SEGMENT BASED VISUAL CRYPTOGRAPHY FOR KEY DISTRIBUTION

Sesha Pallavi Indrakanti[1] and Avadhani P S[2]

[1]Department of Computer Applications, GVP Degree College(Autonomous), Visakhapatnam.
ipallavi@yahoo.com
[2]Department of Computer Science and Systems Engineering, Andhra University College of Engineering(Autonomous), Andhra University, Visakhapatnam.
psavadhani@gmail.com

ABSTRACT

Security is playing a vital role in this era of information technology, it has become a prerequisite in the digital world for maintaining the secrecy of the information. Many techniques have been proposed for handling textual data, maintenance of confidentiality of pictographic data is also becoming a priority. The trend of pictographic data hiding is pixel based, here a version of Visual Cryptography is presented which is segment-based instead of pixel based. The key or the secret which is in the form of digits that is to be distributed is converted into segment display and then encrypted .The result of encryption is two random shares. The decryption process involves the stacking of these two shares. It is easier to view the secret with the human eye by stacking the shares.

KEYWORDS

Visual cryptography , 7-segment display, Encryption, Decryption.

1. INTRODUCTION

The security of data is an ever challenging and concerning issue. There is always a constant requirement for new and outstanding encryption techniques. This becomes has a top priority especially in applications which require transferring of sensitive data. Visual cryptography can provide one such feasible solution. Visual cryptography is a cryptographic technique which handles the encryption of visual information such as pictures, text, etc, the decryption can be done in such a way that the normal the human visual system can identify the secret without the help of computers.

The term visual cryptography was first coined by Moni Naor and Adi Shamir [1] in 1994. They demonstrated a basic (2,2) visual secret sharing scheme, where an secret in the form of an image was broken up into 2 disordered shares so that only someone with those 2 shares could decrypt the image. This technique was latter expanded to a (m, n) scheme where someone who hold those n shares can see the secret, while *m* be the minimum set of shares that depend on *n*. To witness the secret clearly all the *n* should be present, combination of *m* shares also divulge the image but not with clarity. Each share is printed on a separate transparency, and decryption is performed by overlaying these disordered looking shares. When all *n* shares were superimposed, the original secret image would appear.

If individual share is considered alone and the other share is unknown, it is a random collection of blocks. Given only one share, a second share cannot be crafted to reveal any possible image,

DOI : 10.5121/ijcses.2012.3110

therefore, individual shares reveal no information about the original image. Each pixel of the images is expanded into further blocks. There are always the same number white and black blocks. If a pixel is divided into two parts, there are one white and one black block, If the pixel is divided into four equal parts, there are two white and two black blocks.

In the fig.1 we can see that a pixel divided into four parts, can have six different states. If a pixel on layer 1 has a given state, the pixel on layer 2 may have one of the two states: identical or inverted to the pixel of layer 1. If the pixel of layer 2 is identical to layer 1, the overlayed pixel will be half black and half white. Such overlaid pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlaid version will be completely black. This is called an information pixel.

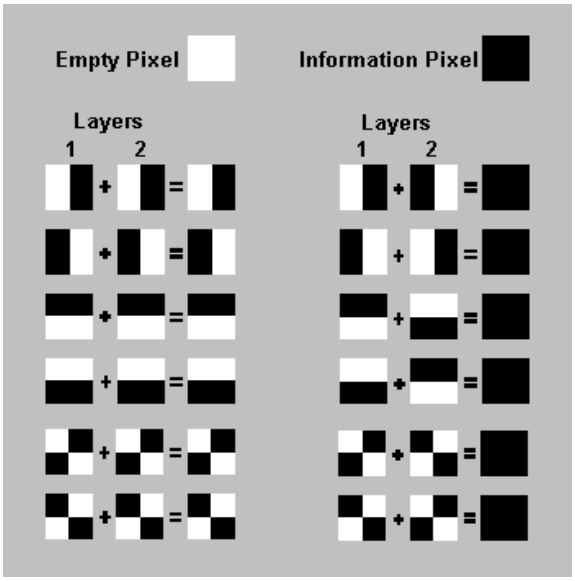

Fig1: Layering in Visual cryptography

Now the two layers can be created. One transparent image, layer 1, has pixels which all have a random state, one of the six possible states. Layer 2 is identical to layer 1, except for the pixels that should be black (contain information) when overlayed. These pixels have a state that is opposite to the same pixel in layer1. If both images are overlayed, the areas with identical states will look grey, and the areas with opposite states will be black.

Visual Cryptography offers perfect confidentiality according to the information theory. The use of Visual Cryptography in secure communications will engage the sender in distributing one or more random layers in advance to the receiver. If the sender has a message, he creates a layer 2 for a particular distributed layer 1 and transmits it to the receiver. The receiver aligns the two layers and the secret information is revealed. The decryption process is done without the need of an encryption device, a computer or performing calculations by hand. The system is unbreakable, as long as both layers don't fall in the wrong hands. When one of the layers is intercepted it's impossible to retrieve the encrypted information. This technique is simple to implement and does not require any NP-Hard problem dependency. Infinite computations also can't predict the message. User need not have any knowledge about cryptography to decrypt the message and the cipher text can be sent through FAX or E-MAIL , these benefits make visual cryptography a distinct technique.

2. SEGMENT DISPLAY

Segment display is a form of displaying decimal numerals. It is an alternative to the more complex dot-matrix displays. Segment displays are used more in electronic devices like digital clocks, electronic meters, and other electronic devices for displaying numerical information. There are different types of segment displays. viz,7-Segment Display, 9-Segment Display, 14-Segment Display, 16- Segment Display

7 Segment display[6] is the most famous and easy of all segment displays. 7 segment displays, as its name indicates, is a composed of seven elements. These seven elements are combined to produce representations of the Arabic numerals as shown in fig.2. The seven segments are arranged as a rectangle of two vertical segments on each side with one horizontal segment on the top, bottom, additionally, the seventh segment bisects the rectangle horizontally.

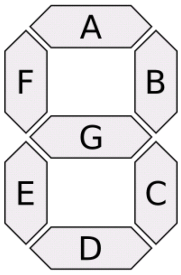

Fig.2: Seven segment Display

The concept of Visual Cryptography has taken several forms in its transition. It started from a 2-out-of-2 secret sharing system and went to an m-out-of-n secret sharing system. Some tried to add steganography to Visual Cryptography, and some tried to move from black-and-white to color images[2][3][4][5]. There are lots of works which concentrated on pixel based images. Visual cryptography is a budding topic. Visual cryptography is a simple and powerful method which can provide high security for confidential information. Recently, various studies about visual cryptography are proposed. Some has proposed a method for splitting the image into two different shares and some proposed on pixel quality enhancement [11][13], original image transmission or secret image transmission[12]. On the other hand, there have been also many reports for productions of meaningful binary halftone share images [14].Fu and Au have dealt with binary or ternary images like text images as secret image[8], while other many researchers have studied about natural gray-scale images like photographs as secret image and image as keys [9], [10].

A paper by Bernd Borchet [7] in 2007 has proposed a different variant of Visual Cryptography, i.e. instead of taking pixels as the smallest units to be encrypted, segments of a segment display are encrypted. The typical segment display is the seven-segment display, see fig.3, it is used to represent the digits 0; 1; 2; 3; 4; 5; 6; 7; 8; 9.

Fig.3: Display of numbers using seven segments

This paper is an application extension of the segment based work proposed earlier. This paper focuses on segment based visual cryptography. The suggested segment-based visual

cryptography can be used to encrypt messages into shares consisting of numbers displayable by a segment display. The features like easy adjustment of the two shares in case of transparencies and easy for a non-expert human user to use are the latent advantages of the segment-based visual cryptography over the pixel-based one

3. KEY DISTRIBUTION

In symmetric key cryptography, both parties must have a secret key which they must exchange before the initiation of encryption process. Distribution of secret keys has become a challenge until recently, because it involved face-to-face meeting of the parties or, use of a trusted courier, or sending the key through an existing encrypted channel. The first thing is impractical, the second thing has become unsafe, as it depends on the mercy of the courier service, while the third depends on the security of a previous key exchange.

In secret sharing a secret (key, pin, trade secret.) is used as a seed to generate a number of distinct secrets (shares), and the pieces are distributed between the recipients so that all the shares put together only can reveal the secret. Secret sharing is also called secret splitting, key splitting, and split knowledge. In real time applications distribution of key is a threat. Physical mail interception and fraud remains a significant risk even in today's modern technological environment.

4. SEGMENT BASED VISUAL CRYPTOGRAPHY FOR KEY DISTRIBUTION

This paper merges the positive aspects of visual cryptography and segment display for key distribution. Keys are vulnerable to unauthorized access when tried to print. The following are the steps of the algorithm for generating a segment based key.

Step 1: Generate a random number of size n

Step 2: Every segment S of the digit in the number is split into two parallel lines S1, S2 closely without intersection. The two parallel lines should be white in color on a black surface.

Step 3: Following step 2 Generate the segment display of the number in step1.

Step 4: Share 1 is generated randomly i.e. either of the parallel segment is generated randomly. The randomly generated segment is kept white and the parallel segment is made black.

Step 5: Share 2 is generated based on share 1 and, assume that a certain digit from 0-9 is to be represented, consider the subset of segments of the digit that is to be highlighted.

Step 5.1: If segment S belongs to this subset then the selection is the same as that in the random share and alternative segment is turned black.

Step 5.2: If the segment S does not belong to the subset then the alternative segment of the one in the random share is selected and random shares segment is made black.

The fig.4 shows the parallel seven segment display. These segments are generated white in color parallel and close to each other. Fig.5 illustrates the parallel seven segment display of a chosen number 4321.

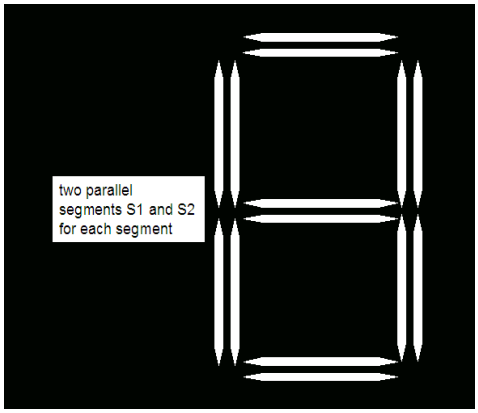

Fig.4: Parallel Seven Segment Display

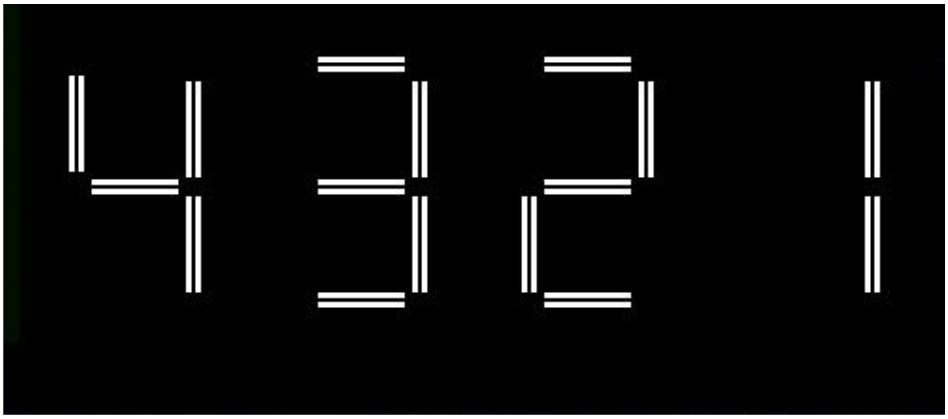

Fig.5: Parallel Seven Segment Display of the chosen number

The random seven segment number with parallel segments illustrated in fig.5 is now subjected to the encryption process which is based on the visual cryptography and algorithm specified above. The result of the encryption process is share 1 and share 2, shown in fig.6. Each digit in these shares appears same as that of the seven segment display. Any eavesdropper or an intruder who captures a single share cannot predict what the number would be. This advantage makes this technique an impartial one.

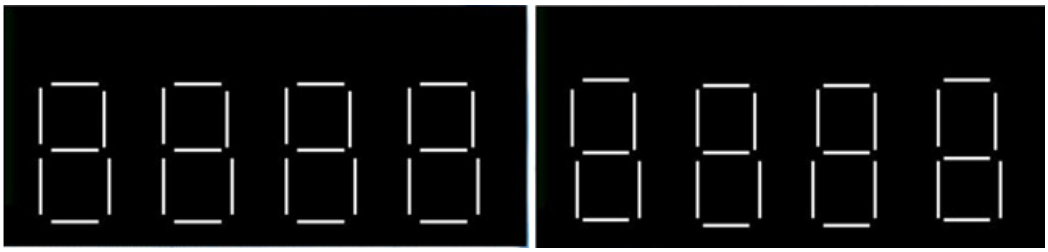

Fig.6: Share 1 and Share 2 of the random parallel seven segment display of the chosen number

The decryption process is a very simple and easy for a non-technical person to use. The shares are printed and stacked on each other to view the secret, the segments belonging to the first subset show transparent areas when the two shares are stacked. Therefore, after stacking, the number to be shown appears to the eye of the beholder. The revealed secret is shown in fig.7

where in the same subset segments appear bright and the alternative subset segments appear grey in color parallel to each other. This application generates and securely prints bank Personal identification number, or cryptographic key components.

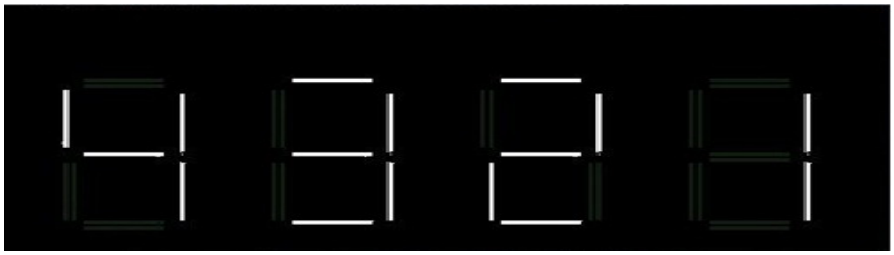

Fig.7: Share 1 and Share 2 of the random parallel seven segment display

5. CONCLUSIONS

Segment-based Visual Cryptography has potential advantages compared to pixel-based Visual Cryptography either in adjusting the shares or in the decryption process. This paves a way for secure yet easy way of transferring secure data with minimal human interference and effective deliverance of data.

REFERENCES

[1] Naor, M. and Shamir, A. 1994, *Visual cryptography*, Eurocrypt'94, *Lecture Notes in Computer Science*, vol. 950, pp. 1–12.

[2] Tzeng, W.G. and Hu, C.M., (2002) "A New Approach for Visual Cryptography", *Designs, Codes and Cryptography*, vol. 27, No. 3, pp. 207–227.

[3] Ming-Shi, Wang and Pei-Fang, Tsai, (2005) "The Implement of Visual Cryptography via Two Shares Embed Three Messages", *The 30th Digital Content, Digital Education, and Management Policy*, pp. 69-77.

[4] Fang, W.P. and Lin, J.C., (2006) "Visual Cryptography with Extra Ability of Hiding Confidential Data", *Journal of Electronic Imaging*, vol. 15, no.2, p. 023020.

[5] B. Dinesh Reddy, V. Valli Kumari, KVSVN Raju, Y.H. Prassanna Raju, (2011) "Rotation Visual Cryptography Using Basic (2, 2) Scheme" ,International Journal of Computing Science and Communication Technologies, VOL. 3, NO. 2.

[6] F.W.Wood: Illuminated Announcement and Display Signal. US Patent 974943, 1908.

[7] Bernd Borchert "Segment-based Visual Cryptography" *WSI-2007-04*.

[8]M. S. Fu, O. C. Au, "A novel method to embed watermark in different halftone images: data hiding by conjugate error diffusion (OHCED)," Proc. IEEE Int. Conf. on Multimedia and Expo, vol. 1, 2003, pp. 609– 612.

[9]Dusmanescu Dorel, "Encrypting messages with visual key," WSEAS TRANSACTIONS on COMPUTERS, Issue 5, vol. 8, 2009, pp. 757–766.

[10]T. Monoth and B. Anto P. Tamperproof transmission of fngerprints using visual cryptography schemes. In Procedia Computer Science, volume 2, pages 143{148, 2010.

[11]J. Weir and W. Yan. Resolution variant visual cryptography for street view of google maps. In Proceedings of the ISCAS, pages 1695{1698, 2010.

[12]S. Cimato and C.N. Yang. Visual cryptography and secret image sharing. CRC Press,Taylor & Francis, 2011.

[13]Vaibhav Choudhary, Kishore Kumar, Pravin Kumar, D.S. Singh " An Improved Pixel Sieve Method for Visual Cryptography", International Journal of Computer Applications Volume 12– No.9, January 2011

[14] Masakazu Higuchi, Aya Emori, Shuji Kawasaki, Jonah Gamba, Atsushi Koike and Hitomi Murakami "Image Encryption Methods Using Intensity Transformations in Visual Cryptography", INTERNATIONAL JOURNAL OF MATHEMATICS AND COMPUTERS IN SIMULATION Issue 1, Volume 5, 2011

Authors

Sesha Pallavi Indrakanti received her M.Sc degree from Andhra University 2002. She received her M.Tech degree in Information technology in 2007 from Andhra University. She has experience of 10 years in teaching and is presently working as aAssociate professor and Head in Department of Computer Applications in G.V.P.Degree College, Visakhapatnam, India. She is pursuing her Ph.D. from Andhra University, Visakhapatnam, India. Her areas of interest are Network Security, Data communications and Networks and Operating systems

Prof. P.S.Avadhani did his Masters Degree and Ph.d from IIT kanpur.He is presently working as a Professor in Department on CSSE Andhra university college of Engineering in Visakhapatnam. He has more than 75 papers published in various national/ inetrnatioanl journals and conferences. His research areas include Cryptography, Data Security, Algorithms, and Computer Graphics.