

Content Based Authentication of Visual Cryptography

Guangyu Wang

A thesis submitted to

Auckland University of Technology

in partial fulfillment of the requirements for the degree

of


Master of Computer and Information Sciences (MCIS)

2014

School of Computer and Information Sciences

Attestation of Authorship

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgements), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning.

Signature: 

Date: 11 September 2014

Acknowledgements

This research was completed as part of Master of Computer and Information Sciences course at the School of Computer and Mathematical Sciences in Faculty of Design and Creative Technologies of the Auckland University of Technology (AUT) in New Zealand. I would like to express my deepest thank to my family for their support throughout my entire academic life. The entire school of the AUT has also provided great assistance in my study.

As a supervisor, Dr Wei Qi Yan had helped me in the best way that a student could expect from a tutor. His patient guidance and insightful advices always drove me get onto the right path. I would also like to thank our school administrator for their support and guidance throughout the Master of Computer and Information Sciences. Finally I am very grateful to my MCIS peers for their great help in figuring out and resolving programming issues and providing me valuable suggestions.

Auckland, New Zealand

September 2014

Abstract

Visual Cryptography (VC) is perceived and studied as a perfect combination of secret sharing and digital image processing. The basic idea of VC is to split original secret image into several partitions which are also called shares. VC schemes include basic VC, grayscale VC, colour VC and multi-secret VC etc. Despite the security nature of VC in secret sharing, one of the common problems of current application of VC shares is that it lacks authentication. Previous related researches have proven the possibility of VC cheating through different methods. Attackers are able to complete both cheating and modification on VC process without being noticed by VC participants. Currently available authentication schemes for VC are derived from the view of utilizing additional shares and blind authentication.

This research analyses effective authentication methods using 2D barcodes and embedding binary codes into VC shares for authentication purpose. A scheme of embedding 2D barcodes into VC shares to prevent cheating will be presented to enhance the use of VC in implementation. The embedding process includes four steps: resolution adaption, image matching and replacement, barcode selection and secret recovery. The aim of this research is to propose a method of embedding 2D barcode into VC shares, thereby strengthening the cheat prevention ability of VC shares by applying the security feature of 2D barcode into VC. As an international standard of reading guidance for the blind people, Braille has been widely used as an effective communication channel. In this thesis, we will also explain Braille encoding and explain how it is applied to handle the authentication problem in VC. Similar to the use of 2D barcode in VC, the utilization of Braille in VC is also attributed to the similarity of structure and construction between Braille cells and VC shares

Even though the research of visual cryptography is based on the combination of image processing and cryptography, knowledge of VC authentication related to digital image processing and cryptography has not been fully utilized in the past years. In this thesis, the analysis of both visual features and cryptographic features of VC will be presented and utilized to assist VC authentication. The visual features of VC in this thesis include moments, histogram, centroid, entropy and Tamura Texture. Compared to those existing methods, the contribution of this research is to propose an authentication

scheme of integrate those features with Hash code and digital signature so as to be embedded into VC shares.

Keywords

Visual cryptography, secret sharing, authentication, digital image processing, cryptography, 2D barcode, Braille

TABLE OF CONTENTS

Attestation of Authorship	I
Acknowledgements	II
Abstract	III
Chapter 1 Introduction	1
1.1 Background and Motivation	1
1.2 Objectives of This Thesis	3
1.3 Structure of This Thesis	5
Chapter 2 Literature Review	7
2.1 Introduction	7
2.2 Basic Knowledge of Visual Cryptography	8
2.2.1 Traditional Visual Cryptography	8
2.2.2 Extended Visual Cryptography	11
2.2.3 Dynamic Visual Cryptography	12
2.2.4 Color Visual Cryptography	12
2.2.5 Progressive Visual Cryptography	13
2.2.6 Applications of Visual Cryptography	14
2.3 Authentication Problem in Visual Cryptography	15
2.4 Barcode and Braille	16
2.4.1 Introduction of Barcode	16
2.4.2 Introduction of Braille	18
2.5 Feature Analysis of Visual Cryptography	19
2.5.1 Visual Features of Visual Cryptography	19
2.5.2 Cryptographic Features of Visual Cryptography	23

2.6	Conclusion.....	28
Chapter 3	Research Methodology	29
3.1	Introduction	29
3.2	Related Study	29
3.3	Research Questions and Hypothesis.....	30
3.4	Data Gathering and Experiment Environment	31
3.5	Solutions for Visual Cryptography Authentication Using 2D Barcode	31
3.6	Braille for Visual Cryptography	34
3.7	Analysis of Visual Cryptography Features	36
Chapter 4	Research Experiments and Findings	39
4.1	Introduction	39
4.2	2D Barcode for Visual Cryptography.....	39
4.2.1	Resolution Adaption	39
4.2.2	Image Matching and Replacement	41
4.2.3	Barcode Selection	44
4.2.4	Secret Recovery	46
4.2.5	Dataset Description.....	47
4.2.6	Experiments	50
4.3	Braille for Visual Cryptography	53
4.3.1	Experiment for Embedding Braille.....	53
4.3.2	Results.....	54
4.4	Features Analysis	57
4.4.1	Experiment for Feature Analysis in Visual Cryptography	57
4.4.2	Results and Analysis.....	58
Chapter 5	Discussions.....	64
5.1	Introduction.....	64
5.2	2D Barcode for Visual Cryptography	64
5.3	Braille for Visual Cryptography	65

5.4 Visual Cryptography Features Analysis.....	66
5.5 Implications and Justifications.....	67
Chapter 6 Conclusion and Future Work.....	69
References	71
Appendix. Standard Testbed for VC Experiments.....	80
A. Logo.....	80
B. Traffic Signs	81
C. Visual Charts	82
D. Maps	83

List of Figures

Figure 2.1 Illustration of pixel expansion in VC.....	9
Figure 2.2 Traditional VC	10
Figure 2.3 Examples of various barcode types (each of these barcode has the same content).....	17
Figure 2.4 Histograms of VC shares (a) Histogram of one VC share (b) Histogram of the modified VC share	20
Figure 3.1 Flowchart of embedding 2D barcode into VC.....	33
Figure 3.2 Examples of Braille	34
Figure 3.3 Flowchart of embedding Braille into VC shares	35
Figure 3.4 The proposed process of producing VC share.....	36
Figure 3.5 The proposed process of VC authentication.....	37
Figure 4.1 The comparison of embedding the same barcode in different resolution.....	40
Figure 4.2 Secret revealing results with different barcodes.....	45
Figure 4.3 Samples of dataset for testing VC share embedded with 2D barcode.....	49
Figure 4.4 Examples of VC shares embedded with barcodes.....	52
Figure 4.5 Regions of VC share are replaced by Braille, the red rectangles are used to indicate Braille cells.....	53
Figure 4.6 Images presented by Braille.	54
Figure 4.7 Pictures in the test set of embedding Braille into VC shares.....	56
Figure 4.8 Data Matrix of Hash code.....	61
Figure 4.9 VC experimental results	62

List of Tables

Table 4.1 The similarity comparison of three types of 2D barcode.....	45
Table 4. 2 Similarities between original and new secret image.....	50
Table 4.3 The accuracy of recovered secret image	56
Table 4.4 Tamura texture value of a VC share	59
Table 4.5 The comparisons between genuine share and modified shares.....	60
Table 4.6 Similarity between original secret and the recovered secret.....	63

Chapter 1 Introduction

1.1 Background and Motivation

The initial awareness of Visual Cryptography (VC) was raised by Naor and Shamir in 1994 (Naor & Shamir, 1995). As a powerful technique for information security, VC indicates the possibility of visually protecting crucial secrets from the view of secret sharing (Weir & Yan, 2010; Shamir, 1979; Yang & Lai, 1999). Unlike commonly used security methods which tend to hide information by applying mathematical transformation on secret in the format of plain text, Visual Cryptography Scheme (VCS) is defined as an activity that a secret is stored in an image (usually black and white). In VC, secret image is split into several images called VC shares. Different from traditional secret sharing where each of participants has the knowledge of part of the secret, every piece of VC shares has no indication of the original secret image while viewers are solely able to clearly perceive the secret by simply overlaying these shares. Therefore VC is a preferable security scheme for the protection of confidential documents such as bank vault password, personal account access password and electrical commodity components.

Among the various kinds of VC, there are five significant VC schemes which are commonly investigated and discussed (Weir & Yan, 2012). Traditional visual cryptography (Weir & Yan, 2010) is the basic VC scheme which utilizes only black and white pixels to encrypt binary images while the VC shares are the pictures without obviously visible and semantic information. The process of extended visual cryptography is similar to that of traditional visual cryptography. The only difference is that VC shares in extended visual cryptography are pictures with meaningful cover information but have no clues of secret. Dynamic visual cryptography indicates the VCS where VC shares can be applied to reveal more than one secret. Colour visual cryptography is used to encrypt colour secret image. Meanwhile progressive visual cryptography copes with the situation where the secret is gradually revealed.

Despite the encryption process of VC can be various according to the specific requirements of different types of VC, the basic idea of VC encryption is conducted on the basis of pixel expansion. Pixel expansion indicates that one pixel on the original secret image is represented by a number of sub-pixels in its corresponding region on VC

shares (Weir & Yan, 2010). One pixel is represented by a randomly selected group of sub-pixels. Thus same pixels in the original secret image are possibly split into sub-pixels in different arrangement, which subsequently lead to the randomness of the appearance of the whole share. Moreover, the colour of a specific pixel on VC shares is determined by the predefined expansion rules of VCS.

As for the decryption process, there are two kinds of VC revealing operations, namely, XOR and OR. The revealing result of using XOR is better than that of OR which is however commonly used as the simplicity of its implementation. In OR operation, VCS result is perceived by Human Visual System (HVS) (Naor & Shamir, 1995; Tuyls, Hollmann, Van Lint & Tolhuizen, 2005). On superimposed VC secret image, light regions are represented by groups of white and black sub-pixels while dark regions are filled up with only black sub-pixels. The contrast of the light regions and dark regions is easily identified by HVS (Memon & Wong, 1998). Therefore VC requires high contrast and low pixel-expansion in secret revealing.

There are two roles in VC activities: 1) A participant who is the holder of VC shares; 2) A dealer who is responsible for the distribution of VC shares and secret recording. In a (k, n) -VCS, a secret image is separated into n shares and the secret can be revealed by superimposing at least k shares. Nevertheless, the secret revealing is failed if the number of authorized VC shares is fewer than k .

The main advantages of VC show in three categories. The first respect is that VC secret is revealed by using only VC shares which are convenient to carry with, unlike other cryptography methods which require complicated computations and powerful computers for the decryption process. Different from typical cryptographic methods which tackle a string of characters or files, VC concentrates on using images as the media for transmission of secret information. Compared to encrypt plain text, images appear to be more flexible in conveying secret content and have larger information storage. Besides, VC is a one-time padding cryptographic technique which makes it unconditionally secure. Moreover, VC is a technique based on secret sharing, which means that the whole procedure of VC is able to be maintained and supervised by all participants and dealers. In summary, with all these outstanding benefits in information hiding and great potential in the development of both theory and application, VC has become one of the most promising security methods in secret sharing.

Even though the advantages of VC are very appealing and inspired to relevant security applications, previous researches have reported the existence of authentication problem of VC (Weir & Yan, 2012). As the whole process of VC is conducted based on VC shares, the security and protection of genuine VC shares are required to make sure the successful revealing of secret. However, based on the analysis of encryption and decryption mechanism of VC, cheating attempts are proven to be effective in VC authentication from both malevolent participants and intruders of VC operations. According to past relevant studies, participants in VC lack of the ability to identify the authenticity of all shares and the secret, hence giving cheaters the opportunity to create unauthorized shares which can simulate the behaviours of valid shares so as to obtain the hidden secret. Thus cheating prevention approaches are needed in association with VC to prevent these cheating practices. Various cheating methods have been created and each of the methods is capable of implementing a cheating scheme.

In VC, both participants and intruders have the opportunities to cheat in some circumstances. Particularly, collusive participants have such chances to cheat by providing fake overlaying results of their shares to other participants or victims. The fake VC shares from intruders can be generated by encrypting fake secret image into shares with different scales and pixel arrangement methods (Hu & Tzeng, 2007). Due to the security weaknesses of existing VC shares, relevant solutions of VC authentication have been raised such as transforming one VCS to another which matches cheating prevention requirements, Chen et al also proposed a cheat preventing method that deals with the cheating immune problem (Chen, Tsai & Horng, 2012). More previous work for VC authentication is introduced in Chapter 2.

1.2 Objectives of This Thesis

Possible effective VC attacks include cheating, cutting and pasting as well as modifications. Other factors may influence the result of VC authentication due to image quality degradation and compression, etc. Cheating prevention of VC has been raised on the basis of the security of its encryption. In VC, cheaters are able to create fake shares so as to coax the genuine one for obtaining the secret. Cutting and pasting as well as modifying are the ways to disrupt the decryption process of VC, which affect VC participants to get a right secret. Therefore it is needed to check the authenticity of VC shares before secret revealing. This research is conducted based on using applicable

methods for VC shares authentication and set up the analysis of VC from the view of features.

Specifically, applicable methods for VC authentication in this thesis include embedding 2D barcode and Braille. Previous researches have investigated on the suitability of embedding 2D barcode into VC shares for authentication. To be specific, there are four main benefits of using 2D barcodes in authentication (Weir & Yan, 2012). Firstly, different from using another share for authentication, 2D barcodes can be embedded into shares, thereby simplifying the authentication process. In addition, cheaters can hardly get the information of the barcode from the prediction of secret. Moreover, as the barcode is able to represent long characters within a small size of pattern, it can be used as a tool to transport secret. Further, using barcode has the advantage of encoding a large scale of authentication information into a controllable set of shares. Lastly, as many applications on mobile devices and personal computers have been developed for scanning barcode, it is convenient for users to decode the barcode by using the built-in cameras on the users' cell phones or laptops.

Barcodes are very resilient to errors and changes in an acceptable extent. The threshold of visual angle for barcode scanning is increasing with the rise of the camera's resolution. This helps to strengthen the robustness of barcode utilization when using the cameras and software applications in cell phones. Especially in the case of embedding 2D barcodes into VC shares which require high security and recognition ability, information verification needs to be fast and accurate in the process of authentication. As the resolution of 2D barcode is adapted to that of the shares, the scanning process is also impacted by the shares. Using VC shares embedded with 2D barcode facilitates the process for dealer to check the correctness of the 2D barcode content. The 2D barcode related part in this thesis mainly concentrates on improving the 2D barcode embedding process to be more practical for VC authentication.

The research of Braille for VC authentication in this thesis is due to the similarity between the dots arrangement of VC shares and that of Braille, which will be explained in Chapter 2.

Extracting features of images is always a significant analysis for image processing, especially in the use of image matching. Therefore by extracting unique features of genuine VC shares, it is possible to gain their identical features for further authentication and verification. From the motivation of making use of VC shares' image

features to help VC dealers distinguish genuine shares from forged ones, it is critical to statistically analyse these shares. As the investigation of VC from the visual and cryptographic aspects in authentication process of VC has not been comprehensively started, this research will focus on the combination of using these two types of features. Specifically, visual features include histogram, entropy, moments and so on while cryptographic features involve Hash code, checksum and digital signature. Both of visual and cryptographic features are able to represent the characteristics of certain images. Different images have different appearances with regard to these features and even slight change on an image will lead to obvious difference on its features. Cryptographic features are employed to encrypt the visual features and these features are stored as a vector for authentication.

1.3 Structure of This Thesis

The whole thesis is divided into three parts. All these three parts are organised based on the process of problem identification and orientation, solution selection and justification as well as experiment and result analysis. The first part is to introduce previous researches related to VC and to analyse current issues of VC. The second part is to describe the research methodology with research hypothesis and experiment design. The last part is the explanation of the experiment conduction and result analysis.

Chapter 2 introduces the definition of VC, various types of VC which are currently researched and VC authentication problem as well as available previously researched methods for handling VC authentication problem. This chapter also introduces those computable, visual and cryptographic features that are suitable for analysing VC shares, how these features could be applied to VC authentication and discussion of the advantages of combining these two kinds of features together for solving the VC authentication problem.

Chapter 3 states the research methodology of the thesis including the main hypothesis and difficulty identification in the process of experiment as well as the explanation of the feasibility of proposed data collection, experiment design and implementation. The main hypothesis is raised based on research questions which are closely related to VC authentication problems.

Chapter 4 describes the experiment results and outcomes. This chapter explicitly describes the experiment environment and relevant algorithms for implementing the experiments are presented based on relevant pseudo code.

Chapter 5 presents the analysis and discussion of the results. Moreover, restrictions of this thesis and expectations for further investigations will also be described.

Chapter 2 Literature Review

2.1 Introduction

The topic of VC has been discussed for a long time before Naor and Shamir formally defined and put forward it. Since then researches of VC have flourished to become a subject with various research directions. There are many types of VC and each of these schemes has its own emphasis on application in practice. The operation of dividing VC image into shares has been focused on the areas of being applied to different types of secret forms (black and white image, grayscale image and colour image) and different methods of pixel expansion. However, on one side, related applications of VC have not been fully developed and popularized. On the other side, VC lacks of the process of authentication.

It is unexpected for a security instrument to be affected by other security problems. Practical security tools ought to comprehensively evaluate every aspect of their applications which may generate opportunities for being assaulted. Security leaks are causing a large amount of cost every year. Similarly, the consequence of successful attacks on VC is highly likely to lead to significantly disasters once VC is widely applied to the industry of information hiding. As obtaining VC shares is the most direct way to access the final secret revealing in VC, it is inevitable that the issue of VC share authentication is closely related to the whole process of VC activities in security. Previous studies of cheating immune VC are productive and typical cases of cheating have been taken into consideration. On the basis of past results and assistance from technologies such as 2D barcode, Braille, digital image processing and cryptography, this thesis mainly focuses on making improvement in enhancing the authentication ability of VC.

In this Chapter, basic knowledge of VC will firstly be introduced to address previous achievements in the research of this subject. These achievements are explained according to classifications of VC. Then the next section explains the authentication problem of VC including previous relevant investigation and remaining issues. Two types of ciphers (2D barcode and Braille) and the adaption of using them in handling VC authentication problem is presented in the following sections. The last part of this chapter is the description of commonly used visual and cryptographic features in digital image processing and media security.

2.2 Basic Knowledge of Visual Cryptography

The basic type of VC is traditional VC which is processed based on only black and white pixels. Using the encryption rules of basic VC, extended versions of VCS were developed in context of certain circumstances. The extended VC was conducted due to the request of enhancing the visual quality of VC shares. Dynamic VC was proposed to meet the demand of improving the capacity of secret information within unique number and scale of VC shares. Colour VC and grayscale VC aim at expanding the diversity of available kinds of pixels to improve its visual effect. As VC is a subset of secret sharing, its encryption and decryption are constructed on the basis of the access structure (Weir & Yan, 2012).

2.2.1 Traditional Visual Cryptography

Traditional VC is processed according to Naor and Shamir's initial assumption for VC. In traditional VC techniques, secret encryption and decryption are achieved by image sharing which is the scheme that can be similar to general secret sharing. Typically, in (k, n) -VCS, the image that carries the secret is separated into n VC shares and the decryption process cannot be successful unless at least k pieces are collected and superimposed (De Bonis & De Santis, 2004). Specifically, the use of these efficient basic schemes would provide a secure form of 2D barcodes which are used as a secret transport mechanism (Weir & Yan, 2012; Hou, 2003). We use pixel value of '1' and '0' representing black pixels and white pixels respectively. The construction of the shares can be indicated by $(2, 2)$ -VCS. Illustration of constructing the pixels of two basis matrix (C_0 and C_1) is indicated below (one pixel from the original image is expanded into four pixels.) (Weir & Yan, 2012):

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

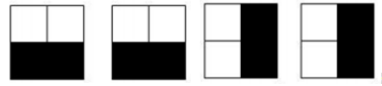
$$C_1 = \{ \text{all the matrices obtained by permuting the columns of } \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \}$$

In basic VC scheme, shares can be generated by the rules of XOR that pick the pattern of four sub-pixels with the same arrangement for both shares if a pixel of secret image is white; if a pixel of the original image is black, pick a complementary pair of patterns. Figure 2.1 illustrates the examples of composition of white pixel and black

pixel in Traditional VC. Figure 2.2 gives an example of VC secret image and its VC shares.



(a) Black pixel



(b) White pixel

Figure 2.1 Illustration of pixel expansion in VC

While the fact that there are solely black and white pixels in traditional VC makes this kind of VCS easily to be implemented, the superimposed result of secret restoration is hard to be secured. This is due to the reason that its decryption operation is based on OR operation which appears to have the problem of contrast loss. HVS is able to differentiate the dark and white region if their contrast is higher than a certain level (Naor & Shamir, 1995). It is proved that using only black pixels to present black pixel in secret appears to have better contrast (Blundo, De Bonis & De Santis, 2001). In VC, the contrast is evaluated by using Hamming weight $w(v)$: existing h_x : for $\alpha > 0$, in the set C_0 , $w(v) < h_x - \alpha m$; while in the set of C_1 , $w(v) > h_x$, where h_x and $h_x - \alpha m$ represent the darkness level and whiteness level respectively; m is the pixel expansion level; α denotes the relative difference in VCS.

In order to improve the contrast of OR operation in VC, previous researches have demonstrated four kinds of solutions. Specifically, the first contrast enhancing method is processed based on analysing the structure of basis matrix (Jiang, Liu & Feng, 2013; Blundo, D'Arco, De Santis & Stinson, 2003; Blundo, De Santis & Stinson, 1999). The second effect way is to use mathematical equations to analyse the disciplines of contrast (Cimato, De Prisco & De Santis, 2005; Hofmeister, Krause & Simon, 2000; Krause & Simon, 2003; Kuhlman & Simon, 2000). Unlike the two methods mentioned above, the third method is to use searching algorithm to search for the scheme which is able to generate the largest contrast (Lee, Na, Sohn, Park, Seo & Kim, 2002; Tuyls, Hollmann, Lint & Tolhuizen, 2002). In spite of the contrast of dark region and white region of recovered secret based on OR in VC can be improved by the three ways mentioned

above, there are still noise (unexpected black pixels) existing. Therefore the fourth effective way of improving contrast is to use VC restoration devices designed with other decryption model such as XOR and cover base which is achieved by distributing more than one VC shares to each participant (Koga, 2002).

In the situation when the original secret image is a grayscale picture, it is possible to replace a pixel on original image to a block of pixels with unique number of black and white dots according to its grayscale, such as halftone and error diffusion techniques. The transformed grayscale image is actually a binary image with only black and white colours, which allow it to be treated as a normal input secret image in traditional VC. The examples of using groups of black and white pixels to represent grayscale pixels are shown in Figure 2.2.

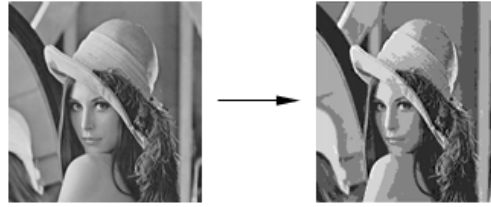


Figure 2.2 Traditional VC

As the pixel expansion in traditional VC is closely related to the similarity between the restored secret and the original secret, it is preferable to decrease the pixel expansion as much as possible to constrain the distortion. On the basis of reducing sub-pixels, past researches have proposed effective scheme for size invariant Visual Cryptography. One preferable size invariant VC uses traditional VC with the pixel expansion equals 1 (Kuwakado & Tanaka, 1999). Similar to traditional VC, this size invariant VCS adopts the access structure to store the information of VC shares and uses OR operation as the basic secret recovery method. A typical example of the basis matrix of a (2,3)-size invariant VCS where the contrast is $\frac{1}{3}$, it can be illustrated as below.

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

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

In the size invariant VC, white pixels on original secret is generated by superimposing two white pixels while the black pixels is obtained by overlaying one black and one white pixel. Further, other researches have also proposed optimised size invariant VCS which effectively reduces the pixel expansion scale (Yang, 2004; Yang & Chen, 2005; Ching-Nung & Tse-Shih, 2005; Yang & Chen, 2006).

2.2.2 Extended Visual Cryptography

Extended VC scheme which allows the construction of visual secret sharing schemes within which the image content of the shares is meaningful (Yang, 2004). In the extended VC, even though the VC shares are meaningful pictures which contain contrast and pattern, the original image and shares are still binary pictures or grayscale pictures which can be transformed into black and white pictures. There are two ways of implementing the extended VC. The first method is to define an access structure of basis matrix which is then used to generate dither matrix to reproduce the input image which are prepared to be embedded into VC shares. The second way of generating embedded VC shares is achieved by calibrating the halftoned input image. The collections $C_c^{c_1 c_2}$, where $c, c_1, c_2 \in \{b, w\}$, of a 2 out of 2 threshold VC scheme (2,2-VCS) are gained by using the following matrices (Ateniese, Blundo, Santis & Stinson, 2001).

$$S_w^{ww} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \quad \text{and} \quad S_b^{ww} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

$$S_w^{wb} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \quad \text{and} \quad S_b^{wb} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

$$S_w^{bw} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \quad \text{and} \quad S_b^{bw} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

$$S_w^{bb} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \quad \text{and} \quad S_b^{bb} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

The evaluation criteria of Extended VC can be defined as $p = t-m/t$, where p represents the percentage of information of original secret which is preserved in the the extended VC shares. The contrast of extended VC is also able to be assessed by using Hamming weight, which is similar to traditional VC. Related researches also conducted investigations of improving the contrast of Extended VC shares so as to enhance the visual quality of their input images. Figure 2.3 gives an example of the extended VC.

2.2.3 Dynamic Visual Cryptography

Dynamic VC aims at using digital image processing techniques to hide more than one secrets by applying one set of access structure. Dynamic VC is developed to meet the requirement of multiple-secret sharing which was firstly pointed out. In a classic (2, 2)-multiple-secret VCS, the first secret can be revealed after superimposing the required two shares S_1 and S_2 . When keeping the position of S_1 unmoved while rotating S_2 into a certain angle, another secret will turn up (Wu & Chen, 1998). As a significant improvement, further researches have changed the appearance of shares from rectangles to circles, which not only tends to add additional information such as some supplementary points, lines or markers, but also extends the flexibility of the rotating angle from 90° , 180° and 270° to any degrees between 0° and 360° (Wu & Chang, 2005; Shyu, Huang, Lee, Wang & Chen, 2007).

Along with the improvement of increasing secret information capacity, multiple-secret visual cryptography was found having disadvantages. The first aspect is the pixel expansion that in traditional VC, each pixel on original secret only needs to be expanded in a small scale whereas in multiple-secret VC, the pixel needs to be expanded n times of that in the traditional VC, n denotes to the number of secrets hidden in VC. The other concern of the multiple-secret VC is the determination of the exact position of two shares for secret revealing. Especially for circular VC shares in the case of not knowing the number of total hidden secrets, it is a problem that slight variance of their position is highly likely to result in the missing of the restoration of unique secrets.

2.2.4 Color Visual Cryptography

As the popularity of colour pictures nowadays, the research of VC has involved the analysis of producing VC shares for colour images. Similar to grayscale images, colour pictures have depth level as well to indicate the intensity of a certain colour. In colour VC scheme, one pixel can be transformed into sub-pixels, each of them can also be subdivided into different colour regions.

There are commonly three ways to achieve Colour Visual Cryptography Scheme (CVCS). In particular, the first method is to directly use the colours appeared in original

secret image (Cimato, De Prisco & De Santis, 2007; Rijmen & Preneel, 1996). This CVCS method can also be classified into two approaches of concealing unused colours on VC shares by black colour and increasing or decreasing the colour depth to imitate different colours. The advantage of this method is that CVCS can be implemented effectively. However, the disadvantage is obvious as well that most of relevant CVCS requires significant pixel expansion and the number of available represented colours is limited. One typical example scheme is to expand every pixel in secret into a group of 2×2 pixels which is filled with red, green, and blue colours. The total 24 combination possibilities are therefore treated as 24 different colours. The expanded pixel blocks are chosen from the 24 combinations which are similar to that of the original pixel in secret. This method effectively reduces the required colours from 24 to 4, however, has the limitation of available colours which can be presented.

The approach of implementing CVCS is to separate color images into three color channels (RGB) firstly and then using halftone-related VCS to encrypt the three images (Liao & Huang, 2013). The advantage of this method is that the pixel expansion is maintained in a satisfied level as the separated image with one color channel can be treated as grayscale pictures and therefore is able to be subdivided by grayscale VCS. However, the disadvantage of grayscale VC, which tends to affect the visual quality of images, is likely to impact this method of CVCS.

The third kind of CVCS was raised by Lukac et al which is conducted on the basis of bit operation. In this CVCS, the original secret image is broken down into its corresponding binary bit-level. Traditional VCS is then employed to make further encryption on these bit-levels. Even though this CVCS is preferable in secret recovery, the operation of this scheme needs assistance from other devices and color extended Visual Cryptography (CEVCS) is hard to be implemented.

2.2.5 Progressive Visual Cryptography

The issue of Progressive Visual Cryptography is raised due to the secret recovery problem. The secret recovery quality depends on how the final image is to build up. Normally the contrast of the final image and how much the noise removed is closely related to the final visual quality of the restored secret. Progressive VC has been developed in grayscale and colour images (Jin, Yan & Kankanhalli, 2005). The basic idea of the progressive VC is that encrypting a colour image into shares and different

qualities of secret can be viewed by stacking different shares. Available techniques of the progressive VC are halftone-based with micro block encoding (Hou, Chang & Tu, 2001). Quality of the recovered secret is increasing in either resolution or the completion of colours by superimposing more shares. Moreover, as for the traditional VCS which requires high recovery quality with less noise, the loss of contrast by using OR operation can be fixed by XOR operation even though the implementation of using devices with computing ability is difficult.

2.2.6 Applications of Visual Cryptography

Creating practical application is always the motivation for researches. The study of VC also expects the security issues can obtain solutions from the aspect of both cryptography and digital image processing. Previous researches have come up with and attempted possibilities of applications of VC. Specifically, VC is preferred in the use of Moiré pattern and watermarking. Moirés patterns are generated when a revealing layer is stacked on to the top of an image with periodically repeated shape. The revealing layer can be of dots or raster. Moiré pattern has been attempted to be embedded into VC shares. Original secret can be revealed by superimposing the shares while when the shares are separated, the embedded image could be viewed. Three different Moiré schemes were proposed in the past researches: lattice rotation, lattice smooth rotation and dot orientation (Hersch & Chosson, 2004; Indebetouw & Czarnek, 1992; Desmedt & Van Le, 2000; Chourasia, 2013).

Another frequently used application for VC is watermarking. Watermarking plays an important role in information hiding and key information embedding. Creating watermarking forms of VC has also been investigated frequently (Memon & Wong, 1998). Similar to normal VC, the implementation of VC in watermarking is based on basis matrix and the final recovered secret is perceived by using contrast between white and black colors. CVCS and halftone-based VC have also been investigated and proved to be robust when applied to watermarking. Embedding VC based watermarking into products is an effective way of preventing cheating, especially for the domains where already get benefits from the use of watermarking.

2.3 Authentication Problem in Visual Cryptography

From the progress of VC investigations, it is obvious that protection of secret image is largely related to the reliability of VC shares. Cheatings in VC are always based on the decryption and analysis of VC shares. Therefore previous work has also made effort in proposing cheat immune VC which aims at preventing cheatings in VC activities.

The role of cheater in VC as well as the authentication and successful cheat in VC are defined by Horng, Chen and Tsai (2006). According to their definition, a cheater is someone who releases a fake share that is different from the one (s)he received from the dealer during the process of secret reconstruction. A secret image is authentic if its appearance with all black and white regions is clearly perceptible. The cheat process in VC is successful when participants who are cheated (called victims) accept the result of secret revealing using fake shares provided by cheaters. Furthermore, Horng, Chen and Tsai (2006) gave an example of cheating process in VC that collusive cheaters are able to transfer transparent VC shares into digital versions and analyse the construction of VC so as to estimate and modify those important parameters. The definition of cheating prevention scheme is defined by Horng, Chen and Tsai (2006) as possibility of successful cheating is negligible and they raised their own cheating prevention scheme by adding confidential logos. These logos are only known to dealer and certain participants. The authentication process fails if the stacked VC shares have no clear appearance of their predefined logos. This method of VC authentication performs effectively in preventing cheating from VC participants.

In 2007, Tsai, Chen & Horng proposed a cheating prevention scheme for binary visual cryptography with homogeneous secret images. A more secure scheme is given to solve the cheating problem without extra workload by adopting multiple distinct secret images. Moreover, for sharing these secret images simultaneously, the share construction method of visual cryptography is redesigned and extended by generic algorithms. Hu and Tzeng (2007) further analyzed VC cheating from two outlooks, namely, cheating from malicious participants (MP) and malicious outsider (MO). MP is a legitimate participant as well as cheater, while MO is an intruder apart from VC participants. Both MP and MO are able to cheat VC secret revealing by producing fake shares.

Chen, Tsai & Horng (2012) reviewed a number of well-known cheating activities and Cheating-prevention Visual Secret-sharing Schemes (CPVSS), and then categorized cheating activities into meaningful cheating, non-meaningful cheating, and meaningful deterministic cheating. Moreover, they analysed the research challenges in CPVSS, and proposed a new cheating prevention scheme which is better than the previous schemes in the aspects of some security requirements.

2.4 Barcode and Braille

2.4.1 Introduction of Barcode

Commonly used ciphers include barcodes and Braille. Therefore it is possible to utilize these two symbols for VC blind authentication. Barcodes can be defined as an optical machine-comprehensible representation of certain data, text or other information which has been attached within the barcodes (Kuo, Wong, Gao & Chang, 2010; Kato & Tan, 2005; Niu, Huang, Wub & Zhang, 2004). There are only black or white pixels existing in barcode, thereby rendering it easily to be detected by scanners but hard to be recognized by human eyes due to its construction structure. Barcode was initially designed to be automatically scanned and decoded only by barcode scanners. Conventionally, its data is stored in one-dimensional barcodes by utilizing parallel lines whose lengths and intervals are varying. With the development of barcode technologies, the adoption of regular two-dimensional patterns, for example, rectangles, dots and hexagons, have also been introduced in the construction of barcodes. Currently, barcode applications have been developed to be used in personal computers. Relevant smartphone applications are also available for barcode scanning. Previous researches have studied applying barcodes into VC. Yang et al proposed a method of setting PDF417 as original secret and divided it into two barcodes in visual secret sharing schemes (Yang, Chen & Ching, 2006).

Barcodes can be classified into two main types, namely linear barcode (stacked barcode, one-dimensional barcode) and 2D barcode (dot matrix barcode). Three examples of 2D barcodes are shown in Figure 2.3.



(a) QR code



(b) Aztec code



(c) Data matrix

Figure 2.3 Examples of various barcode types (each of these barcode has the same content)

Under the context of VC, using 2D barcodes has more advantages than other types of authentication methods. Firstly, 2D barcodes can be applied to VC which handles binary images that colours except for black and white will not be taken into consideration. Secondly, even though the binary characters in 1D barcode can precisely represent certain information by coding based on specific agreements, the use of 1D barcode is restricted as its limited information storage. Therefore 2D barcodes, which have advantages such as large capacity with small size and high security, easy to be carried, is more suitable to be used in VC than 1D barcodes (Gao & Sun, 2012; Yan, Li, Cao, Chen & Xue, 2013). Normally in VC, participants expect the authentication information to be complexity enough to protect the shares from being decrypted by cheaters. At the same time, the size of the authentication container should be as small as the size of the share is always in a controlled scale. Furthermore, the VC shares are all depicted in 2D structure which is similar to that of 2D barcode. Therefore 2D barcodes have the obvious advantage of being used to be embedded into shares for authentication.

According to different encoding principle and structure shapes, 2D barcode (Yan, Li, Cao, Chen & Xue, 2013) can also be subdivided into stacked barcode and dot matrix barcode. Stacked barcode represents information by incorporating height adapted 1D barcode. Typical stacked barcode types include Code 16K and PDF417 (Hahn & Jung, 2006). Stacked barcode is not suitable to be embedded into VC shares as it has some features of 1D barcode. By contrast, dot matrix barcode is only organized by an array of the black and white dots in a regular flat place in order to process the information encoded. Dot matrix barcode is a recently developed coding system which builds up on digital image processing technology. Typical formats of dot matrix 2D barcodes are Aztec Code, Quick Response Code (QR Code), Data Matrix and Maxi Code. Among these various barcodes, Data Matrix and QR Code are widely used and supported by barcode scanner software installed in either personal computers or mobile devices.

A Data Matrix contains three components: the encoded data, four borders, and the quiet zone. Each of these components contains white or black solid squares which are called modules. When being translated into mathematic language, a black module in the barcode can represent '1' and a white module can be '0', or vice versa. To locate the symbols, a Data Matrix Code contains an 'L' shape solid modules to define the orientation, border, and its size. The whole symbol is bordered with white modules marked as the quiet zone. A Data Matrix symbol (Jiang, Liu & Feng, 2013) uses Reed-Solomon Error Correcting Code (ECC) level 200 for error detection and correction which uses Reed Solomon for error checking.

In QR Code, information is stored in both horizontal and vertical dimensions (Rouillard, 2008; Zhang, Ma & Mao, 2011). The basic elements arranged in the barcode are named modules which exist in both horizontal and vertical directions of the barcode and these modules only represent dark or light elements by digits '0' or '1'. QR Code performs better in data capacity, size scale and scanning speed than Aztec Code and Data Matrix. However, as in the context of VC the main purpose of employing 2D barcode is for authentication. The most suitable barcode for a share is highly likely to be the barcode which is the most similar with one specific region in the share to minimize visual effect on secret revealing. Therefore, on the basis of similar usability the barcode types of QR Code, Aztec Code and Data Matrix will all be considered for the authentication tools in VC. In this thesis, we will use QR Code, Data Matrix, and Aztec Code in the authentication for VC shares.

2.4.2 Introduction of Braille

In this thesis, we choose Braille as the cheating prevention tool for authentication in VC. In 1824, a French blind person Louis Blair invented Braille which is designed specifically for the blind person to read by tactile perception (Jiang, Liu & Feng, 2013). In Braille, the alphabet is written in the form of blocks of the six dots which are also called Braille cells (Goldberg & Swan, 2011). Braille cells are small, flat, rectangular objects of a standard size. The surface of each point can either be flat or salient. Each letter of the alphabet is uniquely represented in Braille cells by a pattern formed by certain arrangements of the six dots (Goldberg & Swan, 2011).

While open circles indicate the flat positions in each cell, filled circles indicate salient dots in the cell. The American Library of Congress uses the following Braille print

standard: every dot is 2.5 mm far from its neighbour dot; every cell is 6.0 mm far from its neighbour cell; filled dots are 0.5 mm higher than the surface; the diameter of dot base is 1.5 mm (Goldberg & Swan, 2011).

Blind people read Braille articles by using their fingers padding over Braille cells and perceiving the characters by the dots arrangement in Braille cells. While Braille is very useful for blind people, individuals can hardly understand the content on Braille passages if they have no experience in reading Braille (Goldberg & Swan, 2011). Subsequently Braille appears to be only unrecognizable signs for people who lack the knowledge of Braille. Therefore Braille can be treated as a cipher text.

2.5 Feature Analysis of Visual Cryptography

2.5.1 Visual Features of Visual Cryptography

Except seeking assistance from authentication information stored in ciphers, VC features are also able to help in VC identification. As VC is processing digital images which have visual characteristics, VC secret images and VC shares certainly can be analysed by using techniques from digital image processing. Therefore, we could select visual computable features in digital image processing for VC authentication. Specifically, we determine to use pixel colour sequence, VC share histogram, entropy, moments and centroid, textures (Tamura), coefficients of Discrete Walsh Transform (DWT), etc. Each of these features is related to the VC shares. Even though the information stored in VC images is always massive, the image is able to be perceived by HVS straightforwardly. Moreover, the security of VC shares is also related to the complication of the image computable features. Therefore it is critical to analyse the image from the view of digital image processing for VC authentication.

Digital image processing is used to analyse image features in both spatial and frequency domains. As for the respect of spatial domain, widely discussed features include pixel colour, histogram, entropy, moments and centroid.

Pixel histogram is an effective method for representing the comparison of different pixel distributions in spatial domain using statistical way. The horizontal axis of Figure 2.4 represents the tonal variations, while the vertical axis represents the number of pixels in that particular tone. The left side of the horizontal axis represents the black pixels and the other side represents white areas. The vertical axis represents the percentages of

black and white pixels in the image. Due to the nature of VC schemes, the ratio of black and white pixels in randomly distributed VC shares is approximately 1:1. By recreating VC shares, the ratio is likely to be changed. However, only using histogram for image matching in distinguishing two VC shares is improper since there are only two colors in VC shares. Moreover, the other drawback of histograms for VC analysis is that the representation is dependent on the color of the secret being shared, while ignoring its shape and texture. Figure 2.4 displays the histograms of one VC share (a) and one rebuilt VC share (b). The difference of Y axis in (a) and (b) indicates the ratio of black pixels to white pixels could be changed by adapting the construction of VC schemes.

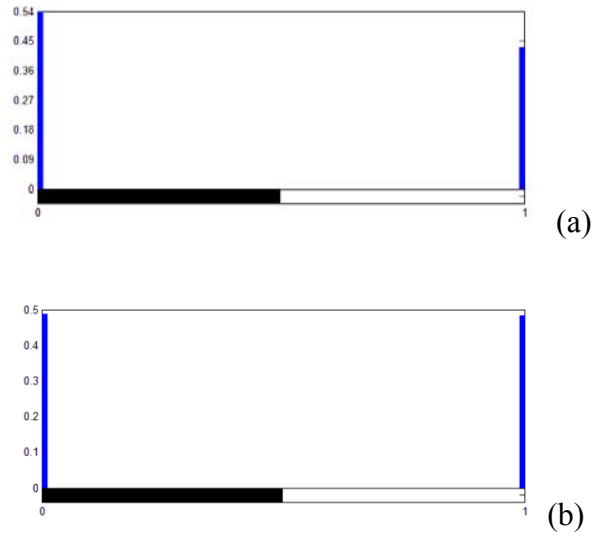


Figure 2.4 Histograms of VC shares (a) Histogram of one VC share (b) Histogram of the modified VC share

Moments are geometric features for describing an object such as region, size location as well as shape (Corke, 2011). The moments in VC authentication can deal with the problem of size invariance and computational complexity. The moment of a share image I is given be:

$$m_{pq} = \sum_{(u,v) \in I} u^p v^q I[u, v] \quad (2.1)$$

where p and q are the order of the moment, (u, v) is the coordinate of a pixel in image I . As for the binary images where only contain black and white pixels, white pixel number can be simply calculated by:

$$m_{pq} = \sum_{(u,v) \in I} I[u, v] \quad (2.2)$$

As with the meaning of geometry, moments are usually defined by using physical interpretations. Similarly, the mass distribution can also be represented by image moments. The total mass of a region is m_{00} and the centroid of the region is,

$$u_c = \frac{m_{10}}{m_{00}}, v_c = \frac{m_{01}}{m_{00}} \quad (2.3)$$

where m_{10} and m_{01} are the first order moments. Therefore, the central moments can be computed as:

$$m_{pq} = \sum_{(u,v) \in I} (u - u_c)^p (v - v_c)^q I[u, v] \quad (2.4)$$

Moment is a size invariant image feature. In the context of VC, the similarity between the given VC share and the genuine VC can be calculated by using moments. Moreover, as the moments are commonly used for pattern recognition, the similarity between the original secret image and its VC share can also be measured. Different from the case of comparing two shares, the similarity between secret and its share is expected to be as low as possible since cheaters are able to extract the features of original secret from shares if the computable feature of a VC share is close to that of the original secret.

Except the features like pixel colour, image histogram and moments, entropy is also a widely utilized measurement for digital image processing. Entropy is a measure of information capacity that can be used to characterize the texture of the input image. Image entropy is a quantity which is used to describe the amount of information which must be coded for by a compression algorithm. Low entropy images have very little contrast and large runs of pixels with the same or similar values. An image that is perfectly flat will have entropy of zero. The expression of entropy is:

$$E = - \sum_{i=1}^n \sum_{j=1}^n P(i, j) \log\{P(i, j)\} \quad (2.5)$$

where $P(i, j)$ represents pixels in VC share, n is the number of pixels.

The texture description of image features can be various based on the actual need in practice. Tamura et al. (Tamura, Mori & Yamawaki, 1978) proposed a global descriptor of six image characteristics. It has been proved that Tamura texture helps significantly in detecting forgery. Therefore we also take advantages of Tamura texture as one of our features in VC authentication. Specifically, Tamura texture is constituted by directionality, contrast, roughness, line-likeness, regularity and coarseness. These

features are corresponding to the psychological point of view on the texture attributes (Liao & Huang, 2013).

Directionality of Tamura texture represents the image alignment in directions with the description of both element shape and position. This feature is calculated by using the sharpness of peaks in image histogram.

$$F_{dir} = \sum_p^{n_p} \sum_{\theta \in w_p} (\theta - \theta_p)^2 H_D(\theta) \quad (2.6)$$

where p represents a peak, w_p represents the peak of the scope, $H_D(\theta)$ represents the histogram constructed by calculating the numbers of all gradient vectors.

Contrast is the feature describing the difference between light region and dark region in an image. In Tamura texture, contrast degree is calculated by a global metrics representing the grayscale histogram with its distribution. Contrast of an image can be calculated by:

$$F_{con} = \frac{\sigma}{\alpha_4^{1/4}} \quad (2.7)$$

where $\alpha_4 = \frac{\mu_4}{\sigma^4}$, μ_4 is the Fourth-order moment of the mean value of gray pixels and σ is the variance.

Computing coarseness of Tamura texture is a method to pick a large size as the best one when a coarse texture is presented, even though micro texture is also presented to pick a small size when only fine texture is presented. The measurement of coarseness in Tamura texture is:

$$F_{crs} = \frac{1}{m \times n} \sum_i^m \sum_j^n S_{best}(i, j) \quad (2.8)$$

where m and n are the effective width and height of the picture respectively.

Line-likeness in Tamura texture is an element of texture that is composed of lines. For this purpose, when the direction and the neighbouring direction for a given edge are nearly equal, we regard such a group of edge points as a line.

$$F_{lin} = \sum_i^n \sum_j^m P_{Dd}(i, j) \cos \left[(i - j) \frac{2\pi}{n} \right] / \sum_i^n \sum_j^m P_{Dd}(i, j) \quad (2.9)$$

$P_{Dd}(i,j)$ is defined as the relative frequency with which two neighbouring cells separated by a distance d along the edge direction occur on the image, one with the direction code i and the other with the direction code j .

Regularity is used to describe repetitive patterns in mathematical form. The equation of computing regularity is defined as:

$$F_{reg} = 1 - r(\sigma_{crs} + \sigma_{con} + \sigma_{dir} + \sigma_{lin}) \quad (2.10)$$

where r is a normalizing factor and each σ_{xxx} means the standard deviation of F_{xxx} .

As the roughness in Tamura texture can be calculated by simply summing the value of coarseness and contrast, we will only apply the five features mentioned above as the features of VC authentication.

In the frequency domain, widely used transforms for digital image proceeding include Discrete Walsh Transform (DWT), Fourier transform and Cosine transform. Walsh transform is a method for binary images which is robust and invertible. Compared to other transforms such as Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform, DWT has two discrete transform results 1 and -1, which is more suitable for the authentication of VC shares. DWT is illustrated as,

$$W_{xy}(u, v) = \frac{1}{N} \frac{1}{N} \sum_{y=0}^{N_y-1} \sum_{x=0}^{N_x-1} f(x, y) \cdot (-1)^\alpha \quad (2.11)$$

The inverse transform is also presented:

$$f(x, y) = \sum_{v=0}^{N_y-1} \sum_{u=0}^{N_x-1} W_{xy}(u, v) \cdot (-1)^\alpha \quad (2.12)$$

where $\alpha = \sum_{r=0}^{P_x-1} x_r u_r + \sum_{s=0}^{P_y-1} y_s v_s$, $f(x, y)$ is the pixel of the image, $f(x, y)$ is the coefficients in frequency domain. The coefficients could be used to identify authentication of VC shares.

2.5.2 Cryptographic Features of Visual Cryptography

Except visual features, cryptographic features of VC shares should be another frequently investigated topic since the invention of VC. Despite the security nature of VC, the previous evaluation of the security of VC mainly focuses on what extent of this

technique is in cheating immune and how to design appropriate VC systems to make this technique more resistant against attacks from cheaters (Weir & Yan, 2010).

There are two widely used authentication methods available for checking shares and secret: 1) Using an additional share to check the authentication of the share images and the revealed secret; 2) Using blind authentication technique to prohibit the prediction of genuine content. A scheme of embedding 2D barcode into VC shares as authentication channel has been proposed recently (Weir & Yan, 2010), this method is effective but has visual artefact on the shares.

Because of the risk that 2D barcode can be decoded and modified by cheaters without being notified by VC share keepers, those methods of one-way encryption (the 2D barcode content cannot be decoded) are needed. Cryptographic Hash function has benefits of easy to calculate the Hash value for any input data, however it is difficult to get data from a given Hash, hard to modify a data without altering the hash and uneasy to find two different data with the same Hash. Besides, Cryptographic Hash Functions are employed in a large range of areas like Message Authentication, Message Integrity and Digital Signatures (Sobti & Geetha, 2012).

A Hash function is the algorithm that maps data of arbitrary length to a specific data with a fixed length (Rompay, 2004). The values returned by a Hash function are called Hash values or Hash codes. The definition of Hash function (Rompay, 2004) can be a function $h: D \rightarrow R$, where the domain $D = \{0,1\}^*$ and $R = \{0,1\}^n$ for some $n \geq 1$. Well-known Hash functions include Message Digest (MD4 and MD5), Secure Hash Algorithm (SHA-1, SHA-2 and SHA-3). MD4 is the Hash code using iteration of a three-round compression function, while MD5 is an updated version of MD4. As effective attacks on MD5 have been raised, SHA appears to be much secure. SHA-3 is an updated version of SHA-2, which uses the sponge construction that separates the input data into several blocks and processes each of these blocks iteratively (Stallings, 2013; Solms & Solms, 2009). The output of processed blocks will be the input for the next iteration. Based on full analysis of these facts, in this thesis we use SHA-3 for encoding visual features.

Our solution for content based authorization problem of VC shares is based on the Hash code in 2D barcode to distinguish the correct share from the unauthorized ones. The advantage of using the Hash code of these features is that modified shares can be

prevented in the authentication process. Thus we decide to use the Hash code of visual features of VC shares in the authentication. All the relevant information of 2D barcode content can also be copied and kept by the dealer who is subsequently able to easily check the correctness of authentication information stored in 2D barcodes of the VC shares by using 2D barcode scanners and decoders.

The proposed scheme of embedding 2D barcode is mainly for the security purpose. Embedding the 2D barcode into the most similar region in VC share can effectively hide the 2D barcode into the environment around it. In the scenario when a VC share holder attempts to cheat others by modifying the content of the share which is embedded with 2D barcode, VC dealers are able to prevent this hoax promptly by verifying the information included in the 2D barcode. Similarly, it appears to be practical for the VC dealer to detect cheatings from attackers other than VC participants. The Confidentiality, Integrity and Availability (CIA) of VC shares thus could be guaranteed. The CIA is a standard content and model of information security which is assigned to measure the security of information. It is, therefore, extremely important to be used to ensure the secure resources. As with the nature of information hiding, the security of VC shares is able to be evaluated by the standard CIA.

Ensuring the confidentiality means that only authorized participants can get access to the protected objects such as hidden private information. Confidentiality prevents the secure items from being reached by unauthorized individuals while ensuring that the real participants are able to acquire it easily.

Ensuring the integrity means that only authorized participants may make changes to the assets. Integrity involves maintaining the consistency, accuracy, and trustworthiness of VC shares through its entire life cycle. VC shares must not be changed in transit, and steps must be taken to ensure that the data cannot be altered by unauthorized people or intruders (for example, in a breach of confidentiality). In addition, integrity also means responsively detecting any changes in the data that might occur as a result of authentication failure. Thus the cheating activities can be noticed and then be prevented before revealing of the VC secrets. In VC, since there are various features that can be encrypted and used in authentication process, the checksum is able to be used to improve the integrity protection (Zhong, 2013). Checksum is a small-size datum computed from an arbitrary block of digital data for the purpose of detecting errors which may have been introduced during its transmission or storage. In practice, a checksum is a count of

the number of bits in a transmission unit so that the receiver can check to see whether the same number of bits arrived. If the counts match, it is assumed that the complete transmission was received. A simple error detection scheme in which each transmitted message is accompanied by a numerical value based on the number of set bits in the message.

Ensuring the availability means that the assets must be available to authorized users when required. By adding authentication process in VC, all the authorized participants should have the chance to read the secret. VC shares can help to distribute the secret meanwhile the embedded 2D barcode can identify the real shares from the unauthorized ones.

Another important security assessment criterion is authorization, auditing and accounting (AAA). In AAA, authorization defines what rights and services the end user is allowed once the permission of access is granted. Authentication and authorization are usually performed together in an AAA managed environment. Authentication provides a way of identifying a user, typically by having the user to enter a valid user name and valid password before access is granted. The process of authentication is based on each user having a unique set of criteria for gaining access. 2D barcode can perform as a key of access to the VC shares, and the authentication of VC shares can thus be ensured since the information stored in 2D barcodes can only be read by certain scanners. The AAA authentication of VC shares can compare a user's authentication credentials with others. The user is granted access to the VC secret revealing process only if the information matches. If the credentials are different, the request of access would be denied and authentication will fail.

Accounting offers the approach for collecting information about the end user's resource consumption, which can then be processed for billing, auditing, and capacity-planning purposes (Solms & Solms, 2009). Accounting measures the resources a user consumes during access. This includes the amount of system time or the amount of data that a user has sent and/or received during a session. As accounting is carried out by logging of session statistics and usage information, it is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities. Auditing functionality permits verifying the correctness of procedures carried out based on accounting data. The information stored in 2D barcodes on VC shares needs to be verified and the process of secret recovery is conducted based on the result of data

matching. In this thesis, we concentrate on the authentication aspect that protecting the security of VC shares from being obtained by cheaters.

Digital signature needs to be issued by a trusted third party to verify the authenticity of a public key. Broadly used algorithms for digital certificate include RSA, Fiat-Shamir, Guillou-Quisquater, Schnorr, Ong-Schnorr-Shamir, DES and so on (Zhong, 2013). Particularly, there are two important keys in the process of authenticating digital signature, namely, the private key and the public key. The private key is created for key distributor to make a digital signature and to decrypt information from other participants. The private key must be kept as private secret, whereas the public key should be distributed to all the participants. The public key is used to reveal a digital signature from key distributor and to response confidential information in a form encrypted by the public key. The private and public keys must not be derived from each other. This key pair is issued by a certification authority that verifies and registers the identity of the signer. As digital signature is a mathematical technique for signifying and validating the legitimacy of a digital document, it has the ability in enhancing the process of authentication. The digital signature has three features in VC. In terms of the respect of authorization, digital signatures can be created with the private key of the sender that only the viewers with public key can read the information. With regard to integrity, VC participant is able to detect that whether the document has been modified if the share is signed. As for the availability, the signer cannot deny that he has sent or signed the VC share that anyone with correct signature has the right to reveal the secret.

Public and private keys are generated by using two random numbers p and q . The modulus for both the public and private keys is $n=p \cdot q$. By using Euclidean function $\Phi(n)$, we can get an integer e and d which comply to the requirements: $1 < e < \Phi(n)$ $e = \gcd(n, \Phi(n))$ and $d \cdot e \equiv 1 \pmod{\Phi(n)}$. The private and public key can be generated from n , e and n , d respectively.

The encryption formula of RSA is,

$$P^e \bmod n = c (k < n) \quad (2.13)$$

The decryption formula is

$$c^d \bmod n = P \quad (2.14)$$

In this thesis, we will combine visual features and cryptographic features and make use of them for VC authentication. To the best of our knowledge, this is the first time that these two kinds of different features are combined together for VC authentication.

2.6 Conclusion

This chapter summarized previous researches of VC and the knowledge that is needed in the proposed scheme in this thesis. Specifically, several critic research areas of VC are introduced including Traditional VC, Extended VC, Dynamic VC, Color VC and Progressive VC. Researches of available applications of VC are described before the explanation of VC authentication problem and cheating immune VC. 2D barcode and Braille are introduced as blind authentication tools for VC. 2D barcodes are binary symbols which contain certain encoded information. The similarities and dissimilarities between 2D barcodes and Braille are analyzed for choosing proper type of barcodes for VC authentication. Braille is a group of six flat or raised dots for blind people's reading by touching these dots. The research of using Braille for VC in this thesis is conducted based on the similarity of Braille and VC shares' structure. The analysis of visual and cryptographic features is expected to provide new knowledge for the research of VC. As the research purpose of this thesis, VC authentication problem is expected to be solved by 2D barcode, Braille and the adoption of visual and cryptographic features.

Chapter 3 Research Methodology

3.1 Introduction

The part of research methodology is built upon major research questions developed from literature review. By addressing the main research object in this thesis, related experiments are designed including data gathering and experiment planning as well as evaluation criteria making.

As mentioned in the previous chapter that one of the main challenges for VC is its weakness of authentication. While attackers are able to cheat based on known information which are detectable on the shares, the assistance from other ciphers, such as 2D barcode and Braille, is expected to be helpful in VC authentication. As different ciphers have dissimilar encoding and decoding rules, embedding other types of ciphers is able to strengthen VC's security. Furthermore, in order to explicitly identify the similarity between a given share and predefined genuine share, visual features and cryptographic features are utilized to realize accurate comparison. To the best of our knowledge, this is the first time visual and cryptographic features of VC have been studied in VC authentication.

In this chapter, the research problem and hypothesis are discussed in detail with relevance to the research gap identified from the background review in Chapter 2. The main aim of this chapter is to identify the research problem and to set up reasonable experiment design based on the research problems.

3.2 Related Study

Previous researches have studied various methods for cheating immune VC (Weir & Yan, 2012). Even though VC is studied as a powerful instrument for information hiding, investigators are attempting to experiment with various types of attack schemes. Simultaneously, effective solutions for protecting VC from being cheated are also under research to deal with attacks.

The suitability of embedding 2D barcode into VC shares for authentication has been studied and proven to be operative. The selection of VC scheme will be processed to choose XOR or OR operation after preparing the secret. Subsequently, two shares will be generated for embedding barcode. The secret image is then decrypted by overlapping

the shares. By embedding the 2D barcode into the secret image, the superimposed image can also be used for authentication by verifying the 2D barcode of the secret.

Dissimilar to the basic VC, in extended VC scheme (Weir & Yan, 2012), more authentication processes are conducted due to its nature of using meaning pictures (2D barcode) as background. Two images are selected as the barcodes which are treated as the background picture of the VC shares. By operating extended scheme of secret sharing process, two shares are generated which can reflect two selected barcodes visually on the entire share images. The original secret will be revealed after superimposed the two shares. Authentication processes exist in both methods before and after the secret revealing in the extended VC.

Apart from the embedding scheme determination, the selection of barcode is also an important task in authentication of VC shares as a suitable barcode not only decreases the observation difficulty of the secret by inducing the negative effect to the visual quality of shares, but also provides much convenience and sufficient information for authentication. The enhancement of the utilization of 2D barcode in VC authentication is focused and experimented in this research. One contribution of this research is to propose a scheme extends the current knowledge of using 2D barcode in VC authentication.

In addition to explaining the adaption of using 2D barcode for VC authentication and providing relevant schemes, Weir et al. also conducted an experiment of embedding 2D barcode. However, in that experiment 2D barcodes are only embedded into four corners of VC shares which significantly affect the visual effect of shares, thereby influencing the secret revealing outcome to some extent.

3.3 Research Questions and Hypothesis

The prime objective of this thesis is to understand how to effectively improve the authentication process of VC. By raising this research question and reviewing previous related works, experiments of utilizing 2D barcode, Braille as well as visual and cryptographic features are proposed to be conducted. Therefore the main research question of this survey is: **How to help improve the effectiveness of VC authentication.**

The following sections in this chapter explain the experiment schemes to be used in this research. Based on the main research question of this thesis and the literature review in Chapter 2, the main research question can be divided into three sub-questions:

1. **How to improve the use of 2D barcode Braille in VC authentication?**
2. **Whether the use of Braille is able to improve VC authentication?**
3. **Whether analyzing the visual and cryptographic features of VC can be helpful for VC authentication?**

Through the process of revising past related researches and the analysis of the adaption of 2D barcode, Braille as well as visual and cryptographic features in VC, the main hypothesis of this thesis can be described as:

The authentication process of VC can be enhanced by properly embedding 2D barcode, Braille and information of visual and cryptographic features into VC shares.

The experiment in this thesis is designed to verify the hypothesis and each of these sub-questions will be answered by the experiment result analysis.

3.4 Data Gathering and Experiment Environment

Even though there are three experiments in this research aiming at the three sub-questions mentioned above, the test bed to be used in these three experiments is the same. Moreover, the research of this thesis is conducted based on basic VC, which requires the images in data set to be binary images. The suggestion data set for VC experiments could be found from the appendix.

3.5 Solutions for Visual Cryptography Authentication Using 2D Barcode

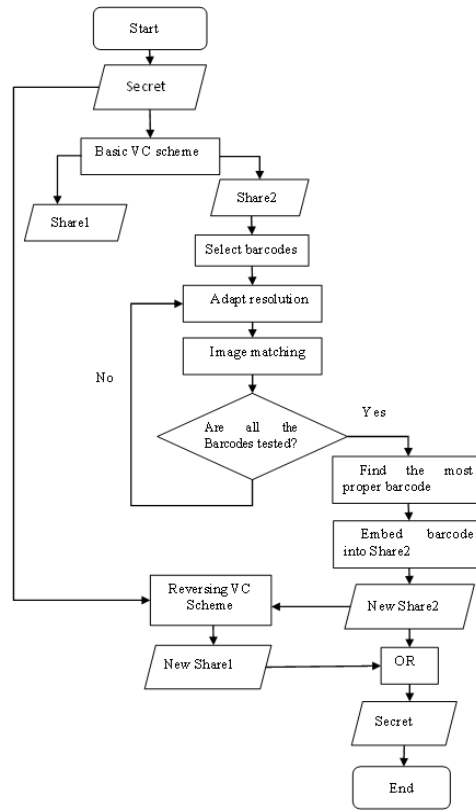
2D barcode has the advantage of only comprising of black and white dots and provides security for authentication, it is therefore reasonable to combine the VC and 2D barcode together for further check and secret verification as in the traditional VC, basic shares are also organized by arrays of only black and white dots.

Embedded 2D barcode into the corner of shares greatly avoids the secret revealing when these shares are superimposed. In some cases when important information is

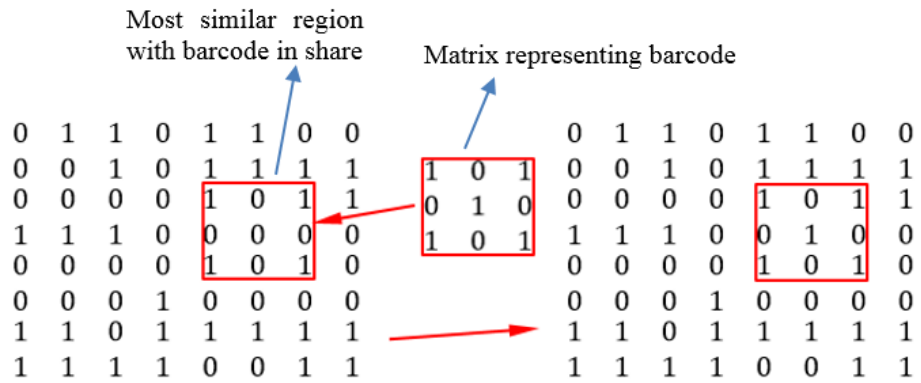
stored around edges of the image, embedding 2D barcode into the corner of shares will significantly impact the visual effect of the secret sharing. More severely, some useful information on the corner of original image will be replaced by 2D barcodes which have not real meanings in revealing secret except for playing as an authentication tool. As a result, it apparently is significant to search for other methods which can achieve both goals of authentication and reveal the full secret.

There are commonly two approaches available. Firstly, searching for the regions which are not occupied by the secret data in the original picture, replacing these regions with 2D barcodes can be an ideal way to preserve the full data of secret and to embed 2D barcodes for authentication. However, to achieve the semantic part of this approach which is to recognize the meaningful regions from other areas of one image is still far from mature, cheaters can probably predict the regions with meaningful information in the original image which tends to facilitate their attack process. Furthermore, when the share is filled with useful information, there will be no available place for barcode embedding. The other effective method is to find a proper 2D barcode to replace certain regions in the shares which are similar with that barcode. This approach is feasible to be applied in practice as the image matching process of finding similar share regions with 2D barcodes can be easily realized by programming languages. Moreover, because of the similarity between the 2D barcode and the replaced region, the secret can still be revealed by using the share which is embedded with 2D barcode. The 2D barcode is required to be similar with the replaced region to a certain extent in order to make the superimposed shares can clearly present the secret, therefore the content of 2D barcodes and embedded regions both dramatically impact the result of secret revealing.

In order to compare the method of directly embedding 2D barcode to the corners of shares and that of replacing similar region of shares with 2D barcode, we propose an algorithm and conduct experiments to verify the improvements in this thesis. Figure 3.1(a) illustrates the proposed process for embedding 2D barcode into VC shares. Figure 3.1(b) presents an example to explain how a barcode is embedded into VC shares.



(a)



(b)

Figure 3.1 Flowchart of embedding 2D barcode into VC

In the proposed scheme, a secret is firstly divided into two shares *Share1* and *Share2*. Then a 2D barcodes with predefined content are constructed. The resolutions of the 2D barcode and *Share2* are adapted before matching these two images to search for the most suitable region on *Share2* to be replaced by the 2D barcodes. The final embedded *Share2* will be determined after comparing the candidates of *Share2* embedded with different barcodes. The original secret image is then used to produce new *Share1* by

using reversing operation of VC scheme. Lastly, new *Share2* and new *Share1* are overlaid to reveal the secret which is closely similar to the original secret.

3.6 Braille for Visual Cryptography

As the blind read articles by touching and identifying salient points on Braille, we need to first find out how salient points on Braille are related to the pixels on VC shares. In order to facilitate the identification of image reading for Braille-users, each block of six pixels on VC shares represents a Braille cell and salient points are only embedded into black pixels. Figure 3.2 shows examples of the correspondence between Braille cells and blocks of six pixels on VC shares.

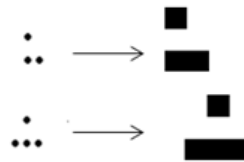


Figure 3.2 Examples of Braille

The Braille is also in support of the grayscale VC. Character ‘a’ is able to represent the pixel with grayscale value of 1 and character ‘b’ or ‘c’ tends to be used for expressing pixels whose grayscale value is 2. In a similar way, Braille of other alphabetic characters can be utilized to represent pixels with certain grayscale values based on the number of their black dots. Furthermore, colour images can be separated into R, G, B channels and each of the RGB channels is able to be represented by Braille on the basis of depth of red, green and blue in the picture.

As Braille cell has three rows, there is also a problem that the height of share may not be multiple of three. Two possible ways are presented. The first choice is to expand the resolution of VC shares to its triple size. The benefit of this operation is that the Braille can be used to occupy the whole space of VC shares. However, it would spend much time on recreating another share. Another way is to change the last one or two rows to be all white. This solution is more preferable than the former choice. The first reason is that a character of space is comprised by two columns of three dots therefore blind people can easily differentiate this extra line from a character of space. Furthermore, this method would not increase the size of VC shares, thereby keep the consistency with the original shares and secret, it also saves time than that of the first method. The flowchart of embedding Braille into a share is shown in Figure 3.3.

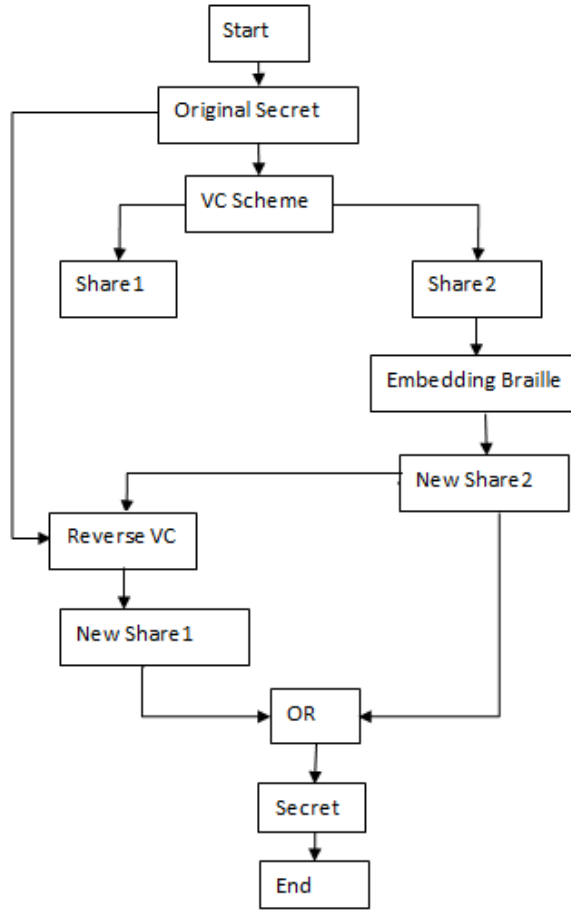


Figure 3.3 Flowchart of embedding Braille into VC shares

The process of embedding Braille into VC can be divided into two main sub-processes. First, using basic VC scheme separates the secret into two shares and one of the shares is replaced by Braille input. The second sub-process is to use the replaced share (New Share2) so as to determine the appearance of the other share. The whole process of embedding Braille focuses on input meaningful Braille information and the secret recovery result.

Since VC secret is obtained by superimposing its shares together, it is possible to get one of the shares by using the XOR operation on the other VC share and the original secret image. As the reversibility of XOR operation, we can get the pixel values of one share depending on the corresponding pixels in the secret and another share. Namely, if one pixel S in secret is gained by conducting XOR on one pixel S_1 in *share1* and another S_2 in *share2*, we can get $S_1 = S_2 \oplus S$ and $S_2 = S_1 \oplus S$. Moreover, the secret image used in producing new *share2* is the overlaid result of original *share1* and *share2* in order to keep the same resolution as new *share1*.

3.7 Analysis of Visual Cryptography Features

The proposed scheme is illustrated in Figure 3.4. In this scheme, the first step is to use (2, 2)-traditional VCS to separate the original secret image into two shares. Next, we use both visual features and cryptographic features to calculate the digital signature, and assign the signature to the 2D barcode. Subsequently we apply Discrete Walsh Transform (DWT) on the shares and embed 2D barcodes into the transformed shares. There are two benefits of printing signatures on the share. On one hand, visual features and the identification of distributors can be stored and coded into digital signatures. On the other hand, as tempers of VC authentication severely affect the secret revealing and share verification, digital signature plays a key role preventing forged share and protecting the genuine share from being modified. In order to verify the digital signatures, we use digital certificate from the key certificate authority (CA) which distributes authorized public key for authentication. Finally, the new shares are created by inversing Walsh transforms on the transformed shares. The flowchart of using features in VC is illustrated in Figure 3.4.

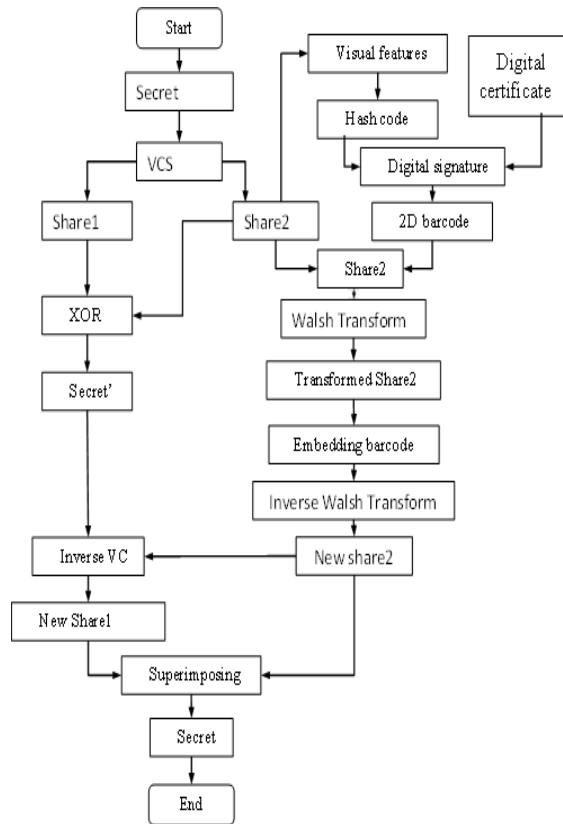


Figure 3.4 The proposed process of producing VC share

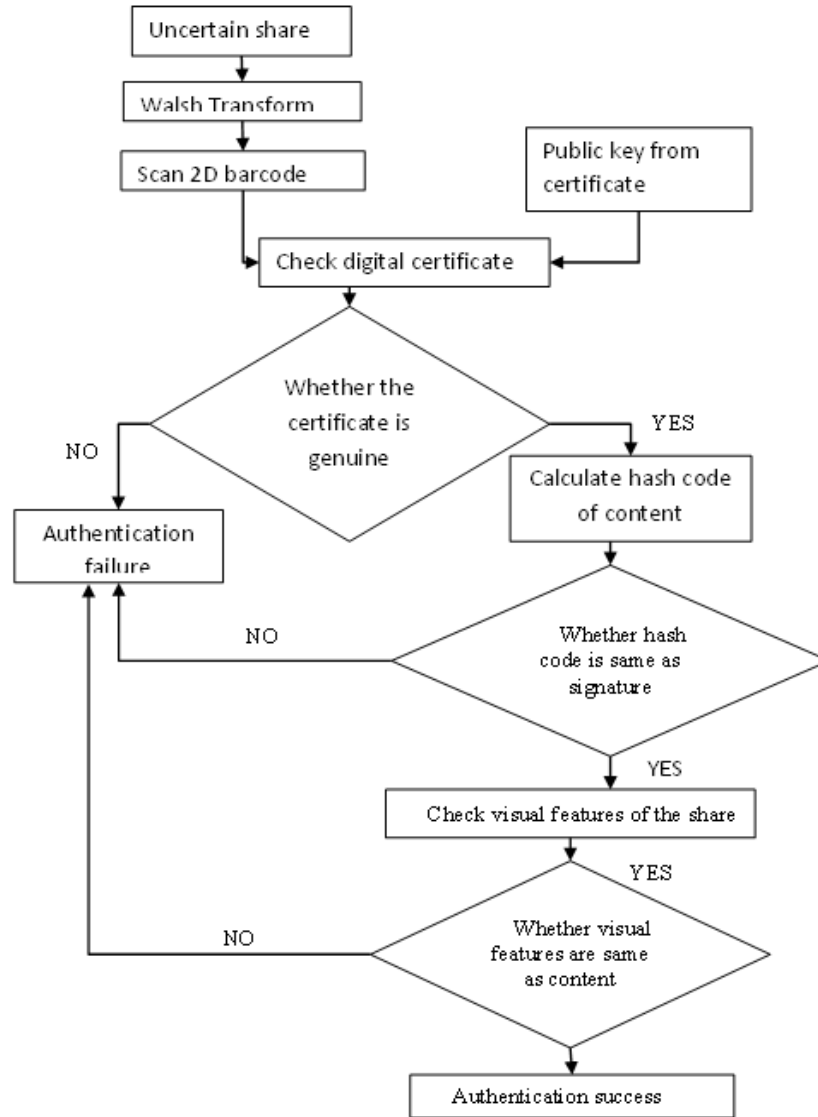


Figure 3.5 The proposed process of VC authentication

Before the final process of secret revealing, the Walsh transform should be applied to the new share so as to obtain the 2D barcode. The decryption process will continue once the authentication information in 2D barcode is verified correctly by the dealer. Hash code of VC share information needs to be stored in 2D barcode. Available information includes pixel number, histogram information, moments, entropy and Tamura texture as shown in Figure 3.5.

The benefit of using Walsh transform is that all the VC shares can be encrypted by using 2D barcode of visual and cryptographic features for authentication without affecting the visual quality of shares and secret revealing. As an extension for our proposed scheme, using visual and cryptographic features is still effective for VC authentication when

applying to (k, n) -VC. And each of the shares has independent authentication process which tends to make sure the authentication of VC shares.

Furthermore, the places where 2D barcodes are embedded into transformed shares will affect the result of inversing Walsh transforms. It is preferable that the embedded region on the share can be similar to barcodes, which tends to have slight visual impact on the new shares.

Chapter 4 Research Experiments and Findings

4.1 Introduction

On the foundation of designed experiment in Chapter 3, three experiments are implemented and the results are collected for further analysis. All these three experiments are explicitly described step by step. Specifically, embedding 2D barcode into VC share has four steps including barcode selection, resolution adaption, image matching and replacement, and secret recovery. Embedding Braille has two steps including Braille selection and Braille embedding. The analysis of visual and cryptographic features has four main steps involving visual features extraction, cryptographic features producing, Walsh Transform and feature information embedding.

4.2 2D Barcode for Visual Cryptography

4.2.1 Resolution Adaption

The resolution of the 2D barcode needs to be adjusted to that of the target share in the first step of the proposed scheme for embedding 2D barcode. Specifically, there are three reasons for the necessity of processing this step: Firstly, from the view of secret sharing, the employment of 2D barcodes is the key for authentication of VC shares. Thus we should minimize the effect of 2D barcodes on the shares at an accepted level that the barcodes can still be scanned and read by normal decoding devices. What is more, the second factor for the necessity of processing resolution adaption is to ensure the percentage of similarity between a 2D barcode and its relevant regions in a share as high as possible. On one hand, if printed dot size of the share is much smaller than that of the 2D barcode which means that one dot in the share can represent four or more dots of the barcode, the required regions in the share to match the barcode will be four or more times than that when the barcode and share have the same dot size. For example, in barcode whose image resolution is half of that of share, the pixel array displays as

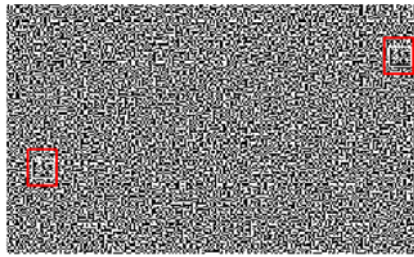
$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$; and in the share the array could be arranged as $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$ while approximately

keeping the hamming weight. However, after decreasing the image resolution of 2D

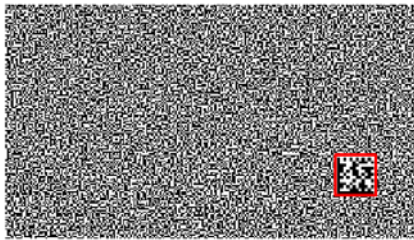
barcodes to be $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, it is easy to find that the barcode can completely match the region at its up-left corner. Moreover, the bigger for the printed dot size of the barcode than

that of the shares, the more dots of the region to be replaced in the share are required, which tends to raise the possibility of the risk to affect the secret decryption.

On the other hand, if image quality of the 2D barcode is larger than that of the share, it will be difficult to find the region which is closely match to the barcode as an array of four dots in the share can only represent one dot in the barcode. Besides, a problem lies in the fact the visual effect of embedding 2D barcodes into a share which has different printed dot size and the problem will be even much obvious when shares are superimposed to detect the secret. Figure 4.1 shows an example of comparing the secret revealing result of embedding 2D barcode with different dot sizes into one VC share.



(a) Embedding barcode (shown in red rectangle) whose size is 21×21



(b) Embedding barcode (shown in red rectangle) whose size is 42×42

Figure 4.1 The comparison of embedding the same barcode in different resolution

Algorithm 4.1: Image resolution adaption

Input: 2D barcode B and VC share matrix D

Output: 2D barcode B' with the same pixel size as VC share

Procedure:

Begin:

Set I_w = the width of barcode B

Set I_l = the length of B

Set I_W = the width of VC share D

Set I_L = the length of D

Set s = the pixel size of barcode and its initial value is 1000

For all width of B ($i = 1, \dots, I_w$)

```

        For all height of B(j = 1, ..., Il)
            If B(j,i-1) equals B(j,i)then
                p=p+1;
            else if s>p, s=p; p=1;
            else p=1;
            end if;
        end For;
    end For

    For all width of D(i = 1, ..., IW)
        For all height of D(j = 1, ..., IL)
            if D(j,i-1) equals D(j,i)then
                q=q+1;
            else if s>q, s=q; q=1;
            else q=1;
            end if
        end For;
    end For

    B' = resize the resolution of B by compress its width
        and height into Il/s and Iw/s respectively;

End.

```

In the step of resolution adaption, the smallest dot size of the VC share and that of 2D barcode are compared. Then the dot size of the 2D barcode is adapted to that of VC share. Scanning an image is able to be completed by evaluating the number of the dots making up the image. If 2D barcode has one dot occupying S pixels while every dot in VC share is represented by C pixels, the dots in 2D barcode can be transferred to be comprised of dots in a number of C (Both S and C are square numbers). One concern of using this adaption method is that it costs much more time in pixel distance computation which is in the process of image matching and replacement. Another way of adaption is to use one dot to represent S pixels in 2D barcode and C pixels in VC share. This method takes more time in the adaption than that of the first method. However, it saves a large amount of time in following process of image searching and matching as the scanning task needs to be processed by scanning C times in that of the first method.

4.2.2 Image Matching and Replacement

After adjusted the resolution of 2D barcodes and the target shares, it appears to be important to search for the region which is the most similar one with the barcodes in

share. Typically, image can be treated as an array of dots with different pixel values. In both VC shares and 2D barcodes, pixel color can be clearly distinguished as they are comprised of only black dots and white dots, thereby greatly facilitate the process of similar region matching.

In the case of VC, as there are only black and white pixels in the image, the record of the number of black and white will not be as diverse as that of various colors, thereby are less persuasive to determine the similarity of certain locations. As for the similarity measures of two images, a way of comparing two images by using the discrete metric within which the discrete distance of images is considered (Veltkamp, 2001):

$$\delta(A, B) = \begin{cases} 0 & \text{if Pixel A matches Pixel B} \\ 1 & \text{otherwise} \end{cases} \quad (4.1)$$

As the resolution of shares and that of barcode are uncertain before the embedding system receives the entities, it is not easy to choose which matching method should be used. For example, the standard revolutions of QR code vary from 21×21 to 172×172 . Commonly if the resolution of the share is larger than a certain scale, the system should use the method of extracting feature points of both share and barcode and then compare them to find the most suitable region (Vincent & Laganière, 2010). However, even though using the feature points can be efficient in dealing with large data, the result of this method cannot represent the entire pixels in image. Moreover, as the details of VC shares have no meaning features (in the case of basic VC) to be extracted for analysis, this method is considered to be improper in VC. Searching every pixel in 2D barcode and that of VC shares by using pixel comparison appears to spend a long time when the pixels have a large amount of numbers, the searching workload will be much less when applied it on small pictures. More importantly, the accuracy of matching each of the pixels in the barcode with the VC share tends to be much crucially. Therefore, the embedding system is determined to calculate the similarity distance between every pair of corresponding pixels on the barcode and the share.

Algorithm 4.2: Image matching and replacement

Input: a VC share D and a 2D barcode B

Output: New share with 2D barcode D'

Procedure:

Begin:

Set I_w = the width of barcode B

Set I_l = the length of B

```

Set IW = the width of VC share D
Set IL = the length of D
Set s = number of the similar pixels
Set p = number of the pixels in the region which is
        the most similar to barcode B
For a=1, ..., (IW-IL+1)
    For b=1, ..., (IL-Iw+1)
        For i=a, ..., (Il+a-1)
            Set s = 0;
            For j = b, ..., (Iw+b-1)
                If D(i,j) equals B(i-a+1,j-b+1),
                    s = s+1;
                end if;
            end For;
        end For;
    end For;
    If s > p,
        p = s;
    end If;
end For;
For a=1, ..., (IW-IL+1)
    For b=1, ..., (IL-Iw+1)
        For i=a, ..., (Il+a-1)
            Set s = 0;
            For j = b, ..., (Iw+b-1)
                If D(i,j) equals B(i-a+1,j-b+1),
                    s = s+1;
                end If;
            end for;
        end for;
        If s equals p,
            o = a;
            r = b;
            For i=1,..., Il
                For j = 1toIw
                    D'(a+i-1, b+j-1) = B(i, j);
                End For;
            end For;
        end If
    end for;
end for;
End

```

In the image matching, we get the pixel values of 2D barcode and VC share, then the pixel values of 2D barcode are compared with that of each region with the same size of 2D barcode in VC share to find out their most similar region(s). The matching standard is eq. (2). The pixel distance between one pixel in a specific region in VC share and its corresponding pixel in 2D barcode is the least if these two pixels have the same pixel value and vice versa. The pixel distance between the region in VC share and 2D barcode is calculated by simply summing up all the pixel distance between all the corresponding pixels in the two images. The most matching region(s) in VC share is the region(s) with the least pixel distance with 2D barcode. Lastly, 2D barcode is embedded into its similar region(s) in VC share.

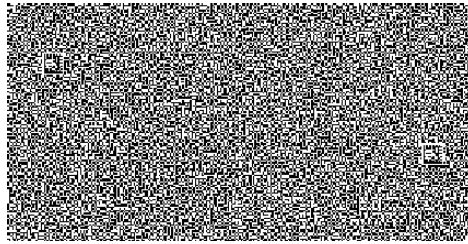
4.2.3 Barcode Selection

Since 2D barcodes have different coding structures and appearances, it is important to select the most suitable one for replacing shares with the least negative effects on visual effect. Furthermore, due to the different data content can be stored within these barcodes which will also lead to the various appearance of barcodes, selecting proper types of 2D barcodes with appropriate content appears to be an important issue in embedding barcodes into basic VC shares.

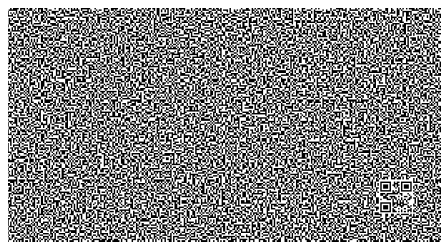
There are rich sources of barcodes available in Internet. It is therefore not hard to get samples of 2D barcodes. As a result, an optimized approach of selecting proper barcodes for a certain share is to try as many barcodes as possible to find out the most suitable one. However, as it will spend a great amount of time in searching suitable barcodes, the author will adopt some of the typical 2D barcodes and try to find out the best one from the given samples to be treated as the embedded barcode.

The result of this experiment also indicates that little change in the barcode can lead to different matching result. Consequently it is important to keep the barcode in the share can be identified clearly and accurately. Besides, different kinds of 2D barcode have obvious distinct appearance due to their encoding methods and various symbol structures. As a result, when embedding one specific type 2D barcode with similar authentication contents, the regions being replaced in the share are always around a certain region and their similarity is kept at a certain level. Thus the candidate barcodes are assumed to be various in both types and contents when being applied in practice. Even though it is obvious that using Data Matrix has less effect on the secret revealing than that of QR Code and Aztec Code as shown in Figure 4.2, the results of using QR

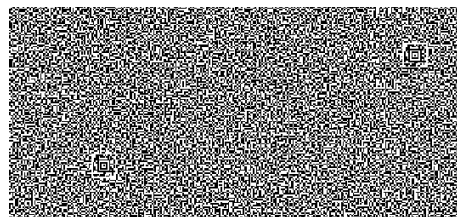
Code and Aztec Code are acceptable as the superimposed region with barcode is close to the content which has similar colour depth. Table 4.1 compares the similarity of three types of 2D barcode and the replaced region in VC shares.



(a) Secret revealing using QR code (Barcode content: AUT)



(b) Secret revealing using Data matrix (Barcode content: AUT)



(c) Secret revealing using Aztec code (Barcode content: AUT)

Figure 4.2 Secret revealing results with different barcodes

Table 4.1 The similarity comparison of three types of 2D barcode

Sample	QR	Data matrix	Aztec
Sample 1	19/400	22/144	5/400
Sample 2	15/400	13/144	7/400
Sample 3	14/400	14/144	6/400

4.2.4 Secret Recovery

Even though the authentication problem of VC could be solved by embedding 2D barcode into the most similar region in VC shares, the visual effect of the share is influenced as the similarity between the 2D barcode and the replaced region is very low. Furthermore, quality of the recovered secret using the replaced share will also be affected greatly. Therefore it appears crucial to make a change to the other share in order to have slight effect on secret revealing.

As the process of secret recovery illustrated in Figure 3, new *Share1* is created by embedding 2D barcode into proper places on *Share1* and the new *Share2* is obtained by making some changes to *Share2* according to the change of the places embedded with 2D barcode on *Share1*. The superimposed result then is proposed to be less affected by embedding 2D barcode.

Algorithm 4.3: Secret Recovery

Input: the VC share embedded with 2D barcode *S1* and the secret image *S3*

Output: a new share of Share *S2*

Procedure:

```
Begin:
    Set S1 = new Share1
    Set S2 = new Share2
    Set S3 = Secret
    Set S = Size-adapted Secret based on the pixel
           expansion of selected VC scheme
    If S equals 0
        S2 = S1
    If S equals 1
        S2 = NOT S1
    S = Q OR N;
End.
```

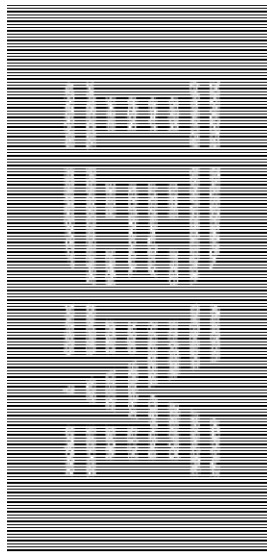
In the last step of the barcode embedding scheme, we firstly get the pixel values of the VC share embedded with 2D barcode (*Share1*) and the secret image. Then the pixel values of new *Share2* are calculated by conducting XOR operation on the value pixels on region of *Share1* replaced by 2D barcode and that of the secret image.

4.2.5 Dataset Description

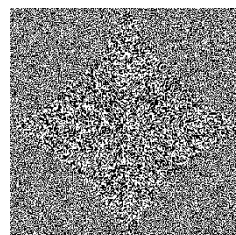
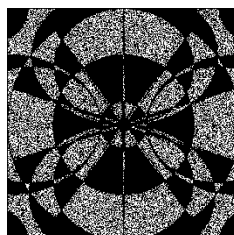
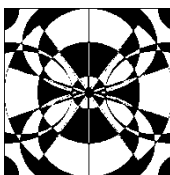
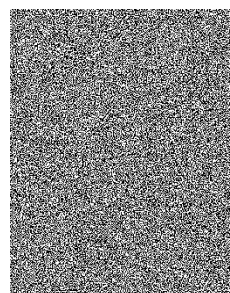
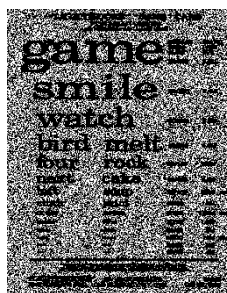
In order to test the proposed scheme of embedding 2D barcode into VC shares, a dataset of test pictures has been built up for evaluation purpose. The source of the dataset can be collected from TV test card, Fax test card, image compression, watermarking and so on. However, as nature of 2D barcode and basic VC operations, the pictures need to be transferred into recognizable binary images with only black and white colours. If the transferred picture is not meaningful or has not contrast of black and white, it should be removed from the dataset. Figure 4.3 displays some of the pictures in the dataset and the embedded ones with 2D barcode.



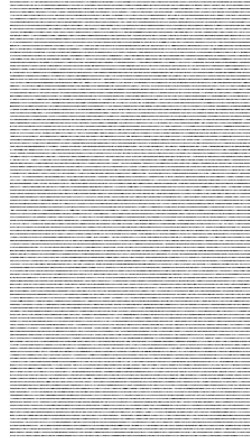
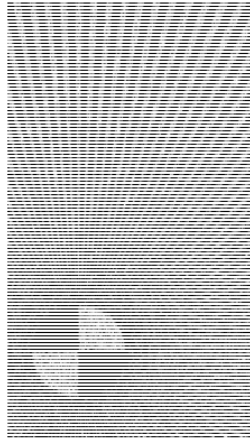
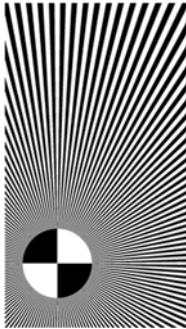
IBM



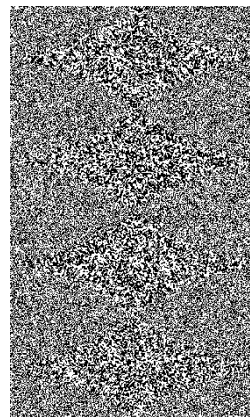
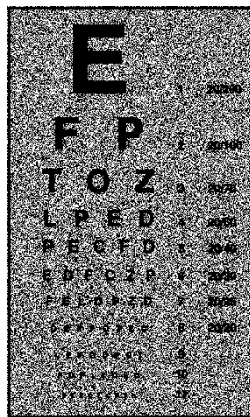
Visual chart1



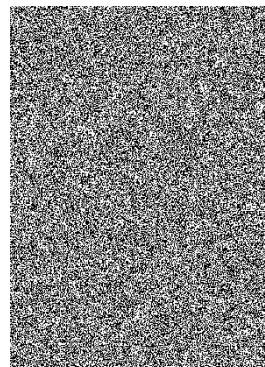
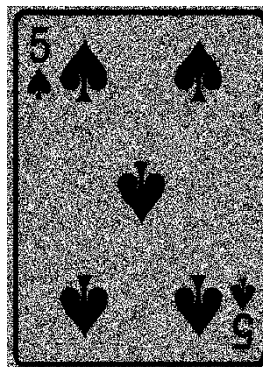
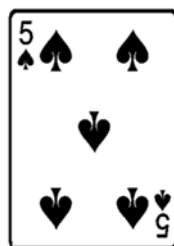
Pattern



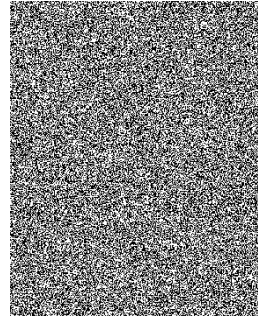
Scatter



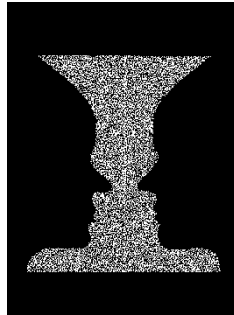
Visual chart2



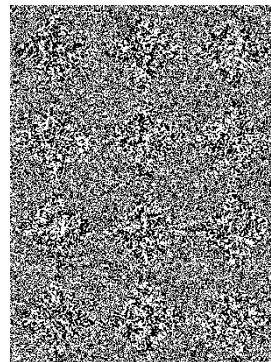
Poker



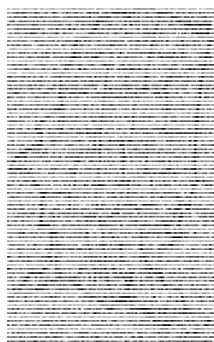
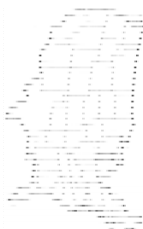
Girl and woman



Human face and
vase



New Zealand map



United States map

Figure 4.3 Samples of dataset for testing VC share embedded with 2D barcode

4.2.6 Experiments

After selecting the candidates of dataset, relevant experiments need to be set up for testing. We firstly collected 10 samples of black and white pictures and divided them into shares by VC approaches.

The table for comparing the similarities between the original secret and the secret obtained by superimposing new shares is shown in Table 4.2. There are three reflections from the results of the experiments. First, the larger secret image is, the smaller the disparity between the recovered secret and original secret will be. Further, the similarity between original share and its replaced share by computing their similar distance is less than that of randomly embedding 2D barcode into shares. Most importantly, the visual effect of embedding 2D barcodes into VC shares is maintained in an acceptable range.

Table 4. 2 Similarities between original and new secret image

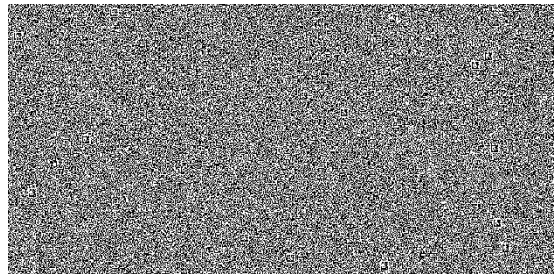
Sample	The impact of 2D barcode on share
<i>IBM</i>	13/886×432(0.003%)
<i>Visual chart1</i>	13/936×1186(0.001%)
<i>Pattern</i>	14/722×720(0.002%)
<i>scatter</i>	14/3840×2160(0.0001%)
<i>Visual chart2</i>	14/2116×3514(0.0002%))
<i>Poker</i>	13/624×872(0.002%))
<i>Girl and woman</i>	13/600×738(0.0006%))
<i>Human face and vase</i>	13/474×636(0.004%))
<i>New Zealand map</i>	14/1010×1274(0.001%))
<i>United States map</i>	14/2596×1610(0.0003%))

It is important to select secure content in authentication process. In the context of embedding a 2D barcode into VC shares, common data stored in 2D barcode are meaningful characters, namely, words, sentences and paragraphs which contain significant authentication information. Another popular kind of 2D barcode content is website. Even though the script of web link itself has not semantic information, the real authentication messages can be easily retrieved on the website.

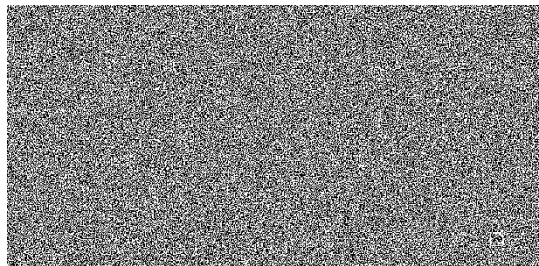
Furthermore, because all kinds of 2D barcode content mentioned above can be decoded and modified by cheaters without being noticed by VC shares holders, methods

of one-way encryption (the 2D barcode content is a cipher text that cannot be decoded) are needed. Cryptographic Hash function has the benefits of easy to calculate a Hash code for any input data, difficult to get data from a given Hash code, difficult to modify a data without altering the Hash code and difficult to find two different data with the same Hash code. Besides, as cryptographic Hash Functions are used in a large range of areas like Message Authentication, Message Integrity, Digital Signatures, Entity Authentication and Digital Steganography (Sobti & Geetha, 2012), we decide to use Hash function to encode the 2D barcode content.

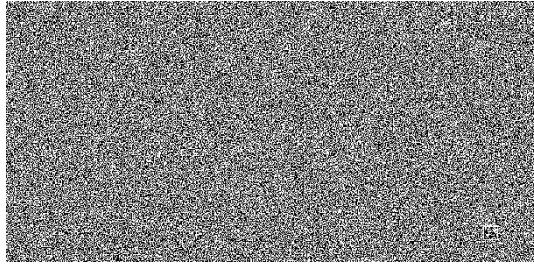
The Hash function MD4 is defined as the iteration of a three-round compression function (Dobbertin, 1998). The 128-bit (16-byte) MD4 Hashes are typically represented as 32-digit hexadecimal numbers. As an updated version of MD4, MD5 is a block-related digest algorithm which is computed over the data in phases of 512-byte blocks organized as 32-bit words. The first block is processed with an initial seed, resulting in a digest that is used as the seed for the next block. When the last block is calculated, its digest is used for the entire computation. This chained seeding prohibits parallel processing of the blocks (Touch, 1995). In this experiment MD5 is used for encoding 2D barcode content.



(a) AUT



(b) [Http://www.aut.ac.nz](http://www.aut.ac.nz)



(c) Hash code of “Height: 432 Width: 886 Blackpixels: 18563 Hints of secret: ibm”

Figure 4.4 Examples of VC shares embedded with barcodes

Another issue in authorization of VC shares is how to use 2D barcode information to differentiate the right share from the unauthorized ones. As for the case of VC share, its recognizable features are size and pixel characteristics. The advantage of using the Hash code of these features as 2D barcode content is that modified shares can be prevented in the authentication process. Moreover, as modified shares can hardly be used to reveal the true secret, hints of secret can also be included as a significant part in barcode content. Thus we decide to use the Hash code of those features of VC shares such as width, length, the number of black and white pixels in the share as well as related information of secret. All the relevant information of 2D barcode content can also be copied and kept by the dealer who is subsequently able to easily check the correctness of authentication information stored in 2D barcodes of the VC shares by using 2D barcode scanners and decoders.

Even though the advantage of embedding 2D barcode into VC shares and its benefits in the authentication which can be evaluated by both CIA and AAA, there exist drawbacks of this approach of authenticating VC share. Firstly, despite the replaced regions in VC share are the most similar region with 2D barcode, the similarity is still very low that cheaters are able to find the 2D barcode on VC share in some occasions. Furthermore, the superimposed result of new shares is not strictly as same as the original picture of secret. This is due to the computational similarity between OR and XOR operation. Therefore it is expected to improve the barcode embedding process to make the authentication process more effectively. Besides, our algorithm of embedding 2D barcode is only applied to $(2, 2)$ -VCS. More cases of (k, n) -VCS are expected to be researched.

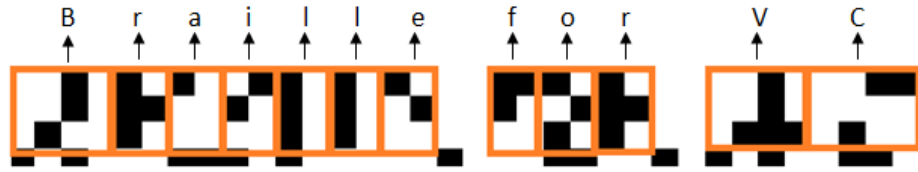
4.3 Braille for Visual Cryptography

4.3.1 Experiment for Embedding Braille

Figure 4.5 shows a region of a share and the region after the original content of this share are replaced by Braille. Every red rectangle in Figure 4.5(b) represents a certain letter with the consideration of whether it is in capital form.



(a) Original share of visual cryptography.



(b) Replaced share (a) by Braille.

Figure 4.5 Regions of VC share are replaced by Braille, the red rectangles are used to indicate Braille cells.

Algorithm 4.4: Embedding Braille into a VC share

Input: Braille string A , VC share Img

Output: A VC share embedded with Braille Img'

Procedure:

$i=0$;

While ($i < \text{Length of } A$)

{

 Judge and find whether $A[i]$ is a capital letter or a number

 If $A[i]$ is capital then $A[i]$ occupies two Braille cells in Img and the pixel at right bottom corner of the first Braille cell turns black;

 If $A[i]$ is number then $A[i]$ occupies two Braille cells in Img and all the pixels of the first Braille cell except the first two in the first column turn black;

 Map $A[i]$ to Braille characters;

 If the lower case of $A[i]$ is from 'a' to 'z' then change the pixel order in every Braille cell-shaped region in Img complying to Braille coding rules.

 If $A[i]$ is from '0' to '9' then change the pixels in Img according to the order of characters from 'a' to 'j';

```

        i++;
    }

```

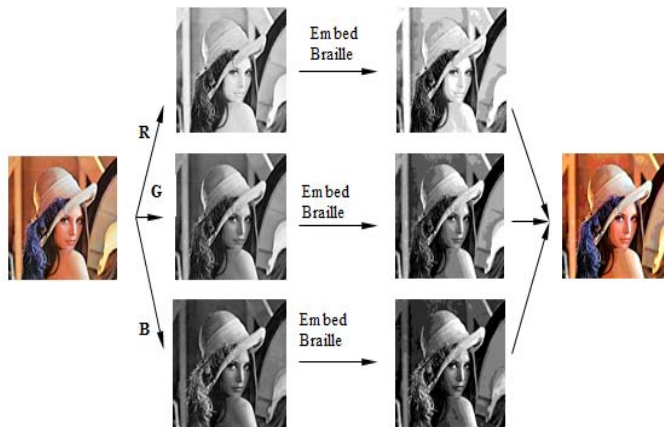
Algorithm 4.4 illustrates how Braille cells are embedded into VC shares. According to Braille rules, capital characters and numbers hold two Braille cells. Besides, every alphabetic character appears to have its own arrangement in the cell.

4.3.2 Results

In this thesis, we use Matlab as our programming platform to conduct this experiment. The dataset of original secret image contains six images as our test bed. These images are transferred into binary images for further analyzing. Figure 4.6 shows the images (gray and color) which are presented by Braille. The tested images and their restored images as VC secrets using Braille are shown in Figure 4.7.

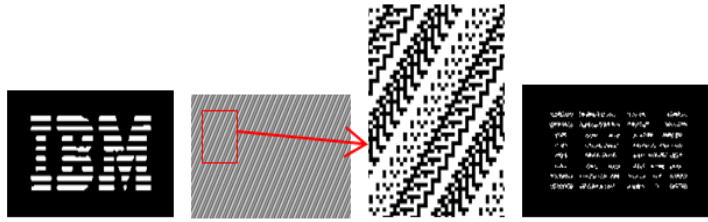


(a) Grayscale image presented by Braille

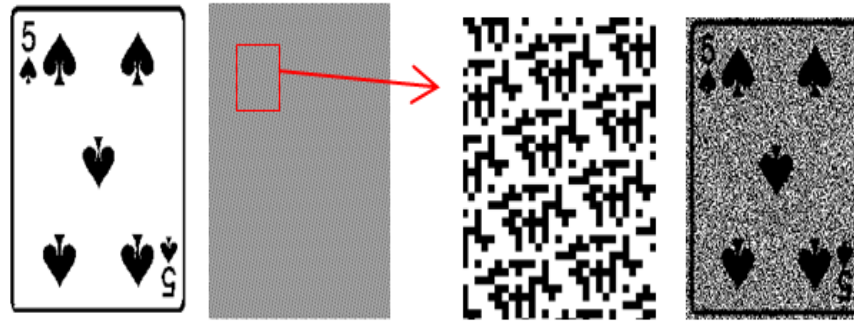


(b) Color images presented by Braille

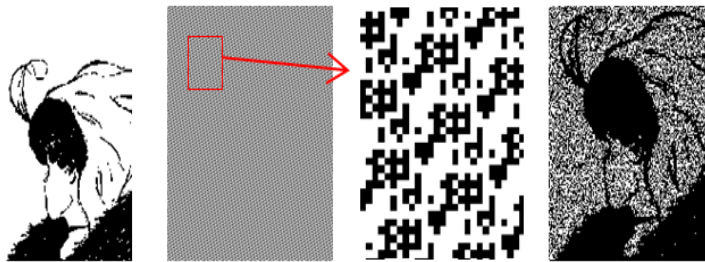
Figure 4. 6 Images presented by Braille.



(a) Sample 1



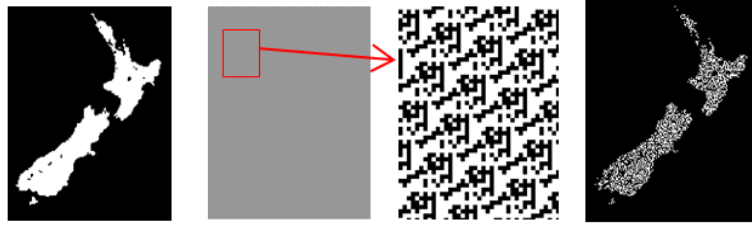
(b) Sample 2



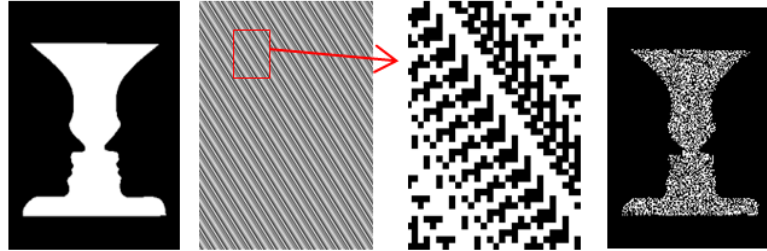
(c) Sample 3



(d) Sample 4



(e) Sample 5



(f) Sample 6

Figure 4.7 Pictures in the test set of embedding Braille into VC shares.

In the process of embedding Braille, it is important to count the number of the Braille cells to be implanted in VC share since the scale of VC share is in a limited size. Table 4.3 indicates the percentage how secret image is affected by embedding the Braille. This table indicates the similarity between the original secret and the recovered VC secret in the test bed. From the results in Table 4.3, it is obvious that secret revealing has only been affected after embedding Braille into one of the VC shares.

Table 4.3 The accuracy of recovered secret image

Samples	Accuracy (%)
1	98%
2	96%
3	97%
4	96%
5	96%
6	98%

4.4 Features Analysis

4.4.1 Experiment for Feature Analysis in Visual Cryptography

In this thesis, we aim at dealing with VC authentication problems by utilizing both visual features and cryptographic features of VC shares. As mentioned previously, available VC visual features include histogram, moments, centroid, entropy and Tamura texture. Any minor changes on the shares are assumed to be revealed by matching these features. In order to facilitate the comparison process, it is important to select a comparison method in the context of VC authentication.

In our proposed scheme, the feature vector \mathbf{V} has a high dimension, it is composed of visual features f_i ($i = 1, 2, \dots, n$). Each feature is treated as a component of the vector, we could write the feature vector as $\mathbf{V} = (f_1, f_2, \dots, f_n)$. All the features in the vector are independent to each other. Each component has its special meaning, the comparison of feature vectors of VC share can be calculated by their scalar quantity.

The relationship between features and cryptographic algorithm in VC can be interpreted as $F_s = C(V(s))$, where s denotes to the share, V means a feature vector and C means the cryptographic algorithm which is calculated based on a certain visual feature vector. Given a VC share, the authentication process can be defined as $d = D(F_{s1}, F_{s2})$, where D is the function which measures the distance between the features of two shares S_1 and S_2 .

The measurement of distance between two VC shares can be calculated by using distance computational method. The most popular distance is Euclidean distance which can be described as:

$$d(x, y) = \sqrt{\sum_{n=1}^m (x_n - y_n)^2} \quad (4.2)$$

where m denotes the number of feature components and $d(x, y)$ represents the similarity between two VC feature vectors x and y . A VC share can be presented by such a vector, and each vector has m dimensions.

Another broadly used distance is inner product (or dot product) which calculates the distance between two vectors. This distance can be computed by:

$$\cos(x, y) = \frac{x \cdot y}{|x||y|} = \frac{\sum_{n=1}^m x_n y_n}{\sqrt{\sum_{n=1}^m (x_n)^2} \times \sqrt{\sum_{n=1}^m (y_n)^2}} \quad (4.3)$$

where m denotes the number of feature components to be used. The equation (16) presents the cosine value of the angle between two vectors, the distance is ranged from 0 to 1, where 0 means completely different and 1 stands for completely same, respectively. In this thesis, we utilize Euclidean distance as our similarity measurement of two vectors. The procedure of our proposed routine is illustrated in algorithm 4.5.

Algorithm 4.5: VC Share Authentication

Input: VC share S_1

Output: New VC share with authentication ability S_2

Procedure:

Step 1: Initializations;

$Coar = \text{Coarseness}(S_1)$
 $Cont = \text{Contrast}(S_1);$
 $Dirc = \text{Directionality}(S_1);$
 $Line = \text{Linelikeness}(S_1);$
 $Reg = \text{Regularity}(S_1);$
 $Mom = \text{Moment}(S_1);$
 $Entr = \text{Entropy}(S_1);$
 $Cent = \text{Centroid}(S_1);$

Step 2: Calculating Hash codes;

$H_1 = \text{hash code}(Coar);$
 $H_2 = \text{hash code}(Cont);$
 $H_3 = \text{hash code}(Dirc);$
 $H_4 = \text{hash code}(Line);$
 $H_5 = \text{hash code}(Reg);$
 $H_6 = \text{hash code}(Mom);$
 $H_7 = \text{hash code}(Entr);$
 $H_8 = \text{hash code}(Cent);$

Step 3: Compose the feature vector $\mathbf{H} = (H_1, H_2, \dots, H_8)$, H_i is its components;

Step 4: Producing 2D barcode B with the content of the digital signature of vector \mathbf{H} according to 2D barcode encoding rules;

Step 5: Applying Digital Walsh Transform on a selected VC share: $W = \text{dwt}(S_1);$

Step 6: Find the most similar region of VC share matched with 2D barcode in frequency domain;

Step 7: Embedding the 2D barcode into W in frequency domain;

Step 8: Find the embedded 2D barcode via Inversing Walsh transform: $S_2 = \text{idwt}(W)$

Step 9: Comparing the Hash codes included in the 2D barcode so as to authenticate the two VC shares.

4.4.2 Results and Analysis

The source of the test set was collected from TV test card, Fax test card, test bed of image compression and digital image watermarking and so on. These pictures are

various in picture size. Furthermore, two of these pictures have the background color of black while the other three have the background color of white.

Table 4.4 Tamura texture value of a VC share

<i>Feature</i>	Coarseness	Contrast	Directionality
<i>Value</i>	0.9125	0.2500	19.2888
<i>Feature</i>	Line-likeness	Regularity	Moment
<i>Value</i>	0.1244	0.9486	6.6132
<i>Feature</i>	Entropy	Centroid	
<i>Value</i>	0.94	(505.5008, 637.5004)	

According to our proposed scheme, all these features will be translated to computable vectors and could be explained by mathematical equations, the vector could be encoded into Hash code. The values of the visual features mentioned are shown in Table 4.4, the Hash code of this vector is:

**B96CC5EA402D4E164A8F885D86F017C5EEEA563A1445D1560954034A10CD2D
A9**

The 2D barcode of embedding this Hash code into Data Matrix is shown in Figure 4.10. Since slight difference in the content of Hash code will lead to a big change in the result, we attempted to make some modifications on a VC share and conducted experiments using our proposed scheme to authenticate the modified share. The result is shown in Table 4.5. Data Matrix of Hash code is shown in Figure 4.8.

Table 4.5 The comparisons between genuine share and modified shares

Share	Hash code	Authentication Result
<i>Original share</i>	B96CC5EA402D4E164 A8F885D86F017C5EE EA563A1445D1560954 034A10CD2DA9	N/A
<i>Slightly modified share</i>	F32E0FFF80C7892E98 D74286BCFC119A476 E0ECAAF5244DA23E5C F8F1B51EAD1C	Failure
<i>Slightly modified share</i>	3DE1C857EA8CC508A E5FA70EE2DD3E9C3 A86F48A9CC35819D0 6112E1B54AC633	Failure
<i>Largely modified share</i>	301976929CD68C6D9B C0A2DD99C0F072698 310E0B500DD1A41AF 3BE92A818611	Failure
<i>Largely modified share</i>	A2E8980A9845CB637 E996F191C2C6908439 9E8DD26B8142E5C27 2F7BF082E7DD	Failure

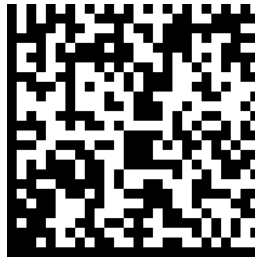
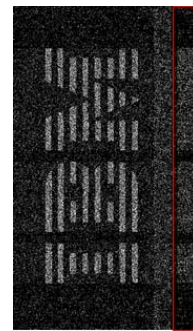
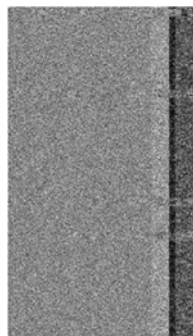
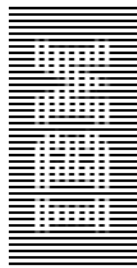
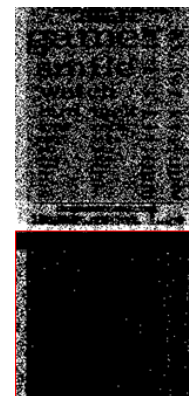
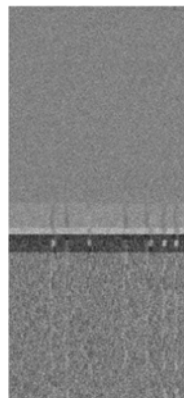


Figure 4.8 Data Matrix of Hash code.

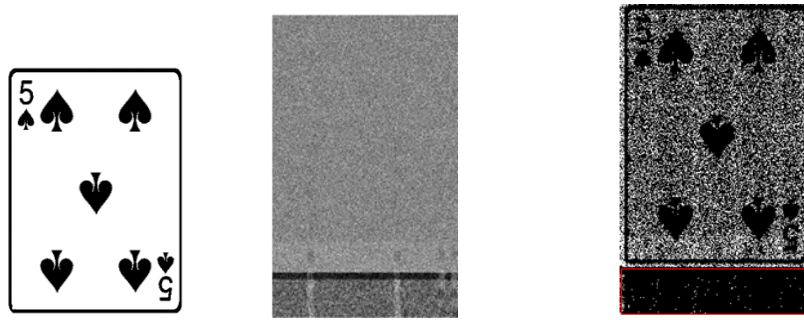
**‘B96CC5EA402D4E164A8F885D86F017C5EEEA563A1445D1560954034A10CD2
DA9’**



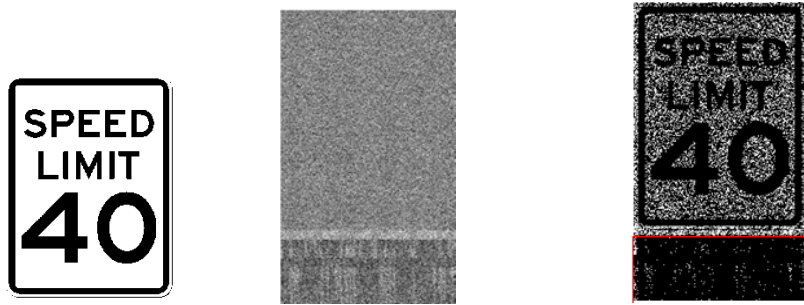
(a) VC example 1



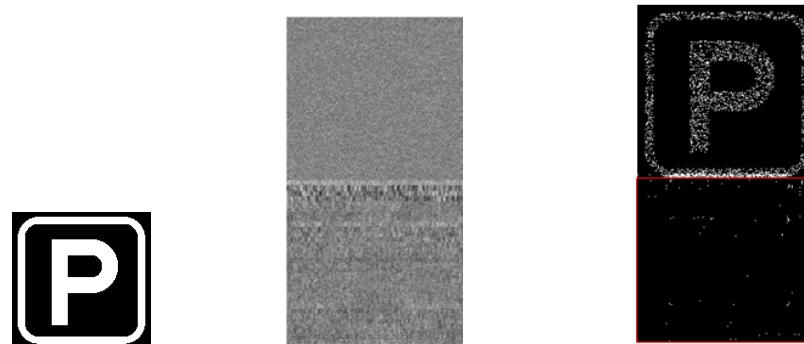
(b) VC example 2



(c) VC example 3



(d) VC example 4



(e) VC example 5

Figure 4.9 VC experimental results

The original secret images are listed on the left side of Figure 4.9 and their VC shares which are processed using our proposed scheme are shown in the middle. The images on the right side of Figure 4.9 are the recovered secrets.

Table 4.6 Similarity between original secret and the recovered secret

VC images	Image size	Similarity
1	886×432	90%
2	936×1186	91%
3	624×872	91%
4	606×800	90%
5	550×528	90%

The result in Table 4.6 shows that recovered secret is closely similar to that of original secret. One noticeable change is that there is a block of black region under each share (marked with red color) and the image of restored secret. This is a kind of salting because the required width and height of the image in the Walsh transform are required as a power of two. However it does not significantly affect the visual quality of each share, the embedded 2D barcode can be revealed for the authentication purpose.

Chapter 5 Discussions

5.1 Introduction

This chapter will use the results of the three experiments presented in Chapter 4 for answering research questions and hypothesis analysis. All of the experiments explained in Chapter 4 respond the research questions raised in Chapter 3. One noticeable issue is that despite the dataset for the experiments is the same, these three experiments are designed for solving VC authentication problem in consideration of different situations and environments. As there is no confliction amongst these three experiments while they have various circumstances, it is preferable to analyse these three experiments separately.

Chapter 5 is organised into four parts. The analysis of the experiments of 2D barcode for VC will firstly be explained. Then embedding Braille into VC shares is considered which is followed by the description of using visual and cryptographic features. Lastly, implications and justifications are presented after answering the raised questions.

5.2 2D Barcode for Visual Cryptography

One of the motivations for improving VC authentication by using 2D barcode is to reduce the visual effect. While the similarity of dots between VC and 2D barcode, their appearances tend to be different according to their different encoding rules. On one side, it is expected to minimize the visual effect by choosing the most similar region in VC share with that of selected 2D barcode. On the other side, it is vital to pick suitable information to be embedded into 2D barcode. The experimental results of embedding 2D barcodes into VC shares show that the visual result of embedding 2D barcode into VC shares is limited into a small range and the secret revealing results are only slightly impacted, which appears to have no effect on correctly secret perception visually.

Despite the explicit merits of using 2D barcode for enhancing the security of VC shares in this research, there are several restrictions which need be discussed. One of the frequently focused issues in experiment is time consuming. In the experiments of this research, the time cost of embedding 2D barcode into VC shares rises with the increase of the image pixels of the tested secret images. Moreover, the configurations of experiment environment also have impacted on the computing speed of this experiment, such as the programming environment and hardware equipment. While the time

consuming is critical in the process of splitting secret image and producing shares embedded with 2D barcode, the accuracy of secret revealing relies on the complexity of tested images and embedding algorithms.

Despite the selected images for 2D barcode embedding are required to be binary images, they are selected from various areas such as visual charts, maps and poker cards. All these images have their own characteristics with different appearances and structures. For example, the secret image of visual chart is used to examine whether small details of secret would be affected after embedding 2D barcode as there are a large number of characters in the chart. The secret image e.g. girl and woman is used to check whether the view of both girl and woman would be impacted by embedding 2D barcode. The variance of the selected test set for the experiment is able to show the adaption of using 2D barcode for VC authentication.

Another issue exists in the pixel expansion of VC secret. While one black pixel in the secret can only be expanded into blocks of black dots in all its shares, the situation of white pixel is just on the contrary that it has two possible expansion approaches, namely, all white pixels in both shares or one white in one share with the other in black. When taking the consideration of embedding 2D barcode into these shares, an optimized solution is to retrieve all the possible shares of the secret and search for the best pair of shares and 2D barcode.

5.3 Braille for Visual Cryptography

The method of embedding Braille into VC shares analyses the effect of Braille on VC shares by experiments. The results reveal that using Braille helps enhancing authentication process of VC by embedding authentication information on shares and has little effect on the shares. Participants are also able to get every dot of secret by simply superimposing the corresponding pixel on each of the shares.

Similar to the experiment of embedding 2D barcode into VC shares, the purpose of embedding Braille aims at enhancing the strength of authentication process. Major benefits of embedding Braille into VC shares include helping blind people understand the content on VC shares, enhancing decryption ability in dark environment and authenticating information being encoded as Braille and embedded into VC shares. And also, Braille can be regarded as a cipher text. Authenticated information can be coded as

Braille and embedded into a VC share. At the same time, the other share also tends to have authentication information.

Dissimilar to the 2D barcode embedding experiment which seeks proper regions on VC shares for barcode embedding, the experiment of embedding Braille attempts to replace the whole content of VC share with the appearance of predefined Braille. The result shows that embedding process has less effect on final secret revealing when there are less repeated patterns on VC shares, namely, repeated contents or closely similar contents. Moreover, the ratio of black and white pixels on VC shares should be approximately 1: 1 as the other reproduced share would appear to have indications of secret according to the VC encoding rules. Therefore the selection of Braille content tends to be critically important for the result of this experiment.

Even though the advantages of Braille in VC, there are drawbacks of Braille in VC needed to pay attention to. First, as meaningful authentication information is embedded into one of the VC shares, the Braille on the other share is possibly meaningless and hard to be verified. Moreover, this thesis mainly concentrates on the (2, 2)-VCS, further related researches are expected to investigate more on other types of VC.

5.4 Visual Cryptography Features Analysis

This thesis also analyses VC authentication problems using visual and cryptographic features. New understanding of visual cryptography authentications is obtained by the way introduced in Chapter 3. With joining visual and cryptographic features in VC shares is able to be attributed to the main factor of the need in VC authentication, accompanied benefits include a comprehensive analysis of VC and the adaption of this scheme in most cases of VC. However, significant issues appear to be argued including properly embed the 2D barcode into shares without affecting the visual quality of secret revealing.

Dissimilar to the experiment of 2D barcode embedding, the experiment of VC features analysis emphasizes on determining the types of features which are able to be used for VC authentication through the channel of 2D barcode and the Walsh Transform as well as the Inverse Walsh Transform. Employed Hash code types in these two experiments are also different. While MD5 has been widely studied and applied, SHA-3 is a lately invented with new features. The comparison of these two types of Hash codes is still expected to be studied further for VC authentication.

Despite 2D barcode is embedded into Walsh transformed images which will be subsequently transferred back into VC shares, it may affect the visual quality because of modifying parts of the share in the frequency domain. When taken the consideration of embedding 2D barcode into these shares, an optimized solution is to retrieve all the possible shares of the secret and search for the best pair of shares and 2D barcode.

Even though there are a range of benefits of using 2D barcodes in shares, the contributions addressed in this thesis have practical applications. The VC research is expected to extend its vision from current VC constructions to a much wider domain such as analysing VC content features. Our proposed VC authentication selects those content based VC features from digital image processing, we will analyse further modern cryptographic features for VC authentication in future.

5.5 Implications and Justifications

Previous researches have studied a range of VC authentication methods. While the use of addition shares is very helpful but lacks of convenience, blind authentication techniques are promising as their consistency and flexibility. This thesis analyses the benefits of using 2D barcodes, Braille as well as visual and cryptographic features for VC share identification and verification. The improvement which has been addressed by this thesis can have practical implications for further coming researchers.

The awareness of embedding 2D barcode into VC shares is mainly due to the factors that this kind of cipher has the similar appearance with that of basic VC and the large storage of saving authentication information within a small size of shape. Moreover, the popularity of barcode in the world also makes it easy to be decoded by using applications on mobile phones and other devices. Therefore, by combining VC with other popular tools, the applications of VC authentication will have a great deal of practical potentialities. Similarly, Braille is the worldwide commonly accepted reading language for the blind, the combination of VC authentication and Braille is highly like to deal with the security problems.

Furthermore, the analysis of visual and cryptographic features is expected to build up a new knowledge of VC which aims at improving the research of VC, especially in the field of VC authentication. Further researches of VC features are expected to be vary from more feature types and features with easy identification and high accuracy are preferable. Practitioners are able to extract and store data of VC features in a repository

where the VC dealers' work would be facilitated by comparing the features of given shares and the electric version of features stored in local or web based devices such as a database or cloud.

Chapter 6 Conclusion and Future Work

As a branch of secret sharing, VC has drawn much attention as its security mechanism involving the consideration of both image processing and cryptography. With the development of VC in the areas of dealing with different types of secret images, the applications of VC appear to be flourished and more practical. However, compared to the awareness of VC secret image types, the authentication of its shares is still far from being maturely researched and cheating immune VC is becoming more and more vital for the security of whole VC process.

Based on reviewing the previous researches of VC authentication and studies of other information protection mechanisms, this thesis raised the research problem of how to improve VC authentication and related hypothesis. In order to design experiments for dealing with the research problem, three possible solutions are proposed and each of these solutions has been integrated into experiments for checking whether these solutions are effective.

The results of the proposed experiments indicate that 2D barcode, Braille and the use of features are effective in VC authentication. Specifically, the use of 2D barcode and Braille is from the view of seeking assistance from other types of cryptography methods, while the use of visual and cryptographic features is investigated based on the analysis of VC shares for the VC identification.

While the ideal of combining barcode and VC shares can be attributed to many factors such as the similarity between their image structures and the usability of 2D barcode recognizing in real life, issues appear to be discussed in the areas of effectively embedding the 2D barcode into shares without affecting the visual effect of final secret revealing. On the basis of previous work of VC and the advantages of various barcodes, the author realized one improved method of expanding the flexibility of embedding 2D barcode into shares by introducing image matching techniques to search for corresponding regions with certain 2D barcode which will then be used to replace the regions in a share. Our main contribution is to search the embedding place of 2D barcodes in a share properly and minimize its visual effect on the revealed secret.

Another expectation for future work is that while in the context of basic VC scheme, the result of embedding 2D barcode appears to be an optimal solution for VC authentication, while the research of how to implement this in other types of VC schemes have not been taken consideration yet.

References

- Campbell, A. (2000). The designer's lexicon: the illustrated dictionary of design, printing, and computer terms. Chronicle Books.
- Amidror, I., & Amidror, I. (2000). The theory of the moiré phenomenon (No. LSP-BOOK-2000-001). Dordrecht; Boston: Kluwer Academic.
- Ateniese, G., Blundo, C., Santis, A.D., Stinson, D.R. (2001) Extended capabilities for visual cryptography. Theoretical Computer Science 250, 143-161
- B. V. Rompay. (2004) Analysis and Design of Cryptographic Hash functions, MAC algorithms and Block Ciphers. Ph.D. thesis, Electrical Engineering Department, Katholieke Universiteit, Leuven, Belgium.
- Blundo, C., De Bonis, A., & De Santis, A. (2001) Improved schemes for visual cryptography. Designs, Codes and Cryptography, 24(3), 255-278.
- Blundo, C., D'Arco, P., De Santis, A., & Stinson, D. R. (2003) Contrast optimal threshold visual cryptography schemes. SIAM Journal on Discrete Mathematics, 16(2), 224-261.
- Blundo, C., De Santis, A., & Stinson, D. R. (1999) On the contrast in visual cryptography schemes. Journal of Cryptology, 12(4), 261-289.
- Braudaway, G. W., Magerlein, K. A., & Mintzer, F. C. (1996) Protecting publicly available images with a visible image watermark. In Electronic Imaging: Science & Technology (pp. 126-133). International Society for Optics and Photonics.
- Ching-Nung, Y. A. N. G., & Tse-Shih, C. H. E. N. (2005) Size-adjustable visual secret sharing schemes. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 88(9), 2471-2474.
- Cimato, S., & Yang, C. N. (Eds.). (2011). Visual cryptography and secret image sharing. CRC Press.
- Cimato, S., De Prisco, R., & De Santis, A. (2005) Optimal colored threshold visual cryptography schemes. Designs, Codes and Cryptography, 35(3), 311-335.

- Cimato, S., De Prisco, R., & De Santis, A. (2007) Colored visual cryptography without color darkening. *Theoretical Computer Science*, 374(1), 261-276.
- Chen, Y. C., Horng, G., & Tsai, D. S. (2012). Comment on “cheating prevention in visual cryptography”. *Image Processing, IEEE Transactions on*, 21(7), 3319-3323.
- Chen, Y.-C., Tsai, D.-S., Horng, G. (2012) Cheating prevention in visual cryptography. *IEEE Transactions on Image Processing*, 21, 3319-3323
- Chen, Y.-C., Tsai, D.-S., Horng, G. (2012) A new authentication based cheating prevention scheme in Naor–Shamir’s5 visual cryptography. *Journal of Visual Communication and Image Representation* 23, 1225-1233
- Chen, S.-Q. (2010) A corner matching algorithm based on Harris operator. 2nd International Conference on Information Engineering and Computer Science (ICIECS), 2010, 1-2.
- Chen, Y.-F., Chan, Y.-K., Huang, C.-C., Tsai, M.-H., Chu, Y.-P. (2007) A multiple-level visual secret-sharing scheme without image size expansion. *Information Sciences* 177, 4696-4710
- Chourasia, J. (2013). Identification and authentication using visual cryptography based fingerprint watermarking over natural image. *CSI Transactions on ICT*, 1-6.
- C.N. Yang & C.S. Lai (1999) Some new types of visual secret sharing schemes, *Proceed. Nat. Compu. Sympo.* 3 260–268.
- C.N. Yang, T.S. Chen and M.H. Ching (2006) Embed additional private information into two-dimensional bar codes by the visual secret sharing scheme, *Integrated Computer-Aided Engineering*, Volume 13, Number 2, pp. 189-199.
- Corke, Peter. (2011) *Image Feature Extraction Robotics, Vision and Control*, Springer, 73, 335-379.
- Desmedt, Y., & Van Le, T. (2000) Moire cryptography. In *Proceedings of the 7th ACM conference on Computer and communications security*, 116-124
- Dobbertin, H. (1998) Cryptanalysis of MD4. *J. Cryptology* 11, 253-271

- De Bonis, A., & De Santis, A. (2004) Randomness in secret sharing and visual cryptography schemes. *Theoretical Computer Science*, 314(3), 351-374
- Goldberg, L. and Swan, L. (2011) A biosemiotic analysis of Braille, *Biosemiotics*, vol. 4, pp. 25-38.
- Gao, M., Sun, B. (2012) Blind watermark algorithm based on QR barcode. In: Wang, Y., Li, T. (eds.) *Foundations of Intelligent Systems*, vol. 122, pp. 457-462. Springer Berlin Heidelberg
- Hahn, H., Jung, J.: Improving performance of the decoder for two-dimensional barcode symbology PDF417. In: Braz, J., AraÚJo, H., Vieira, A., EncarnaÇÃO, B. (eds.)
- Hersch, R. D., & Chosson, S. (2004) Band moiré images. In *ACM Transactions on Graphics (TOG)*, 23(3), 239-247.
- Hu, C.M., Tzeng, W.G. (2007) Cheating prevention in visual cryptography. *IEEE Transactions on Image Processing* 16(1), 36-45
- Hegde, C., Manu, S., Shenoy, P., Venugopal, K., Patnaik, L. (2008) Secure authentication using image processing and visual cryptography for banking applications. In: *16th International Conference on Advanced Computing and Communications*, 65-72
- Hou, Y.-C. (2003) Visual cryptography for color images. *Pattern Recognition* 36, 1619-1629
- Horng, G., Chen, T., Tsai, D.-S. (2006) Cheating in visual cryptography. *Des Codes Crypt* 38, 219-236
- Hou, Y. C., Chang, C. Y., & Tu, S. F. (2001) Visual cryptography for color images based on halftone technology. *Image, Acoustic, Speech and Signal Processing*, part 2.
- Hofmeister, T., Krause, M., & Simon, H. U. (2000) Contrast-optimal k out of n secret sharing schemes in visual cryptography. *Theoretical Computer Science*, 240(2), 471-485.
- Indebetouw, G., & Czarnek, R. (1992) Selected papers on optical moiré and applications. *Society of Photo Optical*, 64.

- Jiang, F., Liu, Z., Feng, X. (2013) Research of Encodation Schemes Selecting Optimization for Character 2D Barcode. In: Yang, Y., Ma, M. (eds.) Proceedings of the 2nd International Conference on Green Communications and Networks 2012 (GCN 2012): Volume 1, vol. 223, pp. 615-623. Springer Berlin Heidelberg
- Jin, D., Yan, W. Q., & Kankanhalli, M. S. (2005) Progressive color visual cryptography. *Journal of Electronic Imaging*, 14(3).
- Kafri, O., & Glatt, I. (1990). The physics of moiré metrology (pp. 89-109). New York: Wiley.
- Kato, H., & Tan, K. T. (2005). 2D barcodes for mobile phones. In *Mobile Technology, Applications and Systems, 2005 2nd International Conference on* (pp. 8-pp). IEEE.
- Kuo, D., Wong, D., Gao, J., Chang, L. (2010) A 2D Barcode Validation System for Mobile Commerce. In: Bellavista, P., Chang, R.-S., Chao, H.-C., Lin, S.-F., Sloat, P.A. (eds.) *Advances in Grid and Pervasive Computing*, vol. 6104, pp. 150-161. Springer Berlin Heidelberg
- Krause, M., & Simon, H. U. (2003) Determining the optimal contrast for secret sharing schemes in visual cryptography. *Combinatorics Probability and Computing*, 12(3), 285-299.
- Koga, H. (2002) A general formula of the (t, n) -threshold visual secret sharing scheme. In *Advances in Cryptology—ASIACRYPT'02*, 328-345. Springer Berlin Heidelberg.
- Kuhlmann, C., & Simon, H. U. (2000) Construction of visual secret sharing schemes with almost optimal contrast. In *Proceedings of the eleventh annual ACM-SIAM symposium on Discrete algorithms*. Society for Industrial and Applied Mathematics, 263-272.
- Kuwakado, H., & Tanaka, H. (1999) Image size invariant visual cryptography. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, 82(10), 2172-2177.
- Lau, D.L. & Arce, G.R. (2011) *Modern digital halftoning*. CRC Press

- Lee, S. S., Na, J. C., Sohn, S. W., Park, C., Seo, D. H., & Kim, S. J. (2002) Visual cryptography based on an interferometric encryption technique. *ETRI journal*, 24(5), 373-380.
- Lee, Y.-S., Chen, T.-H. (2012) Insight into collusion attacks in random-grid-based visual secret sharing. *Signal Processing* 92, 727-736
- Liu, F., Wu, C., Lin, X. (2011) Cheating immune visual cryptography scheme. *IET Information Security* 5, 51-59
- Liu, F., Wu, C.K., Lin, X.J. (2008) Colour visual cryptography schemes. *Information Security, IET* 2, 151-165
- Memon, N., Wong, P.W. (1998) Protecting digital media content. *The Communications of the ACM*, 41, 35-43
- Metz, C. (1999). AAA protocols: authentication, authorization, and accounting for the Internet. *Internet Computing, IEEE*, 3(6), 75-79.
- Myodo, E., Sakazawa, S., Takishima, Y. (2006) Visual cryptography based on void-and-cluster halftoning technique. In *IEEE International Conference on Image Processing*, pp. 97-100.
- Myodo, E., Takagi, K., Miyaji, S., Takishima, Y. (2007) Halftone visual cryptography embedding a natural grayscale image based on error diffusion technique. In *IEEE International Conference on Multimedia and Expo*, pp. 2114-2117.
- Naor, M., & Shamir, A. (1995) Visual cryptography. In *Advances in Cryptology—EUROCRYPT'94* (pp. 1-12). Springer Berlin Heidelberg.
- Nakajima, M., Yamaguchi, Y. (2002) Extended Visual Cryptography fcommor Natural Images. In: *WSCG*, pp. 303-310.
- Naor, M., Pinkas, B. (1997) Visual Authentication and Identification. In: Kaliski Jr., B.S. (ed.) *CRYPTO 1997*. LNCS, vol. 1294, pp. 322–336. Springer, Heidelberg
- Niu, X., Huang, W. J., Wu, D., & Zhang, H. (2004). Information hiding technique based on 2D barcode. *Acta Scientiarum Naturalium Universitatis Sunyatseni*, 43, 21-25

- Revenkar, P.S., Anjum, A., Gandhare, W.Z. (2010) Survey of VC Schemes. *International Journal of Security & Its Applications* 4, 49-56
- Rouillard, J. (2008) Contextual QR codes. In *The Third International Multi- Conference on Computing in the Global Information Technology*, July 27-August 1, pp. 50–55
- Rijmen, V., & Preneel, B. (1996) Efficient colour visual encryption, *EUROCRYPT'96*.
- Shyu, S.J., Huang, S.-Y., Lee, Y.-K., Wang, R.-Z., Chen, K. (2007) Sharing multiple secrets in VC. *Pattern Recognition* 40, 3633-3651
- Solms, S.H., Solms, R. (2009) *Information Technology Governance. Information Security Governance*, Springer, 1-7.
- Sobti, R., Geetha, G. (2012) Cryptographic Hash Functions: A Review. *IJCSI International Journal of Computer Science*, 9, 461-479
- Stoleru, D. (2005) Extended Visual Cryptography Schemes. *Dr. Dobb's Journal* 30, 36-39
- Sheng-Yang, Liao, & Tian-Qiang, Huang. (2013) Video copy-move forgery detection and localization based on Tamura texture features. In *6th International Congress on Image and Signal Processing (CISP)*
- Shamir, A. (1979) How to share a secret. *Communications of the ACM*, 22, 11, 612-613.
- Shyu, S. J., Huang, S. Y., Lee, Y. K., Wang, R. Z., & Chen, K. (2007) Sharing multiple secrets in visual cryptography. *Pattern Recognition*, 40(12), 3633-3651.
- Stallings, W. (2013) Inside SHA-3. *Potentials, IEEE*, 32(6), 26-31. doi: 10.1109/MPOT.2013.2254508
- Tamura, Hideyuki, Mori, Shunji, & Yamawaki, Takashi. (1978) Textural Features Corresponding to Visual Perception. *IEEE Transactions on Systems, Man and Cybernetics*, 8(6), 460-473. doi: 10.1109/TSMC.1978.4309999
- Touch, J.D. (1995) Performance analysis of MD5. *SIGCOMM Comput. Commun. Rev.* 25, 77-86

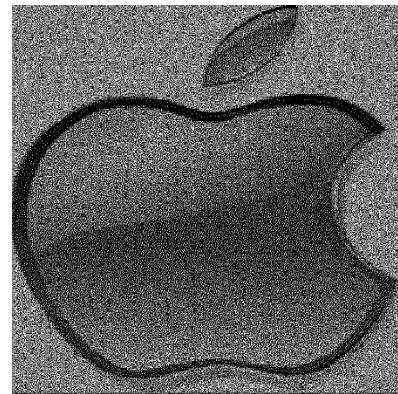
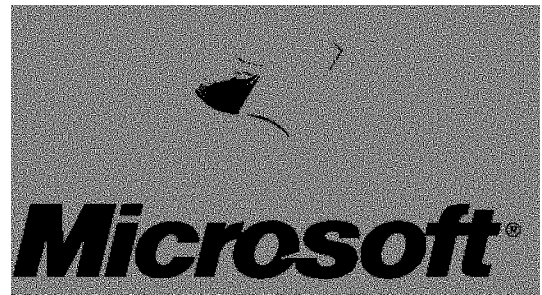
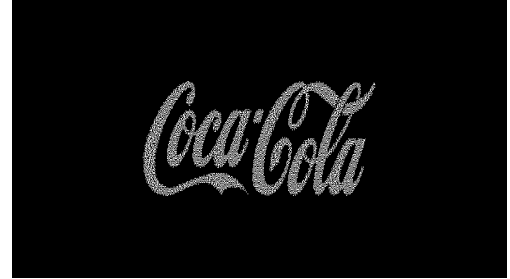
- Tuyls, P., Hollmann, H. D., Van Lint, J. H., & Tolhuizen, L. M. G. M. (2005) XOR-based visual cryptography schemes. *Designs, Codes and Cryptography*, 37(1), 169-186
- Tuyls, P., Hollmann, H. D., Lint, J., & Tolhuizen, L. (2002) A polarisation based visual crypto system and its secret sharing schemes.
- Van Schyndel, R. G., Tirkel, A. Z., & Osborne, C. F. (1994) A digital watermark. In *IEEE International Conference on Image Processing*, Vol. 2, pp. 86-90.
- Veltkamp, R. C. (2001) Shape matching: similarity measures and algorithms. *International Conference on Shape Modeling and Applications*, SMI 2001.
- Vincent, E., Laganière, R.(2005) Detecting and matching feature points. *Journal of Visual Communication and Image Representation* 16, 38-54
- Wang, D., Yi, F., Li, X. (2009) On general construction for extended visual cryptography schemes. *Pattern Recognition* 42, 3071-3082
- Wang, Z., Arce, G.R. (2006) Halftone visual cryptography through error diffusion. In: *IEEE International Conference on Image Processing*, pp. 109-112.
- Weir, J., Yan, W. (2010). A comprehensive study of VC. In: Shi, Y. (ed.) *Transactions on Data Hiding and Multimedia Security V*, 6010, 70-105. Springer Berlin Heidelberg
- Weir, J., Yan, W.-Q. (2009) Dot-Size Variant VC. In: *IWDW 2009. LNCS*, 5703, 136–148. Springer, Heidelberg
- Weir, J., Yan, W. (2010) A comprehensive study of VC. In *Transactions on Data Hiding and Multimedia Security V*, 6010, 70-105. Springer Berlin Heidelberg
- Weir, J., Yan, W. (2012) Authenticating VC shares using 2D Barcodes. In: Shi, Y., Kim, H.-J., Perez-Gonzalez, F. (eds.) *Digital Forensics and Watermarking*, 7128, 196-210. Springer Berlin Heidelberg
- Weir, J., Yan, W., (2009) Sharing multiple secrets using VC. In *ISCAS 2009*, 509-512.

- Weir, J., Yan, W., & Kankanhalli, M. S. (2012) Image hatching for visual cryptography. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMCCAP)*, 8(2S), 32.
- Weir, J. P., & Yan, W. (2012) *Visual cryptography and its applications*, Bookboon.
- Wong, P. W. (1998). A watermark for image integrity and ownership verification. In *IS & TS Pics Conference*, pp. 374-379.
- Wu, C. C., & Chen, L. H. (1998) A study on visual cryptography. Master's thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, ROC.
- Wu, H. C., & Chang, C. C. (2005) Sharing visual multi-secrets using circle shares. *Computer Standards & Interfaces*, 28(1), 123-135.
- Yang, C. N. (2004) New visual secret sharing schemes using probabilistic method. *Pattern Recognition Letters*, 25(4), 481-494.
- Yang, C. N., & Chen, T. S. (2005) Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion. *Pattern Recognition Letters*, 26(2), 193-206.
- Yang, C. N., & Chen, T. S. (2006) Reduce shadow size in aspect ratio invariant visual secret sharing schemes using a square block-wise operation. *Pattern Recognition*, 39(7), 1300-1314.
- Yang, C. N., Chen, T. S., & Ching, M. H. (2006). Embed additional private information into two-dimensional bar codes by the visual secret sharing scheme. *Integrated Computer-Aided Engineering*, 13(2), 189-199.
- Yan, W. Q., Jin, D., & Kankanhalli, M. S. (2004) Visual cryptography for print and scan applications. In *IEEE, ISCAS'04*, pp.572
- Yan, Y., Li, Q., Cao, M., Chen, H., Xue, J. (2013) Application Research of Two-Dimensional Barcode in Information Construction of Colleges. In *International Conference on Information Technology and Software Engineering*, vol. 212, pp. 71-80. Springer Berlin Heidelberg

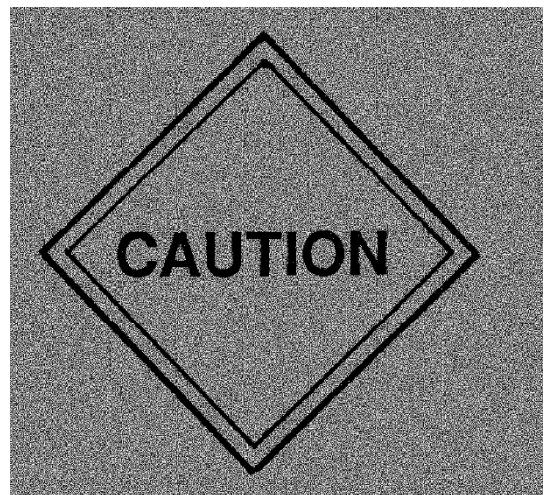
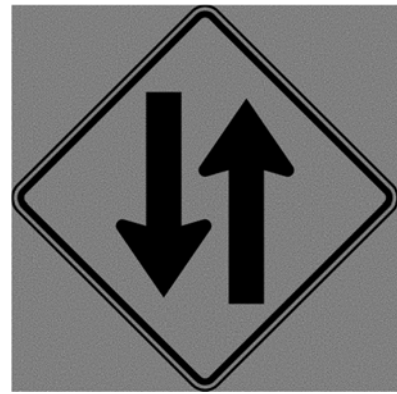
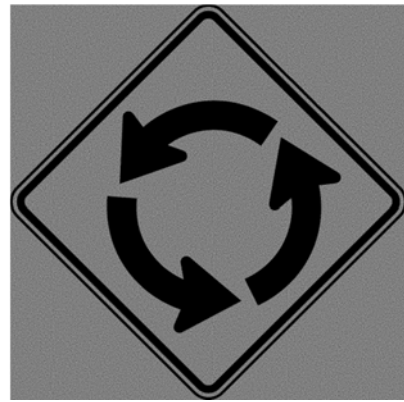
- Yang, C., Lai, C. (1999) Some new types of visual secret sharing schemes. In: National Computer Symposium (NCS 1999), vol. III, pp. 260–268
- Yang, C.-N., Chen, T.-S., Ching, M.-H. (2006) Embed additional private information into two-dimensional bar codes by the visual secret sharing scheme. *Integrated Computer-Aided Engineering* 13, 189-199
- Yunsheng, Zhong. (2013) Secure Digital Certificate Design Based on the RSA Algorithm. *Journal of Digital Information Management*, 11(6), 423-429.
- Yin, J., Wang, L., Li, J.(2010) The research on paper-mediated Braille automatic recognition method, the Fifth International Conference on Frontier of Computer Science and Technology (FCST), pp. 619-624.
- Zhang, C., Ma, L., Mao, D. (2011) A 2D Barcode Recognition System Based on Image Processing. In: Zhu, M. (ed.) *Electrical Engineering and Control*, vol. 98, pp. 683-688. Springer Berlin Heidelberg
- Zhou, Z., Arce, G.R., Di Crescenzo, G. (2003) Halftone visual cryptography. In *ICIP 2003*, pp. I-521-524 vol.521.

Appendix. Standard Testbed for VC Experiments

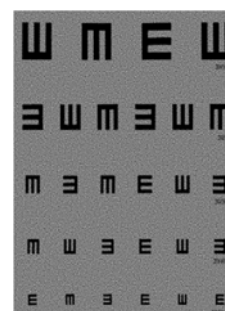
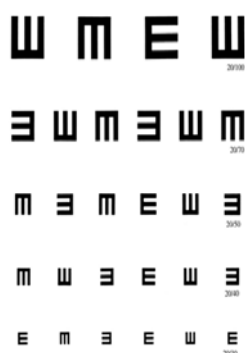
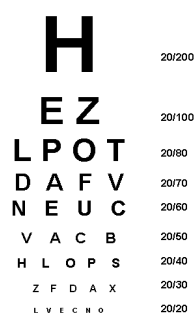
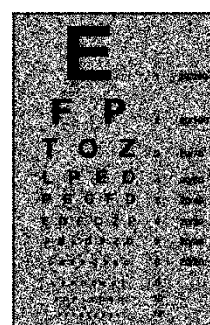
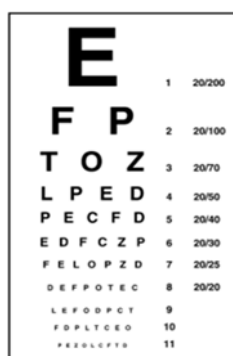
A. Logo



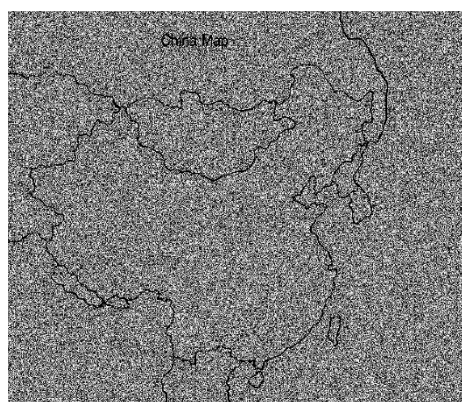
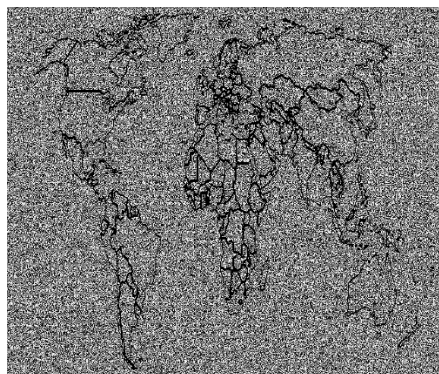
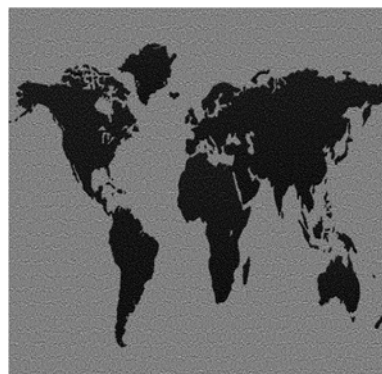
B. Traffic Signs



C. Visual Charts



D. Maps



E. Television Test Cards

