



A Survey on (k,n) and (n,n) Probabilistic Size Invariant Schemes in Visual Cryptography

M.Nirupama Bhat*

Research Scholar, Department of CS,
Sri Padmavathi Mahila Visvavidyalayam, Tirupati
nirupamakonda@gmail.com

K. Usha Rani

Associate Professor, Department of CS,
Sri Padmavathi Mahila Visvavidyalayam, Tirupati
usharanikuruba@yahoo.co.in

Abstract: In this information age, there is an increased concern towards the privacy and security of information stored in the computer systems. Visual Secret Sharing Schemes (VSS) are secured way of storing data in the form of images, divided it into a number of shares and kept at different locations in a distributed form. Recovery of the secret image is performed by stacking all or few of the shares together. Traditional VSS schemes have a drawback of pixel expansion. This can be overcome by the size invariant probabilistic schemes of Visual Cryptography. This paper studies some of the size invariant (k,n) and (n,n) schemes and analyses the characteristics of the recovered image.

Keywords: Visual secret sharing schemes, Size invariant probabilistic schemes, Visual Cryptography

I. INTRODUCTION

The secret sharing scheme was proposed by Blakley[1] and Adi Shamir[2] for the construction of robust key management scheme by distributing the secret information to several participants and can be recovered only by the cooperation of all the participants.

In 1994 Moni Naor and Adi Shamir[3] combined the mechanisms of secret sharing and traditional cryptography, named Visual Cryptography, as it is a kind of secret sharing scheme where a secret in the form of an image is split into random shares and distributed to the participants. The random shares separately doesn't reveal any information of the secret image. The superimposition of these shares recover the concealed information of the secret image by the human visual system without any aid of the computer or computations. One of the main drawbacks of traditional VCSs is the pixel expansion. In traditional VCSs, each pixel in the original secret image is represented using m pixels in each of the resulting shares. The parameter m is known as the pixel expansion, because the recovered image will be m times larger than the secret image [3]. This reduces the quality of the recovered image [4]. Pixel expansion also increases the size of the shares, which creates inconvenience for the participants while carrying them. In order to overcome the practical problems, many size invariant visual cryptography schemes[5-7] were proposed. The shares have the same size as the original secret image.

The size invariant schemes are based on the probabilistic principle, where the size of the transparencies is same as that of the secret image. This paper provides an overview of various probabilistic size invariant visual cryptography schemes.

II. DIFFERENCE BETWEEN DETERMINISTIC AND PROBABILISTIC MODELS OF VISUAL CRYPTOGRAPHY

Cimato et al.[7] has elaborated the difference between the deterministic and probabilistic models of visual cryptography, while reconstructing the secret image. The

deterministic model usually used in previous work[3], subdivides each secret pixel into a number of sub pixels. Hence the reconstructed image is m times bigger than the original one. In probabilistic model of Yang[6], each pixel is reconstructed with a single pixel. Hence, the reconstructed image is size invariant without any pixel expansion. During the reconstruction of the image, an approximation of the secret pixel is guaranteed in the deterministic model, whereas the secret can be reconstructed only with certain probability in the probabilistic model. Yang's aim is to provide schemes with no pixel expansion, which are obviously desirable. However the quality of the reconstructed pixel depends on how big the probabilities are of correctly reconstructing secret pixels. In a deterministic scheme, the reconstruction is guaranteed with a certain pixel expansion. In a probabilistic scheme, the reconstruction with no pixel expansion with a (small) probability of making mistakes in reconstructing the secret image. Thus, depending on the requirement, conventional(pixel expansion) or probabilistic(without pixel expansion) schemes can be used.

III. CONVENTIONAL VISUAL SECRET SHARING SCHEME

Before discussing the probabilistic visual secret sharing scheme let us brief the conventional VSS scheme[3]. Naor and Shamir defined his scheme as follows: The VSS for binary images considers only white and black pixels. Each pixel in the secret image is expanded into m black and white sub pixels in n shares. A $n \times m$ Boolean matrix $S = [s_{ij}]$, where s_{ij} represents the collection of sub pixels in each share. $s_{ij} = 0$ if the j th sub pixel in the i th share is white, and $s_{ij} = 1$ otherwise. When shares i_1, i_2, \dots, i_k are stacked together in a way, which properly aligns the sub pixels, secret image whose sub pixels are represented by the Boolean "OR" of rows i_1, i_2, \dots, i_k in S , will be revealed. The gray level obtained from this stacking process is proportional to the Hamming Weight $H(V)$ of the "OR"ed m -vector V . This gray level is interpreted by the HVS as black if $H(V) \geq d$, and as white if $H(V) \leq d - \alpha m$. d and α correspond to the threshold and relative difference value or contrast respectively.

Definition: A solution to the (k, n) VSS scheme can be described via using the two sets of $n \times m$ Boolean matrices represented by B_0 and B_1 . Each row in each matrix in B_0 or B_1 defines the values of m sub pixels in corresponding shares. One of the matrices in B_0 is randomly chosen to share a white pixel; and to share a black pixel dealer randomly chooses one of the matrices in B_1 . Chosen B_0 and B_1 sets are considered valid if the following three conditions are met [3]:

- For any S in B_0 , the “OR”ed V of any k of the n rows satisfies $H(V) \leq d - am$.
- For any S in B_1 , the “OR”ed V of any k of the n rows satisfies $H(V) \geq d$.
- For any subset $\{i_1, i_2, \dots, i_q\}$ of $\{1, 2, \dots, n\}$ with $q < k$, the two sets of $q \times m$ matrices obtained by restricting each $n \times m$ matrix in B_0 and B_1 , to rows i_1, i_2, \dots, i_q are not distinguishable in the sense that they contain the same matrices with the same frequencies.

The first two criterions represents the contrast, by satisfying the conditions that HVS can distinguish the black and white pixels by the contrast ratio. Last condition is the security condition which states that any $k-1$ or fewer of the shares contain insufficient information for recovering the secret image.

For conventional VSS schemes, a pixel in the original image is expanded to m subpixels and the number of white subpixels of a white and black pixel is h and l . When stacking k shadows, we will have “ $m - h$ ” B “ h ” W subpixels for a white pixel and “ $m - l$ ” B “ l ” W subpixels for a black pixel.

IV. PROBABILISTIC SIZE INVARIANT VISUAL SECRET SHARING SCHEMES

Ito et al [5] has proposed a size invariant (k,n) VSS, k is the threshold shares and n is the total shares. The structure of Ito et al’s scheme is constructed by using two sets of $n \times m$ Boolean matrices C_0 and C_1 . Two $n \times m$ matrices S^0 and S^1 are randomly chosen from C_0 and C_1 and to share a white pixel one of the columns of S^0 and to share a black pixel one of the columns of S^1 are chosen randomly. The column vector is described by a Boolean n -vector $V = [v_i]$, $v_i = 1$ for a black pixel and 0 for a white pixel in the i^{th} share. During the stacking up of shares, the color of the pixel is determined as “OR”ed value of the corresponding elements in V . p_0 and p_1 are the probabilities with which a black pixel in the reconstructed image is generated from a white and black pixels respectively, in the secret image. Thus, the reconstructed image can be recognized as a secret image by the contrast as the absolute difference in the probabilities $\beta = |p_0 - p_1|$. This is a secure scheme and the reconstructed image is well visible.

The Boolean matrices used by Ito in (k,n) scheme is as follows with S^0 as $n \times n$ matrix having one column with 1’s and all other columns as 0’s and S^1 as a unit matrix. This is same as the matrix used by Adi and Shamir in their conventional visual cryptographic scheme. For a $(2,3)$ scheme the following matrices are taken, and $p_0 = 1/3$ and $p_1 = 2/3$ $\beta = |p_0 - p_1| = 1/3$

$$S_0 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \quad S_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Ching-Nung Yang [6] has proposed a size invariant (k,n) VSS scheme giving new definitions to contrast and security conditions. This scheme is non-expansion. The size of the secret and the shares are same. The frequency of white pixels is used to study the contrast of the recovered image. This method has the same contrast level as the conventional VSS scheme. This approach uses pixel operation different from the conventional scheme which uses sub pixel operation. Defined OR operation over the pixels of the shares is the same as the stacking operation of sub pixels in the conventional VSS scheme. This method uses one pixel for each of n share to represent one pixel of secret image while conventional VSS are using m subpixels. Thus, generated shares are the same size with the secret image.

The definition given by Yang is as follows:

Definition: A (k, n) -Prob. VSS scheme can be shown as two sets, white set C_0 and black set C_1 , consisting of n_x and n_y $n \times 1$ matrices, respectively. When sharing a white (resp., black) pixel, the dealer first randomly chooses one $n \times 1$ column matrix in C_0 (resp., C_1), and then randomly selects one row of this column matrix to a relative shadow. The chosen matrix defines the color level of pixel in every one of the n shadows. A Prob. VSS Scheme is considered valid if the following conditions are met.

- For these n_x (resp., n_y) matrices in the set C_0 (resp., C_1) the “OR”-ed value of any k -tuple column vector V is $L(V)$. There values of all matrices form a set λ (reps. γ).
- The two sets λ and γ satisfy that $p_0 \geq p_{TH}$ and $p_1 \leq p_{TH} - a$, where p_0 and p_1 are the appearance probabilities of the “0” (white color) in the set λ and γ , respectively.
- For any subset with $\{i_1, i_2, \dots, i_q\}$ of $\{1, 2, \dots, n\}$ with $q < k$, the p_0 and p_1 are the same.

Here, the frequency of white pixels are used to show the contrast of the recovered image.

It is observed that all the columns of the basis matrices S_0 and S_1 of a conventional VSS scheme can be used as the $n \times 1$ column matrices in the sets C_0 and C_1 , we can let the pixel appear in white color different probability instead of expanding the original pixel to m subpixel and the frequency of white pixel in white and black areas in the recovered image will be $p_0 = h/m$ and $p_1 = l/m$

Various constructions for (n,n) and (k,n) PVSS were proposed by Yang, depending on the basis matrix. The notation $\mu_{i,j}$ is used to represent the set of all $n \times 1$ column matrices with the Hamming weight i of every column vector, and j denotes the matrices belonging to C_j where $j \in \{0,1\}$.

There is a one-to-one correspondence between probabilistic model with no pixel expansion and deterministic model. Yang[6] has proved that a deterministic scheme S with contrast $\gamma(S)$ can be transformed into β -probabilistic scheme S^1 with $\beta(S^1) = \gamma(S)$ with no pixel expansion. Cimato[7] gave a complementary result and proved that the β -probabilistic scheme S with no pixel expansion can be transformed into a

deterministic scheme S^1 with contrast $\gamma(S^1) = \beta(S)$, thus saying that there is a one-to-one correspondence between probabilistic model with no pixel expansion and deterministic model. In various models sometimes the same matrix are used. But, the contrast values changes due to different interpretations given by various researchers.

Conventional VSS Schemes has a guarantee that for every black and white pixel of the original picture, there is a clear difference of these pixels in the stacked image. But, this is not guaranteed in Probabilistic VSS scheme. Thus, the recovered image is not recognizable to Human Visual System if they do not consists of enough pixels .If the secret image selected satisfies the lower bound of pixels, then even if the boundary of black and white areas in the recovered image using Probabilistic VSS Scheme is interfered, the secret can be visualized by the Human Visual System.

V. EXPERIMENTAL RESULTS

The results are compared with three different schemes, implemented by Ito[5], Yang[6] with two different constructions for(2,3) scheme as (k,n)[6] and (2,2), (3,3) schemes of [6,5]. A binary image with size 200x 100 pixels are taken and probabilistic VSS schemes are applied. The number of white pixels in original image taken is 16561 and the number of black pixels in original image: 3439 This image is divided into share images X,Y and Z.It is found that in all the discussed schemes, when all the shares are stacked together 100% black pixels are recovered.



Fig 1.Original Image

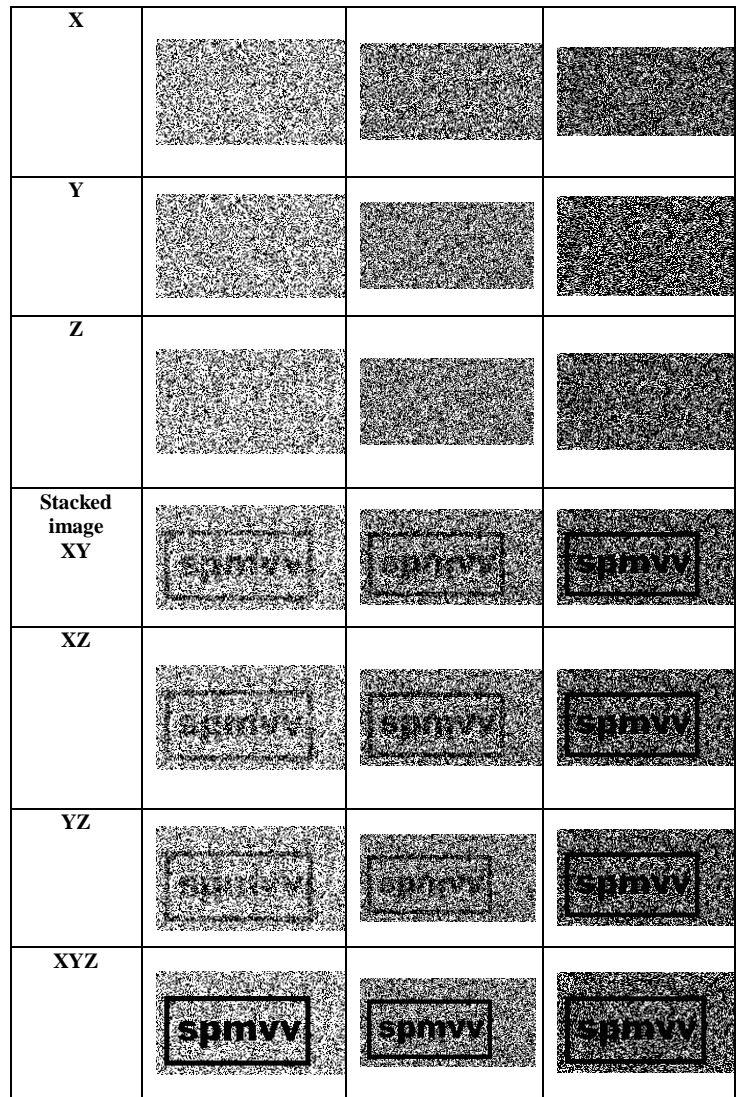


Table 1. Results of (2,3) probabilistic size invariant schemes







Method used	(2,3)[5]	(2,3)Method-1[6]	(2,3)Method-2[6]
Basis Matrix used	---	$\begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$
C_0	$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$	$\{\mu_{0,0}, \mu_{3,0}\}$	$\{\mu_{0,0}, \mu_{3,0}, \mu_{3,0}\}$
C_1	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	$\{\mu_{1,1}, \mu_{2,1}\}$	$\{\mu_{2,1}\}$
P_0	0.33	0.5	0.33
P_1	0.66	.166	0
P_{TH}	---	0.5	0.33
Contrast	$ p_0 - p_1 = 0.66$	0.33	0.33
Percentage of white pixels in (2,3)recovered image	67%	49%	34%
Percentage of black pixels in (2,3)recovered image	67%	84%	100%
Percentage of error pixels in (2,3)recovered image	33%	45%	55%






The results of the demonstrations during the study of (k,n) ie.(2,3)schemes are tabulated in Table 1.The percentage of error pixels, the percentage of white and percentage of black pixels in the recovered image of all the schemes are compared. It is found that in [5], the % of recovery of white and black pixels are same. As it is (2,3) scheme, any two shares like XY,YZ and ZX are stacked. When any two shares are stacked together, there is no visual clarity in the reconstructed image. In both the constructions of [6], the contrast is same. The later method-2[6] has only recovered 34% of white pixels recovered where as 100% of black pixels are recovered. The method_1[6] , has recovered 49% of white pixels and only 84% of black pixels. The stacked images are not clear. Thus, method-2[6] has better visual perception of the reconstructed image when compared with his first method, even when the error percent of the pixels in the recovered image is more.

Various (2,2) and (3,3) size invariant schemes are compared and the results of the demonstrations during the study of the (n,n) schemes are tabulated in Table 2. When the above schemes are implemented, it is found that the matrices used for sharing the images and contrast in [5] and [6] are same. So, the recovered image is same. As 100% of black pixels are recovered, now the way the Human Visual System perceives the image depends on the % of white pixels recovered. So, the image in method-1[6] is viewed

with better contrast. It is also observed that security in all the above schemes is maintained.

Table 2. Results of (2,2) and (3,3) probabilistic size invariant schemes

Method used	(3,3)[5]	(2,2)[6]	(3,3)[6]
Basis Matrix used	---	$\begin{bmatrix} p & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} p & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$
C_0	$\begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$	$\{\mu_{0,0}, \mu_{2,0}\}$	$\{\mu_{0,0}, \mu_{2,0}\}$
C_1	$\begin{bmatrix} p & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$	$\{\mu_{1,1}\}$	$\{\mu_{1,1}, \mu_{3,1}\}$
P_0	.75	0.5	0.25
P_1	1	0	0
P_{TH}	--	0.5	0.5
Contrast	$ p_0-p_1 =.25$	0.5	0.25
Percentage of error in pixels of recovered image	62%	41%	62%
Percentage of white pixels in recovered image	25%	50%	25%
Percentage of black pixels in recovered image	100%	100%	100%
Share X			
Share Y			

Z		As this is (2,2) scheme there wont be the third share	
Stacked image XY in (2,2)/XYZ in (3,3)			

VI. CONCLUSION

This paper has studied the characteristics of deterministic and probabilistic models of visual cryptography. The traditional secret sharing scheme[3] and the size invariant schemes discussed in [5],[6] are studied. The way in which the humans can view the image depending on the clarity and contrast are analyzed. All the implementations are performed using MATLAB.

VII. REFERENCES

- [1]. A. Shamir. How to share a secret. *Comm. ACM*, 22(11):612–613, 1979.
- [2]. G. R. Blakley. Safeguarding cryptographic keys. *AFIPS 1979 Nat. Computer Conf.*, 48:313–317, 1979.
- [3]. M. Naor and A. Shamir. Visual cryptography. In *Advances in Cryptology-EUROCRYPT'94*, page 1. Springer, 1995.
- [4]. Cimato, S., Yang, C.: Visual cryptography and secret image sharing. *Digital Imaging and Computer Vision Series*. Taylor & Francis (2011)
- [5]. Ito, R., Kuwakado, H., Tanaka, H.: Image size invariant visual cryptography. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* 82(10), 2172–2177 (1999)
- [6]. Yang, C.-N.: New visual secret sharing schemes using probabilistic method. *Pattern Recognition Letters* 25(4), 481–494 (2004)
- [7]. Cimato, S., Prisco, R.D., Santis, A.D.: Probabilistic visual cryptography schemes. *Comput. J.* 49(1), 97–107 (2006)