ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

A Survey on Image Security using Visual Cryptography

Farah Khan[1], Prof. Deepa Gianchandani[2]

M.Tech Scholar, Department of Electronics and Communication, SISTec, Bhopal, M.P, India[1]

Assistant Professor, Department of Electronics and Communication, SISTec, Bhopal, M.P, India[2]

ABSTRACT: Information's are being transferred through open channels and the security of those information has been prime concerns. Apart from many conventional cryptographic schemes, visual cryptographic techniques have also been in use for data and information security. Visual cryptography is a secret sharing scheme as it breaks an original image into image shares such that, when the shares are stacked on one another, a hidden secret image is revealed. The Visual Cryptography Scheme is a secure method that encrypts a secret document or image by breaking it into image shares. A unique property of Visual Cryptography Scheme is that one can visually decode the secret image by superimposing shares without computation. Even to make the visual cryptography image shares more secure, public key encryption scheme is applied. Public key encryption technique makes image shares so secure that it becomes very hard for a third party to decode the secret image information without having required data that is a private key.

KEYWORDS: Image, Encryption, RSA

I. INTRODUCTION

Visual cryptography is a cryptographic technique which allows visual information to be encrypted in speci c a way that decryption becomes a mechanical operation that does not require a computer. The idea was about producing image shares of a given secret image in a way that the image shares appear meaningless. Recovery of the image can be done by superimposing speci ed number of share images and, hence, the decoding process requires no special hardware or software and can be simply done by the human eye. Visual cryptography is a little more advantageous for implementation, while compared to conventional cryptography schemes, since the decryption process does not need any computation. Further, the image based information becomes more secure, since only the intended recipient can reveal the true meaning of the decrypted image. Suppose the data (image) D is divided into n shares. D can be constructed from any k shares out of n shares. Complete knowledge of (k-1) shares reveals no information about D. So, k out of n shares is necessary to reveal secret data. For example: let 6 thieves share a bank account but they do not trust each other. The thieves split up the password for the account in such a way that any 3 or more thieves working together can have access to account, but not less than 3.

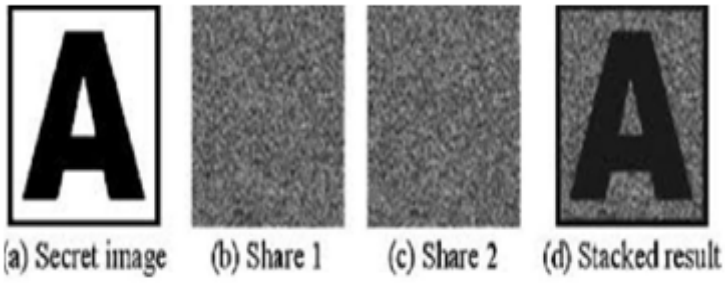

Figure 1. Illustration of visual cryptography

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

II. LITERATURE REVIEW

Visual cryptography technique was introduced by Naor and Shamir in 1994 as an alternative for conventional cryptography .They demonstrated a visual secret sharing plan, where a picture was separated into n imparts so that just somebody to all n shares could decode the picture, while any n 1 shares uncovered no data about the rst original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. At the point when all n shares were overlaid, the rest picture would show up. There are a few speculations of the fundamental plan including k-out-of-n visual cryptography. Rijimen displayed another 2-out-of-2 VC plot by applying the thought of shading mixture. When two transparencies superimposed on one another with distinctive colours, they lead to raises third blended shading.

In 2002, Nakajima predicted a new method of extended visual cryptography. This method is for regular images which are used to produce meaningful binary shares .This system works by taking three pictures as an input and generates two images which correspond to two of the three input pictures. The third picture is recreated by printing the two share pictures onto transparencies and stacking them together. By and large, visual cryptography experiences the deterioration of the image quality. In this also describes the method to improve the quality of the output image.

Binary visual cryptography scheme is proposed Hou et al. in the year 2004, which is applied to gray level images, that a gray level image is transformed into halftone images. The method that uses the density of the net dots to simulate the gray level is called Halftone and transforms an image with gray level into a binary image before processing. Halftone visual cryptography is proposed by the Zhi Zhou et al. In 2006 which produce meaningful and good high quality halftone shares, the generated halftone shares contain the visual information

.

III. VARIOUS VISUAL CRYPTOGRAPHIC SCHEMES

A. K OUT OF K VISUAL CRYPTOGRAPHY SCHEME

A common example of k out of k visual cryptography scheme is 2 out of 2 visual cryptog-raphy schemes. In (2, 2) Visual Cryptography Scheme, the original image is broken into 2 image shares. In original image , every pixel is represented by non-overlapping block of 2 or 4 sub-pixels in each share. If anyone is having only one share, will not be able to reveal any secret information. Both the shares are required to be superimposed to reveal the secret image.

There are many techniques for encoding the pixels of original image. In a technique, in which each pixel in original image is represented by two sub-pixels in each share, while reading the pixels in original image, if a white pixel is encountered, one of the rst two rows in Figure given below is selected with probability 0.5, and the shares are assigned 2 pixel blocks as shown in the third and fourth columns in gure given below. Similarly, if a black pixel is encountered, one of the last two rows is selected with probability 0.5, from which a sub-pixel block is assigned to each share. When two shares are superimposed, if two white pixels overlap, the result will be white pixel and if a black pixel in one share overlaps with either a white or black pixel in another share, the result will be black pixel. This implies that the superimposition of the shares represents the Boolean OR function. The last column in Figure given below shows the resulting sub-pixel when the sub-pixels of both the shares in the third and fourth columns are superimposed.

B. K OUT OF N VISUAL CRYPTOGRAPHY SCHEME

In (2, 2) visual cryptography, both the shares are required to reveal secret information .Due to some problem if one share gets lost then the secret information cannot be revealed. So there is a restriction of keeping all the shares secure to reveal the secret information and user can not a ord to lose a single share. Naor and Shamir generalized basic model of visual cryptography into a visual variant of k out of n visual cryptography scheme to give some edibility to user. In (k, n) visual cryptography scheme, n shares can be generated from original image and distributed. Original image is recognizable only if k or more shares superimposed, where value of k is between 2 to n. If less than k shares stacked together, secret original image cannot be revealed. It gives edibility to user. If user loses some of the shares still secret information can be revealed, if minimum k number of shares is obtained. It also ensures the security as to know the secret information you have to have more than k shares out of n secret shares.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

C. VISUAL CRYPTOGRAPHY SCHEME FOR GENERAL ACCESS STRUCTURE

In (k, n) visual cryptography scheme, all n shares have equal importance. The secret information can be revealed if any k out of n shares are available.The security of system might get compromised due to this. To beat this issue, G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson extended (k, n) visual cryptography model to general access structure. In general access structure scheme, given set of n shares is divided into two subsets namely quali ed and forbidden subset of shares as per the importance of shares. Any k shares from quali ed subset of shares can reveal secret information, but fewer than k shares from quali ed subset of shares can not reveal any secret information. Even k or more shares from forbidden set can not reveal secret information. So, Visual cryptography for general access structure improves the security of system.

D. RECURSIVE THRESHOLD VISUAL CRYPTOGRAPHY SCHEME

In (k, n) visual secret sharing scheme, a secret of b bits is distributed among n shares of size at least b bits each. Since only k out of n shares is needed to reveal secret, every bit of any share conveys at most 1/k bits of secret. It results in ine ciency in terms of number of bits of secret conveyed per bit of shares. To overcome this limitation Abhishek Parakh and Subhash Kak proposed Recursive threshold visual cryptography [7]. The basic idea behind Recursive threshold visual cryptography is recursive hiding of smaller secrets in shares of larger secrets with secret sizes doubling at every step, and thereby increasing the information, every bit of share conveys to (n-1)/n bit of secret which is nearly 100

E. HALFTONE VISUAL CRYPTOGRAPHY SCHEME

Halftone visual cryptography uses half toning technique to create shares. Halftone is the reprographic technique. It simulates continuous tone imagery through the use of dots, which may vary either in size, in shape or in spacing. Zhi Zhou et al. proposed halftone visual cryptography .In halftone visual cryptography a secret binary pixel is encoded into an array of sub pixels, called as halftone cell, in each of the n shares. By using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained. It maintains good contrast and security and increases quality of the shares[3].

F. VISUAL CRYPTOGRAPHY SCHEME FOR GREY IMAGES

All previous visual cryptography schemes were only limited to binary images. These procedures were t for doing operations on just highly contrasting black and white pix-els. It is not su cient for real life applications. Chang-Chou Lin, Wen Hsiang Tsai proposed visual cryptography for gray level images. In this scheme a dithering technique is used to convert gray level image into approximate binary image. Then existing visual cryptography schemes for binary images are applied to create the shares.

G. SECURING VISUAL CRYPTOGRAPHIC SHARES USING PUBLIC KEY ENCRYPTION

The visual cryptography scheme is a secure method that encrypts a secret document or image by breaking it into shares. A unique property of visual cryptography scheme is that one can visually decode the secret image by superimposing shares without computation. By taking the advantage of this property, third person can easily retrieve the secret image if shares are passing in the network. This approach is is for encrypting visual cryptographically generated image shares using public key encryption. RSA algorithm is used for providing the double security of secret image. This scheme provides more security to secret shares that are robust against number of attacks. This way after encryption of image shares even if a third person gets those shares while passing through the network, would not be able to reveal the secret.

IV. CONCLUSION

This scheme generates the VC shares using basic visual cryptography model and then encrypt the shares using RSA algorithm so that the shares will be more secure and protected from the malicious adversaries who may try to alter the bit sequence to create fake shares. During the decryption phase the secret shares are extracted by RSA decryption algorithm and stacked to reveal the secret image.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

REFERENCES

1. Feng Liu, Chuankun Wu, Xijun Lin. "Step Construction of Visual Cryptography Schemes". IEEE transactions on information forensics and security, vol. 5, no. 1, march 2016.
2. N. Askari, H.M. Heys, and C.R. Moloney. "an extended visual cryptography scheme without pixel expansion for halftone images". 26th annual ieee canadian conference on electrical and computer engineering year 2013.
3. Zhi Zhou, Gonzalo R. Arce and Giovanni Di Crescenzo. "Halftone Visual Cryptogra-phy". IEEE transactions on image processing, vol. 15, no. 8, august 2006.
4. Gyan Singh Yadav and Aparajita Ojha. "A Novel Visual Cryptography Scheme Based on Substitution Cipher". Proceedings of the 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013).
5. Archana B.Dhole and Prof. Nitin J. Janwe. "An Implementation of Algorithms in Visual Cryptography in Images". International Journal of Scienti c and Research Pub-lications, Volume 3, Issue 3, March 2013 1 ISSN 2250-3153.
6. Kulvinder Kaur and Vineeta Khemchandani. "Securing Visual Cryptographic Shares using Public Key Encryption".2013 3rd IEEE International Advance Computing Confer-ence (IACC).
7. A. Parakh and S.kak ."A Recursive Threshold Visual Cryptography Scheme ". De-partment of Computer Science, Oklahoma State University Stillwater, OK 74078.
8. D. Jena and S. Jena . "A Novel Visual Cryptography Scheme". 978- 07695-3516-6/08 2008 IEEE DOI 10.1109/ICACC.2009.109.
9. P. S. Revenkar, Anisa Anjum and W. Z. Gandhare. "Survey of Visual Cryptographic Schemes". International Journal of Security and Its Applications Vol. 4, No. 2, April, 2010.
10.Ujjwal Chakraborty et al. "Design and Implementation of a (2, 2) and a (2,3) Visual Cryptographic Scheme" .International Conference [ACCTA-2010], Vol.1 Issue 2, 3, 4, PP 128-13