ISSN:0975-9646

Survey on Size Invariant Visual Cryptography

Biswapati Jana[1] ,Gargi Hait[2] ,Shyamal Kumar Mondal[3]

[1]Assistant Professor, Department of Computer Science, Vidyasagar University, PaschimMedinipur,
[2] Student, Department of Computer Science, Vidyasagar University, PaschimMedinipur
[3]Associate Professor, Department of Mathematics, Vidyasagar University, PaschimMedinipur
West Bengal, India.

Abstract:Security of information hiding become important in a number of application areas of today's world. Audio, video, pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or several number or even help to prevent unauthorized copying directly. Visual Cryptography Scheme (VCS) is a cryptographic technique in which visual information(e.g. printed text, pictures etc.) encrypted by generating shares (transparencies) of a binary secret image into meaningless shadow images, where decryption can be performed by a human visual system without any computational cost. There are various measures on which performance of VCS depends, such as pixel expansion, contrast, security, computational complexity, meaning full or meaningless share generation, types of secret images (either binary or color) and the number of secret images encrypted by the schemes. Some research is going on in VCS with no expansion of share size compared with original secret image. In this survey paper we try to summarize size invariant share generation techniques in VCS.

Keywords: Visual Cryptography (VC), Visual Cryptography Scheme (VCS), Size Invariant Visual Cryptography Scheme (SIVCS), Visual Secret Sharing (VSS).

I. INTRODUCTION

The traditional Visual Secret Sharing (VSS) first proposed by Naor and Shamir[1], which generates shares (transparencies) of a binary secret image into meaningless shadow images, and the recovered secret image can be achieved without any computational cost by human visual system. In Visual Cryptography (VC) a secret image is encrypted into several shares which is completely unrecognizable by human visual system. While the shares are separate, the secret image is completely incoherent. Each share holds different pieces of image and the secret image comes out only by stacking a sufficient number of shares together. Each Participant holds a share. Shares are presented in transparencies. VC eliminates complex, mathematical computation to recover the secret. The encrypted message can be decrypted directly by the human visual system. In Noar and Shamir [1] scheme, there is a main shortcoming, expansion that means the recovered image is bigger than the original one, and it will cause the distortion of the secret image. Performance of any (k,n) VSS is measured against four criteria: security, accuracy, computational complexity and the size of the share generation. The first criterion is satisfied if each share does not convey any information about the original secret image and the original secret image cannot be reconstructed if fewer than k shadows are collected. The second criterion is measured by Peak Signal to Noise Ratio (PSNR) and relative entropy etc., implies similarity between the original secret image and the reconstructed image using shares. A high PSNR implies a high-accuracy secret image sharing scheme and low relative entropy implies a high –accuracy secret image sharing. The computational complexity criterion is concerned with the total number of operators required to generate the set of shares for a secret image and to reconstruct the recovered original secret image by using the k shares collected. The last criterion, which affects data transmission speed, is also called pixel expansion. A large share size implies both high transmission cost and high storage cost.

The main drawback of VSS [2] is the large pixel expansion during reconstruction of secret. Many schemes have been proposed to solve the problem of pixel expansion. Both Ito et al. [3] and Yang [19] applied probability concepts in the design of a probabilistic visual secret sharing scheme called ProbVSS for binary images. Chen et al. [4] proposed a size invariant scheme using block encoding method. In this scheme original image is first divided into several blocks then encode a block instead of a pixel at a time. Each block is encoded into k blocks on k shares and each block generate share is composed of s/2 white pixel and s/2 black pixel. The reconstructed image can be same size of original image. To improve the image quality after the secret image is reconstructed; Lin et al. [6] proposed a method using multi-level encoding. Yang and Chen [4] introduce a new method to achieved aspect ratio invariant VC scheme using image filtering and resizing. Li, Ma and Li [7] proposed an improve aspect ratio invariant VC scheme with optimal size expansion. Compare to the previous schemes their scheme has better visual quality. Lee et al. [18] proposed a multi-level encoding scheme based on Chen's technique and it improve the image quality.

This paper is subdivided into six sections. In section- II, Visual Cryptography and its work has been mentioned. The size invariant Visual Cryptography and their comparison is highlighted in the section-III. In section-IV, comparison of current size invariant VC scheme has been described. In section-V, conclusion of this work has been described.

II. VISUAL CRYPTOGRAPHY (VC)

Visual cryptography (VC) uses two transparent images which generates from original secret. One image contains random pixels and the other image contains the secret information. It is impossible to reveal the secret information from one of the images. Both transparent images and shares are requiring revealing the secret information by stacking together. The easiest way to implement visual cryptography is to print the two shares onto the transparent sheets. The technique was proposed by Moni Naor and Adi Shamir in 1994[1]. They demonstrated a VSS scheme, where an image was broken up according to some predefine matrix into n shares. While any n-1 shares revealed no information about the original image. Each share was printed on separate transparencies, and decryption was performed by overlaying the shares. When all the shares ware stack, the original image would appear.

Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) 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. In the Figure-1, it can show 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.

The system of pixel can be applied in different ways. In this example, each pixel is divided into four blocks. However, we can also use pixels, divided into two rectangle blocks, or even divided into 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. If the pixel states of layer-1 are truly (crypto secure) random, both empty and information pixels of layer-2 will also have completely random states. One cannot know if a pixel in layer-2 is used to create a grey or black pixel, since we need the state of that pixel in layer-1 (which is random) to know the overlay result. If all requirements for true randomness are fulfilled, VC offers absolute secrecy according to the Information Theory.

If VC is used for secure communications, the sender will distribute one or more random layers-1 in advance to the receiver. If the sender has a message, he creates a layer-2 for a particular distributed layer-1 and sends it to the receiver. The receiver aligns the two layers and the secret information is revealed without the need for an encryption device or computer. The system is unbreakable, as long as both layers don't fall in the wrong hands. It is impossible to retrieve the encrypted information from any one layer.

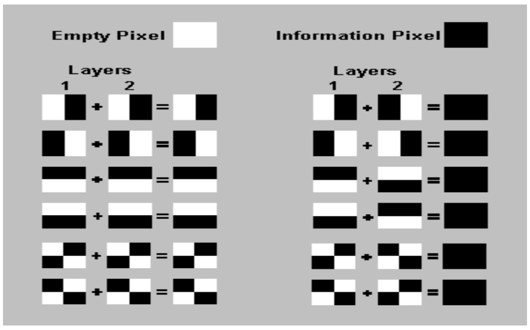


Figure-1: Division of pixel into sub-pixel

In *k out of k* visual cryptography scheme, it generates *k* transparencies from an original secret image. The transparencies are usually shared by *k* participants in such a way that the stacking of any *k* share images will reveal the secret image while from any less than *k* share images one can deduce no information about the secret image. The *k out of n* schemes generates n transparencies from an original secret image. The transparencies are usually shared by n participants so that each participant is expected to keep one transparency. The secret image can be observed if any k or more of them are stacked together. However, the secret image is totally invisible if fewer than k transparencies are stacked. The images on transparencies are called shadow images. The pixels on shadow image are called shares. A share consists of m black and white sub-pixels. The structure is usually described by a n×m Boolean matrix $M = [m_{ij}]$. Here m_{ij}= 0 or 1 if the jth sub-pixel in the ith shadow is white or black respectively.

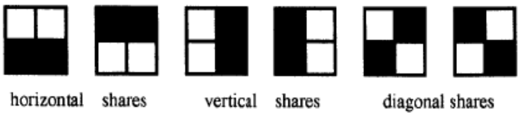


Figure-2**:** Six possible patterns of sub-pixel arrangements with 50% gray. Each pattern is represented as [0 0 1 1], [1 1 0 0], [0 1 0 1], [1 0 1 0], [0 1 1 0], [1 0 0 1] from left to right.

Let M_r denotes the m-D vector obtained by taking the Boolean "OR" of r row vectors. The gray level of a pixel combined by r shares is obtained the Hamming Weight $H(M_r)$ of the "OR"ed m-D vector M_r. Users interprets this gray level as black if $H(M_r) \geq t$ and as white if $H(M_r) > t-\alpha$ m. Here t € {1,…,m} is called threshold, while the value $\alpha > 0$ and the number α m ≥ 1 are called relative difference and contrast respectively.

The (k,n) VSS consists of two collections of n×m Boolean matrices C_w and C_b where any matrix in C_w generates a white pixel with k or more of shares while a matrix in C_b generates a black pixel. The scheme is valid if it fulfils the following three conditions:

1. For any M in C_w, the "OR" vector Mk of any k rows of M satisfies $H(M_k) < t$-αm.
2. For any M in C_b, the "OR" vector Mk of any k rows of M satisfies $H(M_k) \geq t$.
3. For any subset $\{i_1, i_2,\ldots,i_q\}$ of {1, 2,…,n} with q < k, the two collections of $q\times m$ matrices D_w $_{and}$ D_b obtained by extracting rows $i_1, i_2,\ldots,i_q$ from $n\times m$ matrices in C_w and C_b are indistinguishable so that the collections contain the same matrices with the same frequencies.

Size expendable VSS Scheme (single & multiple secret images):

In traditional VSS [1] the process of pixel mapping to sub-block technique is used which introduces pixel expansion. The number of sub pixels represents expansion of the secret image and should be as small as possible. The pixel in the secret image is mapped into (m x n) blocks in each share, so recovered secret image is (m x n) times larger than the original secret image. In this reason the recovered image becomes poor in contrast. Therefore the secret image can be hard to interpret.

Also output share images become larger than secret image so, it increases the storage and/or transmission cost or inconvenient for carrying. Wu and Chen [2] proposed a Visual Secret Sharing for Multiple secrets (VSSM) scheme for two secrets which can encrypt two secret images into two square share images. The first secret image SE1 can be revealed by stacking share images S1 and S2. The second secret image SE2 can be revealed by stacking S2 and S1 that are rotated by theta degree, and theta is designed to be 90^0 and can be modified to be 180^0 or 270^0. As with Naor and Shamir's [1] scheme, Wu and Chen's [2] VSSM scheme expands one pixel of each secret image into a sub-block with a 4 times pixel expansion.

III. Size invariant VSS Scheme

In order to reduce the pixel expansion of VCS, many Size Invariant Visual Cryptography Scheme (SIVCS's) has been developed. Some techniques are summarizing below.

(1) Ito et al. ProbVC technique[3]:

The main idea behind the proposed SIVCS is the probabilistic visual cryptography (ProbVC) which was first proposed by Ito et al.[3]. They constructed the (k, n)-VCS by using two collection of column vectors, C_0 and C_1, which are transformed from basic matrices of the conventional (k, n)-VCS. Suppose the basis matrix contains *n x m* entries, C_1 (C_0) will contain *mn x1* columns vectors. To share a black (white) pixel one of the column vectors in C_1 (C_0) is randomly chosen and then distributes i^{th} entry in the column vector to i^{th} share. In this fashion, each secret pixel within a secret image is encrypted in only one pixel in each constituent share. Thus, image size of shared and stacked images is same as the secret image.

(2) Chen's technique [4]:

In Chen's technique [4] without image size expansion, it divide the original image into several blocks, each containing *m* x *n*=*s* pixels. Next, encode a block instead of a pixel at a time. Each block is encoded into *k* blocks on *k* shares and each block generated in shares is composed of *s*/2 white pixels and *s*/2 black pixels. By this improvement the shares and the reconstructed image can be the same size as the original image. The scheme first computes the average gray-scale intensity of the blocks in the original image and dispatches all the possible values of average intensity into *s*/2+1 level. Consequently, each block in the original image with gray-scale intensity level *x* (x ranges from 0 to s/2) is mapped on the block containing s/2+x black pixels. It is a major improvement compared to the previous scheme. In a traditional VSS, a unit in an original image can simply generate two kinds of corresponding results in the reconstructed image. For example, a pixel generates two kinds of blocks, which uses two black and two white pixels to represent white, and four black pixels to represent black. Only two results are used to represent the secret. However in this scheme, *x* kinds of reconstructed blocks are used to provide a better power of expression. Fangs [8] proposed a visual secret sharing method in reversible style without size expansion. In this method there are four steps to generate the share. Before generating the shares, divide the original image and share into two same size parts, upper part and lower part. This method does not need to define look up table. First secret image can be revealed by stacking the share of two secret images and second secret image is revealed by stacking after turnover the second share. He used random grid method in reversible style. Using random grid method in this scheme recovered image is same size as the original image.

(3) Fang's Shift Style Scheme [9]:

In this scheme there are two phase (1) encoding phase and (2) decoding phase. Two Original Images (512 by 512 pixels) and (368 by 368 pixels) divided into two shares s1 and s2. This method can compute original image by stack the two shares. Stack two share and get first secret image, shift the stack location of second share after that two share are stacked and second secret image is reveal. Lin et al. [6] proposed a encrypting and decrypting process. Encrypting included 3 processes: (1) DSP (dividing and separating process). (2) SP (stacking process).and (3) CMP (camouflaging with maximum block density process). In DSP, the first function was to divide each secret image into blocks with n x n size, and the second function was to separate each block of the two secret image into two subsets without intersection according to the black pixel on one *n* x *n* block. In SP, the function was to stick the subsets obtained by DSP to generate the share images, and two subsets of secret image ware stack to share image s1 and s2 respectively. The first subset of second secret image was directly stack on the corresponding position of s1 while, the second subset was rotated with 180^0 and stack to the corresponding position of s2. The function of the last process, CMP, was to camouflage two share images to make the density of the black pixel on each block of one share image to be equal by referencing maximum block density of all blocks. In the decrypting process, the first secret image was revealed by directly stacking the share image s1 and s2. To reveal the second secret image, share s1 was stacked and share image s2 with a rotated 180^0. It is applicable only two secret images, not more than two. At the beginning two empty share images (i.e., the pixel color is white) with a size equal to that of the secret image must be generated. Then, each secret image must be divided into with n x n size. According to the position of each black pixel and the sum of black pixels on the block, one block can be randomly separated to two subsets without any black pixel being overlapped and the difference in the number of black pixel between two subsets must be equal to or less than one. Stacking these subsets they get the reconstructed image which size is same as original secret image. To share each block in the secret image using shadow images, Lin et al. [12] divided the blocks of the secret image into three categories. The first category contains secret blocks with at least one black color; the second category contains secret block with two black colors; and the third category contains secret blocks with three or four black colors. After dividing all blocks into three categories, the next step is to examine the black color's position in the secret block, and then choose the share pair according to a predesigned codebook. The purpose of Lin et al.'s[12] method is to achieve similarity between the secret block and the recovered block, so that the stacking result can conform to the corresponding secret block.

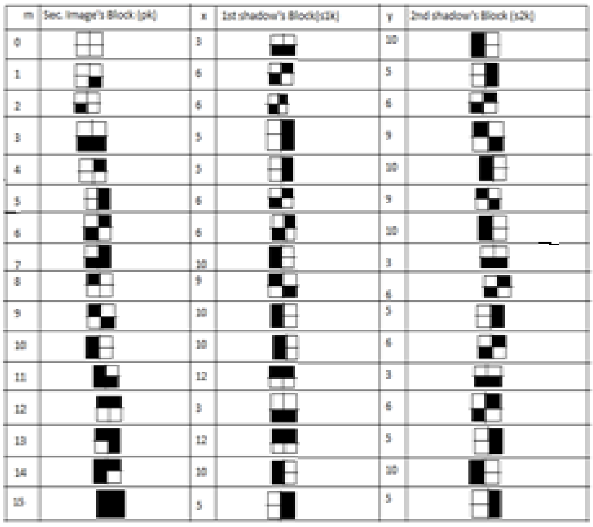
(4) Wang & Chang Scheme[14]:

This method is a non-expansion and reversible secret image sharing based on multi-level encoding. They encode the secret image into two meaningless shadow images; therefore, this scheme is a (2,2) secret image sharing scheme. The size of the secret image is M x N. The software Photoshop was used to transform the gray scale image G into the halftone image I. For the security purpose, they first use a key k to randomly generate an image of the same size of the secret image, which is used to permute I, and generate the permuted secret image P. After the permutation, divide P into non-overlapping 2x2 blocks, and generate the codebook by the following equation

$$m = (2 * x + y) \bmod 16 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

where m is the decimal value of the 2x2 permuted secret Block P_k, and x and y are two decimal values of the shared blocks S_{1k} and S_{2k}, respectively. To get the binary sequence from P_k and convert it into decimal value, They scan the 2x2 blocks of secret image in the order of left to right, up to down. The codebook of their scheme can be seen in Table-1. The white color corresponds to bit 0, and the black color to bit 1.The first, third and fifth columns are the decimal values of m, x and y, which corresponding to the secret block, first shadow block and second shadow block as shown in the second, fourth and sixth columns, respectively. Finally, the key k is divided into two parts where each part must be sent to different users, as well as the shadows. To decrypt the secret from the two shadows, the users must cooperate with each other, since each of them have a part of the key k and one shadow. First they use Equation-1 to recover the permuted secret image P. And then, the key k is used to calculate the inverse permutation and to reconstruct the original secret image I without any distortion on the contrast quality. Askari, Moloney & Heys Scheme[16] is construct a (2, 2) scheme share but can be easily extended to the schemes developed in earlier studies, such as the (k, n) VSS scheme. The block section, mapping process and encoding process are the three steps in the scheme. At first the image is divided into number of blocks with 2 x 2 pixels. The secret image is called as a secret block, and the block in the secret image a share block. The next step is to categories the secret blocks: if the secret block contain one black pixel (three white pixels) or three black pixels (one white pixel) they are randomly mapped to one of the three secret blocks.

Otherwise no mapping process is required. In the encoding process 8 patterns of share blocks are available for each secret block, with all the share blocks comprised of 0, 2, or 4 black pixels. Since each share block is equally likely occur for any original secret image block, no information of the secret image can be gained by examining only one share. So this scheme provide better security. Shares are created by randomly selecting one of the 8 possible share blocks as the first share block and then selecting the second share block in a way such that the reconstructed secret block is obtained by stacking the first and second share together using the XOR operation (where the XOR of two pixels with same color is black and two pixels of different color is white). As a result the secret image, share image and reconstructed image have the same size and recovered secret blocks differ only slightly from the original secret block. Thus the scheme introduces some noise into the recovered secret image.



m	Sec. Image's Block (pk)	x	1st shadow's Block(s1k)	y	2nd shadow's Block (s2k)
0	□□ □□	3	□□ ■■	10	■□ ■□
1	□□ □■	6	□■ ■□	5	□■ □■
2	□□ ■□	6	□■ ■□	6	□■ ■□
3	□□ ■■	5	□■ □■	9	■□ □■
4	□■ □□	5	□■ □■	10	■□ ■□
5	□■ □■	6	□■ ■□	9	■□ □■
6	□■ ■□	6	□■ ■□	10	■□ ■□
7	□■ ■■	10	■□ ■□	3	□□ ■■
8	■□ □□	9	■□ □■	6	□■ ■□
9	■□ □■	10	■□ ■□	5	□■ □■
10	■□ ■□	10	■□ ■□	6	□■ ■□
11	■□ ■■	12	■■ □□	3	□□ ■■
12	■■ □□	3	□□ ■■	6	□■ ■□
13	■■ □■	12	■■ □□	5	□■ □■
14	■■ ■□	10	■□ ■□	10	■□ ■□
15	■■ ■■	5	□■ □■	5	□■ □■

Table-1: Codebook of Wang and Chang scheme

(5) Huang & Chang Scheme[17]:

At first the original image is divided into four regions. According to block encoding, the original secret image is divided into a number of blocks with 2×2 pixels in each region. In the secret block, same color pixels are considered as a group, and each group generates a number of combinations of share group. According to each region of the original image, region shares are generated in the second phase. They follow certain sequence to generate region shares, and sequence is according to orderly original region to share. By the way, all region shares are collected as share image S1 and share image S2. Moreover, extra confidential data can also be revealed by reversing one of share images then stacking. The extra confidential data can prevent the detection of information.

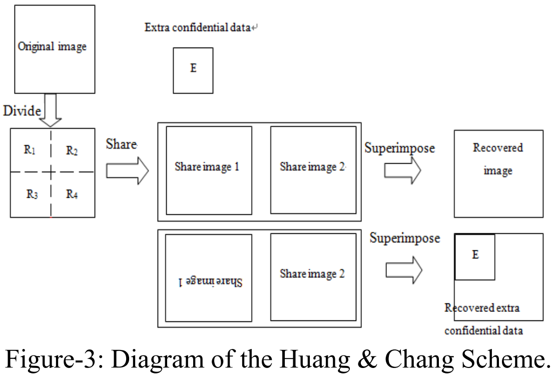
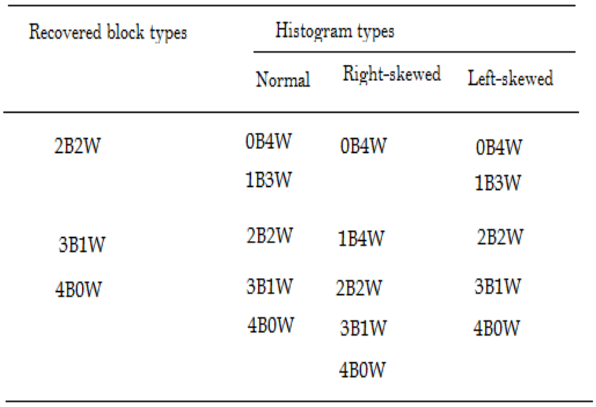


Figure-3: Diagram of the Huang & Chang Scheme.

Pixel expansion is a serious issue to solve this problem and improve the image quality this study divides the original image into four regions and combines the scheme with authentication.

(6) Lin et al. Scheme [18]:

The secret image I is a gray-scale image. In Step-1, the half tone process is used to transform the secret image I into a half tone image called IH. The error diffusion is one of the simpler techniques with lower time complexity and high visual quality. The half tone technique simulates gray scale image by the density of black pixels. The denser the black pixels, the higher the degree of grayness. On the contrary, the sparser the black pixels, the lower the degree of grayness. In Step2, the histogram of the secret image is obtained by censusing the frequency of each gray value. It presents the time distribution of different gray values. By observing the distribution of the histogram, the property of image can be recognized, e.g. its darkness, brightness, or normal situation. In the third step, their scheme observes the distribution of the histogram, and then determines if it is a right-skewed, left-skewed, or normal distribution Note that in traditional investigations, each pixel of the original image is mapped on to a block consisting of several pixels. Due to the expansion, there covered secret is distorted and the cost transmission is increased. They adopt a block-by-block method to encode IH to avoid this issue. This scheme divides halftone image IH into blocks which consist of four pixels each. Which have three kinds of gray levels, and five kinds of block types, 0B4W, 1B3W, 2B2W, 3B1W, and 4B0W. Their proposed encoding method of different block types



Recovered block types	Histogram types		
	Normal	Right-skewed	Left-skewed
2B2W	0B4W 1B3W	0B4W	0B4W 1B3W
3B1W	2B2W	1B4W	2B2W
4B0W	3B1W 4B0W	2B2W 3B1W 4B0W	3B1W 4B0W

Figure-4: Block types

The above operation is taken repeatedly block after block. When all the blocks in IH are encoded, the two shares can be generated. At the last step, they super impose the two shares. Result show that the proposed scheme is prior to the previous investigation.

IV. COMPARISON

In this paper various size invariant visual cryptography schemes are studied and their performance is evaluated on some criteria: number of secret images, pixel expansion, and image format and type of share generated etc. While selecting visual cryptography for a particular application Table-3 is helpful. If minimum bandwidth is available to share the secrets then some schemes are better choice. For sharing multiple color images schemes be employed. For avoiding attention of hackers while transmitting the confidential messages, some technique can use steganography combination with visual cryptography. In Noar and Shamir scheme they use single secret image and their recovered image is 4 times larger than the original image and poor contrast image is recovered. Based on the Noar and Shamir scheme Wu and Chen proposed a scheme using two secret image but in this scheme image size also expanded 4 times. Ito et al. scheme first proposed a non-expanded VSS scheme, recovered image same size as original image but the quality of the recovered image is low. Chen et al. scheme improve the image quality but in this scheme reconstruct image have some regionalization visual effect. In Wang scheme they make a low computation to decrypt secret and they achieve a loss less reconstruction of the original image and guarantee the security of the image but in Lin et al. scheme they cannot achieve reversibility in the reconstruct image and neither guarantee the security of the secret image. Askari's scheme applied both for binary and halftone images. Their scheme is substantially clear than in other proposed non-expansion scheme but this scheme also have some noise into the recovered image. Based on Chen et al. scheme Lee et al. scheme proposed a multi-level encoding scheme depend on histogram distribution and the recovered image is same size as the original image and high quality than the previous proposed scheme.

Scheme	*Year*	*Shares*	*No of Secret*	*Encoding method*
Ito et al.	1999	n	Single	Pixel Encoding
Chen's Scheme	2007	2	Single	Block Encoding
Fang's Scheme	2009	2	Double	Random Grid
Lin et al.	2010	2	Double	Block Encoding
Lin et al.	2010	2	Single	Block Encoding
Wang's Scheme	2011	2	Single	Multi-level Encoding
Askari's Scheme	2012	2	Single	Block Encoding
Huang's Scheme	2013	2	Double	Block Encoding
Lee et. al. Scheme	2013	2	Single	Multi-level Encoding

Table-2: Comparison table with respect to encoding method

Technique name	*Share generation*	*Decoding method*	*Share no*	*Numb secret*	*Attacks*	*Security analysis*	*Multi-level encoding*
Ito et al	Using two basic matrix C0 and C1	Overlap all shares	n	1	Not tested	Yes	No
Chen's scheme	Based on their basic code	Stack two share	2	1	Not tested	Yes	Yes
Fang's 1st Scheme	Using random greed method	Stack two share 1st secret recover stack one share with turnover another 2nd secret recover	1 for each	2	Not tested	No	No
Fang's 2nd Scheme	Using random greed method	Stack two share 1st secret recover stack one share with shift of another 2nd secret recover	1 for each	2	Not tested	No	No
Lin et al	Using DSP,SP and CMP	Stack two share 1st secret get stack one share with 180^0rotate of another share 2nd secret get	2	2	Not tested	No	No
Lin scheme	Account the no of black pixel this scheme have a code book and depending on this code book share is generated	Stack share images together	2	1	Not tested	No	No
Wang and Chang scheme	Generate a codebook by the equation **m=(2*x+y) mod 16** and depending on this code book share is generated	Using this equation permuted secret image recover and the key k is used to calculate inverse permutation and to reconstruct the original secret	2	1	Not tested	Yes	Yes
Askari's scheme	Shares are created by randomly selecting one of the 8 possible share blocks (share blocks comprised of 0, 2 or 4 black pixels)	Stack two share using XOR operation	2	1	Not tested	Yes	No
Hung and Chang scheme	Region share are collected as share image1 and share image2	Original image recovered by stacking two share and extra confidential data can be revealed by reverse stacking of one share	2	2	Not tested	No	No
Lee et al.	According to the type of histogram encode halftone image into two shares based on the basic code of Chen's scheme	Superimpose the two shares	2	1	Not tested	No	Yes

Table-3: Comparison with respect to decoding method, security analysis and multilevel encoding method**.**

V. CONCLUSION

In this paper, we give an overview of SIVCS as special instances of secret sharing method among participants. We described about visual cryptography and its work, and combined a different kinds of SIVCS and there comparison. Some authentication with steganography and cheating prevention schemes are used in SIVCS. Also visual cryptography for color multiple secrets are emerging in this field. Extended Visual Cryptography Schemes (EVCS) for natural image used in many real application.

REFERENCES

[1] M. Naor and A. Shamir, “Visual cryptography,” *Advance in Cryptology: Eurpocrypt'94*, Lecture Notes In Computer Science, Springer Verlag, Germany, Vol. 950, pp. 1–12, 1995.

[2] Wu, C.C. & Chen, L.H. “ A study on visual cryptography”. Master thesis. Institute of Computer and Information Science, National Chaio Tung University, Taiwan, R.O.C.(1998).

[3] R. Ito, H. Kuwakado, H. Tanaka,“ Image size invariant visual cryptography”, IEICETrans. Fundam. Electron. Commun. Comput. E82-A (10)(1999)2172–2177.

[4] Y. F. Chen, Y. K. Chan, C. C. Huang, M. H. Tsai, Y. P. Chu, “ A multiple-level visual secret-sharing scheme without image size expansion”, Inform. Sci. 177(21)(2007)4696–4710.

[5] Lin, T. H.; Shiao, N. S.; Chen, H. H.; Tsai, C. S.: “A new non-expansion visual cryptography scheme with high quality of recovered image”, IET International Conference on Theory, Technologies and Applications, Frontier Computing., 2010, pp. 258-263.

[6] T. L. Lin, S.J. Horng, K. H. Lee, P. L. Chiu, T. W. Kao, Y. H. Chen, R. S. Run, J. L. Lai, R. J. Chen: “A novel visual secret sharing scheme for multiple secret without pixel expansion”. (2010) pp. 7858-7869.

[7] P. Li, P. J. Ma, D. Li. : “Aspect ratio invariant visual cryptography scheme with optimal size expansion”. (2012). pp. 219-222.

[8] W. P. Fang: “Non-expansion visual secret sharing in reversible style”. (2009). Vol. 9. pp. 204-208.

[9] W.P. Fang.: “Non expansion hiding secret image in visual secret sharing with shift style”. (2009) pp. 555-558.

[10] Z. Zhou, G. R. Arce, G. Di Crescenzo. “Halftone visual cryptography”. (2013). pp. 521-524.

[11] Chandramathi S. , Ramesh Kumar R. , Suresh R. and Harish S.” An overview of visual cryptography”. International journal of computational intelligence techniques. (2010) vol.1. pp. 32-37

[12] T. H. Lin, N. S. Shiao, H. H. Chen, C. S. Tsai. ”A new non-expansion visual cryptography scheme with high quality of recovered image”. (2010) pp. 258-263.

[13] S. J. Lin, S. K. Chen, J. C. Lin.: ”Flip visual Cryptography(FVC) with perfect security, conditionally optimal contrast, and no expansion” (2010) pp. 900-916.

[14] Z. H. Wang, C. C. Chang, M. S. Pizzolatti. “ A new reversible secret image sharing scheme based on multi-level encoding”. (2011) pp. 607-612.

[15] F. Liu, T. Guo, C. Wu, L. Qian.“Improving the visual quality of size invariant visual cryptography scheme” (2012) pp. 331-342.

[16] N. Askari, C. Moloney, H. M. Heys.: “ A novel visual secret sharing scheme without image size expansion”. (2012). IEEE 25th Canadian conference on electrical and computer engineering.

[17] Y. J. Huang, J. D. Chang.: “Non-expanded visual cryptography scheme with authentication”. (2013) pp. 165-168.

[18] C. C. Lee, H. H. Chen, H. T. Liu, G. W. Chen, C. S. Tsai: “A new visual cryptography with multi-level encoding”.(2013).

[19] C.N. Yang, New visual secret sharing schemes using probabilistic method, Pattern Recognition Letters 25 (4) (2004) 481–494.