Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 5, Issue. 2, February 2016, pg.150 – 153

SECRET IMAGE SHARING SCHEMES: A REVIEW

Ms. Sejal V. Gawande[1], Dr. Prashant R. Deshmukh[2]
[1]Student, Computer Science and Engineering, Sipna C.O.E.T., Amravati, Maharashtra, India

[1] gawandesejal@gmail.com; [2] pr_deshmukh@yahoo.com

Abstract*— In this paper, we emphasize on the study concerning various secret sharing schemes. To provide security for sharing information, various techniques proposed for the visual cryptography. Visual cryptography is a technique that encrypts a secret image into n shares with each participant holding one or more shares. Conventional visual secret sharing scheme hide secret images in shares that are either printed or in digital form. Meaningful images or noise like pixels appears due to hiding secret image in shares. In this paper we provide a review of various techniques used for visual cryptography. We will discuss various visual cryptography techniques like Halftone Visual Cryptography Scheme, Multiple Secret Sharing Scheme, Extended Visual Cryptography Scheme, Visual secret sharing, Natural Image Based Visual Secret Sharing etc.

***Keywords*— Information security, Secret sharing scheme, Visual Cryptography, Data hiding, Natural images**

I. INTRODUCTION

Nowadays, information gets more value when shared with others. Due to internet, it is possible to share information like audio, video, images easily .There are security related issues. Hacker’s access unauthorized data. Various techniques can be used to solve this problem. Today, in computer-aided environment sharing visual secrets images has becomes an important issue today. The secret images can be various types such as handwritten documents, photographs and others. Naor and Shamir [1] proposed the concept of Visual cryptography (VC) which allows the encryption of secret information in the image form. Visual cryptography is a technique that encrypts a secret image into n shares with each participant holding one or more shares. By using the concept of visual cryptography, a secret image was broken up into some shares and then distributed to the n participants. By stacking their n shares, the secret information can be revealed and visually recognized by human visual system. Visual cryptography (VC) scheme is more secure and very easy to implement. To solve pixel expansion problem use Extended Visual Cryptography Scheme. Cover images are added on each share in Extended Visual Cryptography Scheme. In the Threshold Visual Cryptography scheme images are converted into the binary form. Threshold visual cryptography scheme was first proposed by Naor and Shamir. A secret image is encrypted into n- number of shares then printed on transparencies; shares

are generated with the help of n-number of natural images and one secret image and then spread among n- number of participants.
Visual Secret Sharing scheme (VSS) is implemented to hide secret images that are either printed transparencies or are encoded and stored in digital form. Visual secret sharing is a technique used to deliver and transmit secret images. They satisfy the security requirement for protecting secret content, but they suffer from transmission risk problem because holding noise like shares will create hacker's suspicion and share may be intercepted. The shares can be defined as the noise-like pixels or display low quality images.VSS scheme use a single carrier for sharing images. To solve this problem, Natural image based Visual Secret Sharing (NVSS) is proposed. NVSS scheme uses diverse media for sharing digital images. Transmission risk problem can be solved easily.

II. Literature Review

In this paper propose the visual cryptography that encrypts the secret image into n shares. Security is important issue when we transmit the secret image. Secret image contain the important information so to hide such information from hacker we need to provide security to the secret image in shares. Here shares are nothing but the meaningful images or noise like pixels but it increases interception risk during the transmission of shares. Hence VSS scheme suffers from transmission risk problem. So we propose various visual cryptography techniques.

A. Various visual cryptography techniques

1. (2, 2) Visual Cryptography Scheme

In (2, 2) Visual Cryptography Scheme, original image is split up into 2 shares. In the original image each pixel is represented by the non-overlapping block of 2 or 4 sub-pixels in each share. Anyone who involved in the scheme for n-1 shares cannot revealed any secret information. Both the shares are superimposed the secret image is appeared [3]. There are various techniques for encoding the pixels of original image. Each share has a pair of pixels for every pixel in the original image. In a technique, if the original image pixel is black, the pixel pairs in the image must be complementary. They randomly shared black-white and other white-black. These complementary pairs are overlapped they appeared dark gray. On the other hand they appeared light gray. So when the two shares are superimposed the original image appears. Each component image has a pair of pixels for every pixel in the original image.

2. Halftone Visual Cryptography Scheme

Halftone visual cryptography uses half toning technique in which shares are created. A halftone image is made up of a series of dots rather than a continuous tone. These dots can be various sizes, colors and shapes. Zhi Zhou, Member, Gonzalo R. Arce, Fellow and Giovanni Di Crescenzo proposed Halftone Visual Cryptography in 2006 [2]. They used blue-noise dithering principles with void and cluster algorithm. In Halftone visual cryptography, encoded a binary image into n different halftone shares. Appropriate size of the halftone cells can be used. They obtained the halftone shares. It maintains security and increases quality of the shares.

3. Visual Cryptography Scheme for Grey images

In the previous techniques, operations were only done on the black and white pixels. In real life application it is not efficient. Chang-Chou Lin, Wen-Hsiang Tsai proposed visual cryptography for graylevel images [7]. A dithering technique is used in this scheme. This technique convert graylevel image into approximate binary image. In this scheme shares can be created by using appropriate binary images.

4. Multiple Secret Sharing Scheme

All the previous researches in visual cryptography, only one image can be secured at a time. Wu and Chen [10] proposed a scheme to share two secret images in two shares. In this scheme, two secret binary images can be hidden into two random shares. They are denoted as A and B. By stacking the two shares can be seen in the first secret denoted by $A\otimes B$. For rotating A by 90 degree anti-clockwise the second secret can be obtained .The J Shyu et al [5] proposed a scheme for multiple secrets sharing in visual cryptography. In this scheme, more than two secret images can be used. At a time two shares can be secured.

5. Extended Visual Cryptography Scheme

Nakajima, M. and Yamaguchi, Y. proposed Extended visual cryptography scheme (EVS) in 2002 [6]. In an Extended visual cryptography scheme, instead of random shares meaningful shares are created in traditional visual cryptography. It helps to avoid a possible problem which may arise by noise like shares. The advantage of this scheme is that meaningful shares are generated and improved the quality of output image. In this scheme consider one secret image and n-number of natural image. In this scheme cover image hides a secret image. In this paper, proposed general approach to solve the pixel expansion problems. In this approach only for binary secret images are used. In this paper two phase algorithm is used. In the first phase, use optimization technique to construct meaningful shares. In second phase using stamping algorithm adds cover image in each shares. The experimental result shows that the pixel expansion problem can be solved by extended visual cryptography scheme for general access structure.

6. Threshold Visual Cryptography Scheme

Pei-Ling Chiu and Kai-Hui Lee [6] proposed that a simulated annealing algorithm for general threshold visual cryptography schemes. Threshold visual cryptography scheme considers only binary image. In this paper an optimization technique is proposed based on pixel expansion free threshold visual cryptography scheme. They distinguish blackness level as an efficient metric in the assessment of the display quality of the recovered image. In order to maximize the contrast of the recovered image they first solve the problem as a mathematical optimization. Then they establish a stimulated annealing based algorithm to solve this problem.

7. Visual Secret Sharing Scheme

Visual secret sharing is a technique used to deliver and transmit secret images. They satisfy the security requirement for protecting secret content, but they suffer from transmission risk problem because holding noise like shares will cause hacker's suspicion and share may be intercepted. Visual secret sharing scheme use a single carrier for sharing images. In a (2, 2)-VSS scheme, the cipher text and secret random key can be denoted as two shares in the scheme. They are distributed to two participants who involve in the scheme. The participants can decrypt the secret to the shares in the decryption process.

8. Natural Image Based Visual Secret Sharing Scheme

NVSS uses diverse media for sharing the secret images. The two participants can distribute the natural image and the generated share (i.e., cipher text). In decryption process, the secret key will be extracted again from the natural image. Then the secret key as well as the generated share can recover the original secret image. In the NVSS scheme natural shares can be gray colors of photographs, even flysheet, bookmarks etc. The natural shares can be in digital and printed form. Transmission risk problem can be easily solved.

B. Comparative Analysis

For hiding secret image various schemes can be proposed. In (2, 2) Visual Cryptography Scheme, original image is split up into 2 shares. This scheme is very secure and easy to implement [1]. Zhi Zhou, Member, Gonzalo R. Arce, Fellow and Giovanni Di Crescenzo proposed Halftone Visual Cryptography. Secret binary images are encoded into n shares. The visual quality is better. It increases quality of the shares and maintains security [2]. Chang-Chou Lin, Wen-Hsiang Tsai proposed visual cryptography for gray level images [3]. A dithering technique is used in this scheme. To create shares binary images are applied. The J Shyu et al [5] proposed a scheme for multiple secrets sharing in visual cryptography. At a time two shares can be secured.

Author	**Technique used**	**Number of secret image**	**Pixel expansion**	**Merits**	**Demerits**
Naor and Shamir	Traditional VC	1	1:2	Provide security for binary image	Not generate meaningful share image
M. Nakajima and Yamaguchi	Extended VC	1	1:2	Generate meaningful share	Contrast loss occur
Kafri and Keren	Random grid VC	1	1:1	No pixel expansion	Lower visual quality
Wu and Chen	Multiple secret sharing VC	2	1:4	Image can encrypt two secret images between two shares. Rotating angles is 90^o	Size of the shares is 4 times the size of the main secret image.
Young-Chang Hou and Zen-Yu Quan	Progressive VC	1	1:1	No pixel expansion	No absolute guarantee on the correct reconstruction of the original pixel
Wu and Chang	Multiple secret sharing VC	2	1:4	Rotating angle is invariant	Pixel expansion is more
Zhongmim Wang, Gonzalo R. Arce	Halftone VC	1	1:4	Provide meaningful share images	Trade off between pixel expansion and contras of original image

K. H. Lee and P. L. Chiu proposed an extended visual cryptography algorithm for general access structures [6]. In this paper, two phase encryption algorithm of extended visual cryptography for general access structure can be used. The pixel expansion problem can be solved easily. In this paper cover images are added on each share. So it maintains the security. Pei-Ling Chiu and Kai-Hui Lee [8] proposed that a simulated annealing algorithm for general threshold visual cryptography schemes. Only binary secret images are used. The display quality of recovered images can be controlled more precisely. The contrast of the recovered images can be improved significantly. Visual secret sharing scheme uses unity carrier for sharing a secret image. It suffers from the transmission risk problem. Because it will awake suspicion and increase interception risk during transmission of the shares [8]. Kai-Hui Lee and Pei-Ling Chiu proposed Digital Image Sharing by Diverse Image Media in 2014 [9]. Natural Image Based Visual Secret Sharing Scheme uses diverse media for sharing the secret images. Diverse media contains hand-printed pictures, digital images, printed images and so on. To reduce transmission risk problem use natural image based visual secret sharing scheme.

III.CONCLUSIONS

In this paper we review all the existing techniques of visual cryptography. We have discussed a various visual cryptography techniques such as (2, 2) Visual Cryptography Scheme, Halftone visual cryptography scheme, Visual Cryptography scheme for Grey images, Multiple Secret Sharing Scheme, Extended Visual Cryptography scheme, Threshold Visual Cryptography Scheme , Visual secret sharing scheme ,Natural image based visual secret sharing scheme. For each technique we have provided a detailed explanation of the techniques which are used to provide security for the secret image. From this analysis, a number of shortcomings and limitations were highlighted of these techniques. Visual secret sharing scheme suffers from the transmission risk problem. The transmission risk problem can be solved very easily using Natural image based visual secret sharing scheme.

REFERENCES

[1] Moni Naor and Adi Shamir ,"Visual cryptography", In Proceedings of Advances in Cryptology, EUROCRYPT 94, Lecture Notes in Computer Science, 1995, (950):pp. 1-12.

[2] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography," IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453,Aug. 2006.

[3] Chang-Chou Lin, Wen-Hsiang Tsai, "Visual cryptography for graylevel images by dithering techniques", Pattern Recognition Letters, V.24 n.1-3.

[4] C.C. Wu, L.H. Chen, "A Study On Visual Cryptography", Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[5] S. J. Shyu, S. Y. Huanga,Y. K. Lee, R. Z. Wang, and K. Chen, "Sharing multiple secrets in visual cryptography", Pattern Recognition, Vol. 40, Issue 12, pp. 3633 - 3651, 2007.

[6] K. H. Lee and P. L. Chiu, "An extended visual cryptography algorithm for general access structures," IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 219–229, Feb. 2012.

[7] Nakajima, M. and Yamaguchi, Y., "Extended visual cryptography for natural images" Journal of WSCG. v10 i2 , 303-310.

[8] P. L. Chiu and K. H. Lee, "A simulated annealing algorithm for general threshold visual cryptography schemes," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 992–1001, Sep. 2011.

[9] Kai-Hui Lee and Pei-Ling Chiu,"Digital Image Sharing by Diverse Image Media,"IEEE transactions on information forensics and security, vol. 9, no. 1, January 2014.

[10] G. Selvapriya and J. Jayapriya Jayapal, " Secret Sharing Schemes With

[11] Diverse Image Media", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 11, November 2014

[12] Thottempudi Kiran and K. Rajani Devi,"A Review On Visual Cryptography Schemes", Journal of Global Research in Computer Science Review Article, Volume 3, No. 6, June 2012.

[13] Suhas B. Bhagate , P.J.Kulkarni," An Overview Of Various Visual Cryptography Schemes", International Journal of Advanced Research in Computer and Communication Engineering