ISSN:0975-9646

An Enhanced NVSS Scheme for Visual Secret Sharing

Chinju V.C.[#1], Dr.D.Loganathan[*2]

[1]*Final year M. Tech CSE, MET'S School of Engineering, Mala, Trissur, Kerala.*
[2]*HOD, Department of CSE, MET'S School of Engineering, Mala, Trissur, Kerala.*

***Abstract*— Nowadays internet has emerged has one of the convenient and most widely used media for information exchange. The information's exchanged by users through internet include secret data's, images, text etc. Thus, it leads to the need for security and enhanced privacy in internets to protect these information's from unauthorized hacking process. Visual secret sharing is a technique that encrypts visual information's using simple algorithm in place of complex ones that used in traditional cryptography. The new existing VSS scheme is called Natural-Image Based Visual Secret Sharing Scheme (NVSS) which share one digital image over n-1 natural image and one noise-like share image. This scheme is proposed with an aim to reduce the transmission risk during the transmission phase. But it fails to solve this problem fully. So to avoid this problem this paper presents an enhanced NVSS scheme which helps in avoiding the transmission risk problem.**

***Keywords*- Secret sharing scheme, Visual cryptography, Pixels, Security.**

I. INTRODUCTION

With the recent advancement in network technology internet has become the medium of transport for information exchange worldwide. Various confidential data which also include multimedia information's are transmitted over internet conveniently. Hence it is mandatory to provide security of the data and to protect the data from unauthorized hacking process. In the present era, different encryption/decryption technologies are available to secure the data. With such technologies the data is disordered after encryption and is recovered by using the correct key.

To conceal the secret data many cryptographic methods are introduced which include complex computational process and requires high computation cost for encryption and decryption process. As a result, many visual secret sharing schemes are proposed which uses simple algorithms. Visual cryptography (VC) is a technique used to encrypt image-based-secrets [1]. The secret information can be plain text, written document, images etc. The basic concept in visual cryptography is to encrypt the secret image into n shares, which separately reveals no knowledge about the secret image and distribute it to participants as shown in figure 1. Each participant will get a piece of secret share.

And decoding is performed by human visual system without any need of complex computation process. The secret image is only revealed once sufficient number of shares is combined together. In short, it needs neither cryptographic knowledge nor complex computations. The simplicity of this technique attracts each domain to adopt this technology to secure information against misuse and un-authorized access.

Different domains have different requirements for the security of their secret image and so different visual cryptographic techniques are introduced to the world. But whatever visual cryptographic technique is employed, the main goal of these techniques is to provide secure data transmission and to stop the unauthorized users to access the secret data. Sharing and delivering secret information's is also called as Visual Secret Sharing (VSS) Scheme.

This paper attempts to examine different visual secret sharing techniques for secure data transmission and introduce a enhanced NVSS scheme for VSS.

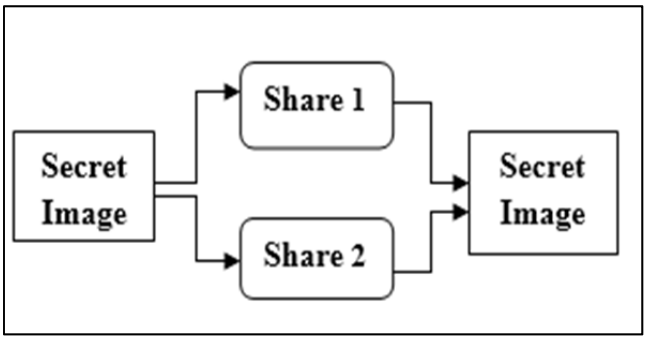

Fig 1: Traditional Visual Cryptography Scheme.

II. LITERATURE SURVEY

Networks, both internet and intranet provides variety of opportunities, but not without some risk. Internet usage and online applications are experiencing a spectacular growth. Similarly, the intruder's and the evolution of their technique are also increasing. Without proper cryptographic method in websites, the data is subjected to several kinds of attacks. Visual cryptography is a kind of cryptographic technique for securing visual secret images. Various techniques in visual cryptography are as follows:

A. Basic Visual Cryptography

Basic Visual Cryptographic technique was introduced by Moni Naor and Adi Shamir in 1994 [1] and [4]. They proposed a (k,n) threshold visual cryptography scheme

which encodes a given binary secret image into n shares and distributed among n participants, where each participant receives one share. Participants are unaware of the shares given to each other. In this technique decryption is successful only by collecting atleast k pieces or more together and is superimposed. Any k-1or fewer of them fail to recover the secret image. If user loses some of the shares even then the secret image can be revealed, if minimum k number of shares is obtained.

B. Visual Cryptography Schemes For General Access Structures

In (k, n) visual cryptography scheme, any k out of n shares can reveal the secret information. And it may compromise the security of system. So to solve this problem, (k, n) visual cryptography model to general access structure is introduced [3]. In this technique, the set of n shares is divided into two subsets namely qualified and forbidden subset of shares depending upon the importance of shares. Stacking k shares from qualified subset of shares can reveal secret information, but fewer than k shares from qualified subset of shares can not reveal any secret information. And no secret information can be revealed from forbidden subset of shares.

C. Visual Cryptography Schemes For Gray Images

All the above visual cryptography schemes are limited to binary images. That means this technique can be applied to only black and white pixels images. But this may not be sufficient for real time applications. So to meet this problem, visual cryptography schemes for gray images are introduced [5] and [9]. In this technique a dithering method is used to convert gray level image into approximate binary image. After conversion, existing visual cryptography techniques for binary images are applied to create the shares.

D. Visual Cryptography Schemes For Color Images

In this technique, a color image to be protected is taken along with a binary image which is used as a key to encrypt and decrypt is taken as input as in [5] and [10]. The secret image to be secured is decomposed into three monochromatic images based on YCbCr color space system. After this, the monochromatic images are converted into binary image, and finally the obtained binary images are encrypted using binary key image, forming share 1.Then the binary images are combined to obtain share 2. For encryption Exclusive OR operation is done between binary key image and three half-tones of secret color image separately. In the decryption process, the shares are decrypted, and the recovered binary images are inverse half toned and combined to get secret color image.

E. Extended Visual Cryptography Techniques

In previous visual cryptography schemes, shares are created as random patterns of pixels and the shares appears as noise like images. This will arouse the suspicion of intruder's that there is some hidden data in this images. And this may compromise the security of the system. So as a solution to this problem extended visual cryptography scheme is introduced [6]. In this scheme it adds a cover image to each noise like share image and in that cover image it will hide the secret image. There are two phases in this technique. In the first phase based on an access structure, using an optimization technique the meaningful shares are constructed. And in next phase, using stamping algorithm cover images are added to each shares. By using this technique pixel expansion problem can be reduced.

Table 1. Comparison summary of different Visual Cryptography techniques.

Visual Cryptography Techniques	Merits	Demerits
Basic VC	Provide security of binary images	Secret cannot be decoded by any or fewer participants
VC Schemes For General Access Structures	It is better for pixel expansion	Only qualified shares decrypt the secret image not forbidden shares
VC Schemes For Gray images	This technique increase in size& quality of o/p image	This scheme is not useful for color images
VC Schemes For color images	It decrease the pixel expansion & provide better quality due to binary representation of color image	Time consuming and contrast loss on decryption and images losses the information due to halftone Process.
Extended VC	It suitable for natural images	It generate meaningful shares but its quality is poor
Visual Secret Sharing Scheme	It suitable for natural images	Uses only single carrier and have transmission risk problem
NVSS Scheme	Uses digital secret image and diverse media as carrier	Transmission risk problem is not solved fully

F. Visual Secret Sharing Scheme

This is a technique used to deliver and transmit secret images. Visual secret sharing scheme use a single carrier for sharing images. In a (2, 2)-VSS scheme, the cipher text and secret random key is taken as two shares and they are distributed to two participants who involve in the scheme [1]. In the decryption process, the participants can decrypt the secret images through shares. This technique uses only single carrier.

G. Natural Image Based Visual Secret Sharing Technique

The above VSS scheme suffers from transmission risk problem. So to remove this problem a new technique called Natural Image Based Visual Secret Sharing Technique is introduced [7]. In this scheme the secret image is divided into n shares and distributed into participants. These natural shares along with the generated

share are then transmitted to the receiver side. In the decryption process, using the secret image and natural shares the original image is recovered. The natural image can be printed or in digital form. This NVSS scheme used diverse media for sharing secret image.

III. Comparison Among Visual Cryptography Schemes

All visual cryptography techniques are different. None of them have same usage and each one is used for special purpose needs. Moreover, different implementations of the same cryptographic schemes will provide very different levels of security. Above discussed all schemes are different and have both merits and demerits. Comparison summary of different visual cryptography techniques is as follows.

(a) (b)

Fig 2: Examples of natural images that can be used as shares.

IV. Existing Nvss Scheme

From the above comparison study, it clearly point out that each visual cryptography technique has its own merits and demerits. The last technique NVSS has more advantages. In the previous techniques they allowed either binary or gray scale images. But in this technique, any images can be used like natural images as in figure 2, printed images etc.

This NVSS scheme also has some demerits that, it cannot fully solve the transmission risk problem. So to solve this problem some enhancement is provided to the NVSS scheme and is explained further in this paper. The method used in the existing NVSS scheme is that, it can share a true color secret image by dividing it into n shares and distributed among the participants [7]. There are mainly five modules in this method.

A. Image Processing

In the proposed NVSS scheme the natural shares can be either printed or digital images [7]. If the natural share is printed image, it will undergo an image processing step. In this step the printed images are preprocessed by cropping the input image and are resized to the predicted size. The cropping is done by manually and the image is stored for further processing.

B. Feature Extraction

Feature extraction process extracts features from each one of the natural shares. There are mainly three steps carried out in this process as proposed in [7]. The first step is binarization step, in which it divides the natural shares into different blocks of same size. And then a binary feature matrix is extracted from each of the natural share by calculating the median of each pixel values. Next step is stabilization process. This step is carried out with the result of binarization process. Stabilization process is used to balance the number of black and white pixels in each block of the extracted feature image. This process makes sure that number of black and white pixel in each block is same. Third step in feature extraction is chaos process. This process is used to terminate the texture that may appear on the extracted feature images and generated share. Then the original feature matrix is disordered by adding noise in it.

C. Encryption

In case of printed images before encryption, pixel swapping of these images is carried out in order to provide tolerance of the image distortion caused due to image processing step. In NVSS scheme, it can encrypt a true color secret image and n-1 natural share and it generates a noise like share [7].

D. Data Hiding

After encryption, the output generated will be a noise like share image. So this data need to be hided somewhere, in order to avoid intruder's attack. For this purpose Quick Response (QR) code technique is used [7], which conceals the noise like share image into a QR code.

E. Decryption

Reversal process of encryption is done to decrypt the secret image [7]. And again pixel swapping and feature extraction is done to predict the true color secret image.

V. Enhanced Nvss Scheme

The existing NVSS scheme shares a true color secret image using n-1 natural shares and one noise-like share image. The main purpose of this method is to avoid the transmission risk problem that usually occurs due the intruder's. And using this existing NVSS scheme the transmission risk problem is recovered but not completely. It is because after encryption, the output generated is a noise-like share image. And this noise-like share data is concealed using a data hiding technique called QR code techniques.

The QR code is a two-dimensional code, which encodes meaningful information in both dimensions and in the vertical and horizontal directions. This technique is widely used today in daily life on surface of products, in commercial catalogs etc. It is this nature of QR code; it is now widely used as a means of secret communications. And this point out the disadvantage of existing NVSS scheme. Because in the existing NVSS, the noise-like share image is hided using QR code technique. This causes intruder's to easily suspect that there is some

hidden data inside it and leads to transmission risk problem. So to avoid this problem, an enhanced NVSS scheme is introduced in this paper to convert this noise-like share image to another digital image. And this conversion can be done using Lazy Wavelet technique, a latest stagenographic technique available in market today.

In this technique, initially Lazy wavelet transformation is applied to the cover image, in which the data is to be hidden. The result of this wavelet transformation is four sub bands of image namely Approximate Coefficients (CA), Vertical Coefficients (CV), Horizontal Coefficients (CH), Diagonal Coefficients (CD).The next step in this technique is to hide the noise like data in one of these sub bands. The data can be hidden in any of the three sub bands namely CV, CH , CD . Once the data is hidden inverse wavelet transform is applied to transform the sub bands back into image. For decryption reverse process is done.

VI. CONCLUSION

In current scenario, confidentiality of data has become a major concern in internets. Level of security increases, depends on how much confidential the data is. Security system should consider reliability, usability and human factors. Visual cryptography serves as an important aspect for security of visual images. Different visual cryptographic methods are used for different images. In this paper, an enhanced method for Natural Image Based Visual Secret Sharing (NVSS) Scheme is proposed. It is found that this method is very simple, effective and user friendly and also recover's the transmission risk problem completely.

REFERENCES

[1] "Visual cryptography". In Proceedings of Advances in Cryptology, EUROCRYPT 94, Lecture Notes in Computer Science, 1995, (950):pp. 1-12,

[2] Moni Naor and Adi Shamir"An Overview Of Various Visual Cryptography Schemes", International Journal Of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 9 ,September 2013,

[3] Suhas B. Bhagate,P.J.Kulkarni "Visual cryptography for general access Structure," Inf. Comput., pp. 86–106 , 1996 ,

[4] G. Ateniese , C. Blundo A. D. Santis and D. R. Stinson. "A Survey on Visual Cryptography Techniques and their Applications", International Journal of Computer Science and Information Technologies, Vol. 6 (2) , 2015, 1076-1079,

[5] Ms. Bhawna Shrivas, Prof.Shweta Yadavs."Visual Cryptography Scheme : A Review ", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064,

[6] Anjali Maharudra Bhunje, Premanand K. Kadbe. "Extended VC for natural images," J. WSCG, vol. 10, no. 2, 2002, M. Nakajima and Yamaguchi., Digital Image Sharing by Diverse Image Media,"ieee transactions on information forensics and security, vol. 9, no. 1, january 2014,

[7] Kai-Hui Lee and Pei-Ling Chiu."An Extended Visual Cryptography Algorithm for General Access Structures,"ieee transactions on information forensics and security, vol.7, no.1, February 2012,

[8] Kai-Hui Lee and Pei-Ling Chiu."Visual cryptography for graylevel images by dithering techniques", Pattern Recognition Letters, V.24 n.1-3,

[9] Chang-Chou Lin, Wen-Hsiang Tsai."Colour Visual Cryptography Schemes" , IET Information Security, vol. 2,No. 4, pp 151-165, 2008, F. Liu, C.K. Wu, X.J. Lin.

Chinju V.C. received B.tech degree in computer science and engineering from Calicut University, Kerala, India. And currently pursuing M.Tech in computer science from MET'S School of Engineering, Mala, Calicut university, Kerala, India.

Dr.D.Loganathan is a Professor and Head of Computer Science and Engineering department in MET'S School of Engineering, Mala, Trissur, Kerala. After his B.E., and M.E degree, he accomplished a doctoral degree from Anna University, Chennai, India. He has more than 19 years of teaching experience and having 7 years of research experience in engineering field. His research interest includes Wireless Communication, Wireless Ad hoc Networks and Image Processing. He has published several research papers in various international journals.