Secure Authentication Using Visual Cryptography

Deepti Chaudhary
M.Tech Scholar, CSE Department
SRCOEM
Nagpur, India
chaudharydr@rknec.edu

Rashmi Welekar
Associate Professor, CSE Department
SRCOEM
Nagpur, India
welekarr@rknec.edu

***Abstract -Visual Cryptography* is a cryptographic technique which allows visual information (text, picture, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. Visual Cryptography deals with any type of secrets such as printed or pictures, etc. These secrets are delivered into the system in a digital (image) form. The secrets which are in a digital form divided into different parts based on the pixel of the digital secret. These parts are called shares. To visualize the secret, the shares are then overlapped correctly.This paper introduces secure authentication using Visual Cryptography. In any authentication system the major problem is the authenticity of the customer. Due to unavoidable hacking of the database on the internet, it is always difficult to trust the information on the internet. To solve this authentication problem, we are discussing with the two most important topics based on image processing and visual cryptography.**

Keywords: Authentication, Overlap, Secret, Shares, Sub pixels, Visual Cryptography.

I. INTRODUCTION

The web banking is going to become more popular among young Internet-savvy people for many years, its popularity is expected to grow more rapidly as Internet usage grows internationally and people discover the many advantages that it provides. But it may have its own drawbacks. it is nearly impossible to be sure whether a computer that is connected to the internet can be considered trustworthy and secure or not. The major question is how to handle applications that require a high level of security, such as internet banking and core banking.

In core banking, there is a chance of encountering fake signature for transaction, and in net banking, the password of the customer may be hacked and changed. With the beginning of internet, various online attacks have been reported on today and among them the most common and popular attack is phishing. Phishing is fraudulent attempt usually made through email.

The concept of image processing and an improved visual cryptography is used. Image processing is any form of signal processing for which the input is in the form of an image and the output of image processing may be either an image or a set of characteristics.

One of the well-known techniques has been credited to Moni Naor and Adi Shamir, who developed it in 1994. They defined a visual secret sharing scheme, where an image was divided 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. To decode the image a subset s of those n shares are picked and copied on separate transparencies. If **S** is a qualified subset, then stacking all these transparencies will allow visual recovery of the secret.

The major drawback of this scheme is that visually blind people cannot make use of this technique. The simple example of visual cryptography is shown in Figure –

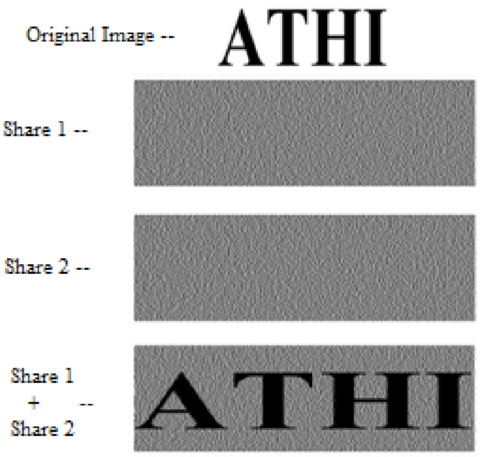

Fig. 1- Example of Share Creation in Visual Cryptography

This paper is organized as follows: Section 2 comprises Some Basic Schemes, section 3 comprises Related Work, section 4 comprises Proposed System and Conclusion is in section 5.

II. SOME BASIC SCHEMES

A. (k, n) visual cryptography scheme

In (k, n) scheme, data suppose D divided into n number of shares and any k or more shares reveal the information about data but even complete knowledge of k-1 shares reveal no information.

B. (2, 2) visual cryptography scheme

In (2, 2) scheme, data is divided into exactly 2 shares and both shares are required to reveal the information about data.

C. (2, 3) visual cryptography scheme

In (2, 3) scheme, data is divided into 3 shares and any 2 shares are required to reveal the information about data.

D. (3, 3) visual cryptography scheme

In (3, 3) scheme, data is divided into 3 shares and all 3 shares are required to reveal the information about data

III. RELATED WORK

The Visual Cryptography was introduced by Moni Naor and Adi Shamir [1] in 1994. According to this algorithm, (2, n) visual cryptography scheme can be solved by the following m×n matrices.

$$Co = \{\text{all the matrices obtain by permuting the columns of } \begin{bmatrix} 100\ldots0 \\ 100\ldots0 \\ \ldots \\ 100\ldots0 \end{bmatrix} \}$$

$$C1 = \{\text{all the matrices obtain by permuting the columns og } \begin{bmatrix} 100\ldots0 \\ 010\ldots0 \\ \ldots \\ 000\ldots1 \end{bmatrix} \}$$

Fig. 2- Share generation by Moni Naor and Adi Shamir

Here matrix C1 refers the matrix for constructing pixels for the black pixels and C0 for the white one.

In year 2000 a neural network based approach for visual cryptography proposed by Tai-Wen Yue and Suchen Chiang [2]. In this technique combination of two pixels are generated with two different options for each pixel with equal probability.

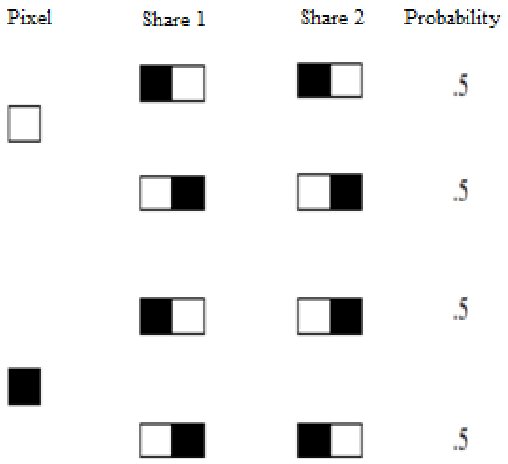

Fig. 3- Share generation by Tai-Wen Yue and Suchen Chiang

Jena and Jena [3] devised a technique for (2, 2) visual cryptography in 2008 where a single pixel generates either two pixels or four pixels in each share.

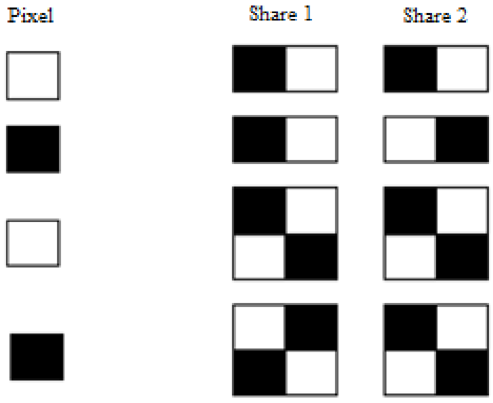

Fig. 4- Share generation by Jena and Jena

In 2008 an algorithm for visual cryptography has been developed by Chetana Hegde, Manu S, P Deepa Shenoy, Venugopal K R, and L. M. Patnaik for Banking Applications [4]. The authors stated that visual cryptography based signature authentication is more secured than password based authentication. The aim of their algorithm was to design an efficient technique for checking authenticity of the customer in core banking and internet banking system. The black pixel is an information pixel denoted by 1 and the white pixel represents background denoted by 0. The initial Boolean matrices for black pixel, S1 and for white pixel, S0 matrix shows for two shares in (2, 2) scheme given below

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

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

Fig. 5- Share generation by Chetana Hegde, Manu S, P Deepa Shenoy, Venugopal K R, and L. M. Patnaik

In 2010 Jayanta Kumar Pal, J. K. Mandal and Kousik Dasgupta developed a (2, n) Visual cryptography [5] where two consecutive pixels had taken at a time as the one time input. If we take n=2, the pixel generation technique by this process is given in the Figure 5.

Pixels	Share 1	Share 2	Probability of Occurance
■■	■□	□■	0.5
	□■	■□	0.5
■□	■□	■□	1
□■	□■	□■	1
□□	■□	■□	0.5
	□■	□■	0.5

Figure 6- Share generation by Jayanta Kumar Pal, J K Mandal and Kousik Dasgupta

Various other algorithms are available for different visual cryptographic schemes, [6,7,8] where efforts have been made to enhance the security. In these cases all customers who hold shares are assumed to be truthful, that is, they will not present any false or fake shares during the phase of recovering the secret image. Thus in all cases the image shown on the stacking of shares is considered as the real secrete image. But, this may not be true in all cases. So, a cheating prevention methodologies are introduced by Yan et al.[9], Horng et al[10] and C M Hu [11]

In 2013, a secure authentication using image processing and visual cryptography for banking application proposed by Chetana Hegde, Manu S, P Deepa Shenoy, Venugopal K R, L M Patnaik [12], their algorithm provide an efficient way to improve security in core banking as well as in internet banking here decrypted image is tested for authentication and correlation technique used for checking the authenticity. This is the best known algorithm so far.

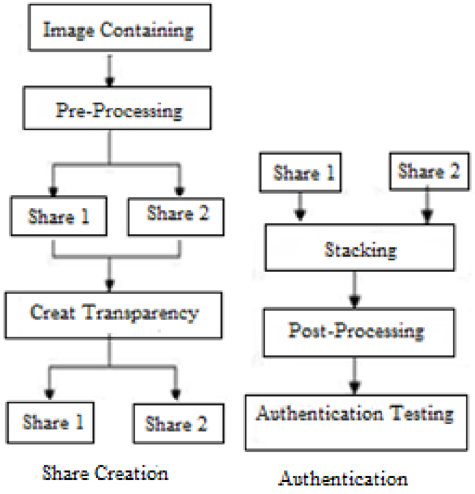

Fig. 7- Share generation by Chetana Hegde, Manu S, P Deepa Shenoy, Venugopal K R, L M Patnaik(II)

IV. PROPOSED SYSTEM

Previous methods in the literature review show good results for black and white or gray scale Visual Cryptography schemes, but they are not sufficient to be applied directly to colour shares due to different colour structures. Here Visual Cryptography Technique is applied on colour images and we will use the concept of Steganography to enhance the security of the system. Steganography is the process of hiding a secret message within an ordinary message and extracting it in its destination

V. CONCLUSION

In the above sections we presented and discussed various algorithms that have been made to enhance the security and that handle applications which require high level of security such as net banking and core banking. It can be used in different fields and different area to enhance security. The individual share is unable to reflect secrecy of the data. The permutations and combinations schemes are failure against the shares. The visual cryptography scheme is also known as secret sharing scheme.

REFERENCES

[1] M. Naor, and A. Shamir, (1994) “Visual Cryptography”, Advances in Cryptography-Eurocrypt '94, vis Lecture Notes in Computer Science 950, pp1-12.

[2] Tai- Wen Yue and, Suchen Chiang (2000) “A Neural Network Approach for Visual Cryptography”, IEEE-INNS-ENNS International Joint Conference on Neural Networks, vol.5,pp 494-499

[3] Jena, and S. K .Jena,(2009) “A Novel Visual Cryptography Scheme”, The 2009 International Conference on Advanced Computer Control, pp-207-211.

[4] C. Hegde, Manu S, P. D.Shenoy, Venugopal K R and L. M. Patnaik (2008), “Secure Authentication using Image Processing and Visual Cryptography for Banking Applications”16th International Conference on Advanced Computing and Communication (ADCOM 2008),MIT Campus, Anna University, Chennai, India, pp. 433-439.

[5] K. Pal, J. K. Mandal and K. Dasgupta (2010) “A Novel Visual Cryptographic Technique through Grey Level Inversion (VCTGLI)” Proceedings of The Second International conference on Networks & Communications, Chennai, India, pp. 124-133

[6] M. Heidarinejad, A. A. Yazdi,; K.N. Plataniotis, (2008) “Algebraic Visual Cryptography Scheme for Color Images” IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 1761 – 1764.

[7] G.R Zhi Zhou Arce,. G. Di Crescenzo (2006) “Halftone Visual Cryptography”. IEEE Transactions on Image Processing. , Volume: 15, Issue: 8pp- 2441-2453

[8] Houmansadr, S. Ghaemmaghami, (2006) “A Novel Video Watermarking Method UsingVisua Cryptography” IEEE International Conference on Engineering of Intelligent Systems, , Islamabad, Pakistan, pp 1-5.

[9] H. Yan, Z. Gan and K. Chen, .A Cheater Detectable Visual Cryptography Scheme,. Journal of Shanghai Jiaotong University, vol. 38, no. 1,2004.

[10] B. Horng, T. G. Chen and D. S. Tsai, .Cheating in Visual Cryptography,. Designs, Codes, Cryptography, vol. 38, no. 2, 2006,pp. 219-236

[11] C. M. Hu and W. G. Tzeng, ”Cheating Prevention in Visual Cryptography” IEEE Transaction on Image Processing, vol. 16, no. 1, Jan-2007,pp. 36-45

[12] Chetanatii Hegde, Manu S, P Deepa Shenoy, Venugopal K R, L M Patnaik “Secure Authentication using Image Processing and Visual Cryptography for Banking Applications” 978-1-4244-2963-9/13/$26 © 2013 IEEE