 ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

A Secured Visual Cryptography Mechanism

[1]P B Siva Varma, [2]V V Siva Rama Raju, [3]K R S Ramaraju, [4]T V K P Prasad
[1,4]Dept. of CSE, S.R.K.R Engg. College, Affiliated to Andhra University, Bhimavaram, AP, India

Abstract
To prevent the confidential information from being disclosed, one needs to apply some techniques to protect it. Visual cryptography scheme is a secret sharing technique used for encrypting binary images. It splits a binary image into n shares, and gathering more than k shares can recover the secret. The remarkable feature of a visual cryptography scheme is that the decoding process is done by human eyes. A conventional visual cryptography scheme encodes a pixel on the secret image into m subpixels. This gives a study of the cheating problem in visual cryptography and extended visual cryptography schemes. This dissertation reviews the attacks of malicious adversaries who may deviate from the scheme in any way and presents three cheating methods and applied them on attacking existent visual cryptography or extended visual cryptography schemes. This dissertation proposed a generic method that converts a visual cryptography scheme to another visual cryptography scheme that has the property of cheating prevention. The overhead of the conversion is near optimal in both contrast degression and pixel expansion.

Keywords
Cryptography, Encryption, Decryption, Visual Cryptography;

I. Introduction

A. Visual Cryptography

To prevent the content of confidential information from being disclosed, one has to do some process to protect it via some method. There are many kinds of techniques to protect confidential information. Cryptography is a technique to encode the secret message through a complex algorithm and a private key. Without the appropriate key, the cipher message is hard to be recovered. While cryptography attempts to scramble the content, steganography tends to conceal the secret message into innocuous carriers to cheat eavesdroppers. Information with disordered content is highly possible to attract eavesdropper's interests, but an innocuous carrier may be ignored. Hence the inside secret will not be intercepted. While cryptography and steganography generate only one copy of the cipher message, secret sharing splits the secret message into many shares, each of which is hold by one participant [1-2].

According to the processes and consequences of each technique discussed above, we know that no single technique is applicable everywhere. Therefore, it is not uncommon to design a protection scheme compounded of several techniques. Furthermore, the features of each kind of digital information, such as text, images, audio, etc. are different. Those different features are usually worth utilizing for the design of the protection scheme. Besides, which technique should be used sometimes depends on occasions. Due to all kinds of reasons above, we know that the design of protection scheme for digital information is not a simple task [3-5].

A very interesting and simple cryptographic method was introduced by Naor and Shamir [6] named as visual cryptography to protect secrets. Basically, visual cryptography has two important features. The first feature is its perfect secrecy, and the second feature is its decryption method which requires neither complex decryption algorithms nor the aid of computers. It uses only human visual system to identify the secret from the stacked image of some authorized shares. Therefore, visual cryptography is a very convenient way to protect secrets while computers or other decryption devices are not available.

Actually visual cryptography is came as a solution of a problem described [7] below. "Suppose four intelligent thieves have deposited their loot in a Swiss bank account. These thieves obviously do not trust each other. In particular, they do not want a single member of themselves to withdraw the money and fled. However, they assume that withdrawing money by two members of the group is not considered a conspiracy; rather it is considered to have received 'authorizations'. Therefore, they decided to encode the bank code (with a trusted computer) into four partitions so that any two or more partitions can be used to reconstruct the code. Since the thieves' representatives will not have a computer with them to decode the bank code when they come to withdraw the money, they want to be able to decode visually: each thief gets a transparency. The transparency should yield no information about the bank code (even implicitly). However, by taking any two transparencies, stacking them together and aligning them, the secret number should 'pop out'".

The simplest version of the visual secret sharing method assumes that the image to be encrypted consists of a collection of black and white pixels and each pixel is handled separately. It divides an image into several encrypted slides under its encryption rule. This basic model can be extended into the case of (k, n)-threshold visual cryptography schemes, in which the secret image is visible if any k or more transparencies are stacked together. Thus, the framework can use any of n!/(k!(n−k)!) possible combinations of k shares to recover the secret message. After Noar and Shamir [6] proposal of a (k, n)-VCS many improvements and extensions are done [8-13]. Most of the previous works on visual cryptography focused on improving two parameters. One is pixel expansion and another one is contrast [11-13].

Visual cryptographic solutions operate on binary or binarized inputs. Therefore, natural (continuous-tone) images must be first converted into halftone images to simulate the original gray or color levels in the target binary representation. Halftoning is a process to convert gray images into binary images. Generally every one use an integer value between 0 and 255 to represent a pixel value in a gray image, where 0 represents a pure white and 255 a darkest black, and use 0 and 1 to represent an uninked (white) pixel and an inked (black) pixel in a halftone image, respectively. With halftoning, an image is produced with a series of dots printed on the paper. If the dots are small enough, the eye cannot detect individual dot patterns. Instead it integrates halftone dots and unprinted areas as varying shades. The varying intensities of the black dots produce a simulation of a continuous-tone image. Then, the halftone version of the input image is used instead of the original secret image to produce the shares. Few years later, Verheul and Tilborg [10] developed a scheme that can be applied on colored images as shown in fig. 1.

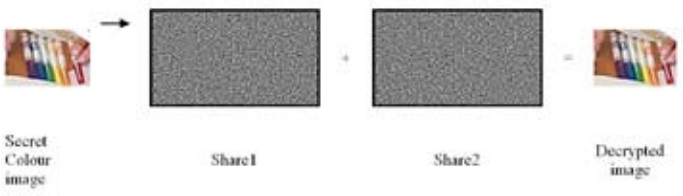

Fig. 1: Visual Cryptography for Color Images

B. Extended Visual Cryptography

A visual cryptography scheme with some extended characteristic is called extended visual cryptography scheme (EVCS) [6]. An EVCS is like a VCS except that each share displays a meaningful image, which will be called share image. Different shares may have different share images.

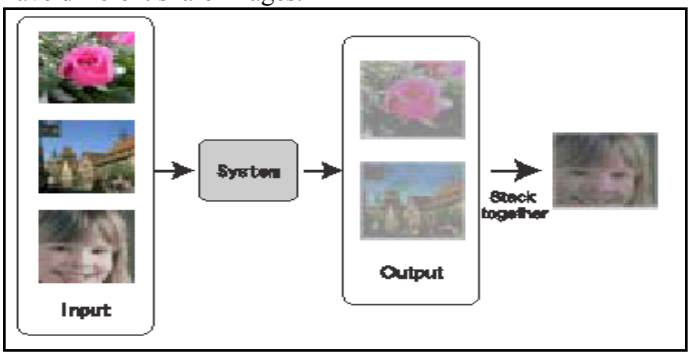

Fig. 2: Extended Visual Cryptography

As shown in fig. 6, our visual cryptography system takes three pictures as an input and generates two images which correspond to two of the three input pictures. The third picture is reconstructed by printing the two output images onto transparencies and stacking them together. This type of visual cryptography, which reconstructs the image by stacking some meaningful images together, is especially called Extended Visual Cryptography

C. Applications of Visual Cryptography

Visual Cryptography Schemes can decode concealed images based purely on human visual systems, without any aid from cryptographic computation. This nice property gives birth to a wide range of encryption applications [7].

1. Electronic-Balloting System

Nowadays, most of the voting are managed with computer systems. These voting machines expected voters to trust them, without giving proof that they recorded each vote correctly. To solve this dilemma, Chaum [14] proposed a secret-Ballot Receipts system that is based on (2, 2)-threshold binary VCS. It generates an encrypted receipt to every voter which allows her to verify the election outcome - even if all election computers and records were compromised.

2. Encrypting Financial Documents

The VCS principle can also be applied in transmitting confidential financial documents over Internet. VCRYPT is an example of this type of system being proposed by A. Yasinsac, W. Hawkes et al. [5]. VCRYPT can encode the original drawing document with a specified (k, n) - VCS, then send each of the encoded n shares separately through Emails or FTP to the recipient. The decoding only requires bitwise "OR" operation on all shares in the specified directory, and needs no extra effort of cryptographic computation. Financial documents often contain a lot of digits. Therefore, after applying VCS, we will expect that the greying effect will prevent us from recognizing the "fuzzy" digits in decoded documents. To work around this problem, VCRYPT proposed a post filtering process to return the decoded image precisely to its original form. It evaluates every set of m sub-pixels against the encoding threshold and displays the final pixel as black if the number of black sub-pixels is above the threshold and white otherwise.

3. Other Applications

Along with these applications, there are some applications utilizing visual cryptography, such as authentication, human identification, watermarking, mobile ticket validation, electronic cash, visual signature checking, computer generated hologram, etc.

III. Background

A. Mathematical Representation

In the visual cryptography scheme, the secret image consists of collection of black and white pixels and each pixel is subdivided into a collection of black and white sub-pixels in each of the n-shares. The collection of sub-pixels can be represented by nxm boolean matrix S=[Sij], where rows a row for each share ,a column for each sub pixel. Sij=1 if and only if the j-th subpixel of i-th share is black. The grayness of the stack of k shares determined by the Hamming weight of the OR of the corresponding k rows.
Mathematically visual cryptography can be defined as fallows. Let P= $\{P_1, P_2, P_3,\ldots, P_n\}$be the set of n participants. Each Pi holds a share Si, $1\le i\le n$. A set $X\subseteq P$ is called a qualified set if the stacking of the shares of the participants in X reveals the secret image. A set $Y\subseteq P$ is called a forbidden set if the stacking of their shares reveals no information about the secret image. $\Gamma=(P,Q,F)$ is an access structure if $Q\cap F=\varnothing$ and $Q\cup F=2P$. The access structure $\Gamma=(P,Q,F)$ for (k, n)-secret sharing is that $X\in Q$ if and only if $|X|\ge k$, where |X| is the number of participants in X. In (Γ,m)-VCS, the value m is called pixel expansion, which is the number of subpixels that each pixel of the secret image is encoded into in each share.

B. Cheating Process in Visual Cryptography

Visual cryptography assumes all participants, who hold shares are semi-honest, that is, they will not present false or fake shares during the phase of recovering the secret image.

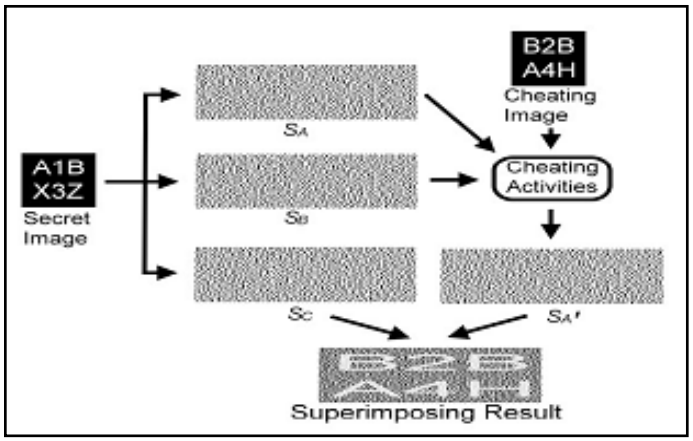

Fig. 3: Cheating Process in Visual Cryptography

Thus, the image shown on the stacking of shares is considered as the real secret image. Nevertheless, cryptography is supposed to guarantee security even under the attack of malicious adversaries

who may deviate from the scheme in any way. But it is possible to cheat [15,16], a visual cryptography scheme though it seems hard to imagine. Horng et al. [17] proposed that cheating is possible in (k,n)-visual cryptography scheme when k is smaller than n. The key point of cheating is how to predict and rearrange the positions of black and white subpixels in the victim's and cheater's share. For cheating, a cheater presents some fake shares, illustrated in fig. 3, such that the stacking of fake and genuine shares together reveals a fake image.

C. Types of Cheaters in Visual Cryptography

There are two types of cheaters in visual cryptography. One is a malicious participant (MP) who is also called as a legitimate participant, and the other is a malicious outsider (MO), where. In this, we show that not only a malicious participant can cheat, but also a malicious outsider can cheat under some circumstances.

D. Phases in Developing Fake Shares

A cheating process against a VCS consists two phases that are stated as fallows:

1. Fake share construction phase: the cheater generates the fake shares
2. Image reconstruction phase: the fake image appears on the stacking of genuine shares and fake shares.

In order to cheat successfully, honest participants who present their shares for recovering the secret image should not be able to distinguish fake shares from genuine shares.

Cheating Methods in Visual Cryptography

E. Cheating a VCS by Malicious Participants

Without loss of generality, assume P1 is cheater .He uses his genuine share as template to construct a set of fake shares with white pixel as in original share and for each black pixel randomly assigns white and black subpixels. These shares are indistinguishable from its genuine share. The stacking of these fake shares and other shares reveals the fake image.

F. Cheating a VCS by Malicious Outsider

In this type of cheating technique malicious outsider can cheat without any genuine shares at hand. It uses optimal (2,2)-visual cryptography scheme to construct the fake shares for the fake image. After then tunes the size of fake shares so that he can be stacked with genuine shares.

G. Cheating an EVCS by Malicious Participant

In this type of cheating technique the malicious participant uses the fake shares to reduce the contrast between the share images and the background. Simultaneously, the fake image in stacking of fake shares has enough contrast against the background.

IV. Objectives

The success of the application depends upon meeting the following core set of objectives

- Any cheating activities should not deviate the scheme in any way.
- A cheat-preventing method should be applicable to any visual cryptography scheme.
- The increase to pixel expansion should be as small as possible.
- The contrast of the secret image in the stacking of shares is not reduced significantly in order to keep the quality of visual cryptography.

Present the first cheat-preventing method of Yang and Laih needs a trusted authority to hold the special verification share for detecting fake shares. It generates (n+1) shares VS,S1,S2,…Sn, where VS is the verification share. If VS+Si shows the verification image that is known to all participants, the share Si is genuine. In the cheat-preventing method of Horng et al. [15], each participant Pi has a verification share Vi. The share's Si s are generated as usual. Each Vi is divided into (n-1) regions Ri,j, $1 \le j \le n$, $j \ne i$. Each region Ri,j of Vi is designated for verifying share Sj. The region Ri,j of Vi+Sj shall reveal the verification image for Pi verifying the share Sj of Pj. The verification image in Ri,j is constructed by a (2,2)-visual cryptography scheme. The second cheat-preventing method of Yang and Laih is a transformation of a (Γ,m)-visual cryptography scheme (but not a(2,n) –visual cryptography scheme) to another cheat-preventing (Γ,m+n(n-1))visual cryptography scheme. The stacking of any two shares reveals the verification image.

A. Drawbacks

Our attack on the first cheat-preventing method of Yang and Laih, involves two malicious participants. Without loss of generality, we assume that they are P1 and P2. P1 and P2 together constructs a fake share FS such that FS+VS reveals the verification image and FS cheats other participants.

In their attack on Horng et al.'s Cheat-Preventing Methods, without loss of generality assume that P1 knows the regions of the verification share Vi. P1 generates a fake share FS1 to cheat as follows. The pixels of FS1 in the region Ri,1 are the same as those in S1. The rest pixels of FS1 (outside the region Ri,1) are constructed by first cheating technique (stated above by malicious participant). As a result, the correct verification image appears on the region Ri,1 of FS1+Vi and Pi believes that FS1 is a genuine share. By first cheating technique (stated above by malicious participant), the stacking of FS1 and other genuine shares reveals a reasonable fake image. Moreover, even the cheater does not know the verification region assigned to a participant, the attack is still possible. Since the verification share is divided into (n-1) regions, each verification region is small for a fairly large n. We choose a simple fake image. The probability that no overlapping between the fake image and the region Ri,1 occurs is high. By setting the background pixels in FS1 from S1, FS1+Vi shows the verification image in the verification region Ri,1 of Vi .

Even though the improved Yang and Laih's cheat-preventing Method is somewhat better cheating-method when compared to first two cheating-prevention mechanisms. The only drawback of this method is construction of verification image by adding extra n(n-1) subpixels to each pixel of original picture, which is over head to construction of verification images.

In this paper, our conversion generates two shares for each participant. One is the secret share and the other is the verification share. i.e., for each participant Pi, it generates a verification share Vi, for a chosen verification image. If participant Pi, wants to verify the share Sj of participant Pj , he checks whether Vi+Sj shows his verification image or not. If Vi+Sj shows his verification image then Sj is not fake share. Otherwise Sj can be considered as fake share.

Each participant has his own private verification image, which is not known to other participants. Since the first two subpixels [1 0] of all shares are the same, a participant Pi, even with all shares cannot know the positions of black pixels of the verification image of participant Pj, $j \ne i$. Therefore Pi, cannot produce a fake share FSi such that Fsi+Vj shows the verification image of Pj. Participant Pi cannot cheat participant Pj for $i \ne j$. Furthermore,

we see that collaboration of some participants cannot succeed to cheat, either.

IV. System Architecture

System Architecture describes "the overall structure of the system and the ways in which that structure provides conceptual integrity".

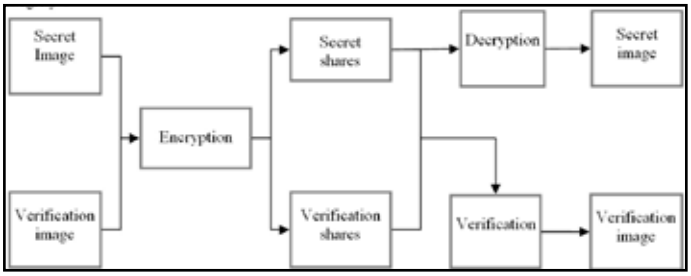

Fig. 4: Architecture of System

Architecture is the hierarchical structure of a program components (modules), the manner in which these components interact and the structure of data that are used by that components. Architecture of the secured visual cryptography mechanism is as follows in the below diagram. It consists of three modules: encryption, decryption and verification. Visual cryptography encrypts secret image and verification image to generate secret shares and verification shares respectively. After generation of secret and verification shares, secret shares are validated by using verification shares. If they are successfully validated, then only decryption of secret shares can be done. Otherwise secret shares are assumed as corrupted. It is shown in fig. 4.

V. Implementaion

A. Overview of Software used

This application is developed and executed with the J2SDK1.4.0 handling the J2SE java part with User interface Swing component. Java is robust, object oriented, multi-threaded, distributed and secure and platform independent language. It has wide variety of package to implement our requirement and number of classes and methods can be utilized for programming purpose. These features make the programmer's to implement to require concept and algorithm very easier way in Java.

Working Procedure This mainly contains three modules the are encryption, decryption and verification

B. Module 1: Encryption

Visual cryptography encrypts the secret image into several transparencies called shares. While in verification module we need verification shares along with secret shares for verification. For that we have to select a verification image and encrypt it also. This system splits the secret and verification images into two pairs of shares.

C. Module 2: Decryption

In Decryption module visual cryptography stacks the secret shares on one another. For this we need secret shares generated at encryption module. As visual cryptography splits a white pixel of original image into several subpixels, of black and white colours, the resulting decrypted secret image is somewhat less contrast than the real secret image. We can directly saw the decrypted image without any computations.

D. Module 3: Verification

Before decryption module the shares may be corrupted by miscellaneous adversaries. Hence this system proposes a new method for verification. In this verification part we select a secret share and verification shares of different users and decrypt them. If the resulting image is the verification image corresponding to verification share, then we can conclude that the selected image is not corrupted by any one. Otherwise we can conclude the secret share is modified by someone.

Description of classes

E. Encoding Proposed Class

This class describes GUI in the encryption process of the visual cryptography and the functions are

openSecretPath(): This function is used to select the secret image

openVerifyPath(): This function is used to select the verification image.

F. Decoding Proposed Class

This class describes the GUI in the decryption process of visual cryptography. Functions defined here are

actionPerformed(): The actions to be performed by the user of the system are defined in this class. They are selecting secret shares, selecting verification shares, verify the secret shares, and decrypting the secret shares.

displayResult(): This function displays the result after the verification process in the form of text messages.

G. VisCrypt Proposed Class

This class describes the encryption and decryption scenarios. The functions are

encode(): This function performs the encoding scenarios by taking the image as an argument

decode(): This function describes the decoding scenario of visual cryptography.

H. Globals class

This class is just like a supported class for both encryption and decryption. The functions in this class are

findRandom(): This function used to split the a pixel into subpixels randomly.

displayPGM(): This function used to display the image to the user.

I. PGM class

This class is a supported class to set and get properties of the pgm image. Functions in this class are

readimage(): This function is used read the pgm file

writeimage(): This function is used to write a file in pgm format

writeimageAs(): This function is used to write pgm file in a specific path.

VI. Test Cases

A. Test Case 1(It is shown in Fig. 5)

Summary: If wont select any verification or secret shares then we will get an error message

Initial Condition: Not selecting any secret shares and verification shares.

Steps to run: click verify button without selecting any shares

Expected Output: Message showing error

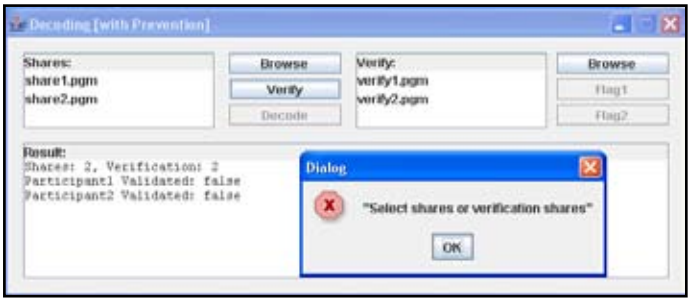

Fig. 5: Message Box Showing Error

B. Test Case 2: (It is shown in Fig. 6)

Summary: If we select wrong verification share for a secret share then we have to get an error message in command prompt.
Initial Condition: Secret shares and verification shares.
Steps to run: Select one fake share, one verification share and click verify button
Expected Output: Message displaying error.

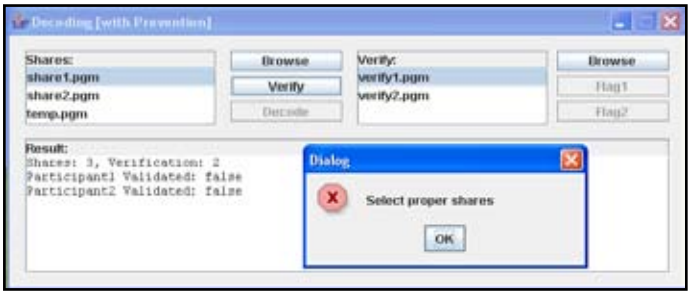

Fig. 6: Message Box Showing Error

C. Test Case 3: (It is shown in Fig. 7)

Summary: Selecting a fake share in verification then we will get an error message
Initial Condition: Secret shares and verification shares along with at least one fake share.
Steps to run: Select one fake share, one verification share and click verify button
Expected Output: Message showing error.

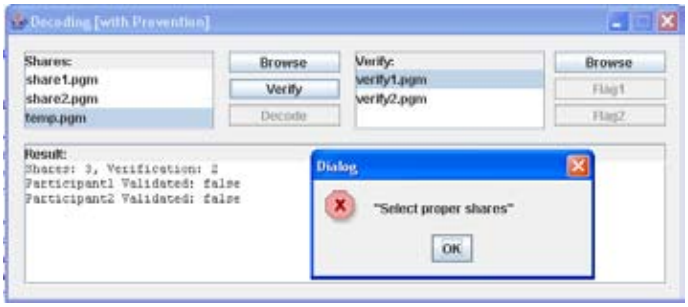

Fig. 7: Message Box Showing Error

VII. Summary of Contribution

This treatise contains a study on the cheating problem in visual cryptography and extended visual cryptography schemes. It includes three cheating methods. These attacks are to reveal fake images to cheat honest participants. These attacks are more like the man-in-the-middle attack in cryptography, and are very general for all kinds of visual cryptography schemes without cheating-prevention mechanism.
This has a general method that converts a visual cryptography scheme to another visual cryptography scheme that has a property of cheating prevention (also called cheat-preventing visual cryptography scheme). The overhead of the conversion is near optimal. The contribution is summarized as follows.

1. This paper includes three cheating methods against visual cryptography scheme and extended visual cryptography schemes. The first two methods are applied to attack visual cryptography schemes and the third one is applied to attack extended visual cryptography schemes. These three methods are easy to implement and satisfy the cheating definition for cheating traditional secret sharing schemes.
2. This reviews some previously proposed cheat-preventing visual cryptography or extended visual cryptography schemes and demonstrate that those schemes are either not robust enough (still cheatable) or improvable.
3. This proposes some necessary criteria for a VCS to be secure against cheating robustly. By these criteria, we propose a generic method that converts any VCS to another VCS with the property of cheating prevention. Our conversion is very efficient and incurs little overhead compared with the original VCS. The digression in contrast of the converted VCS is almost optimal. For each pixel of the secret image, we add two additional subpixels to the encoded subpixels only, no matter how many the encoded subpixels are.

VIII. Conclusion

This paper involves three cheating methods against visual cryptography scheme and extended visual cryptography scheme. This work examines previous cheat-preventing schemes and found that they are either not robust enough or still improvable. This contains an improved cheat-preventing scheme. By considering the attacks on visual cryptography, this theory gives essential principles for a robust cheat-preventing visual cryptography scheme. This includes an efficient transformation of visual cryptography scheme for cheating prevention. Our transformation incurs minimum overhead on contrast and pixel expansion. It only added two subpixels for each pixel in the image and the contrast is reduced only slightly.

A. Future Research

Even though the work gives more security from attacking, there are some problems left unsolved. Some of them are limitations in this research and some of them can be issues for future work:

1. The construction of the proposed visual cryptography scheme depends on the conventional visual cryptography scheme, i.e. the two basis matrices. Hence the basis matrices have much influence on recovered images. Therefore, we may try to construct basis matrices with better less pixel expansion.
2. The original is a clear one, but the stacked image generated by the visual cryptography scheme is somewhat less contrast than the original grey-scale image.
3. Here this makes use of dithering process, which generates halftone images. We may investigate whether this dithering technique may make any difference on the visual effect of the stacked image.
4. The participants may change the way of stacking shares to recover different secrets.

References

[1] E. R. Verheul, H. C. A. Van Tilborg,"Constructions and properties of k out of n visual secret sharing schemes", Designs, Codes, Cryptog, Vol. 11, No. 2, pp. 179–196, 1997.
[2] D. Q. Viet, K. Kurosawa,"Almost ideal contrast visual

cryptography with reversing", in Proc, Topics in Cryptology, 2004, Vol. 2964, LNCS, pp. 353–365.
[3] C.-N. Yang,"New visual secret sharing schemes using probabilistic method", Pattern Recognit. Lett., Vol. 25, No. 4, pp. 481–494, 2004.
[4] C.-N. Yang, C.-S. Laih,"Some new types of visual secret sharing schemes", in Proc. Nat. Computer Symp., 1999, Vol. 3, pp. 260–268.
[5] A. Yasinsac, W. Hawkes, C. Cline,"An Application of Visual Cryptography to Financial Documents", technical report TR001001, Florida State University, 2000.
[6] M. Naor, A. Shamir,"Visual cryptography", in Proc. Advances in Cryptology, 1994, Vol. 950, LNCS, pp. 1–12.
[7] Jim Cai (2004),"A Short Survey on Visual Cryptography Schemes", [Online] Available: http://www.cs.toronto.edu/jcai/paper.pdf.
[8] G. Ateniese, C. Blundo, A. De Santis, D. R. Stinson,"Visual cryptography for general access structures", Inf. Comput., Vol. 129, No. 2, pp. 86–106, 1996.
[9] I.Biehl, S.Wetzel,"Traceable visual cryptography", in Proc. 1st Int.Conf. Information Communication Security, 1997, Vol. 1334, LNCS, pp. 61–71.
[10] C. Blundo, A. De Santis,"Visual cryptography schemes with perfect reconstructions of black pixels", Comput. Graph., Vol. 22, No. 4, pp. 449–455, 1998.
[11] C. Blundo, A. De Santis, D. R. Stinson,"On the contrast in visual cryptography schemes", J. Cryptol., Vol. 12, No. 4, pp. 261–289, 1999.
[12] C. Blundo, P. D'Arco, A. De Santis, D. R. Stinson,"Contrast optimalthreshold visual cryptography schemes", SIAM J. Discrete Math., Vol. 16, No. 2, pp. 224–261, 2003
[13] E. F. Brickell, D. R. Stinson,"The detection of cheaters in threshold schemes", SIAM J. Discrete Math., Vol. 4, No. 4, pp. 502–510, 1991.
[14] D Chaurn,"Secret-ballot receipts: True voter-verifiable elections", IEEE Security and Privacy, 2004, pp. 38-47.
[15] Z. Gan, H.Yan, K. Chen,"Acheater detectable visual cryptography scheme", (in Chinese) J. Shanghai Jiaotong Univ., Vol. 38, No. 1, 2004.
[16] T. Hofmeister, M. Krause, H.-U. Simon,"Contrast-optimal k out of n secret sharing schemes in visual cryptography", Theoret. Comput. Sci., Vol. 240, No. 2, pp. 471–485, 2000.
[17] G.-B. Horng, T.-G. Chen, D.-S. Tsai,"Cheating in visual cryptography," Designs, Codes, Cryptog., Vol. 38, No. 2, pp. 219–236, 2006.