Chapter 3

Visual Cryptography

3.1 Introduction

1994, Naor and Shamir [48] described a new $(k,\ n)$ visual cryptographic scheme using black and white images, where the dealer encodes a secret into n participants. In this scheme, a shared secret information (printed text, handwritten notes, pictures, etc.) can be revealed without any cryptographic computations. For example, in a $(k,\ n)$ visual cryptography scheme, a dealer encodes a secret into n shares and gives each participant a share, where each share is a transparency. The secret is visible if any k(or more) of participants stack their transparencies together, but none can see the shared secret if fewer than k transparencies are stacked together. By identifying that the result of stacking the transparencies are the same as Boolean-OR operation denoted by $\vee$ on the binary digits involved, it

is possible to extend the Visual Cryptography schemes to any binary string. For example, the following scheme describes how one could implement Visual cryptography scheme for a single binary digit. In order to share a binary string, each binary digit in it could be shared independently, one after the other using the same scheme.

Example 3.1

Let the secret, $s, \in \{0, 1\}$. *The* $(2, 7)-$ *visual secret sharing problem can be solved as follows:*

$$Let\ A = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

and

$$B = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Let $\mathcal{C}_0$ *be the set of all the matrices obtained by permuting the columns of* A, *and* $\mathcal{C}_1$ *be the set of all the matrices obtained by permuting the columns of* B

To share a bit, $s = 0$ or 1, the dealer randomly chooses one of the matrix $\in \mathcal{C}_s$. Each rows of chosen matrix defines shares to be given to each one of the 7 participants.

A single share in either $\mathcal{C}_0$ or $\mathcal{C}_1$ is a random choice of three 1s and four 0s, and so they are equally likely. So by having only one share, one cannot identify whether it is from $\mathcal{C}_0$ or from $\mathcal{C}_1$. On the other hand, if we combine (i.e., "OR") any two shares, we get a binary string of length 7, consists of all 0s, or four 1s and three 0s depending on whether the shares belong to $\mathcal{C}_0$ or $\mathcal{C}_1$. In this scheme, the size of one share is 7 bits. So a bit is expanded to 7 times.

Since each binary digit in the secret is shared by choosing a matrix independently, there is no information to be gained by looking at any group of binary digits on a share, either. This demonstrates the security of the scheme.

Remark 3.1

For implementing the visual cryptographic scheme as above, one does not have to generate the entire collection of matrices such as $\mathcal{C}_0$ and $\mathcal{C}_1$. One could simply generate two matrices A and B and store them. During the process of sharing individual bits, depending on the value of s, choose the matrix A or B, generate a random permutation, μ, of $\{1,2,\ldots,m\}$, where, m is the number of columns in it; and permute the rows of the chosen matrix with respect to μ. The rows of the resulting matrices may be regarded as shares, and be distributed to the various participants.

3.2 Division of the pixel

In this section, we shall review the basic visual cryptography scheme proposed by Naor and Shamir. Here a secret black and white image is divided into two grey images. In order to share a secret black and white image, the concept of their scheme is to transform one pixel into two sub-pixels and divide each sub-pixel two color regions. The sub-pixels are half white and half black (can be called grey).

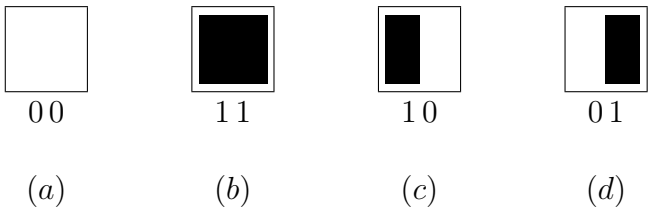

Figure 3.1: Different types of pixels along with the representation.
(a) White pixel (b) Black pixel
(c) LB pixel (d) RB pixel

For example, Figure 3.1 represents four different type of pixels. The first is a white pixel, the next is a black pixel, and the last two are grey pixels. Note that in the grey pixels, the black and white portions are different. Let us call these pixels as LB and RB pixels respectively. We represent a white pixel by 00, black by 11, LB-pixel by 10 and RB-pixel by 01. They can be thought of as modified version of pixels to be used in shares.

3.3 Superposition of pixels

If we stack two LB pixels (or two RB pixels) we get nothing new, where as, if we stack an LB pixel and an RB pixel, we get a black pixel. This can be shown as in Figure 3.2. We can see that by the representation used for pixels, the superposition of two pixels can be thought of as if a binary "OR" operation.

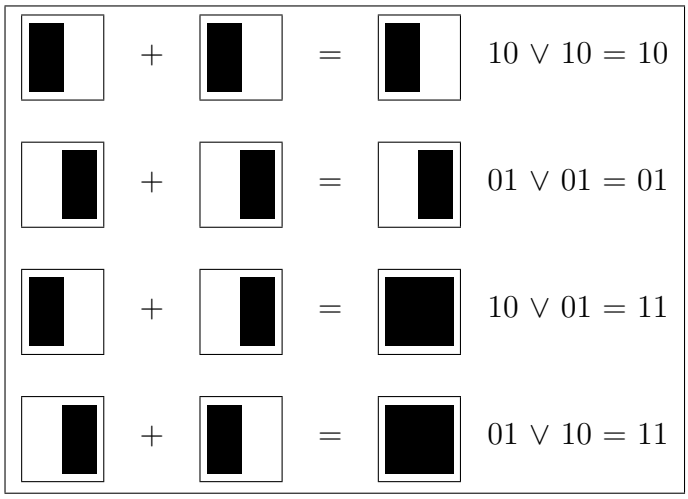

Figure 3.2: Superposition of two grey pixels.

3.4 Dealing of a B/W Image

3.4.1 Algorithm to share a pixel into two shares

The following algorithm specifies how to encode a single pixel into two shares:

Algorithm 3.1 (Share a single pixel into two shares)

Input: A pixel P, which is either Black or White

Output : Two sub-pixels s_1 and s_2.

Step 1. *Let $x \in \{H, T\}$ be the outcome of a coin toss*

if (P = white)

if ($x = H$) $r = 1$

else $r = 2$

else if ($x = H$) $r = 3$

else $r = 4$

Step 2. *Then the pixel P is encrypted as two sub-pixels in each of the two shares, as determined by the r^{th} row in the figure 3.3.*

Naor and Shamir devised the following scheme, illustrated in Figure 3.3 below.

Every pixel is encrypted using algorithm 3.1. Suppose we look at a pixel P in the first share. One of the two sub-pixels in P is black and the other is white. Moreover, each of the two possibilities "black-white" and "white-black" is equally likely to occur, independent of whether the corresponding pixel in the secret image is black or white. Thus the first share gives no clue as to whether the pixel is black or white. The same argument applies to the second share. Since all the pixels in the secret image were encrypted using independent random coin flips, there

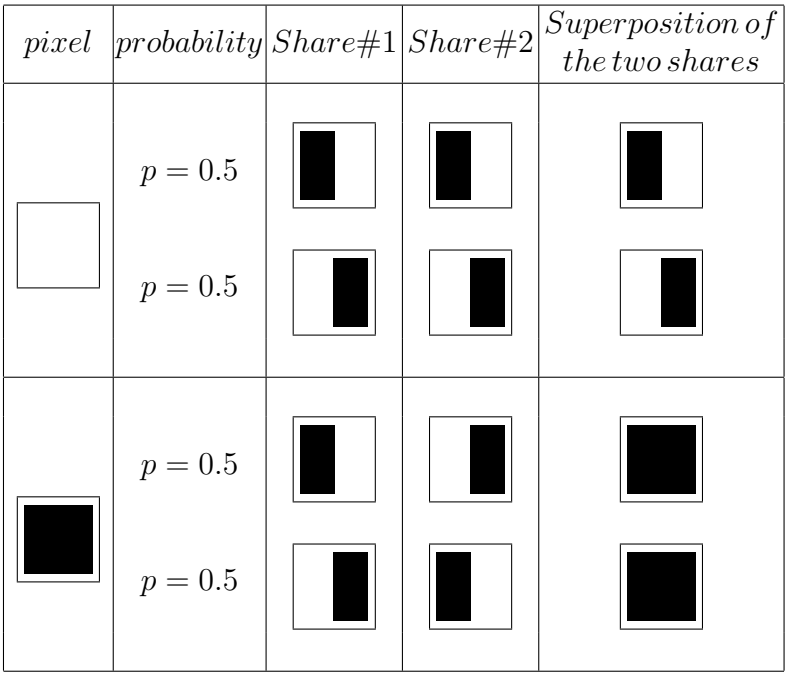

Figure 3.3: Superposition of two grey pixels.

is no information to be gained by looking at any group of pixels on a share, either. This demonstrates the security of the scheme.

Now let us consider what happens when we superimpose the two shares (here we refer to the last column of the figure 3.3. Consider one pixel P in the image. If P is black, we get two black sub-pixels when we superimpose the two shares; if P is white, we get one black sub-pixel and one white sub-pixel when we superimpose the two shares. Thus, we could say that the reconstructed pixel (consisting of two sub-pixels) has a grey level

of 2, if P is black, and a grey level of 1, if P is white. There will be a 50% loss of contrast in the reconstructed image, but it should still be visible. In this case, each pixel is divided into two sub-pixels.

Definition 3.1
The ratio of the size of the share to the size of the secret is called the *blowing factor.*

Since the result of stacking of pixels can be completely determined by the binary "OR" operation, the visual cryptography scheme could also be implemented to any binary strings of 0s and 1s. This method could be extended to any number of participants. When more number of participants are involved, the pixels should be divided into more parts. For example, Noar and Shamir [48] described how to solve the $(2, n)$ visual secret sharing. We present next their solution.

3.4.2 Shamir's solutions for small k and n

$$Let\ A = \begin{bmatrix} 1 & 0 & 0 \cdots 0 \\ 1 & 0 & 0 \cdots 0 \\ \cdots\cdots & & \\ 1 & 0 & 0 \cdots 0 \end{bmatrix}\ and\ B = \begin{bmatrix} 1 & 0 & 0 \cdots 0 \\ 0 & 1 & 0 \cdots 0 \\ \cdots\cdots & & \\ 0 & 0 & 0 \cdots 1 \end{bmatrix}$$

The $(2, n)$ visual secret sharing problem can be solved by the following collections of $n \times n$ matrices:
$\mathcal{C}_0 = \{$all the matrices obtained by permuting the columns of $A\}$

and $\mathcal{C}_1 = \{$all the matrices obtained by permuting the columns of $B\}$

Any single share in either $\mathcal{C}_0$ or $\mathcal{C}_1$ is a random choice of one black and $n-1$ white sub-pixels. To share a pixel $P \in \{0,1\}$, randomly choose one of the matrix from $\mathcal{C}_P$. Then the pixel P is shared with the n participants, by giving each row of the chosen matrix to each participant. If we superimpose any two shares of a white pixel, will have one black and $n-1$ white sub-pixels, whereas any two shares of a black pixel, will have two black and $n-2$ white sub-pixels, which looks darker. So the shared secret bit is recovered. The visual difference between the two cases becomes clearer as we stack additional transparencies.

The blowing factor of this $(2, n)$ scheme is n. That is, the size of a share is n times larger than the size of the secret. It can be shown that the blowing factor can be made smaller. In example 3.2, we present a (2, 9) visual secret sharing, in which, the blowing factor is 6. In Chapter 5, we present a better scheme to achieve the same, in which the blowing factor is of $O(log_2 n)$.

Example 3.2

$$Let\ A = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \quad and\ B = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

Let $\mathcal{C}_0$ be the set of all the matrices obtained by permuting the columns of A

and $\mathcal{C}_1$ be the set of all the matrices obtained by permuting the columns of B

In this example, one bit is expanded to six bits.

3.5 A general scheme for (k, k) Visual cryptography

We now describe a general construction which can solve any (k, k) visual secret sharing problem, having a blowing factor 2^{k-1}.

Let e_i be a column vector consisting of i 1s and $k - i$ 0s. The length of e_i is k, and so there are $\binom{k}{i}$ such vectors.
Let B_i be the exhaustive collection of all e_i's. B_i can be thought of as a matrix of order $k \times \binom{k}{i}$.

$$Let\ \ R = B_i^{(1)} \vee B_i^{(2)} \vee B_i^{(3)} \vee \ldots \vee B_i^{(r)},$$

where, $B_i^{(1)}, B_i^{(2)}, B_i^{(3)}, \ldots B_i^{(r)}$, are any r distinct rows from B_i. Let $n_0(R)$ and $n_1(R)$ denote the number of 0s and 1s, respectively, in R.

Consider a particular bit in R. It can be 0, if and only if, all the selected $B_i^{(j)}$'s have the corresponding bit 0. In other words, since any column contains exactly i 1s, the unselected $k-r$ rows collectively must have all the i 1s in the respective column. Hence $n_0(R) = \binom{k-r}{i}$. Since the length of $R = \binom{k}{i}$, the number of 1s in R is given by the following formula:

$$n_1(R) = \binom{k}{i} - \binom{k-r}{i}. \tag{3.1}$$

Lemma 3.1

Let k be a non negative integer. Then, if $k \neq 0$,

$$\sum_{\substack{i=0,\\ i\,is\,even}}^{k} \binom{k}{i} = \sum_{\substack{i=0,\\ i\,is\,odd}}^{k} \binom{k}{i} = 2^{k-1}, \tag{3.2}$$

and if $k = 0$,

$$\sum_{\substack{i=0,\\ i\,is\,even}}^{k} \binom{k}{i} = 1, \quad and \quad \sum_{\substack{i=0,\\ i\,is\,odd}}^{k} \binom{k}{i} = 0. \tag{3.3}$$

Proof: The case when $n = 0$, can be verified.
So, consider the case when $n \neq 0$. From the equation

$$\sum_{i=0}^{k} (-1)^i . \binom{k}{i} = (1-1)^k = 0 \tag{3.4}$$

separating the negative and nonnegative terms, we get first part of equation (3.2). Also we have,

$$2^k = (1+1)^k = \sum_{i=0}^{k} \binom{k}{i} . \tag{3.5}$$

So,

$$\sum_{\substack{i=0,\\ i\,is\,even}}^{k} \binom{k}{i} = \sum_{\substack{i=0,\\ i\,is\,odd}}^{k} \binom{k}{i} = 2^{k-1} \tag{3.6}$$

Let X denote the matrix obtained by concatenating B_i for all nonnegative even integer $i \leq k$, and let Y be the matrix obtained by concatenating B_i for all nonnegative odd integer $i \leq k$.

Now, the number of columns in the matrix X and that of Y are

$$\sum_{\substack{i=0,\\ i\,is\,even}}^{k} \binom{k}{i} , \quad and \quad \sum_{\substack{i=0,\\ i\,is\,odd}}^{k} \binom{k}{i} ,$$

respectively, and by lemma 3.1, both equal to 2^{k-1}.

So, both X and Y are the same order, $k \times 2^{k-1}$.

$$Let \;\; W = X^{(1)} \vee X^{(2)} \vee X^{(3)} \vee \ldots \vee X^{(r)}, \tag{3.7}$$

where, $X^{(1)}, X^{(2)}, X^{(3)}, \ldots X^{(r)}$, are any r distinct rows from X.

Then, by equation (3.1),

$$\begin{aligned} n_1(W) &= \sum_{i \text{ is even}} \left\{ \binom{k}{i} - \binom{k-r}{i} \right\} \\ &= \sum_{i \text{ is even}} \binom{k}{i} - \sum_{i \text{ is even}} \binom{k-r}{i} \\ &= \begin{cases} 2^{k-1} - 2^{k-r-1}, & \text{if } r \neq k \\ 2^{k-1} - 1, & \text{if } r = k \end{cases} \\ &= \begin{cases} 2^{k-r-1}.(2^r - 1), & \text{if } r \neq k \\ 2^{k-1} - 1, & \text{if } r = k \end{cases} \end{aligned} \tag{3.8}$$

Similarly, if we take r distinct rows from Y, say, $Y^{(1)}, Y^{(2)}, Y^{(3)}, \ldots, Y^{(r)}$, and if we compute

$$Z = Y^{(1)} \vee Y^{(2)} \vee Y^{(3)} \vee \ldots \vee Y^{(r)}, \tag{3.9}$$

then, the number of 1s in Z is given by,

$$\begin{aligned} n_1(Z) &= \sum_{i \text{ is odd}} \left\{ \binom{k}{i} - \binom{k-r}{i} \right\} \\ &= \sum_{i \text{ is odd}} \binom{k}{i} - \sum_{i \text{ is odd}} \binom{k-r}{i} \\ &= \begin{cases} 2^{k-1} - 2^{k-r-1}, & \text{if } r \neq k \\ 2^{k-1}, & \text{if } r = k \end{cases} \\ &= \begin{cases} 2^{k-r-1}.(2^r - 1), & \text{if } r \neq k \\ 2^{k-1}, & \text{if } r = k \end{cases} \end{aligned} \tag{3.10}$$

Let $\mathcal{C}_0$ be the set of all the matrices obtained by permuting the columns of X Let $\mathcal{C}_1$ be the set of all the matrices obtained by permuting the columns of Y

Equation (3.8) and equation (3.10) tells that any $r(< k)$ shares of a secret bit from either $\mathcal{C}_0$ or $\mathcal{C}_1$ together has a random

collection of $2^{k-r-1}.(2^r - 1)$ 1s. Consequently, the analysis of any $r(< k)$ shares makes it impossible to distinguish between $\mathcal{C}_0$ and $\mathcal{C}_1$. On the other hand, k shares from $\mathcal{C}_0$ results in a collection of single 0 along with $2^{k-1} - 1$ 1s, where as k shares from $\mathcal{C}_1$ results in a collection of all 1s(no 0s).

Example 3.3

Let $n = 4$. Consider the matrices X and Y obtained by concatenating $\{B_0, B_2, B_4\}$ and $\{B_1, B_3\}$ respectively.

$$So, \quad X = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$and \ Y = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Let $\mathcal{C}_0$ and $\mathcal{C}_1$ be the set of all the matrices obtained by permuting the columns of X and Y respectively.

Any single row from $\mathcal{C}_0$ or $\mathcal{C}_1$, contains four 1s, any combined $(\vee)$ pair of rows contains six 1s, any combined triplet of rows contains seven 1s, and any combined quadruple of rows contains seven or eight 1s depending on whether the rows were taken from $\mathcal{C}_0$ or $\mathcal{C}_1$.

In [48] Naor and Shamir also describes, how to extend a $(k,\ k)$ scheme to $(k,\ n)$ scheme for arbitrary $n > k$.

Various schemes have been discovered. But a generalized scheme is not invented so far.

3.6 Concluding remarks

In this chapter, we have seen how the Visual Cryptography schemes are distinguished from traditional secret sharing schemes. We have also seen some examples, to illustrate the benefits of Visual Cryptography.