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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Secured Visual Cryptography Scheme Using Meaningful Shares

Er. Rimsy Dua[(1)], Er. Narender Singh[(2)]

M.Tech. Student, Department of Computer Science & Engineering, GITM, Bilaspur, Haryana, India[(1)]

Assistant Professor, Department of Computer Science & Engineering, GITM, Bilaspur, Haryana, India[(2)]

ABSTRACT: One of the best technique for the security of images or text is "Visual Cryptography" .Initially, This technique was developed for black and white images but later on same was extended for color images as well. The (k,n) threshold visual cryptography scheme has been successfully described. Splitting of image into shares is the basic concept of visual cryptography technique .Shares can be meaningful or meaningless depending on the study conducted by different authors. Halftoning, color decomposition and pixel expansion are the three basic terminologies that has been used by different authors for the encryption of color images using visual cryptography technique. There are two basic fundamentals of colormodels. One is additive model and another is subtractive model. Color decomposition is done into R(red),G(green),B(blue) if additive model is used and C(cyan),M(magenta) and Y(yellow) if subtractive model is used. The main objective of this paper is to make comparative analysis of various visual cryptography techniques used by different authors.

KEYWORDS: Visual Cryptography; Shares; Encryption; Security ; Image quality; Number of shares; Decryption

I. INTRODUCTION

In the modern era the network security has become an important concern as we all know that now a days it is not difficult to get any information on internet. To make an information fully protected from hackers is a big challenge. Encryption is the solution of this problem so that even if the hackers steal the encrypted data, they cannot get any information from the data.

A new cryptography technique called visual cryptography is used to secure the visual content such as texts or images. In this technique,division of image takes place into parts called shares and then these shares are distributed to the participants. The decryption side gets the original image by stacking the shares.first of all,the concept of visual cryptography was given for binary or monochrome images. Later on, this technique was enhanced for the color images like gray images and rgb/cmyk images. The different methods are developed for rgb or cmyk images based on the color decomposition techniques[9].

An encryption technique called visual cryptography does not allow cryptic to be possible unless the proper key is supplied by the user and it is possible to perform decryption without computer intervention. the main principle is the splitting of image into k shares and decryption is possible if the user has all the shares.if the user has k-1 shares then it will not reveal any useful information [4].

One of the approach to keep a secret safe is secret sharing. Visual Cryptography is the well known approach if the secret is an image.Most of the studies discuss the concept of visual cryptography for binary images. Later on,Visual Cryptography was extended for Gray Scale Images.Another visual cryptography scheme is (k, n)-threshold scheme.This scheme was described by Naor and Shamir. In this,a secret image is encoded into n shadow images also called shares .Recovering secret image involves stacking any k of the n shares but if number of stacking shares is k-1 or less then no information about the secret image can be revealed[2].

In VCS, an image is splitted into a collection of secret shares and after that these shares are printed on transparencies. Any information will not be revealed by separated shares about the original image. Recovery of image can be done only by superimposing a threshold number of shares. No computation is involved in this recovery process. Human vision system is used for performing the OR logical operation(pixel wise) on the superimposed pixels of the shares. In case the pixels are small and are packed in high density then we use the human vision system for averaging out the

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

colors of surrounding pixels and a smoothed image will be formed in human's mind.Earlier the main focus of visual cryptography scheme was on black and white images. Dithering is used for preprocessing of the original image in case of gray scale images that could degrade the image quality.Pixel expansion is the another issue which means that size of the secret share is several times bigger than the original image. Quality of reconstructed images has two important parameters i.em , the pixel expansion rate which represents the resolution loss from the original image to the shares[3].

1.1 VCS SCHEMES FOR GRAY-SCALE IMAGES

To encrypt and decrypt data,a number of cryptographic techniques are used. The concept of visual cryptography was firstly introduced by M. Naor and A. Shamir in 1994 .The main use of visual cryptography is in encrypting the visual information i.e pictures, signatures etc.. No requirement of complex mathematical computation for the decryption of message is the main advantage of visual cryptography and we can use any human visual system to perform decryption .Earlier,VCS scheme was only defined for binary images which involves encoding of black and white pixels two shares and original image can be reconstructed by stacking the both shares. The visual cryptography scheme for color images was first proposed by Verheul and Van Tilborgin 1997. In this, transformation of one pixel into m subpixels is done and further division of each subpixel into c color regions.

Here the halftone technology is used on which visual cryptography technique is used Digital halftoning is used for transforming a digital gray-scale image to an array of binary values .These binary values are represented as dots in the process of printing. Error Diffusion is one of the type of halftoning technique .In this,the quantization error of a pixel is dispersed to neighboringpixelswhich have not yet been processed. The conversion of a secret colorimage is done into a halftone imageusing this concept and then two shares(share 1 and share T) are generated for each color component of the halftone image.

Then, shares like shareT is distributed in another two shares like share2 and share3. Finally the stacking of three shares (share1, share2 andshare3) is done for the decryption of original halftone image. In this method,there is an involvement of two levels of security. In firstlevel , taking any one of the share will reveal no information.In the next level,no information is revealed by stacking any two of the threeshares. To get back the information ,there is need to stack all the three shares. This approach canfurther be extended to (n, n) visual cryptography scheme[9].

Due to the limitation in black-and-white VCS schemes, another VCS scheme called k-out-of-n VCS was proposed by Verheul and Tilborg in 1997 for gray-scale images. In 2003, Lin and Tsai proposed another VCS scheme for gray-scale images for improving the pixel expansion of Verheul and Tilborg's VCS .They applied pre processing techniques such that the rate of pixel expansion is the same as that of black and white VCS scheme proposed by Naor and Shamir.
Chen et al. proposed a gray-scale VCS scheme in 2007 by extendingthe results to gray-scale images without any pixel expansion.On the other hand, this scheme had no support for colored images and only (k,k) threshold setting is supported. Also preprocessing needs to be done before secret sharing on the original images.

1.1.1 (K,N) THRESHOLD SCHEME

In this a secret division takes place into n number of shares and then distribution of shares is done among n persons.The secret can be recovered if and only if k or more of these persons i.e k<=n bring their shares together. However, if the number of persons is k-1 then secret reconstruction will fail. Because of this threshold scheme, it is also referred as a (k, n) threshold secret sharing scheme.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

1.1.2 FUNDAMENTALS OF COLOR MODEL

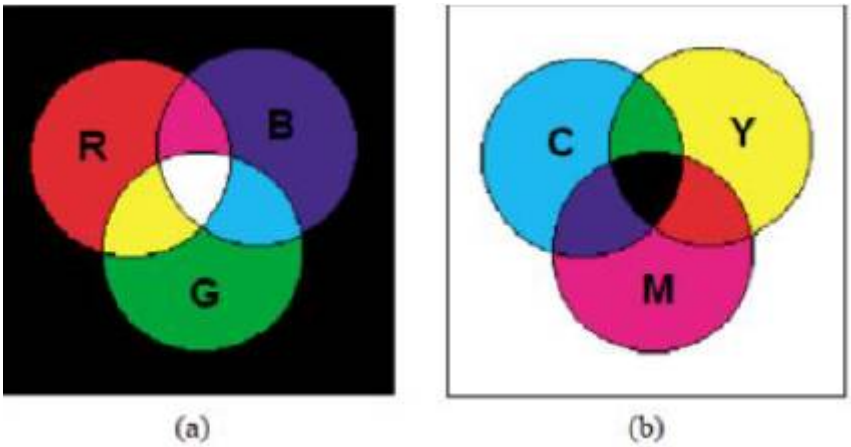

Fig .1 (a) Additive Model **Fig.1(b) Subtractive Model**

1.1.3 BASIC CONCEPTS FOR HANDLING VCS

The basic terminologies that are used in encrypting colored images through Visual Cryptographic method are discussed below.

Halftoning: This approach uses the net dots density to simulate the gray level and is called "Halftone" .It also transforms a gray level image into binary image before processing.

Color Decomposition: In this method,color decomposition is done into three primary colors. They can be C, M ,Y if subtractive model is used or R,G.,B if additive model is used.Every pixel of a color secret image is expanded into a 2x2 block in the sharing images and also two colored and two transparent pixels are kept in the block.

Pixel expansion: Pixel expansion m means the number of subpixels in the generated shares and those subpixels represents a pixel of the original input image. If pixel size is small then size of the share will be smaller. Loss in resolution can occur from the original picture to the shared one[6].

II. RELATED WORK

In [1],The characteristics of human vision are used by visual cryptography to decrypt encrypted images. Neither cryptography knowledge nor complex computation is needed. It is also ensured that hackers cannot get any clues about a secret image from individual cover images.Inthis,three methods are proposed for visual cryptography of gray-level and colorimages.The methods are proposed based on past studies in black-and-white visual cryptography,thecolor decomposition method and the halftone technology.In [2], Hou's method has been extended further so that there can be a fault-tolerant ability in new scheme.Also the secret image can still be revealed if there is a delay in one of the generated shares because of communication channel failure or by natural crash of the storage equipment,or it can be even destroyed by hackers. In this proposed scheme, a color secret image is decomposed into three shares.The secret image cannot be revealed by an individual share alone. However, if we gather any two of the three shares then secret image can be unveiled .In [3], a scheme that can satisfy all the following five commonly desired properties: (1) supporting images having arbitrary number of colors; (2) no expansion of pixel; (3) no original images preprocessing; (4) support of k-out-of-n threshold setting; and (5) a number of color levels is tunable in the secret share creation process is proposed.In [4],An efficient color image visual cryptic filtering scheme has been presented by this proposal for improving the image quality on restored original image from visual cryptic shares. A deblurring effect is presented by the proposed color image visual cryptic filtering scheme on the non-uniform distribution of visual cryptic share pixels. After the elimination of blurring effects on the pixels, there is need to apply fourier transformation for the normalization of the unevenly transformed share pixels on the original restored image.Thererfore,thequality of restored visual cryptographic image is improved to its optimal point.In [5],acolor visual cryptography scheme is proposed that uses meaningfulshares.Hackers attention will not be aroused bythese meaningfulshares . The halftone technique, secret coding table and cover coding table is utilized by the proposed scheme, to generate two meaningful shares. Comparative analysis have demonstrated that new scheme is perfectly applicable and also high security level is

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

achieved.In [6], compares and analyze the performance of various visual cryptography schemes on various parameters such as pixel expansion, shares generated,contrast etc. The compared algorithms came into aura by the rectification of their limitations.In [7], For secure transmission, there are three possible major common approaches.These are key encryption, steganography and visual cryptography. A new algorithm in which all the three approaches will be combined is proposed and this will help to overcome problems associated with these and provide additional security. A symmetric secret key is used by this scheme for the encryption of the image and then secret shares of cipher image are generated by secret sharing algorithm with steganography. So, finally meaningful stego shares of input secret image are produced by experimental results and these results also show that better quality of recovered original image is obtained by this scheme.In [8],a new design for friendly visual cryptography scheme is proposed. The hiding of secret will take place into two meaningful shares. The ratio of black-appearing in each block of the shares is same for the corresponding black (rep. white) secret pixel.Itis notpossible to disclose any information related to the secret image on each share which achieves the goal of improving security.In [9],a new scheme for encrypting secret message has been applied by authors where the secret message is embedded in three shares. For the reconstruction of the secret message all the three shares are to be stacked one by one. This is fully secured method as no information can be retrieved until and unless all the three shares are used together.The present system may be applied in different applications like defense security system, banking system, biometric data security system for the protection of dataprivacy.In [10],A new model called "A Secure Mail Application that uses Visual Cryptography and the Steganography" is proposed to improve the security of email messages. The email message which has to to be transmitted is converted to an image and then shares are generated using (2, 2) Visual Cryptographic Technique. Out of two shares, One of the shares is sent to the receiver's mail box and another one is kept with the server . There is no possibility of man in the middle attack as these shares are transmitted through different medium.Two shares are fetched at the receiver side and decrypted to get the image. The original message is reconstructed from this image.In [11],Double layer encryption and Double layer hiding is proposed which is supposed to give security to the secret data and the secret images. There is a usage of X- or base visual cryptography and higher LSB data hiding method. A Visual cryptography (VC) technique encrypts a secret image into n shares.Each participant holds one or more shares. The original motivation of Visual Cryptography is to securely share secret images in non-computer-aided environments.Devices with computational powers are ubiquitous. Double security and less complexity is proposed compared to existing system.

III .COMPARATIVE ANALYSIS

NAME OF THE AUTHOR	YEAR	TECHNIQUES USED	MERITS
1.Young-Chang-Hou*	2002	Human Visual System to decrypt secret Images.	Have backward compatibility with previous results.
2. Kun-Yuan Chao* et.al	2006	Three shares for color secret image and is fault tolerant.	Fault tolerant ability.
3.Xiaoyu Wu et.al	2009	k-out-of-n visual cryptography scheme.	No pixel expansion and combination of desired properties.
4. Shiny Malar F.R et.al	2011	Error Diffusion and Pixel Synchronization.	Complete removal of noise effects and improvement in image quality.
5. . Ch. Priyanka et.al	2012	Extended Visual Cryptography Scheme with enhanced security.	Generation of meaningful shares and high security level is achieved.
6. Neha Gupta et.al	2013	Analyze and compare performance of various VCS schemes.	Performance analyzation of various Visual cryptography scheme.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

7. PoonamBidgar et.al	2014	Key encryption, stegnography and visual cryptography.	Three approaches are combined together and provides a reliable solution.
8. Young-Chang Hou et.al	2015	Secret hiding into meaningful shares.	Friendly visual cryptography scheme and hiding of secret into two meaningful shares.
9.Sankar Das et.al	2015	Embedding of secret message into three shares.	Fully secured scheme.
10.Vidhya Lakshmi R et.al	2015	(2,2) Visual cryptographic technique for email security.	Security is ensured by using AES Algorithm and secure email messaging is achieved.
11.Anuja R. Yeole* et.al	2016	Double Layer Encryption.	Double security and less Complexity.

VI. CONCLUSION

The main conclusion is that if an image is splitted into shares(meaningless or meaningful) then the original image can be recovered if and only if some acceptable number of shares are stacked otherwise original image of same quality will not be obtained.In extended visual cryptography technique,meaningful shares are generated and high level of security is achieved.If error diffusion and pixel synchronization is used then there is complete removal of noise effects with image quality improvement . Visual cryptography ,stegnography and key encryption are combined to provide a reliable solution.Hiding of secret into two meaningful shares is the friendly visual cryptography scheme.Also,AES algorithm is used for ensuring security.Double security and less complexity is provided by double layer encryption.

REFERENCES

1. Young-Chang Hou*,'Visual Cryptography For Color Images', The Journal Of The Pattern Recognition Society : Department of Information Management, National Central University, Jung Li, Taiwan 320, ROC ,June 2002.
2. Kun-Yuan Chao* , Ja-Chen Lin,'(2, 3)-threshold visual cryptography for color images', Proc. of the 6th WSEAS Int. Conf. on Signal Processing, Computational Geometry & Artificial Vision, Elounda, Greece, August 21-23, pp.89-94,2006.
3. Xiaoyu Wu, Duncan S. Wong, and Qing Li,'Threshold Visual Cryptography Scheme for Color Images with No Pixel Expansion', Proceedings of the Second Symposium International Computer Science and Computational Technology(ISCSCT '09) Huangshan, P. R. China, 26-28,Dec. 2009, pp. 310-315 © 2009.
4. Shiny Malar F.R, Jeya Kumar M.K,'Error Filtering Schemes for Color Images in Visual Cryptography', International Journal of Advanced Computer Science and Applications, Vol. 2, No. 11, 2011.
5. Ch. Priyanka, Prof.ThaduriVenkataRamana, and T.Somashekar,' Analysis of Secret Sharing & Review on Extended Visual Cryptography Scheme',International Journal of Engineering Inventions,ISSN: 2278-7461, ISBN: 2319-6491Volume 1, Issue 10 (November2012) pp: 43-51,2012.
6. NehaGupta,Manish Gupta and AbhishekMishra,'Journey of VCS from Black and White Images to Colored Images with their Performance Analysis',International Journal of Computer Applications (0975 – 8887) Volume 79 – No9, October 2013.
7. PoonamBidgar,NehaShahare ,'Secret Image Transmission through Image Sharingusing Secret Key and LSB Embedding',International Journal of Electronics Communication and Computer Engineering Volume 5, Issue (4) July, Technovision-2014.
8. Young-Chang Hou, Zen-Yu Quan, and Hsin-Yin Liao,'New Designs for Friendly Visual Cryptography Scheme',International Journal of Information and Electronics Engineering, Vol. 5, No. 1, January 2015.
9. Sankar Das, SandipanChowdhury and DibyaChakraborty,'Visual Cryptography using Three Independent Shares in Color Images',International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 Issue 4, Volume 2 , april 2015.
10. Vidhya Lakshmi R ,Selin M,'A Secure Mail Application Using Steganography and Visual Cryptography', Global Journal of Engineering Science and Research Management, ISSN 2349-4506, September, 2015.
11. Anuja R. Yeole*, Prof. Mahip M. Bartere,'A X-or base image encryption and data security through higher lsb data hiding approach: a review',International Journal Of Engineering Sciences & Research Technology,ISSN: 2277-9655 ,February, 2016

BIOGRAPHY

Er. Rimsy Dua is a student of M.Tech.(Computer Science) at Ganpati Institute of Technology and Management, Bilaspur, Yamunanagar, Haryana, India, affiliated to Kurukshetra University, Kurukshetra. Shecompleted her Bachelor of Engineering (B.E) in 2014 from Ganpati Institute of Technology and Management, Bilaspur, Yamunanagar, Haryana, India, affiliated to Kurukshetra University, Kurukshetraand pursuing Master of Technology (M.Tech.) in

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Computer Science from Ganpati Institute of Technology and Management, Bilaspur, Yamunanagar, Haryana, India, affiliated to Kurukshetra University, Kurukshetra.Her research interests are Security(Visual Cryptography,Graphical Password Authentication),Software Testing,Intelligent computing etc.

Er. Narender Singh is an Assistant Professor in the department of Computer Science and Engineering atGanpati Institute of Technology and Management, Bilaspur, Yamunanagar, Haryana, India, affiliated to Kurukshetra University, Kurukshetra. He completed his Bachelor of Engineering (B.E) in 2006 from C.R.State College of Engineering, Murthal, Sonipat, Haryana, India and Master of Technology (M.Tech.) in 2010 from MIET, MMU, Mullana,Ambala, Haryana, India.He Published 16 research papers in various research Journals, International & National Conferences. His research interests are Simulation, Computer Networks (wireless Networks), Intelligent Computing, Neural Networks & Genetics Algorithms, etc.