A Survey on Various Visual Secret Sharing Schemes with an Application

John Justin.M
PG Research Scholar,Image Processing Group
Karunya University
Coimbatore,India.

Alagendran.B
PG Research Scholar,Image Processing Group
Karunya University
Coimbatore,India.

Manimurugan.S
Assistant Professor, Dept of Computer Science and Technology
Karunya University
Coimbatore,India.

ABSTRACT
This paper focuses mainly on the different kinds of Visual Secret sharing techniques that are existing, and framing all the techniques together as a literature survey. Aim an extensive experimental study of implementations of various available VSS techniques. Also focuses on the encryption techniques that are used in each schemes with their performance parameter, concentrates on to the security issues. This study extends to an application of the visual secret sharing scheme that embeds an extra confidential image with pair key structure with no pixel expansion.

General Terms
Image Encryption, Information Encryption, Double Encryption, Chaotic Encryption.

Keywords
Open Multimedia Applications Platform, Blind source separation based encryption, Least Square Approximation, Block-Based Image Encryption Algorithm

1. INTRODUCTION
In recent years of internet world, many people transmit their secret information through the Internet. Hence it is necessary to provide safety and security to our data and to protect our data from unauthorized hacking processes. In spite of the security of sharing secret information, people usually conceal the secret data with symmetric or asymmetric cryptography, these cryptographic methods should need high computation cost in encryption and decryption processes. Therefore, many visual secret sharing schemes were proposed.

Visual secret sharing (VSS) scheme is an efficient secure method for hiding a secret image by dividing it into share images and any one can decode it easily by the human visual system. The main concept of the original visual secret sharing (VSS) scheme is to encrypt a secret image into n meaningless share images. It cannot leak any information of the shared secret by any combination of the n share images except for all of images.

2. LITERATURE SURVEY
Visual cryptography needs only the characteristics of human vision to decode the encoded images. It does not need any cryptographic knowledge or any kind of complex computation to decode the encoded image.

Mainly this visual cryptography focuses on the security aspects to safeguard the secret image from two or more cover images so that any attacker cannot retrieve any data. Naor and Shamir proposed the fundamental model of the visual cryptography, starting from their many visual cryptographic methods been evolving day by day.

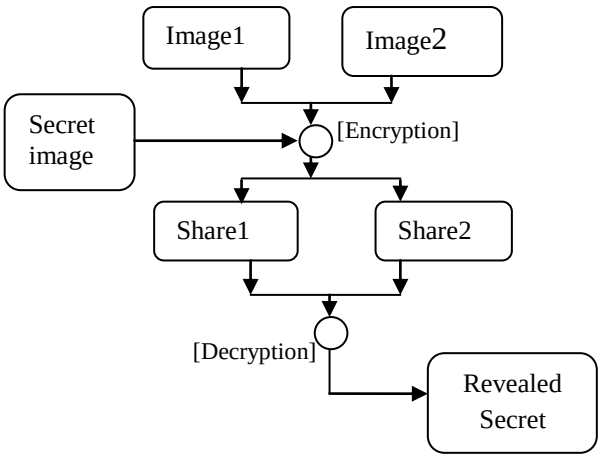

Fig 1: Idea of VSS

Hence to promote good confidentiality in transmitting of secret data via images in internet, selection of good visual secret sharing scheme is necessary. Therefore it is necessary to study all the recent technologies that are evolved and written as a literature to understand the concept of visual cryptography in a better way

Most secret sharing schemes are based on cryptography such that the encryption and decryption processes need high computation costs. Visual secret sharing schemes hide the secret image into several share images and distribute these share images to participants. With no computation, human beings are able to obtain the secret image by stacking the share images.

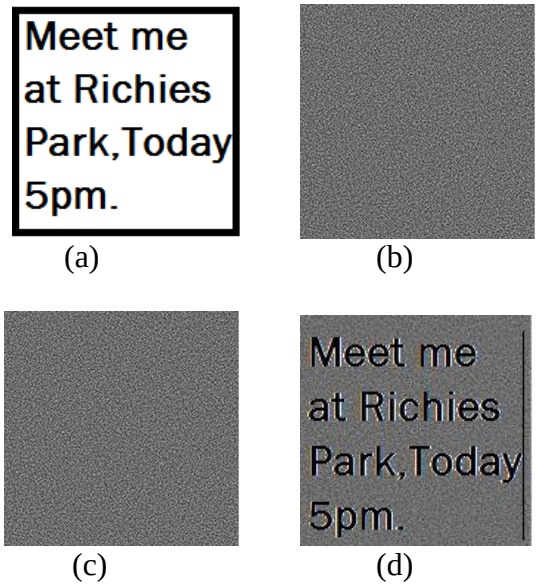

Fig 2: (a) Secret Image (b)Share Image1 (c)Share Image2 (d)Revealed Secret Image

From Fig 2the secret image was diffused and embedded on the share image 1 and the share image2. At last the secret image is revealed on staking of both the share images

Du-Shiau Tsai et al have jointly proposed a secret image sharing method for the color images with the size constraint .the concept carries by the neural networks along with the variant visual secret sharing. The main advantages of this scheme are, it supports the 24 bit color secret image, Size constraint, increased number of quality in Camouflage images, performance of bandwidth and effective memory area, Low computation time and power. Results proves its feasibility with very good PSNR value of the reconstructed image.[1]

T.H. Chen, K.H.Tsao has published a paper called Visual secret sharing by random grids. They have proposed n out of n and 2 out of n secret image sharing schemes which is based on the Random Grids .the main advantage in this technique is here there is no pixel expansion during encryption or decryption. Also codebook is used for encryption process. Where as in decryption process, the receiver has to superimpose one is by all or other one is at least two cipher-grids without any computation, resulted in getting good recognizable of secret image by the human visual system. [2] The same authors have revisited the same paper called Visual secret sharing by random grids to enhance it to the extent of basic 2-out-of-2 scheme to the n-out-of-n scheme also 2-out-of-n scheme. To calculate the performance of this scheme resulted in a good value when using the random grids [3]

Jen-Bang Feng et al have proposed a technique called Visual secret sharing for multiple secrets, in this method, the graph of the stacking process of the secret image and share images were generated for the encryption phase. Hence the secret images were got from the two share images at the aliquot stacking angles. Therefore, this paper proves the secret distortion ratio is directly related to the share destruct ratio. To prove this statement, 5% and 10% of the random distortions is added purposefully on the share image two. Resulted in, the secret information is recognizable at good rate by our visual system.[4]

Zhongmin Wang, Gonzalo R. Arce and Giovanni Di Crescenzo have jointly proposed a technique called Halftone Visual Cryptography via Error Diffusion. In this Halftone conversion techniques are used for error diffusion process. Error diffusion has the low complexity but can support the halftone share images to good extent of image quality. [5]

Another VSS (visual secret sharing scheme) was proposed by Ching-Nung Yang using probabilistic method. In this proposal, the frequency of the white pixels were used for showing the color contrast of the recovered secret image .also this method uses pixel operation with absolute non expansion of pixels.[6]

Tsung-Lieh Lin et al have jointly designed a framework for visual secret sharing scheme (VSS) with multiple secrets without the pixel expansion. In this framework, the visual secret sharing methods has been dealt in a different way, which is used along with the two binary secret images on two rectangular share images that promotes non expansion of pixels leads to high image quality. The main advantage of this method is multiple secrets were used. As the result of this, the framework has very good quality in recovering the secret image.[7]

A multi level visual secret-sharing scheme with no size expansion of pixels was put forth by Yung-Fu Chen et al. here the visual secret sharing scheme selects a block of secret image in correspondence to the same sized block in each of the share images with no pixel size expanding. In this proposal, histogram width equalization (HWE) and histogram depth equalization (HDE) were the two techniques that were used for generating the corresponding share images. Results in the increase in the quality of the reconstructed secret image when comparing with other techniques.[8]

An another color visual secret sharing scheme using non-expanded meaningful shares with authentication was proposed by Der-Chyuan Lou et all .In this proposal, visual secret sharing scheme for hiding the secret image into two meaningful cover images are used those are the share images without any pixel expansion. At the same time, this method embeds an extra confidential image in the share images. Whoever combines both the share images can reveal the secret image by super imposing them one on another without any complex computation. When one of the share images is shifted for n/2 units, the extra confidential image has been revealed. [9]

A new visual cryptography scheme by using the smooth looking decoded images of different sizes for the grey level images was designed by Tua, S.F. Houb, and Y.C. The paper addresses the problem of pixel expansion and improvement of quality of the stacked image. Here Halftoning is used for grey scale conversion. Resulted in, good visual effect on stacked image when compared to the other schemes.[10]

2.1. Comparison

This Part compares the features of some of the visual secret sharing schemes that were analyzed and studied in the literature. The Table.1 depicts the comparison between some of the VSS schemes focusing mainly on their encryption technique and the pixel expansion.

Table 1.Comparison of different VSS schemes

Schemes	Encryption Techniques	Meaningful Shares	Color Secret Share	Quality of Recovered	Pixel Expansion
[5]	Probabilistic	No	No	Recognizable	No
[4]	Error Diffusion	Yes	No	Recognizable	Yes
[9]	Codebook	No	No	Recognizable	No
[2]	Random Grids	No	No	Recognizable	No
[8]	Pixel swapping	Yes	yes	Recognizable	no

3. AN APPLICATION OF VSS

The visual secret sharing method has become an important scheme in the world of internet in transacting the images throughout the globe. The following is an application for the visual secret sharing scheme by embedding of an extra confidential image with pair key structure.

3.1. Halftone Conversion

The two input images, secret image and the extra confidential image has to be converted into halftone image in order to diffuse the secret image and the extra confidential image in the two input images. Hence halftone conversion can be done by using the Floyd Steinberg dithering process. The Floyd Steinberg dithering process can be described by the following equations (1) and (2) here 128 is the threshold value to be checked for each pixels.[9]

$$Q(u_{i\,j}) = \begin{cases} 255\ (white\ pixel\ color), u_{i,j} \geq 128 \\ 0\ (black\ pixel\ color), u_{i,j} < 128 \end{cases} \quad (1)$$

$$e_{i,j} = \begin{cases} u_{i,j} - 255, u_{i,j} \geq 128 \\ u_{i\,j}, u_{i,j} < 128 \end{cases} \quad (2)$$

Where,

$e_{i,j}$ is the quantified error at location (i, j), and

$Q(u_{i\,j})$ is used to determine a pixel value to be 0 or 255,

Here the threshold value is 128; every pixel value has to be checked with the threshold value. If the pixel value is above the threshold value then the pixel value has to be replaced by 255 which is the white pixel color and then the pixel value has to be subtracted by 255 according to the first conditions in equation (1) and (2).

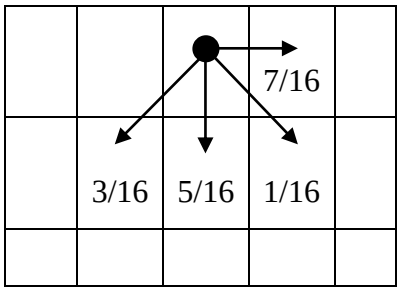

Fig 3: Floyd Steinberg diffusion matrix of distributing the error to neighboring pixels.[9]

if the pixel value is below the threshold value, then it should be replaced by '0'(zero) which is the black pixel color. And hence the residues obtained by the above equations have to be distributed to its neighboring pixels. The fractions of the residues that are to be distributed to the four neighboring pixels of right forward position, right diagonal position, down and left diagonal positions that are depicted in the figure fig 3.

3.2. Diffusion

Diffusing the secret image and the extra confidential image into the two input images to create the share image A and Share image B. Therefore this can be done by swapping each of the pixels in the images. Pixel swapping Algorithm was proposed by Chang et al [11]. Here each pixel has to undergo the process of pixel swapping, once if the pixel has been swapped then the resultant image is called the share images which holds or hides the secret image and the extra confidential image.

3.3. Pair Key Structure

The two input images and one secret image has been converted to the halftone image. When converting the extra confidential image to halftone and diffuse it within the input images, a pair key should be given in order to the sender and receiver to get paired mutually. If the key value matches between the sender and receiver, the receiver can further reveal the extra confidential image. If the pair key fails the receiver can shift the image but no extra confidential image has been revealed. This structure is designed in order to promote good security level in modern VSS.

3.4. Stacking

The two share images that are transmitted via internet holds the secret image, hence to reveal the secret image both the share images has to be stacked i.e. superimposing first input image with second input image.

3.4. Shifting

Shifting is the process of placing the first share constantly and shifting the second share image to certain unit say N/2. [9] to reveal the extra confidential image. If the pair key from the sender and the receiver matches then it proceeds for revealing. If does not matches no secret image has been revealed to the participant.

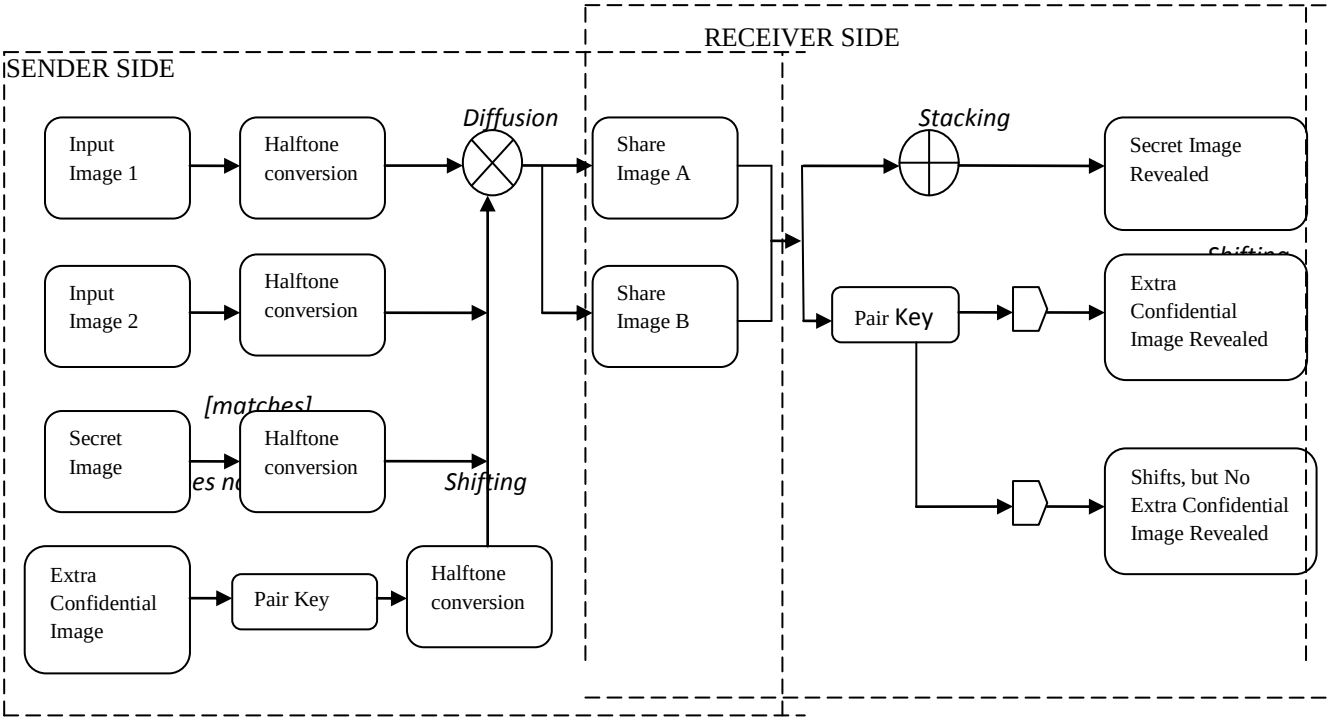

Fig 4: Visual Secret Sharing Scheme, embeds an extra confidential image with pair key structur

3.5. Sender Side

The process on the sender side goes like this, initially the input image 1, the input image 2 and the secret image are converted into the halftone image by using the Floyds Halftone method.[9] then the extra confidential image which holds the authentication details of the participant is converted into halftone image by using the pair key. Then the secret image and the extra confidential image are diffused into the two input images by pixel swapping method. [11] Once the diffusion and pixel swapping has done then the resultant share images that hides the secret image and extra confidential image is ready for the transaction via internet to the receiver depicted clearly in the above figure Fig 4.

3.6. Receiver Side

The process on the receiver side goes like this, the receiver who receives the share image A and share image B, starts stacking the shares together to reveal the secret image. And reveal the extra confidential image, the receiver has to get paired with the sender by giving the pair key. If the pair key matches then the extra confidential image is revealed to the receiver, if does not matches no extra confidential image is revealed to the receiver. Therefore the pair key structure promotes the good level of security in the VSS process..

4. PERFORMANCE PARAMETERS

The evaluation of performance of any visual cryptography schemes, which can done by considering the parameters such as PSNR (peak signal-to-noise ratio),AR (Accurate rate), and others parameters like pixel expansion, contrast of image, security enhancement, computational complexity, meaningful or meaningless shares used etc,.

The accurate rates of stacking result of original cover images and share images that are generated are discussed in Der-Chyuan Lou et al‘s model [9]. Accurate rates can be evaluated for both the Black pixel area and the White pixel area which is denoted here as ARB and ARW. The formula to calculate the Accurate Rate for Black and White pixel area is given in the following equations (3) and (4).

$$AR_B = \frac{|SR=SI=0|}{|SI=0|} \ldots\ldots\ldots\ldots\ldots (3)$$

$$AR_w = \frac{|SR=SI=1|}{|SI=0|} \ldots\ldots\ldots\ldots\ldots (4)$$

From the (3) (4), where,

SR is the stacking result of share image1 and share image 2,

SI is the secret image, symbol ‘0’ denotes black pixel, and symbol ‘1’ denotes white pixel.

5.CONCLUSION

The internet is in need of security in all the aspects of transactions of data through it. Visual secret sharing scheme promotes some level of security. Hence to know more about different kinds of visual secret sharing schemes and its performance, the Literature has been done in this paper. To sum up, all the techniques are different and used for different usages in real time. Some techniques are sensible, because they suit for appropriate places but not in all the places. Everyday new VSS techniques are evolving hence selection of the fast and secure Visual secret sharing technique will always useful mainly in terms of security issues. An application that has been discussed in this paper holds a pair key structure which promotes good level of security in revealing the extra confidential image.

6. REFERENCES

[1] Du-Shiau Tsai , Gwoboa Horng , Tzung-Her Chen c, Yao-Te Huang " A novel secret image sharing scheme for true color images with size constraint" *Information Sciences*, vol. 179, pp. 3247–3254, 2009.

[2] T.H. Chen, K.H. Tsao, "Visual secret sharing by random grids ", *Pattern Recognition*, vol. 42, no.9, pp.2203–2217, 2009.

[3] T.H. Chen, K.H. Tsao, "Visual secret sharing by random grids revisited", *Pattern Recognition*, vol. 42, no.9, pp.2203–2217, 2009.

[4] J.B. Feng, H.C. Wu, C.S. Tsai, Y.F. Chang, Y.P. Chu, "Visual secret sharing for multiple secrets", *Pattern Recognition*, vol.41, no.12, pp. 3572–3581 , 2008.

[5] Z. Wang, G.R. Arce, G.D. Grescenzo, "Halftone visual cryptography via error Diffusion", *IEEE Transactions on Information Forensics and Security*, vol. 4, no.3, pp. 383-396, 2009.

[6] C.N.Yang, "New visual secret sharing schemes using probabilistic method", *Pattern Recognition* Letters, vol.25, no.4, pp. 481–494, 2004.

[7] Tsung Lieh Lin et al, "A novel visual secret sharing (VSS) scheme for multiple secrets without pixel expansion", *Expert Systems with Applications*, vol. 37, pp. 7858–7869, 2010.

[8] Yung-Fu Chen , Yung-Kuan Chan , Ching-Chun Huang , Meng-Hsiun Tsai c, Yen-Ping Chu "A multiple-level visual secret-sharing scheme without image size expansion", *Information Sciences*, vol. 177 , pp. 4696–4710, 2007.

[9] Der- Chyuan Lou, Hong-Hao Chen, Hsien-Chu Wu, Chwei Shyong Tsai, "A novel authenticable color visual secret sharing scheme usin non-expanded meaningful shares", Elsevier on Displays,vol.32,pp.118-134,2011

[10] Tua, S-F,Houb, Y-C, "Design of visual cryptographic methods with smooth looking decoded images of invariant size for grey-level images", *Imaging Science*,vol.55,pp.90-101,2007.

[11] Y.-F.Chang,J.-B.Feng,,C.-S.Tsai,Y.-P.Chu,H.C.Syu, "New data hiding scheme using pixel swapping halftone images" The Imaging Science Journal, vol 56,pp no.279 -290, 2008.

AUTHORS PROFILE

1. M.John Justin received the B.E degree in Computer Science and Engineering from the Anna University, Chennai, India, in 2010, and pursuing his M.Tech degree in Software Engineering in Karunya University, Coimbatore, India .His research interests include image processing, software engineering.

2.B.Alagendran received the B.E degree in Computer Science and Engineering from the Anna University, Chennai, India, in 2010, and pursuing his M.Tech degree in Software Engineering in Karunya University, Coimbatore, India. His research interests include image processing, software engineering, data mining.

3. S.Manimurugan received the B.E. degree in Computer Science and Engineering from the Anna University, Chennai, India, in 2005, and the M.E. degree in Computer Science and Engineering in 2007. He is currently pursuing the Ph.D. degree in Computer Science and Engineering in Anna University, Coimbatore, India. His current research interests are in Image Processing, Information Security.