IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 15-18
www.iosrjournals.org

ViCry: Visual Cryptography Schemes for Security (An overview of different types of visual cryptography schemes)

Febin Baby, Arun R, Dr. Suvanam Sasidhar Babu
Dept. of CSE (Cyber Security) Sree Narayana Gurukulam College of Engineering Kadayiruppu, Kerala, India
Dept. of CSE Sree Narayana Gurukulam College of Engineering Kadayiruppu, Kerala, India

Abstract: Visual Cryptography is a special kind of cryptographic technique in which the decryption can perform by the human visual capability. Ingeneral,for some criticalsecurityissue the visual cryptography scheme is used, for example to identify the difference in human and machine. Security has become an inseparable issue as Information Technology is ruling the world now. Cryptography in the study of mathematical techniques related aspects of information security such as confidentialities, data security, entity authentication, but it is not only the means of providing information security, rather one of the techniques. Visual cryptography can be applied for copy right for images, access control to user images ,visual authentication and identification any kind images of images like(normal or digital).Visual cryptography is a new technique which provides information security which user simple algorithm unlike the complex, computationally intensive algorithms used in other techniques like traditional cryptography. Similarly some other applications also use the visual cryptography schemes like scanning and printing, captcha etc. Hence the researchers developed many methods and techniques for the visual cryptography schemes. This paper is intended to study the various visual cryptography schemes and also to analysis the performance on the basis of expansion of pixel, number of secret images, image format and type of share generated. In addition we present a concise description about the instructions for future research.

Keywords*: Pixels, Contrast, Secret sharing, Shares, Stacking, Analysis*.

I. Introduction

Visual cryptography is a visual version of secret sharing proposed by Moni Naor and Adi Shamir in 1994[1].This technique refers to the information security like data integrity, confidentiality and authentication, Visual cryptography is one of the simple, secure and effective cryptographic schemes. It is used for protecting image based secrets. The secret image is divided into n number of shares, contain number of pixels. The combination of shares reveals secret when done decryption using algorithms [1]. Each share was printed on a separate transparency, and description was performed by overlaying the shares. When all n shares were overlaid, the original image could appear. Main advantage of this scheme is mathematical computation complexity is reduced compared to conventional cryptographic techniques. There are so many generalization of this basic scheme.

Since the origin of this, various extensions have been developed to improve the things. These extensions to basic visual cryptography are outlined in this paper in Section II, which includes Basic visual cryptography model,(2,2) Visual Cryptography Scheme, (k, n) visual Cryptography scheme, Visual cryptography scheme for General Access Structure, Halftone visual cryptography scheme, Visual Cryptography scheme for Grey images, Visual Cryptography scheme for color images, Multiple Secret Sharing Scheme, Extended Visual Cryptography scheme, Progressive Visual Cryptography scheme, Region Incrementing Visual Cryptography scheme and Segment based Visual Cryptography Scheme. Section III contains conclusion and future work.

II. Visual Cryptographic Schemes

1. *(2, 2) Visual Cryptography Scheme*

In (2, 2) visual cryptographic scheme, only two shares are generated from the original image. Each pixel in original image is represented by non-overlapping block of 2 or 4 sub-pixels in each share. Anyone, having only one share will not be able to reveal any secret information. Both the shares are required to be superimposed to reveal the secret image [7]. This is equivalent to using the logical OR operation between the shares.

There is a simple algorithm for binary (black and white) visual cryptography that creates 2 encrypted images from an original unencrypted image. The algorithm is as follows: First create an image of random pixels

the same size and shape as the original image. Next, create a second image the same size and shape as the first, but where a pixel of the original image is the same as the corresponding pixel in the first encrypted image, set the same pixel of the second encrypted image to the opposite color. Where a pixel of the original image is different than the corresponding pixel in the first encrypted image, set the same pixel of the second encrypted image to the same color as the corresponding pixel of the first encrypted image. The two apparently random images can now be combined using an exclusive-or (XOR) to re-create the original image.

2. (K, n) Visual Cryptography Scheme

Both shares are required for reveal the secret information in (2, 2) visual cryptographic scheme[7]. A *k*-out-of-*n* threshold VC is capable of encoding a secret image into *n* random-looking images called shares or shadows. Any groups of *k* or more shares can visually recover the secret image by printing the shares on transparencies and stacking them together. Whereas, any groups of $k - 1$ or less shares give no clue about the secret. It gives flexibility to user. If user loses some of the shares still secret information can be revealed, if minimum k number of shares is obtained.[6] The
important parameters of a scheme are its contrast, i.e., the clarity with which the message becomes visible, and the number of sub pixels needed to encode one pixel of the original picture.

3. Visual Cryptography Scheme for General Access Structure

In (k, n) basic model any k shares will decode the secret image which reduces security level. The model proposed by G Ateniese, C Blundo, A De Santis D R Stinson for overcome this issue is known as general access structure. Where an access structure is a specification of qualified and forbidden subsets of shares(k) contained in the qualified set reveals the secret image; but less than k shares from qualified subsets of shares cannot reveals any secret information. The shares containing forbidden set are independent in secret image formation [2]. Construction of schemes is still satisfactory in the aspects of increase in relative size and decoded image quality [5].

***4.* Visual Cryptography schemes for grey images**

In real time application not only binary images were used, but the previous works to be restricted to binary images. These techniques were capable of doing operations only on black and white pixels. The technique for grey level images was proposed by Chang-Choulin, Wen-Hsiang Tsai [4]. A dithering technique is used rather than using grey sub pixel directly to construct shares. Dithering technique is employed to convert grey level images into absolute binary images. Then for creating shares of binary images the existing visual cryptography scheme is used. The scheme increase the relative size and decode image quality even when the grey level of images still expands[5].

5. Halftone Visual Cryptography

The technique proposed by Zhi Zhou, Gouzalo R Arce and Giovanni Di Crescenzo, for crating meaningful image shares [8]. The meaningful image shares improve the suspicion of data encryption. In halftone visual cryptography, a secret binary pixel P is encoded into an array of Q1 X Q2 rather than m in basic model pixel known as halftone cell for each share. Halftone shares created using the approximate sizes of halftone cells. Image property like contrast is maintained and also security factor improves.

6. Visual Cryptography Scheme for Color images

Visual cryptography scheme were applied to only black and white images still year 1997. The first color visual cryptography scheme was proposed by Verheul and Van Tilborg [4]. In color image VC , the pixels are distributed into m sub pixels and sub pixels 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.

Later this approach extended by F.Lin, C.K.Wu and X.J.Lin. Main specifications in their proposal are 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. Also another approach deals that 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 half toning process [10]. Last approach describes that binary representation of color of a pixel is used and secret image is encrypted at bit-level. This results in better quality of image.

7. Region Incrementing Visual Cryptography

In traditional visual cryptography scheme, one whole image is considered as a single secret and same encoding rule is applied for all pixels of one image. So it reveals either entire image or nothing. It may be the situation that different regions in one image can have different secrecy levels, so we can't apply same encoding rule to all pixels [2]. Ran-Zan Wang developed a scheme "Region Incrementing Visual cryptography" for sharing visual secrets of multiple secrecy level in a single image [ ]. In this scheme, different regions are made of a single image, based on secrecy level and different encoding rules are applied to these regions.

Region Incrementing Visual cryptography for sharing visual secrets in multiple secrecy level in a single image [9]. The „n" level RIVC scheme, an image S is designated to multiple regions associated with secret levels, and encoded to shares with the following features:

(a) Each share cannot obtain any of the secrets in S,
(b) Any t(2<t<n+1) shares can be used to reveal (t-1) levels of secrets
(c) the number and locations of not-yetrevealed secrets are unknown to users,
(d) all secrets in S can be disclosed when all of the (n+1) shares are available

8. Segment based Visual Cryptography scheme

Traditional visual cryptography schemes were based on pixels in the input image. The limitation of pixel based visual cryptography scheme is loss in contrast of the reconstructed image, which is directly proportional to pixel expansion. Bernd Borchert proposed a new scheme which is not pixel-based but segment-based [4].It is useful to encrypt messages consisting of symbols represented by a segment display. For example, the decimal digits 0, 1,... ,9 can be represented by seven-segment display [5]. The advantage of the segment-based encryption is that, it may be easier to adjust the secret images and the symbols are potentially easier to recognize for the human eye and it may be easier for a non-expert human user of an encryption system to understand the working.

9. Extended Visual Cryptography Scheme

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 [3] proposed Extended visual cryptography for natural images constructs 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, [ ] establishes the extended visual cryptography scheme suitable for natural images.

III. Conclusion

This paper discusses the introduction of different types of Visual Cryptography schemes. It compares the image quality and security using various visual cryptography schemes. In order to hide the secrecy we go for expansion and increasing of the number of shares, but this affects the resolution. Therefore an optimum number of shares are required to hide the secrecy. At the same time security is also an important issue. Hence research in visual cryptography (VC) is towards maintaining the contrast at the same time maintaining the security.

References

[1] "Visual Cryptography"-/Moni Shamir & Adi Shamir
[2] "Extended Capabilities for XOR-Based Visual Cryptography"//Xiaotian Wu and Wei Sun- ieee transactions on information forensics and security, vol. 9, no. 10, October 2014
[3]. "Extended capabilities for visual cryptography "G. Ateniese et al. / Theoretical Computer Science 250 (2001)
[4]. "An Overview Of Various Visual Cryptography Schemes"-Suhas B. Bhagate , P.J.Kulkarni// International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 9, September 2013
[5] "An Introduction to Different Types of Visual Cryptography Schemes"- Néelima. Guntupalli & Mr: P.D.Ratna Raju // International Journal of Science and Advanced Technology (ISSN 2221-8386) Volume 1 No 7 September 2011
[6] "k Out of n Region Incrementing Scheme in Visual Cryptography"-Ching-Nung Yang, Senior Member, IEEE, Hsiang-Wen Shih, Chih-Cheng Wu, and Lein Harn
[7] **"**A Novel Two Stage Binary Image Security System Using (2,2) Visual Cryptography Scheme" Mr. Rohith S, Mr. Vinay G /International Journal Of Computational Engineering Research / ISSN: 2250– 3005 // IJCER | May-June 2012 | Vol. 2 | Issue No.3 |642-646 Page 642
[8] International Journal for Research in Applied Science & Engineering Technology (IJRASET) "A secured approach for sharing critical data on halftone image Using advance visual cryptography" Volume 3 Issue I, January 2015 ISSN: 2321-9653

[9] "Visual Cryptographic Technique for Enhancing the Security of Image Transaction" International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 5, May 2014 by Akshatha M M, Lokesh B, Nuthan A C

[10] "Maintaining the Secrecy in Visual Cryptography Schemes" by Divya.A and k.Rajalakshmi // 978-1-4244-8679-3/11/$26.00 ©2011 IEEE