International Journal On Engineering Technology and Sciences – IJETS™
ISSN (P): 2349-3968, ISSN (O): 2349-3976
Volume 2 - Issue 5, May 2015

Extended Visual cryptography Scheme

Mrs.Nidhina.K
PG Scholar,
Department of Computer Science and Engineering,
Paavai College of Engineering , Namakkal,

Mr.P.Manikandan
Associate Professor,
Department of Computer science & Engg,
Paavai Group of institutions, Namakkal,

Abstract- *The secret sharing scheme which uses images distributed as shares such that, a hidden secret image will be revealed if the shares are superimposed. Visual cryptography is a secret sharing scheme which extended the share images will constructed to contain a meaningful cover images, and also to provide biometric security techniques. In this, a new method for processing halftone images used that will helps to improves the quality of the share images and also it will recovered a secret image in an extended visual cryptography scheme for which the recovered image is the same as for the original halftone secret image and also the size of the share images . The new proposed method helps to maintain the perfect security of the original extended visual cryptography approach. This method helps to inrease the seurity.*

Key words: Visual cryptography ,biometric security techniques. halftone secret image.

I. INTRODUCTION

Visual cryptography is a technique used for security purpose. This techniques was proposed by Naor and Shamir in the year 1994.This is a special encryption technique which is uses two transparent images, Thus ensuring more security One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both the transparent images and layers are required to reveal the information. This is a special encryption technique used to hide information in images. The technique hides the information in such way that it can be encrypted by human vision only if the correct key image is used. By printing the two layers onto a transparent sheet is the easiest way to implement visual cryptography.

It offers a unbreakable encryption when the random images contains truly random pixels and can be seen as a one –time pad system. In the overlay animation you can observe the two layers sliding over each other until they are correctly aligned and the hidden information appears. This can be tried out by ourselves ,For the same you can copy the example layers 1 and 2, and print them onto a transparent sheet or thin paper. Ensure that you use a program that displays the black and white pixels correctly and set the printer so that all pixels are printed accurately (no diffusion or photo enhancing etc). You can also copy and paste them on each other in a drawing program like paint and see the result immediately, While doing this make sure that you select transparent drawing and align both layers exactly over each other.

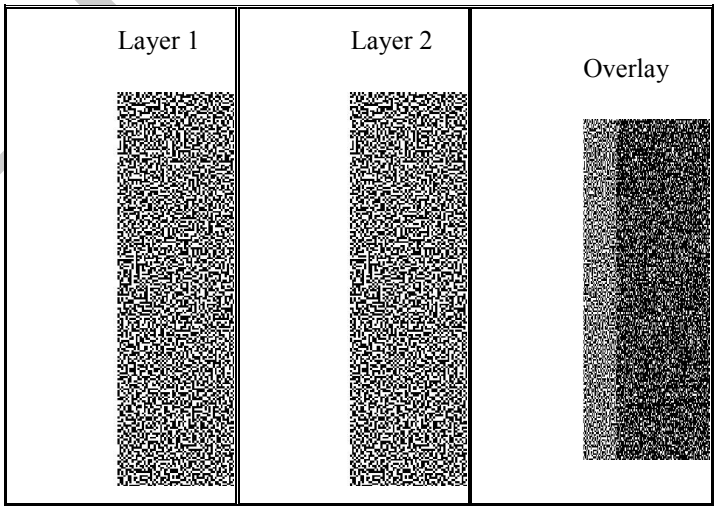

Fig .1 **How Visual Cryptography works**

Each pixel of the images are divided into smaller blocks. The blocks always consist of equal number of white (transparent) and black blocks. If a pixel is divided into two parts, there are one white and one black block. Similarly If the pixel is divided into four equal parts, there are two white and two black blocks. The example images above uses pixels that are divided into four parts.

On the right side of the table 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 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 overlayed pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlayed version will be completely black. This is an information pixel.

We can now create the two layers. One transparent image of 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 layer 1. If both images are overlayed, the areas with identical states will look gray, and the areas with opposite states will be black.

We can apply system of pixels in different ways. In our example, each pixel is divided into four blocks. However, you can also use pixels, divided into two rectangle blocks, or even divided circles. Also, it doesn't matter if the pixel is divided horizontally or vertically. There are many different pixel systems, some with better contrast, higher resolution or even with color pixels.

If the pixel states of layer 1 are truly (crypto secure) random, both empty and information pixels of layer 2 will also have completely random states. One cannot know if a pixel in layer 2 is used to create a grey or black pixel, since we need the state of that pixel in layer 1 (which is random) to know the overlay result. If all requirements for true randomness are fulfilled, Visual Cryptography offers absolute secrecy according to the Information Theory.

When Visual Cryptography is used for secure communications, the sender will distribute one or more random layers 1 in advance to the receiver. If the sender has a message, he creates a layer 2 for a particular distributed layer 1 and sends it to the receiver. The receiver aligns the two layers and the secret information is revealed, this without the need for 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 both layers is intercepted it's impossible to retrieve the encrypted information.

II. ARCHITECTURE

Initially the halftone image is given as the input where the first process to preprocess the gve halftone image and the BBR/SBR method can be apply to construct the share image and then th share halftone image can be impose ad it helps to reconstruct the image and finally the secret data can be revealed. By this the original secrete message can be obtained with high security.

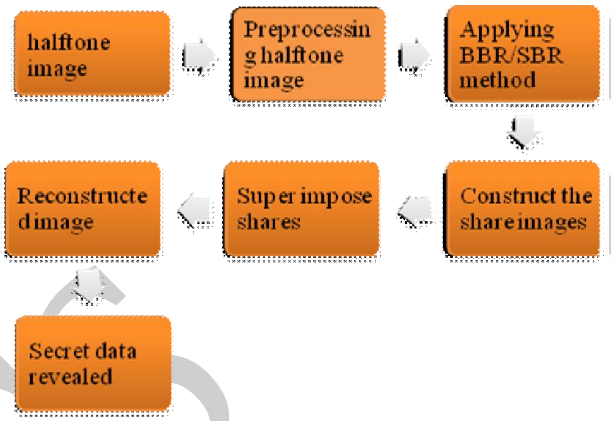

Fig.2 System Architecture

III. RELATED WORKS

The author Dr WeiQi Yan in 2001 proposed that the data security methods known as visual cryptography is presented. Visual Cryptography allows the efficient and effective secret sharing between the number of trusted parties. As per consideration the , trust is the most difficult part in many cryptographic schemes. It provides a powerful technique by which one secret can be distributed into two or more shares. When the shares xeroxed onto transparencies and then it can be superimposed exactly together so the original secret can be discovered without any computer participation. The difficulty facing is the contrast of reconstructed image is not maintaineda d also the additional processing required for colored images.

The authors Robert Sedgewick and Kevin Wayne proposed that Halftone is the reprographic technique that will simulates continuous through the use of dots, , in shape or in spacing, varying either in size thus generating a gradient like effect. Halftone can also used to refer to the image that is produced by this process.Where the continuous tone imagery contains an infinite range of colors or greys, where the halftone process reduces the visual reproductions to an image that is printed in dots of differing size with only one color of ink.

The author G.Tejeswar Reddy, M.Tech Scholar, proposed that the Black and white image of each pixel divided in 2 sub-pixels. Where randomly choose between black and white. If the black then the randomly selected between one of the two rows for black. If white, then the randomly seleted one of the two rows for white. The two sub pixels per pixel can able to distort the aspect ratio of the original image. The major goal to build the patterns of the two blocks for share images S1 and S2. The sticking results an able to generated according to the decrypting function. The secret image SE1 is revealed by directly stacking share images S1 and S2. The major difficulty facing the proposed system is that it does not provide a friendly environment to encrypt or decrypt data.

IV. SYSTEM SPECIFICATION

In the existing system a basic 2-out-of-2 visual cryptography scheme produces two share images from the original image and both shares to reproduce the original image. Combining k shares to recover the secret image. If the original pixel is white, then one of six combinations of the share pixels is randomly created. After stacking the shares with black opaque and white transparent, the original secret image will be revealed. Where black equivalent to '1' and the white is equivalent to '0'. Share images and the recovered secret image contain 4 times more pixels than the original image. The shares appear to be random, that might be helpful in security context. For example, if the share image could be selected to the fingerprint of the share holder, then this could be useful in the authenticating of a user's right to hold that share when the parties need to combine their share images to find out the secret. It suffers a management problem, because of which the dealers cannot identify each share. Recovered image has decreased in visual quality and also contrast between white and black is decreased.

The processing halftone images that will hels to improves the quality of the share images and that can recovered sercret image for which the recovered image is the same as for the original halftone secret image and the size of the share images.The resulting scheme is maintains the perfect security.

V .COMPARITIVE ANALYSIS.

On using the half tone images the recovery of the secret can be done by superimposing the share images.On comparing the two system the system using half tone images will provide good quality image as this system does not have pixel expansion..

V. RESULT

In this paper,we have n this paper, we have explored extended visual cryptography without expansion. We have shown that using an intelligent pre-processing of halftone images based on the characteristics of the original secret image, we are able to produce good quality images in the shares and the recovered image. Note that other applications can also benefit from the pre-processing approach, such as multiple image visual cryptography, which hides multiple images in shares

VI. CONCLUSION

The proposed method of visual cryptography is enhanced where using an intelligent pre-processing of the halftone images based on the characteristics of original secret image, able to produce very best quality images in the shares and also the recovered image. Where other applications can also be benefit from the pre-processing approach, like multiple image visual cryptography, which will hides multiple images in shares .

REFERENCE

[1] Y.C. Hou, F. Lin, C.Y. Chang, Improvement and implementation of the secret color image sharing technique, Proceedings of the Fifth Conference on Information Management, Taipei, November 1999, pp. 592–597.

[2] A. Ross and A. A. Othman, "visual cryptography for Biometric Privacy", IEEE transactions on information forensics and security, vol. 6, no. 1, pp. 70-81, 2011.

[3] N. Askari, C. Moloney and H.M. Heys,"A Novel Visual Secret Sharing SchemeWithout Image Size Expansion", IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Montreal, pp. 1-4, 2012.

[4] G. Ateniese, C. Blundo, A. De Santis and D.R. Stinson, "Extended Capabilities for Visual Cryptography", Theoretical Computer Science, vol. 250, pp. 143-161, 2001.

[5] Y.C. Hou, F. Lin, C.Y. Chang, A new approach on 256 color secretimage sharing technique, MIS Review, No.9, December 1999, pp. 89–105.

[6] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. Kumar,"Biometric encryption," in ICSA Guide to Cryptography. New York: Mc-Graw-Hill, 1999.

[7] M. Nakajima and Y. Yamaguchi, Extended Visual Cryptography for Natural Images, in Proceeedings of WSCG, pp. 303-310, 2002.

[8] C.L. Chou,"A Watermarking Technique Based on Nonexpansible Visual Cryptography", Thesis, Department of Information Management, National University, Taiwan, 2002.

[9] C.C. Wu and L.H. Chen, "A Study on Visual Cryptography",Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, 1998.

[10] A. Jain, P. Flynn, and A. Ross, Handbook of Biometrics. New York: Springer, 2007.

[11] Naor, M. and Shamir, A., Visual cryptography, In Proc. Eurocrypt 94, Perugia, Italy, May 9–12, LNCS 950, Springer Verlag., 1994, pp. 1–12.

[12] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT,1994, pp. 1–12.

[13] G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through off-line biometric identification," in Proc. IEEE Symp.Security and Privacy, 1998, pp. 148–157.

[14] B. Thuraisingham and W. Ford, "Security constraint processing ina multilevel secure distributed database management system," IEEETrans. Knowl. Data Eng., vol. 7, no.2, pp. 274–293, Apr. 1995

[15] M. Nakajima and Y. Yamaguchi, "Extended visualcryptography fornatural images," J. WSCG, vol. 10, no. 2, pp. 303–310, 2002.

[16] Y.C. Hou, C.Y. Chang, F. Lin, Visual cryptography for color images based on color decomposition, Proceedings of the Fifth Conference on Information Management, Taipei, November 1999, pp. 584–591.

[17] A. Jain, K. Nandakumar, and A. Nagar, "Biometric templatesecurity,"EURASIP J. Advances Signal Process., pp. 1–17, 2008.

[18] Y. Rao, Y. Sukonkina, C. Bhagwati, and U. Singh, "Fingerprintbased authentication application using visual cryptography methods(improved id card)," in Proc. IEEE Region10 Conf., Nov. 2008, pp.1–5.

[19] M. Naor and A. Shamir, "visual cryptography", in EUROCRYPT'94 proceedings, lecture Notes in computer science, springer-verlag, vol. 950, pp. 1-12, 1995.

[20] V. Rijmen, B. Preneel, Efficient colour visual encryption for shared colors of Benetton, Eurocrypto'96, Rump Session, Berlin, 1996.

[21] C.C. Chang, C.S. Tsai, T.S. Chen, A technique for sharing a secret color image, Proceedings of the Ninth National Conference on Information Security, Taichung, May 1999, pp. LXIII–LXXII.

[22] Hiroki Koga and Hirosuke Yamamoto, Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images. IEICE Transaction on Fundamentals, E81-A(6):1262– 1269.

[23] Haibo Zhang, Xiaofei Wang, Wanhua Cao and Youpeng Huang, "Visual Cryptography for General Access Structure Using Pixelblock Aware Encoding", JOURNAL OF COMPUTERS, VOL. 3, NO. 12, DECEMBER 2008.