International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 3, Issue 05, March 2016
Available at http://internationaljournalofresearch.org

A Survey on Visual Cryptography Schemes

Amal C[1], R. Joshua Samuel Raj [2]

[1]PG student of MCA, KVM College of Engineering and Information Technology, Cherthala, Kerala
[2] Vice Principal and Professor, KVM College of Engineering and Information Technology, Cherthala, Kerala

Abstract- *This paper provides an analysis of the emerging visual cryptography (VC) and related security method which can be applied to any of the visual cryptography method. The actual encrypted data embedded image is displayed if and only if the user overcomes the cued click point verification. Hacking is the main issue faced during sharing secrets in visual schemes. The cued click point method can solve the issue up to a limit. Cued click point is a technology where the user has to verify the click points as a security measure and only then the user is provided with the actual visual secret image.*

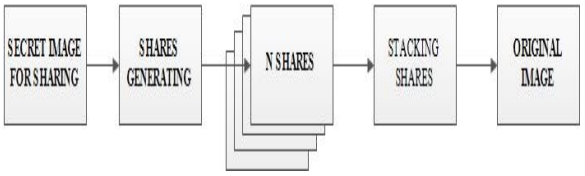
Keywords: Visual Cryptography; Cued Click points; Stereograms.

INTRODUCTION

Visual cryptography is a new technique which provides information security and uses simple algorithms unlike the complex, computationally intensive algorithms used in other techniques in traditional cryptography. This technique allows visual information (pictures, text, etc.) to be encrypted in such a way that their decryption can be performed by the human visual system, without any complex cryptographic algorithms. The basic model of visual cryptography proposed by Naor and Shamir accepts binary image "I" as secret image, which is divided into "n" number of shares. Each pixel in image "I" is represented as "m" sub pixels in each of the "n" shared images. The resulting structure of each shared image is described by Boolean matrix "S" Where S= [S_{ij}] an [n x m] matrix S_{ij}=1 if the j^{th} sub pixel in the i^{th} share is black S_{ij}=0 if the j^{th} sub pixel in the i^{th} share is white. When the shares are stacked together secret image can be seen but the size is increased by "m" times [1].

S_{ij}=1 if the jth sub pixel in the ith share is black
S_{ij}=0 if the jth sub pixel in the ith share is white

Detailed diagram of basic cryptography



Basic flow of visual cryptography

COMPARATIVE STUDY

1. Visual cryptography for general access structures

In (k,n) Basic model any "k" shares will decode the secret image which reduces security level. To overcome this issue the basic model is extended to general access structures by G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, where an access structure is a specification of all qualified and forbidden subsets of "n" shares. Any subset of "k" or more qualified shares can decrypt the secret image but no information can be obtained by stacking lesser number of qualified shares or by stacking disqualified shares. The length of encoding at one run is equal to the number of the consecutive same pixels met during scanning the secret image Construction of scheme is still satisfactory in the aspects of increase in relative size and decoded image quality [2].

2. Visual cryptography for gray level images

A (*k*,*n*)-threshold visual cryptography scheme is proposed to encode a secret image into *n* shadow images, where any *k* or more of them can visually recover the secret image, but any *k*−1 or fewer of them gain no information about it. Previous efforts in visual cryptography were restricted to binary images which is insufficient in real time applications. Chang- ChouLin, Wen-Hsiang Tsai proposed visual cryptography for gray level images by dithering techniques. Instead of using gray sub pixels directly to constructed shares, a dithering technique is used to convert gray level images into approximate binary images. Then existing visual cryptography schemes for binary images are applied to accomplish the work of creating shares. The effect of this scheme is still satisfactory in the aspects of increase in relative size and decoded image quality [3].

3. Recursive Threshold visual cryptography

In recursive hiding of secrets, the user encodes additional information about smaller secrets in the shares of a larger secret without an expansion in the size of the latter, thereby increasing the efficiency of secret sharing. The (k,n) visual cryptography needs „k" shares to reconstruct the secret image. Each share consists at most [1/k] bits of secrets. This

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 3, Issue 05, March 2016
Available at http://internationaljournalofresearch.org

approach suffers from inefficiency in terms of number of bits of secret conveyed per bit of shares. Recursive threshold visual cryptography proposed by Abhishek Parakh and SubhasKak eliminates this problem by hiding of smaller secrets in shares of larger secrets with secret sizes doubling at every step. When Recursive threshold visual cryptography is used in network application, network load is reduced. [4]

4. Halftone Visual Cryptography

Based on the blue-noise dithering principles, the proposed method utilizes the void and cluster algorithm to encode a secret binary image into n halftone shares (images) carrying significant visual information. The meaningful shares generated in extended visual cryptography proposed by Mizuho Nakajima and Yasushi yamaguchi was of poor quality which again increases the suspicion of data encryption. Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo proposed halftone visual cryptography which increases the quality of the meaningful shares. In halftone visual cryptography a secret binary pixel "P" is encoded into an array of Q1 x Q2 ("m" in basic model) sub pixels, referred to as halftone cell, in each of the "n" shares. By using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained which also maintains contrast and security [5].

5. Progressive visual cryptography

The application of digital half toning techniques results in some downgrading of the original image quality due to its inherently lossy nature and it is not possible to recover the original image from its halftone version. Duo Jin Wei-Qi Ya n, Mohan S, Kankanhalli[6] proposed a new encoding method that enables us to transform gray-scale and color images into monochrome ones without loss of any information. Incorporating this new encoding Scheme into visual cryptography technique allows perfect recovery of the secret grayscale or color image.

6. Regional incrementing Visual Cryptography

In the RIVC scheme, the content of an image S is designated to multiple regions associated with n secret levels, and encoded to n+1 shares. VC schemes mentioned above usually process the content of an image as a single secret i.e. all of the pixels in the secret image are shared using a single encoding rule. This type of sharing policy reveals either the entire image or nothing, and hence limits the secrets in an image to have the same secrecy property. Ran-Zan Wang proposed Region Incrementing Visual cryptography for sharing visual secrets in multiple secrecy level in a single image. The "n" level RIVC scheme, an image S is designated to multiple regions associated with secret levels, and encoded to shares [7].

7. Extended visual cryptography for natural images

Extended Visual Cryptography is a type of cryptography which encodes a number of images in the way that when the images on transparencies are stacked together, the hidden message appears without a trace of original images. All of the VC methods suffer from a severe limitation, which hinders the objectives of VC. The limitation lies in the fact that all shares are inherently random patterns carrying no visual information, raising the suspicion of data encryption. Mizuho nakajima and Yasushi yamaguchi proposed extended visual cryptography for natural images constructing meaningful binary images as shares. This will reduce the cryptanalysts to suspect secrets from an individual shares. While the previous researches basically handle only binary images, this scheme establishes the extended visual cryptography scheme suitable for natural images [8].

8. Visual cryptography for color images

The researches in visual cryptography leads to the degradation in the quality of the decoded binary images, which makes it unsuitable for protection of color image .F.Liu, C.K. Wu X.J. Lin proposed a new approach on visual cryptography for colored images. They proposed three approaches as follows: [9]

1. The first approach to realize color VCS is to print the colors in the secret image on the shares directly similar to basic model. It uses larger pixel expansion which reduces the quality of the decoded color image.

2. The second approach converts a color image into black and white images on the three color channels (red, green, blue or equivalently cyan, magenta, yellow), respectively, and then apply the black and white VCS to each of the color channels. This results in decrease of pixel expansion but reduces the quality of the image due to halftone process.

3. The third approach utilizes the binary representation of the color of a pixel and encrypts the secret image at the bit-level which results in better quality but requires devices for decryption.

9. Single Image Random Dot Stereogram visual cryptography

This method exacerbates the pixel expansion problem and visual quality degradation problem for recovered images. A binocular VCS (BVCS), called the (2, n)-BVCS, and an encryption algorithm are proposed to hide the shared pixels in the single image random dot stereograms (SIRDSs). Because the SIRDSs have the same 2D appearance as the conventional shares of a VCS, this method uses SIRDSs as cover images of the shares of VCSs to reduce the transmission risk of the shares. The encryption algorithm alters the random dots in the SIRDSs according to the construction rule of the (2, n)-BVCS to produce non pixel expansion shares of the BVCS. Altering the dots in

CONCLUSION

In this study we have referred some of cryptography schemes for sharing visual secrets. Among the various schemes the Single Image Random Dot Stereogram visual cryptography method seems to be more advantageous than the rest since it overcomes pixel expansion problem and visual quality degradation problem for recovered images. Combining Single Image Random Dot Stereogram visual cryptography method with cued click points will improve the security of the shared visual content.

Sr.No	Authors	Merits	Demerits
1	Naor and Shamir	Provide Security for binary image Does not generate meaningful share image	Does not generate meaningful share image
2	G. Ateniese, C. Blundo, A. De Santis, D. R. Stinson,	No information can be obtained by stacking lesser number of qualified shares	Increased size of image
3	Zhongmin Wang, Gonzalo R. Arce	Provide meaning full share images	Trade-off between pixel expansion and contras of original image
4	Abhishek Parakh and SubhasKak	When Recursive threshold visual cryptography is used in network application, network load is reduced.	Suffers from inefficiency in terms of number of bits of secret conveyed per bit of shares.
5	F.Liu,C.K. Wu X.J. Lin	Visual cryptography for color image	Requires devices for decryption.
6	Ran-Zan Wang	All of the pixels in the secret image are shared not using a single encoding rule.	Limits the secrets in an image to have the same secrecy property.
7	Mizuho NAKAJIMA, Yasushi YAMAGUCHI	This will reduce the cryptanalysts to suspect secrets from an individual shares.	All shares are inherently random patterns carrying no visual information.
8	Duo Jin Wei-Qi Ya n, Mohan S, Kankanhalli	Transform gray-scale and color images into monochrome ones without loss of any information	Downgrading of the original image quality
9	Kai-Hui Lee and Pei-Ling Chiu	The pixel expansion problem and visual quality degradation problem for recovered images.	Degrade the visual quality of the reconstructed 3D objects.

REFERENCES

[1]. Zhongmin Wang, Gonzalo R. Arce, and Giovanni Di Crescenzo, "Halftone Visual Cryptography via Error Diffusion," IEEE Transactions on Information Forensics and Security, vol. 4, no. 3, September 2009

[2].M. Naor and B. Pinkas, "Visual authentication and identification," Crypto97, LNCS, vol. 1294, pp. 322–340, 1997.

[3]. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone Visual Cryptography," IEEE transactions on Image Processing, to appear in 2006.

[4]. M. Naor and A. Shamir, "Visual Cryptography," in Proceedings of Euro crypt 1994, lecture notes in Computer Science, 1994, vol. 950, pp. 1–12.a SIRDS will degrade the visual quality of the requirement of SIRDSs to develop construction rules for a (2, n)-BVCS that maximize the contrast of the recovered image in the BVCS [10].

[5]. A. Bonnis and A. Santis, "Randomness in secret sharing and visual cryptography schemes," Theory. Computer. Science, 314, pp 351- 374 (2004).

[6]. E.Myodo, S. Sakazawa, Andy. Takishima, "Visual cryptography based on void-and-cluster half toning technique," in Proc. IEEE ICIP, Atlanta, GA, Oct. 2006.

[7]. R. Hwang, "A digital Image Copyright Protection Scheme Based on Visual Cryptography," Tambang Journal of science and Engineering, vol.3, No.2, pp. 97-106 (2000).

[8] Mizuho nakajima, Yasushi yamakuchi "Extended visual cryptography for natural images". Department of Graphics and Computer Sciences, Graduate School of Arts and Sciences, The University of Tokyo 3-8-1 Komaba, Meguro-ku, Tokyo 153-8902, Japan.{mitzy, yama}@graco.c.u-tokyo.ac.jp

[9]. Sozan Abdulla "New Visual Cryptography Algorithm for Colored Image", Journal of computing, Vol. 2, issue 4, April 2010, ISSN 2151-9617

[10]. Kai-Hui Lee and Pei-Ling Chiu, "Sharing Visual Secrets in Single Image Random Dot Stereograms", IEEE Transactions on image processing, Vol. 23, No. 10, october 2014