

# Threshold Schemes in Visual Secret Sharing

# Visual Secret Sharing Scheme

- cryptographic technique to encode a secret image into shadow images.
- certain qualified subsets of shares enable the “visual” recovery of the image.
- recovery involves stacking the transparencies of the qualified set of shadow images over one another.

# Contents

- Introduction
- The Model
- Basis Matrices
- Threshold Schemes
- $(2,2)$ -Threshold VTS
- General Access Structure
- $(3,n)$ -VTS using BCH Codes
- $(3,n)$ -VTS using Canonical Matrices
- Improvements in the Schemes

# Introduction

## VISUAL SECRET SHARING SCHEME(VSSS)

- Proposed by Naor and Shamir.
- A black-white image is encrypted to  $n$  black-white images called shares, where  $n \geq 2$ .
- A  $(t,n)$ -threshold VCS for a set  $P$  of  $n$  participants encodes into  $n$  shares
- Each participant in  $P$  receives one share.
- Any (qualified) set of  $t$  or more participants can “visually” recover the secret image.

# Parameters of VCS

## PIXEL EXPANSION

It is the number of sub pixels each pixel of the original image is encoded into.

## RELATIVE CONTRAST

It is the “difference” between a black and a white pixel in the reconstructed image.

# The Model

- Let  $P = \{1, \dots, n\}$  be the set of participants, and let  $2$  denote all the subsets of  $P$ .
- Let  $T_{\text{qual}} \subseteq 2P$  and  $T_{\text{forb}} \subseteq 2P$ , where  $T_{\text{qual}} \cap T_{\text{forb}} = \emptyset$ .
- $T_{\text{qual}}$ -qualified sets,  $T_{\text{forb}}$ -forbidden sets.
- Let  $T_0$  consist of all the minimal qualified sets:
- $T_0 = \{A \in T_{\text{qual}} : A' \in T_{\text{qual}} \text{ for all } A' \subseteq A, A' \neq A\}$
- A participant  $X \in P$  as an essential participant if a set  $X \subseteq P$  such that  $X \cup \{P\} \in T_{\text{qual}}$  but  $X \notin T_{\text{qual}}$ .

# The Model (cont...)

- Each pixel appears in  $n$  versions called shares, one for each transparency.
- Each share is a collection of  $m$  black and white subpixels.
- The structure is an  $n \times m$  matrix  $S = [s_{ij}]$ , where  $s_{ij} = 1$  iff the  $j$ th sub pixel in the  $i$ th transparency is black.
- The gray level is obtained by stacking the transparencies  $i_1, \dots, i_s$ , is proportional to the Hamming weight  $w(V)$  of the  $m$ -vector.
- $V = \text{OR}(r_{i_1}, \dots, r_{i_s})$ , where  $r_{i_1}, \dots, r_{i_s}$ , are the rows of  $S$  associated with the transparencies we stack.

# Definition 1

Let  $(T_{\text{qual}}, T_{\text{forb}})$  be an access structure on a set of  $n$  participants. Two collections (multisets) of  $n \times m$  matrices  $C_0$  and  $C_1$  constitute a  $(T_{\text{qual}}, T_{\text{forb}}, m)$  VCS if there exist values  $\alpha(m)$  and  $\{t_x\}_{x \in T_{\text{qual}}}$  satisfying:

- Any qualified set  $X = \{i_1, i_2, \dots, i_p\} \in T_{\text{qual}}$  can recover the shared image by stacking their transparencies. For any  $M \in C_0$ , the “or”  $V$  of rows  $i_1, i_2, \dots, i_p$  satisfies  $w(V) \leq t_x - \alpha(m) \cdot m$ ; whereas, for any  $M \in C_1$  it results that  $w(V) \geq t_x$ .
- Any nonqualified set  $X = \{i_1, i_2, \dots, i_p\} \in T_{\text{forb}}$  has no information on the shared image.



# Definition 1 (cont...)

- Each pixel will be encoded into  $n$  pixels each one consisting of  $m$  subpixels.
- $\alpha(m)$  - relative difference, the number  $\alpha(m) \cdot m$  is the contrast of the image.
- The set  $\{t_x\}_{x \in T_{\text{qual}}}$  is called the set of thresholds.
- The contrast should be as large as possible and  $\alpha(m) \geq 1/m$ .

# Definition 2

- Let  $(T_{\text{qual}}, T_{\text{forb}})$  be an access structure on a set of  $n$  participants. A  $(T_{\text{qual}}, T_{\text{forb}}, m)$  VCS with relative difference  $\alpha(m)$  and set of thresholds  $\{t_x\}_{x \in T_{\text{qual}}}$  is realized using the  $n \times m$  basis matrices  $S^0$  and  $S^1$  if the following two conditions hold:
- If  $X = \{i_1, i_2, \dots, i_p\} \in T_{\text{qual}}$  is a qualified set, then the “or”  $V$  of rows  $\{i_1, i_2, \dots, i_p\}$  of  $S^0$  satisfies  $w(V) \leq t_x - \alpha(m) \cdot m$ ; whereas, for  $S^1$  it results that  $w(V) \geq t_x$ .
- If  $X = \{i_1, i_2, \dots, i_p\} \in T_{\text{forb}}$  is not a qualified set then the two  $p \times m$  matrices obtained by restricting  $S^0$  and  $S^1$  to rows  $\{i_1, i_2, \dots, i_p\}$  are equal up to a column permutation.

# Threshold Schemes

- A  $(k, n)$ -threshold structure is any access structure  $(T_{\text{qual}}, T_{\text{forb}})$  in which  $T_0 = \{B \subseteq P : |B| = k\}$  and  $T_{\text{forb}} = \{B \subseteq P : |B| \leq k - 1\}$ .
- In any  $(k, n)$ -threshold VCS, the image is visible if any  $k$  or more participants stack their transparencies, but totally invisible if fewer than  $k$  transparencies are stacked together

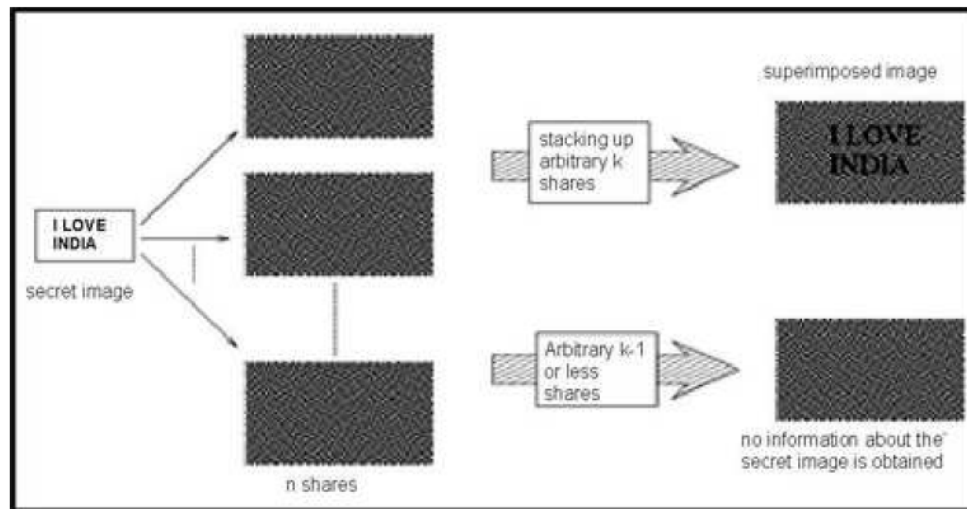


Figure 1:  $(k,n)$  VTS for black and white image

# (2,2)-Threshold VTS

- The two  $2 \times 2$  basis matrices  $S^0$  and  $S^1$  given as follows.

$$S^0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \quad S^1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

- We encrypt a white pixel, we apply a random permutation to the columns of  $S^0$  to obtain matrix T.
- Then distribute row i of T to participant i.
- To encrypt a black pixel, we apply the permutation to  $S^1$ .
- Relative contrast in this case is  $1/2$  while the pixel expansion is 2 .

.











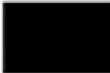



pixel		share # 1	share # 2	superimposition of two shares
	$p=.5$			
	$p=.5$			
	$p=.5$			
	$p=.5$			

Figure 2: (2,2) VTS for black and white image

# General Access Structure

- We consider a boss  $B$ , two managers  $M_1$  &  $M_2$  and two users  $U_1$  &  $U_2$ .
- The qualified sets include  $\{B, M_1, U_1\}$  and  $\{B, M_2, U_2\}$ .
- The basis matrices  $S^0$  and  $S^1$  can be obtained by solving the following equations:

$$\text{Set 1:} \quad b + m1 + u1 = 0$$

$$b + m2 + u2 = 0$$

$$\text{Set 2:} \quad b + m1 + u1 = 1$$

$$b + m2 + u2 = 1$$

- The solution of the equations of set (1) gives us the matrix  $S^0$  and that of set (2) gives us the matrix  $S^1$ .
- The Matrices are :

$$S^0 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix} \quad S^1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$



- If we take the ‘OR’ of rows of any set of participants, the weight in  $S^1$  is greater than that in  $S^0$ .
- For any other combination the weight is same in both the basis matrices.
- The pixel expansion in this case is 8.
- The weight on doing the “OR” operation in case of  $S^1$  is 8.
- It is 6 in the case of  $S^0$  thereby producing a relative contrast of  $1/4$ .

# (3,n)-VTS using BCH Codes

## CONSTRUCTION OF (K,K)-VTS

- Consider a ground set  $W = \{1, 2, \dots, k\}$  of  $k$  elements and let  $\pi_1, \pi_2, \dots, \pi_{2^{k-1}}$  be a list of all subsets of  $W$  of even cardinality and let  $\alpha_1, \alpha_2, \dots, \alpha_{2^{k-1}}$  be a list of all subsets of  $W$  of odd cardinality.
- Each list defines the following  $k \times 2_{k-1}$  matrices  $S^0$  and  $S^1$  : For  $1 \leq i \leq k$  and  $1 \leq j \leq 2_{k-1}$   
let  $S^0[i, j] = 1$  iff  $i \in \pi_j$  and  $S^1[i, j] = 1$  iff  $i \in \sigma_j$  .

- In our case we have constructed the basis matrices for the (3,3)-VTS.
- The subsets of odd cardinality of the set  $\{1,2,3\}$  in this case include  $\{1\}$ ,  $\{2\}$ ,  $\{3\}$ ,  $\{1,2,3\}$  and the sets of even cardinality are  $\phi$ ,  $\{1,2\}$ ,  $\{2,3\}$ ,  $\{1,3\}$ .
- $S^0$  and  $S^1$  are given by

$$S^0 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \quad S^1 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

# Initial Matrix Definition

- Let  $n, l, k$  be integers such that  $k|n$ . An initial matrix  $IM(n, l, k)$  is an  $n \times l$  matrix whose entries are elements of a ground set  $A = \{a_1, a_2, \dots, a_k\}$  in which the set of columns is equal to the set of vectors in which each element of  $A$  appears  $n/k$  times.
- The number of columns,  $l$ , of an initial matrix  $IM(n, l, k)$  is equal to the number of "anagrams" of the word

$a_1 \dots a_1 (n/k \text{ times}) \dots a_i \dots a_i (n/k \text{ times}) \dots a_k \dots a_k (n/k \text{ times})$

that is ,

$$l = \frac{n!}{(n/k)!^k}$$

- Given an initial matrix  $IM(n, l, k)$  we can construct a  $(k, n)$ -threshold VCS as follows:

The  $n \times (l \cdot 2^{k-1})$  basis matrices  $S_0$  and  $S_1$  are constructed by replacing the symbols  $a_1, a_2, \dots, a_k$ , respectively, with the 1st,  $\dots$ ,  $k$ th rows of the corresponding basis matrices  $T_k^0$  and  $T_k^1$  of the  $(k, k)$ -threshold VCS.

- The pixel expansion and Relative Contrast in this case are

$$m = \frac{n!}{((n/k)!)^k} \cdot 2^{k-1} \quad \alpha(m) = \frac{(n/k)^k}{\binom{n_0}{k}} \cdot 2^{k-1}$$

# Orthogonal arrays and BCH codes

## DEFINITION 1

A cyclic code of length  $n$  over  $GF(q)$  is a BCH code of designed distance  $\delta$ , if for some integer  $b \geq 0$ ,

$g(x) = \text{l.c.m.}\{M^{(b)}(x), M^{(b+1)}(x), \dots, M^{(b+\delta-2)}(x)\}$  i.e  $g(x)$  is the lowest degree monic polynomial over  $GF(q)$  having  $\alpha^b, \alpha^{b+1}, \dots, \alpha^{b+\delta-2}$  as zeroes.

## DEFINITION 2

- An orthogonal array  $OA_\lambda(t, k, v)$  is a  $\lambda v^t \times k$  array, say  $A$ , of elements from a set  $X$  of cardinality  $v$ , with the property that within any  $t$  columns of  $A$  every possible  $t$ -tuple of elements from  $X$  occurs in exactly  $\lambda$  rows.

## THEOREM 1

- Suppose there exists an  $OA(t, k, v)$ . Then there exists a strong  $(k, n)$ - threshold VCS with

$$m = \lambda k^k 2^{k-1} \text{ and } \alpha(m) = \frac{(k-1)!}{(2k)^{k-1}}$$

# THEOREMS

- If there exists an  $[n, l, d]_q$  code, then there exists an  $OA_\lambda(d-1, n, q)$  where

$$\lambda = q^{n-l-d+1}$$

- If there exists an  $[n, l, d]_q$  code, then there exists a  $(q, n)$ -threshold VCS with  $m = q^{n-1} 2^{q-1}$

$$\alpha(m) = \frac{(q-1)!}{(2q)^{q-1}}$$



- By Theorem 1, construct the finite field  $GF(3)$  using the polynomial  $x^2 + x + 2$  which is irreducible over  $GF(3)$ .
- Let  $\alpha$  be the root of this polynomial in the extension field. The field is given by

$$00 = 0 = \alpha^{-\infty}$$

$$10 = 1 = \alpha^0$$

$$01 = \alpha = \alpha^1$$

$$12 = 1 + 2\alpha = \alpha^2$$

$$22 = 2 + 2\alpha = \alpha^3$$

$$20 = 2 = \alpha^4$$

$$02 = 2\alpha = \alpha^5$$

$$21 = 2 + \alpha = \alpha^6$$

$$11 = 1 + \alpha = \alpha^7$$

# Definition 1

- The minimal polynomial over  $GF(p)$  of  $\beta$  is the lowest degree monic polynomial  $M(x)$  with coefficients from  $GF(p)$  such that  $M(\beta) = 0$ .

$$g(x) = l.c.m. \{M^{(1)}(x), M^{(2)}(x), M^{(3)}(x)\}$$

$$= l.c.m. \{x^2 + x + 2, x^2 + 1\}$$

$$= x^4 + x^3 + x + 2$$

# (3,n)-VTS using Canonical Matrices

## DEFINITION OF CANONICAL MATRICES

Let  $(S^0, S^1)$ , be the basis matrices of a  $(k, n)$  threshold VCS. They are in canonical form if, for  $i = 0, 1$ , the following two properties are satisfied.

- For any two columns  $c$  and  $c'$  such that  $w(c) = w(c')$  it results that  $f_{c,i} = f_{c',i}$  where denotes the multiplicity of the column  $c$  in .
- For any column  $c$  it results that

$$\begin{aligned} f_{c,i} &= f_{c',i} && \text{if } k \text{ is even} \\ &= f_{c',1-i} && \text{if } k \text{ is odd .} \end{aligned}$$

# THEOREM 1

$S(h_0)$  and  $S(h_1)$  are basis matrices of a  $(k, n)$ -threshold VCS with pixel expansion  $m$  and contrast  $\alpha$  if the following properties are satisfied:

$$\sum_{j=0}^n \binom{n}{j} h_{j,0} = \sum_{j=0}^n \binom{n}{j} h_{j,1} = m.$$

$$\sum_{j=l'}^{n-l+l'} \binom{n-l}{j-l'} h_{j,0} = \sum_{j=l'}^{n-l+l'} \binom{n-l}{j-l'} h_{j,1} \text{ for } 1 \leq l \leq k-1 \text{ and } 0 \leq l' \leq l$$

$$\sum_{j=0}^{n-k} \binom{n-k}{j} (h_{j,0} - h_{j,1}) = \alpha m.$$

# THEOREM 2

For any  $n \geq 4$  and any integer  $1 \leq g \leq n/2$ , the scheme  $S(3, n, g)$  described earlier is a strong  $(3, n)$ -threshold VCS having pixel expansion and contrast equal to

$$m = 2 \binom{n-1}{g} \quad \text{and} \quad \alpha = \frac{g(n-2g)}{2(n-1)(n-2)}, \quad \text{resp.}$$

$$h_{0,0} = h_{n,1} = \binom{n-1}{g} - \binom{n-1}{g-1} \quad \text{and} \quad h_{n-g,0} = h_{g,1} = 1$$

- Thus in we have 14 columns of 0's and 28 columns of weight 6. has 14 columns of weight 8 and 28 columns of weight 2.

$$S^0 = \begin{bmatrix} 0 & 0 & \dots & 0 & 1 & 1 & \dots & 0 \\ . & . & \dots & . & 1 & 1 & \dots & 0 \\ . & . & \dots & . & 1 & 1 & \dots & 1 \\ . & . & \dots & . & 1 & 1 & \dots & 1 \\ . & . & \dots & . & 1 & 1 & \dots & 1 \\ . & . & \dots & . & 1 & 0 & \dots & 1 \\ . & . & \dots & . & 0 & 1 & \dots & 1 \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 1 \end{bmatrix}$$

$$S^1 = \begin{bmatrix} 1 & 1 & \dots & 1 & 0 & 0 & \dots & 1 \\ . & . & \dots & . & 0 & 0 & \dots & 1 \\ . & . & \dots & . & 0 & 0 & \dots & 0 \\ . & . & \dots & . & 0 & 0 & \dots & 0 \\ . & . & \dots & . & 0 & 0 & \dots & 0 \\ . & . & \dots & . & 0 & 1 & \dots & 0 \\ . & . & \dots & . & 1 & 0 & \dots & 0 \\ 1 & 1 & \dots & 1 & 1 & 1 & \dots & 0 \end{bmatrix}$$

# Improvements in the Schemes

## FUTURE WORK

- The relative contrast and the pixel expansion obtained from the above two schemes are so large that it is practically impossible to “see” the image after recombination.
- Aspect Ratio Maintenance and Tuning of the image are used to lower the aspect ratio and tune the image after recombination.

## ASPECT RATIO MAINTENANCE

Replace the single row by blocks the product of whose dimensions is equal to the length of the row in the basis matrix. For eg. if the pixel expansion is 36 we can have blocks of size  $6 \times 6$ .

## TUNING OF THE IMAGE

Take each block of sub-pixels corresponding to a pixel of the original image and replace it with the pixel value occurring greater number of times, i.e. if black(white) pixel occurs more than the white(black) pixel then we replace the block with the black(white) pixel.