International Journal of Research in Advent Technology (IJRAT) (E-ISSN: 2321-9637)

Special Issue

National Conference "CONVERGENCE 2016", 06th-07th April 2016

A REVIEW ON VARIOUS VISUAL CRYPTOGRAPHY SCHEMES

Neha K. Lakde [1], Dr. P. M..Jawandiya [2]

P. G . Scholar, Dept of Computer Science and Engg, PLITMS, Buldana , [1] Principal of PLITMS ,Buldana[2]

Email: neha.lakde123@gmail.com [1] , Principal@plit.ac..in[2]

Abstract: In our daily life Information is increasingly important. Information gets more value when shared with others. Due to advances in technologies related to networking and communication, it is possible to share the information like audio, video and image easily. There are lots of security related issues. Hacker's may try to access unauthorized data and misuse it. Various techiques are required to solve this problem. Techniques to provide security, while sharing information are termed as Secret sharing schemes. When it comes to visual information like image and video, it is termed as Visual secret sharing scheme. Visual cryptography (VC) is a technique used for protecting image-based secrets.This paper presents a detail survey of different visual cryptography scheme used for visual cryptography . The basic concept of visual cryptography scheme is, to split secret image into some shares, which separately reveals no knowledge about the secret information. Shares are then distributed to participants. By stacking these shares directly, secret information can be revealed and visually recognized. All shares are necessary to combine to reveal the secret image. we discuss different visual cryptography scheme like Halftone Visual Cryptography Scheme, Multiple Secret Sharing Scheme, Extended Visual Cryptography Scheme, Visual secret sharing, Natural Image Based Visual Secret Sharing etc.

Index Terms- Secret sharing scheme, Visual Cryptography, Data hiding

1. 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. There has been a steadily growing interest in visual cryptography. Visual cryptography is simple, secure, effective cryptographic scheme and very easy to implement.

G.R. Blakley and Adi Shamir independently invented secret sharing scheme in 1979[1, 2]. When it comes to visual information like image and video, it is termed as Visual secret sharing scheme.

The outlined of this paper is as follows : Section 2. Describes Basic Visual Cryptography Scheme, Halftone visual cryptography scheme, Visual Cryptography scheme for Grey images, Visual Cryptography scheme for color images, Multiple Secret Sharing Scheme, Extended Visual cryptography scheme, Threshold Visual cryptography

scheme, visual secret sharing scheme, Natural Image Based Visual Secret Sharing, Progressive Visual Cryptography scheme. Section 3 : Comparative Analysis ,Section 4 : conclusion and last but not least Acknowledgement and References .

2.VARIOUS VISUAL CRYPTOGRAPHY TECHNIQUES

2.1. Basic Visual Cryptography Scheme

In the domain of the visual cryptography , a secret image can be revealed by stacking two share image. Figure 1 shows the basic representation of visual cryptography , first the secret image is divided into 4 regions; consider R1, R2, R3, R4 . According to block encoding the original secret image is divided into a number of blocks, with 2* 2 pixel in each region .same color pixels in each region . Second , certain sequence is used to generate region shares and sequence is according to orderly original region to share.

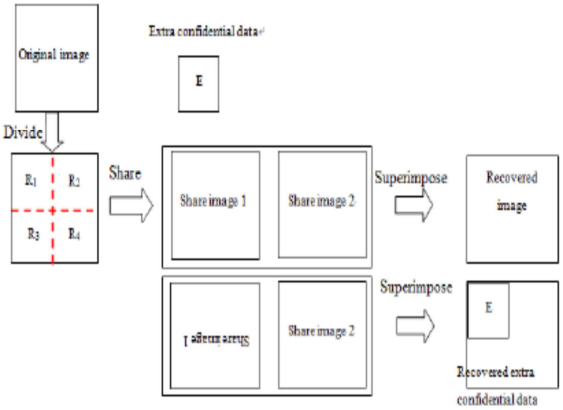

Fig 1: Basic representation of visual cryptography

All region shares are collected as share image 1 and share image 2, extra confidential data can also be revealed by reversing one of share images then stacking . [1,2]

2.2. Halftone Visual Cryptography Scheme

Halftone visual cryptography uses halftoning technique to create shares. Halftone is the reprographic technique. It simulates continuous tone imagery through the use of dots, which may vary either in size, in shape or in spacing. Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo proposed halftone visual cryptography [3].In halftone visual cryptography a secret binary pixel is encoded into an array of sub pixels, called as halftone cell, in each of the „n" shares. By using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained. It maintains good contrast and security

2.3. Visual Cryptography Scheme for Grey images

All previous visual cryptography schemes were works with the bimary images only. These schemes were able to do operations on only black and white pixels but it is not sufficient for real life applications. Chang-chou Lin ,Wen - Hsiang Tsai proposed visual cryptography for grey level images. [4]. To convert grey level image into approximate binary image , a dithering techniques is used. After this existing visual cryptography schemes for binary images are applied to create shares.

2.4. Visual Cryptography Scheme for Color images

Visual cryptography schemes were applied to only black and white images till year 1997. Verheul and Van Tilborg proposed first color visual cryptography scheme [8]. In this visual cryptography scheme one pixel is distributed into m sub pixels, and each sub pixel is divided into c color regions. In each sub pixel, there is exactly one color region colored, and all the other color regions are black.

F.Liu, C.K.Wu, X.J. Lin proposed a new approach for colored visual cryptography scheme [5]. They proposed three different approaches for color image representation:

- In first approach, colors in the secret image can be printed on the shares directly. It works similar to basic visual cryptography model. Limitations of this approach are large pixel expansion and quality of decoded image is degraded.
- In second approach separate three color channels are used. Red, green, blue for additive model and cyan, magenta, yellow for subtractive model. Then normal visual cryptography scheme for black and white images is applied to each of the color channels. This approach reduces the pixel expansion but quality of image gets degraded due to halftoning process.
- In third approach, binary representation of color of a pixel is used and secret image is encrypted at bit-level. This results in better quality of image.

2.5. Multiple Secret Sharing Scheme

All the previous researches in visual cryptography were focused on securing only one image at a time. Wu and Chen [6] were first researchers, who developed a visual cryptography scheme to share two secret images in two shares. In this scheme, two secret binary images can be hidden into two random shares, namely A and B, such that the first secret can be seen by stacking the two shares, denoted by A⊗ B, and the second secret can be obtained by rotating A by 90 degree anti-clockwise. J Shyu et al [7] proposed a scheme for multiple secrets sharing in visual cryptography, where more than two secret image can be

secured at a time in two shares.

26. Extended Visual Cryptography Scheme

In traditional visual cryptography scheme, shares are created as random patterns of pixel. These shares look like a noise. Noise-like shares arouse the attention of hackers, as hacker may suspect that some data is encrypted in these Noise like images. So it becomes prone to security related issues. It also becomes difficult to manage noise-like shares, as all shares look alike. Nakajima, M. and Yamaguchi, Y., developed Extended visual cryptography scheme (EVS) [9]. An extended visual cryptography (EVC) provide techniques to create meaningful shares instead of random shares of traditional visual cryptography and help to avoid the possible problems, which may arise by noise-like shares in traditional visual cryptography.[8]

2.7. Natural Image Based Visual Secret Sharing Scheme

In NVSS [10]scheme diverse media is used for sharing the secrete Images .The participants can distribute the natural image and the generated share (i.e. ciphertext) In decryption process, from the natural image secret key will be extracted again. Then the secrete key as well as the generated share can recover .The original secrete image. In the NVSS scheme natural shares can be grey colors of photographs, even flysheet, bookmarks etc. The natural shares can be in digital and printed form. Transmission Risk problem can be easily solved by using NVSS.

2.8. Progressive Visual Cryptography Scheme

In (k, n) visual secret sharing scheme, it is not possible to recover the secret image though one less than k shares are available. This problem is solved in progressive visual cryptography scheme developed by D. Jin, W. Q. Yan, and M. S. Kankanhalli [12]. In progressive visual cryptography scheme, it is not necessary to have at least k shares out of n, as in (k, n) secret sharing scheme. If more than one share obtained, it starts recovering the secret image gradually. The quality of recovered image improves, as the number of shares received increases.[11]

3. COMPARATIVE ANALYSIS

In Basic Visual Cryptogaphy Scheme original image is split up into 2 shares. This schme is very secure and easy to implement [1].

Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo proposed halftone visual cryptography. In this secret binary images are encoded into n shares . It increases quality of shares so visual quality is better and maintains security [3].

Chang-chou Lin ,Wen -Hsiang Tsai proposed visual cryptography for grey images.[4] In this scheme dithering technique is used. To create shares binary images are applied. F.Liu, C.K.Wu, X.J. Lin proposed colored visual cryptography scheme. It reduces the pixel expansion and results better quality of image.

The J Shyu et al [7] praposed a scheme for multiple secrets sharing in visual cryptography. At a time 2 shares can be secured. K. H. Lee and P. L. Chiu proposed an extended visual cryptography algorithm for general access structures [7]. In this scheme pixel expansion problem can be solved easily and cover images are added on each share. So it maintains the security level.[8,9]

Kai-Hui Lee and Pei-Ling Chiu proposed Digital Image Sharing by Diverse Image Media in 2014 [10]. 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. NVSS reduses transmission risk problems .

D. Jin, W. Q. Yan, and M. S. Kankanhalli developed a Progressive Visual Cryptography Scheme . If more than one share obtained , it starts recovering the secret image and it increases quality of shares.[11,12]

4. CONCLUSION

In this paper we review the existing techniques of visual cryptography. We were 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, Natural image based visual secret sharing scheme and Progressive Visual Cryptography Scheme. For each technique we have provided a detailed explanation of the techniques which are used to provide security as well as quality for the secret image. From this analysis, a number of shortcomings and limitations were highlighted of these techniques. From the origin of visual cryptography , variousbextensions have been developed to improve the quality ,security , ranging from basic visual cryptography to progressive visual cryptography, black and white to color images . Many researches carried out on these extensions , still there is scope to do research in Moni Naor and Adi Shamir's visual cryptography scheme.

5. 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] Blakely, G. R. 1979. Safeguarding Cryptographic Keys. Proceedings of the National Computer Conference, American Federation ofInformation Processing Societies Proceedings. 48: 313-317.

[3] 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.

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

[5] F. Liu, C.K. Wu, X.J. Lin, "Colour Visual Cryptography Schemes", IET Information Security, vol. 2,No. 4, pp 151-165, 2008.

[6] 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.

[7] 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.

[8] 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.

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

[10] 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

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

[12] D . Jin, W. Q. Yan, and M. S. Kankanhalli, "Progressive color visual cryptography," J. Electron. Imag., vol. 14, no. 3, pp. 1–13, 2005.