Secret Sharing
and
Visual Cryptographic Schemes

Prof. Bimal Roy
Applied Statistics Unit
Indian Statistical Institute
Kolkata 700108

Secret Sharing

Definition

A secret S has to be *shared* amongst some *participants* so that only designated subsets of the set of all participants can *recover* the secret and no other subset *can*.

Secret Sharing
Example 1: 2-out of-2 scheme

- Two participants: A and B.
- Both together can while one of them can not recover the secret.
- Secret: $S = 01001000010011$.
- Let $P = 1001101010101$ be a pseduo random binary string.
- Let $T = S \oplus P = 1101001000110$.
- Two shares are P and T.
- Recovery: $S = P \oplus T$.
- One can show that if P is *random* then neither P nor T has any information about the secret S.
- Strength of the scheme: how *random* P is.

Visual Cryptography

- Secret S is an image.
- Shamir's notion of recovery is simply through superimposing the shares.

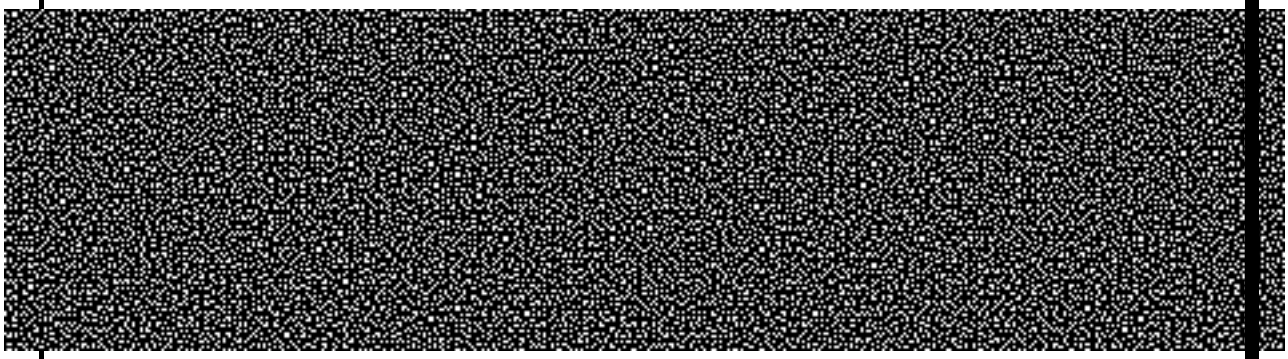
Practical Example of $(2,4)$-VTS

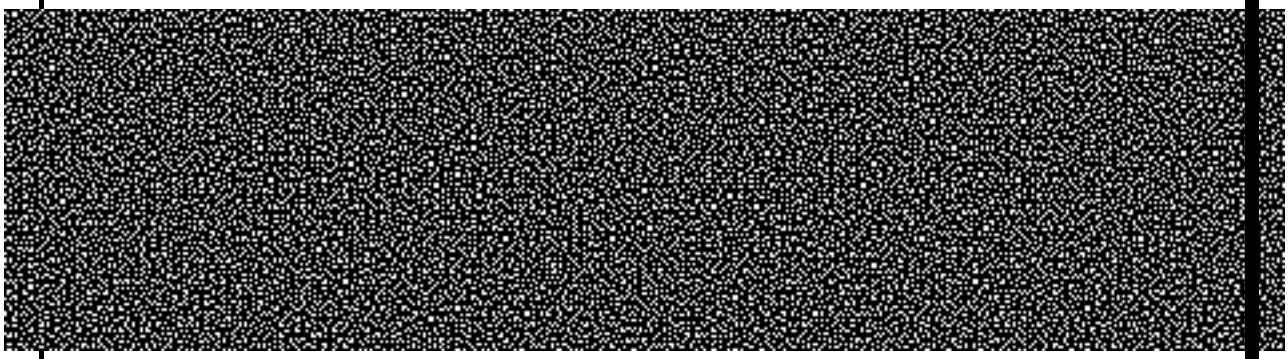
- **Original Picture**

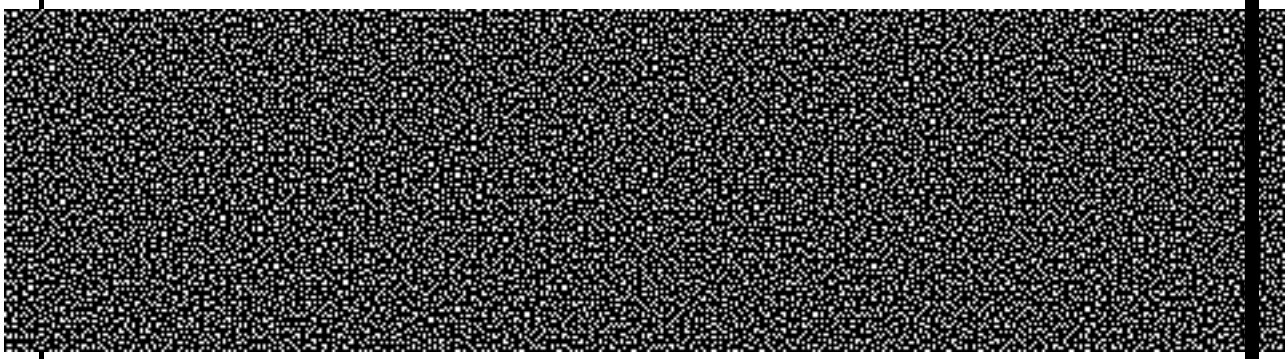
- **Shared Pictures**

Visual Cryptography

Bimal Roy



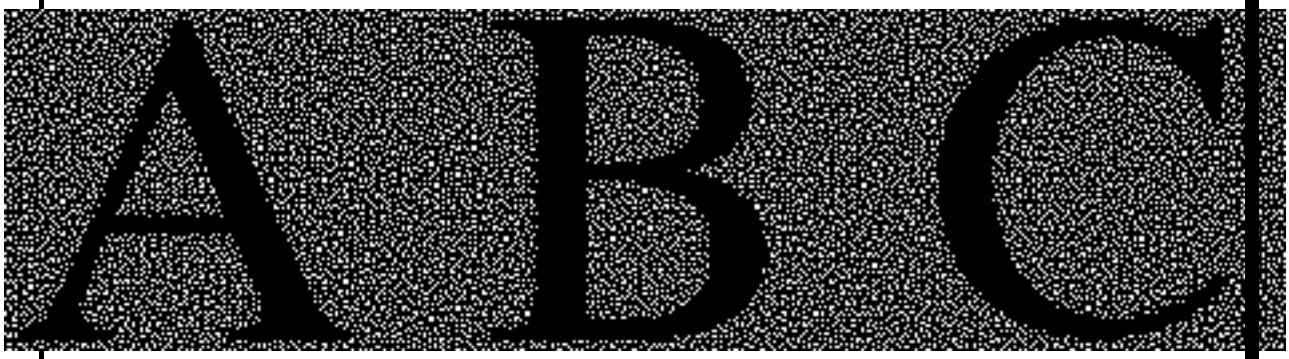




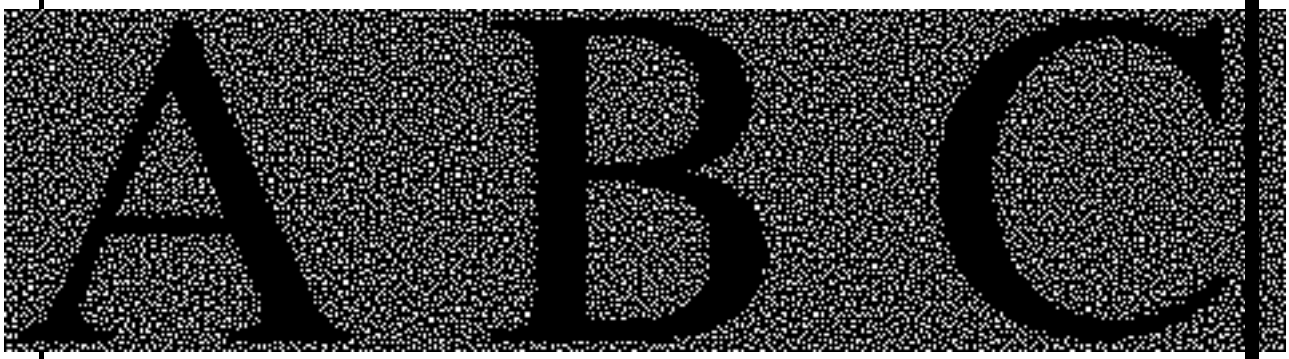
Cryptology Research Group

Indian Statistical Institute

- **Superimposing 2nd and 4th shared pictures**

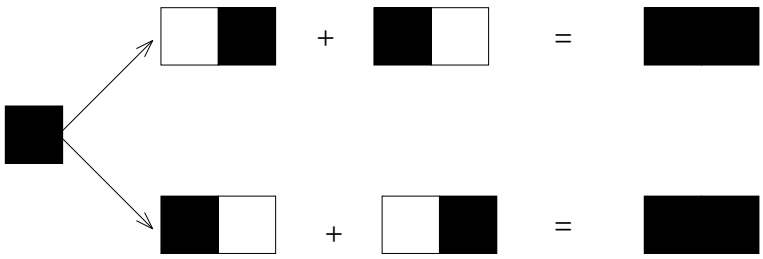


- **Superimposing 1st and 3rd shared pictures**

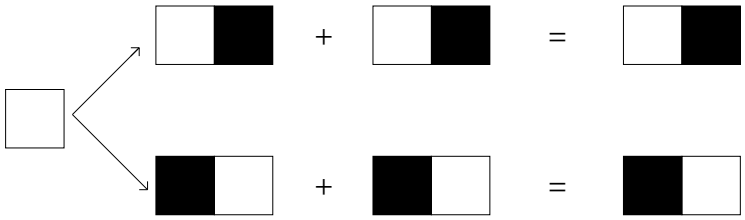


$(2,2)$-Visual Threshold Scheme

- For Black Pixel:



- For White Pixel:



- Mathematically, we can express the above images through the Boolean matrices.

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

Example of basis matrices for (2,2)-VTS

- $S^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $S^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$, where S^1 and S^0 are the basis matrices for black and white pixels respectively. Here the pixel expansion is 2 and the relative difference is $1/2$.
- Another example of $(2, 4)$-VTS as follows

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

Share distribution algorithm

For each pixel P do the following:

1. Generate a random permutation π on the set $\{1, 2, \ldots, m\}$.
2. If P is a black pixel apply π to the columns of S^1 else apply π to the columns of S^0. Call the resulting matrix T.
3. For $1 \leq i \leq n$, row i describes the distribution of black and white subpixels in the ith share.

(v, k, λ)-BIBD (Definition)

A (v, k, λ)-Balanced Incomplete Block Design (BIBD) is a pair $(\mathcal{X}, \mathcal{A})$ such that the following properties are satisfied :

- $\mathcal{X}$ is a set of v elements called points,
- $\mathcal{A}$ is a collection of subsets of $\mathcal{X}$ called block,
- each block contains exactly k points, and
- every pair of distinct points is contained in exactly λ blocks.

$(2, n)$-VTS using BIBD

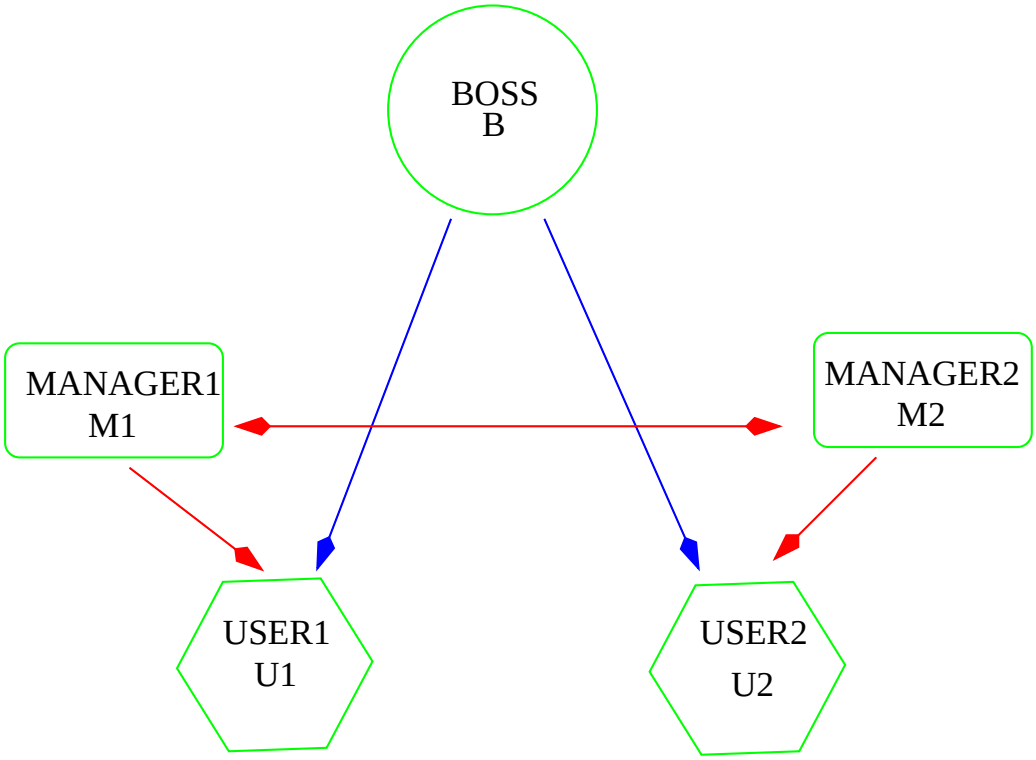
Let S^1 be the incidence matrix of an (n, b, r, k, λ)-BIBD. Define S^0 to be the $n \times b$ Boolean matrix in which every row consists of r 1's followed by $(b - r)$ 0's. Then S^0 and S^1 form the basis matrices of a $(2, n)$-VTS with pixel expansion $m = b$ and relative contrast $\alpha(m) = \frac{2r-\lambda-r}{b} = \frac{r-\lambda}{b}$.

Example $(2, n)$-VTS

Using the incidence matrix of a $(7, 7, 3, 3, 1)$-BIBD, basis matrix S^1 for a $(2, 7)$-VTS can be constructed as follows :

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

Visual Cryptography for General Access Structure :

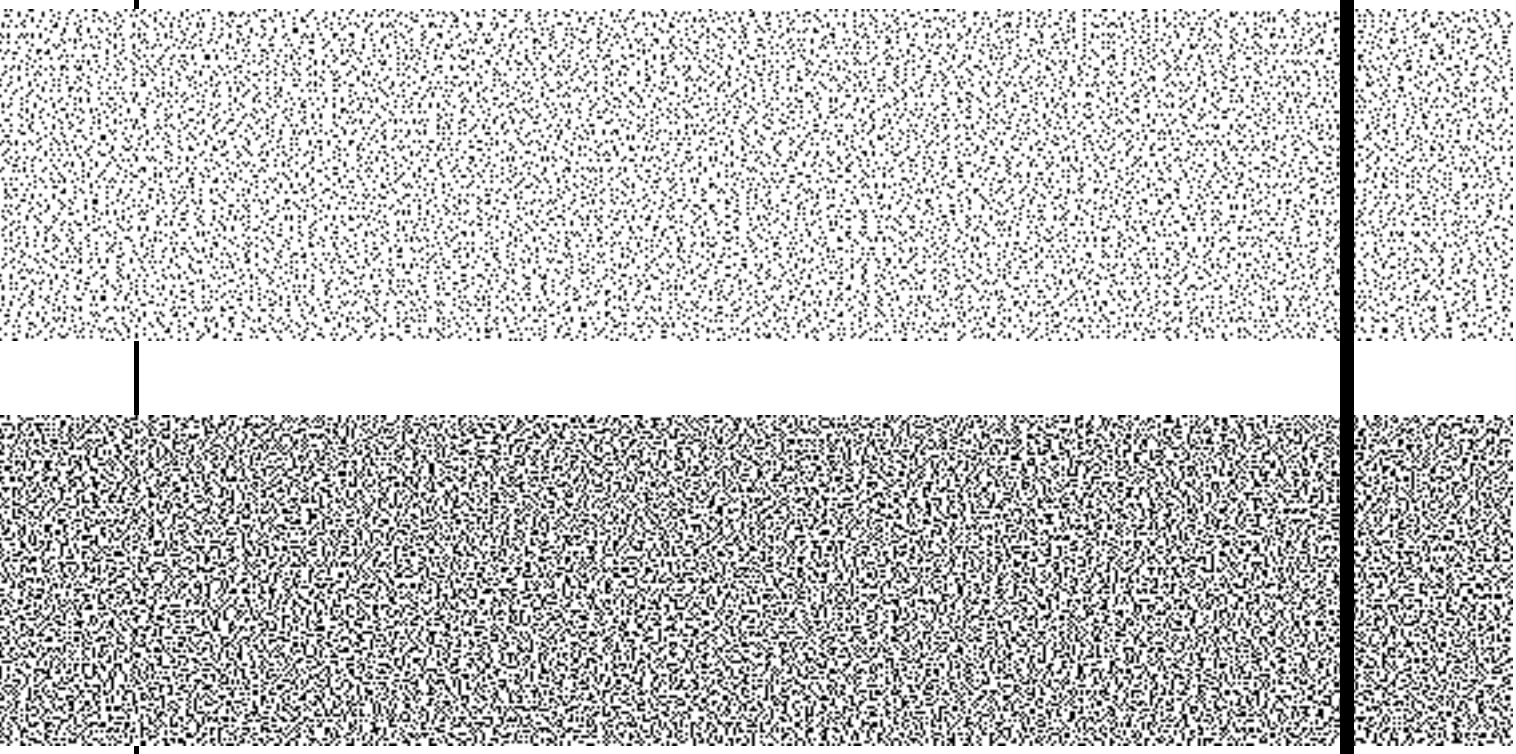


$$\Gamma_0 = \{\{B, U1\},\ \{B, U2\},$$
$$\{M1, M2, U1\},\ \{M1, M2, U2\}\}.$$

Visual Example of the Access structure

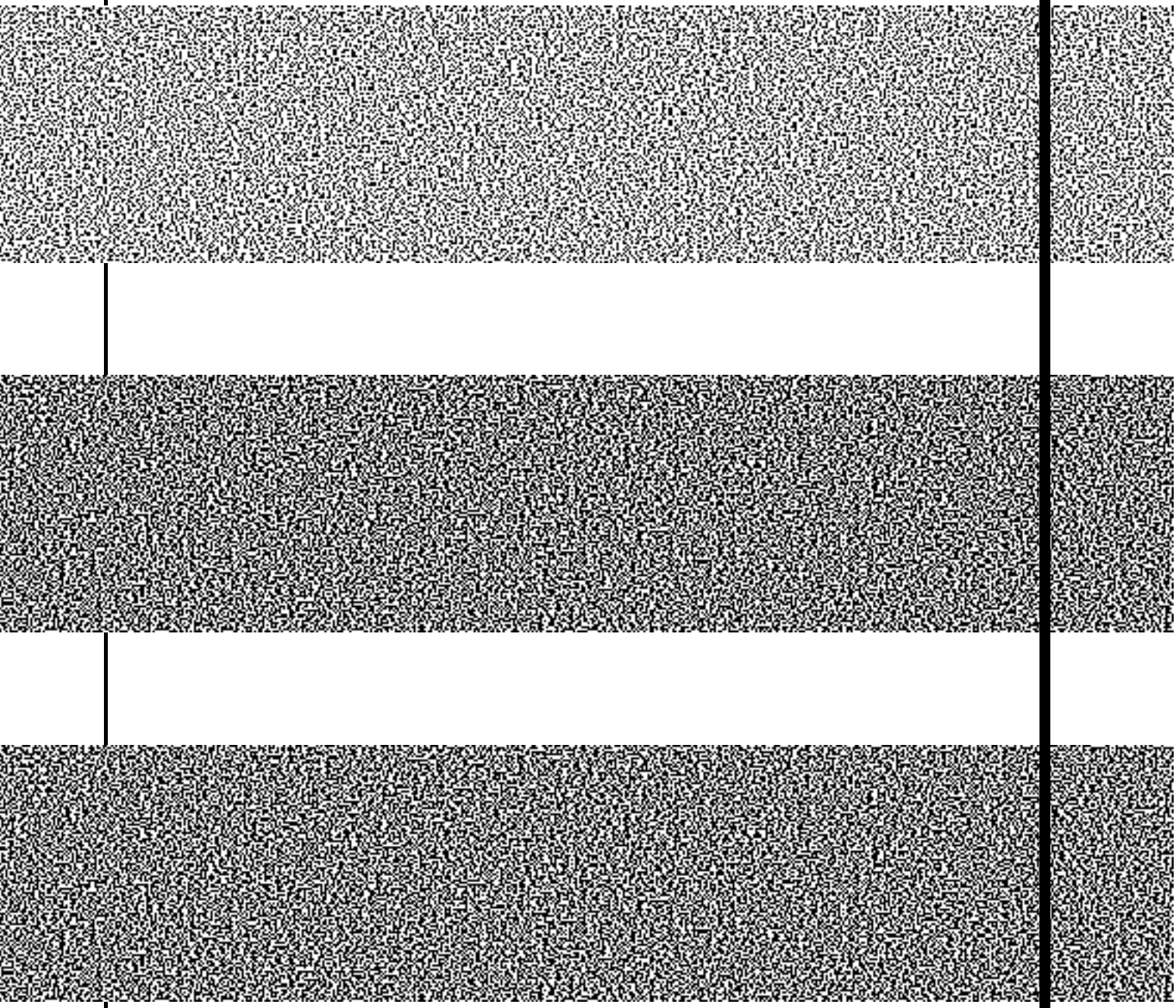
- **Original Picture**

- **Shared Pictures of Boss, Manager1, Manager2, User1, User2**



Visual Cryptography

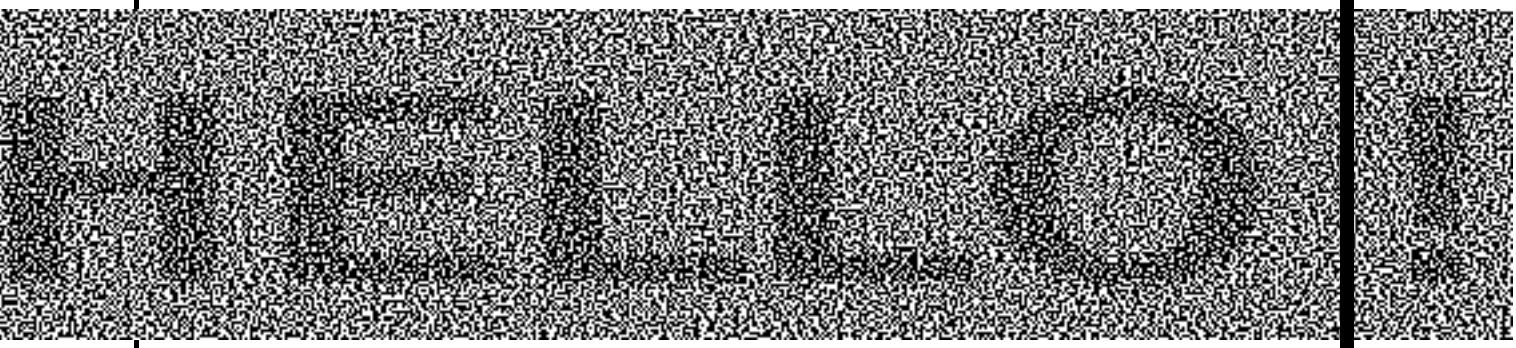
Bimal Roy



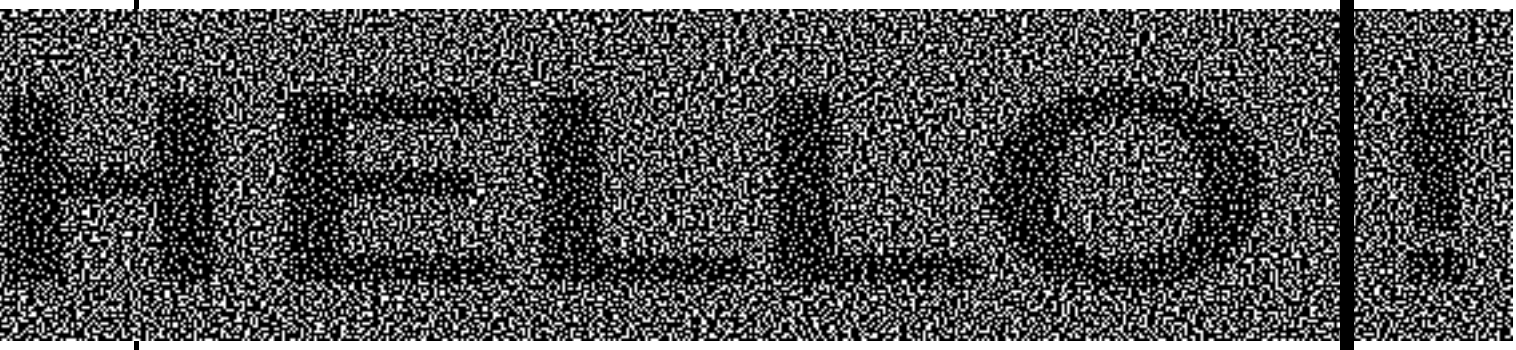
Cryptology Research Group

Indian Statistical Institute

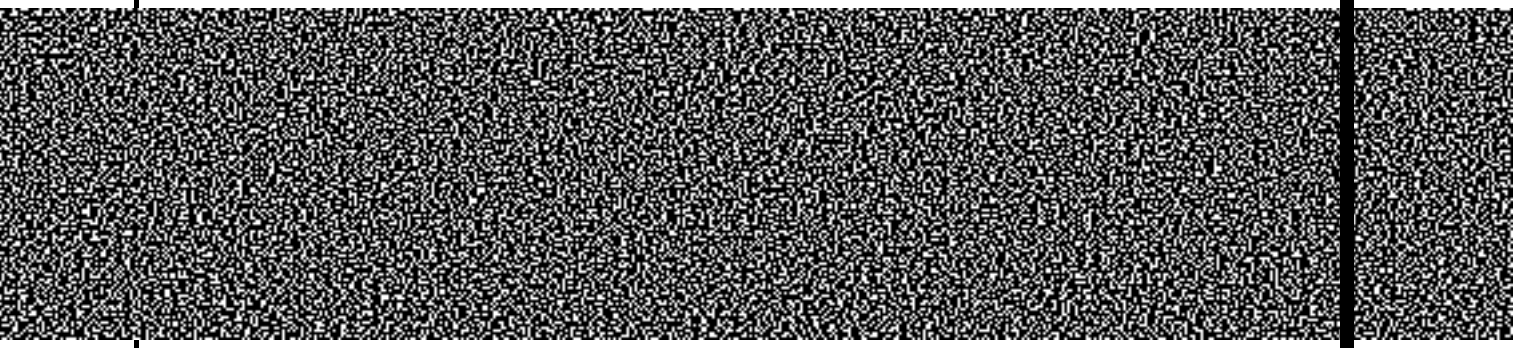
- **Superimposing Boss and User2's shared pictures**



- **Superimposing Manager1, manager2 and User1's shared pictures**



- **Superimposing Manager1, User1 and User2's shared pictures**



A New B/W VCS

- First assign to each participant a variable: $B \rightarrow x_1$, $M_1 \rightarrow x_2$, $M_2 \rightarrow x_3$, $U_1 \rightarrow x_4$ and $U_2 \rightarrow x_5$.
- Consider the subset $\Gamma_0^1 = \{\{B, U1\}, \{B, U2\}\}$.
- Form two system of linear equations :

$$\left.\begin{array}{rcl} x_1 + x_4 & = & 0 \\ x_1 + x_5 & = & 0 \end{array}\right\} \ (I) \ \textit{and} \ \left.\begin{array}{rcl} x_1 + x_4 & = & 1 \\ x_1 + x_5 & = & 1 \end{array}\right\} (II)$$

- The two basis matrices are follows :

$$S_1^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } S_1^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \end{bmatrix}.$$

A New B/W VCS (Cont.) :

- Similarly we consider

$$\Gamma_0^2 = \{\{M1, M2, U1\},\ \{M1, M2, U2\}\}.$$

- Form the two systems of equations as follows:

$$\left.\begin{aligned} x_2 + x_3 + x_4 &= 0 \\ x_2 + x_3 + x_5 &= 0 \end{aligned}\right\} \ and \ \left.\begin{aligned} x_2 + x_3 + x_4 &= 1 \\ x_2 + x_3 + x_5 &= 1 \end{aligned}\right\}$$

- The two basis matrices are follows:

$$S_2^0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \text{ and } S_2^1 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}.$$

A New B/W VCS (Cont.)

From following two submatrices (presented in two previous slides)

$$S_1^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad S_1^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \end{bmatrix}$$

$$S_2^0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \quad \text{and} \quad S_2^1 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix},$$

we have the basis matrices as given by :

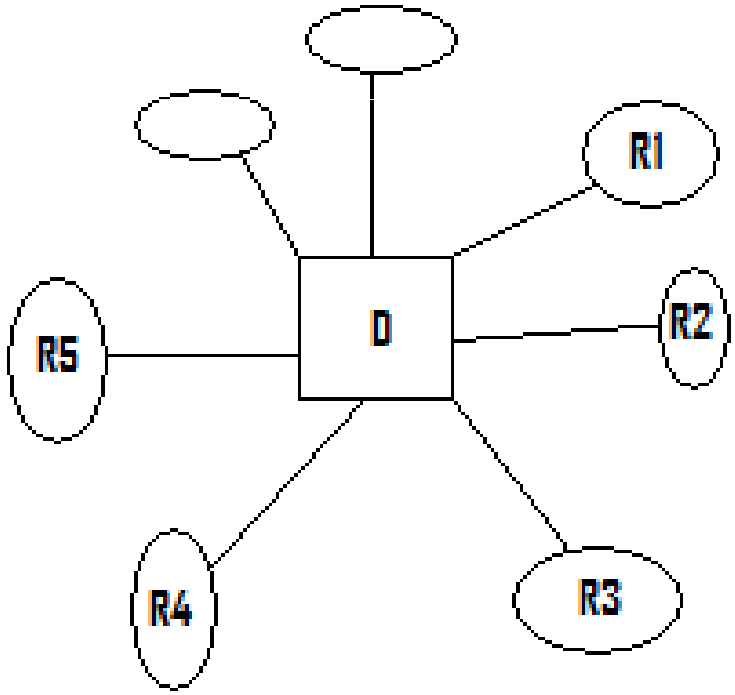
$$S^0 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix} \text{ and } S^1 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0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

Applications of VC

- Secret Broadcasting
- Independent secrets to multiple recipients
- Secured Finger print base Authentication

Secret Broadcasting

- Dealer D wants to send secret S to recipients R1, R2, R3, etc..

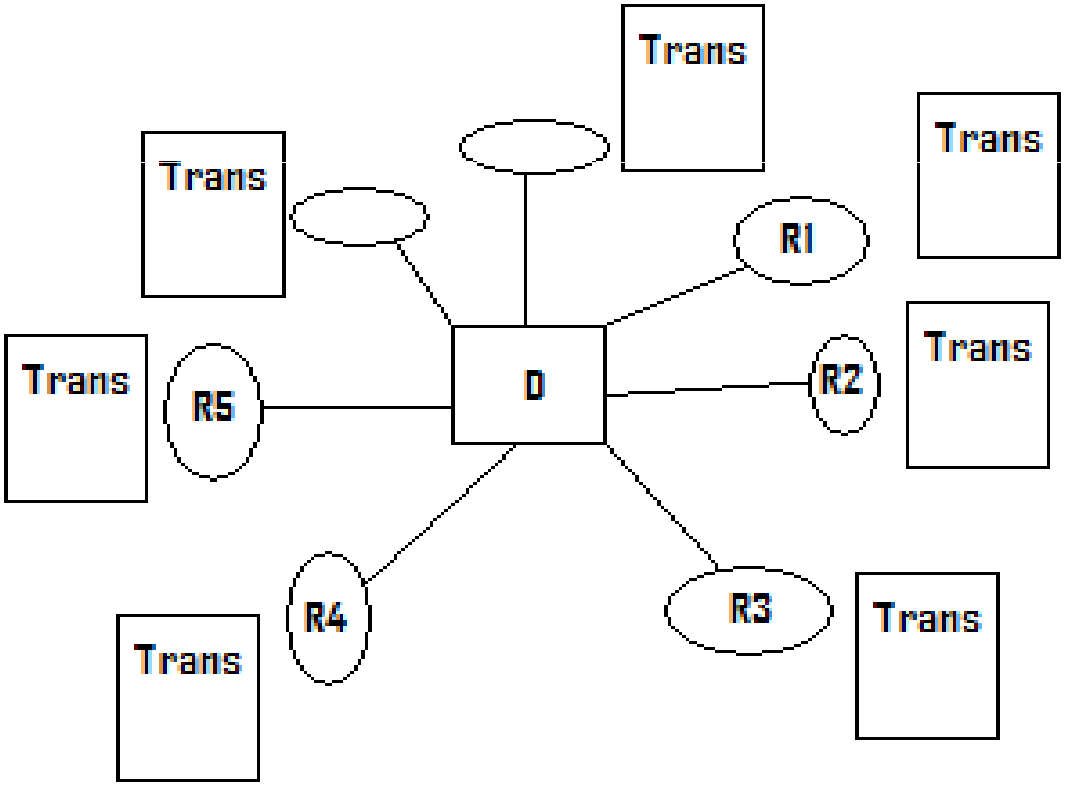


Secret Broadcasting

- Consider a binary picture and blow up each pixel of it to a 2x2 block with 2 white, 2 black representing white pixel and 1 white, 3 black representing black pixel.
- D Prints this blown up picture on n transparencies and gives one to each Ri.

Secret Broadcasting

- Each Ri has a copy of transparency.

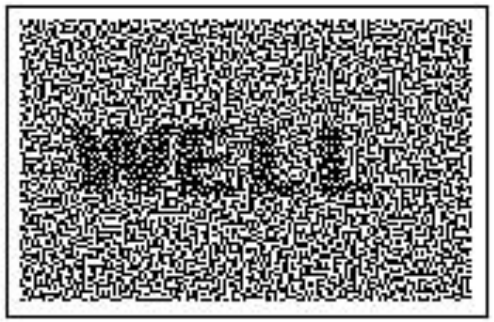


Secret Broadcasting

- Considering picture on transparency as share A, dealer D construct share B from secret S.
- This share B can be broadcasted in non secure media such as news paper or web page etc.
- Ri's with copy of transparency can place it on broadcasted share B, to see the secret S

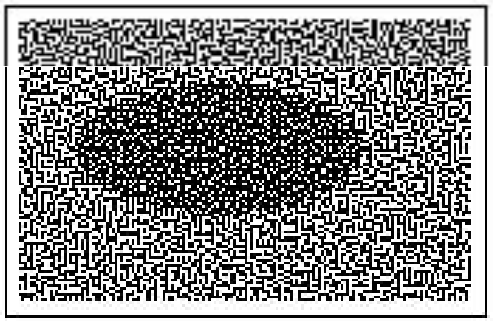
Secret Broadcasting (Example)

Innocent picture

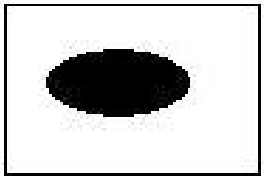


Share A on transparency

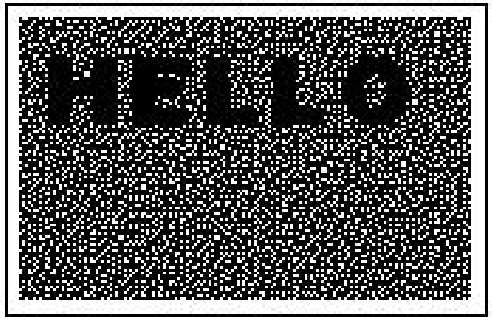
Secret image



Share B (broadcast this)



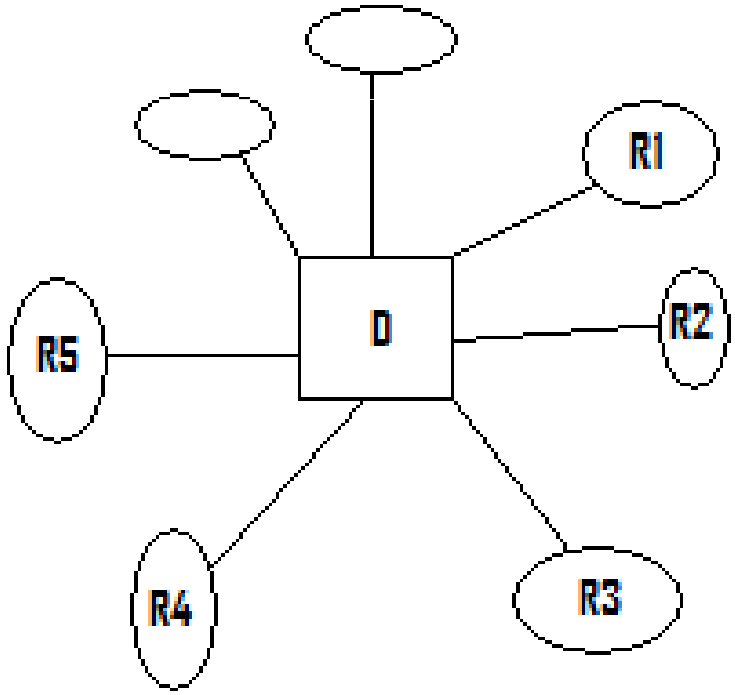
Cover 2



Share A + Share B

Multiple Secret Broadcasting

- Dealer D wants to send secrets S1, S2, …, Sn to recipients R1, R2, …, Rn respectively.

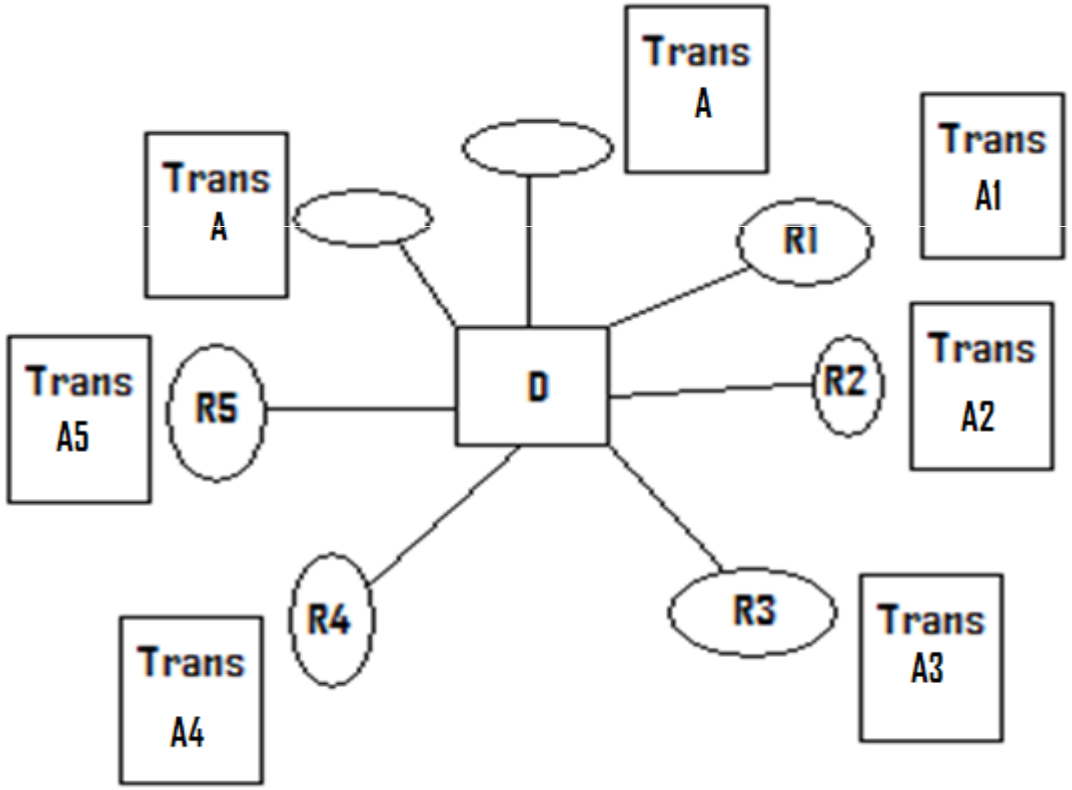


Multiple Secret Broadcasting

- Dealer D creates shares A1, A2, …, An, as discussed in multi secret sharing scheme.
- Prints each Ai on a transparency and gives it to recipient Ri.

Multiple Secret Broadcasting

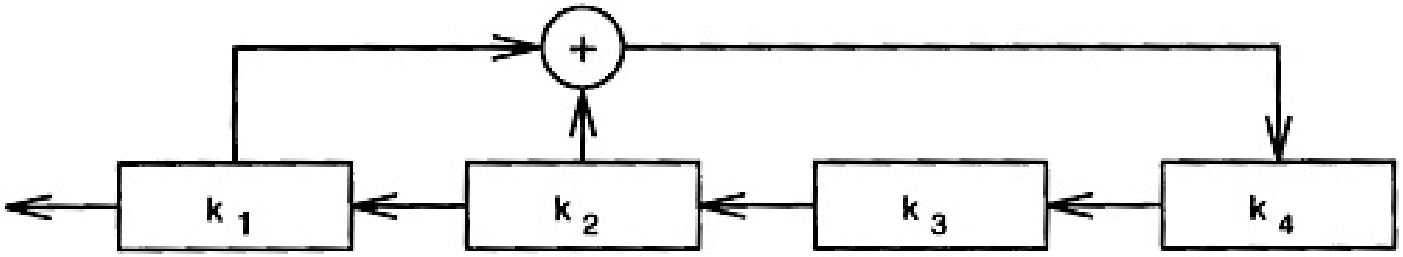
- Each Ri has a transparency with share Ai on it.



Multiple Secret Broadcasting

- If S1, S2, … Sn are secret for R1, R2, … Rn respectively, then using A1, A2, …, An, D can construct share B as explained multi secret sharing scheme.
- This share B can be broadcasted in non secure media such as news paper or web page etc.
- Each Ri's with his Ai on transparency can place it on broadcasted share B, to see the secret Si

Linear Feedback Shift Register(LFSR)



- A linear feedback shift register(LFSR) of length L consists of L stages numbered 1, 2, . . . , L, each capable of storing one bit and having one input and one output, and a clock which controls the movement of data. During each unit of time the set of operations are performed.

Linear Feedback Shift Register(LFSR)

- These operations are
- 1. The content of stage 1 is output and forms part of the output sequence, represented as O(LFSR);
- 2. The content of stage i is moved to stage i - 1 for each i, $2 \leq i \leq L$; and
- 3. The new content of stage L is the feedback bit $K_{i+1} = (c_1K_1+c_2K_2+\ldots+c_LK_L)\text{Mod } 2$, where $c_i=1$ if i^{th} bit is involved in xor operation else $c_i=0$.
- So, an LFSR can be represented as $(c_1c_2\ldots c_L;K_1K_2\ldots K_L)$, where c_i's are coefficients of above feedback function and K_i's are initial values.

Data/Picture hiding scheme

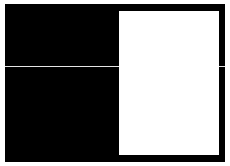
- Assume that, 256x256 pixel binary image S is to be hidden in a 256x256 pixel gray scale image P
- Represent pixels of these images as S_i and P_i, for i ranging from 0 to 2^{16}-1

Data/Picture hiding scheme

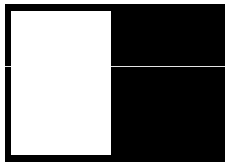
- let L1 and L2 be two LFSRs of length 16 bits each. So, each of them can generate 2^{16}-1, nonrecurring values and also random bit output stream of same length.

Data/Picture hiding scheme

- we represent the basic bocks as block 0 and block 1 as in figure



block 0



block 1

Data/Picture hiding scheme

- **LFSR L1 is used to generate a random bit to choose block 0 or block 1.**
- **LFSR 2 is used generate a random number to choose the location in share 1, to place this block chosen with the help of L1.**
- **Except 0^{th} block all other blocks of share 1 are fixed by using the non recurring values of L1 and L2 and 0^{th} block can be given just block 0.**

Data/Picture hiding scheme

- **Now using this share 1 and secret *S*, one can get share 2.**
- **This share 2 can also represented by stream of bits, by using 0 and 1 to represent block 0 and block 1 respectively.**
- **This stream is written to image *P*, by replacing least significant bit of j^{th} byte by the j^{th} bit of the stream, for j from 0 to 2^{16}-1**

Finger prints

- In any finger print based system, details are usually stored in data bases, which are vulnerable for attacks.
- Picture hiding algorithm can help in handling such data bases.
- Consider finger print image as secret S to be shared.
- Let L1 and L2 be two LFSRs represented by (X1,Y1) and (X2,Y2) respectively.

Finger prints

- Using these LFSRs share 1 and share 2 are generated as suggested above and then share 2 is written into photo based id card that can be given to the user.
- (X1,Y1) and (X2,Y2) are stored in data base along with other non sensitive information of the user.
- So, the data base will have only these integers and no more information about finger prints are stored in data bases.

Thank you