Computer Science and Information Engineering
National Chi Nan University

The Principle and Application of Secret Sharing

Dr. Justie Su-Tzu Juan

Lecture 6. Visual Secret Sharing Scheme

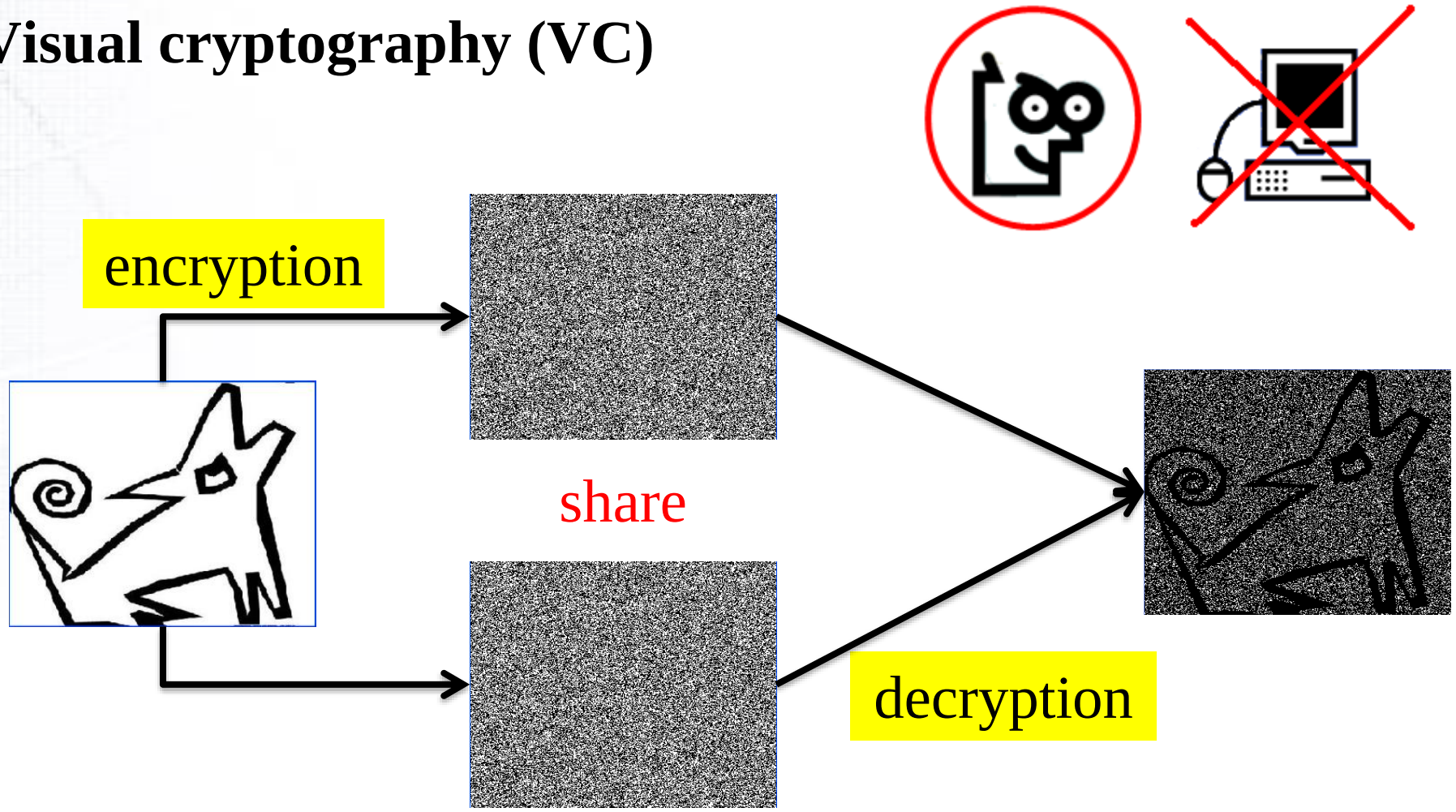
§ 6.1 Visual Cryptography

Slides for a Course Based on

M. Naor and A. Shamir, "Visual Cryptography," EUROCRYPT '94, LNCS 950, pp. 1-12,1995.

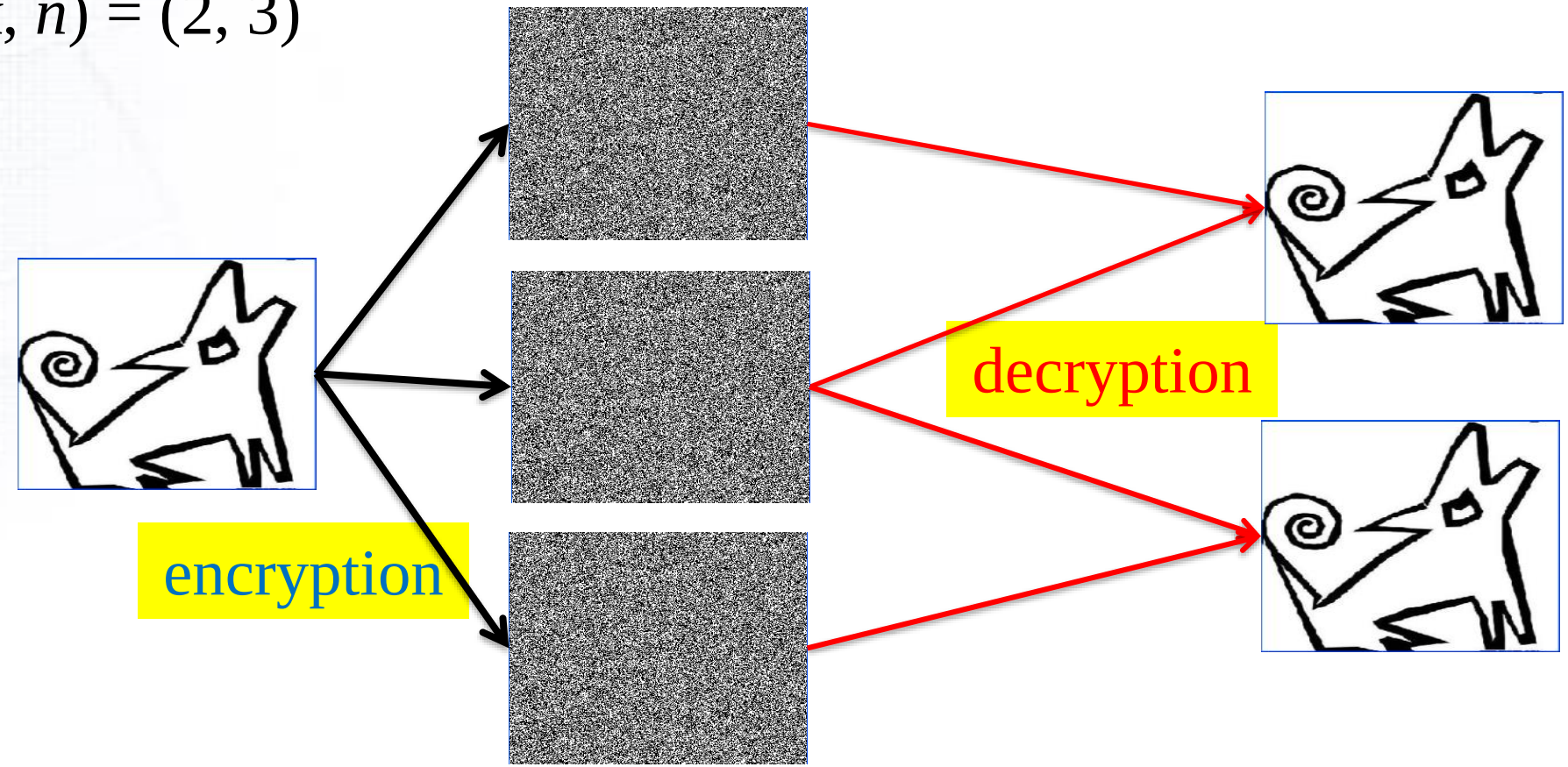
§ 6.1 Visual Cryptography

- **Def: Visual cryptography (VC)**



§ 6.1 Visual Cryptography

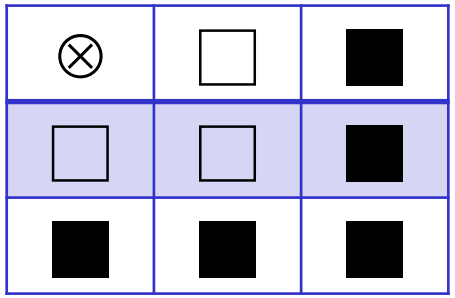
- **Def: (*k*, *n*)-threshold Secret Sharing**
- **Ex**: (*k*, *n*) = (2, 3)



§ 6.1 Visual Cryptography

- **Def:** For **binary** image, only black/white pixel:
  - black → 1
  - white → 0

- Stack = logical **OR** ⊗ operation:
  - 0 ⊗ 0 = 0
  - 0 ⊗ 1 = 1 ⊗ 0 = 1 ⊗ 1 = 1



⊗	□	■
□	□	■
■	■	■

⊗	0	1
0	0	1
1	1	1

§ 6.1 Visual Cryptography

- **Def**: ***Light transmittance rate*** of an area (or an image) S is

  $T(S)$ = # white pixel / all pixels in S.

  $T(S, t)$ = # white pixel / all pixels in the stacked t shares of S.

- **Def**: ***contrast*** α_{NS}**:** The relative difference of the light transmittance between white pixel and black pixel of stacking k shares.

  $\alpha_{NS}(S) = T(S_0, k) - T(S_1, k)$, where S_0 (S_1, resp.) is the area of the stacked k images corresponding to the white (black, resp.) area of the original secret image. If α is lager, it represents the image is clearer to visible.

- **Def**: ***contrast*** $\alpha(t) = \min_{\text{all subset of } N \text{ with size } t} [T(S_0, t) - T(S_1, t)]/[1 + T(S_1, t)]$.

  contrast $\alpha(S) = [T(S_0) - T(S_1)]/[1 + T(S_1)]$. (ps. $N = \{1, 2, \ldots, n\}$)

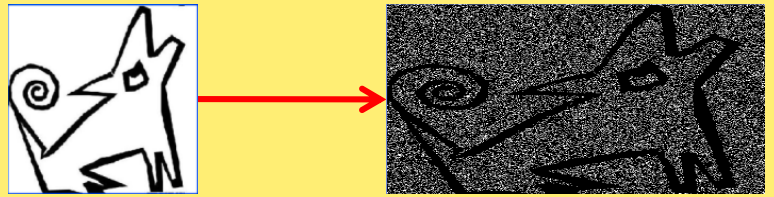
§ 6.1 Visual Cryptography

- **1. For $(k, n) = (2, n)$**
  - **Ex: (2, 2)**

  - White: the same v.s. Black: the complement

$$T(S_0, 2) = ½ \text{ v.s. } T(S_1, 2) = 0$$

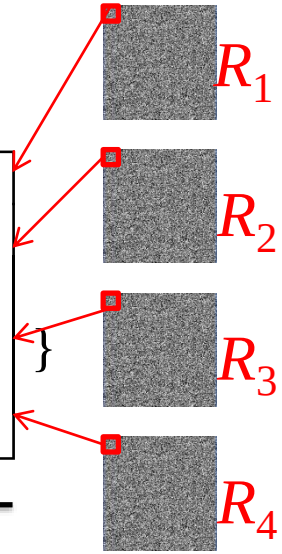
§ 6.1 Visual Cryptogr

VC scheme : 

- **1. For $(k, n) = (2, n)$**
  - **C_0 : white pixel; C_1 : black pixel**
  - **Ex: (2, 4)**

C_0 = {all the matrices obtained by permuting the columns of $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$ }

$C_1 = \{ \ldots \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \}$



OR

R_1 and R_2	$[1 \quad 0 \quad 0 \quad 0]$	$[1 \quad 1 \quad 0 \quad 0]$
R_1, R_2 and R_3	$[1 \quad 0 \quad 0 \quad 0]$	$[1 \quad 1 \quad 1 \quad 0]$
R_1, R_2, R_3 and R_4	$[1 \quad 0 \quad 0 \quad 0]$	$[1 \quad 1 \quad 1 \quad 1]$

§ 6.1 Visual Cryptography

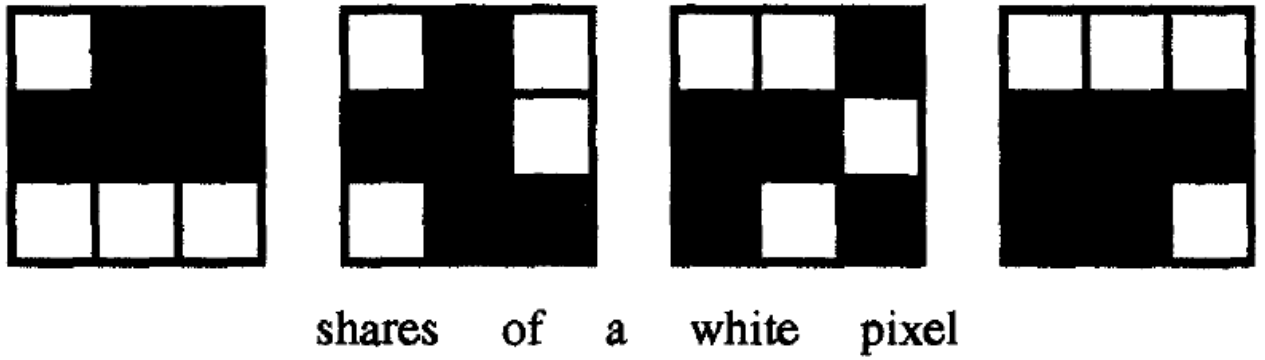
- **2. For $(k, n) = (3, 3)$**
  - C_0 = {all the matrices obtained by permuting the columns of $\begin{bmatrix}0011\\0101\\0110\end{bmatrix}$}
  - C_1 = {all the matrices obtained by permuting the columns of $\begin{bmatrix}1100\\1010\\1001\end{bmatrix}$}
  - $T(S_0, 1) = ½$ v.s. $T(S_1, 1) = ½$;
  - $T(S_0, 2) = ¼$ v.s. $T(S_1, 2) = ¼$;
  - $T(S_0, 3) = ¼$ v.s. $T(S_1, 3) = 0$.

§ 6.1 Visual Cryptography

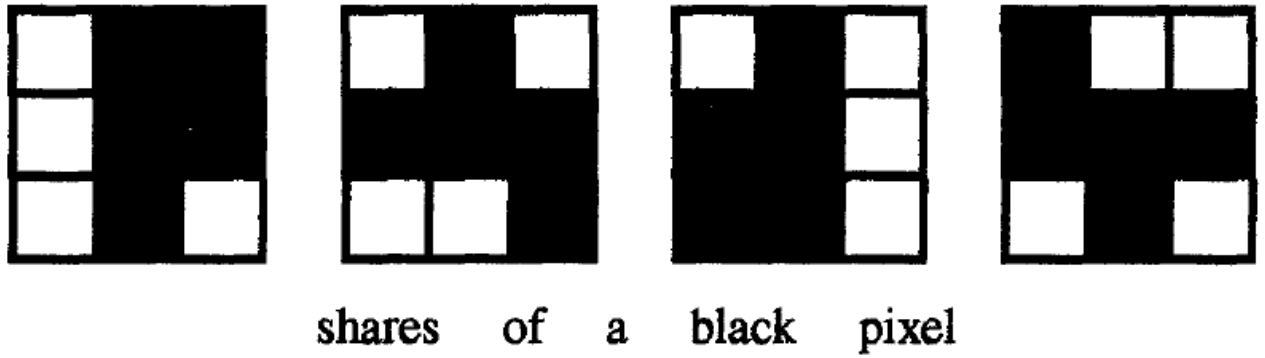
- **3. For $(k, n) = (3, n)$**
  - C_0 = {all the matrices obtained by permuting the columns of $\begin{bmatrix} 0 & 001\cdots1 \\ 0 & 010\cdots1 \\ \vdots & \vdots\ \vdots\ \vdots\ \ddots\ \vdots \\ 0 & 011\cdots0 \end{bmatrix}_{n\times(2n-2)}$},
  - C_1 = {all the matrices obtained by permuting the columns of $\begin{bmatrix} 1 & 110\cdots0 \\ 1 & 101\cdots0 \\ \vdots & \vdots\ \vdots\ \vdots\ \ddots\ \vdots \\ 1 & 100\cdots1 \end{bmatrix}_{n\times(2n-2)}$}.
  - $T(S_0, 1) = (n-1)/(2n-2)$ v.s. $T(S_1, 1) = (n-1)/(2n-2)$;
  - $T(S_0, 2) = (n-2)/(2n-2)$ v.s. $T(S_1, 2) = (n-2)/(2n-2)$;
  - $T(S_0, t) = (n-2)/(2n-2)$ v.s. $T(S_1, 3) = (n-t)/(2n-2)$ for $t \geq 3$.

§ 6.1 Visual Cryptography

- **4. For $(k, n) = (4, 4)$**
  - $T(S_0, 1) = 4/9$ v.s. $T(S_1, 1) = 4/9$;
  - $T(S_0, 2) = 2/9$ v.s. $T(S_1, 2) = 2/9$;
  - $T(S_0, 3) = 1/9$ v.s. $T(S_1, 3) = 1/9$;
  - $T(S_0, 4) = 1/9$ v.s. $T(S_1, 3) = 0$.



shares of a white pixel



shares of a black pixel

§ 6.1 Visual Cryptography

- **5. For $(k, n) = (k, k)$**
  - **Ex: (4, 4)**
  - C_0 = {all the matrices obtained by permuting the columns of $\begin{bmatrix} 00001111 \\ 00110011 \\ 01010101 \\ 01101001 \end{bmatrix}_{4\times 8}$},
  - C_1 = {all the matrices obtained by permuting the columns of $\begin{bmatrix} 10001110 \\ 01001101 \\ 00101011 \\ 00010111 \end{bmatrix}_{4\times 8}$}.

§ 6.1 Visual Cryptography

- **6. For (*k*, *n*)**
  - Thm: For any n and k there exists a visual secret sharing scheme with parameters $m = n^k \cdot 2^{k-1}$, $\alpha = (2e)^{-k}/\sqrt{(2\pi k)}$ and $r = n^k(2^{k-1}!)$.

- **For Meaningful shares:**
  - For white pixel:

two white shares | white and black shares | two black shares

  - For black pixel:

two white shares | white and black shares | two black shares

§ 6.1 Visual Cryptography

- **The drawbacks of Naor and Shamir's VC:**
  - Pixel expansion ($m > 1$)
  - Need code book.
  - Small α.

Computer Science and Information Engineering
National Chi Nan University

The Principle and Application of Secret Sharing

Dr. Justie Su-Tzu Juan

Lecture 6. Visual Secret Sharing Scheme

§ 6.2 A (k, n)-threshold Progressive Visual Secret Sharing without Expansion

Slides for a Course Based on

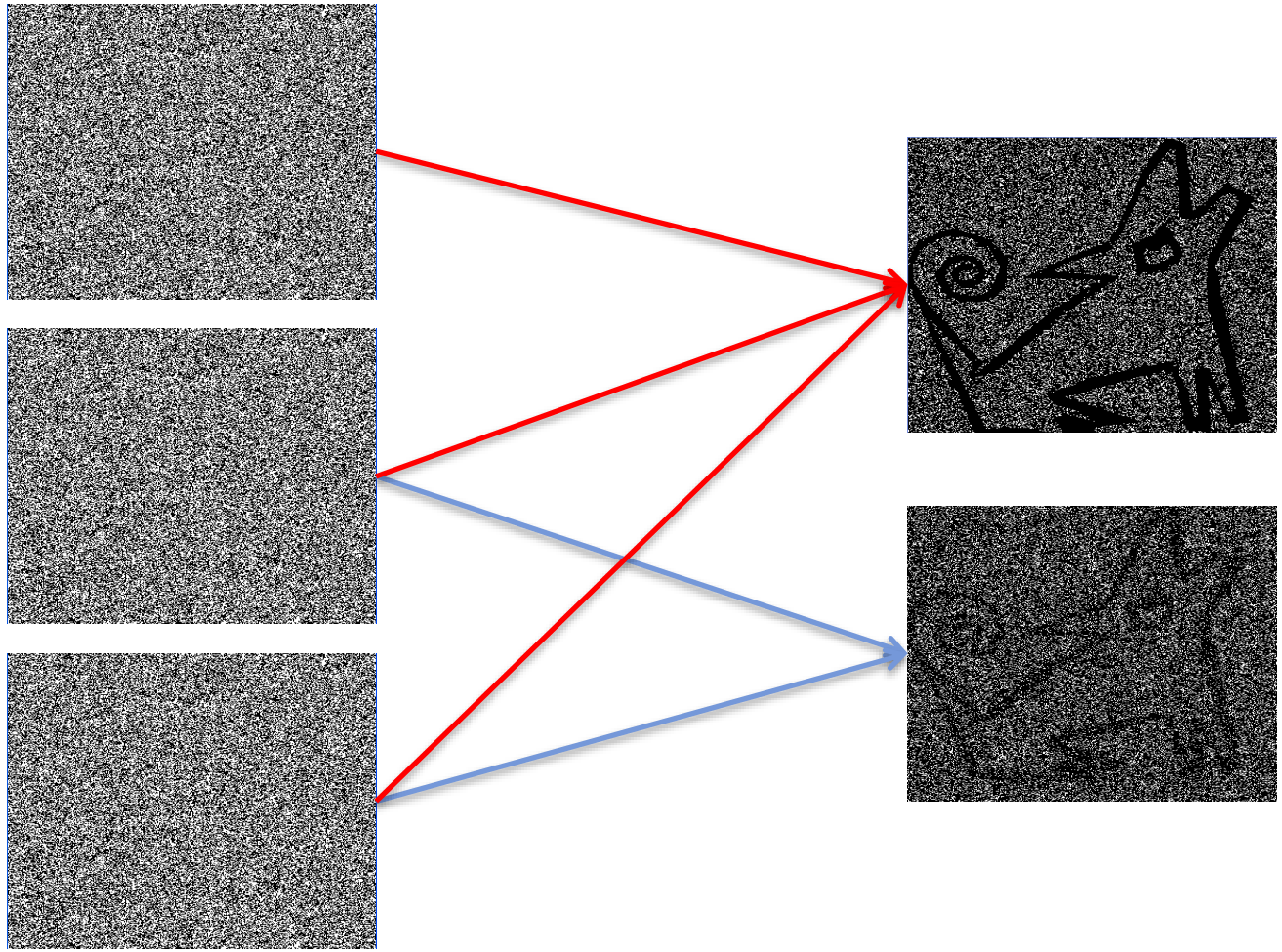
Y.-Y. Chen "A Study of (k, n)-threshold Secret Image Sharing Schemes in Visual Cryptography without Expansion", Master Thesis of Department of SCIE, National Chi Nan University, 2011.

Outline

- Introduction
- Related Work
- Preliminary
- The (4, *n*)-threshold Secret Sharing Scheme: CJ0 Scheme
- The (*k*, *n*)-threshold Secret Sharing Scheme: CJ Scheme
- Comparison
- Conclusion

Introduction – Progressive visual secret sharing

- Progressive visual secret sharing (PVSS)



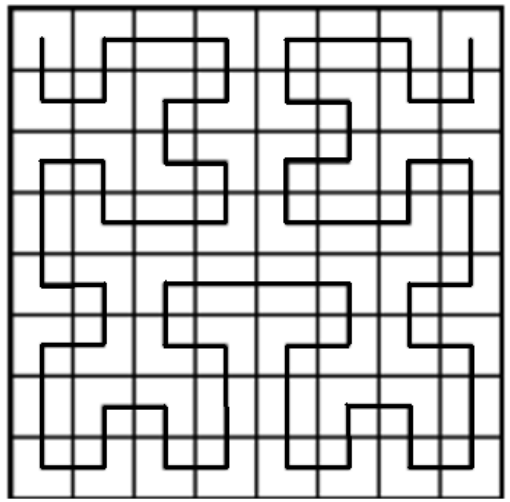
Related Work

- Fang et al. (2008)

  They construct a (k, n)-threshold secret sharing scheme in VC without expansion.

  - They use the method of "Hilbert-curve."

  - The size of the discussed images can only be $2^r \times 2^r$, for $r \in N$.



Preliminary

- **Definition 1**.

  An $n \times m$ 0-1 matrix $M(n, j)$ is called *totally symmetric* if each column has the same weight, say j, and m equals to C_j^n, where the *weight* of a column vector means the sum of each entry in this column vector.

- $M(4, 2) = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$, $M(4, 1) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

  $m = C_2^4 = 6$

Preliminary

$\begin{bmatrix} A \end{bmatrix}$ $\begin{pmatrix} \end{pmatrix}$ $\begin{bmatrix} B \end{bmatrix}$

- **Definition 2**.

  Given an $n \times m_1$ matrix A and an $n \times m_2$ matrix B, we define

  1. $[A||B]$ be an $n \times (m_1 + m_2)$ matrix that obtained by concatenating A and B;
  2. $[a \times A||b \times B]$ be an $n \times (a \times m_1 + b \times m_2)$ matrix that be obtained by concatenating A for a times and B for b times.

$$A = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \quad [2A||B] = \overbrace{\begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}}^{2A} \overbrace{\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}}^{B}$$

Preliminary

- **Lemma 1**.

  Given an $n \times m$ totally symmetric matrix $A = M(n, j)$. For $i = 1, \ldots, n$, let $f_i(A)$ represent the Hamming weight of the row vector that is the result of applying "or" operation for any i rows in A. Then $f_i(A) = f_i(M(n, j)) = C_j^n - C_j^{n-i}$

$A = M(4, 2) =$

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

$f_2(A) = 5$

1 1 1 1 1 0

or

$f_1(A) = 3$ $f_2(A) = 5$ $f_3(A) = 6$ $f_4(A) = 6$

Preliminary

- **Lemma 2**.

  $f_i([A||B]) = f_i(A) + f_i(B)$ for any two totally symmetric matrices A and B.

$$A = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \quad [A||B] = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

$$f_2([A||B]) = 2 = 0 + 2 = f_2(A) + f_2(B)$$

Preliminary

- **Definition 3**.

  Light transmission rate $\mathfrak{T}$ = white pixel / all pixel
  = 1 – (black pixel / all pixel).

- **Definition 4**.

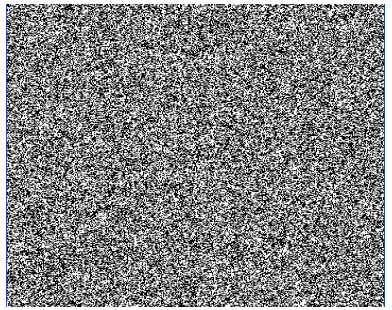
  Given an $n \times m$ totally symmetric matrix B, we define $\mathfrak{T}(B, t) = 1 - (f_t(B) / m)$, where $t \leq n$.

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

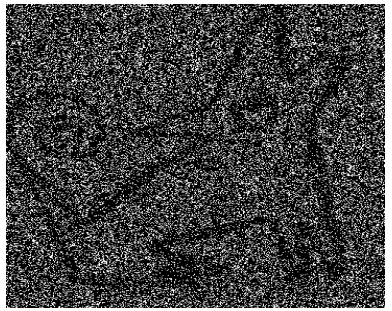
$$\mathfrak{T}(B, 2) = 1 - (f_2(B) / 4)$$
$$= 1 - 2 / 4 = 1 / 2$$

The (4, *n*)-threshold Secret Sharing Scheme: CJ0 Scheme

- Two conditions :
  - $\mathfrak{I}(C_0, t) = \mathfrak{I}(C_1, t)$ for $1 \le t \le 3$.



  - $\mathfrak{I}(C_0, t) > \mathfrak{I}(C_1, t)$ for $t \ge 4$.



Ying-Yu Chen, Justie Su-Tzu Juan*, July 2011, "A 4 out of *n* Secret Sharing Scheme in Visual Cryptography without Expansion," *Proc. of Int. Conf. on Foundations of Computer Science*, Monte Carlo Resort, Las Vegas, Nevada, USA, July 18-21, 2011, pp. 28-33.

CJ0 Scheme – Algorithm

- **Input** : A binary secret S with size $w \times h$ and the value of n.
- **Output** : n shares $R_1, R_2, \ldots, R_n$, each with size $w \times h$.

1. Let $C_0 = [M(n, 2) \,||\, (\sum_{k=1}^{n-3} k)\, M(n, 0) \,||\, (n - 3)\, M(n, n)]$

   $C_1 = [(n - 3)\, M(n, 1) \,||\, M(n, n - 1)]$
2. for $(1 \le i \le h;\ 1 \le j \le w)$

   x = random(1..m)

   for $(1 \le t \le n)$

   if ($S(i, j) == 0$)

   $R_t(i, j) = C_0(t, x)$;

   else

   $R_t(i, j) = C_1(t, x)$;

CJ0 Scheme – Algorithm

Theorem 1.

In the proposed scheme, if we stack at least four shares, it can reveal the secret; and if we stack less than or equal to three shares, it cannot reveal the secret.

- **Proof**

$$\mathfrak{I}(C_0, t) = \mathfrak{I}(C_1, t) \text{ for } 1 \leq t \leq 3.$$

$$\mathfrak{I}(C_0, t) > \mathfrak{I}(C_1, t) \text{ for } t \geq 4.$$

CJ0 Scheme – Experimental Results

- **Example: (4, 5)**
  - $C_0 : [M(5, 2) \,\|\, 3 \times M(5, 0) \,\|\, 2 \times M(5, 5)]$

$$\left[\begin{array}{cccccccccc|ccc|cc} 0&0&0&1&0&0&1&0&1&1 & 0&0&0 & 1&1 \\ 0&0&1&0&0&1&0&1&0&1 & 0&0&0 & 1&1 \\ 0&1&0&0&1&0&0&1&1&0 & 0&0&0 & 1&1 \\ 1&0&0&0&1&1&1&0&0&0 & 0&0&0 & 1&1 \\ 1&1&1&1&0&0&0&0&0&0 & 0&0&0 & 1&1 \end{array}\right]$$

$M(5, 2)$ $3M(5, 0)$ $2M(5, 5)$

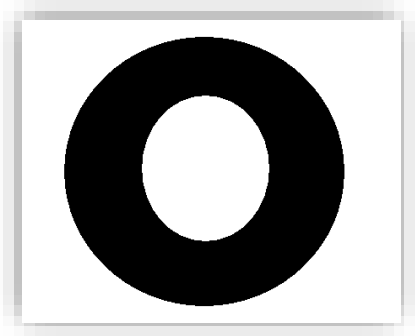
  - $C_1 : \; [2 \times M(5, 1) \,\|\, M(5, 4)]$

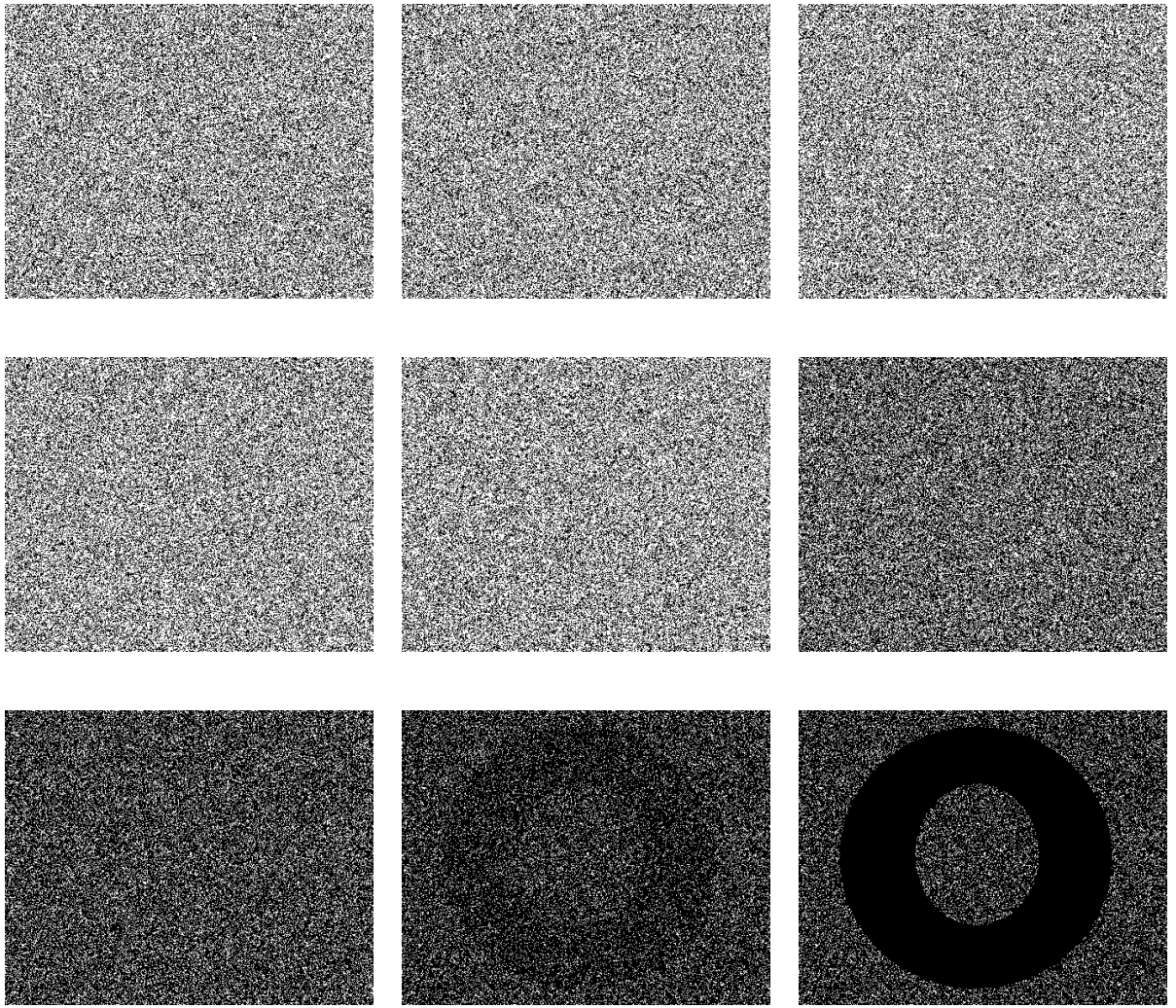
$2M(5, 1)$ $M(5, 4)$

$$\left[\begin{array}{cccccccccc|ccccc} 0&0&0&0&1&0&0&0&0&1 & 1&1&1&1&0 \\ 0&0&0&1&0&0&0&0&1&0 & 1&1&1&0&1 \\ 0&0&1&0&0&0&0&1&0&0 & 1&1&0&1&1 \\ 0&1&0&0&0&0&1&0&0&0 & 1&0&1&1&1 \\ 1&0&0&0&0&1&0&0&0&0 & 0&1&1&1&1 \end{array}\right]$$

CJ0 Scheme – Experimental Results

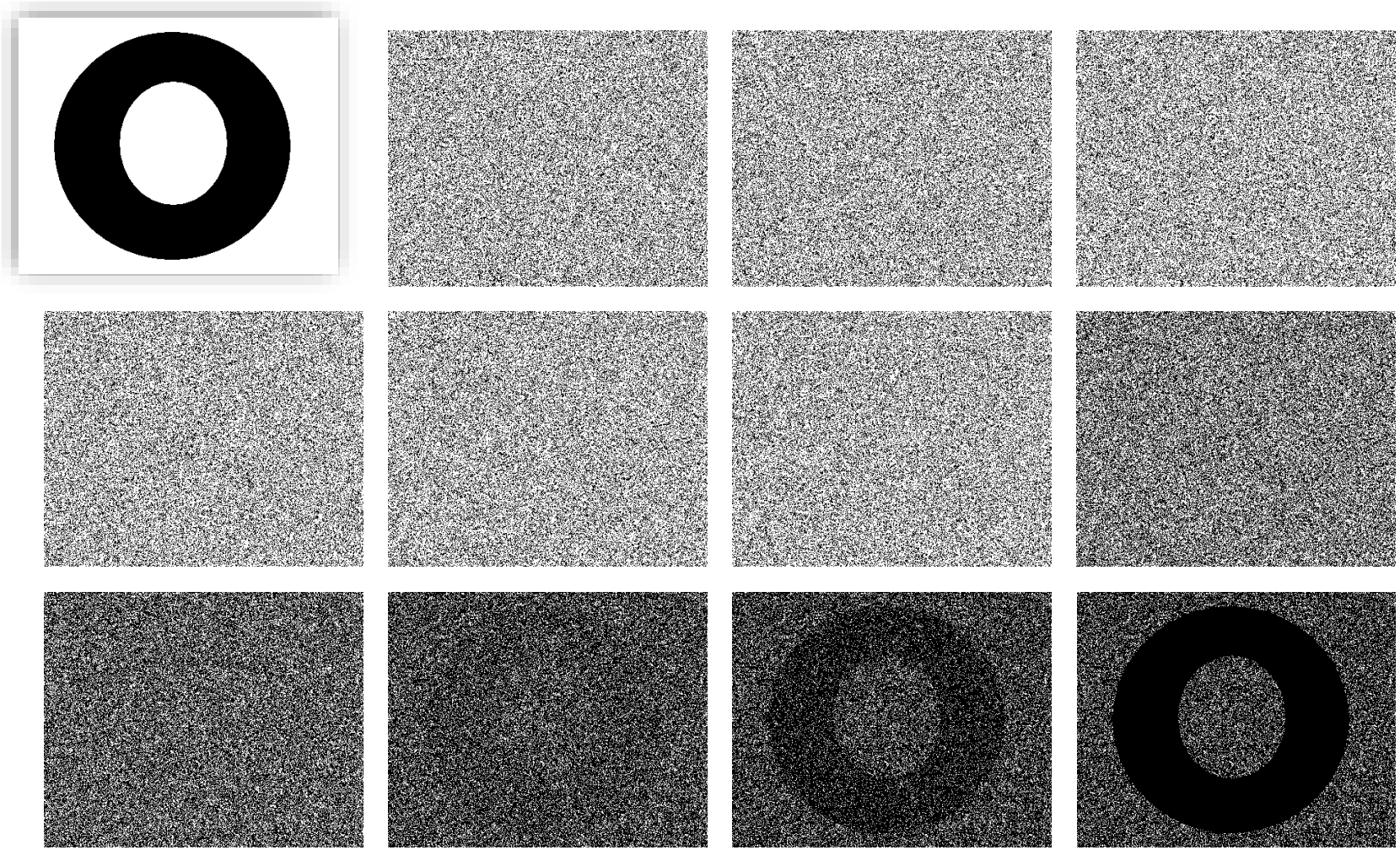
- (4, 5)





CJ0 Scheme – Experimental Results

- (4, 6)



The (k, n)-threshold Secret Sharing Scheme: CJ Scheme

- For any two positive integer $2 \le k \le n$.

- Two conditions :
  - $\mathfrak{I}(C_0, t) = \mathfrak{I}(C_1, t)$ for $1 \le t \le k-1$.
  - $\mathfrak{I}(C_0, t) > \mathfrak{I}(C_1, t)$ for $t \ge k$.

Ying-Yu Chen, Bo-Yuan Huang and Justie Su-Tzu Juan*, "A (k, n)-threshold Progressive Visual Secret Sharing without Expansion," *Cryptography*, Vol. 2, Iss. 4, (September 2018) 28. (https://www.mdpi.com/2410-387X/2/4/28).

CJ Scheme – Algorithm

- **Input** : A binary secret S with size $w \times h$ and the value of n and k.
- **Output** : n shares $R_1, R_2, \ldots, R_n$, each with size $w \times h$.

1. if (k mod 2 == 1)

$$C_0 = \left[M(n,2) \,||\, C_2^{n-k+2} M(n,0) \,||\, \sum_{t=1}^{(k-3)/2} C_{k-2t-2}^{n-2t-2} M(n, n-2t+1) \right]$$

$$C_1 = \left[(n-k+1) M(n,1) \,||\, C_{k-3}^{n-3} M(n,n) \,||\, \sum_{t=1}^{(k-3)/2} C_{k-2t-3}^{n-2t-3} M(n, n-2t) \right]$$

else

$$C_0 = \left[M(n,2) \,||\, C_2^{n-k+2} M(n,0) \,||\, C_{k-3}^{n-3} M(n,n) \,||\, \sum_{t=1}^{k/2-2} C_{k-2t-3}^{n-2t-3} M(n, n-2t) \right]$$

$$C_1 = \left[(n-k+1) M(n,1) \,||\, \sum_{t=1}^{k/2-1} C_{k-2t-2}^{n-2t-2} M(n, n-2t+1) \right]$$

2. for ($1 \le i \le h$; $1 \le j \le w$)

x = random(1..m)

for ($1 \le t \le n$)

if ($S(i, j)$ == 0)

$R_t(i, j) = C_0(t, x)$;

else

$R_t(i, j) = C_1(t, x)$;

CJ Scheme – Proof

Definition 4:
Given an $n \times m$ totally symmetric matrix B, we define $\mathcal{I}(B, t) = 1 - (f_t(B) / m)$, where $t \leq n$.

Theorem 2.

In the proposed scheme, if we stack at least k shares, it can reveal the secret; and if we stack less than or equal to $k - 1$ shares, it cannot reveal the secret.

- **Proof**

$\mathcal{I}(C_0, t) = \mathcal{I}(C_1, t)$ for $1 \leq t \leq k - 1$.

$\mathcal{I}(C_0, t) > \mathcal{I}(C_1, t)$ for $t \geq k$.

$\mathcal{I}(C_0, t) = 1 - (f_t(C_0) / m_{C0})$;
$\mathcal{I}(C_1, t) = 1 - (f_t(C_1) / m_{C1})$.

- Case 1: k is odd.
- Case 2: k is even.

CJ Scheme – Proof

- Denominator

  No matter what k and n are, $m_{C0} = m_{C1}$.

  $$m_{C0} = C_2^n + C^{n-k+2}{}_2 C_0^n + \Sigma_{k=1}^{(k-3)/2} [C_{k-2t-2}^{n-2t-2} C_{n-2t+2}^{n}]$$

  $$m_{C1} = (n-k+1)C_1^n + C_{k-3}^{n-3} C_n^n + \Sigma_{k=1}^{(k-3)/2} [C_{k-2t-3}^{n-2t-3} C_{n-2t}^{n}]$$

We proof it by induction on j, where $j = n - k$,

1. If $j = 0 \Rightarrow n = k$

   $$m_{C0} = C_0^k + C_2^k + \ldots + C_{k-1}^k$$

   $$m_{C1} = C_1^k + C_3^k + \ldots + C_k^k$$

According to the Pascal theorem $\therefore m_{C0} = m_{C1}$ is true.

CJ Scheme – Proof

2. Assume $j = m \Rightarrow n = k + m$, $m_{C0} = m_{C1}$ is true.

$$C_{2}^{k+m} + C_{2}^{m+2} C_{0}^{k+m} + \sum_{k=1}^{(k-3)/2} [C_{k-2t-2}^{k+m-2t-2} C_{k+m-2t+1}^{k+m}]$$

$$= (m+1) C_{1}^{k+m} + C_{k-3}^{k+m-3} C_{k+m}^{k+m} + \sum_{k=1}^{(k-3)/2} [C_{k-2t-3}^{k+m-2t-3} C_{k+m-2t}^{k+m}]$$

3. It implies to $j = m + 1 \Rightarrow n = k + m + 1$

$$m_{C0} - m_{C1}$$

$$= \{C_{2}^{k+m+1} + C_{2}^{m+3} C_{0}^{k+m+1} + \sum_{k=1}^{(k-3)/2} [C_{k-2t-2}^{k+m-2t-1} C_{k+m-2t+2}^{k+m+1}]\}$$

$$-\{(m+2) C_{1}^{k+m+1} + C_{k-3}^{k+m-2} C_{k+m+1}^{k+m+1} + \sum_{k=1}^{(k-3)/2} [C_{k-2t-3}^{k+m-2t-2} \times C_{k+m-2t+1}^{k+m+1}]\}$$

$$= 0.$$

Consequently, for all j, $m_{C0} = m_{C1}$ by the Principle of Mathematical Induction.

CJ Scheme – Proof

Lemma 1: $f_i(A) = f_i(M(n, j)) = C_j - C_j$

Lemma 2: $f_i([A||B]) = f_i(A) + f_i(B)$ for any two totally symmetric matrices A and B.

$\mathcal{I}(C_0, t) = \mathcal{I}(C_1, t)$ for $1 \le t \le k - 1$.

$\mathcal{I}(C_0, t) > \mathcal{I}(C_1, t)$ for $t \ge k$.

- Numerator

$f_t(C_1) = f_t(C_0)$ for $1 \le t \le k - 1$.

$f_t(C_1) > f_t(C_0)$ for $t \ge k$.

Proof by induction on t for $1 \le t \le n$.

1. If $t = 1$:

   Proof by induction on j, where $j = n - k$:

   1. If $j = 0$

      $f_1(C_1) - f_1(C_0) = 0$ is true.

   2. Assume $j = m$, $f_1(C_1) - f_1(C_0) = 0$ is true.
   3. It implies when $j = m + 1$,

      $f_1(C_1) - f_1(C_0) = 0$ is true.

$f_t(C_1) = f_t(C_0)$ for $1 \le t \le k-1$.
$f_t(C_1) > f_t(C_0)$ for $t \ge k$.

$\mathfrak{I}(C_0, t) = \mathfrak{I}(C_1, t)$ for $1 \le t \le k-1$.
$\mathfrak{I}(C_0, t) > \mathfrak{I}(C_1, t)$ for $t \ge k$.

CJ Scheme – Proof

2. Assume for all $j = n - k$, $t = s$ for $s \ge 2$,

$$f_s(C_1) - f_s(C_0) = f_{s,j} = \begin{cases} 0, & \text{if } s < k; \\ 1, & \text{if } s = k; \\ >1, & \text{if } s > k. \end{cases}$$ is true.

3. When consider $t = s + 1$:

   Proof by induction on j, where $j = n - k$.

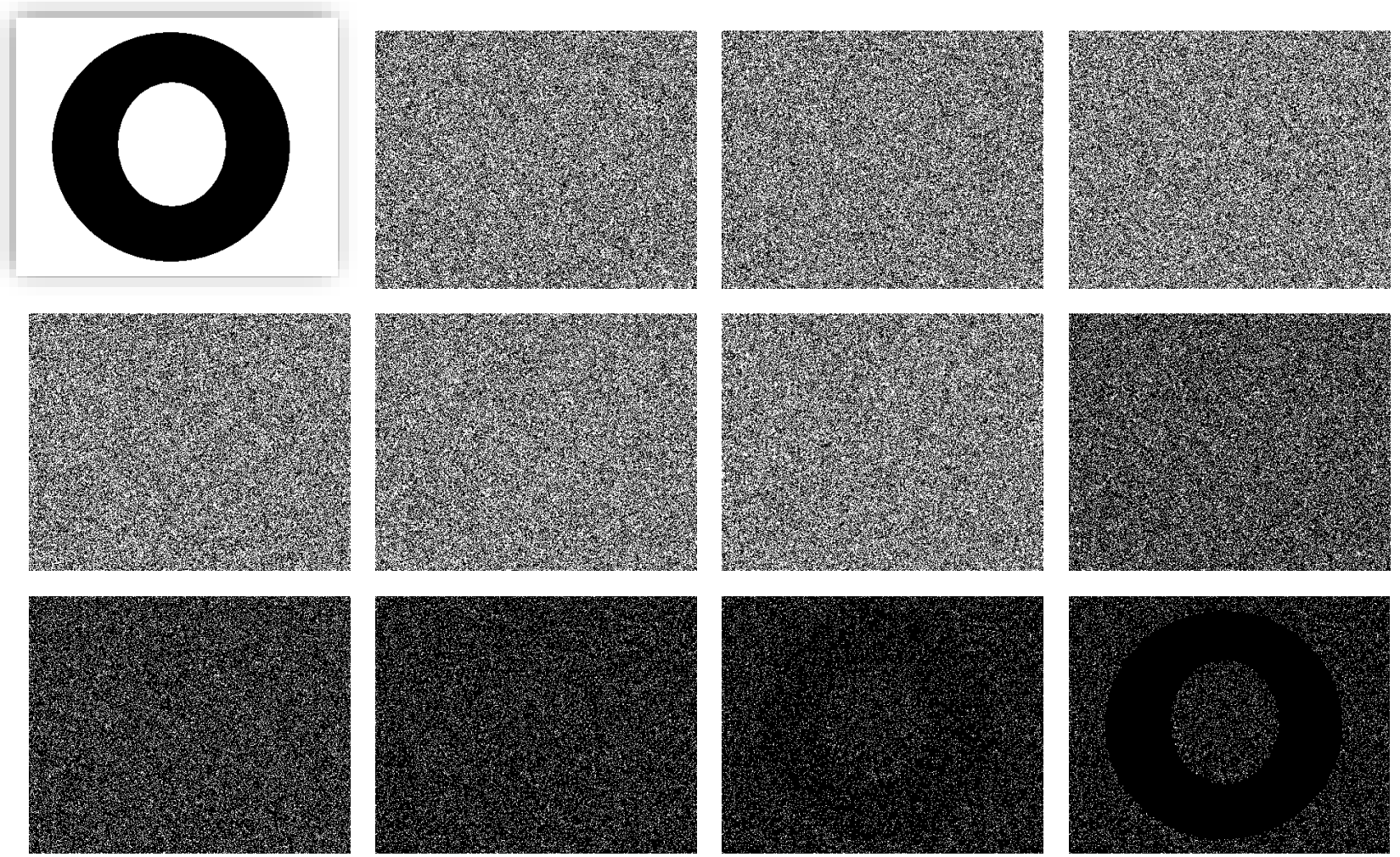
   1. If $j = 0$, $f_{s+1}(C_1) - f_{s+1}(C_0) = f_{s+1,0}$ is true.
   2. Assume $j = m$, $f_{s+1}(C_1) - f_{s+1}(C_0) = f_{s+1,m}$ is true.
   3. Consider $j = m + 1$,

$$f_{s+1}(C_1) - f_{s+1}(C_0) = \begin{cases} 0, & \text{if } s+1 < k; \\ 1, & \text{if } s+1 = k; \\ >1, & \text{if } s+1 > k. \end{cases}$$ is true.

Consequently, for all j and t, $f_t(C_1) - f_t(C_0)$ is true by the Principle of Mathematical Induction.

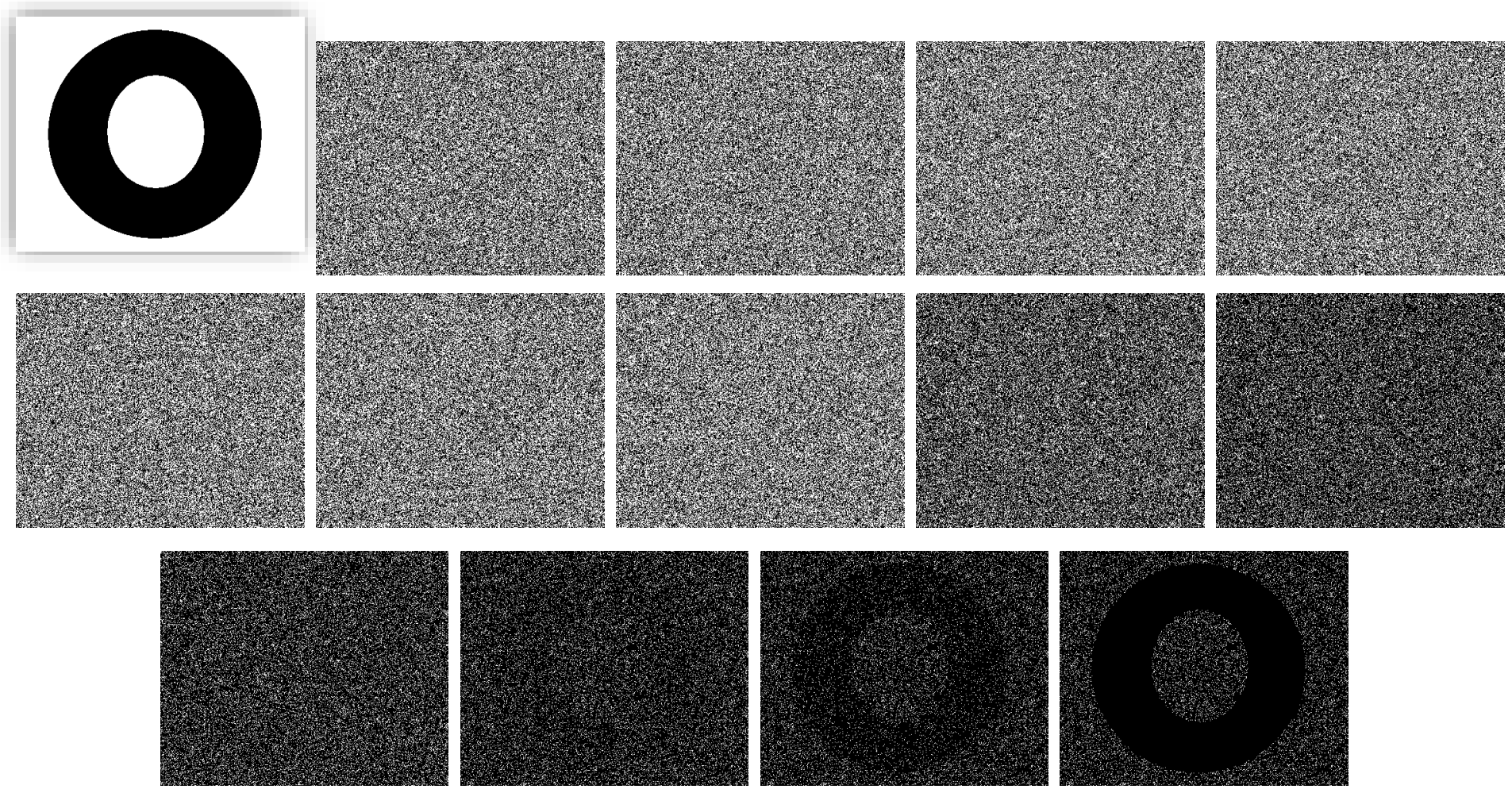
CJ Scheme – Experimental Results

- (5, 6)



CJ Scheme – Experimental Results

- (5,7)



Comparison

The value of α

	NS scheme [1]	FLL scheme [2]	Our scheme
(4, 5)	≅ 1/4261	≅ 1/4261	1/15
(4, 6)	≅ 1/4261	≅ 1/4261	1/24
(4, 7)	≅ 1/4261	≅ 1/4261	1/35
(5, 6)	≅ 1/12820	≅ 1/12820	1/30
(5, 7)	≅ 1/12820	≅ 1/12820	1/48
(6, 8)	≅ 1/152200	≅ 1/152200	1/128
(7, 8)	≅ 1/887707	≅ 1/887707	1/175

Comparison

	NS scheme [1]	FLL scheme [2]	Our scheme
Free size	Yes	No	Yes
Non-expansion	No	Yes	Yes
The value of α	Small	Small	Larger

[1] M. Naor and A. Shamir, “Visual cryptography,” 1995.
[2] W.-P. Fang, S.-J. Lin, and J.-C. Li, “Visual cryptography (VC) with non-expanded shadow images: a Hilbert-curve approach,” 2008.

Conclusion

- There is no expansion in our scheme.
- With larger α, the stacked image in our scheme is clearer.
- This scheme can be applied on any size of the image.

Computer Science and Information Engineering
National Chi Nan University

The Principle and Application of Secret Sharing

Dr. Justie Su-Tzu Juan

Lecture 6. Visual Secret Sharing Scheme

§ 6.3 Better (*k*, *n*)-threshold PVSSS

Slides for a Course Based on

H.-B. Chen, H.-C. Hsu, J.S.-T. Juan, "An Easy-to-implement Construction for (*k*, *n*)-threshold Progressive Visual Secret Sharing Schemes", arXiv:2002.09125, 2020.

§ 6.3 Better (*k*, *n*)-threshold PVSSS

- **Def:** **A (*k*, *n*)-threshold progressive visual secret sharing (PVSS) scheme must satisfy:**
  - 1. For any $1 \le t < k$, $T(S_0, t) = T(S_1, t)$;
  - 2. For any $k \le t \le n$, $T(S_0, t) > T(S_1, t)$;
  - 3. $\alpha(k) < \alpha(k+1) < \ldots < \alpha(n)$.

- **Def:** We call $(a_0, a_1, \ldots, a_n)$ the **coefficient sequence** of the basis matrices, for given $\boldsymbol{a_0 M_0^n - a_1 M_1^n + \ldots + (-1)^j a_j M_j^n + \ldots + (-1)^n a_n M_n^n}$, where $|(-1)^j a_j| M_j^n$ is in C_0 if $(-1)^j a_j \ge 0$, and $|(-1)^j a_j| M_j^n$ is in C_1 if $(-1)^j a_j < 0$.

§ 6.3 Better (*k*, *n*)-threshold PVSSS

- **Def:** We call $(a_0, a_1, \ldots, a_n)$ the **coefficient** sequence of the basis matrices, for given $\boldsymbol{a_0 M_0^n - a_1 M_1^n + \ldots + (-1)^j a_j M_j^n + \ldots + (-1)^n a_n M_n^n}$, where $|(-1)^j a_j| M_j^n$ is in C_0 if $(-1)^j a_j \geq 0$, and $|(-1)^j a_j| M_j^n$ is in C_1 if $(-1)^j a_j < 0$.

- **Ex:**

Reference	Model	Coefficient Sequence
Naor & Shamir [30]	$(2, n)$-threshold	$(n-1, 1, 0, 0, \cdots, 0, (-1)^n)$
Naor & Shamir [30]	$(3, n)$-threshold	$(n-2, 1, 0, 0, \cdots, 0, (-1)^{n-1}, (-1)^{n-1}(n-2))$
Naor & Shamir [30]	(n, n)-threshold	$(1, 1, \cdots, 1)$
Chen & Juan [6]	$(4, n)$-threshold	$(\frac{n^2-5n+6}{2}, n-3, 1, 0, 0, \cdots, 0, (-1)^n, (-1)^n(n-3))$

§ 6.3 Better (*k*, *n*)-threshold PVSSS

- **Def:** We call $(a_0, a_1, \ldots, a_n)$ the **coefficient** sequence of the basis matrices, for given $\boldsymbol{a_0 M_0^n - a_1 M_1^n + \ldots + (-1)^j a_j M_j^n + \ldots + (-1)^n a_n M_n^n}$, where $|(-1)^j a_j| M_j^n$ is in C_0 if $(-1)^j a_j \geq 0$, and $|(-1)^j a_j| M_j^n$ is in C_1 if $(-1)^j a_j < 0$.

- **Ex:**

Reference	Model	Coefficient Sequence
Naor & Shamir [30]	$(2, n)$-threshold	$(n-1, 1, 0, 0, \cdots, 0, (-1)^n)$
Naor & Shamir [30]	$(3, n)$-threshold	$(n-2, 1, 0, 0, \cdots, 0, (-1)^{n-1}, (-1)^{n-1}(n-2))$
Naor & Shamir [30]	(n, n)-threshold	$(1, 1, \cdots, 1)$
Chen & Juan [6]	$(4, n)$-threshold	$(\frac{n^2-5n+6}{2}, n-3, 1, 0, 0, \cdots, 0, (-1)^n, (-1)^n(n-3))$

§ 6.3 Better (*k*, *n*)-threshold PVSSS

- **Def:** Define $C(N, 0) = 1$ for any integer N, and $C(N, M) = N! / [(N - M)!\, M!]$ for any positive integer M. The Pascal's formula can produce the generalized Pascal's triangle:

NS's $(2, n)$

NS's $(3, n)$

CJ's $(4, n)$

$(n-1, n-2) \ldots (-1, n-2)$

$(n-2, n-3) \ldots (-2, n-3)$

$(n-2, n-4) \ldots (-2, n-4)$

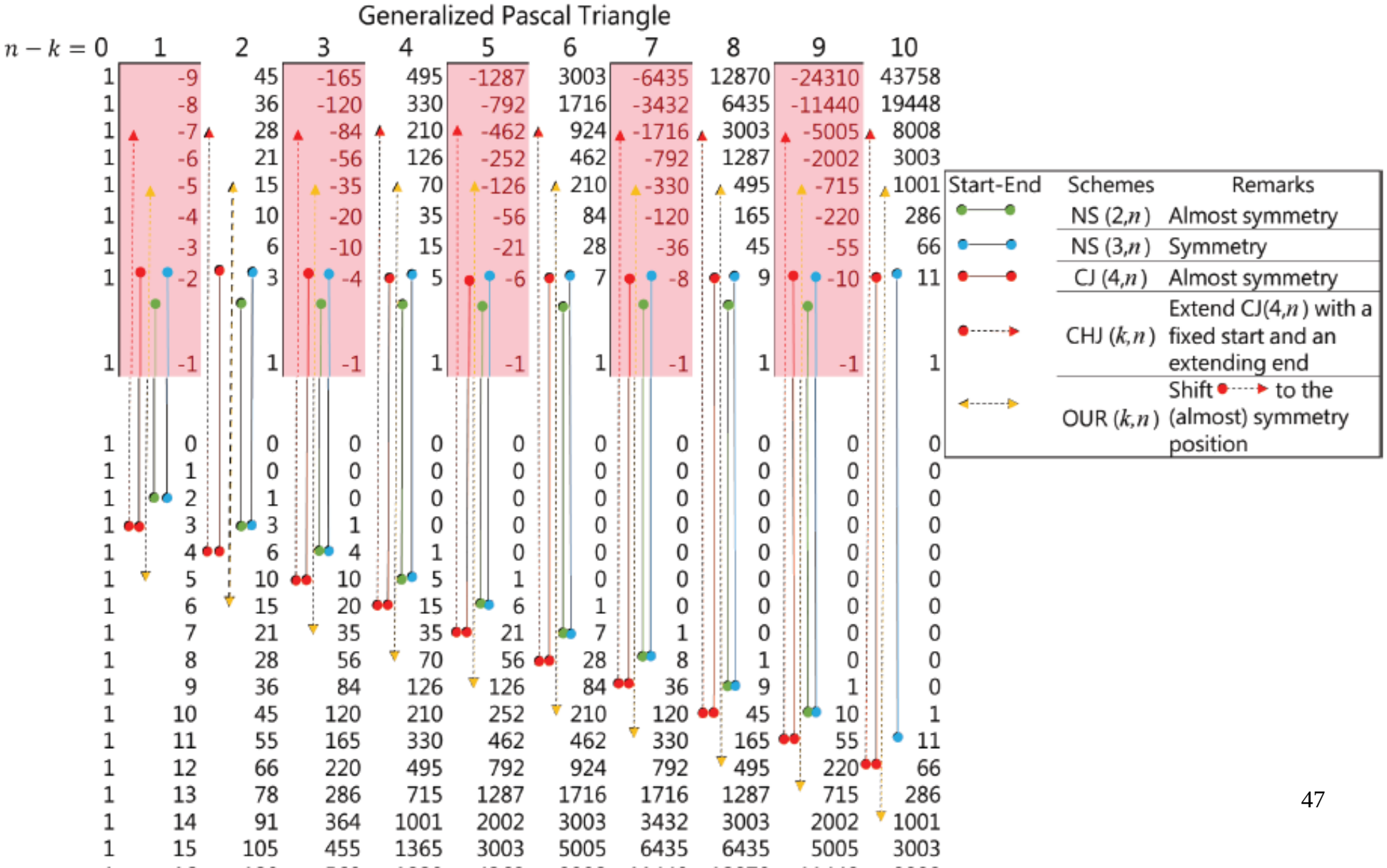
$\mathcal{N} \setminus \mathcal{M}$	0	1	2	3	4	5	6	7	8	9	10
-8	1	-8	36	-120	330	-792	1716	-3432	6435	-11440	19448
-7	1	-7	28	-84	210	-462	924	-1716	3003	-5005	8008
-6	1	-6	21	-56	126	-252	462	-792	1287	-2002	3003
-5	1	-5	15	-35	70	-126	210	-330	495	-715	1001
-4	1	-4	10	-20	35	-56	84	-120	165	-220	286
-3	1	-3	6	-10	15	-21	28	-36	45	-55	66
-2	1	-2	3	-4	5	-6	7	-8	9	-10	11
-1	1	-1	1	-1	1	-1	1	-1	1	-1	1
0	1	0	0	0	0	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0	0	0	0
2	1	2	1	0	0	0	0	0	0	0	0
3	1	3	3	1	0	0	0	0	0	0	0
4	1	4	6	4	1	0	0	0	0	0	0
5	1	5	10	10	5	1	0	0	0	0	0
6	1	6	15	20	15	6	1	0	0	0	0
7	1	7	21	35	35	21	7	1	0	0	0
8	1	8	28	56	70	56	28	8	1	0	0
9	1	9	36	84	126	126	84	36	9	1	0

§ 6.3 Better (*k*, *n*)-threshold PVSSS

- **CHJ's PVSS scheme:**
- **Construction 1:** Given any positive integer k and n with $2 \le k \le n$, let C_0 and C_1 be the basis matrices whose coefficient sequence starts **from $(n - \lceil k/2 \rceil, n - k)$ entry and up to the $(-\lceil k/2 \rceil, n - k)$ entry** in the generalized Pascal's triangle.

- **Thm:** Given any positive integer k and n with $2 \le k \le n$, the basis matrices C_0 and C_1 in Construction 1 are valid for a (k, n)-threshold PVSS schemes.

§ 6.3 Better (*k*, *n*)-threshold PVSSS



§ 6.3 Better (k, n)-threshold PVSSS

- **Comparisons**

	[38]	[7]	[36]	[16]	[37]	[5]	OURS
(2, 2)-threshold, $q = 2$	0.4999	0.4987	**0.5007**	0.4999	0.4978	0.5000	0.5000
(2, 3)-threshold, $q = 2$	0.2502	0.1415	0.2840	0.1444	**0.2849**	0.1250	0.2500
(2, 3)-threshold, $q = 3$	**0.6670**	0.2485	0.4990	0.2526	0.4992	0.5000	0.6667
(2, 4)-threshold, $q = 2$	0.1663	0.0697	0.1991	0.1427	**0.2872**	0.0555	0.1667
(2, 4)-threshold, $q = 3$	0.3995	0.1181	0.3325	0.2499	**0.5018**	0.2000	0.4000
(2, 4)-threshold, $q = 4$	0.7495	0.1252	0.4993	0.2499	0.5018	0.5000	**0.7500**
(3, 3)-threshold, $q = 3$	0.2496	0.2500	0.2496	**0.2503**	0.2497	0.2500	0.2500
(3, 4)-threshold, $q = 3$	0.1029	0.0571	0.1117	0.0581	0.1134	0.0909	**0.1429**
(3, 4)-threshold, $q = 4$	0.3327	0.1250	0.2509	0.1263	0.2531	**0.3333**	**0.3333**
(4, 4)-threshold, $q = 4$	0.1252	**0.1250**	0.1246	0.1247	0.1245	**0.1250**	**0.1250**
(3, 5)-threshold, $q = 3$	0.0557	0.0224	0.0626	0.0224	0.0854	0.0454	**0.1000**
(3, 5)-threshold, $q = 4$	0.1704	0.0481	0.1368	0.0480	0.1889	0.1578	**0.2222**
(3, 5)-threshold, $q = 5$	**0.3752**	0.0625	0.2506	0.0622	0.2485	0.3750	0.3750
(4, 5)-threshold, $q = 4$	0.0450	0.0238	0.0480	0.0235	0.0469	**0.0588**	**0.0588**
(4, 5)-threshold, $q = 5$	0.1669	0.0625	0.1267	0.0616	0.1254	**0.2000**	**0.2000**
(4, 6)-threshold, $q = 4$	N/A	0.0078	N/A	0.0078	0.0319	**0.0333**	**0.0333**
(4, 6)-threshold, $q = 5$	N/A	0.0204	N/A	0.0204	N/A	**0.1154**	**0.1154**
(4, 6)-threshold, $q = 6$	N/A	0.0313	N/A	0.0313	N/A	**0.2500**	**0.2500**
(5, 6)-threshold, $q = 5$	N/A	0.0101	0.0204	0.0101	0.0204	**0.0313**	**0.0313**
(5, 6)-threshold, $q = 6$	N/A	0.0313	N/A	0.0313	N/A	**0.1000**	**0.1000**

§ 6.3 Better (*k*, *n*)-threshold PVSSS

- **Programming Homework #3**: (5/16) Implement **CHJ's PVSS** scheme.
- 1. Try (*k*, *n*) = (4, 5), (4, 6), (4, 7), (5, 6), (5, 7).
- 2. Shows the **O**riginal secret image, the **S**hares, the **R**econstructed images for stacking any 2 ~ *n* shares.
- 3. Calculate the contrast (and average contrast) of your experimental results (the **R**econstructed images for stacking any 2 ~ *n* shares).