Secret Image Sharing

Introduction

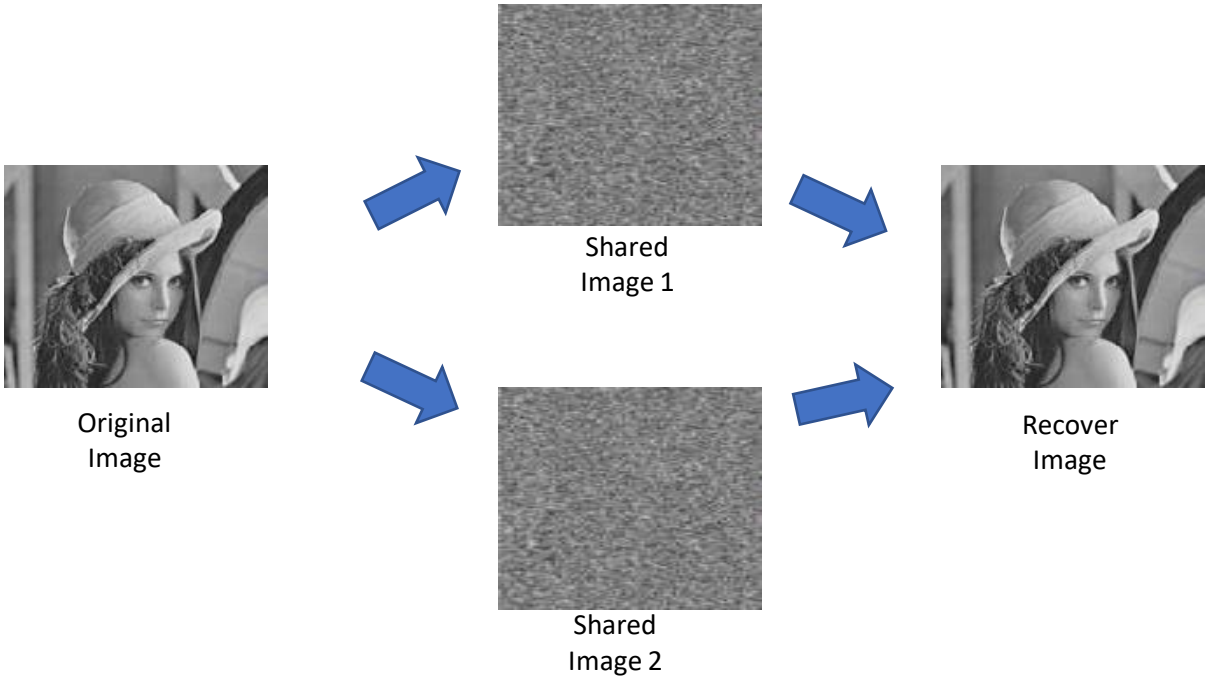
- Background
  - Some secrets are too important to be kept by one person.
  - *"It is easier to trust the many than the few"*
  - Secrecy (trust) and robustness.

- Secret Sharing
  - Distribute a secret amongst a group of participants.
  - Each participant is allocated a share of the secret.
  - Secret can be reconstructed only when the shares are combined together.
  - Individual shares are of no use on their own.

Introduction

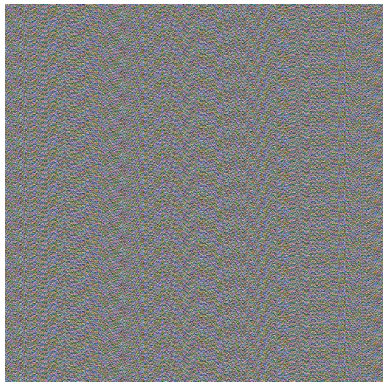
- Traditional Cryptography
  - Encryption and Decryption by computer.
  - Needs the knowledge of cryptography, keys and possess high computational complexity
  - Single point of failure.

Secret mage Sharing (gray-scale)

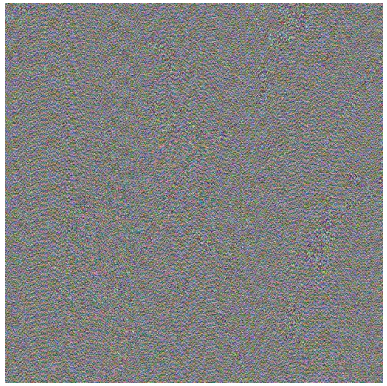


Secret Image Sharing (color)

Original
Image



Shared
Image 1



Shared
Image 2

Recover
Image

Secret Image Sharing

- The concept of secret sharing was independently introduced by Blakely and Shamir in 1979.
- SIS scheme can broadly classified into two categories-
  - Polynomial based Secret Image Sharing (PSIS)
  - Visual secret Sharing (VSS)

Polynomial Based

- Based on Polynomial equation.
- The scheme is used a linear polynomial equation of order k-1 as

$$f(x) = a_0 + a_1 x + a_2 x_2 + ... + a_{(k-1)} x_{(k-1)} (\text{mod } p)$$

where

p is a prime number

n number of participants

a_0 is the secret data

$a_1, a_2, ...a_{k-1}$ coefficient are randomly chosen from [0..p-1]

Note: In case of gray scale image, we use p=251(prime number)nearest to 255

Polynomial Based Contd…

Reconstruction is done by following Langrange interpolation.

$$a_0 = \sum_{i \in s} y_i , B_{i,\{s\}}$$

$$B_{i,\{s\}} = \prod_{m \in s, m \neq i} \frac{-x_m}{x_i - x_m}$$

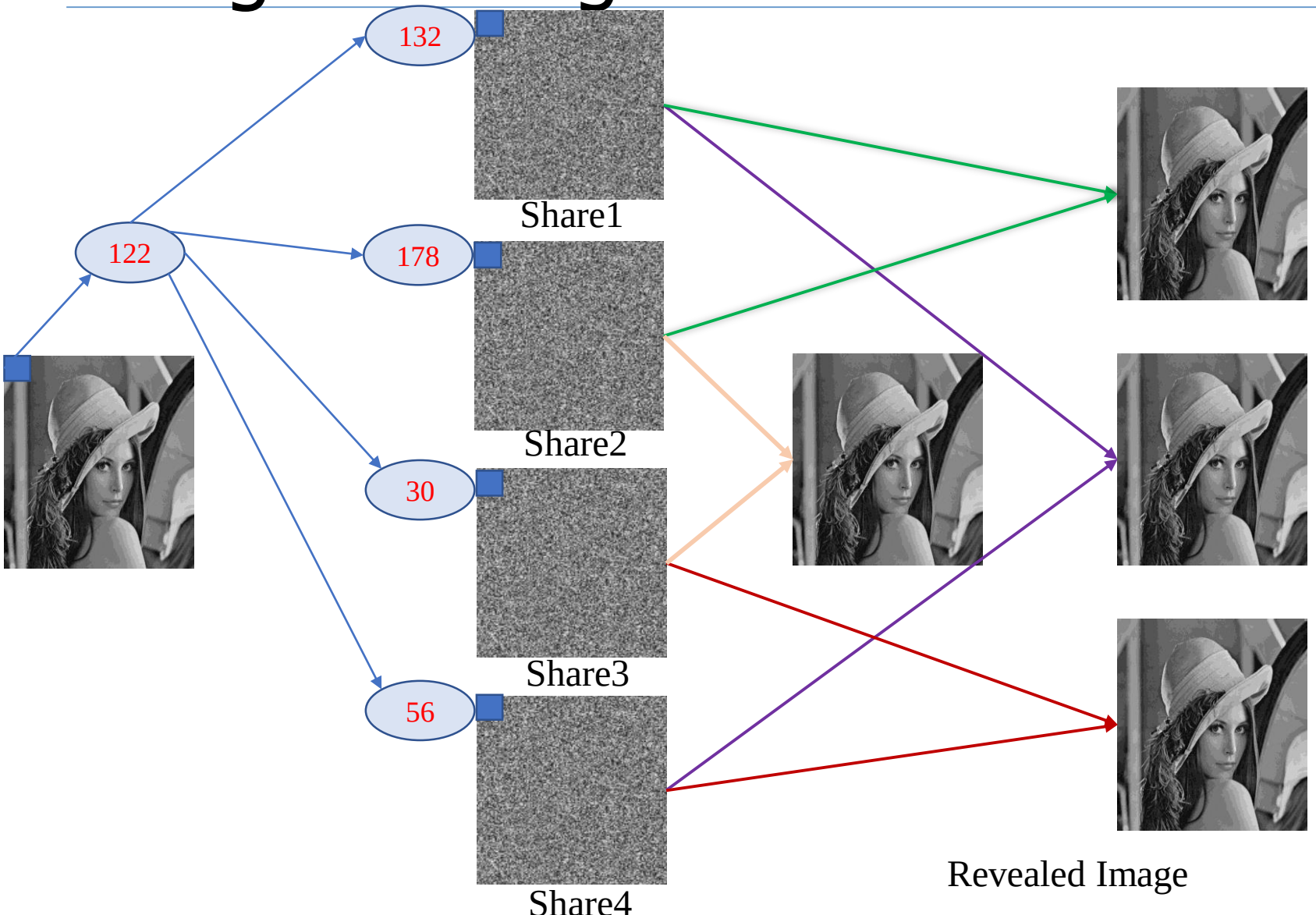
- where (x_i, y_i) is a pair of secret share of secret data.

Polynomial Based-(K,n) Secret Image Sharing

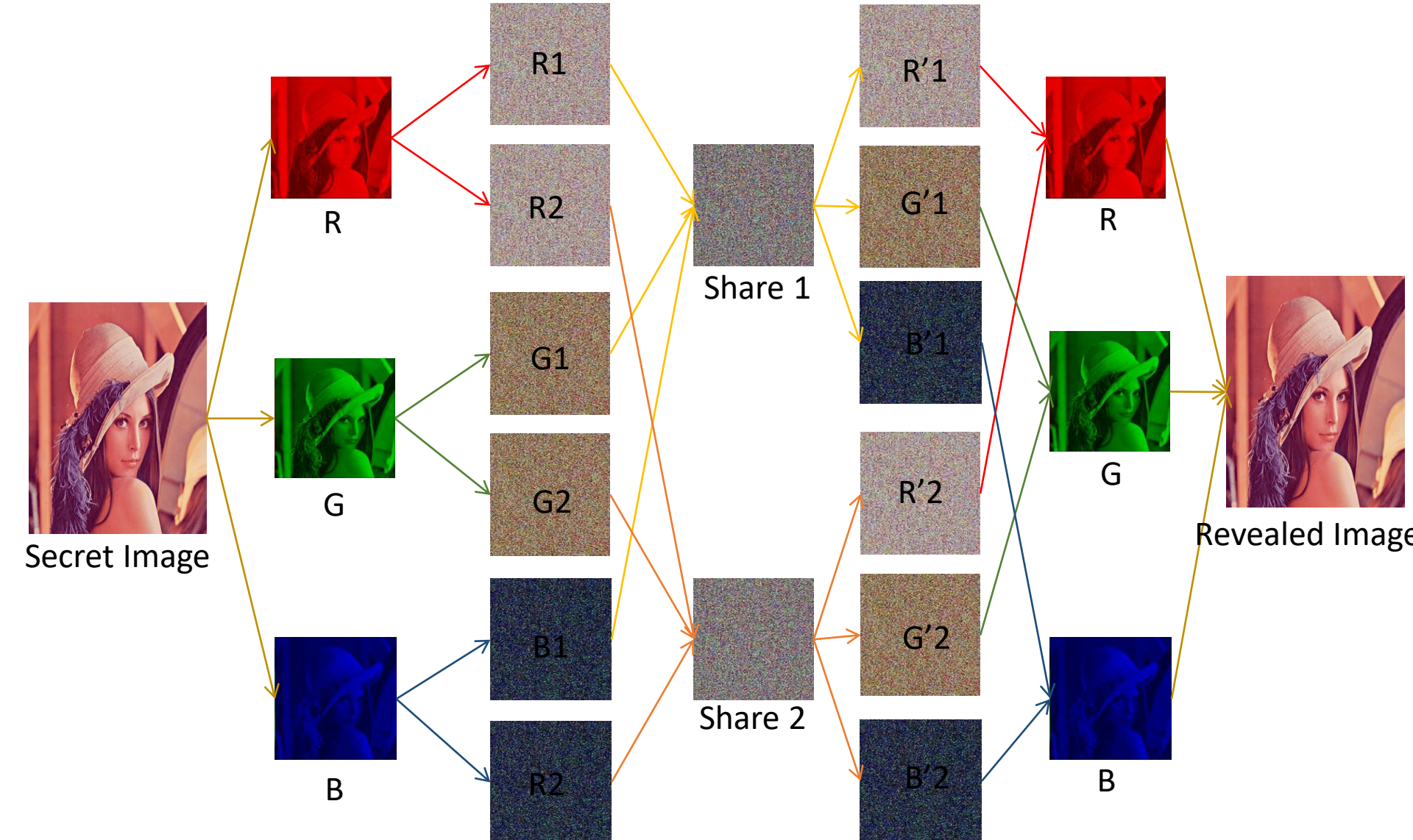
Suppose a image I is divided into n shares.

- I can be constructed from any k shares out of n.
- Complete knowledge of k-1 shares no information about I.
- K of n shares is necessary to reveal secret image.

Polynomial Based-(2,4) Secret Image Sharing



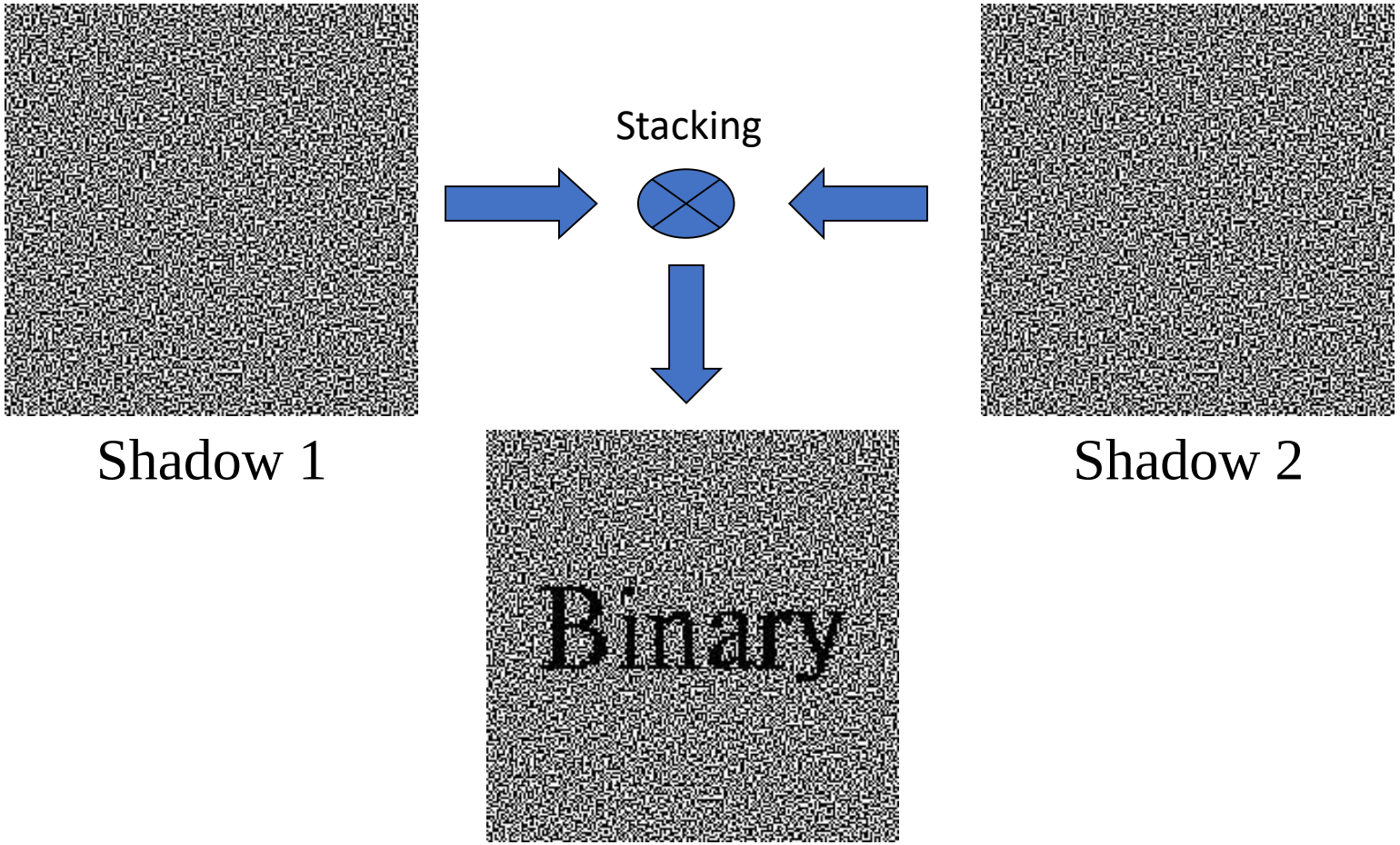
Polynomial Based-(2,2) Secret Image Sharing



Visual Cryptography

- Visual Cryptography (VC), also called Visual Secret Sharing (VSS) was introduced by Moni Noar and Adi shamir in Eurocrypt in 1994
  - Encrypted by computer, Decrypted by human vision.
  - Needs neither cryptography knowledge nor complex computation.

Visual cryptography



Shadow 1

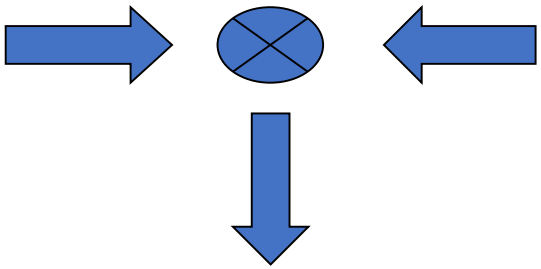
Shadow 2

Secret

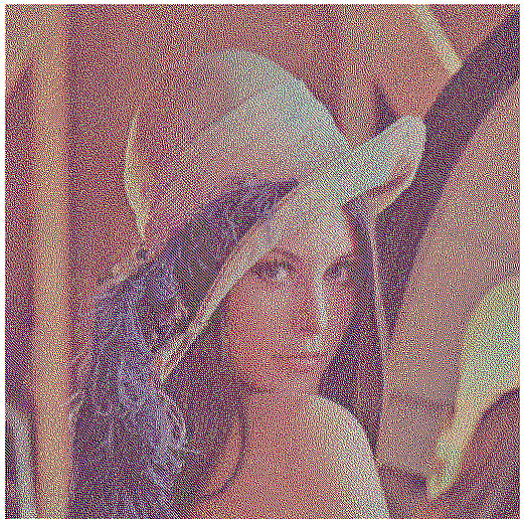
Visual cryptography

Shadow 1

Stacking

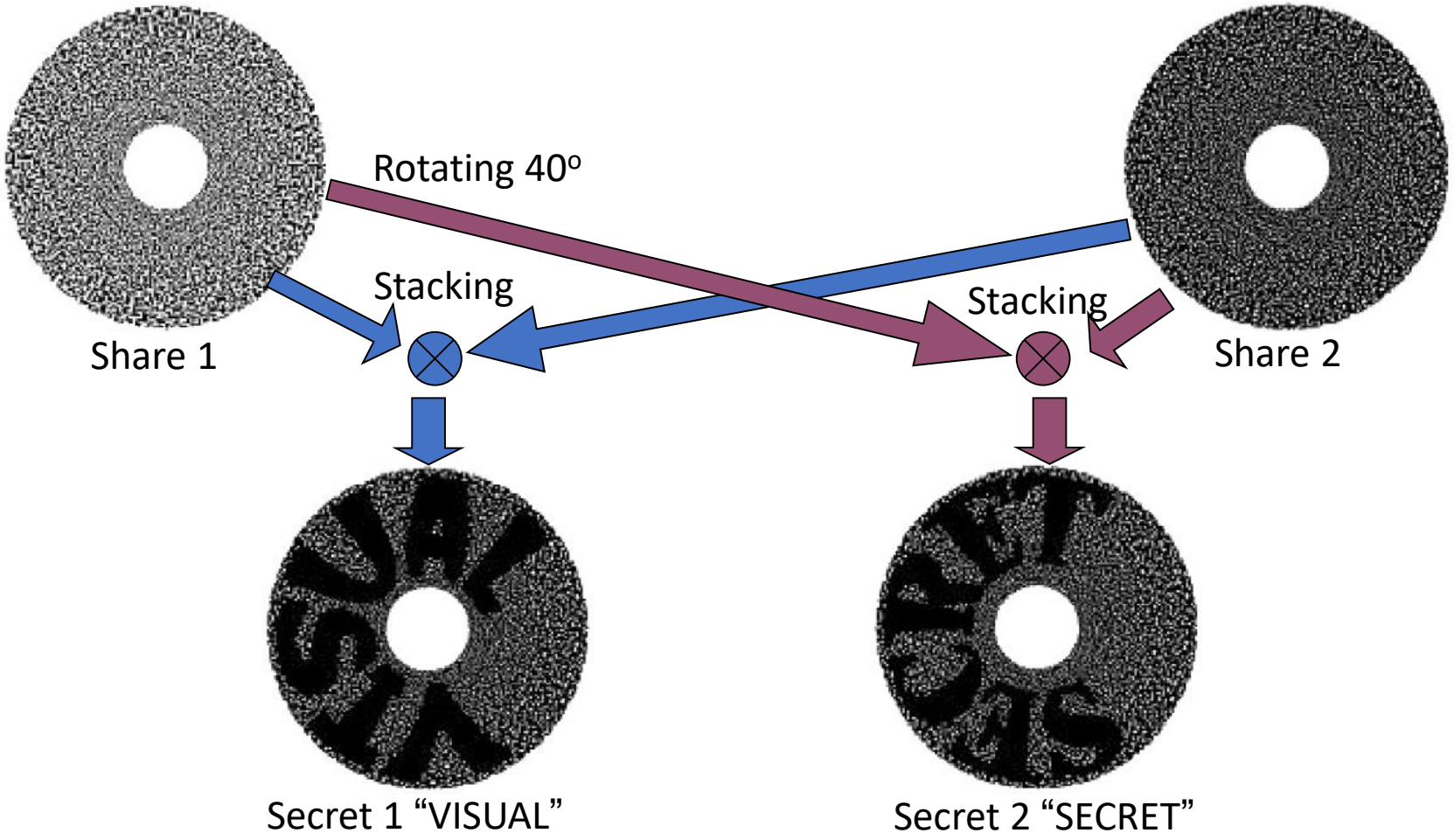


Secret



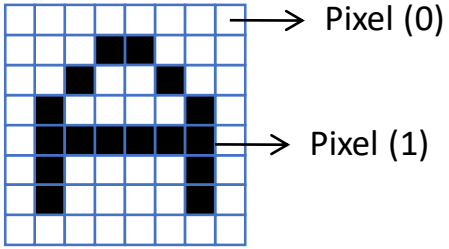
Shadow 2

Visual cryptography (Cont.)



How to make?

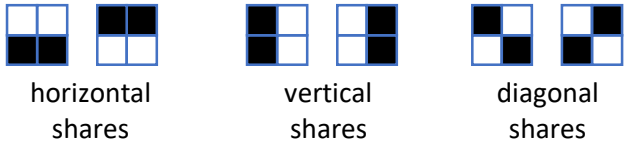
- The simplest visual cryptography
  - Message consists of a collection of black and white pixels.
  - ‘OR’ Operation



$$\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

How to make?

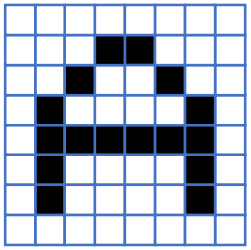
- The simplest visual cryptography



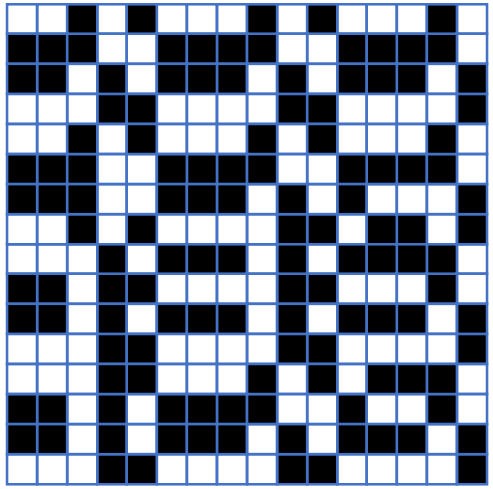
horizontal shares

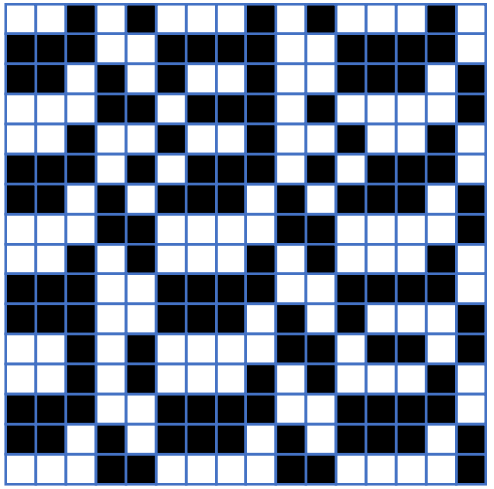
vertical shares

diagonal shares



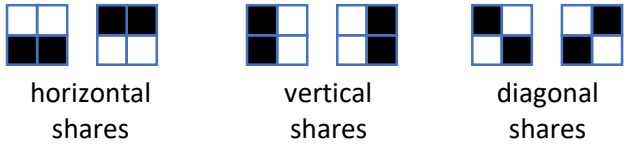
Secret Message

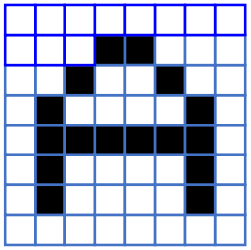


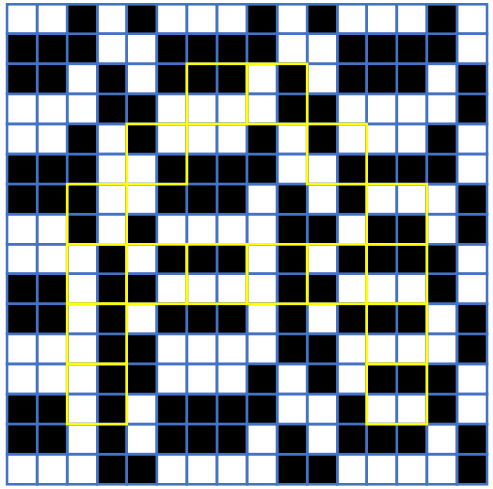


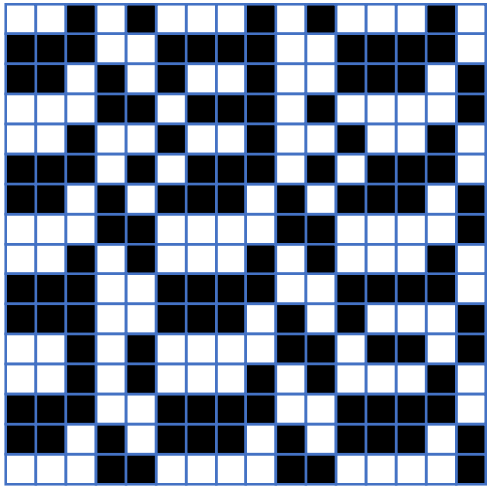
How to make?

- The simplest visual cryptography









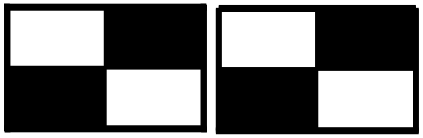
VSS Scheme for Binary Image

- Naor and Shamir (1994) proposed a (k, k)–VSS scheme
  - Extend a secret pixel into a block of 2×2 sub-pixels
  - Contain two white pixels and two black pixels for each block
    - White pixel: transparent
    - Black pixel: black

Secret pixel	Share1	Share2	Stacked image
			
			
			
			

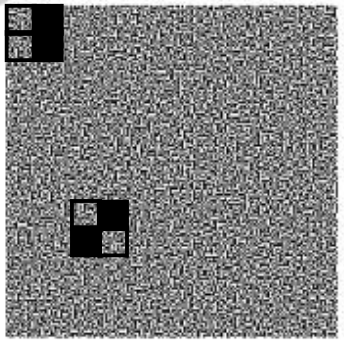
Secret image

Share 1 

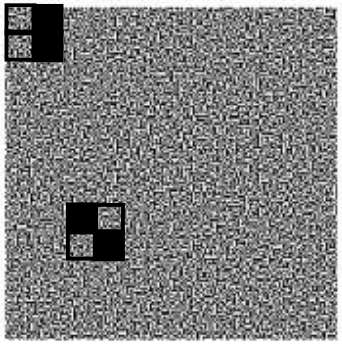
Share 2 

Secret pixel color / Share blocks	White						Black					
2×2 block of the first share												
2×2 block of the second share												
Stacked 2×2 block												

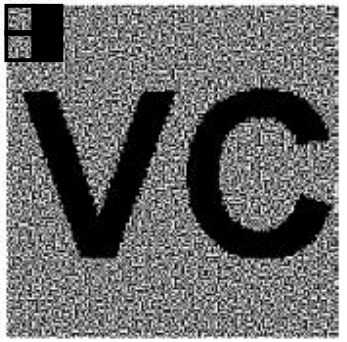
(a) Original secret image



(b) First share image



(c) Second share image



(d) Stacked result of (a) and (b)

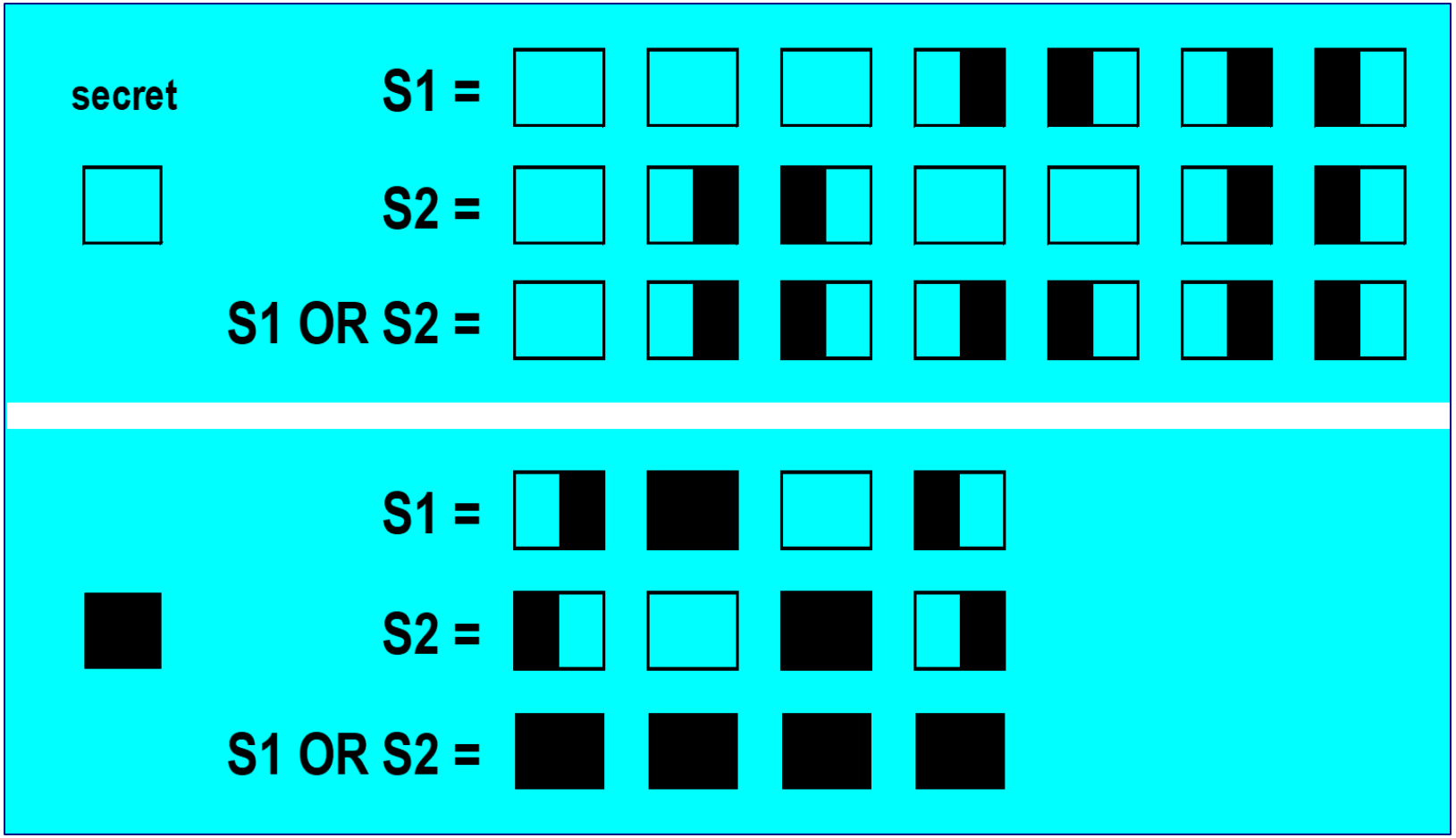
(k, k) Scheme

- In the (k, k)–VSS scheme,
- The first “ k” means that it needs all the k share images to retrieve the secret image.
- The second number “k” means that the secret image is hidden into k share images.

2 out of 2 scheme (2 sub-pixels)

- Black and white image: each pixel divided in 2 sub-pixels
- Choose the next pixel; if white, then randomly choose one of the two rows for white.
- If black, then randomly choose between one of the two rows for black.
- Also we are dealing with pixels sequentially; in groups these pixels could give us a better result.

2 out of 2 scheme (2 sub-pixels)



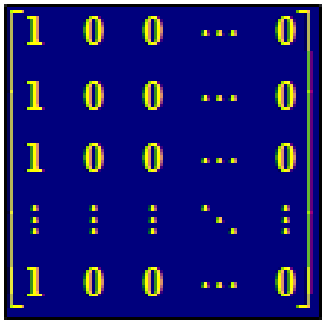
2 out of 2 scheme (2 sub-pixels)

Pixel		Share 1	Share 2	Result
	P = ½			
	P = ½			
	P = ½			
	P = ½			

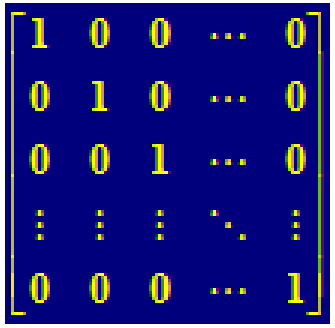
$$C_0 = \left\{ \begin{bmatrix} 01 \\ 01 \end{bmatrix} \begin{bmatrix} 10 \\ 10 \end{bmatrix} \right\} \qquad C_1 = \left\{ \begin{bmatrix} 01 \\ 10 \end{bmatrix} \begin{bmatrix} 10 \\ 01 \end{bmatrix} \right\}$$

General 2 out of n scheme

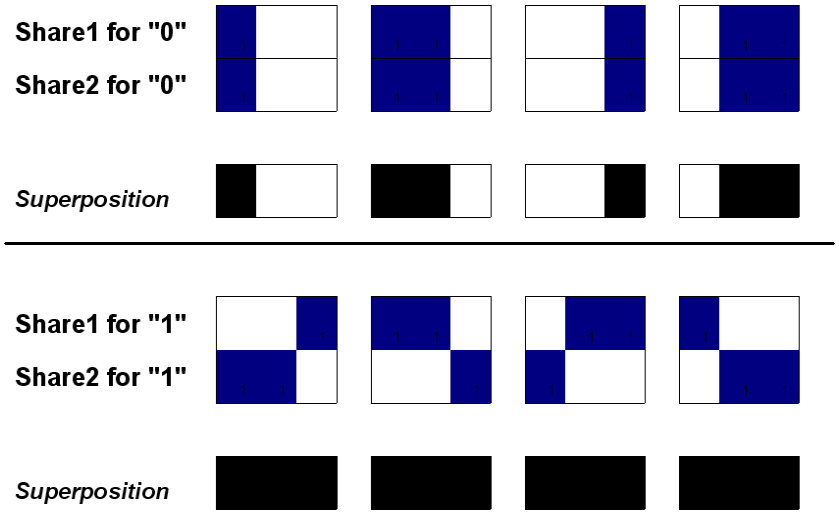
- We take m=n
- White pixel - a random column-permutation of:



- Black pixel - a random column-permutation of:



2 out of 2 scheme (3 sub-pixels)



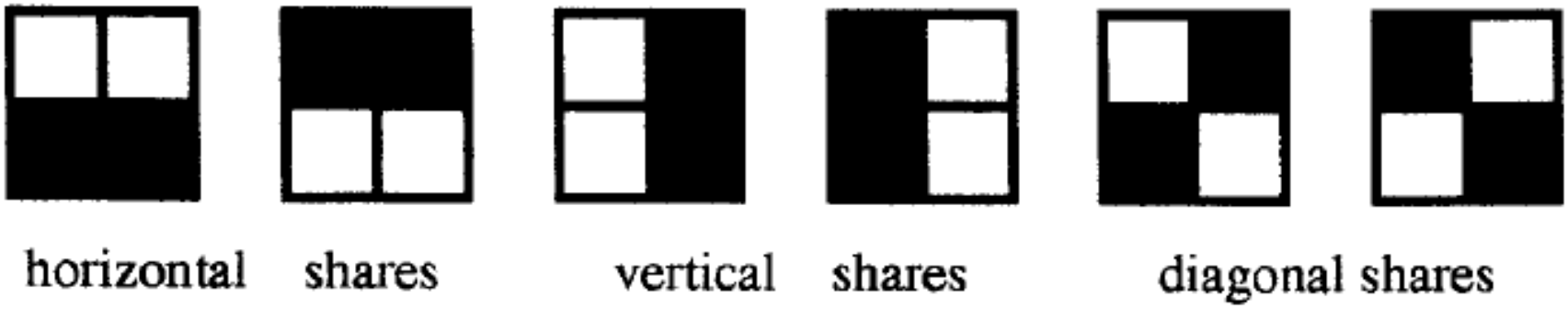
$$S_0 = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \right\}$$

$$S_1 = \left\{ \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \right\}$$

- Each matrix selected with equal probability (0.25)
- Sum of rows is 1 or 2 in S_0, while it is 3 in S_1
- Each share has one or two dark sub-pixels with equal probabilities (0.5) in both sets.

2 out of 2 Scheme (4 sub-pixels)

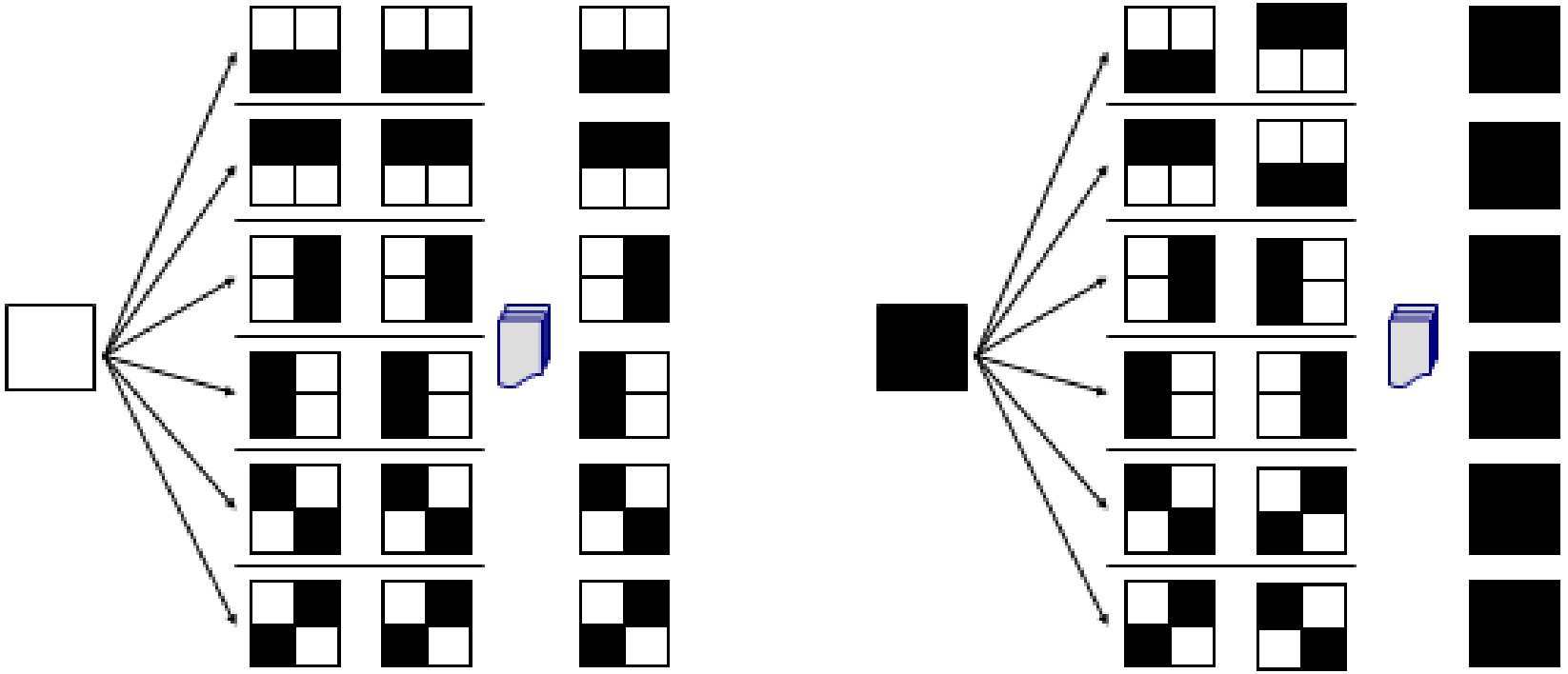
- The 2 sub-pixel scheme disrupts **the aspect ratio of the image**.
- A more desirable scheme would involve division into a square of sub-pixel (size=4)



2 out of 2 Scheme (4 sub-pixels)

$$C_0 = \left\{ \begin{bmatrix} 0101 \\ 0101 \end{bmatrix} \begin{bmatrix} 1010 \\ 1010 \end{bmatrix} \begin{bmatrix} 0011 \\ 0011 \end{bmatrix} \begin{bmatrix} 1100 \\ 1100 \end{bmatrix} \begin{bmatrix} 0110 \\ 0110 \end{bmatrix} \begin{bmatrix} 1001 \\ 1001 \end{bmatrix} \right\}$$

$$C_1 = \left\{ \begin{bmatrix} 0101 \\ 1010 \end{bmatrix} \begin{bmatrix} 1010 \\ 0101 \end{bmatrix} \begin{bmatrix} 0011 \\ 1100 \end{bmatrix} \begin{bmatrix} 1100 \\ 0011 \end{bmatrix} \begin{bmatrix} 0110 \\ 1001 \end{bmatrix} \begin{bmatrix} 1001 \\ 0110 \end{bmatrix} \right\}$$



VSS for color image (Halftone)

- CMY color model is used to represent colors.
- C = 255−R, M = 255−G, Y = 255−B
- (0; 0; 0) ->white
- (255; 255; 255) ->black
- The three monochromatic halftone images will be (cyan, white), (magenta, white) and (yellow, white)

VSS for color image (Halftone)

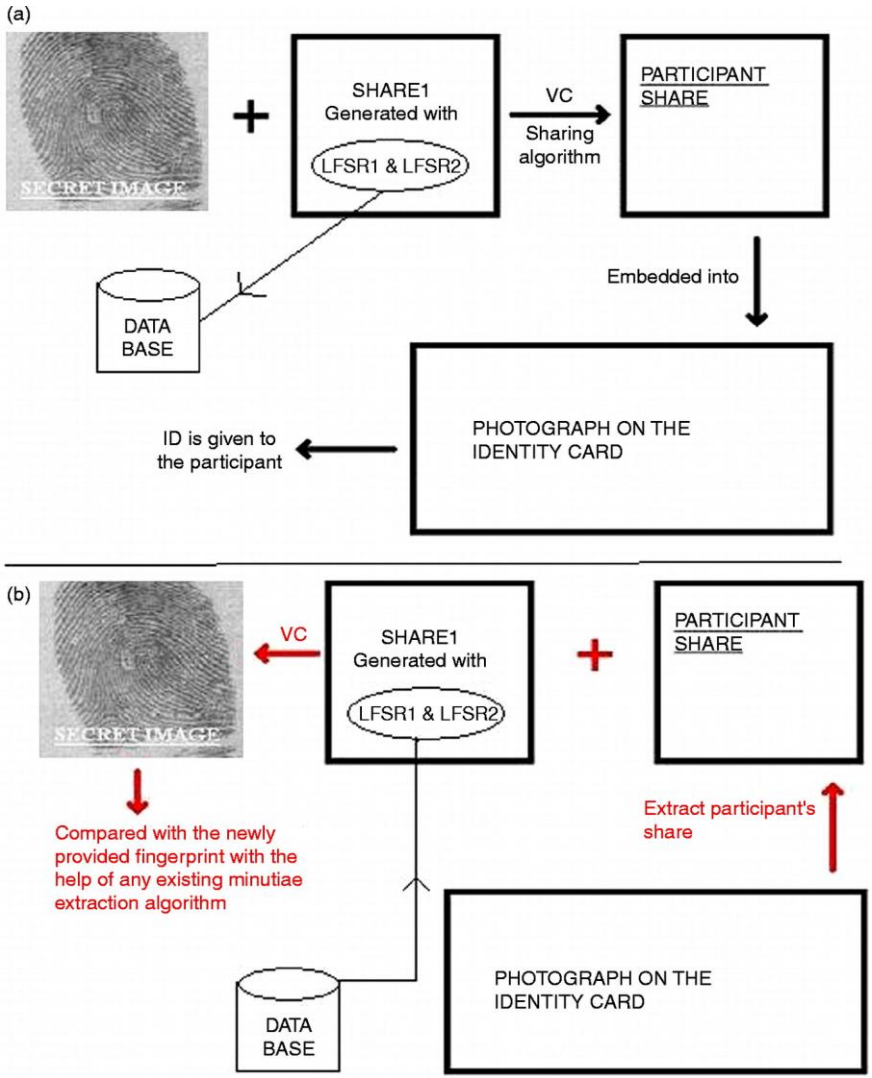
Mask	Revealed color (C,M,Y)	Share1(C)	Share2(M)	Share3(Y)	Stacked image	Revealed color quantity (C,M,Y)
	(0, 0, 0)					(1/2, 1/2, 1/2)
	(1, 0, 0)					(1, 1/2, 1/2)
	(0, 1, 0)					(1/2, 1, 1/2)
	(0, 0, 1)					(1/2, 1/2, 1)
	(1, 1, 0)					(1, 1, 1/2)
	(0, 1, 1)					(1/2, 1, 1)
	(1, 0, 1)					(1, 1/2, 1)
	(1, 1, 1)					(1, 1, 1)

A half black-and-white mask is designed to shade unexpected colors on the stacked sharing images so that only the expected colors show up.

Applications

- Biometric Security
  - Shared Fingerprint
- Watermarking
- Steganography
- Remote Electronic voting
- Bank customer identification

Applications – Shared Fingerprint



(a) Registration

(b) Authentication

Advantages

- Simple to implement.
- Decryption algorithm not required (use human visual system).
- Lower computational cost.
- Infinite Computation Power can’t predict the message
- Cipher text can be sent through fax, email, WhatsApp.

Disadvantage

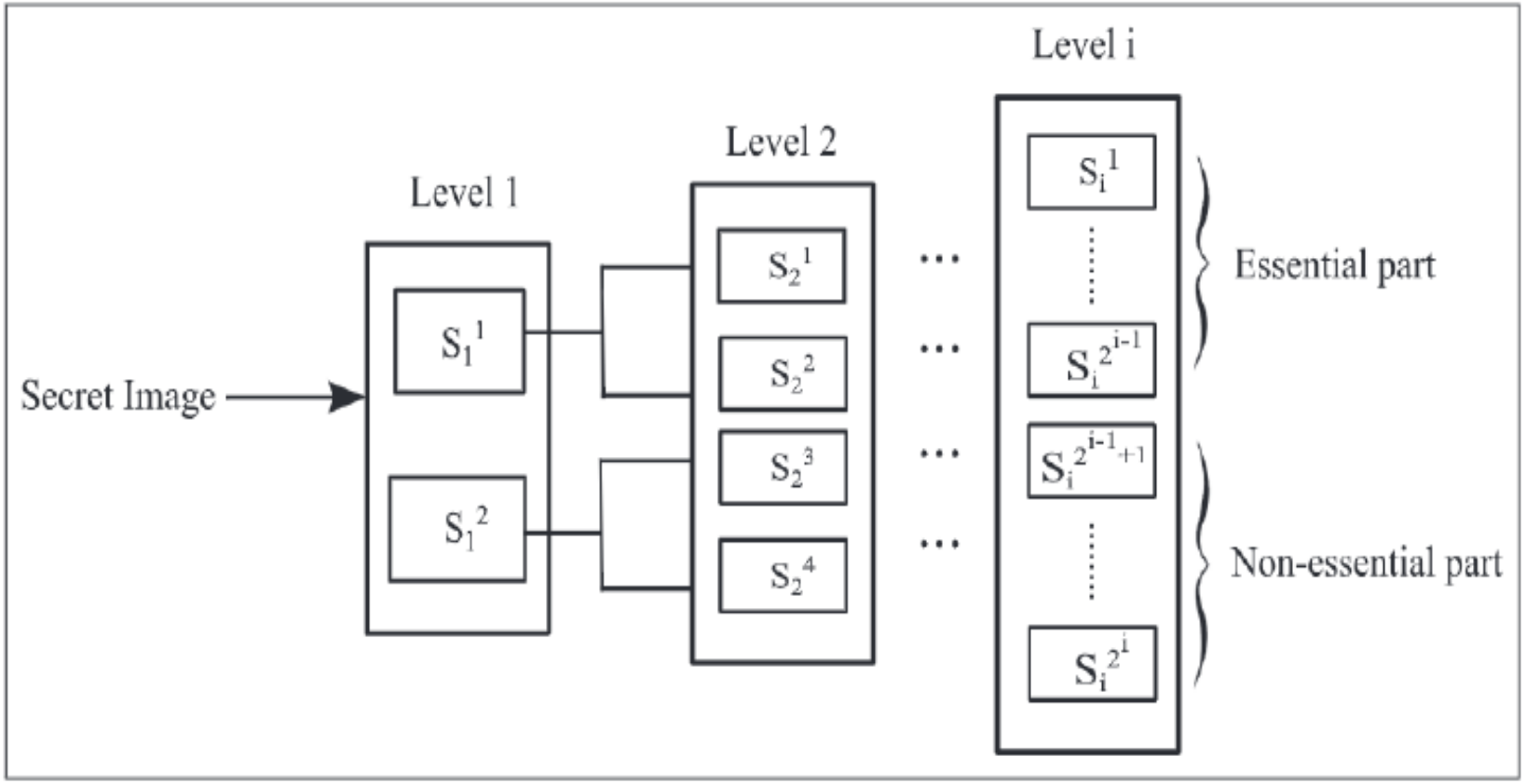
- It’s a Challenge to maintain the contrast of reconstructed image.
- Loss of information.
- Additional processing required for color images.

Affine Boolean Classification in Secret Image Sharing for Progressive Quality Access Control

Objectives

- A lossless secret image sharing scheme, in which generated shadow image's size is smaller to the input image.
- A lossless image sharing scheme in which different shadows have different importance with fault tolerance capability.
- A Secret Image sharing scheme in which generated shadows are more secure compare to exist scheme that used XOR operation.

SIS Scheme


Level i
Level 2
Level 1
Secret Image
S_1^1
S_1^2
S_2^1
S_2^2
S_2^3
S_2^4
S_i^1
$S_i^{2^{i-1}}$
$S_i^{2^{i-1}+1}$
$S_i^{2^i}$
Essential part
Non-essential part

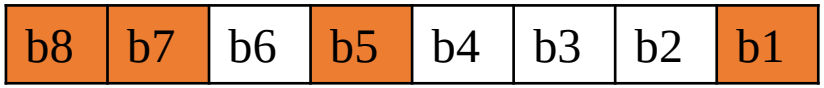
Affine Boolean function

	b8	b7	b6	b5	b4	b3	b2	b1
0	0	0	0	0	0	0	0	0
1	0	1	0	1	0	1	0	1
2	0	0	1	1	0	0	1	1
3	0	1	1	0	0	1	1	0
4	0	0	0	0	1	1	1	1
5	0	1	0	1	1	0	1	0
6	0	0	1	1	1	1	0	0
7	0	1	1	0	1	0	0	1
8	1	1	1	1	1	1	1	1
9	1	0	1	0	1	0	1	0
10	1	1	0	0	1	1	0	0
11	1	0	0	1	1	0	0	1
12	1	1	1	1	0	0	0	0
13	1	0	1	0	0	1	0	1
14	1	1	0	0	0	0	1	1
15	1	0	0	1	0	1	1	0

Fixed bit computation

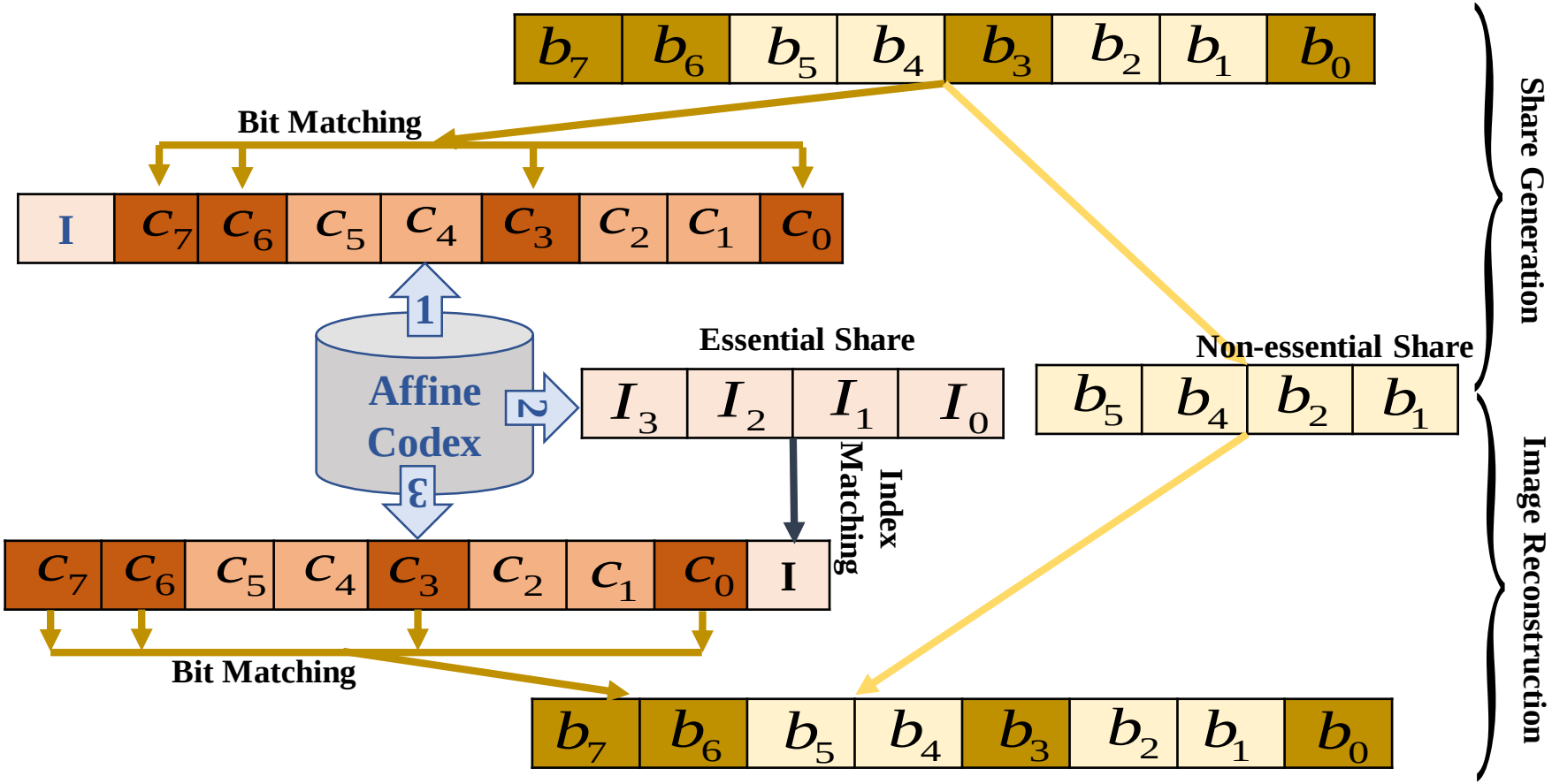
$$F(n) = P_n - 2^k$$

$$Where\ P_n = 2^n + 1\ \&\&\ k = 0,1,2,..n$$



Rout, R.K., Pal Choudhury, P. and Sahoo, S., 2013. Classification of boolean functions where affine functions are uniformly distributed. *Journal of Discrete Mathematics, 2013.*

Share generation and reconstruction procedure



Example

3- Variable Boolean affine function

b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1
1	0	1	0	1	0	1	0

Input Image

1	0	1	0	1	1	1	0

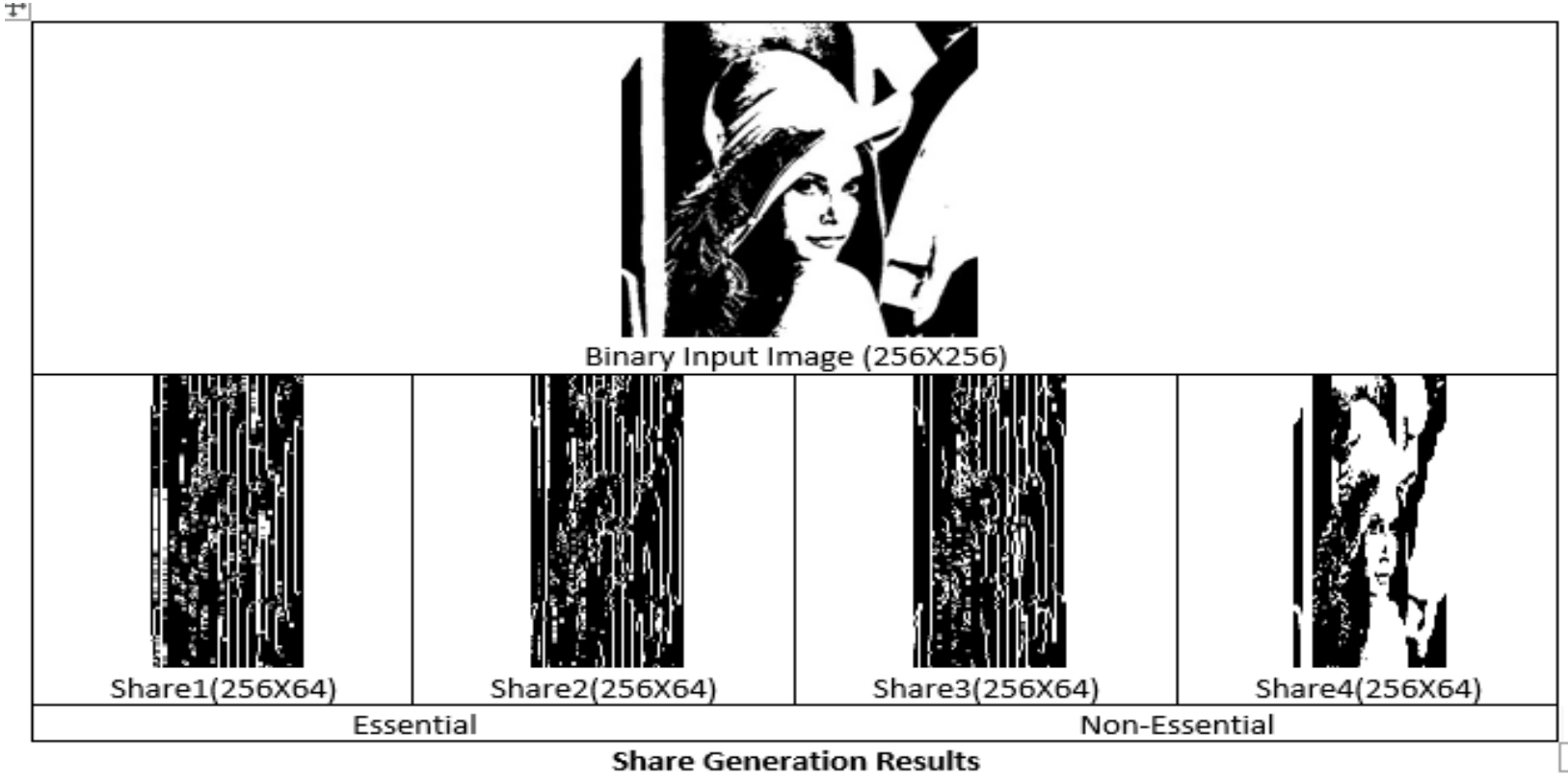
Share1: Index value of affine function

1	0	0	1

Share2: Variable value

1	1	1	1

Binary SIS (Share Generation)



Share Generation Results

Binary SIS (Secret Reconstruction)

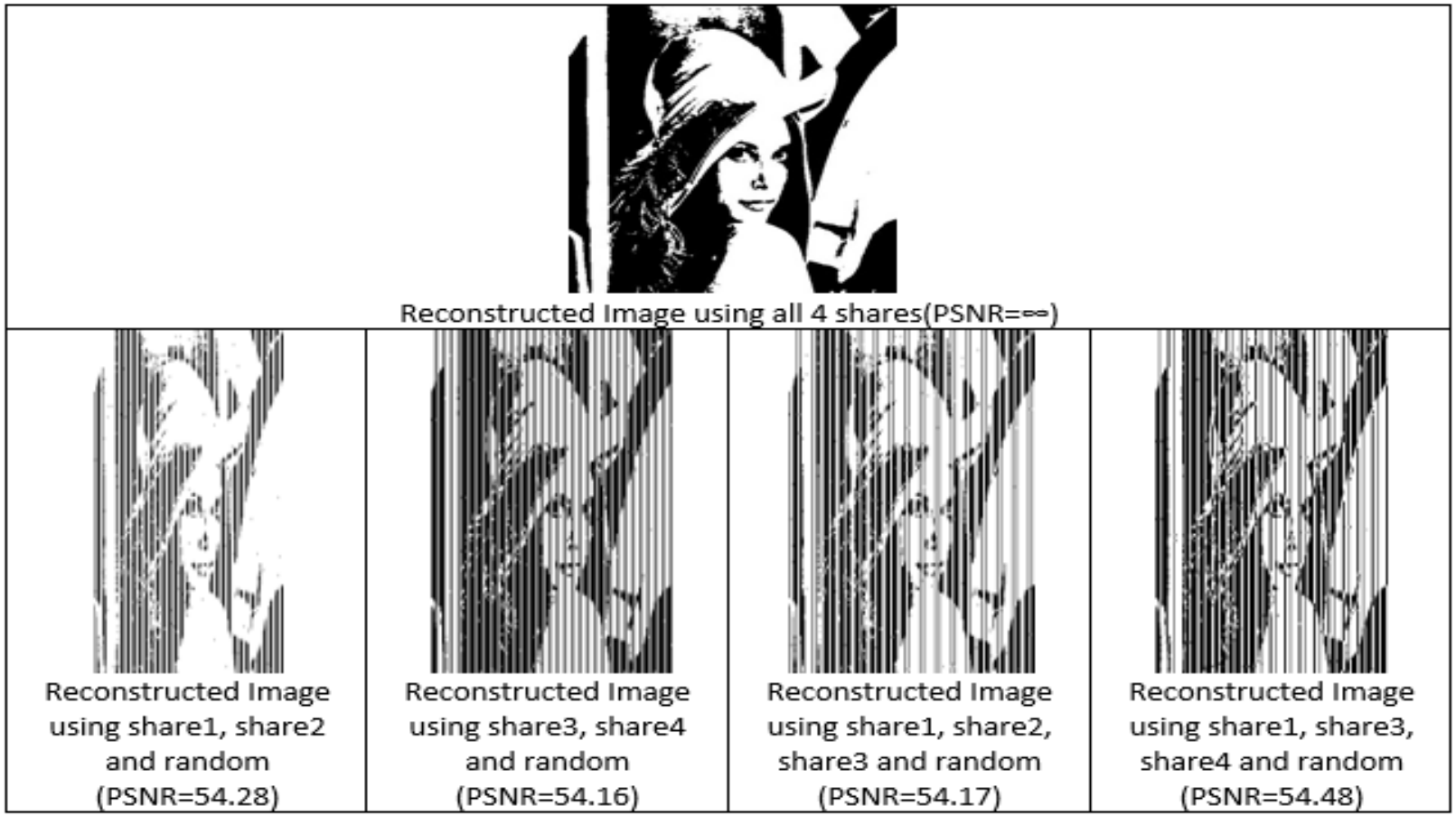
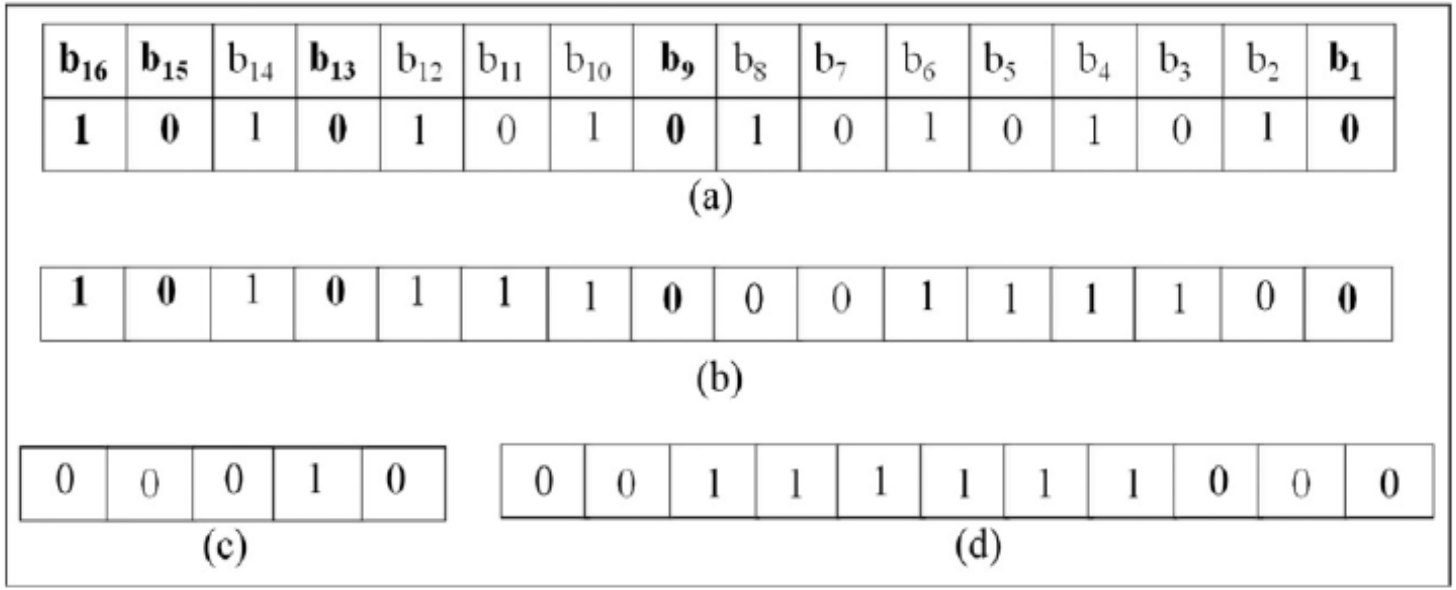


Image Reconstruction Results

SIS for 4 variable function



$\mathbf{b_{16}}$	$\mathbf{b_{15}}$	b_{14}	$\mathbf{b_{13}}$	b_{12}	b_{11}	b_{10}	$\mathbf{b_9}$	b_8	b_7	b_6	b_5	b_4	b_3	b_2	$\mathbf{b_1}$
1	**0**	1	**0**	1	0	1	**0**	1	0	1	0	1	0	1	**0**

(a)

1	**0**	1	**0**	1	**1**	1	**0**	0	0	**1**	1	**1**	1	0	**0**

(b)

0	0	0	1	0

(c)

0	0	1	1	1	1	1	1	**0**	0	**0**

(d)

Gray image SIS

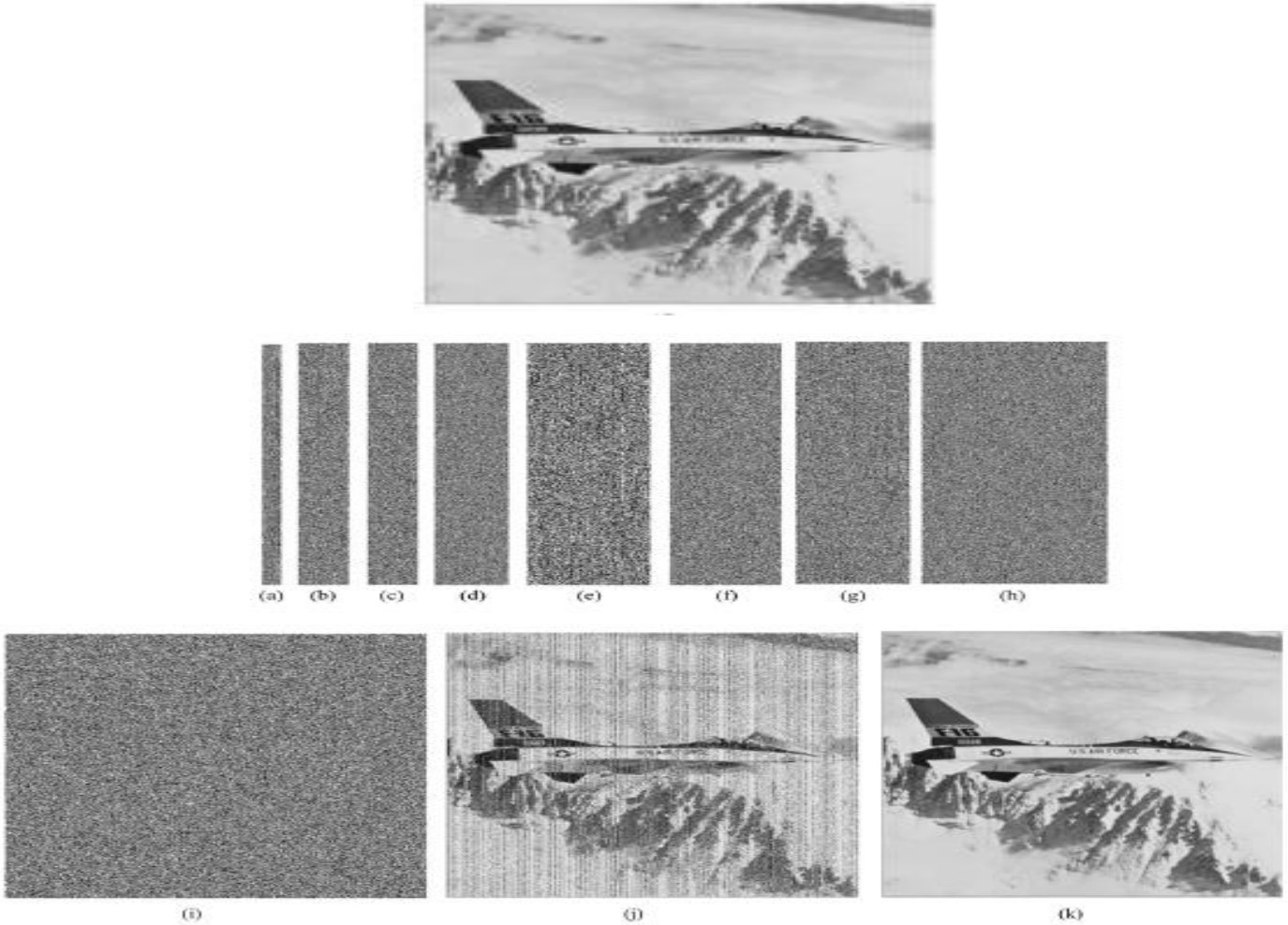


Fig. 5. Share images and the decoded images for the gray scale secret image, F161 : (a)–(h) share images; (i) reconstructed secret image with all the non-essential shares and the random values for the essential shares (PSNR = 9.87 dB); (j) reconstructed secret image using the essential components and the random values for the non-essential components (PSNR = 31.56 dB); (k) reconstructed secret image from all the shares (PSNR = Infinity).

Experimental Results

Table 1
Correlation values of a (4, 8) scheme for a binary secret image.

No. of essential shares	No. of non-essential shares	NCC
0	4	0.00053
1	4	0.0033
2	4	0.0289
3	4	0.0536
4	0	0.63
4	1	0.69
4	2	0.75
4	3	0.82
4	4	1

Table 2
SSIM and PSNR values of a (4, 8) scheme for a gray scale secret image.

No. of essential shares	No. of non-essential shares	SSIM	PSNR
0	4	0.000126	9.87
1	4	0.0011	15.54
2	4	0.0053	28.13
3	4	0.0587	20.56
4	0	0.59	31.56
4	1	0.65	35.87
4	2	0.76	39.28
4	3	0.84	45.01
4	4	1	Infinity