Hierarchical Visual Cryptography Applications: A Review

Ms. Pratima Mahamuni[1], Dr. A.S. Hiwale [2]

[1]Research Scholar, Dept of E&TC Engg, GSMCOE, SPPU, Pune, Maharashtra, India
[2]Professor, MITCOE, SPPU Pune, Maharashtra, India

Abstract: **Visual cryptography is a cryptographic secret sharing scheme which allows secret visual data to be encrypted in such a way that only after decryption process we can get original secret information without the aid of computers. There are various measures on which performance of visual cryptography scheme depends, such as pixel expansion, contrast, security, accuracy, computational complexity, share generated is meaningful or meaningless, type of secret images and number of secret images encrypted by the scheme. This paper is on study and performance analysis of the visual cryptography schemes on the basis of pixel expansion, image format and type of shares generated. This paper describes the novel idea of hierarchical visual cryptography on basis of VC. The key concept behind hierarchical visual cryptography is to encrypt the secret information in number of levels. As the number of levels in hierarchical visual cryptography increases, the secrecy of data tends to increase. The keyshare generated out of Hierarchical visual cryptography is found to be random giving no information and the original secret size is retained in the shares at all levels.**

Keywords: **VC, Hierarchical VC, secrecy, shares, Expansionless.**

I. INTRODUCTION

In today's digital world, information sharing and transfer is increased exponentially. With rapid advancement of multimedia information and communication system, various confidential data such as military maps, commercial identification are transmitted over the Internet. While using secret (confidential) data, security issues should be taken into consideration i.e. data needs to be protected from unintended recipients. Establishing trust is very important in human and digital network. So providing security, in this paper we review performance of Hierarchical VC on basis of Visual cryptography.

Visual Cryptography is a type of secret sharing encryption technique which was developed to secretly share images and information without using encryption or decryption keys. This technique simply takes the secret image, data, divides it into parts; each part is called "share". When these shares are superimposed together, the secret image can be revealed easily and no need for calculations or computations. The important point in this concept is that every share alone can reveal no information about the secret image. Three types of images are used in VC; binary, gray and color images. Visual cryptography (VC) scheme is secure and very easy to implement. Visual cryptography possesses these characteristics: 1) security 2) Decryption (secret restoration) without the aid of a computing device 3) Robustness against lossy compression and distortion due to its binary attribute. Following figures shows 2 by 2 Visual cryptography secret sharing scheme

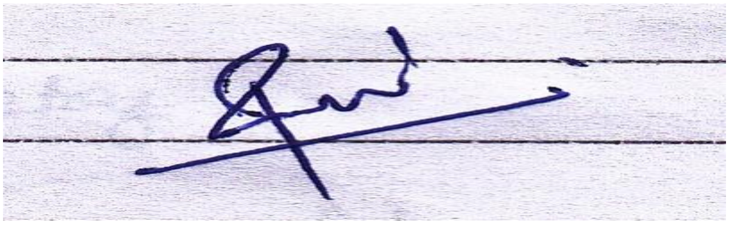

Fig.1: Secret image

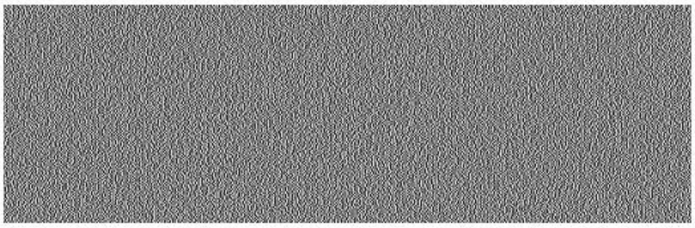

Fig.2: Share1

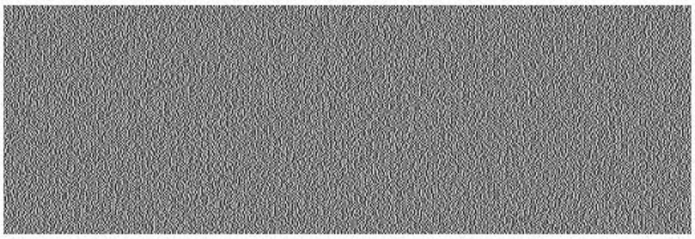

Fig.3: Share 2

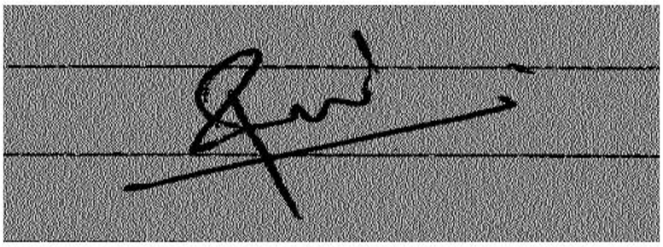

Fig.4: Revealed secret image

Visual cryptography was first introduced by Moni Naor and Adi Shamir in 1995 at [1]. They produced a basic scheme for sharing a secret binary image. The binary image is divided into two shares. If the pixel in the secret image is white, 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 1 is used to make share1 and share2. 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.

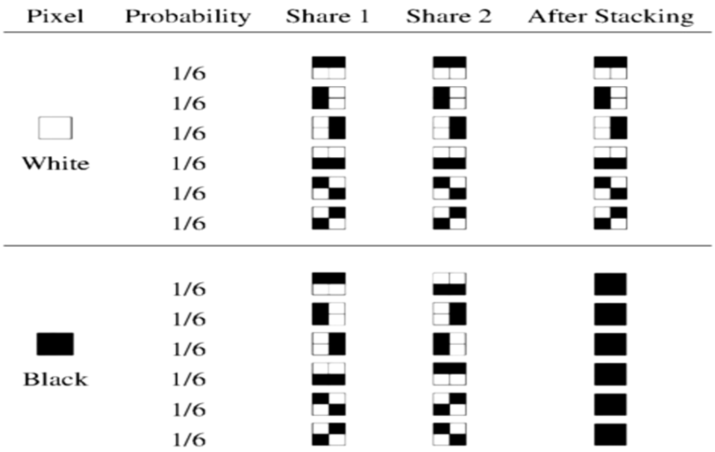

Fig.5: Illustration of a (2, 2) VC scheme.

1.1 RELATED WORK:

In 1995 Naor and Shamir have introduced first time to solve the secret sharing problem by cryptographic structure called Visual Cryptography (VC). In the proposed approach the secret is divided into two shares, which are printed onto the two transparencies (shares) and given to the participants. Only these two participants who possess the transparencies can reconstruct the secret by superposition of shares. One cannot recover a secret without the other one. In the visual threshold scheme, the shares are images represented on transparencies consisting of black and white (transparent, actually) pixels. The visual systems perform a Boolean OR operation, which is easy to visualise using the (2, 2)[1]. Y.V. Subba Rao and P.S. Revenkar trying to introduce an visual cryptography and application based Authentication system to improve the security and cost of the overall process on basis of biometrics like fingerprint, iris. His approach is to enable the completely synchronized combination of VC , the fingerprint or iris scanner and ID card system. Considering fingerprint or iris as a secret image, this distribute it among the two shares [2][3]. George Abboud introduced Stereography and visual cryptography concepts were combined by to share the hidden message for achieving improvement in security ,reliability. He also compare different methodologies for same. He gives the quite novel idea but increased complexity during the computation of shares[4]. Pratiksha Patil implemented new technique of halftone visual cryptography to encode a secret binary image into halftone share carrying significant visual information. This method overcome problem related to extended visual cryptography[5]. Pallavi V Chavan applied this hierarchical VC in authentication system to increase secrecy. She also gives technique to reduce expansion problem [6][10].Manimurugan.S define drawback of VC and also gives idea to remove pixel expansion. By using modified RLE compression [7]. Sathiya K says compare different images as input to VC technique to increase quality of revealed image after XORing decoding[8]. Chandrasekhara applies hierarchical VC in Banking system to protect bank against unauthorized person and maintain secrecy [9]. Ruchita Tekade and Jonathan Weir,WeiQi Yan gives no. of application of Visual cryptography[13][14].

1.2 PROPOSED SYSTEM:

VC is used in different system to maintain secrecy of that system. Bur the drawback of VC is graying effect and pixel expansion. New idea propose here is, Hierarchical VC, which encode secret image of different format into two level VC and increase security and reduce graying effect and pixel expansion. Small size of pixel expansion converted small size of shears. Information gray and color image format should be encoded by the schemes. Other performance measures such as contrast, accuracy, security and computational complexity that affect the efficiency of visual cryptography

Following figure indicates hierarchical visual cryptography encoder. Original secret is an input to the system. Two shares are generated out of expansion less visual cryptography module. These two shares are independently encrypted. Key share generator module is responsible for generation of key share. Key share is combination of first three shares taken from previous level of hierarchy. Here *A* indicates key share and *B* indicates remaining share.

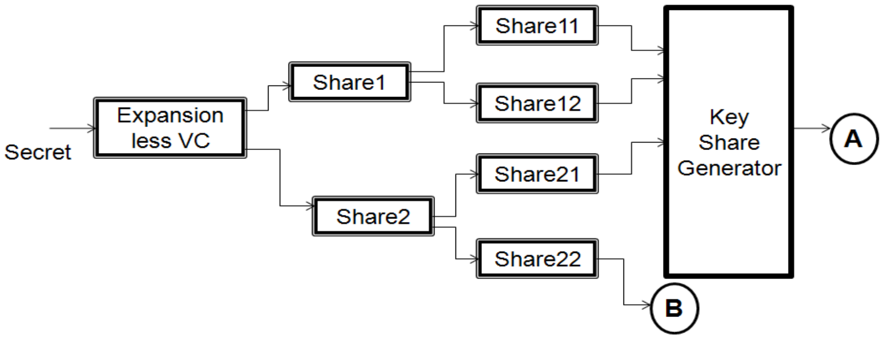

Fig.6: Encoding process of Hierarchical VC

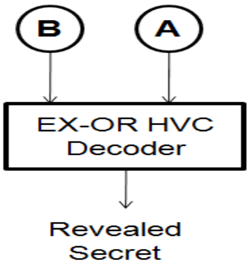

Fig.7: Decoding process of HVC

Above figure indicates hierarchical visual cryptography decoder in which shares are superimposed together to reveal original secret[12].

A. Applications of HVC:

1. Moiré pattern: A potential application for VC is its use in conjunction with Moiré pattern induced when a revealing layer dot screen or line is superimposed on top of periodically repeating shape. The resulting pattern is changing geometric parameters characterizing the individual grids.

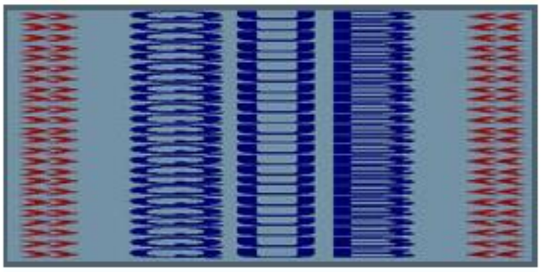

Fig.8: Moiré Pattern

VC has been implemented using Moire patterns.Moire cryptography model embbeded secret image is randomized into two shares, known as preshares.These are independent of the original image.XORing these preshares will recover the original[14].

2. In E voting System: E-Voting solutions generally aim at increasing participation, improving the outcomes elections by addressing challenges associated with traditional voting practices. The notion of e-voting refers to the use of technology to support one or more of the major phases of the electoral process - from registration stage in the pre-voting phase to voting/balloting and verification to counting or tallying after voting, in all this process security is maintained with VC.[13]

3. In academic institute for enroll employee’s presenty: This system is implemented on basis of ID smart card.

4. In banking system: Protect Bank system from unauthorized person. [9]

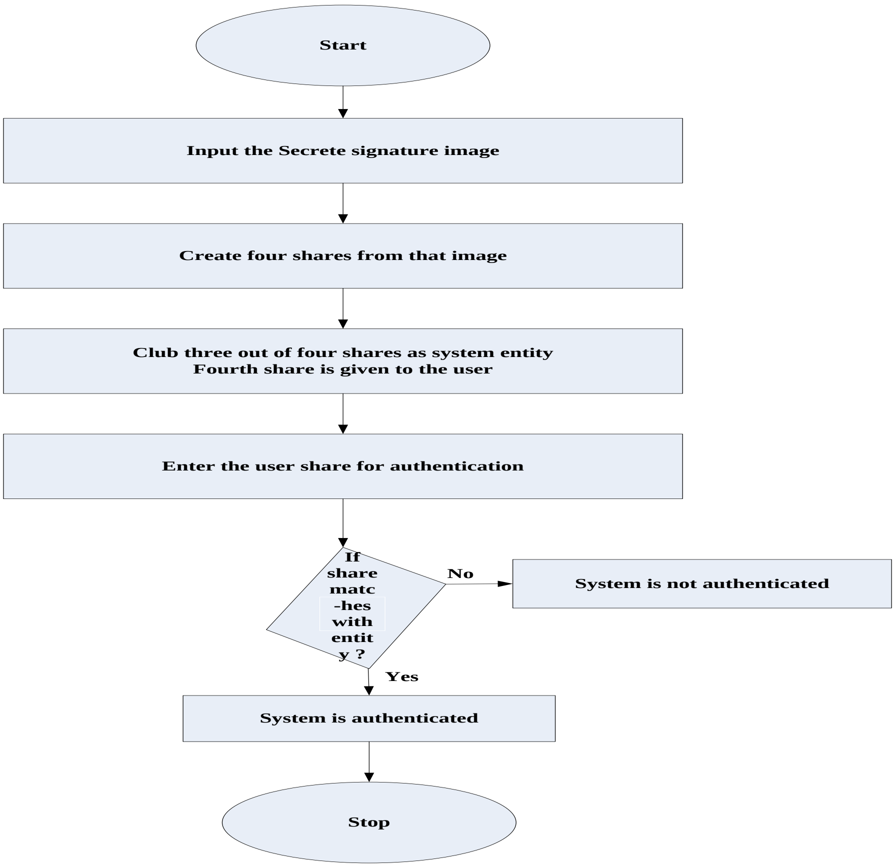
Start
Input the Secrete signature image
Create four shares from that image
Club three out of four shares as system entity
Fourth share is given to the user
Enter the user share for authentication
If share matc -hes with entit y ?
No
System is not authenticated
Yes
System is authenticated
Stop

Fig.9: Data flow Diagram

This is Data flow Diagram which shows authentication for banking system.

2. CONCLUSION

In this paper VC and Hierarchical VC literature has been review as well as a applications of HVC are also highlighted, It is concluded that the share generated out of Hierarchical visual cryptography represents the same size of secret. The keyshare generated out of Hierarchical visual cryptography is found to be random giving no information and the original secret size is retained in the shares at all levels.

REFERENCES

[1] Shamir, “How to share a secret”, Communications of ACM vol. 22, no. 11, pp. 612–613, 1979.

[2] S. Rao, Sukonkina, “Fingerprint based authentication application using visual cryptography methods (improved id card)”, Proceedings of IEEE Region 10 Conference, pp. 1–5, November2008.

[3] P.S. Revenkar, Anisa Anjum, “Secure iris authentication using visual cryptography”, International Journal of Computer Science and Information Security, vol. 7 No. 3, pp. 217–221, March 2010.

[4] Yampolskiy R.V. Abboud G, Marean J, “Steganography and visual cryptography in computer Forensics” Proceedings of 5th IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, pages 25-32, 2010.

[5] Y.M. Patil “Visual Cryptography Based on Halftoning” of IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) ISSN :2278-2834, ISBN : 2278-8735, PP : 65-69

[6] Pallavi V Chavan, Dr. Mohammad Atique “An Intelligent System for Secured Authentication using Hierarchical Visual Cryptography-Review” processing with Int. Joint Colloquium on Emerging Technologies in Computer Electrical and Mechanical,2011

[7] Manimurugan.S, Ramajayam.N “Visual Cryptography Based On Modified RLE Compression without Pixel Expansion” processing with International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 3, September 2012

[8] Sathiya K , Senthamilarasi K , Janani G , Akila victor “Comparison of Visual Cryptographic Algorithms for Quality Images Using XOR” processing with International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) ISSN 2278-6856 Volume 2, Issue 2, March – April 2013

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

[10] Pallavi Vijay Chavan, Dr. Mohammad Atique and Dr. Latesh Malik “Design and Implementation of Hierarchical Visual Cryptography with Expansionless Shares” in International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014

[11] N. Gowdham, S.D. Libin Raja, M. Sornalakshmi, M. Navaneetha Krishnan “Two Step Share Visual Cryptography Algorithm for Secure Visual Sharing” in International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 2 Issue: 3,2014

[12] Vinish Alikkal, Dr.T.Senthil Prakash , Ajmal Hussain “Enhanced Hierarchical Design For Visual Cryptography-Overview” in International Journal On Engineering Technology and Sciences – IJETS™ ISSN (P): 2349-3968, ISSN (O): 2349-3976 Volume 2 Issue 4, April -2015

[13] Ruchita Tekade1, Prof. Reena Kharat2, Varsha Magade3, Marjina Shaikh4, Pallavi Mendhe5,” E-Voting System using Visual Cryptography & Homomorphic Encryption” processing with International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 1, January 2016

[14] Jonathan Weir,WeiQi Yan ,Visual Cryptography and It’s Applications, Ventus Publishing, 2012