Visual Cryptography: A Review

Dipesh Vaya
Department of CSE
GITS, Udaipur

Sarika Khandelwal
Department of CSE
GITS, Udaipur

Teena Hadpawat
Department of CSE
CTAE, Udaipur

ABSTRACT

In today's world handling and security of information from attacks becomes very important aspect for the individuals. Researchers are innovating new techniques to secure the information from unwanted intrusions. Various cryptography techniques are discovered and many are yet to be revealed. Here in this paper we are going to review an advanced method of information hiding i.e. Visual Cryptography. Visual Cryptography emerged as a special encryption technique for information hiding using images. In way that encrypted image can be decrypted by the human vision if the correct image key is used. By this cryptographic technique we can encrypt visual information (pictures, text, etc.) in a way that human visual system can perform decryption of encrypted information & no aid of computers needed. In visual cryptography a secret image is transformed into several share images. These share images are meaningful but noisy or distorted images. Combination of these share images can reveal the original secret image.

This paper reviews two methods for visual cryptography of color images based on Shamir encryption method variants of k-out-of-n i.e.2-out-of-2, 2-out-of-n, n-out-of-n, and k-out-of-n scheme encryption method.

Keywords

CAPTCHA, Color Decomposition, Color Visual Cryptography, MD5, SHA, Meaningful Shares..

1. INTRODUCTION

The concept of Visual cryptography firstly implemented by Naor & Shamir in 1994 [1]. They conceptualized a completely new and secure method for secret sharing. According to them a secret image can be split into n shares in encryption phase. And while decryption a person should have all n shares to reconstruct the secret image. The beauty of this method was that any n-1 shares are not capable to reveal the secret image. When all n shares were superposed, the initial image would seem. Image which will be thought of for Visual Cryptography may be Binary Image, Grayscale Image and Color Image. The technique given by Naor and Shamir for sharing a secret binary image was by mistreatment their own cryptography table. During this process the binary image is split into 2 shares, for the white component within the secret image, one in all the higher 2 rows of table 1 is chosen to create share1 and share2. Pixel expansion is the main feature in which each pixel of the secret image is extended to four pixels. So, regenerated image will be 4 times the original secret image as the pixels are extended to four pixels. By imposition of all shares together will generate a four times larger image than the original secret image. But the resolution quality will be degraded of reconstructed image than the original secret image due to decomposition of each white pixel. The decomposition process includes decomposition of each white pixel into two black and two white pixels.

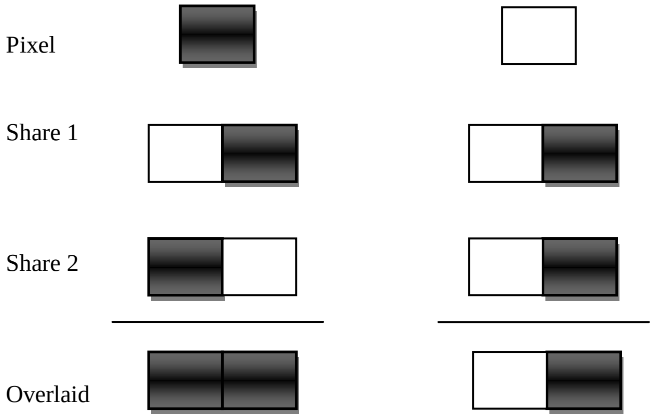


Fig. 1 Encoding of pixels

2. REVIEW OF LITERATURE

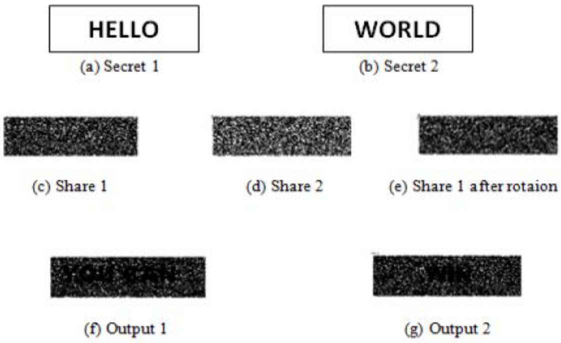
Different scientist has worked on the theme planned by Nair and Shamir to boost the performance. In 1994 visual cryptography scheme have been proposed by Naor & Shamir [1]. This can be the essential theme of visual cryptography within which the key image is split into 2 shares. The shares generated area unit unimportant. Once the 2 shares area unit stacked along, it produces the first secret image. This theme is merely for black & white pictures.

An extension of visual cryptography was proposed by Ateniese, Blundo & Stinson [2] in 1996. This scheme contains significant shares. The (2,2) EVC theme projected throughout this required enlargement of 1element at intervals the initial image to four sub pixels which can then be chosen to produce the required pictures for each share. Up to 1997, Visual cryptography schemes were applied to solely black & white images. First colored visual cryptography scheme was proposed by Verheul & Tilborg [3]. The shares generated by this scheme were meaningless. In 1998, Wu and Chen [4] work on the visual cryptography schemes to share two secret images in two shares. An another scheme was proposed by Hsu et al [5] in 2004, The scheme was about hiding two secret images in two share images with arbitrary rotating angles. One more method was proposed by Verheul and Van Tilborg [3]. In this paper, a scheme for colored secret images can be shared is proposed. In this the concept of arcs was used to construct a colored visual cryptography theme. the multiple secrets sharing in visual cryptography was first proposed by S J Shyu et al [11]. This theme encodes a group of n ≥ two secrets into 2 circle shares. The n secrets are often obtained one by one by stacking the primary share and also the rotated second shares with n totally different rotation angles. In [8] a new method for processing halftone images that improves the quality of recovered secret images in a VC scheme had been proposed. Later, in year 2016 [10], we proposed hardware efficient visual cryptography scheme. It optimizes time for image transmission. For reduction in time, modification of Shamir's equation was done.

3. VISUAL CRYPTOGRAPHY SCHEMES

3.1 For Binary Images

Wu and Chen [4] in 1998 were the first researchers to present the visual cryptography schemes to share 2 secret images in 2 shares. During this scheme 2 secret binary images were thought of that were hidden into 2 random shares, specifically share A and share B. In retrieving section the primary secret image is disclosed by stacking the 2 shares, denoted by A XOR B, and therefore the second secret is discovered by initial rotating share A by angle Ө anticlockwise.



(a) Secret 1 (b) Secret 2

(c) Share 1 (d) Share 2 (e) Share 1 after rotaion

(f) Output 1 (g) Output 2

Fig 2: Sample example for hiding secret images

Above scheme relies on rotation angle for the image and unimportant shares. to beat the angle restriction in above scheme, in 2004 Hsu et al [5] proposed another scheme. in this scheme 2 secret images are hidden in 2 share images with impulsive rotating angles. 2 confidential data sets are encrypted into shadow images beneath totally different overlapping angle using the encrypting Table II of 2x2 enlarged pixel squares given below [5]. This is one among most promising approach of visual cryptography.

3.2 For Color Images

3.2.1 For Single Secret Sharing

Till 1997 visual cryptography schemes were applied to solely black and white pictures. Verheul and Van Tilborg [3] developed colored visual cryptography scheme. Colored images are extremely popular in use, colored secret pictures are often shared using this method; the idea of arcs was accustomed construct a colored visual cryptography theme. As color pictures are very renowned, in c-colorful visual cryptography scheme one picture element is remodeled into m sub pixels, and every sub picture element is split into c color regions. In every sub picture element, there's precisely one color region colored, and every one the opposite color regions are black. The color of 1 picture element depends on the interrelations between the stacked sub pixels. For a colored visual cryptography theme with r colors, the picture element growth m is r× three. These schemes share generated were unimportant.

3.2.2 Keyless Visual Cryptography

The color image is taken into account here, the shares thus generated using this method reveal no information regarding the first secret image and to retrieve the key image all the shares are required. The planned technique is enforced with the Seiving-Division-Shuffling rule planned in this paper and involves 3 steps. In the first step seiving the key image is split into primary colors. In step 2 Division these split pictures are haphazardly divided. In step 3 Shuffling these divided shares are then shuffled each inside itself to get final random shares.

4. APPLICATIONS OF VISUAL CRYPTOGRAPHY

Visual cryptography method is proved to be a secure and reliable cryptographic method and hence application of this method has increased. Here we are discussing some of applications

4.1 Watermarking

Watermarking process includes the technique of visual cryptography. Process consists of two steps.

1. Watermark embedding:
2. Watermark retrieving.

In the process of embedding splits the watermark into shares with the help of visual cryptography technique. After this the host image and one share is embedded together on the basis of frequency domain of host image, and another share is kept by the owner [12]. To claim the original image, owner has to extract another share from image. The combination of extracted share and owner's share generates original image.

4.2 Anti- Phishing Systems

Credential information such as security pins, debit credit card numbers and passwords are crucial information and can be theft by intruders. And phishing is used highly to steal secret credential from their owners. To save from phishing attacks cryptography technique can be applied. Use of visual cryptography provides the confidence of security to user while using any website. By imposing the two shares, one received from server site and second his own share, user can ensure a website without phishing [13].

4.3 Human machine identification

Kim et al. [14] proposed human/terminal machine identification technique. A more generalized form was extended by Kim after Katoh and Imai's [15] scheme.

4.4 Secure Banking Communication

In a core banking industry, there's an opportunity of encountering forged signature for transaction. And in the web banking system, the password of client is also hacked and exploited. In [16] a scheme is proposed for securing the client information and to stop the doable forgery of password hacking. The idea of image processing, in visual cryptography is employed**.**

4.5 Defense System

Visual Cryptography scheme is an encryption technique that uses combinatory techniques to code secret written materials. this can be terribly helpful in defense system to guard terribly sensitive data, once information like secretor any code is to transferred from one place to a different that secret data is it can hidden in cover image, the share of the image is to be regenerate into shares. Those multiple shares is unbroken with multiple partners. any one partner cannot retrieve the secret code from the one share he has, all the shares from all the partners are needed to retrieve secret data hidden within the image. so information is safe in hands all the partner.

4.6 CAPTCHA

CAPTCHA was proposed in [8] as a technique for authentication supported Visual Cryptography. It stands for completely automated Public Turing test to tell Computers and Humans Apart (CAPTCHA). Their method consists of 3 processes:

4.6.1 *Share Creation Process:*

User registers by furnishing their credentials like name, date of birth, address, PIN, etc [8]. These credentials are hold on within the information. The secret personal identification number provided by the user can act as a basis for the creation of the CAPTCHA image distinctive in nature. The CAPTCHA is then divided into 2 shares. One share is hold on within the information and also the alternative is given to the customer [8].

4.6.2 *Hash Code Generation:*

MD5 is employed for the hash code generation. MD5 transforms a variable length message into a fixed length output of 128 bit. The input message is divided into blocks of 512 bits. The message is padded in such how that its length becomes fully separable by 512 [8].

4.6.3 *Authentication Process:*

The client must offer his share for any dealing. A hash code is generated for the share and also the value is compared with the value already stored within the database [8]. If a match happens, the client share is stacked with the share present within the database server. The stacked image is then processed to get rid of any noises. Then the authentication testing is finished to just accept or reject the user.

4.7 Offline QR Code Authorization

Fang [6] proposed an algorithmic rule for the authentication of offline QR (Quick Response) code. He used Visual Secret Sharing Scheme for the authentication. A QR code is matrix barcode that is readable by specific readers dedicated to QR code [6]. The code consists of a white background on that black modules are organized in an exceedingly square pattern. The information that's encoded in an exceedingly QR code will be any text or URL or the other information [6].

There are five vital options of a QR code [6]:

(i) High capability coding of data.
(ii) Tiny output signal size.
(iii) Dirt and harm resistance.
(iv) Readable from any direction in
(v) A structure append feature.

5. ANALYSIS OF VISUAL CRYPTOGRAPHIC SCHEMES

Following table summarizes the various Visual Cryptography schemes in terms of their merits and demerits. Factors like types of share generated, form of image thought-about, range of secret pictures, range of shares shaped, form of range of shares, and also the technique employed in these Visual Cryptography schemes.

Table 1: List of various Visual Cryptographic Schemes

Author	Type of Image	Types of Shares Generated	No. of Secret Images
Naor & Shamir, 1994 [1]	Binary	Meaningless	1
Ateniese, Blundo & Stinson, 1996 [2]	Binary	Meaningful	1
E.R. Verheul & Ven Tilborg, 1997 [3]	Colored	Meaningless	1
Wu & Chen, 1998 [4]	Binary	Random	2
Hsu at el, 2004 [5]	Binary	Meaningless	2
Daoshun Wang, 2009 [6]	Binary, Grayscale, Color	Meaningful	n>=1
Siddharth Malik,Anjali Sardana, Jaya, 2012 [7]	Colored	Random	1
Hirdesh Kumar, Awadhesh Srivastava, 2014 [8]	Colored	Meaningful	1
Dipesh vaya, Sarika Khandelwal, 2016 [9]	Colored	Meaningless	n>=1

6. CONCLUSION

The significance of securing data in communication is the motivation behind learning numerous visual cryptography schemes. Visual Cryptography (VC) is a cryptography scheme used to share secret image. It encodes image into n shares. These shares are either written on transparencies or are encoded and hold on in a digital form. All the shares are needed to retrieve secret data. There are several factors, which decide performance of those schemes. The factors considered are types of image, types of share generated and number of secret images. The table of comparison is given in this paper to summarize the various options of every technique reviewed. As mentioned in numerous applications systems are created safer and reliable by the appliance of visual cryptography techniques.

7. REFERENCES

[1] Naor, M. and Shamir, A. 1995. Visual Cryptography, in Advances in Cryptology – Eurocrypt. A. De Santis, Ed., Vol. 950 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, pp 1-12, 1995.

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

[3] Verheul, E. and van Tilborg, H. 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. and Chen H. A Study On Visual Cryptography, Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[5] Hsu, H., Chen, T. and Lm, Y. 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] Wang, D. Feng, Y. and Xiaobo, L. On General Construction For Extended Visual Cryptography Schemes, Pattern Recognition 42 (2009), pp 3071 – 3082, 2009.

[7] Malik, S. Jaya, A. A Keyless Approach to Image Encryption,2012 international conference on Communication systems and Network Technologies ©2012 IEEE

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

[9] Vaya D., Khandelwal S. (2016) A Fast and Hardware-Efficient Visual Cryptography Scheme for Images. In: Advances in Intelligent Systems and Computing, vol 379, pp. 133-142, Springer, New Delhi

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

[11] Warren, H., Akhawe, D., Jain, S. Shi, E. and Song, D. Shadowcrypt: Encrypted web applications for everyone. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pp. 1028-1039. ACM, 2014.

[12] Reddy, L., and Munaga P. Extended Visual Cryptography Scheme for Multi-secret Sharing. In Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics, pp. 249-257. Springer India, 2016.

[13] Kim, M., Park, J. and Zheng, Y. Human-machine identification using visual cryptography. In Proceedings of the 6th IEEE International Workshop on Intelligent Signal Processing and Communication Systems, pp. 178-182. 1998.

[14] Katoh, T., and H. Imai. An Application of Visual Secret Sharing Scheme Concealing Plural Secret Images to Human Identification Scheme. In Proc. of SITA, vol. 96, pp. 661-664. 1996.

[15] Chandrasekhara and Jagadisha, 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.