ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 5 , May 2015

Enhanced Hierarchical Design for Visual Cryptography- Overview

Vinish Alikkal, Dr.T.Senthil Prakash, Ajmal Hussain

PG Scholar, Department of CSE, Shree Venkateshwara Hi-Tech Engineering College, Tamilnadu, India

Head/Department of CSE ,Venkateshwara Hi-Tech Engineering College, Tamilnadu, India

PG Scholar, Department of CSE, Shree Venkateshwara Hi-Tech Engineering College, Tamilnadu, India

ABSTRACT: Visual cryptography is cryptographic techniques that encrypts the plain text and send it through the secure channel. The encryption procedure follows the shares creating and the input is in the form of images and the visual systems or human visual systems performs the decryption of the scrambled message that comes from the channel. The visual cryptography scheme performance depends on different surveys such as computational complexity, security, pixel expansion, accuracy, contrast; share generated is meaningful or meaningless, different types of secret images and collection of secret images encrypted by VC scheme. The proposed system is study of visual cryptography schemes and performance analysis based on a complementary method. The performance analysis done on the basis of pixel expansion, group of secret images, image format and type of shares generated. The idea behind this hierarchical visual cryptography is encrypting the secret image or group of images in different levels and the secrecy will increased if the number of hierarchical levels is increased in Visual Cryptographic scheme. In hierarchical visual cryptography the expansion ratio is reduced to 1:2 from 1:4. Each different hierarchical level has an intelligent authentication system for the secrecy and the encryption shares have been generated in different levels and which found to be a random one.

KEYWORDS: Visual Cryptography, Recursive threshold.

I. INTRODUCTION

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. Visual Cryptography uses two transparent images. 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 transparent images and layers are required to reveal the information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet. When the random image contains truly random pixels it can be seen as a one-time pad system and will offer unbreakable encryption. In the overlay animation you can observe the two layers sliding over each other until they are correctly aligned and the hidden information appears. To try this yourself, you can copy the example layers 1 and 2, and print them onto a transparent sheet or thin paper. Always use a program that displays the black and white pixels correctly and set the printer so that all pixels are printed accurate. You can also copy and paste them on each other in a drawing program like paint and see the result immediately, but make sure to select transparent drawing and align both layers exactly over each other.

This document is set in 10-point Times New Roman. If absolutely necessary, we suggest the use of condensed line spacing rather than smaller point sizes. Some technical formatting software print mathematical formulas in italic type, with subscripts and superscripts in a slightly smaller font size. This is acceptable. Each pixel of the images is divided into smaller 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. The example images from above uses pixels that are divided into four parts. In the table on the right we

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 5 , May 2015

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 overlaid 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 an information pixel.

We can now create the two layers. 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 overlaid. These pixels have a state that is opposite to the same pixel in layer 1. If both images are overlaid, the areas with identical states will look gray, and the areas with opposite states will be black.
The system of pixel can be applied 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.

II. RELATED WORKS

A. INTELLIGENT SYSTEM FOR SECURED AUTHENTICATION USING VISUAL CRYPTOGRAPHY

This system introduces the idea of hierarchical visual cryptography. Authentication is the important issue over the internet. This paper describes a secured authentication mechanism with the help of visual cryptography. Visual cryptography simply divides secret information in to number of parts called shares. These shares are further transmitted over the network and at the receiving end secrets are revealed by superimposition. Many layers of visual cryptography exist in proposed system hence called hierarchical visual cryptography. Remote voting systems now a day's widely using visual cryptography for authentication purpose. Visual cryptography is the art of encrypting information such as handwritten text, images etc. in such a way that the decryption is possible without any mathematical computations and human visual system is sufficient to decrypt the information. The cryptography scheme is given by the following setup. A secret image consists of a collection of black and white pixels. Here each pixel is treated independently. To encode the secret image, we split the original image into n modified shares such that each pixel in a share now subdivided into n black and white sub-pixels. To decode the image, a subset S of those n shares are picked and copied on separate transparencies.

The authentication scheme proposed here is providing security in multiple levels. The share individually is unable to reflect secrecy of the data. The permutations and combinations are failure against the shares. The visual cryptography scheme is also known in the form of secret sharing scheme. Color visual cryptography schemes also exist which is equivalent to stegnography concept in network security.

B. VISUAL SECRET SHARING USING CRYPTOGRAPHY

The Visual Cryptography Scheme is a kind of secret sharing scheme that focuses on sharing secret images. The basic idea of the visual cryptography scheme is to split a secret image into number of random shares which separately reveals no information about the secret image other than the size of the secret image. The secret image can be reconstructed by stacking the shares. The paper proposed the extended visual cryptography scheme for natural images. Next it showed
A method to improve the image quality of the output by enhancing the image contrast beyond the
Constraints given by the previous studies. The method enables the contrast enhancement by extending the concept of error and by performing half toning and encryption simultaneously. The trade-off between the image quality and the security are assessed by observing the actual results of this method. Furthermore, the optimization of the image quality at a given contrast is discussed. Under an assumption that the occurrence of the violations is stochastically even in the images, a function is introduced for the image quality optimization. The validity of the assumption and the effect of image quality improvement are also verified with the experiments.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 5 , May 2015

III. PROBLEM DESCRIPTION

Various parameters are recommended by researchers to evaluate the performance of visual cryptography scheme. Naor and Shamir suggested two main parameters: pixel expansion m and contrast α. Pixel expansion m refers to the number of sub pixels in the generated shares that represents a pixel of the original input image. It represents the loss in resolution from the original picture to the shared one. Contrast α is the relative difference in weight between combined shares that come from a white pixel and a black pixel in the original image.

Jung-San Lee et al advised security, pixel expansion, accuracy and computational complexity as a performance measures. Security is satisfied if each share reveals no information of the original image and the original image cannot be reconstructed if there are fewer than k shares collected. Accuracy is considered to be the quality of the reconstructed secret image and evaluated by peak signal-to-noise ratio measure. Computational complexity concerns the total number of operators required both to generate the set of n shares and to restructure the original secret image.

C. Chang et al suggested that visual cryptography scheme should support wide image format like color and gray scale. Author also argued that random looking shares appear to be suspicious and thus are vulnerable to attacks by attackers in the middle, to fill in this security gap, meaningful shares should be produced. Jen-Bang Feng et al suggested that visual cryptographic schemes should support multiple secret to work efficiently. If scheme support only one secret to share at a time to share multiple secret images numerous shares has to be generated, transmitted and maintained. The disadvantage of the schemes is that only one set of confidential messages can be embedded, so to share large amounts of confidential messages several shares have to be generated

IV. EXISTING SYSTEM

A. SECURE VISUAL CRYPTOGRAPHY

In existing system the dealer or sender takes a secret image and encodes into shares. After encoding this shares are sent to participants. The receiver collects the shares and stack to get decoded secret image. Here no verification is done so easy cheating is done. In this paper they proposed a system such that the dealer or sender takes one secret image and verification image. These two images are encoded into shares, after encoding sends one secret share and one verification share to the participants. Each participant verifies the share and other participant secret share reveals the secret image. In this way cheating is avoided.

In this paper they proposed a technique of well known secret sharing on both black and white and color images. At the time of dividing an image into n number of shares we have used random number generator, which is a new technique not available till date. This technique needs very less mathematical calculation compare with other existing techniques of visual cryptography on color images. This technique only checks '1' at the bit position and divide that '1' into (n-k+1) shares using random numbers. In most of our experimental results, each share reflects very little or even no information regarding the original image to human eye. But the main drawback of the algorithm is in its number of loops. For n=6, k=5 and a 32 bit pixel with 50% '1', number of loop operation required is 32. For n=6, k=4 with other conditions same, number of loop operation required is 48. For n=6, k=3 with other conditions same, number of loop operation required is 64.

B. VISUAL CRYPTOGRAPHY FOR GRAY LEVEL IMAGES

Previous efforts in visual cryptography were restricted to binary images which is insufficient in real time applications. Chang- ChouLin, Wen-HsiangTsai proposed visual cryptography for gray level images by dithering techniques. Instead of using gray sub pixels directly to constructed shares, a dithering technique is used to convert gray level images into approximate binary images. Then existing visual cryptography schemes for binary images are applied to accomplish the work of creating shares. The effect of this scheme is still satisfactory in the aspects of increase in relative size and decoded image quality, even when the number of gray levels in the original image still reaches 256.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 5 , May 2015

C. VISUAL CRYPTOGRAPHY FOR GENERAL ACCESS STRUCTURES

In (k, n) Basic model any „k" shares will decode the secret image which reduces security level. To overcome this issue the basic model is extended to general access structures by G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, where an access structure is a specification of all qualified and forbidden subsets of „n" shares. Any subset of „k" or more qualified shares can decrypt the secret image but no information can be obtained by stacking lesser number of qualified shares or by stacking disqualified shares. Construction of scheme is still satisfactory in the aspects of increase in relative size and decoded image quality, even when the number of gray levels in the original image still reaches 256.

D. HALFTONE VISUAL CRYPTOGRAPHY

The meaningful shares generated in extended visual cryptography proposed by Mizuho Nakajima and Yasushi Yamaguchi was of poor quality which again increases the suspicion of data encryption. Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo proposed halftone visual cryptography which increases the quality of the meaningful shares. In halftone visual cryptography a secret binary pixel „P" is encoded into an array of Q1 x Q2 sub pixels, referred to as halftone cell, in each of the „n" shares. By using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained. Also maintains contrast and security.

E. RECURSIVE THRESHOLD VISUAL CRYPTOGRAPHY

The (k, n) visual cryptography explained in section I needs "k" shares to reconstruct the secret image. Each share consists at most [1/k] bits of secrets. This approach suffers from inefficiency in terms of number of bits of secret conveyed per bit of shares. Recursive threshold visual cryptography proposed by Abhishek Parakh and SubhasKak eliminates this problem by hiding of smaller secrets in shares of larger secrets with secret sizes doubling at every step. When Recursive threshold visual cryptography is used in network application, network load is reduced.

F. REGIONAL INCREMENTING VISUAL

Visual cryptography schemes usually process the content of an image as a single\ secret i.e. all of the pixels in the secret image are shared using a single encoding rule. This type of sharing policy reveals either the entire image or nothing, and hence limits the secrets in an image to have the same secrecy property. Ran-Zan Wang proposed Region Incrementing Visual cryptography for sharing visual secrets in multiple secrecy level in a single image. The "n" level scheme, an image S is designated to multiple regions associated with secret levels, and encoded to shares with the following features:
(a) Each share cannot obtain any of the secrets in S,
(b) Any t (2<t<n+1) shares can be used to reveal (t-1) levels of secrets
(c) The number and locations of not-yet revealed secrets are unknown to users,
(d) All secrets in S can be disclosed when all of the (n+1) shares are available,

V. PROPOSED SYSTEM

Visual cryptography is a cryptographic technique which allows visual information to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation. This property makes visual cryptography especially useful for the low computation load requirement.

Taking limited bandwidth and storage into consideration two criteria pixel expansion and number of shares encoded is of significance. Smaller pixel expansion results in smaller size of the share. Encoding multiple secret images into the same share images requires less overhead while sharing multiple secrets. Meaningful shares avoid attention of hacker considering the security issues over the communication channels. To meet the demand of today's multimedia

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 5 , May 2015

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 are also discussed in this paper.

Hierarchical visual cryptography is based upon the concept of visual cryptography. The basic idea behind visual cryptography technique is to divide the secret information into two shares. The piece of information in scrambled form is known as share.

Visual cryptography requires both shares while decrypting the information. To decrypt the secret, shares are superimposed. Decryption does not require any mathematical computation. Human eyes are sufficient to identify the secret after superimposition. Visual cryptography is defined in terms of various schemes. Basic scheme is 2 out of 2 visual cryptography. It is also known as secret sharing. Sharing a secret among group of participants indicates that each participant hold exactly one share. To reveal the secret, all shares are required to be gathered. Shares generated out of visual cryptography are expanded in terms of size. Each pixel information in original secret is represented by 4 pixels in the shares. Thus the pixel expansion ration is 1:4. If the size of original secret is nXm then the size of shares become 2nX2m. Each pixel is encoded with some combination of black and white pixels.

Hierarchical visual cryptography encrypts the secret in number of levels. Initially the secret is divided into exactly two share called share 1 and share 2. Each share is then encrypted independently resulting in four shares: share 11, share 12, share 21 and share 22. Later, among these four shares, any three shares are chosen to generate the key share. The superimposition of key share with the remaining share reveals the secret information. The superimposition is logically performed by the X-OR operation. As the level of encryption in hierarchical visual cryptography increases, the secrecy tends to increase.

Data Flow Diagram is an important tool used during system analysis, A DFD model is a system using external entity from which data flows into a process, while transforms the data and create the output. Data flows through the other process or external entities or files. Data in files may also flow to process as inputs. A DFD shows the usual flow of data through a system. It views a system as a function that can transform the inputs into desired outputs. The DFD aims to capture the transformations that take place within a system to the input data so that eventually the output data is produced. The main merit of the DFD is that it can provide an overview of what data the system should process, what transformation of data area done and where the results flow. So the DFD shows a movement of data through the different transformations or process in the system

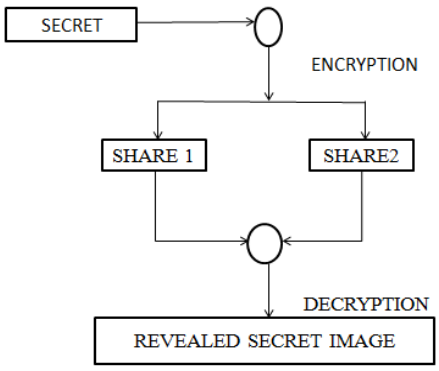

Fig. 1 Hierarchical Model

The requirement of this proposed method is that the secret should be in binary form i.e. black and white passwords, signatures, handwritten text etc. Before encrypting, the original secret is mapped into the size which is multiple of 4. Before encrypting the secret, it is normalized. The resize function of International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014 94 OCTAVE/MATLAB is chosen to convert any secret whose size is multiple of 4. After resizing the secret starting with top left corner of secret every 2X2 pixel block is selected for encoding independently. The encoding of 2X2 block is done among various random combinations. If 2X2 block in

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 5 , May 2015

original secret is entirely black then this block is encrypted using 4 possibilities represented by equation 1 - 8. There are multiple possibilities for the 2X2 pixel blocks.

Encryption

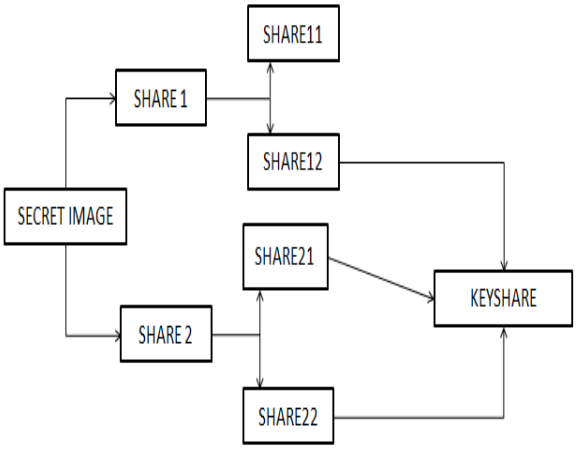

Fig 2. Encryption

Decryption

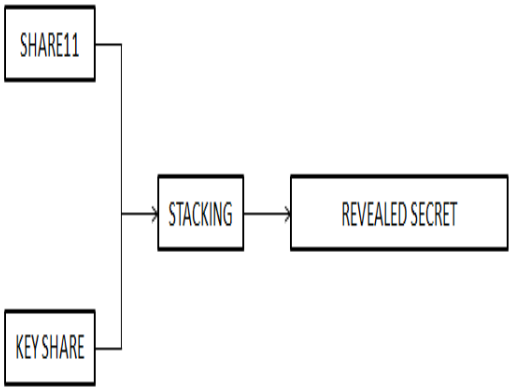

Fig 3. Decryption

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 5 , May 2015

VI. CONCLUSION

This paper discusses the introduction of different types of Visual Cryptography schemes. It compares the image quality and security using various visual cryptography schemes. In order to hide the secrecy we go for expansion and increasing of the number of shares, but this affects the resolution. Therefore an optimum number of shares are required to hide the secrecy. At the same time security is also an important issue. Hence research in visual cryptography is towards maintaining the contrast at the same time maintaining the security. The encryption of random secret is successful. The shares generated are expanded version of the original secret with expansion ration of 1:4 in first experimentation. Later the expansion ratio is reduced to 1:2. The methodology of key share generation is defined with a set of four shares of original secret. Any random secret could be encrypted using this experimentation.

REFERENCES

[1] Hegde C ,Manu S, Shenoy P D, Venugopal, K. R., Patnaik L. M, "Secured Authentication using Image Processing and Visual Cryptography for Banking Applications," i*n Proceedings of 16th IEEE International Conference on Advanced Computing and Communications, ADCOM 2008,*2008, pp. 65-72.

[2] Moni Naor, Adi Shamir, "Visual Cryptography," in *International Journal of Springer-Verlag*, 1998, pp. 1-11.

[3] Adi Shamir, "How to Share a Secret," in *Communications of ACM*, Vol. 22, no.11, 1979, pp. 612-613.

[4] Zhongnin Wangarce, G.R., "Halftone Visual Cryptography by Interative Halftoning," *in Proceedings of 2010 IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP)*, March 2010, pp. 1822-1825.

[5] M. Nakajima, Y. Yamaguchi, "Extended Visual Cryptography for Natural Images", volume 2, pp. 2002-2009.

[6] Tzung, Chang Sain, Wei Lee, "A Novel Subliminal Channel Found in Visual Cryptography and Its Application to Image Hiding," in *Proceedings of* 3rd *IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Vol. 1, 2007, pp. 421-424.

[7] Che Lee, Wen Tsai, " Authentication of Binary Images in PNG Format Based on a Secret Sharing Technique," in *Proceedings of IEEE International Conference on System and Engineering, Taipei*, July 2010, pp. 506-510.

[8]R. Youmaran, A. Adler, A. Miri, "An Improved Visual Cryptography Scheme for Secret Hiding," in *Proceedings of 23rd IEEE Biennial Symposium on Communications*, 2006, pp. 340-343.

AUTHORS BIOGRAPHY

Mr. Vinish Alikkal received the B.Tech Degree from Calicut University from Govt. Engineering College, Palakkad, Kerala in India 2004-2008 and worked as Lecturer in MEA Engineering College from 2009 – 2013 and pursuing ME (CSE) from Shree Venkateswara Hi-Tech Engineering College, Erode, Tamilnadu India 2013-2015. His research interests are Network Security, Databases, Cloud Computing and Artificial Intelligent. He published an International Journal on Moderate Denial-of-Service attack detection based on Distance flow and Traceback Routing in International Journal on Engineering Technology and Sciences – IJETS™. He participated in National workshop on Computational Intelligence and participated on National workshop on Android application development.

Dr.T.Senthil Prakash received the Ph.D. degree from the PRIST University, Thanjavur, India in 2013 and M.E (CSE) degree from Vinayaka Mission's University, Salem, India in 2007 and, all in Computer Science and Engineering. He is a member in ISTE New Delhi, India, IAENG, Hong Kong..IACSIT, Singapore SDIWC, USA. He has the experience in Teaching of 10+Years and in Industry 2 Years. Now He is currently working as a Professor and Head of the Department of Computer Science and Engineering in Shree Venkateshwara Hi-Tech Engineering College, Gobi, Tamil Nadu, and India. His research interests include Data Mining Data Bases, Artificial Intelligence, Software Engineering etc.,He has published several papers in 17 International Journals, 43 International and National Conferences.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 5 , May 2015

Mr. Ajmal Hussain received the B.Tech Degree from MEA Engineering College, Perinthalmanna, Malappuram, Kerala,India 2004-2007 and worked as Lecturer in MEA Engineering College from 2010 – 2013 and pursuing ME (CSE) from Shree Venkateswara Hi-Tech Engineering College, Erode Tamilnadu India 2013-2015.
His research interests are, Web Technology, Embedded Systems, and Artificial Intelligent. He participated in National workshop on Computational Intelligence and participated National workshop on Android application development