IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 06-12
www.iosrjournals.org

Survey on Visual Cryptography: Techniques, Advantages and Applications

[1]Shruti M. Rakhunde [2]Manisha Gedam
[1](shruti.rakhunde@raisoni.net, Assit. Prof., G. H. Raisoni Institute of Information Technology, RTM Nagpur University, Nagpur(MS),India)
[2](manisha.gedam@raisoni.net, Assit. Prof., G. H. Raisoni Institute of Information Technology, RTM Nagpur University, Nagpur(MS),India)

Abstract: *Visual Cyptography (VC) is widely used secret communication technique. Visual Cryptography is the method used for secret-sharing that encrypts a secret image into several shares. These shares are either printed on transparencies or are encoded and stored in a digital form. The shares can look as noise-like pixels or as meaningful images. Decoding require all n shares. There are various measures which decide over the performance of visual cryptography scheme like type of shares, number of shares, pixel expansion, security, accuracy, computational complexity, share generated is meaningful or meaningless, type of secret images and number of secret images encrypted by the scheme. These shares are supposed to be printed on transparences and after stacking them top to each they will reveal the secret image. This paper focuses on study of different techniques of visual cryptography its detail analysis with respect to applications and advantages of techniques is also presented*

Keywords - Visual Cryptography (VC), meaningless shares, meaningful shares

I. INTRODUCTION

Visual Cryptography is the method used for secret-sharing that encrypts a secret image into several shares ; intervention of computer, or calculations are not to decrypt the secret image. The hidden secret image can be retrieved visually by overlaying the encrypted shares and then the secret image becomes clearly visible. This technique was given by Moni Nair and Adi Shamir, thus this is credited to their name. They demonstrated a visual secret sharing scheme, where an image is split into *n* shares so that only someone with all *n* shares could decrypt the image, while any $n - 1$ shares revealed no information about the original image. Each share after printing on a separate transparencies can be superimposed to decrypt the secret image [1]. When all *n* shares were superimpose, the original image would appear.

Image that can be considered for Visual Cryptography can be Binary Image, Grayscale Image and Color Image. The scheme given by Nair and Shamir for sharing a secret binary image was by using their own coding table. In this scheme the binary image is divided into two shares, for the white pixel in the secret image, one of the upper two rows of table I is chosen to make share1 and share2. If the pixel of the secret image is black, one of the lower two rows of table I is used to make share1 and 2. This scheme consists of pixel expansion where every pixel from the secret image is expanded to 4 pixels, so when the shares are generated and superimposed together the reconstructed image will be four times the original secret image size because of this pixel expansion. Also the resolution of the reconstructed image will be less than the original secret image as every white pixel is decomposed into two white & two black pixels. Only one secret could be hidden using this technique.

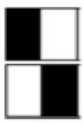
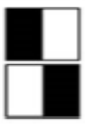
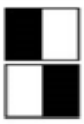
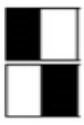
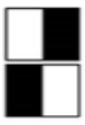
pixel		share #1	share #2	superposition of the two shares
	$p = .5$ $p = .5$			
	$p = .5$ $p = .5$			

TABLE 1: NAIR AND SHAMIR SCHEME FOR ENCODING BINARY PIXEL

Basic visual cryptography scheme can explained with the following figure. Fig (a) is the binary secret image, fig (b) and (c) are the shares and fig (d) is the recovered image.

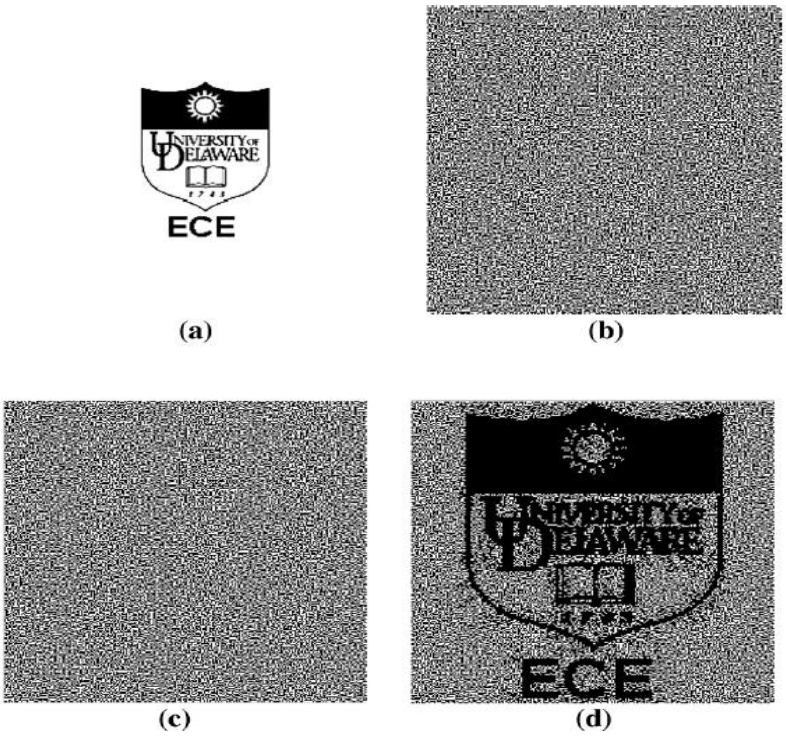


FIGURE 1: EXAMPLE OF BASIC VISUAL CRYPTOGRAPHY. (A) BINARY SECRET IMAGE. (B)SHARE 1. (C) SHARE 2. (D) RECOVERED SECRET MESSAGE

The rest of this paper is organized as follows. Section II discusses literature survey for visual cryptography techniques. In section III, various visual cryptography techniques is discussed, while section IV provides detail analysis of visual cryptography schemes, section V shows applications of VC and section VI comprises the conclusion.

II. LITERATURE SURVEY

Different researcher has worked on the scheme proposed by Nair and Shamir to improve the performance.

Naor & Shamir[1] proposed visual cryptography scheme in 1994. This is the basic scheme of visual cryptography in which the secret image is divided into two shares. The shares generated are meaningless. When the two shares are stacked together, it produces the original secret image. This scheme is only for black & white images.

Ateniese, Blundo & Stinson [2] proposed extended visual cryptography in 1996. This scheme contains meaningful shares. The (2,2) EVC theme projected during this needed enlargement of one picture element within the original image to four sub pixels which may then be chosen to supply the specified pictures for every share. Up to 1997, Visual cryptography schemes were applied to only black & white images.

Verheul & Tilborg [3], proposed first colored visual cryptography scheme. But this scheme produces meaningless share.

Wu and Chen [4] in 1998, were the first researchers to present the visual cryptography schemes to share two secret images in two shares

Hsu et al [5] proposed another scheme in 2004. The scheme hides two secret images in two share images with arbitrary rotating angles.

Verheul and Van Tilborg [3] proposed a scheme for colored secret images can be shared; the concept of arcs was used to construct a colored visual cryptography scheme

S J Shyu et al [7] were first researchers to advise the multiple secrets sharing in visual cryptography. This scheme encodes a set of $n \geq 2$ secrets into two circle shares. The n secrets can be obtained one by one by stacking the first share and the rotated second shares with n different rotation angles. To encode unlimited shapes of image and to remove the limitation of transparencies to be circular

III. VISUAL CRYPTOGRAPHY SCHEMES

A. Visual Cryptographic Schemes for Black and White Images / Binary Images

1) ***Binary Secret Images:*** Wu and Chen [4] in 1998, were the first researchers to present the visual cryptography schemes to share two secret images in two shares. In this scheme two secret binary images were considered which were hidden into two random shares, namely share A and share B. In retrieving phase the first secret image can be revealed by stacking the two shares, denoted by A⊗ B, and the second secret can be revealed by first rotating share A by angle Θ anticlockwise. The rotation angle Θ was designed to be 90◦.

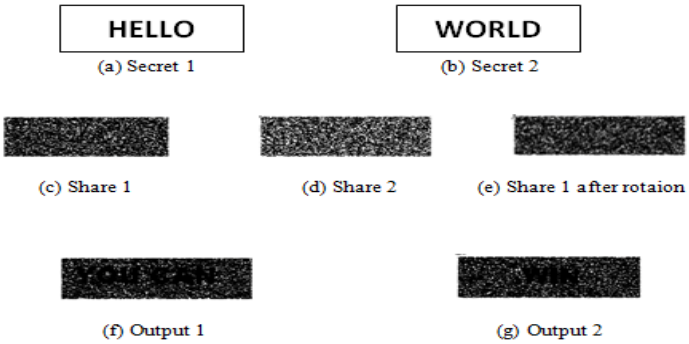


FIGURE 2: SAMPLE EXAMPLE FOR HIDING TWO SECRET IMAGES.

2) Above scheme is based on rotation angle for the image and meaningless shares. To overcome the angle restriction in above scheme, in 2004 Hsu et al [5] proposed another scheme. In this scheme two secret images are hidden in two share images with arbitrary rotating angles. Two confidential data sets are encrypted into shadow images under different overlapping angle using the encrypting Table II of 2x2 expanded pixel squares given below [5]. This is one of most promising approach of visual cryptography.

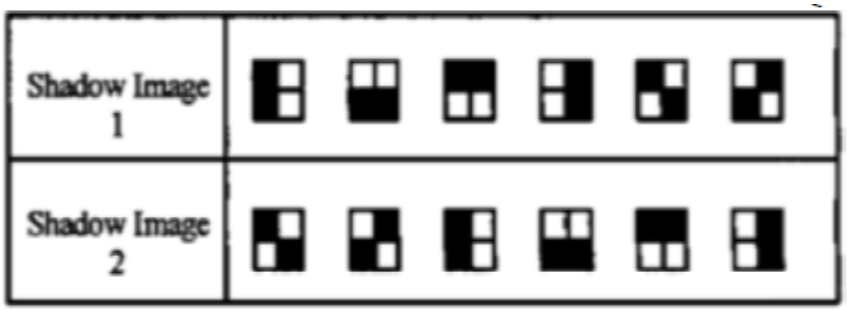


TABLE II: ENCRYPTING TABLE OF 2X2 EXPANDED PIXEL SQUARE

Circular visual cryptography was introduces in 2005[4]. In this scheme, circular images are used where circular shadow image can hide two or more confidential data sets simultaneously into circular images and display them at both the inner and outer region of the circular images. It can only produce a circular shadow image without the central part causing a low resolution on the images at the inner portion. The encryption of data is on two ringed shadow images. This allows hiding of two confidential data sets simultaneously [9]. This is the advantage of this scheme.

B. Visual Cryptography Schemes for color images

1. For Single Secret Sharing:

Till 1997 visual cryptography schemes were applied to only black and white images. Verheul and Van Tilborg [3] developed Colored visual cryptography scheme. Colered images are very popular in use, Colored secret images can be shared using this method; the concept of arcs was used to construct a colored visual cryptography scheme. As color images are extremely famous, in c-colorful visual cryptography scheme one pixel is transformed 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. The color of one pixel depends on the interrelations between the stacked sub pixels. For a colored visual cryptography scheme with r colors, the pixel expansion m is r× 3. These schemes share generated were meaningless.

2. For Multiple Secret Sharing:

Above scheme was sharing single secret whereas researcher developed multiple secret sharing scheme. Wu and Chen [4] gave a scheme to share multiple secret were first researchers to present the visual cryptography schemes to share two secret images in two shares. They have hidden two secret binary images into two random shares, 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 retrieved by first rotating A Θ anti-clock wise. The scheme considered the rotation angle Θ to be 90◦. However, it is easy to obtain that Θ it can be 180 ◦ or 270◦. To overcome the angle restriction of Wu and Chen's scheme [4], Hsu et al. [3] proposed a scheme to hide two secret in two rectangular share images with arbitrary rotating angles. Wu and Chang [7] also refined the idea of Wu and Chen [4] by encoding shares to be circles so that the restrictions to the rotating angles i.e: Θ=90◦,180◦ or 270◦ can be removed.

This approach of sharing Multiple Secret was taken forward by Tzung-Her Chen et al in [6], they worked on a multi-secrets visual cryptography which is extended approach of traditional visual secret sharing. In this scheme the codebook of traditional visual secret sharing method is implemented to generate share images macro-block by macro-block in such a way that these multiple secret images are converted into only two share images and decode all the secrets one by one by stacking two of share images in a way of shifting. This scheme can be used for multiple gray, binary and color secret images. Pixel expansion is 4.

Later Daoshun Wang et al [7] provided general construction for extended visual cryptography schemes. The approach of matrix extension algorithm was used. A general construction method for multiple or single image, where binary, grayscale, color secret images using matrix extension utilizing meaningful shares was suggested. Using matrix extension algorithm, any existing visual cryptography scheme with random-looking shares can be easily modified to utilize meaningful shares.

3. Keyless Visual Cryptography

This was again more promising approach. It was introduced by Jaya and Sardana, this scheme involves splitting an image into multiple shares. The color image is considered here, the shares so generated using this method reveal no information about the original secret image and to retrieve the secret image all the shares are required. The proposed technique is implemented with the Seiving-Division-Shuffling algorithm proposed in this paper and involves three steps. In step one seiving the secret image is split into primary colors. In step two Division these split images are randomly divided. In step three Shuffling these divided shares are then shuffled each within itself to get final random shares.

FIGURE 3: COLOR VISUAL CRYPTOGRAPHY USING SDS (SIEVING— DIVISION – SHUFFLING) ALGORITHM

4. Key based Visual Cryptography

Above scheme is based on the concept of keyless visual cryptography where keys are not involved, it is advantageous in term that Key generation and management is not required, it is simple, complexity of key based approaches is not involved. Based on this approach, a scheme was presented in [9] aiming to achieve key safeguarding and secret image sharing. Mathematical calculations were used to generate an image acting as Key Image. This Key is generated from the secret image and some chosen securing images (p). To reconstruct the secret color image, the Key image and q securing images are used where q<p. This is called (p,q) threshold scheme.

IV. ANALYSIS OF VISUAL CRYPTOGRAPHY SCHEME

Following table summarizes the various Visual Cryptography schemes in terms of their pros and cons. Factors like type of image considered, number of secret images, number of shares formed, type of number of shares, and the technique used in these Visual Cryptography schemes.

Author	Year	No. of Secret Images	Type of Image	Types of Shares Generated	Description	Reference No.
Naor & Shamir	1994	1	Binary	Meaningless	Use coding table to generate the shares.	[1]
Ateniese, Blundo & Stinson	1996	1	Binary	Meaningful	Extended visual cryptography scheme	[2]
E.R. Verheul and van Tilborg	1997	1	Colored	Meaningless	Colored secret images can be shared; the concept of arcs was used to construct a colored visual cryptography scheme.	[3]
Wu and Chen	1998	2	Binary	Random	This visual cryptography scheme is to share two secret images in two shares, with rotation angle restriction	[4]
Hsu et al	2004	2	Binary	Meaningless	Arbitrary angle rotation to create the second secret.	[5]
Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei	2008	n>=2	Binary, Gray, Color	Meaningless	turn more secret images into the same share images	[6]
Daoshun Wang	2009	n>=1	binary, grayscale, color	Meaningful	Extended visual cryptography schemes using matrix extension algorithm	[7]
Siddharth Malik, Anjali Sardana, Jaya	2012	1	Colored	Random	The proposed technique is implemented with the SDS algorithm and involves three steps that are Seiving, Division and Shuffling	[8]
Hirdesh Kumar , Awadhesh Srivastava	2014	1	Colored	Meaningful	based on secret image sharing and key safeguarding technique, an effective and generalized scheme of color image hiding is proposed by means of numerical computations	[9]

TABLE III: COMPARISON BETWEEN SEVERAL SCHEMES

V. APPLICATIONS OF VISUAL CRYPTOGRAPHY

An application for Visual Cryptography involves:

1. Watermarking

Watermarking is another application area of Visual Cryptography. The scheme in [15] explains the use of visual cryptography in watermarking which composes of two phases: the watermark embedding and watermark retrieving. During the watermark embedding phase, a watermark is split into two shares by means of visual cryptography. Then, one of the two shares is embedded into the frequency domain of the host image, and the other is distributed to the owner. To prove the ownership, the owner has to address his/her share, extract the other share from the image and then combine these two shares to reveal the watermark. Based on the security condition of visual cryptography, we can make sure that the two shares cannot leak any information about the watermark. This application is discussed in [15].

2. Secure Banking Communication

In a core banking system, there is a chance of encountering forged signature for transaction. And in the net banking system, the password of customer may be hacked and misused. Thus security is still a challenge in

these applications. In [16] a scheme is proposed for securing the customer information and to prevent the possible forgery of password hacking. The concept of image processing, in visual cryptography is used.

3. Defense System

Visual Cryptography Scheme is an encryption method that uses combinational techniques to encode secret written materials. This can be very useful in defense system to protect very sensitive data, when data like password or any code is to transferred from one place to another that secret data can be it can hidden in cover image, the share of the image is to be converted into shares. Those multiple shares can be kept with multiple partners. Any one partner cannot retrieve the secret code from the single share he has, all the shares from all the partners are required to retrieve secret information hidden in the image. Thus data is safe in hands all the partner.

4. Anti- Phishing Systems

Anti phishing system can be one of the application of Visual Cryptography. Phishing websites aims to steal sensitive and personal information such as passwords, credit cards numbers, pins, etc. They trick customers by making identical web site to a real one where the customer submits his information. The work of [14] solves this problem by using visual cryptography technique. The customer can ensure if this is the genuine web site or not by typing his user name. The server will send a share from its database. The client will superimpose his own share with the one sent by the site to ensure this is not phishing web page and then user can type the information

5. Signature Based Authentication using Contrast Enhanced Hierarchical Visual Cryptography

Employee System can be prevented by using authentication system based on visual cryptography [13] [11].Here authentication can be done using shares to prevent the systems from some attacks such as brute force attack. Any institute can be considered as an application. Firstly, employees will register in the system, the signature of the employee is scanned and entered in the system to get its key share this key is printed on a card and given to the employee and the simple share is entered to the system database. During authentication, the employee inserts his own card in the card reader mounted in the entrance to read the key share from the card and superimposes over the corresponding simple share available in the database.

VI. CONCLUSION

The significance of securing data in communication is the motivation behind studying various visual cryptography schemes. Visual Cryptography (VC) is a encryption scheme used to share secret image. It encodes image into n shares. These shares are either printed on transparencies or are encoded and stored in a digital form. All the shares are required to retrieve secret data. There are many factors, which decide performance of these schemes. Among the factors are number of shares, image format, encrypted shares' size, and the type of share to be generated. The table of comparison is presented in this paper to summarize the different features of each technique reviewed. As discussed in various applications systems can be made more secure and reliable by the application of visual cryptography techniques.

REFERENCES

[1]. M. Naor & A. Shamir, ―Visual Cryptography‖, advances in cryptology- Eurocrypt'94.Lecture notes in computer science,1-12,1994.

[2]. G. Ateniese, C. Blundo, A. Santis & D. R. Stinson, ―Extended capabilities for visual cryptography‖, ACM Theor. Comput. Sci., Vol.250,pp. 143-161,2001.

[3]. E. R. Verheul & H.C.A. van Tilborg, ―Construction & properties of k out of n visual secret sharing schemes‖, Designs, codes & cryptography, vol.11, no. 2, pp.179-196, 1997.

[4]. 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]. Hwa-Chiug Hsu , Tung-Shou Chen, Yu-Hsuan Lm, *The Ring Shadow Image Technology Of Visual Cryptography By Applying Diverse Rotating Angles To Hide The Secret Sharing*, in Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control, Taipei, Taiwan, pp. 996–1001, March 2004.

[6]. Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, *New Visual Cryptograpgy System on Circular Shadow Image and Fixed Angle Segmentation*, Journal of Electronic Imaging 14(3), 033018 (Jul–Sep 2005).

[7]. Daoshun Wang, FengYi, XiaoboLi, "On General Construction For Extended Visual Cryptography Schemes", Pattern Recognition 42 (2009),pp 3071 – 3082, 2009.

[8]. Siddharth Malik, Anjali Sardana, Jaya, "A Keyless Approach to Image Encryption",2012 international conference on Communication systems and Network Technologies ©2012 IEEE

[9]. Hirdesh Kumar , Awadhesh srivastava, A *Secret Sharing Scheme for Secure Transmission of Color Images*, International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT) 2014.

[10]. 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.

[11]. Mona F. M. Mursi*, May Salama, Manal Mansour**,** "Visual Cryptography Schemes: A Comprehensive Survey", International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-11)

[12]. 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.

[13]. Pallavi Vijay Chavan, Signature Based Authentication using Contrast Enhanced Hierarchical Visual Cryptography, 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science

[14]. Mr. K. A. Aravind, Mr. R .Muthu Venkata Krishnan, *Anti-Phishing Framework for Banking Based on Visual Cryptography*, International Journal of Computer Science and Mobile Applications, Vol.2 Issue. 1, January-2014.

[15]. Ching-Sheng Hsu and Shu-Fen Tu, "Digital Watermarking Scheme with Visual Cryptography", Proceedings of the International MultiConference of Engineers and Computer Scientists 2008 Vol IIMECS 2008, 19-21 March, 2008, Hong Kong

[16]. Chandrasekhara & 2Jagadisha, Secure Banking Application Using Visual Cryptography against Fake Website Authenticity Theft, International Journal of Advanced Computer Engineering and Communication Technology (IJACECT), ISSN (Print): 2278-5140, Volume-2, Issue – 2, 2013

[17]. Yi-Jing Huang, Jun-Dong Chang, Non-expanded Visual Cryptography Scheme with Authentication, IEEE 2nd International Symposium on Next-Generation Electronics (ISNE) - February 25-26 , Kaohsiung , Taiwan.

[18]. C.Yang and C. Laih, "New Colored Visual Secret Sharing Schemes". Designs, Codes and cryptography, 20, pp. 325–335, 2000.

[19]. 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.

[20]. Hwa-Chiug Hsu , Tung-Shou Chen, Yu-[3]Hsuan Lm, *The Ring Shadow Image Technology Of Visual Cryptography By Applying Diverse Rotating Angles To Hide The Secret Sharing*, in Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control, Taipei, Taiwan, pp. 996–1001, March 2004.

[21]. Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multi-Secrets Visual Secret Sharing", Proceedings of APCC2008, IEICE, 2008.

[22]. P.S.Revenkar, Anisa Anjum, W .Z.Gandhare, "Survey of Visual Cryptography Schemes", International Journal of Security and Its Applications Vol. 4, No. 2, April, 2010

[23]. P.S.Revenkar, Anisa Anjum, W .Z.Gandhare Secure Iris Authentication Using Visual Cryptography,(IJCSIS) International Journal of Computer Science and Information Security,Vol. 7, No.3, 2010

[24]. Megha B. Goel, Vaishali B. Bhagat, Veena K. Katankar, "Authentication Framework Using Visual Cryptography", International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308