Chapter 4

Modified Visual Cryptography

4.1 Introduction

We have seen that in the case of visual cryptography schemes, the result of stacking of transparencies, can be completely characterized by the boolean "OR" operation. We know that it favours 1s to 0s. i.e., If we "OR" two random bits, the result is more likely towards 1 than 0. When more random bits are involved, it will be more and more likely that the result is 1. So, when k increases, the distinguishing threshold for 0 bit and 1 bit will be at a higher level. So, it is natural that as k increases, the blowing factor also increases. This threshold will not effect the security of the system. Its purpose is only to distinguish the two bits from one another. So, if one could reduce the distinguishing threshold,

the blowing factor may decrease. Since "XOR" does not favour either 0 or 1, it could be a better choice to "OR". This is the difference between traditional Visual Cryptography and Modified Visual Cryptography. This cannot be implemented in the case of images, where as for binary strings it can be done. It is easy to see that, in modified visual cryptography, the blowing factor will never increase, (if not decreased) compared with ordinary visual cryptography.

4.2 A Modified scheme for (k, k) Visual Cryptography

We now describe a general construction which can solve any $(k,\ k)$ modified visual secret sharing problem, having a blowing factor, one. Let B_i, X, and Y be the matrices defined in section 3.5. In Modified Visual Cryptography we perform $\oplus$ instead of $\vee$. So, let

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

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

$$n_1(R) = \sum_{\substack{j \\ j \text{ is odd}}} \binom{r}{j} \binom{k-r}{i-j} \tag{4.1}$$

Consider a particular bit in R. It can be 1, if and only if, there are an odd number of $B_i^{(j)}$'s having the corresponding bit 1.

Since any column contains exactly i 1s, the unselected $k - r$ rows collectively must have the remaining $(i - j)$ 1s. Since the rows are independent, this is possible in

$$\sum_{\substack{j=1 \\ j \text{ is odd}}}^{r} \binom{r}{j} \binom{k-r}{i-j}$$

many places. Here, the range of j can be unrestricted, because $\binom{p}{q} = 0$, if $p < q$.

So, equation (4.1) is established.

$$Let \;\; W = X^{(1)} \oplus X^{(2)} \oplus X^{(3)} \oplus \ldots \oplus X^{(r)}, \tag{4.2}$$

where, $X^{(1)}, X^{(2)}, X^{(3)}, \ldots X^{(r)}$, are any r distinct rows from X. Then, by equation (4.1),

$$n_1(W) = \sum_{\substack{i \\ i \text{ is even}}} \sum_{\substack{j \\ j \text{ is odd}}} \binom{r}{j} \cdot \binom{k-r}{i-j} \tag{4.3}$$

Because the right side of this equation evaluates to a finite number, we can interchange the summation, and get,

$$n_1(W) = \sum_{\substack{j \\ j \text{ is odd}}} \sum_{\substack{i \\ i \text{ is even}}} \binom{r}{j} \cdot \binom{k-r}{i-j} \tag{4.4}$$

The inner $\sum$ runs on variable i, and so, $\binom{r}{j}$ is constant. So we get,

$$n_1(W) = \sum_{\substack{j \\ j \text{ is odd}}} \left[\binom{r}{j} \cdot \sum_{\substack{i \\ i \text{ is even}}} \binom{k-r}{i-j} \right] \tag{4.5}$$

Since i is even and j is odd, $i - j$ is odd, and so by a change of variable,

$$\begin{aligned} \sum_{\substack{i \\ i \text{ is even}}} \binom{k-r}{i-j} &= \sum_{\substack{i \\ i \text{ is odd}}} \binom{k-r}{i} \\ &= \begin{cases} 2^{k-r-1}, & \text{if } r \neq k \\ 0, & \text{if } r = k \end{cases} \qquad (4.6) \\ & \quad [by \ \ lemma \ 3.1, \end{aligned}$$

So,

$$n_1(W) = \begin{cases} 2^{k-r-1} \sum_{j \text{ is odd}}^{j} \binom{r}{j}, & \text{if } r \neq k \\ 0, & \text{if } r = k \end{cases} \qquad (4.7)$$

Again by lemma 3.1, being $r \neq 0, \sum_{j \text{ is odd}}^{j} \binom{r}{j} = 2^{r-1}$.
So, equation (4.7) becomes,

$$n_1(W) = \begin{cases} 2^{k-2}, & \text{if } r \neq k \\ 0, & \text{if } r = k \end{cases} \qquad (4.8)$$

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

$$Z = Y^{(1)} \oplus Y^{(2)} \oplus Y^{(3)} \oplus \ldots \oplus Y^{(r)}, \qquad (4.9)$$

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

$$\begin{aligned} n_1(Z) &= \sum_{\substack{i \\ i \text{ is odd}}} \sum_{\substack{j \\ j \text{ is odd}}} \binom{r}{j} \cdot \binom{k-r}{i-j} \\ &= \sum_{\substack{j \\ j \text{ is odd}}} \sum_{\substack{i \\ i \text{ is odd}}} \binom{r}{j} \cdot \binom{k-r}{i-j} \end{aligned}$$

$$= \sum_{\substack{j \\ j \text{ is odd}}} \left[\binom{r}{j} \sum_{i \text{ is odd}} \cdot \binom{k-r}{i-j} \right] \tag{4.10}$$

Since both i and j are odd, $i - j$ is even, and so by a change of variable,

$$\begin{aligned} \sum_{\substack{i \\ i \text{ is odd}}} \binom{k-r}{i-j} &= \sum_{\substack{i \\ i \text{ is even}}} \binom{k-r}{i} \\ &= \begin{cases} 2^{k-r-1}, & \text{if } r \neq k \\ 1, & \text{if } r = k \end{cases} \\ &\quad [by \ \ lemma \ 3.1, \end{aligned} \tag{4.11}$$

So, equation (4.10) becomes,

$$\begin{aligned} n_1(Z) &= \begin{cases} 2^{k-r-1} \sum_{\substack{j \\ j \text{ is odd}}} \binom{r}{j}, & \text{if } r \neq k \\ \sum_{j \text{ is odd}} \binom{r}{j}, & \text{if } r = k \end{cases} \\ &= \begin{cases} 2^{k-r-1}.2^{r-1} = 2^{k-2}, & \text{if } r \neq k \\ 2^{k-1}, & \text{if } r = k \end{cases} \end{aligned} \tag{4.12}$$

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.

Equation (4.8) and equation (4.12) 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-2} 1s and 0s. Consequently, the analysis of $r(< k)$ 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 only 0s, where as k shares from $\mathcal{C}_1$ results in a collection of only 1s.

4.2.1 Comparison of the schemes

While both the schemes are equally secure, in the former scheme, the result of combining $r(< k)$ shares (i.e., the number of 1s = $2^{k-r-1}.(2^r - 1),$) varies on r, where as in latter one, it is a fixed value (i.e., 2^{k-2}). This phenomena does not enhance or reduce the security of the system. So, we suspect that the former scheme, has done some extra effort for unnecessarily distinguishing the number of shares combined, which is insignificant. So we strongly believe that the blowing factor could be reduced, by striking at a better modified visual cryptography scheme, than the corresponding one. When the secret is recovered by combining all the k shares, in the former, we have to search for the single 0 present, in case, the secret bit is 0. Where as in the latter one, because the result is either all zeros or all 1s, one can recover the secret bit just by looking at the first bit itself. So, though both are equally secure, the modified cryptographic scheme is at least more efficient in the combining process.

4.3 A simple Modified scheme for (k, k)

The following is a very simple algorithm to share a binary string in a (k, k) Modified Visual Cryptography scheme:

Algorithm 4.1 ((k, k) Modified Visual Cryptography construction)

Input: A secret binary bit $S \in \{0, 1\}$

Output : k bits $s_1, s_2, \ldots, s_k$

Step 1. *let* $y = 0$

For $i = 1$ *to* $k - 1$ *do*

Generate a random bit, say $x, \in \{0, 1\}$

$s_i = x$

$y = y \oplus x$

Step 2. $s_k = y \oplus S$

Step 3. *The shares are* $s_1, s_2, \ldots, s_k$

The algorithm 4.1 computes k shares of a single binary digit S. In Step 1, after setting a variable y is 0, it computes $k - 1$ shares, $s_i, 1 \leq i \leq k - 1$, which are nothing but random bits. Also note that, when the for loop in step 1 terminates, the value of y is $s_1 \oplus s_2 \oplus \ldots \oplus s_{k-1}$. In step 2., the last share, s_k is computed as, $s_k = y \oplus S = s_1 \oplus s_2 \oplus \ldots \oplus s_{k-1} \oplus S$. This implies that, $S = s_1 \oplus s_2 \oplus \ldots \oplus s_k$. All the $k - 1$ shares being random, and the secret S being unknown, s_k will also be random. So, there is no information to be gained by looking at r number of shares, for $r < k$. Each and every bit of the secret could be shared one after the other using the same algorithm. Since every bit is shared using random bits, looking at consecutive shares also gains no information. This proves the security of the scheme. The blowing factor of the scheme is 1.

4.4 Generalization of (3, 3) scheme

The following scheme generalizes the (3, 3) scheme described in the last chapter into a (3, n) scheme for an arbitrary $n > 3$. Let B be the black $n \times (n-2)$ matrix which contains only 1s, and let I be the identity $n \times n$ matrix which contains 1s on the diagonal and 0s elsewhere. Let BI denote the $n \times (2n-2)$ matrix obtained by concatenating B and I, and let $\overline{BI}$ be the Boolean complement of the matrix BI. Then $\mathcal{C}_0 = \{$all the matrices obtained by permuting the columns of $\overline{BI}\}$ $\mathcal{C}_1 = \{$all the matrices obtained by permuting the columns of $BI\}$ has the following properties: Any single share contains an arbitrary collection of $n-1$ black and $n-1$ white sub-pixels; any pair of shares have $n-2$ common black and two individual black sub-pixels; any stacked triplet of shares from $\mathcal{C}_0$ has n black sub-pixels, whereas any stacked triplet of shares from $\mathcal{C}_1$ has $n+1$ black sub-pixels, which looks darker.

4.5 Concluding remarks

Here, we have seen the difference between traditional Visual Cryptography and Modified Visual Cryptography. We have also proposed a very simple modified sharing scheme.