Visual Cryptography Survey

Rizwan Shaikh
Sinhgad Academy of Engineering, Pune

Shreyas Siddh
Sinhgad Academy of Engineering, Pune.

Tushar Ravekar
Sinhgad Academy of Engineering, Pune

Sanket Sugaonkar
Sinhgad Academy of Engineering, Pune

ABSTRACT

Cryptography is a process of transforming original information into a format such that it is only read by the desired recipient. It is used to protect information from other people for security purpose. Visual cryptography is a method which is used to encrypt information in any format like text, image, led display such that decryption is done by human eye. It does not require any key for decryption. Visual cryptography is mainly of two types segment based visual cryptography, pixel based visual cryptography. Initially this method was developed only for monochrome images then it was upgraded to grey level and then coloured images. As it does not require any key to decrypt that is why this method is unbreakable. This method is useful in vast applications which handle high value assets. It can replace the second factor that is token or key in multifactor authentication system. It can be used in online shopping sites, online banking sites, government sites. This paper gives detailed survey of visual cryptography methods and their applications.

Keywords

Visual cryptography, segment, security, secret sharing.

1. INTRODUCTION

With rapid development in internet technology, different types of information can be transferred over internet. Hence there are security issues associated with transmitting high value assets like commercial data, user personal information, banking or transaction data, data related to military. Security of such data transfer must be taken into consideration because hacker can use various methods and steal such high value assets which results in high monetary, social, personal loss. Various schemes are developed to protect such high value assets. Visual cryptography was developed in 1994 by Naor and Shamir. This method is developed to eliminate the use of decryption key in secure information transformation. In visual cryptography, decryption is done by human visual system hence no need to securely store decryption key. In visual cryptography original image is divided into two parts called as shares. The single share doesn't give any information about original image. When the shares are superimposed together then we can see original image. This method is of two types pixel based and segment based.

2. METHODS

2.1 Pixel based visual cryptography

In pixel based visual cryptography each pixel of original image is divided into two sub pixels such that it does not give any information about original pixel. For this, there is k out of n secret sharing system. In k out of n secret sharing system, image is divided into n shares and given to k users such that any k out of n user can see the original image by superimposing k shares but k-1 users cannot extract any information from it. Now consider 2 out of 2 sharing system. Here image is divided into 2 shares and only original image can be produced by superimposing two shares. Any 1 share does not give any information about original image.

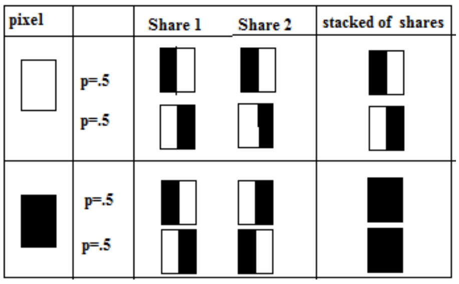

Figure 1: Naor and Shamir 2 out of 2 secret sharing system.

Binary image is divided into 2 shares. Here white pixel is divided into 2 shares as given in the figure 1. There are two choices of generating shares. The black pixel is also divided into 2 shares as given in figure 1. Here every pixel is divided into 4 sub pixel so that when we superimpose the shares it gives original image which less bright. Due to this pixel expansion the reconstructed image will be 4 times the original image.

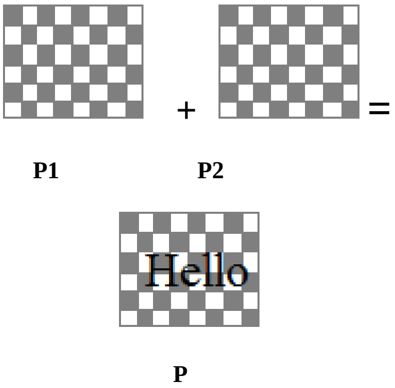

Figure 2

Here in figure 2, from given black and white picture p, two shares p1 and p2 are produced. They are produced randomly. Each white pixel is divided into black and white pixel or black and black pixel. And each black pixel is divided into black and white or white and white pixel. Images p1, p2 shows probability distribution. When the p1 and p2 are superimposed it gives original information "hello". But neither of p1 and p2 alone can reveal original information even if some extensive computations are performed. Hence this method is unbreakable. 2 out of 2 secret sharing system has encryption power of onetime pad.

In above (2, 2) secret sharing system:

1. Secret p= p1 XOR p2

2. p1, p2 can take value (0, 1)

0 XOR 0= 0, 0 XOR 1= 1,

1 XOR 0= 1, 1 XOR 1= 0.

3. Black pixel is associated with binary digit 1 and white pixel is associated with binary digit 0.

4. 0 on 0= (good)

0 on 1= (good)

1 on 0= (good)

1 on 1= (oops)

5. Visual system performs Boolean OR instead of XOR

In (k, n) secret sharing system:

1. k shares are required to reveal the secret.

2. <k shares do not reveal any information.

2.2 Segment based visual cryptography

It is version of visual cryptography which is based on segment and not pixel based images. It is used to encrypt message which is represented by LED display which include digits from 0-9 and literals from A-Z. Advantage of segment based visual cryptography is it is easier to convert images into segment shares which can be easily recognised by human eye in contrast issues.

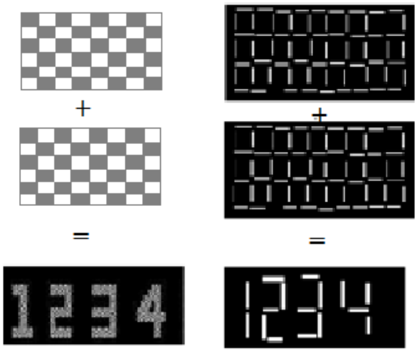

Figure3: Pixel based (left) versus segment based visual cryptography.

In segment based visual cryptography instead of using pixel as smallest unit of encryption, segment of segment display is considered. Most typical segment display is seven segment display which shows the numbers from 0 to 9 as shown in figure 4. Literals A to Z can also be represented.

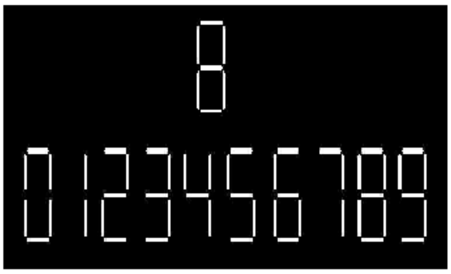

Figure 4: Seven segment display

Segment based visual cryptography is used for messages which are represented by numbers and literals. An example of such message is bank account number, shopping sites password and passwords of any websites.

2.2.1 Principle

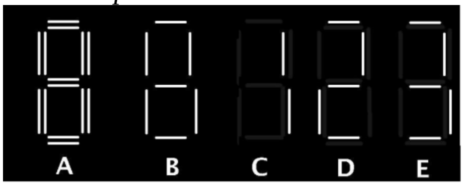

Figure 5: Principle applied to seven segment display.

It uses seven bars, four of them vertical and three are horizontal which together form 8 as shown in figure 4. In this method for each segment s, draw in white on black background segment s1 and s2 which are parallel to each other but do no intersect. See for part A in figure 5 where this is applied to seven segment display. Like pixel based method in which each pixel is divided into two shares here each segment s is divided into s1 and s2 and which is randomly selected for encryption. Selected segment is kept white (transparent) and other parallel segment is turned into background colour which is black in this case. Such random selection is shown in part B of figure 5.

Second share is produced as follows. Assume that certain number is to be shown. Consider subset of segment in symbol that is to be shown.

1. If segment s belongs to this subset then in second share same share s1 or s2 is selected which are selected for first share and other parallel segment is turned black.

2. If segment s does not belong to this subset then in second share other segment is selected and segment which is selected randomly turns black.

In total when these two shares are superimposed we get original segment. In figure 5 part C is second share selected in the way that the set of segment exactly represent 1. Similarly, part D and E of figure 5 shows for digits 2 and 3. Here probability of choosing share is 1/2.

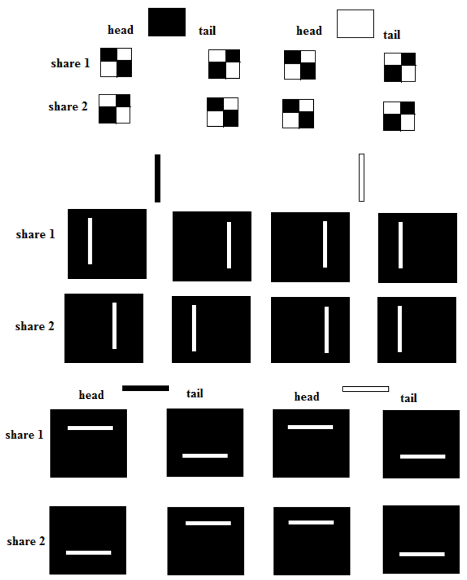

Figure 6: pixel based (above) versus segment based (below) visual cryptography.

3 APPLICATIONS

3.2 In online banking

In banking website visual cryptography can be used for authentication of user. Instead of using TAN transaction number, bank user gets block of shares with number associated with each share from bank server and when user wants to know the transaction information sever asks for share by giving number then this share is superimposed with other one and if they matched then only customer will have the transaction information.

3.3 In anti-phishing framework

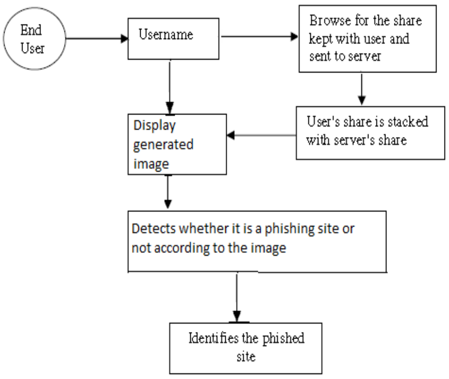
End User
Username
Browse for the share kept with user and sent to server
User's share is stacked with server's share
Display generated image
Detects whether it is a phishing site or not according to the image
Identifies the phished site

Figure 7: Anti-phishing framework

In this user can know whether site is phished or not before entering into the site. Here sever is provided with image which is divided into 2 shares. One share is kept with user and other share is kept with server. At the time of login user have to give their share to server. On superimposing 2 shares if it produces original image then user can detect whether the site is phished or not as shown in figure 7.

4 CONCLUSION

Importance of secretly transmitting high value assets is main motive behind surveying visual cryptography method. There are two methods based on pixel and segment share. No decryption key is required for decryption hence this method is unbreakable. These methods have vast applications in securely transmitting high value assets. There are various bright and innovative extensions exist for visual cryptography. In visual cryptography scheme it is required to increase brightness of decoded image so that it fully resemble with original image.

5 ACKNOWLEDGEMENT

We sincerely thank all authors in reference section. All reference papers are very useful for our proposal. We thank our guide prof. S.S.Vanjire for her comments and our friends for providing their useful and constructive comments.

6 REFERENCES

[1] Ollmann G., “The Phishing Guide Understanding &Preventing Phishing Attacks”, NGS Software Insight Security Research, IBM Global Technology Services.

[2] M. Naor and A. Shamir, “Visual Cryptography,” Advances in Cryptology EUROCRYPT, 1994, Proceeding, LNCS vol. 950, Springer-Verlag, 1995, pp. 1–12.

[3] G. R. Blakley, “Safeguarding Cryptographic Keys”, Proceedings of AFIPS Conference, vol. 48, 1970, pp. 313-317.

[4] B. Borchert, “Segment Based Visual Cryptography”, WSI Press, Germany, 2007.

[5] W-Q Yan, D. Jin and M. S. Kanakanahalli, “Visual Cryptography for Print and Scan Applications”, IEEE Transactions, ISCAS-2004, pp.572-575.

[6] T. Monoth and A. P. Babu, “Recursive Visual Cryptography Using Random Basis Column Pixel Expansion”, In Proceedings of IEEE International Conference on Information Technology, 2007, pp. 41-43.

[7] C. Blundo and A. De Santis, “On the contrast in Visual Cryptography Schemes”, In Journal on Cryptography, vol.12, 1999, pp. 261-289.

[8] 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.

[9] S. S. Hegde, Bhaskar Rao, “Cloud Security Using Visual Cryptography”, International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012,pp.9- 13.

[10] Sian-Jheng Lin and Wei-Ho Chung, “A Probabilistic Model of (t, n) Visual Cryptography Scheme With Dynamic Group”, IEEE Transactions on Information Forensics and Security, vol. 7, No. 1, February 2012, pp.197-207.