Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 4, April 2015, pg.5 – 9

RESEARCH ARTICLE

Implementation of Different Schemes of Visual Cryptography

[1]Snehal N.Ghule, [2]Rupali R.Bathe, [3]Jyoti D.Thomabre, [4]Swapnali S.Misal

[1234]Computer Engineering Savitribai Phule Pune University, Trinity Academy of Engineering, Pune, India – 411038

[1] Snehalghule@gmail.com, [2] Bathe.rupali91@gmail.com

[3] Adhya.thombare09@gmail.com, [4] swapnalimisal@ymail.com

Abstract*— Visual cryptography (VC) is a secret sharing scheme in which an image is converted into shares.VC uses two transparent image, one image contains random pixels and other image contains the secret information.VC is a cryptographic technique which allows visual information (picture, text, etc.) to be encrypted. This survey reviews the different methods of visual cryptography. No information can be revealed by observing any share. Different significant research advances are identified in this paper to ease reader to sort out similarities and differences in various methods of VC. Presented research gives a brief idea about VC, how to generate secret shares and to verify generated shares. Depending on extent of security of VC is decided.*

Keywords*— Secret shares, Stacking , Visual Cryptography (VC), Cryptographic Scheme, Encryption, Decryption*

I. INTRODUCTION

Visual cryptography (VC) is technology which is developed to confidentially share pictures and knowledge with encryption or decryption key. VC method grips any private image, divides it into elements which are called as "shares". These shares are published on a unique sheet of material (transparencies). When these shares are combined together, the image can be revealed easily using VC, without any calculation. The weighty point in this technology is a single share alone cannot display information of private image. This provides more security. Binary, grey and colourful images widely used in VC. VC gives a basic way for sharing confidential binary pictures using their own coding table. The binary image is partition into two shares. If the pixel in the secret image is white one of the upper two rows of table is chosen to make share1 and share2 If the pixel in the secret image is black, one of the lower two rows of table is chosen to make share1 and share2. Each share pixel is convert plain text into two white and two black pixels.

Every share alone cannot provide, clue about pixel whether the pixel is black or white. . Visual Cryptographic is one of the new techniques which provide information security. This allows visual information like pictures to be encrypted in such a way that their decryption can be performed by human visual system without any complex algorithms. This is known as (k, n) VC schemes where k represents minimum no of shares needed to decrypt the secret image and n is the total number of shares generated by the visual cryptographic scheme [4].

VC process can be summarized as:

Plain text [in the form of image]
↓
Encryption [creating shares]
↓
Channel [Fax, E-mail]
↓
Decryption [Human visual system]

Although the Visual cryptography system was designed especially for remote Internet voting, nothing prevents it from being deployed for poll-site or kiosk voting, depending on the security requirements.

II. RELATED WORK

A. *Visual cryptography schemes*

The information about the original image will be revealed only after stacking sufficient number of shares. There are various schemes present in VC, 2 out of 2, k out of n, n out of n. n*m matrices are mostly used in construction of visual cryptography schemes.

2 out of 2 VC Scheme-

This type of VC scheme the secret image is divided into two shares based on the matrix obtained after representing black and white pixels in grey scale image. This type of scheme mainly used in major application such as Internet voting system [9]. Internet voting system uses the 2 out of 2 scheme for the authentication purpose. To detect the original image these two shares are required to be stacked together [10].

TABLE I

CONSTRUCTION OF 2 OUT OF 2 SCHEME

Original Pixel	Pixel Value-e	Share1	Share2	Share1+ Share2
□	0	■□	■□	□■
□	0	■□	□■	■□
■	1	□■	■□	■
■	1	□■	■□	■

The pixel selection is random so that the shares S_1 and S_2 consist of equal number of black and white pixels. Therefore, by inspecting a single share, one cannot identify the secret pixel as black or white. This method provides perfect security. In visual cryptography, the white pixel is represent by 0 and the black pixel by 1.

Basic matrices for the 2 out of 2 VCS. S0 and S1 are designed as follows:

$$S0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$$

$$S1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

The relative difference α and contrast β, for the above basis matrices can be computed as:

$$\alpha = ½$$

$$\beta = 1$$

n out of k Visual Cryptography

This kind of scheme allows dividing a secret image (secret data) into k number of shares. Then the secret image can be revealed from any n number of shares among k. For example, In 3 out of 6 VC scheme, any 3 shares out of 6 shares are sufficient to reveal the secret data. The major problem associated with this scheme is that the user needs to maintain many shares which may result into loss of shares. Also more number of shares means more memory consumption. The *k-out-of-n* visual cryptography can be illustrated by a *3-out-of-6*-VCS case. The starting matrix SM designed as:

$$SM = \begin{bmatrix} a1 & a2 & a3 \\ a1 & a3 & a2 \\ a2 & a1 & a3 \\ a2 & a3 & a1 \\ a3 & a1 & a2 \\ a3 & a2 & a1 \end{bmatrix}$$

For the above basis matrices, the relative difference α and contrast β are computed as:

$$\alpha = {}^{1}/_{12}$$

$$\beta = 1$$

k out of k Visual Cryptography

Here original secret is divided into k number of shares. For reconstruction of the secret, all k shares are necessary. For example, in 3 out of 3 VC scheme, Secret is revealed only after stacking all the 3 shares, where k= 3. This scheme is not so popular because managing k number of shares is difficult task and it also increases time complexity. The *k-out-of-k* visual cryptography can be best described by considering a *3-out-of-3* VCS case.

The basis matrix S0 and S1 is designed as :

$$S0=\begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$S1=\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

For the above basis matrices, the relative difference α and contrast β are computed as:

$$\alpha = {}^{1}/_{4}$$

$$\beta = 1$$

B Method of Encryption and Decryption

A voter visits the election web site and enters the type able username. The election web site maintains a list of the username values used to generate the transparencies and checks that the entered key is on the list and has not been used already (extensions that would allow a voter to change a previously cast vote are possible but not considered here). If the entered username is valid, the election server can calculate the corresponding transparency image. The election server then generates a random string to use as a password, and generates an image containing that string rendered as a bitmap image. The complementary image to the password image for the voter's transparency is generated and displayed on a web page returned to the voter. After the web server displays the corresponding image generated from username, the voter combines both the transparency to reveal the password as shown in Fig [8].

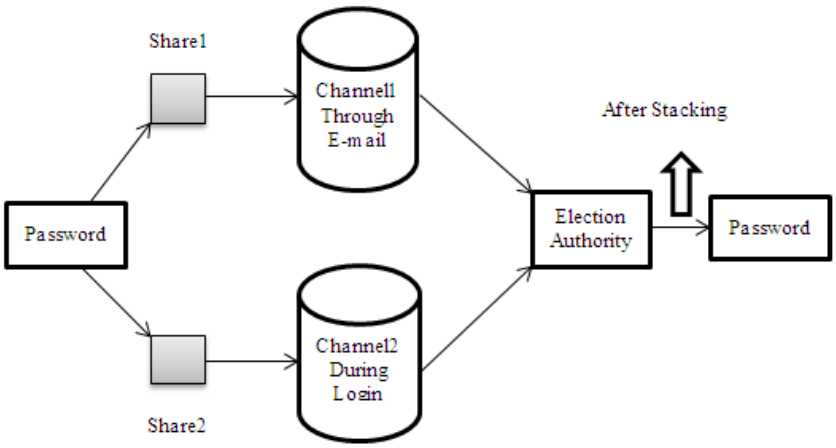

Fig. 1 Encryption and Decryption

Algorithm to continue the voting process, the voter enters the revealed password. This protocol serves to both authenticate the voter to the election server and the election server web site to the voter. Only someone with the correct username transparency could decode the password in the generated image; Algorithm to continue the voting process, the voter enters the revealed password. This protocol serves to both authenticate the voter to the election server and the election server web site to the voter. Only someone with the correct username transparency could decode the password in the generated image. In addition, we suspect from anecdotal evidence (but no scientific user studies yet) that nearly everyone will find the process of revealing a secret by holding a transparency up to an image on a monitor to be a satisfying and reassuring experience. Previous studies have analysed how much a user needs to know in order to make rational decisions in the security of computer services, and the users showed they did not have a solid grasp on the security aspects of the system. With our system, voters do not need to understand how visual cryptography works, but are directly involved in performing the decryption in an intuitive and physical way. Our authentication scheme ensures that the voter cannot continue with the voting process without also verifying the server is legitimate.

III. CONCLUSIONS

In this paper we have studied the different schemes of visual cryptography and described how to implement them we have done the comparative study of the above schemes and concluded that as the number of shares increases, the security as well as complexity increases.2 out of 2 is simple to implement but provides less security. for more secure applications , one can choose k out of n or n out of n Visual cryptography schemes .

Acknowledgement

We express deepest gratitude to our project guide Prof. S.G.Nandanwar, who modeled us both technically and morally for achieving greater success in life. As a men- tor and torchbearer, she guided us to overcome the odds and evens faced during the project work. The supervision and support that she gave indeed paved the path for the smooth completion of the project. We are deeply indebted to our Head of the Department Prof. S.N.Maitri and to our Project Co-ordinator Prof. C.P.Kedia for their unwavering moral support and motivation during the entire course of the project. We would also like to thank our Principal Dr. V.J.Kakhandki who encouraged us and created a healthy environment for all of us to learn in best possible way. We also thank all the staff members of our college and technicians for their help in making this project a successful one.

REFERENCES

[1]Adi Shamir (1979), "How to share a Secret", Communications of the ACM, pp .612-613.

[2]M. aor and A. Shamir (1995), "Visual Cryptography", Advances in Cryptology-Eurocrypt '94 Proceeding, LNCSvol. 950, Springer-Verlag, pp. 1-12.

[3]Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman, (2012) "Attacking the Washington, D.C.Internet Voting System", n Proc. 16th Conference on Financial Cryptography & Data Security,pp .1-18

[4]Moni Naor and Adi Shamir, *Visual Cryptography*, Advances in cryptology– Eurocrypt, pp 1-1995.

[5]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.

[6]Hussein Khalid Abd-alrazzq1, Mohammad S. Ibrahim2 and Omar Abdurrahman Dawood (2012), "Secure Internet Voting System based on Public Key Kerberos", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 3, pp. 428-434.

[7]Adhikari Avishek and Bimol Roy (2007) "Applications of Partially Balanced Incomplete Block Designs in Developing (2,n) Visual Cryptographic Schemes". IEICE Trans. Fundamentals,Vol.E90–A, No .5 , pp. 949-951

[8]Marek R.Ogiela, Urszula Ogiela(2009) "Linguistic Cryptographic Threshold Schemes", International Journal of Future Generation Communication and Networking.Vol.2, No.1,pp. 33-40

[9]Carlo Blundo, University of Salerno, Alfredo De Santis andDouglas R Stinson (1998), "On the contrast in visual cryptography scheme".pp. 1-28

[10]Thomas Monoth, Babu Anto P (2009), "Achieving optimal Contrast in Visual Cryptography schemes without pixel expansion". International Journal of Recent Trends in Engineering, Vol 1, No 1, pp. 468-471.

[11]Pallavi V Chavan, Mohammad Atique, and Anjali R Mahajan, (2011) "An Intelligent System for Secured Authentication using Hierarchical Visual Cryptography-Review", ACCE Int J. on Network Security, vol. 02, No. 04.pp. 7-9

[12]Rajendra Basavegowda, Sheshadri Seenappa(2013) "Electronic Medical Report Security Using Visual Secret Sharing Scheme",IEEE UKSim 15th International Conference on Computer Modeling and Simulation Proceedings, pp, 78-83

