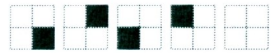
In Chapter 2, we introduced visual cryptography schemes which are developed to split a secret image, composed of black and white pixels, into a number of shares to protect the secret information. Therefore, these methods can deal with only two pixel tones: black and white. However, sharing secret grayscale images is also of considerable interest. For example, a face image on an ID card will tend to be grayscale, if not colour. Hence, using halftoning techniques to convert grayscale images to binary images is a useful pre-processing step for visual cryptography [20]. The halftoning process itself will result in a reduction of the grayscale image quality. Since visual cryptography schemes also result in loss of information, using halftoned images as the secret image in VCS would lead to additional loss of contrast in the recovered images. Based on our research and experimental results in Chapter 3, a method introduced by Chou [20] is an efficient non-expansion scheme that can be applied to

traditional VCS, multi-image VCS and EVCS for halftoned grayscale images. This method is secure and easy to implement. However, the reconstructed images obtained by this scheme are dark and have poor contrast. Thus, the human visual system may have difficulty to identify the secret information from the recovered image. In order to enhance the visual quality of the recovered images, in this chapter, we modify Chou's visual cryptography scheme by introducing three algorithms. Using these algorithms in multiple image VCS and EVCS remedies the drawbacks of image size expansion and contrast degradation of the resulting images and makes these algorithms suitable for different authentication applications.

4.2 Chou's Non-expansion Method

For the goal of producing no pixel expansion in both shares and the reconstructed image, Chou proposed a method in his 2002 Master's thesis [20]. Unlike the other visual cryptography methods which rely on pixel-wise operations, this approach is based on block-wise operations. Chou's scheme considers four pixels in one 2×2 block, referred as a secret block, and generates the shares block by block. As each secret block with four pixels encodes into two secret shares each containing four pixels, the size of the reconstructed image is the same as the original secret image after stacking the two shares together. In this technique, all the secret blocks in an image need to be processed before VCS encoding or, in another words, each secret block is replaced by one of a predetermined set of secret blocks which are eligible to be used in the encoding process and share generation. Each secret block is replaced by the corresponding predetermined candidate which is a block with 4 white pixels or a block with 4 black pixels. The procedure of converting secret blocks to their appropriate corresponding block is called the *block replacement process* in this chapter. Also, the

Table 4.1: The block replacement process proposed by Chou

Category	Classification	Secret blocks before classification
Black		
White		

two predetermined blocks for Chou's scheme are called *white block* and *black block*.

The block replacement process in Chou's scheme is based on a number of black and white pixels in each secret block. Table 4.1 shows Chou's classification rules. According to this table, all the secret blocks of four pixels are classified into two groups named black and white. If the number of black pixels in a secret block is larger or equal to 2, the secret block converts to a black block. If the number of black pixels in a secret block is less than or equal to 1, it is converted to a white block. This step produces a new secret image which contains only white and black secret blocks. The image obtained from this step is referred to as a *processed secret image*. The processed image is now ready to be used as a secret image in visual cryptography schemes such as traditional VCS. Figure 4.1(a) and (c) shows two halftoned images named Lena and baboon, both with the size 512×512 . The original two grayscale images are transformed to halftoned images by utilizing the Floyd-Steinberg halftoning technique as described previously. Figure 4.1 (b) and (d) are the processed Lena and processed baboon results from Chou's block replacement process, respectively. Obviously the results obtained by this step are unsatisfactory, as the processed secret images are very dark with poor quality and the loss of many fine details in the images.

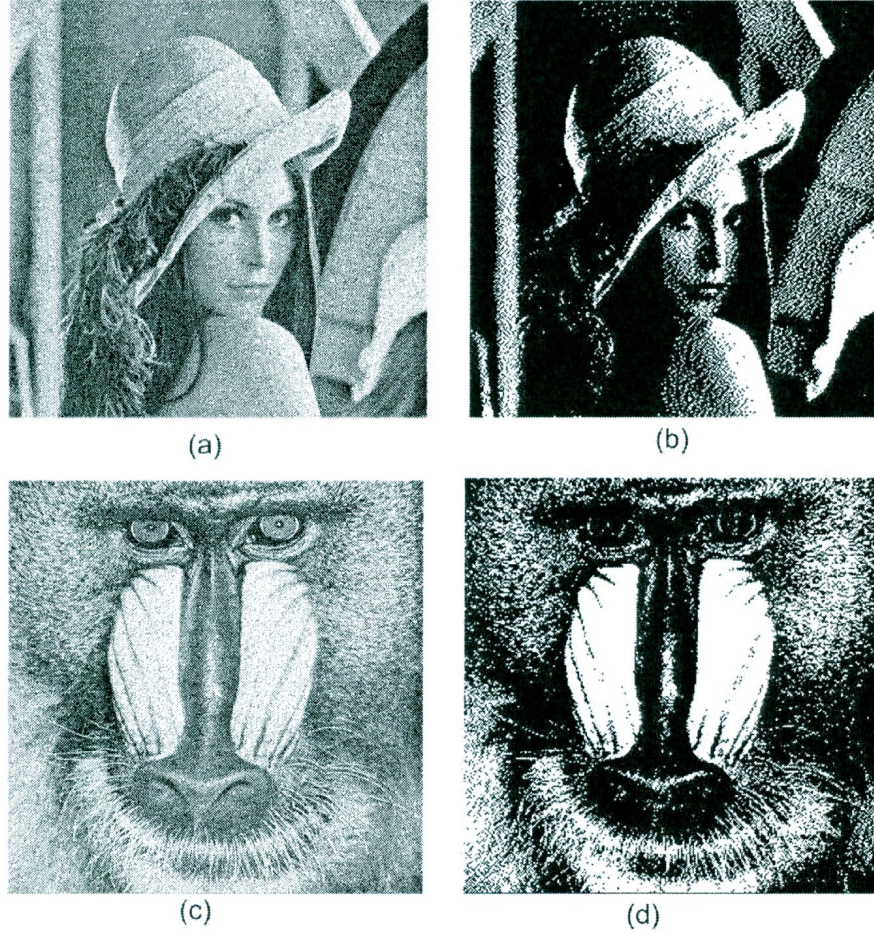


Figure 4.1: Block replacement process in Chou's method: (a) halftoned Lena; (b) processed Lena; (c) halftoned baboon; (d) processed baboon


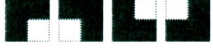

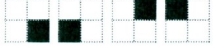



The reason for the very poor visual quality of the processed images can be explained according to the classifying rules in Chou's block replacement process. As every block of 2 white and 2 black pixels in the original secret converts to black secret blocks, the black pixels outnumber the white pixels in the processed secret image. This allocation results in contrast degradation by losing the information of two pixels in a secret block. It is clear that, when the processed secret image uses as a secret

image in visual cryptography schemes, the recovered secret image obtained is also very dark and difficult to interpret by human eyes. Chou's method may be more efficient for binary black and white images, as these images usually do not have many blocks of four pixels with 2 black and 2 white pixels in comparison with halftoned images. Our aim is to propose techniques to improve the block replacement processing step proposed by Chou, by replacing the secret blocks in the halftoned image to both light and dark tones. Thus, the visual appearance of the halftoned processed image is improved by reducing the black pixels and also the reconstructed image looks smoother and more visually pleasing.

4.3 Random Conversion Method

Measuring the quality of the halftoned image is not easy as the definition of quality varies from application to application. One of the measurement methods is based on the human visual system (HVS) [34]. Researchers and studies in the area of human vision indicate that human vision is a complicated nonlinear system. Also, the human vision system has a low pass filter characteristic, so it can interpret low frequency details more than high frequency details [35]. Distributing black and white pixels as homogeneously as possible in an image is one way to increase the high frequency components and create an illusion of a clearer image. As noted before, during the block replacement process, the majority of secret blocks in a halftoned image turn to black and the minority of secret blocks turn to white. Therefore, reducing the majority pixels and spreading minority pixels and majority pixels homogeneously is an effective technique to improving the visual quality of the image viewed by the human visual system. Hence, we modify Chou's scheme by incorporating a random

Table 4.2: The block replacement process in random conversion method

Category	Classification	Secret blocks before classification
Black		
White		
Black or white	 or 	

conversion technique as a new block replacement process. Our goal is to produce a visually pleasing processed secret image with homogenous distribution of black and white blocks.

In this approach, a grayscale secret image with the size $2x \times 2y$ is transformed into a halftoned image, and the halftoned image is divided into several non-overlapping 2×2 blocks with four pixels, called secret blocks. Similar to Chou's scheme, each secret block needs to be replaced by a corresponding predetermined block. If the number of black pixels in a secret block is equal to or greater than 3, then the secret block is regarded as black block. If the number of black pixels in a secret block is equal to or less than 1, the secret block is regarded as a white block. Furthermore, if the number of black pixels are 2, then the secret block is randomly converted with equal likelihood to a white block or a black block. In this chapter, we refer to a block with two black and two white pixels as a candidate block.

Table 4.2 demonstrates the block replacement process in our random conversion method, Figure 4.2 illustrates the halftoned processed images obtained after applying this technique. The simulation results show that the proposed method can improve

the visual quality of the processed halftoned image by effectively reducing the number of black blocks and replacing some of them with white blocks instead. Although in both processes (Chou's scheme and our random conversion scheme), the number of pixels in error is the same for candidate blocks, distributing black and white blocks in a more balanced manner can lead to a better visual quality of the processed image. It is clear that the more homogeneously the black and white blocks are distributed, the better visual quality we have for the processed image and consequently the better reconstructed secret image to be obtained from a VCS.

In our scheme, since all the candidate blocks are randomly converted to black or white blocks, homogeneity of the distribution of black and white blocks is a considerable issue and cannot be guaranteed. For example, assume an image has 10 candidate blocks adjacent to one another. If the randomness applies on candidate blocks, different replacement of black and white blocks can appear. Therefore there is a probability that only one or two of the blocks may convert to white blocks and the rest may be replaced with black blocks or vice versa. It is obvious that in this block replacement, the black and white pixels do not necessarily distribute uniformly and homogeneously. To obtain a visually pleasant image, it is important to convert and distribute the candidate blocks to black and white blocks as evenly as possible, and with a similarity to the original image as possible. The more similar the two images, the higher the image quality of the processed halftone image. The two proposed algorithms in the following section are preferred solutions to the problem of the potential lack of homogeneous distribution in the random conversion method.

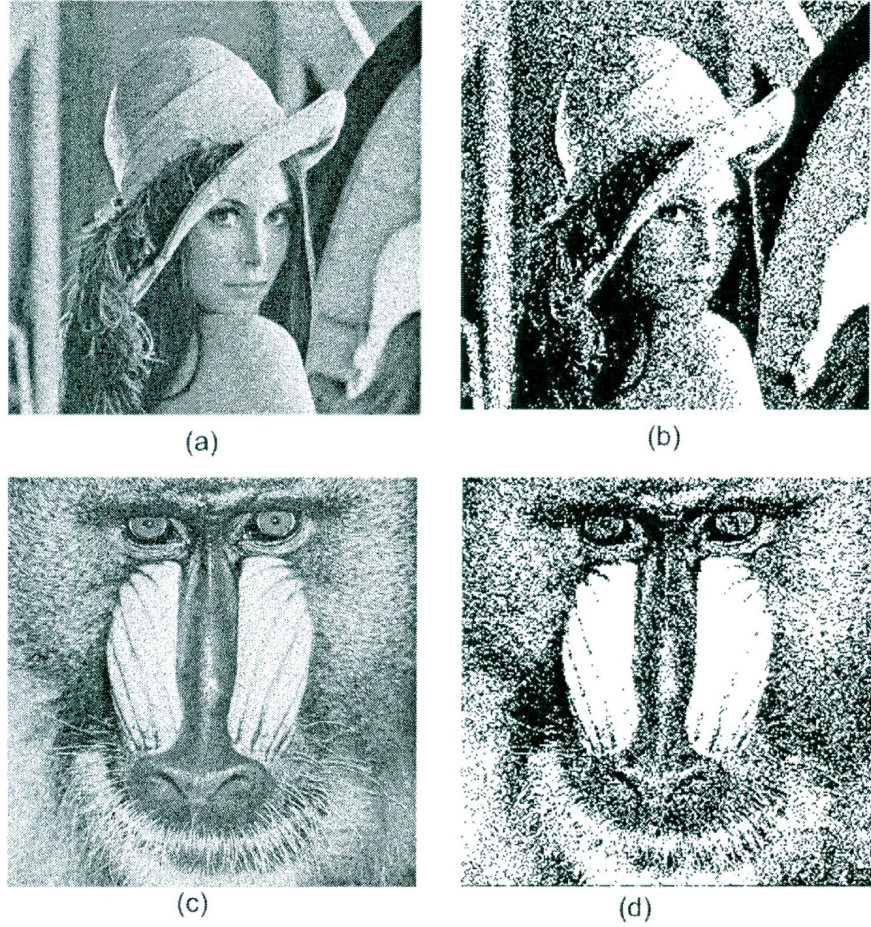


Figure 4.2: Block replacement process in random conversion method: (a) halftoned Lena; (b) processed Lena; (c) halftoned baboon; (d) processed baboon

4.4 Clustering and Thresholding Method

As argued above, the choice of the patterns in the block replacement process has an impact on the characteristics of the processed halftoned image and the random process for the candidate blocks may not distribute the black and white blocks as uniformly as possible. As a result of the randomness, the visual quality of the processed

image and also the reconstructed image may be reduced. Therefore, we now propose new algorithms, that can deliberately process and convert the candidate blocks to appropriate blocks that result in improved visual quality. In this section, we propose two new algorithms inspired by the concept of the void-and-cluster halftoning technique [36].

4.4.1 Void-and-Cluster Halftoning Method

As was reviewed in Chapter 2, halftoning is a process of transforming a grayscale image to a pattern of black and white pixels in a way that the transformed image has the appearance of the original grayscale image. To have an image with good resolution and visual quality, different halftoning techniques have been proposed [31]. We reviewed the error diffusion method [30] in Chapter 2 and now we utilize the concept of the void-and-cluster dithering array algorithm to improve the visual quality of the processed halftoned image. In the dither array halftoning method, each pixel in the image is compared with the threshold value to decide the location and tone of the output image. The void and cluster algorithm [36] is a type of dither array method for producing patterns that distribute black and white pixels homogeneously. If more than half of the pixels in an image are black, then the majority pixels are black and minority pixels are white or vice versa. In this method, a *cluster* refers to a tight group of minority pixels and *void* refers to a large group of majority pixels. The purpose of void-and-cluster algorithm is to determine the tightest cluster location and largest void location in an image, then move pixels from tight clusters into large voids [36]. This strategy will lead to a more uniformly halftoned image with pleasant visual quality.

4.4.2 Clustering and Constant Threshold Method

Our new method is inspired by the concept of the void-and-cluster dither array algorithm. In this algorithm, instead of random conversion of candidate blocks, we propose a new pattern for replacing candidate blocks based on the distribution and intensity of the majority and minority pixels in a secret halftoned image. We refer to this method as a Clustering and Constant Threshold (CCT) algorithm. The process of transforming a halftoned secret image to the processed secret image with better visual quality is described in the following section.

4.4.2.1 CCT Method

We start with transforming a grayscale image into halftoned image named HS whose width and height are even. As before, HS is divided into a number of non-overlapping blocks of 2×2 pixels. In the first phase of the block replacement process, if the secret block contains 3 or 4 black pixels, it is regarded as a black block and if a secret block contains 3 or 4 white pixels, it is regarded as a white block. Other secret blocks (all black, all white and candidate blocks) do not change in this step. The output of this step is called the initial processed image. This initial image only contains white, black and candidate blocks. After this step, the initial processed image is divided into a number of overlapping squares of 2×2 blocks. Each square of 4 blocks is referred to as a cluster in this algorithm. There are 16 pixels available in each cluster and the threshold value is taken to be 8. Therefore if the number of black pixels in each cluster is more than 8, we call it a dense cluster and if the number of white pixels is less than 8, it is called sparse cluster in this algorithm. However, if the number of black and white pixels are equal it is a uniform cluster. After partitioning the clusters, phase 2 of the process starts from the first block top left and then goes through all blocks in the cluster from left to right and then top to bottom. If the

block is a candidate block, the numbers of black and white pixels in its cluster are computed. If the cluster is dense, it means the number of black pixels is more than the threshold so the candidate block should be replaced with a white block. Similarly, in the case of a sparse cluster, the candidate block should be replaced with a black block. In the case that the number of black pixels in the neighbouring pixels in a cluster is exactly 8, the candidate block randomly changes to either a black or white block. This process continues until all the candidate blocks are processed and assigned to white or black blocks.

The output of this algorithm is called the processed image. This procedure aims to create a balance between the number of black and white pixels in every cluster and in the halftoned image. The clustering and constant threshold method is explained in detail with the following example.

4.4.2.2 Example

The following example elaborates phase 2 of the CCT algorithm. In this example, Figure 4.3 is assumed to be the initial processed image of size 6×6 pixels, which contains 9 secret 2×2 blocks: 2 white blocks, 1 black block and 6 candidate blocks. According to the partitioning step, this image is divided into 4 overlapping clusters, each containing 4 secret blocks. The process is started by examining the first secret block in the first cluster (first block top left corner), as is shown in Figure 4.3(a). Because this block is white, no processing is needed; therefore we move to the next block on the right and analyze the second block in the cluster which is a candidate block. As this block needs to turn to either a black or white block, the number of black pixels in its cluster are counted for thresholding. As there are 4 black pixels available in this cluster, the candidate block is replaced with a black block based on our thresholding rule. After this, the first block from the left in the second row is

examined and obviously it does not need processing as it is a white block. According to the cluster in Figure 4.3 (a), the last block in this cluster is a candidate block and is replaced with black block as there are 6 black pixels in the cluster which is less than our threshold value. It should be noted that the number of black pixels at each iteration is dependent on the last candidate block update.

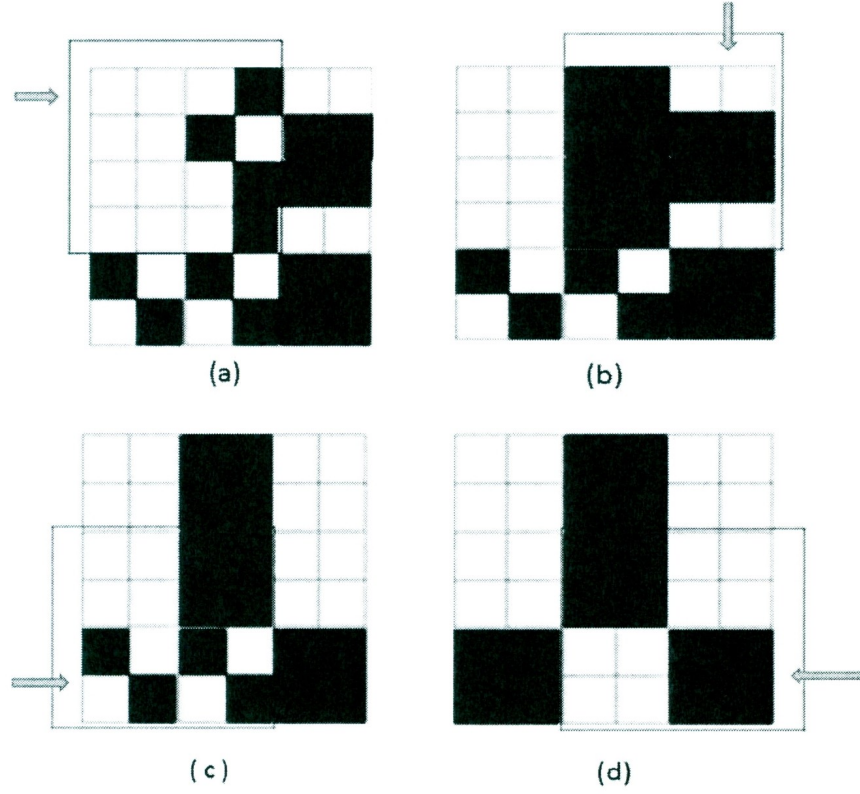


Figure 4.3: Example of the block replacement process in CCT method

Figure 4.3(b) depicts the updated initial processed image and the second cluster, which has two of the blocks processed in the previous cluster, while the other two blocks need to be evaluated. Obviously, the first candidate block in the second cluster is replaced with a white block since there are 12 black pixels in this cluster which is more than the threshold value. Based on this strategy, the last candidate block in

this cluster is also replaced with a white block. In the next iteration, there are two candidate blocks in which the first one randomly turns to a black or white block as it is a uniform cluster. In the figure, we assume it has been replaced with a black block; obviously, the next candidate block is replaced with a white block according to the number of black pixels after updating the last candidate block. The thresholding and clustering process continues until all the secret candidate blocks in an initial processed image are changed to black and white blocks. The result of this example is illustrated in the Figure 4.3(d) after 4 iterations are executed.

It is noted that the edges of the image (top row and the left column) is non-causal, so they are dependent on blocks that may change later. For example, in Figure 4.3(a), the first candidate block that needs to be replaced is in the top row of the first cluster and its replacing condition is based on the number of black and white pixels of the 3 other secret blocks in the cluster. One of these 3 secret blocks is a candidate block and it also needs to be changed later. In all the other clusters except the ones that contain blocks from the first row or left column, only one secret block needs to be processed (ie. Figure 4.3(d)) and it is causal. Another approach that can be taken for edges is to replace all the secret blocks in the top row and the left column of the image randomly to a white or black blocks in advance.

4.4.2.3 Experimental Results

The black and white blocks in the processed image obtained by the proposed algorithm are distributed as homogeneously as possible and there is a mitigation of sparse and void clusters in this image. To analyse this more, Figure 4.4 shows two final processed images which are processed by the CCT method. As shown, there is a significant improvement in the visual quality and clarity of the results in Figure 4.4 in comparison with the results obtained after applying Chou's scheme in Figure

4.1. Comparing the results of this method with the random conversion method in Figure 4.2, it can be observed that the very light and very dark regions of the final processed images are greatly reduced. Although features such as Lena's nose and lips are not recovered properly, there is an improvement in some features such as Lena's hair and the baboon's eyes. The results generated by our proposed method is more homogeneous and visually smoother than the random conversion method.

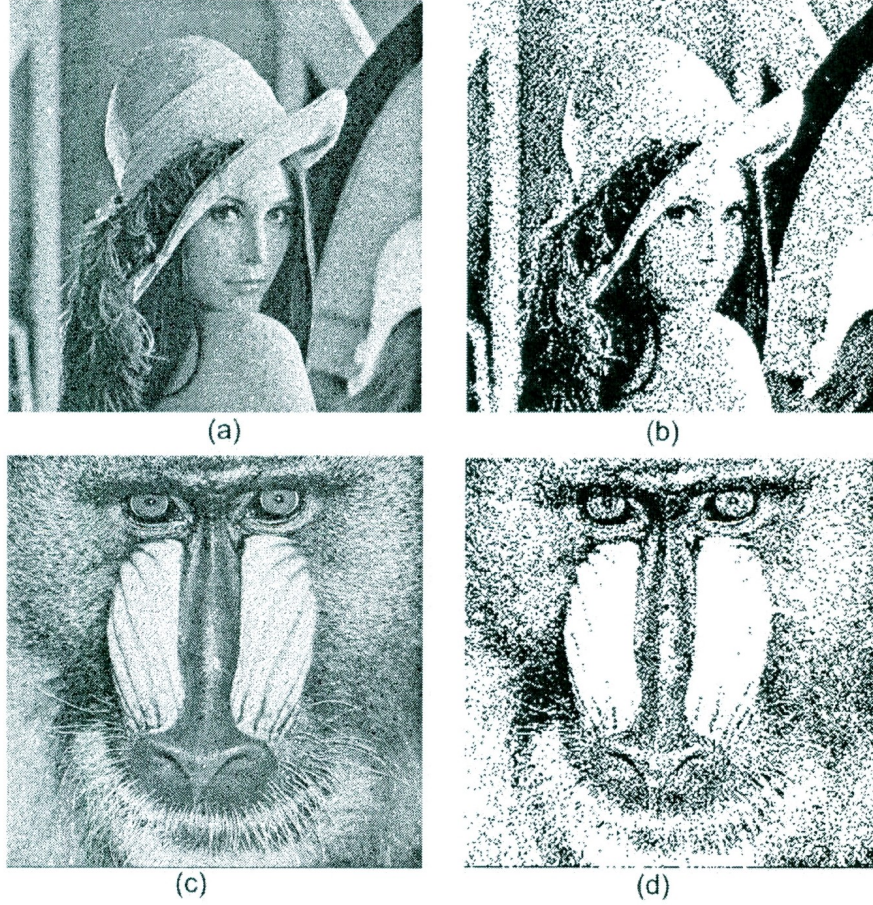


Figure 4.4: Block replacement process in CCT method: (a) halftoned Lena; (b) processed Lena; (c) halftoned baboon; (d) processed baboon

4.4.3 Clustering and Variable Threshold Method

We now present another novel and effective method for replacing the candidate blocks, which we refer to as the clustering and variable threshold (CVT) method. This method is similar to the clustering and constant threshold method. The main new task in this pattern is to assign and change the candidate blocks based on the distribution of black and white pixels in an original halftoned image. As discussed before, keeping the details of grayscale image in the halftoned binary image is very important. Therefore, we improve the random conversion technique by changing the candidate blocks in a way that the number of black and white pixels in each cluster have the most similarity to the original image, hence the homogeneity between black and white pixels is also encouraged. The CVT algorithm is summarized in the following section.

4.4.3.1 CVT Method

We start with transforming a grayscale image into a halftone image named HS and dividing the HS image into a number of non-overlapping blocks of 2×2 pixels. Then, the HS image is divided into a number of overlapping squares of four 2×2 blocks. As in the CCT method, each grouping of 4 blocks is referred to as a cluster. In the next step, the number of black pixels in each cluster from the HS image are counted and saved in a template. This number is the threshold value. The first phase of the process starts with classifying all the secret blocks containing 1 black (resp. white) pixel. This phase is similar to phase 1 in the previous algorithm; therefore, if the secret block contains 1 black (resp. white) pixel it is considered as a white (resp. black) block. The image obtained from this step is referred to as the initial processed image.

The second phase starts from the first block in the top left of the first cluster. The

order of processing the secret blocks in each cluster is same as the CCT algorithm. When the first candidate block in a cluster is identified, the number of black pixels in the cluster are counted. The purpose of this algorithm is to keep the number of black and white pixels in the initial processed image as close as possible to the threshold value in the clusters of the HS image. Therefore the number of black pixels in the case of changing the candidate block to the black or white block is computed and is compared to the threshold value that was derived from the same cluster in the HS image. Obviously, if the corresponding candidate block converts to a black block, 2 pixels will be added to the number of black pixels in a cluster and if the candidate block turns to white block, 2 black pixels will be deducted from a cluster. The determination is based on the smallest difference between the threshold and the number of black pixels in the initial image. If changing the candidate block to black makes this difference smaller, the candidate block is converted to a black block. Similarly, if turning the candidate block to white makes this difference smaller, the block converts to a white block. In the case that turning the candidate to black or white produces the same difference, the block randomly converts to a black or white block.

Note that the candidate blocks located in the top row and the left column have the same issues as for the CCT method. The block replacement pattern proposed in this method tries to keep the arrangement of black and white pixels in the processed image close to the original halftoned image. Therefore, the resulting image is homogeneous and similar to the original image. Generally, this new block technique is an enhancement of the previous CCT method.

4.4.3.2 Example

Figure 4.5 is an example of how the proposed algorithm works. A halftoned image of size 6×6 is assumed to be an original halftoned image in this example. According to the proposed algorithm, the HS image is divided into 4 overlapping clusters each containing 4 secret blocks. As shown in Figure 4.5(a), the numbers of black pixels for each cluster are computed and saved in a template. In the next step, phase 1 of the algorithm is applied to the HS image. Figure 4.5(b) is the output of the first phase and is an initial processed image, in which only the black, white and candidate blocks exist. The second phase of the algorithm starts with partitioning the initial processed image into overlapping clusters. Figure 4.5(b) illustrates the first cluster in an initial image; this cluster contains 1 candidate block and 6 black pixels. According to the algorithm, the threshold value is 7 for this cluster and we want to replace the candidate block in a way that the number of black pixels will be very close to 7. It is obvious that if we change the block to black block, the number of black pixels will be 8 and if we turn it to a white block, the number of black pixels in this cluster will reduce to 4. Therefore, the block will be replaced with a black block. This procedure is repeated for the next 3 clusters and the final processed image is shown in Figure 4.5(f). It is noted that, for this example, it is a coincidence that the final processed image of the CCT method in Figure 4.3(d) is the same as the processed image for the CVT method in Figure 4.5(f). In general, the results of the two algorithms differ, as is clear visually from the results of Figure 4.6 compare to Figure 4.4.

4.4.3.3 Experimental Results

The resulting images for the processed Lena and processed baboon after utilizing the CVT method are shown in Figure 4.6. Compared to the results of the CCT method in Figure 4.4, we can see that the second algorithm produces a smoother and clearer

image. Features such as Lena's hat and face and also the baboon's eyes and nose are examples of this improvement. Therefore, we can conclude that the new replacement process can be an improvement of the previous one and can be a better solution to the problem. Of course, the processed images in both figures show obvious improvements in comparison with the random conversion method and Chou's method.

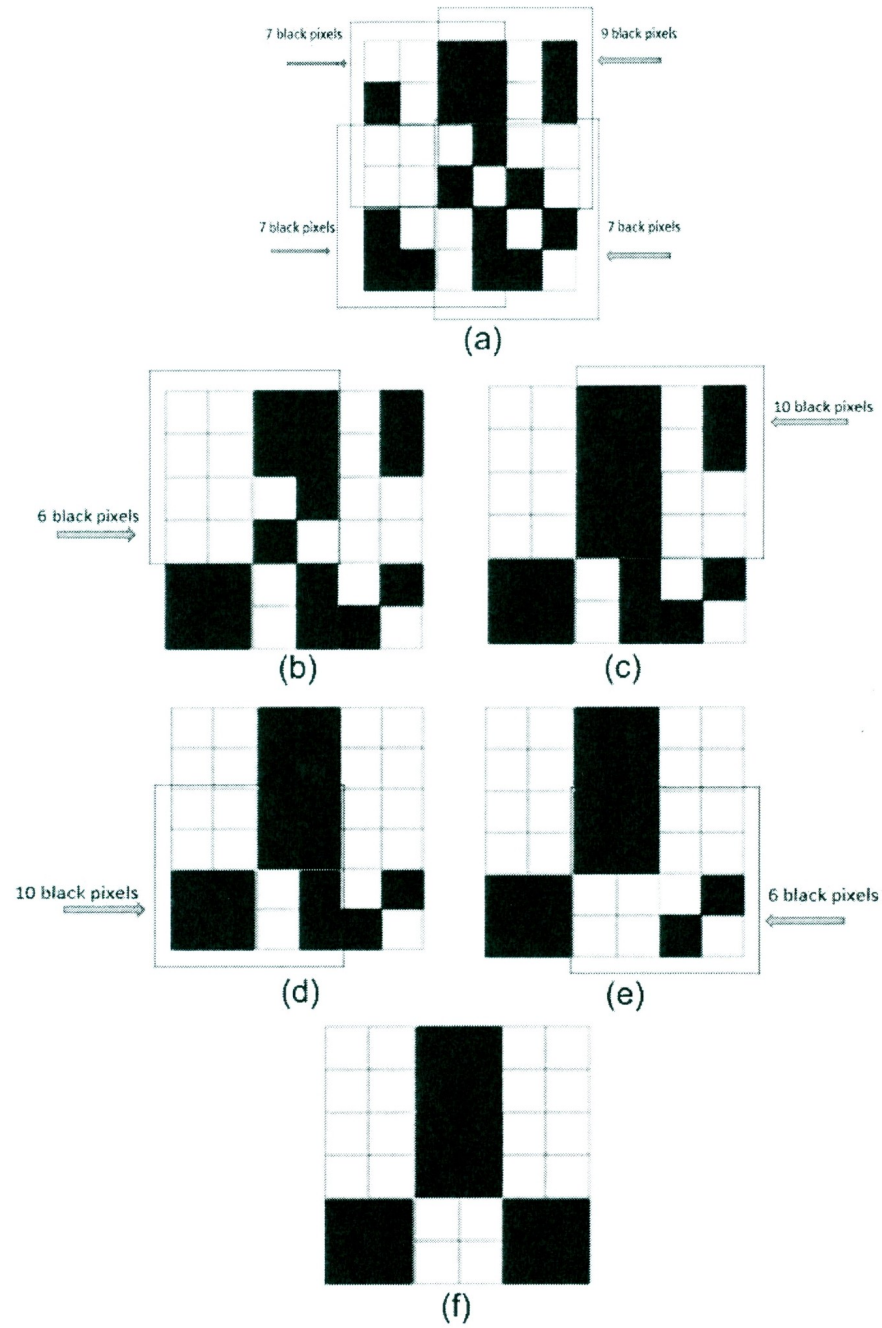


Figure 4.5: Example of the block replacement process in CVT method

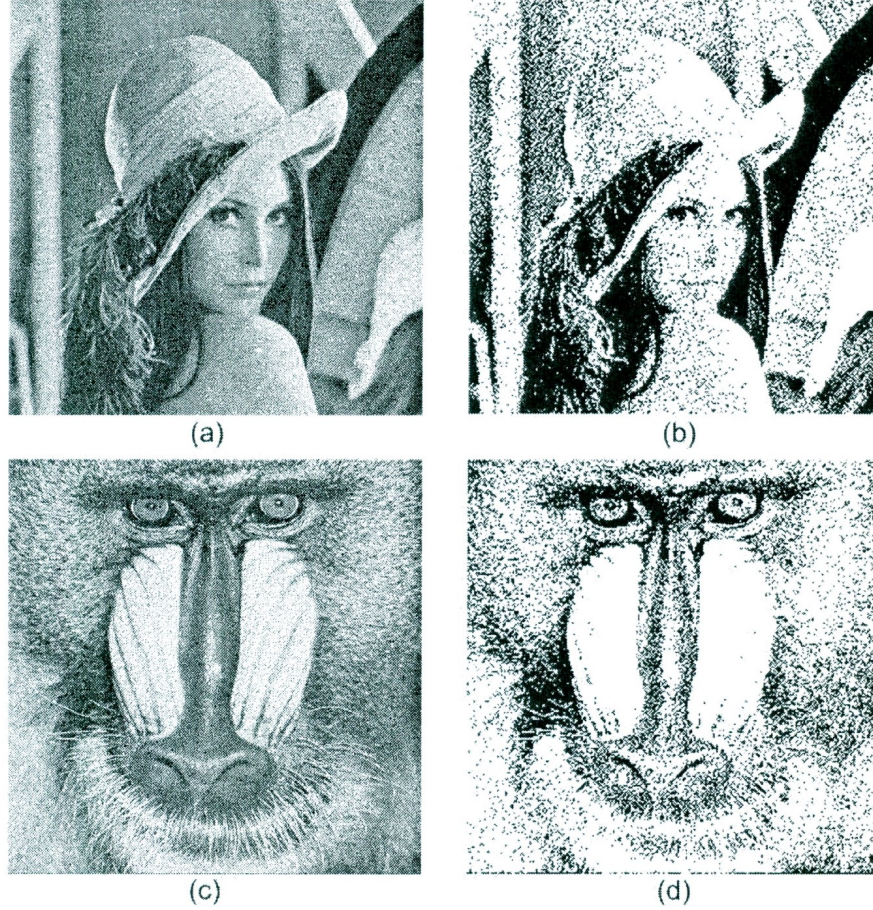


Figure 4.6: Block replacement process in CVT method: (a) halftoned Lena; (b) processed Lena; (c) halftoned baboon; (d) processed baboon

4.5 Conclusion

In this chapter, we utilized the main idea behind Chou's method to solve the problem of contrast loss for gray scale images when the shares and recovered images have the same size as the original secret images. Furthermore, we have demonstrated the following improvements of the visual effect of the processed halftoned images on

VCS: 1) random conversion method, 2) CCT method and 3) the CVT method. In the random conversion method, the idea is to improve the visual quality of the halftoned images by providing uniformity in both light and dark tones. For this, candidate blocks are randomly converted to either black or white blocks. This block replacement method is easy to implement and does not require significant computations. However, due to the random conversion, there is a probability that the resulting image is not as homogeneous as we expect. Unlike the random conversion method, which treats each candidate block individually, in the CCT method, the conversion of candidate blocks are determined based on a constant threshold generated for its cluster of blocks. The aim of this method is to provide a balance between the distribution of black and white blocks in the halftoned secret image. Instead of using a fixed threshold in the CCT method, variable thresholds in the CVT method are defined according to the distribution of black and white pixels in an original halftoned image. Based on visual experimental results with the CVT and CCT method, its final processed images present better visual quality and more details are preserved in comparison with the Chou's method and the random conversion method.

In Chapter 5, we use these pre processing algorithms as a first step in multiple-image VCS and extended VCS without image size expansion.

Chapter 5

Multiple Image VCS and Extended VCS Without Image Size Expansion

5.1 Introduction

In Chapter 3, we proposed a novel visual cryptography scheme for sharing a single secret image, solving the problem of image size expansion and mitigating contrast degradation of the reconstructed image. However, our proposed scheme is able to hide only one secret image. Therefore this scheme is not suitable for multiple-image visual cryptography schemes. As explained in Chapter 2, in order to conceal two secret images, a multiple image visual cryptography scheme is proposed by Chen and Wu [11]. This scheme uses share rotation for concealing more than one secret image. Utilizing multiple image VCS is likely to be a practical method for concealing two or more biometric characteristics in security and authentication systems. As an example, multiple image VCS may be used in the application of an ID card with

biometric samples in an authentication system. Increasing a user's biometric samples or using different types of biometric samples in a template can lead to increasing the accuracy and security in an authentication system. Moreover, it makes biometric systems spoofing more difficult. Authentication systems in large companies may have thousands of users and it is therefore desirable to minimize the cost and capacity of storing biometric templates in a database. However, the previously proposed multiple image visual cryptography schemes suffer from the image expansion problem and a loss in contrast which makes these schemes less effective for authentication systems.

As we discussed, both our novel VCS and multi-image VCS generate meaningless and noise-like shares to hide secret images. In Chapter 2, we showed that this problem was solved by the extended visual cryptography scheme (EVCS), which adds a meaningful cover image in each share. Using EVCS in the application of an ID card has potential for broad application. Assume the scenario of the application for an entrance security system in a company using a biometric sample. For authentication, the user will be provided with a share in the form of ID card. Utilizing EVCS in the system, provides the user with an ID card which is meaningful and contains an image or information which is not related to the secret biometric sample. However, like most visual cryptography schemes, image expansion is a problem in EVCS too. In Chapter 4, we proposed three novel algorithms that solve the problem of pixel expansion and loss of visual quality of grayscale images to use in any visual cryptography scheme. In this chapter, we extend our study in Chapter 4 and apply our block replacement algorithms for use with multiple image VCS and EVCS as a solution for having multiple image VCS and EVCS without image size expansion and with better visual quality of the recovered images.

5.2 Multiple Image Visual Cryptography Without Image Size Expansion

To extend the number of secret images, Chen and Wu proposed a $(2, 2)$ visual secret sharing scheme for two secret images [27]. This scheme encodes two binary secret images into two shares using a share rotation technique. The two secret images are expanded by a factor of 2 in each dimension. To overcome the disadvantage of image expansion and improve the visual quality of the halftoned reconstructed images, in this section we propose a multiple image VCS for grayscale images without image size expansion. As explained in Chapter 2, in Chen and Wu's scheme, shares are generated and encoded based on the assignment of white and black pixels in the two secret images and also based on a chosen rotation angle. In our new scheme, one of the algorithms introduced in Chapter 4 is utilized in Chen and Wu's scheme with the goal of hiding two halftone secret images and recovering the secrets with the same size as the original secret images and with good visual quality.

5.2.1 A New Scheme

Our $(2, 2)$ novel VC scheme takes two halftoned secret images that need to be hidden. Before the images encode into 3 shares, one of the block replacement algorithms introduced in the previous chapter is selected for converting a halftoned secret to the processed secret image. According to the visual results shown in the previous chapter, the processed images obtained after applying a cluster and threshold algorithm have better visual quality compared to the random conversion and Chou's scheme. Figure 5.1 depicts an example of the encoding and decoding steps in the proposed method. Halftoned Lena and halftoned baboon each of size 512×512 are assumed to be the secret images. The outputs of the block replacement process are the processed Lena

and processed baboon which are the two secret images used as input images in the multiple image VCS.

In the next step, each processed secret image is divided into a number of non-overlapping blocks with four pixels. We know that each block is a white or black block as they are already processed, and each secret block in the processed images is ready to be encoded into 2 independent shares and 1 dependant share with the same size as the original secret blocks. Table 5.1 shows how the shares are generated and how the secret images are recovered. Note that Table 5.1 is the same as Table 2.3, except that Table 5.1 starts with blocks for a non-expansion scheme, whereas Table 2.3 starts with pixels and is for multiple-image with image size expansion. The rotation angle is assumed to be 90° counterclockwise in this example.










After encoding all the secret blocks for two images, two share images (share s1 and share s2) are produced with the same size as the original images are produced. The first secret image is recovered by stacking the first and the second share with the OR operation. The second secret image is revealed by rotating the pixel blocks of share 1 counterclockwise 90° (share s3 in Figure 5.1) and superimposing it on share s2, again using the OR operation.

5.2.2 Visual Experimental Results and Discussion

The effectiveness of the proposed method is evaluated by comparison of visual experimental results. To demonstrate that the reconstructed halftone images obtained by utilizing our clustering and thresholding methods have better visual quality, we also utilize Chou's method and the random conversion method to encode the same two halftoned images through the multiple VCS. Halftoned Lena and halftoned baboon both of size 512×512 are taken to be secret images in this experiment.

As is expected, all the reconstructed images obtained in this experiment have the

Table 5.1: Illustration of the (2, 2) multiple image VCS

Block of the processed																
secret 1																
Block of the processed																
secret 2																
s1																
s2																
s3																
s1 stack s2																
s3 stack s2																

same size as the original secret images. Figure 5.2 shows the results of using Chou's block replacement method. The reconstructed secret images are shown in Figures 5.2(e) and (f). Compared with the original halftoned images in Figures 5.2(a) and (b), it is hard to recognize the countour of the Lena and baboon faces as the images are very dark and the results lose important information such as the eyes of the baboon and details of the face of Lena.

Using the random conversion method in a block replacement process resulted in processed Lena and processed baboon as shown in Figure 5.3(c) and (d). Consequently, Figure 5.3(e) and (f) illustrates the two reconstructed halftoned images obtained by applying the multiple scheme on the two processed images. The improvement in the visual quality of the reconstructed images can be observed in the recovered images. As discussed earlier, classifying the candidate blocks randomly into white blocks as well as black blocks in the block replacement process leads to smoother visual quality of the processed images and the reconstructed images. Nevertheless, the reconstructed images still do not appear to be smooth enough, but have a chaotic appearance. Therefore, instead of randomly determining the classifying rules in the block replacement process, we have proposed two algorithms to replace the candidate

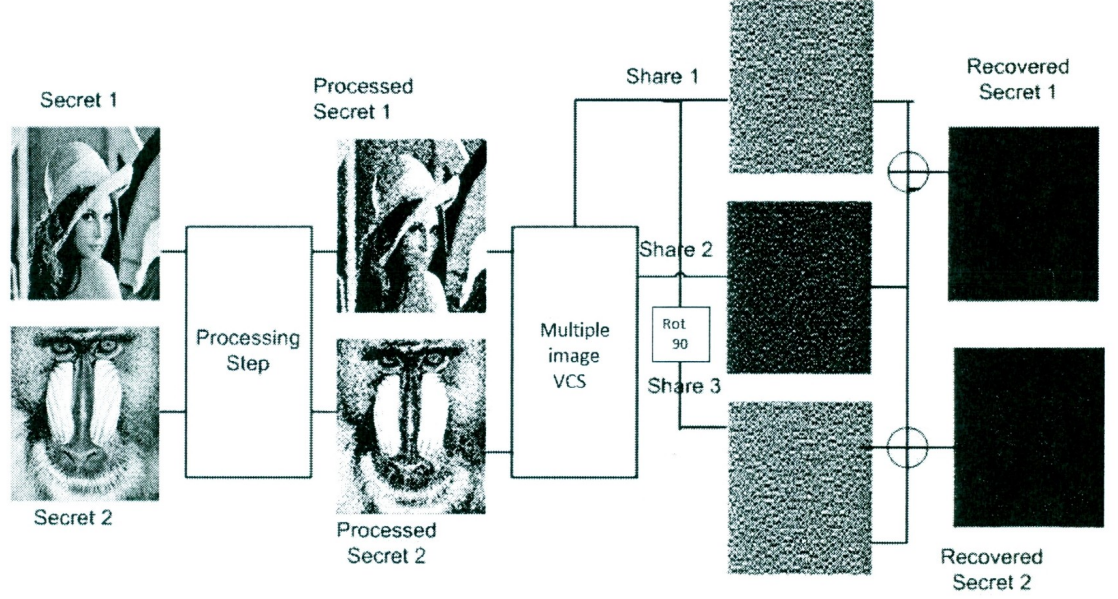


Figure 5.1: Sample encoding/decoding process for multi-image VCS

blocks in an effective way.

The processed images in Figure 5.4(c) and (d) are the results of utilizing the CCT method on the two halftoned images and Figure 5.5(c) and (d) are the processed images obtained by applying the CVT method on the same images. Observing Figure 5.4 and 5.5 we can see that both methods perform better in the visual effect of the processed images and reconstructed secret images. However, results shown in Figure 5.5 show that the reconstructed images that were processed by the CVT method in advance, have more detailed information especially in the baboon's eyes and Lena's face. So the images look clearer than the previous methods. The main reason for that is due to the fact that the clustering and variable threshold algorithm roughly break the arrangements of black and white pixels of the halftone image while preserving the same visual level of gray found in the original gray scale image. Based on our experience, we suggest the use of the CVT algorithm since it balances the requirements of

contrast enhancement and similarity to the original halftoned images. From the above experimental results, we can conclude that the CVT block replacement for multiple-image VCS is effective in improving the visual quality of the reconstructed halftoned secret images. Therefore, our non expansion multiple-image VCS can achieve high quality visual recovery and at the same time possesses information security.

5.3 Extended Visual Cryptography Without Image Size Expansion

As reviewed in Chapter 2, an extension of VCS called extended visual cryptography scheme (EVCS) was introduced by Ateniese in 1996 [12]. Their (k, n) -EVCS, generates n shares for a secret image, in which shares are also meaningful pictures, called cover images. To generate these 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 share information into the n meaningful cover images in such a way that given any $k-1$ or fewer 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. Creating shares with meaningful pictures makes the method more friendly and easier for many applications [37]. However, as was shown before, this scheme suffers from an image size expansion problem. In this section, we introduce a new EVCS which can use grayscale images as the basis for shares without image size expansion.



Figure 5.2: Experimental results of multi-image VCS with Chou's method; (a) halftoned baboon; (b) halftoned Lena; (c) processed baboon; (d) processed Lena; (e) reconstructed baboon; (f) reconstructed Lena



Figure 5.3: Experimental results of multi-image VCS with random conversion block replacement method: (a) half-toned baboon; (b) half-toned Lena; (c) processed baboon; (d) processed Lena; (e) reconstructed baboon; (f) reconstructed Lena

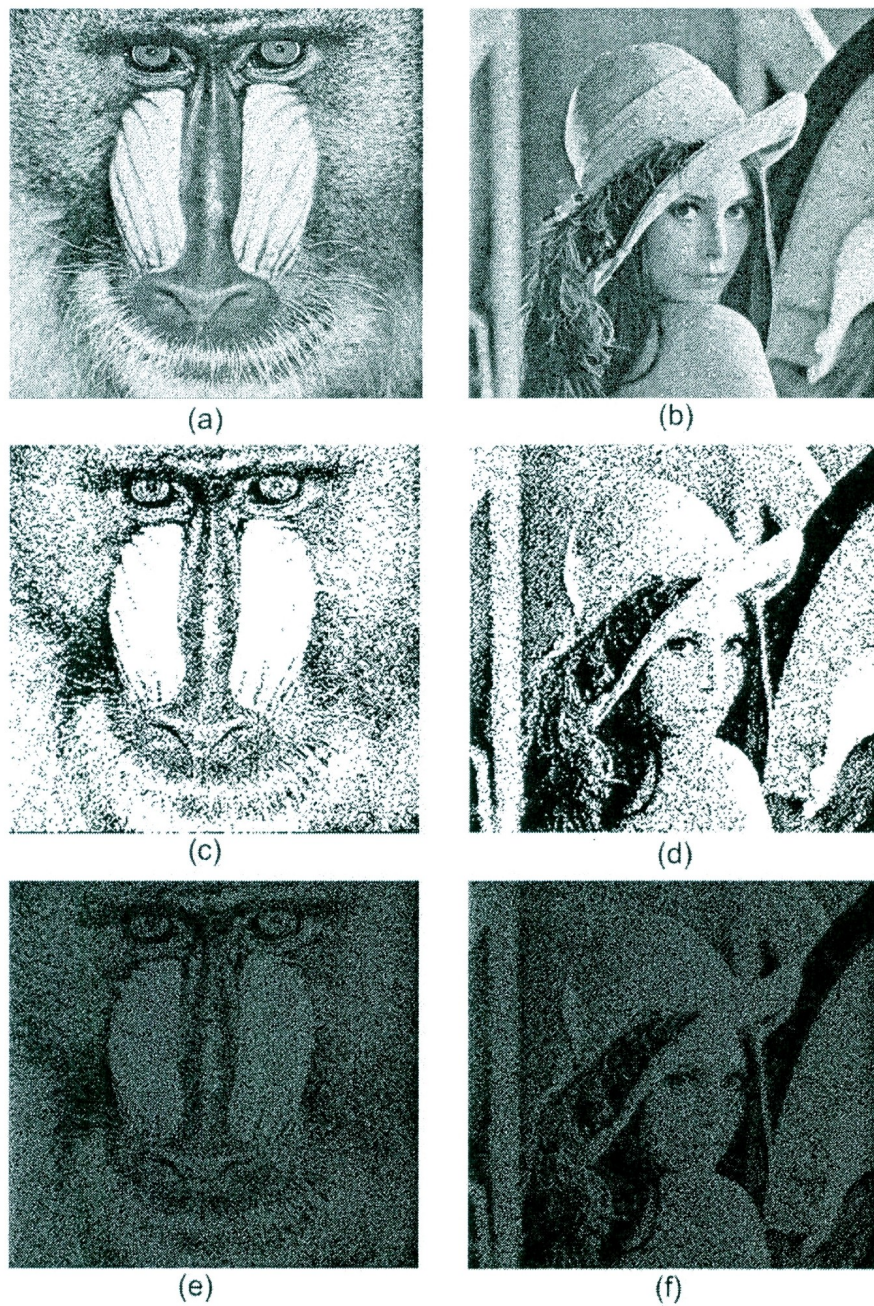


Figure 5.4: Experimental results of multi-image VCS with CCT block replacement method: (a) halftoned baboon; (b) halftoned Lena; (c) processed baboon; (d) processed Lena; (e) reconstructed baboon; (f) reconstructed Lena

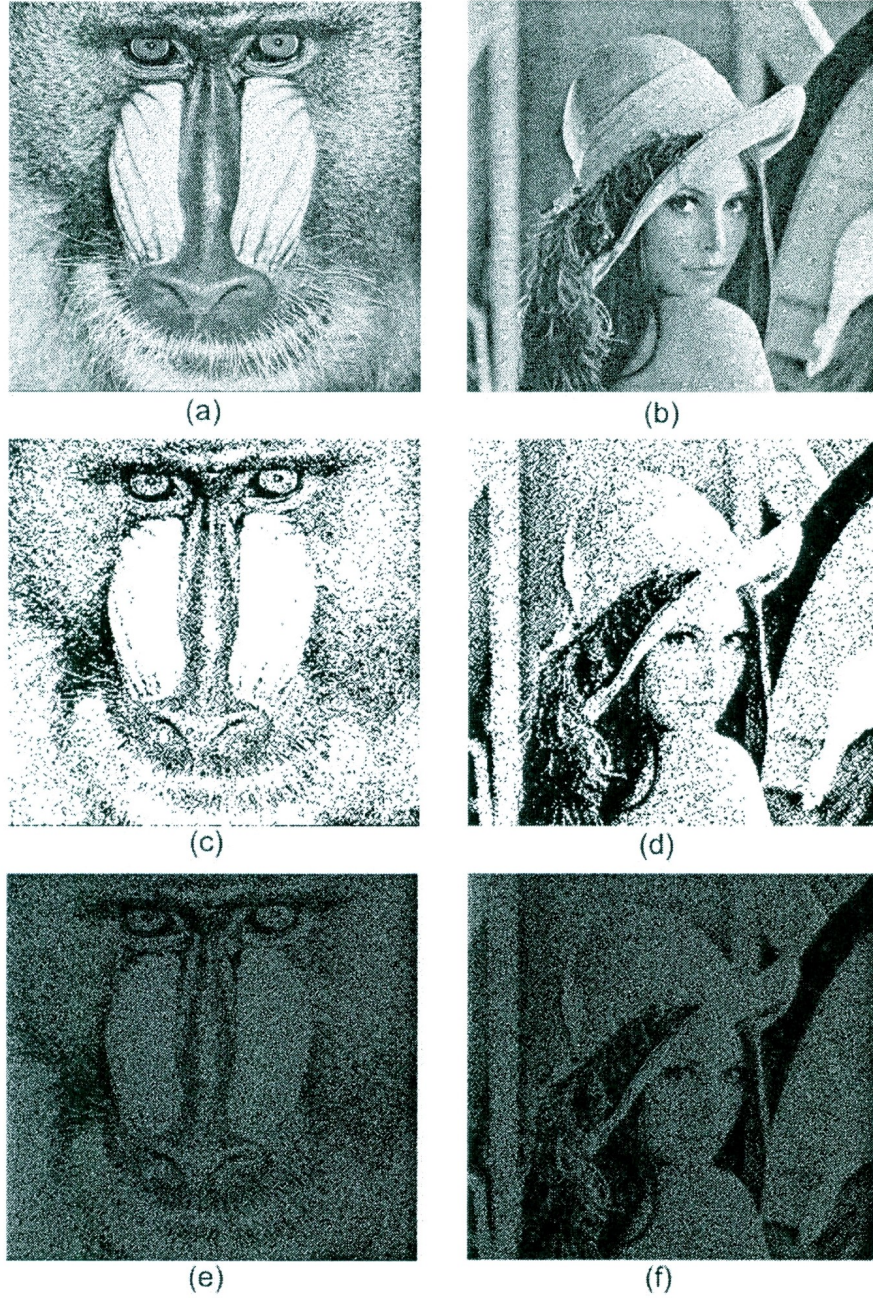


Figure 5.5: Experimental results of multi-image VCS with CVT block replacement method: (a) halftoned baboon; (b) halftoned Lena; (c) processed baboon; (d) processed Lena; (e) reconstructed baboon; (f) reconstructed Lena

5.3.1 A New EVC Scheme

To construct a $(2, 2)$ EVCS without image size expansion, we take three halftoned images of size $2x \times 2y$ as inputs. The first two images are considered as meaningful cover images and the third image is the secret image. One of the block replacement algorithms, ie. one of the random conversion method, CCT method or CVT method is selected to convert the three input images into the processed images. A processed image contains white and black blocks and can be used as an input secret image in any visual cryptography encoding process. After producing the three processed images by the appropriate method, the two cover images are generated according to the EVCS encoding process. The encoding and decoding process for EVCS is described in detail in Chapter 2. The secret image is obtained by stacking two meaningful shares together when all the shares and the secret image have the same size as the original input images. It should be noted that our novel non-expansion EVCS scheme is as secure as the scheme introduced by Ateniese in [12], as the new scheme does not change the encoding process and the share generation of the EVCS.

5.3.2 Visual Experimental Results and Discussion

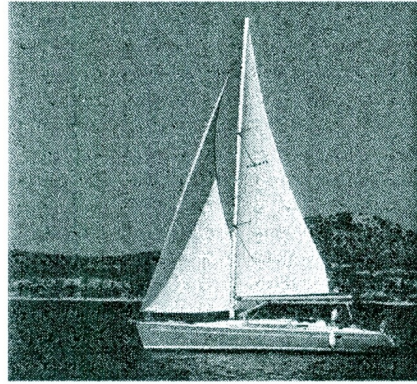
In order to check the validity of the proposed scheme and also evaluate the effects of the three proposed block replacement algorithms on the visual quality of the cover images and the recovered image, we have conducted a visual experiment. As depicted in Figure 5.6, a halftoned boat and the halftoned baboon, both of size 512×512 , are considered as two cover images and halftoned Lena with the same size as the cover images is assumed to be a secret image. Figure 5.7 shows the results of using Chou's block replacement method in EVCS. Results shown in Figure 5.7 (a),(b) and (c) are the processed boat, baboon and Lena, respectively, obtained by applying Chou's block replacement methods on three images. Results illustrated in Figure 5.7 (e) and (f)

are the two meaningful shares and (d) is the recovered secret image obtained after stacking the two shares together. As it was expected, the shares and the recovered secret image have the same size as the original halftoned images; however, compared with the original halftoned images, the shares and the recovered image are much darker and the image visual quality is very poor caused by a severe darkening effect.

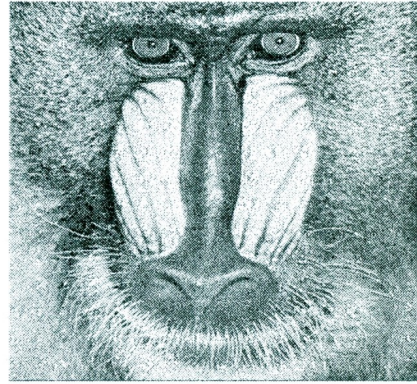
Figure 5.8 demonstrates the effect of utilizing the random conversion method in the EVCS. A significant improvement can be observed in the visual quality of the two shares and reconstructed image. However, the resulting images appear to be covered by a mist which affects on the shares and the reconstructed image details. We further applied CCT method and CVT method on the EVCS. Figures 5.9 and 5.10 illustrate the visual effect of these two approaches. Compared to the random conversion method, applying the CCT and the CVT method on EVCS, result in much clearer shares as well as a visually improved reconstructed secret image. Looking into the details of the images in Figure 5.9 and 5.10, we see that the details are preserved more with utilizing the CVT method on EVCS.

5.4 Conclusion

In this chapter, we used the random conversion method, CCT method and CVT methods developed in Chapter 4 for proposing multiple image VCS and EVCS without image size expansion. Based on the visual experimental results, when using the CVT method, the recovered images in multi-image VCS and also the cover images and the recovered image in EVCS present better visual quality and more details are preserved in comparison with the Chou's method, the CCT method and the random conversion method.



(a)



(b)



(c)

Figure 5.6: Images used for EVCS: (a) halftoned boat; (b) halftoned baboon; (c) halftoned Lena

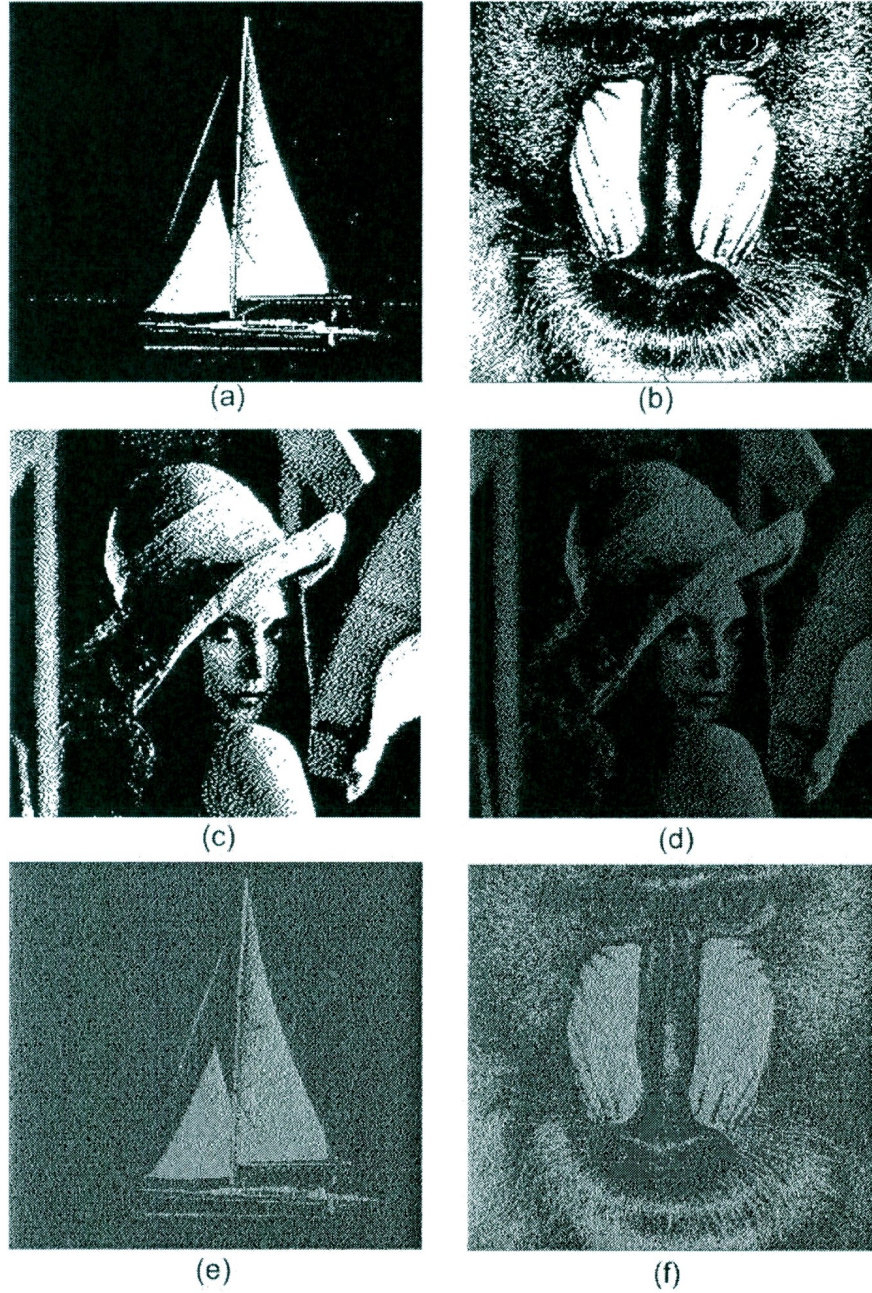


Figure 5.7: Experimental results of EVCS with Chou's method: (a) processed boat; (b) processed baboon; (c) processed Lena; (d) reconstructed Lena; (e) first cover image; (f) second cover image

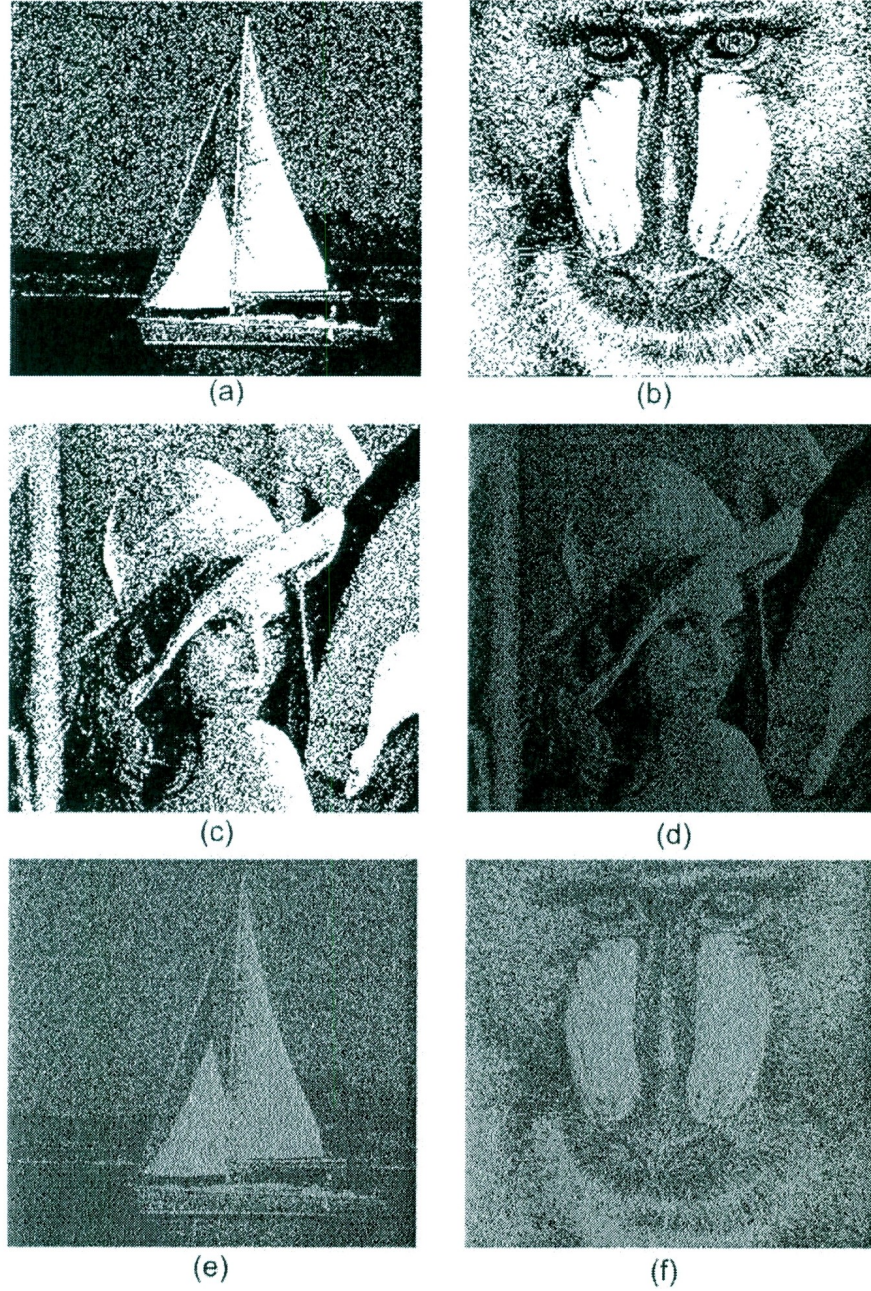


Figure 5.8: Experimental results of EVCS with random conversion block replacement method: (a) processed boat; (b) processed baboon; (c) processed Lena; (d) reconstructed Lena; (e) first cover image; (f) second cover image

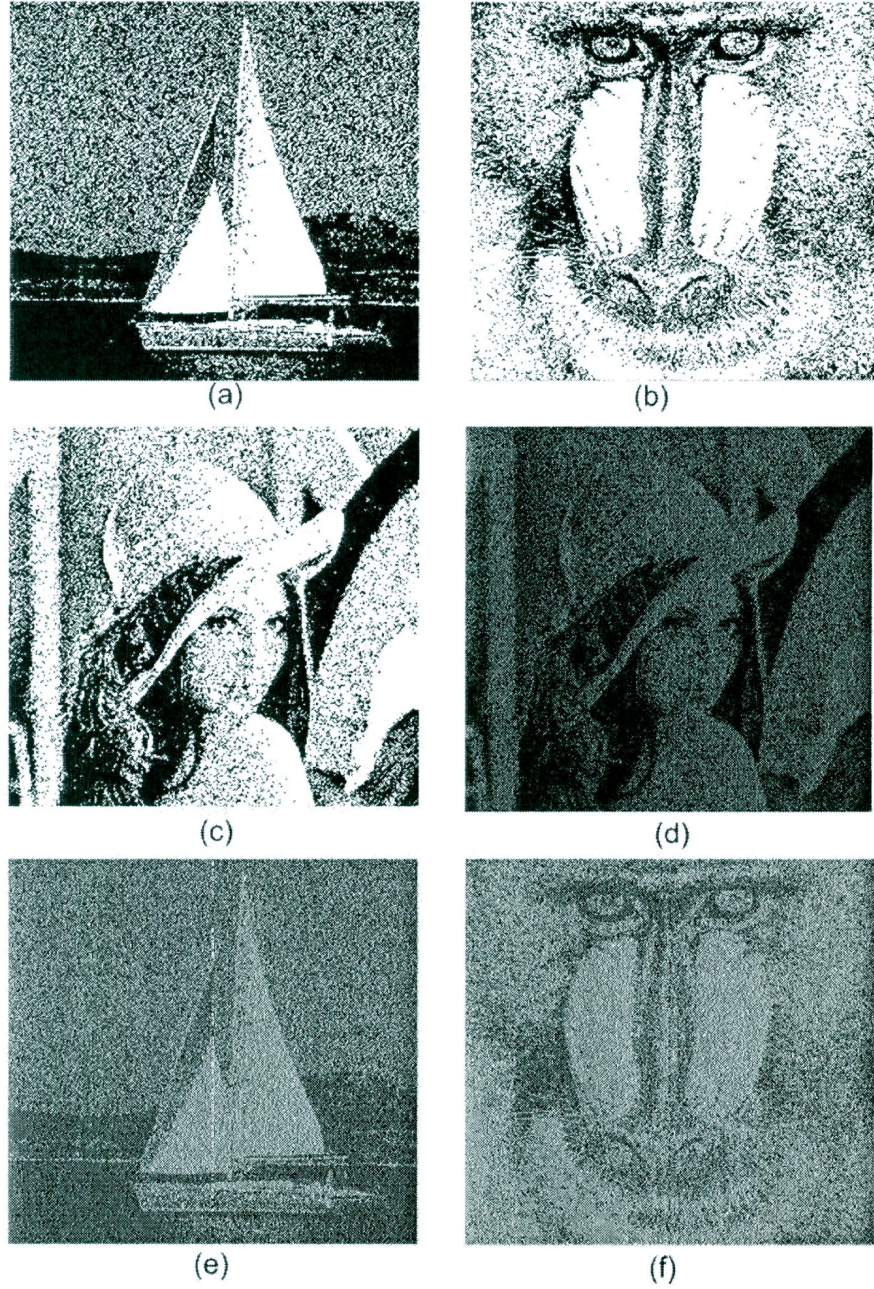


Figure 5.9: Experimental results of EVCS with CCT block replacement method: (a) processed boat; (b) processed baboon; (c) processed Lena; (d) reconstructed Lena; (e) first cover image; (f) second cover image

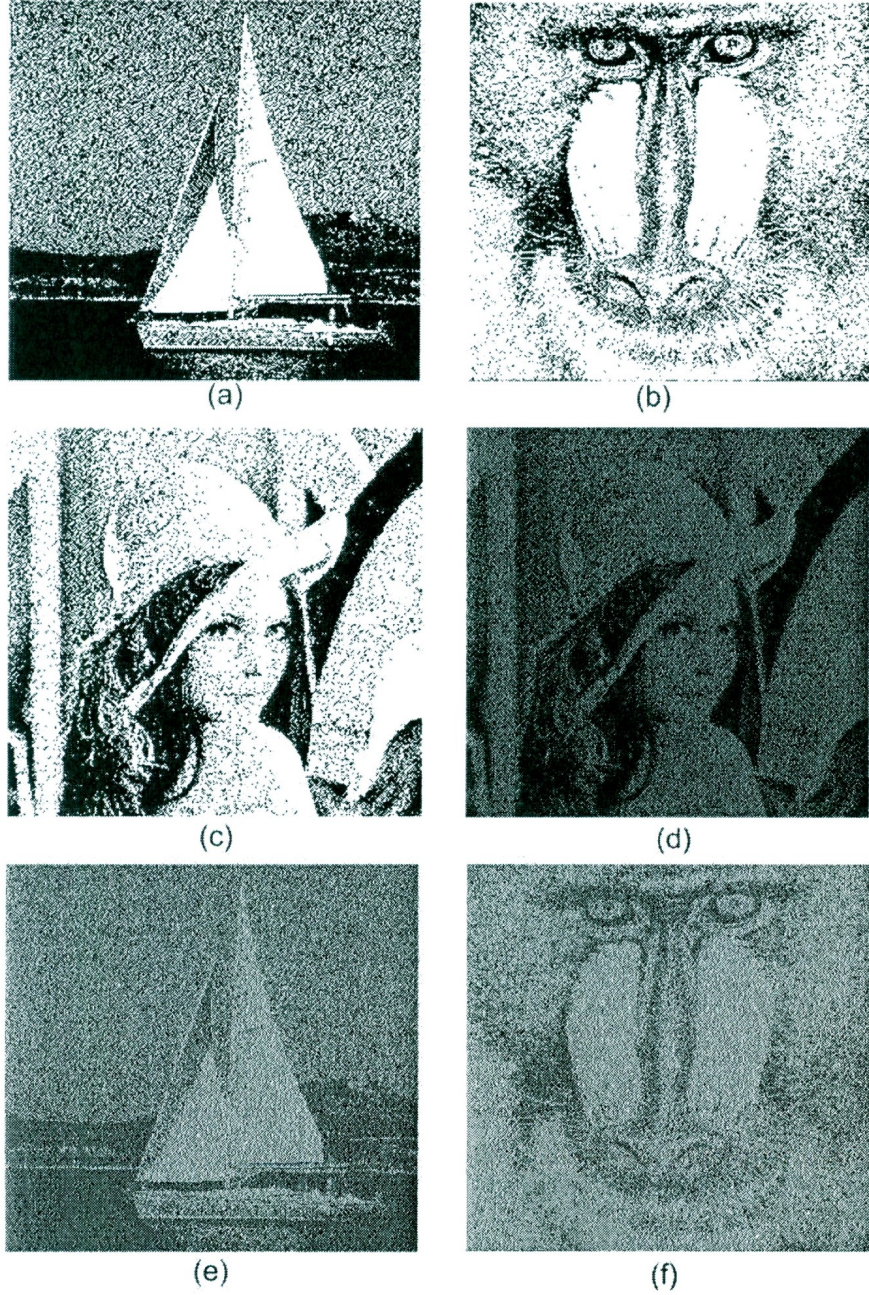


Figure 5.10: Experimental results of EVCS with CVT block replacement method: (a) processed boat; (b) processed baboon; (c) processed Lena; (d) reconstructed Lena; (e) first cover image; (f) second cover image

Chapter 6

Conclusions and Future Work

6.1 Conclusions

In this thesis research, we have focused on important issues in visual cryptography, including image expansion and improvement of visual quality for both binary and halftone images. The problem of pixel expansion and the improvement of contrast for sharing a single secret image were solved by introducing a novel visual cryptography scheme without pixel expansion. In Chapter 3, we used the basic concept of traditional $(2, 2)$ visual cryptography scheme and proposed a new block wise encoding and decoding process. As a result of the proposed scheme, a secret image is divided into two random shares with the same size as the secret image such that superimposing the two shares with the XOR operation reveals the secret image. In both numerical and visual experimental results, we have shown that compared to other non-expansion visual cryptography schemes, the reconstructed images obtained by our novel scheme present better visual quality. The results also showed that the proposed method is the best solution to the problems of security, pixel expansion and the loss of contrast for both halftoned grayscale images and binary images. In one example we showed

that 50% of the recovered pixels obtained by the traditional VCS are in error, when this number is 1% after applying our novel scheme on the same sample image.

In Chapter 4, we extended our study to introduce new block replacement methods that result in non-expansion VCS with improved visual quality on the reconstructed secret images. Experimental results in Chapter 3 showed that, although using Chou's method is a good solution for sharing secret images in VCS, the visual quality of the reconstructed images is very poor and difficult to interpret when incorporating with grayscale images. Therefore, three block replacement algorithms were proposed to deal with the problem of contrast loss in halftone grayscale images. The random conversion method, the CCT method and the CVT method are used to control the effect of contrast reduction. These methods are inspired by principles behind halftoning techniques such as the void and cluster dithering technique. The main focus of these methods is to produce a visually pleasing processed (and therefore potentially reconstructed) images by distributing the black and white pixels homogeneously and similar to the original halftoned image.

In Chapter 5, the block replacement methods developed in Chapter 4 are applied on two well-known VCS named multiple image VCS and EVCS. According to the experimental results and in comparison to Chou's method, we showed that all the introduced methods have better effect on contrast enhancement and visual quality of the reconstructed images. However, the quality of random conversion method is less than the CCT and CVT methods, as the distribution of white and black pixels is done randomly and does not follow a systematic approach. In our experience, we suggest the use of the CVT method because it balances the requirements of visual quality enhancement and similarity to the original image. Visual experimental results obtained after utilizing the CVT method on multiple image VCS and extended VCS demonstrate the effectiveness of this method on the visual quality on the reconstructed

images.

6.2 Future Work

In this thesis, new methods have been presented for overcoming the problems of image size expansion and poor visual quality of the reconstructed images, in the $(2, 2)$ traditional VCS, $(2, 2)$ multiple image VCS and $(2, 2)$ extended VCS. For future work our novel $(2, 2)$ -VCS can be extended and applied on general (k, n) visual cryptography schemes.

In Chapter 5, we focused on either increasing the number of secret images or creating meaningful shares for one secret image, with no image size expansion and good contrast and visual quality. This work can be extended to new methods that increase the number of secrets and create meaningful shares at the same time, with the recovered images and meaningful shares of the same size as the original secrets, and all with good visual quality.

Finally, the schemes developed in this thesis can be applied to a range of biometric applications for security of personal data in a 21st century context.

Bibliography

- [1] D. Luciano and G. Prichett, “Cryptology: From caesar ciphers to public-key cryptosystems”, *The College Mathematics Journal*, vol. 18, no. 1, pp. 2-17, Jan 1987.
- [2] G. R. Blakley, “Safeguarding cryptographic keys”, *Proceeding of AFIPS 1979 National Computer Conference*, vol. 48, New York, pp. 313-317, June 1979.
- [3] A. Shamir, “How to share a secret”, *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, Nov. 1979.
- [4] M. Naor and A. Shamir, “Visual cryptography”, in *Eurocrypt 94 Proceeding*, LNCS, Springer-Verlag, vol. 950, pp. 1-12, 1995.
- [5] G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, “Visual cryptography for general access structures”, *Inf. Computat*, vol. 129, pp. 86-106, 1996.
- [6] M. Naor and B. Pinkas, “Visual authentication and identification”, *Proc. CRYPTO97*, Springer-Verlag LNCS, vol. 1294, pp. 322-336, 1997.
- [7] A.K. Jain and A. Ross, “Biometrics: a tool for information security”, *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, Jun. 2006.

- [8] Y. Rao, Y. Sukonkina, C. Bhagwati and U. Singh, "Fingerprint based authentication application using visual cryptography methods (Improved ID Card)", *Proc.IEEE Region 10 Conf*, pp.1-5, Nov 2008.
- [9] A. Ross and A. A. Othman, "Visual Cryptography for Biometric privacy", *IEEE Transaction on Information Forensics and Security*, vol. 6, no. 1, 2011.
- [10] M. Naor and A. Shamir, "Visual cryptography:Improving the contrast via the cover base", *IACR Eprint archive*, 1996.
- [11] L.-H. Chen and C.-C. Wu," A study on visual cryptography", *Master Thesis*, National Chiao Tung University, Taiwan, ROC, 1998.
- [12] G. Ateniese, C. Blundo, A. De Santis and D.R. Stinson, "Extended schemes for visual cryptography", *Theoretical Computer Science*, 1996.
- [13] Wu. Xiaoyu , W. S. Duncan and Qing Li, "Extended visual cryptography scheme for color images with no pixel expansion", *IEEE Trans. Image Process*, 2010.
- [14] C. Blundo, A. De Santis and M. Naor, "Visual cryptography for grey level image", *Information Processing Letters*, vol. 75, pp. 255-259, 2000.
- [15] Y.C. Hou, "Visual cryptography for color images", *Pattern Recognition*, vol. 36, pp. 1619-1622, 2003.
- [16] F. Liu1, C.K. Wu and X.J. Lin , "Colour visual cryptography schemes", *IET Information Security*, vol. 2, no. 4, pp 151-165, 2008.
- [17] R. Ito, H. Kuwakado and H. Tanaka, "Image size invariant visual cryptography", *IEICE Trans.fundamentals*, vol. E82-A, no. 10, pp. 2172-2177, 1999.
- [18] C.N. Yang, "New visual secret sharing schemes using probabilistic method", *Pattern Recognition*, pp. 481-494, 2004.

- [19] C.L. Wang, C.T. Wang and M.L. Chiang, “The image multiple sharing schemes without pixel expansion”, *International Conference on Machine Learning and Cybernetics*, Guilin, 2011.
- [20] C.L. Chou, “A watermarking technique based on non-expansible visual cryptography”, *Thesis*, Department of Information Management, National University, Taiwan, 2002
- [21] T. Monoth and B.A. P “Tamperproof transmission of fingerprints using visual cryptography schemes”, *Procedia Computer Science*, vol. 2, pp. 143-148, 2010.
- [22] N. Askari, C. Moloney and H.M. Heys, “Application of visual cryptography to biometric authentication”, *Newfoundland Electrical and Computer Engineering Conference*, 2011.
- [23] Z. Zhou and G. R. Arce and G. Di Crescenzo, “Halftone visual cryptography”, *IEEE Trans. Image Process*, vol. 15, pp. 2441-2453, 2006.
- [24] J.B. Feng, G.C. Wu, C.S. Tsai, Y.F. Chang and Y.P. Chu, “Visual secret sharing for multiple secrets”, *Pattern Recognition*, vol. 41, pp. 3572 - 3581, 2008.
- [25] H. C. Wu and C. C. Chang, “Sharing visual multi-secrets using circle shares”, *Computer Standards and Interfaces*, vol.28, pp. 123-135, 2005.
- [26] M. Nakajima and Y. Yamaguchi, “Extended visual cryptography for natural images”, *J.WSCG*, vol. 10, no. 2, pp. 303-310, 2002.
- [27] Y.F. Chen et al, “A multiple-level visual secret-sharing scheme without image size expansion”, *Information Sciences*, vol. 177, no. 21, pp. 4696-4710, 2007.
- [28] R. A. Ulichney, *Digital Halftoning*, Cambridge, MIT Press, 1987.

- [29] B.E. Bayer, “An optimum method for two level rendition of continuous tone pictures”, *IEEE ICE*, pp. (26-11)-(26-15), 1973.
- [30] R. W. Floyd and L. Steinberg, “An adaptive algorithm for spatial gray scale”, in *Proceedings of the Society for Information Display*, vol.17, no. 2, pp.75-77, 1976.
- [31] R. A Ulichney, “Review of halftoning techniques”, in *Proceedings of SPIE*, vol. 3963, pp. 378-391, 1999.
- [32] N. Askari, C. Moloney and H.M. Heys, “A novel visual secret sharing scheme without image size expansion”, *IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, Montreal, 2012.
- [33] C. Blundo and A. De Santis and D.R. Stinson, “On the contrast in visual cryptography schemes”, *Journal of cryptography*, vol. 12, 1996.
- [34] D. L. Lau and R. Ulichney and G.R. Arce, “Fundamental characteristics of halftone textures: Blue-Noise and Green-Noise, *HP Laboratories Cambridge*, 2003.
- [35] T. Mitsa and K. J. Parker, “Digital halftoning technique using a blue noise mask” *Journal of the Optical Society of America*, vol. 9, pp. 1920-1929, 1992.
- [36] R. A. Ulichney, “The void-and-cluster method for dither array generation”, in *Proceedings SPIE*, vol. 1913, pp. 332-343, 1993.
- [37] F. Liu and Ch. Wu, “Embedded extended visual cryptography schemes”, *IEEE Transaction on information forensics and security*, vol. 6, no. 2, 2011.