Analysis of (n,n) Size Invariant Visual Cryptography Schemes

M.NIRUPAMA BHAT1, K.USHA RANI2
1Department of MCA, Vignan’s University, Vadlamudi,Guntur,INDIA
2Department of Computer Science, Sri Padmavati Mahila Visvavidyalayam,Tirupati,INDIA
1nirupamakonda@gmail.com, 2usharanikuruba@yahoo.co.in

ABSTRACT

Security and privacy of information is very much essential to be maintained in the digital media. Visual Secret Sharing (VSS) is a way to protect a secret image among a group of participants by using the secret sharing. However, the size of each share generated by conventional VSS is m times bigger than the original secret image, where m is called pixel expansion. Size invariant schemes are an alternative approach to implement VSS without pixel expansion. This paper compares various (n,n) size invariant visual cryptography schemes and analyses the characteristics of the recovered image. Experimental results are provided, demonstrating the effectiveness of these schemes.

Keywords: Visual Secret Sharing, Size Invariant Visual Cryptography Schemes, pixel expansion

1. INTRODUCTION

The secret sharing scheme is a robust secret management scheme proposed by Blakley[1] and Adi Shamir[2]. The secret information is shared among several participants and is recovered only by the cooperation of all the participants. In 1994 Moni Naor and Adi Shamir[3] have constructed the mechanism of secret sharing scheme on images and termed as Visual Cryptography. It is a kind of secret sharing scheme where the secret is in the form of an image. It is split into random shares and distributed to the participants. These random shares individually don’t reveal any information of the secret image. The superimposition of these shares recover the concealed information of the secret image. This can be viewed by the human visual system without any aid of the computer or computations. One of the main drawbacks of Visual Cryptography Scheme 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 secret shares as well as the recovered image will be m times larger than the secret image [3]. This reduces the quality of the recovered image. Pixel expansion increases the size of the shares and creates inconvenience for the participants while carrying the shares. Many size invariant visual cryptography schemes[5-11] were proposed to overcome this practical problems. In size invariant visual cryptography schemes, the shares have the same size as the original secret image. Thus it reduces the storage space.

Various size invariant schemes are constructed by many researchers using probability methods, random grids and multipixel encoding techniques. The traditional Visual Secret Sharing (VSS) schemes decode the secret without computation, but due to pixel expansion, it is inconvenient for the participants to carry the transparencies along them. The quality of the reconstructed image is reduced and it takes a large storage area. In order to reduce the pixel expansion many size invariant visual cryptography schemes have been proposed such as probabilistic size invariant schemes, random grids scheme and multipixel encryption size invariant visual cryptography schemes.

Probabilistic Size invariant visual secret sharing schemes[4,5,6] for a binary image use only one subpixel to share the secret image i.e. each pixel is encrypted individually or independently in a probabilistic manner. Thus, the generated shares has the same size as the secret image, thus it is size invariant. Ito[4] in 1999 proposed a method of (k,n) probabilistic scheme by using the basis matrix used by Shamir in traditional visual Cryptography. The probabilistic method proposed by Yang[5] uses the frequency of white pixels to show the contrast of the recovered image. Random grid[9] scheme is another method, which encodes a secret image into two noise-like images, where each image is referred as a Random Grid. The size of a RG is the same as that of the secret image i.e. without pixel expansion. However, a reconstructed secret has lower visual quality in RG-based VC. To improve the visual quality of the recovered image and reduce the number of operations, multipixel[10,11] encryption strategy was proposed. Multipixel encryption methods grouped the pixels into blocks and encrypted the blocks at a time. This also improves the visual quality of the recovered image.

This paper provides an analysis of various size invariant visual cryptography schemes like probabilistic scheme[4-6], random scheme[7] and multipixel[8-11] encryption. The paper is organized as follow: Section 2 defines the traditional visual cryptography. The next 3 sections provides the overview of probabilistic, random grids and multipixel size invariant schemes. The performance of (n,n) size invariant visual cryptography schemes, where n=2, i.e.(2,2) are analyzed and results are tabulated in section 6, followed by conclusion.

2. TRADITIONAL VISUAL CRYPTOGRAPHY

Noar and Shamir[3] defined the Traditional Visual Cryptography scheme as follows: The Visual Secret Sharing scheme for binary images considers only white and black pixels. For a (k,n) scheme, each pixel in the secret
image is expanded into m black and white sub pixels and placed into n different shares. A \( n \times m \) Boolean matrix \( S = [s_{ij}] \) has 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 at least \( k \) shares \( i_1, i_2, \ldots, i_k \) are stacked together in a proper aligned way, the sub pixels superimpose on each other and the secret image is revealed. The stacking of the sub pixels are represented by the Boolean “OR” of rows \( i_1, i_2, \ldots, i_k \) in \( S \). 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 Human Visual System as black if \( H(V) = d \), and as white if \( H(V) < d - \alpha m \). \( d \) and \( \alpha \) correspond to the threshold and relative difference value or contrast respectively.

**Definition 1.** A solution to the \((k, n)\) VSS scheme can be described 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]:

1. For any \( S \) in \( B_0 \), the “OR”ed \( V \) of any \( k \) of the \( n \) rows satisfies \( H(V) \leq d - \alpha m \).
2. For any \( S \) in \( B_1 \), the “OR”ed \( V \) of any \( k \) of the \( n \) rows satisfies \( H(V) > d \).
3. For any subset \( \{i_1, i_2, \ldots, i_q \} \) of \( \{ 1, 2, \ldots, n \} \) 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 \( i_1, i_2, \ldots, i_q \) are not distinguishable in the sense that they contain the same matrices with the same frequencies.

The first two criterions represent 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.

3. **PROBABILISTIC SIZE INVARIENT VISUAL SECRET SHARING SCHEMES.**

In probabilistic mode, each pixel is reconstructed with a single pixel. So, the reconstructed image is size invariant without any pixel expansion. The secret can be reconstructed only with certain probability in the probabilistic model. The quality of the reconstructed pixel depends on how big the probabilities are of correctly reconstructing the secret. Ito et al [4] 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 subpixels of \( S^0 \) and to share a black pixel one of the subpixels of \( S^1 \) are chosen randomly. The column vector is described by a Boolean \( n \)-vector \( V = [v_1] \), \( v_1 = 1 \) 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 matrices used by Adi and Shamir in their conventional visual cryptographic scheme.

Ching-Nung Yang [5] 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 subpixel operation. Defined OR operation over the pixels of the shares is the same as the stacking operation of subpixels 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 2** A \((k, n)\)-Prob. VSS scheme can be shown as two sets, white set \( C_0 \) and black set \( C_1 \), consisting of \( n_1 \) and \( n_1, n_1 \times 1 \) matrices, respectively. When sharing a white (resp., black) pixel, the dealer first randomly chooses one \( n_1 \times 1 \) 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.

1. For these \( n_1 \) (resp., \( n_1 \)) 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 \( \lambda \) (reps. \( \gamma \)).
(2) The two sets $\lambda$ and $\gamma$ 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 $\lambda$ and $\gamma$, respectively.

(3) For any subset with $\{1, 2, 3, \ldots, q\}$ of $\{1, 2, \ldots, n\}$ 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 $p_0 = l/m$ and $p_1 = l/m$.

Various constructions for $(n,n)$ and $(k,n)$PVSS were proposed by Yang, depending on the basis matrices. The notation $\mu_{ij}$ 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 $j \in \{0,1\}$.

4. RANDOM GRIDS SCHEME

A simple technique for encryption of 2-D patterns was proposed by Kafri and Karen [7]. This is a $(2,2)$ scheme. This method can encrypt a binary image into two shadows images, called random cipher grids. The number of pixels in the encrypted shares are same as the original secret. In Visual Cryptography, each image pixel is represented as either transparent (white) or opaque (black). The two type of pixels are likely to occur. Light is transmitted through the transparent pixel, while the opaque pixel stops it. Depending on the characteristics of the shadows in the random grids, Kafri et al. proposed three visual secret sharing algorithms using random grids that differ from each other in their contrast quality.

Algorithm 1: The first shadow $RG_1(i,j)$ is generated randomly by the bits 0 or 1. The size of this share is same as the secret image. Then, if the secret binary pixel $SI(i,j)$ is equal to 0, the binary pixel of the second shadow $RG_2(i,j)$ at the same position will be the same as in $RG_1(i,j)$; otherwise, the binary pixel in $RG_2(i,j)$ will be the complement of $RG_1(i,j)$.

$$RG_2(i,j) = \begin{cases} RG_1(i,j) & \text{if } SI(i,j) = 0 \\ \bar{RG}_1(i,j) & \text{otherwise} \end{cases}$$ (1)

Algorithm 2: The first shadow $RG_1(i,j)$ is generated randomly by the bits 0 or 1. The size of this share is same as the secret image. Then, if the secret binary pixel $SI(i,j)$ is equal to 0, the binary pixel of the second shadow $RG_2(i,j)$ at the same position will be the same as in $RG_1(i,j)$; otherwise, the binary pixel in $RG_2(i,j)$ will be generated randomly by the function $f_1(0,1)$.

$$RG_2(i,j) = \begin{cases} RG_1(i,j) & \text{if } SI(i,j) = 0 \\ f_1(0,1) & \text{otherwise} \end{cases}$$ (2)

Algorithm 3: The first shadow $RG_1(i,j)$ is generated randomly by the bits 0 or 1. The size of this share is same as the secret image. Then, if the secret binary pixel $SI(i,j)$ is equal to 0, the binary pixel in $RG_2(i,j)$ will be generated randomly by the function $f_1(0,1)$; otherwise, the binary pixel in $RG_2(i,j)$ will be the complement of $RG_1(i,j)$.

$$RG_2(i,j) = \begin{cases} f_1(0,1) & \text{if } SI(i,j) = 0 \\ \bar{RG}_1(i,j) & \text{otherwise} \end{cases}$$ (3)

The contrast is defined as the absolute difference of light transmission rates between black pixel and white pixel area of the recovered image. It is found that contrasts in the three algorithms is $\frac{1}{2}$, $\frac{1}{4}$ and $\frac{1}{4}$ respectively.

5. MULTIPixel ENCRYPTION SCHEME

The multi pixel encryption scheme is a size invariant scheme. Instead of encrypting a single pixel at a time, few pixels are blocked together and encrypted at a time and divided into shares.

Chou[12] has proposed a scheme where a block of 4 pixels is taken. The secret image is divided into blocks of size 4. When the block has 0 or 1 black pixel, then it is taken as white block and if the block has 2 to 4 black pixels, it is seen as a black block. Feng Liu et al. [8] has extended the definition of multi-pixel encryption size invariant visual cryptography scheme as follows.

Definition 3: A $(k,n,t)$-Multi-pixel encryption size invariant visual cryptography scheme encrypts a block of $t$ adjacent pixels at a time, where the chosen of the $t$ pixels does not relate to the content of the secret image. For the encryption of any two blocks $B$ and $B'$ in the secret image, a $(k,n,t)$-ME-SIVCS-2 generates $n$ shares $s_1, \ldots, s_n$ satisfying

1. (Contrast) Denote $v$ and $v'$ as the vectors that consist of the secret pixels at $B$ and $B'$ respectively, and denote $v^p$ and $v'^p$ as their corresponding vectors that are no the shares $s_p$ for $P = 1, \ldots, n$. Without loss of generality, suppose $w(v) > w(v')$, then for any $k$ out of $n$ shares $\{s_{q1}, \ldots, s_{qk}\} \subseteq \{s_1, \ldots, s_n\}$, let $V_Q = v_{q1}$ OR $\ldots$, OR $v_{qk}$ and $V'_Q = v'_{q1}$ OR $\ldots$, OR $v'_{qk}$ then stacking result satisfies $w(V_Q) > w(V'_Q)$ where $w(v_Q)$ for example is the average values of $w(v_Q)$ for all the possible values of $v_Q$. 


2. (Security) Denote CF and CF as the collections of all the possible sub-matrices of any less than k shares for blocks B and B’ respectively, then CF and CF are indistinguishable since they contain the same sub-matrices with the same frequencies.

The share matrix collection C0 and C1, are taken from [8] and (2,2) Visual secret sharing scheme is applied. C0 is the matrix used to share a white block and C1 is the matrix used to generate a black block. These are generated using the matrices M0 and M1. Let $M_0 = \begin{bmatrix} 1 & 9 \\ 0 & 1 \end{bmatrix}$ and $M_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ are (2,2) basis matrix used in traditional Visual Cryptography. If the pixel to be shared is white(resp. black), the columns of M0 (resp. M1) are randomly permuted and two sub-pixels are distributed to the two shares. This process is repeated twice.

$$C_0 = \{[1010], [0110], [0001], [1011]\}$$

$$C_1 = \{[1010], [0110], [0001], [1110]\}$$

If the image block is white, one of the matrix in C0 is selected randomly and each row is distributed to each share. If the image block is black , one of the matrix in C1 is selected randomly and each row is distributed to each share. Thus shares are generated.

6. EXPERIMENTAL RESULTS

Three different (2,2) size invariant schemes of Yang[5] and random grids[7] and multipixel encryption [8,12], are implemented on binary image and the results are tabulated. A binary secret image in Figure.1 with size 200x100 pixels is taken and size invariant VSS schemes are applied. The number of white pixels in original image is 16561 and the number of black pixels in original image is 3439. It is found that in all the above discussed (2,2) schemes almost 100% black pixels are recovered. The results are tabulated in the Table.1.

![Fig.1. Secret Image.](image)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>C0</td>
<td>${[0], [1]}$</td>
<td>${[1010], [0110], [0001], [1011]}$</td>
<td></td>
</tr>
<tr>
<td>C1</td>
<td>${[1], [0]}$</td>
<td>${[1010], [0110], [0001], [1011]}$</td>
<td></td>
</tr>
<tr>
<td>P0</td>
<td>0.5</td>
<td>0.5</td>
<td>0.5</td>
</tr>
<tr>
<td>P1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Contrast</td>
<td>0.5</td>
<td>0.5</td>
<td>0.5</td>
</tr>
<tr>
<td>Percentage of error in pixels of recovered image</td>
<td>41%</td>
<td>42%</td>
<td>43%</td>
</tr>
<tr>
<td>Percentage of white pixels in recovered image</td>
<td>50%</td>
<td>50%</td>
<td>48%</td>
</tr>
<tr>
<td>Percentage of black pixels in recovered image</td>
<td>100%</td>
<td>100%</td>
<td>99%</td>
</tr>
<tr>
<td>Share X</td>
<td><img src="image" alt="Share X" /></td>
<td><img src="image" alt="Share Y" /></td>
<td><img src="image" alt="Stacked image XY in (2,2)" /></td>
</tr>
<tr>
<td>Share Y</td>
<td><img src="image" alt="Share Y" /></td>
<td><img src="image" alt="Share Y" /></td>
<td><img src="image" alt="Stacked image XY in (2,2)" /></td>
</tr>
<tr>
<td>Stacked image XY in (2,2)</td>
<td><img src="image" alt="Stacked image XY in (2,2)" /></td>
<td><img src="image" alt="Stacked image XY in (2,2)" /></td>
<td><img src="image" alt="Stacked image XY in (2,2)" /></td>
</tr>
</tbody>
</table>
When the above schemes are implemented, it is found that in all the three methods the contrast is 0.5, i.e., 50%. The percentage of recovery of black pixels is almost 100 and that of white pixels is around 50%. If the amount of pixels are considered, the recovery is same in all the three methods. The Human Visual System perceives the recovered image of multipixel encryption method with better contrast. Security is maintained in all the three schemes. All implementations are implemented using MATLAB tool.

CONCLUSION

The probabilistic, random grids and multipixel encryption size invariant schemes are studied and analysed. Though the contrast is same in all the recovered secrets, there is difference in the visual quality of the images. The perceived quality of the recovered image is an important issue especially in size invariant schemes, as preserving the size of the image definitely loses some information in the image. The human visual system does not depend only on the contrast of the recovered image. It also depends on the way the pixels are organised in the image.

REFERENCES