Computer Science and Information Engineering
National Chi Nan University

The Principle and Application of Secret Sharing

Dr. Justie Su-Tzu Juan

Lecture 7. Visual Cryptography with Various Functions

§ 7.1 RG-based Multi-VSS Scheme

Slides for a Course Based on

Joy Jo-Yi Chang and Justie Su-Tzu Juan*, "Multi-VSS Scheme by Shifting Random Grids," *Proc. of World Academy of Science, Engineering and Technology*, Vol. 65, Tokyo, Japan, May 29-30, 2012. pp. 1277-1283.

§ 7.1 RG-based Multi-VSS Scheme

- **Random Grid (RG) based VSS**
  - O. Kafri, and E. Keren, "Encryption of pictures and shapes by random grids," *Optics Letters*, vol. 12, no. 6, 1987, pp. 377-379.
  - Three encryption algorithms for black and white images:

```
Generate a random grid: share1
For any pixel in secret image
if (image.pixel = 1)
   share2.pixel = 1 – share1.pixel
else
   share2.pixel = share1.pixel
```

KK1

```
Generate a random grid: share1
For any pixel in secret image
if (image.pixel = 1)
   share2.pixel = random (0, 1)
else
   share2.pixel = share1.pixel
```

KK2

```
Generate a random grid: share1
For any pixel in secret image
if (image.pixel = 1)
   share2.pixel = 1 – share1.pixel
else
   share2.pixel = random (0, 1)
```

KK3

§ 7.1 RG-based Multi-VSS Scheme

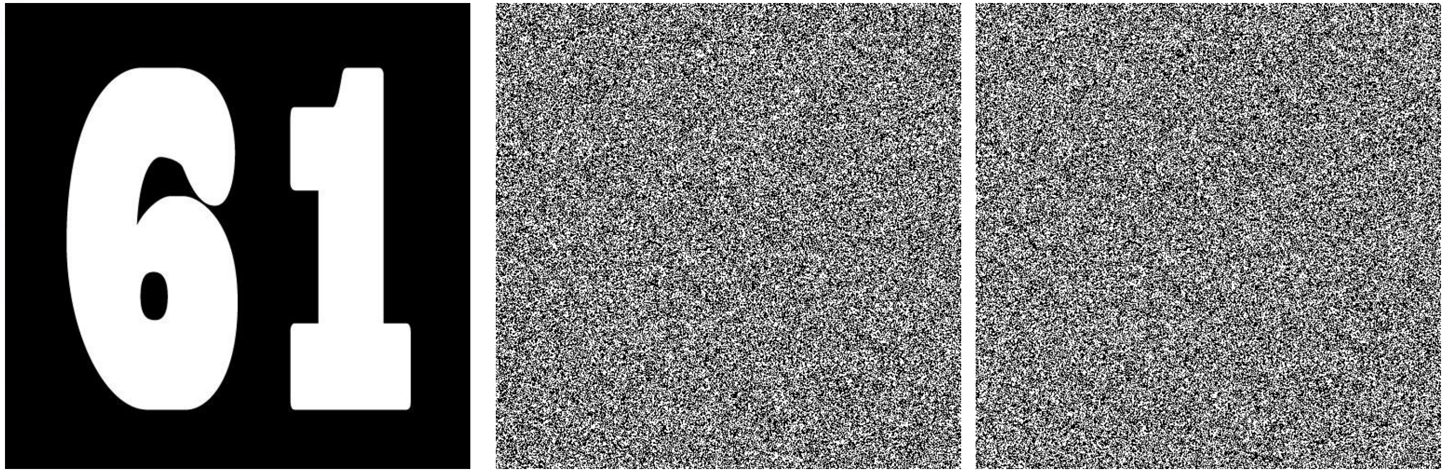
- **<u>Def</u>: Random Grid (RG) based VSS**
  - Three encryption algorithms for black and white images.
  - KK1:

S	Probability	G_1	G_2	$G_1 \oplus G_2$	$T(G_1 \otimes G_2)$
□	1/2	□	□	□	½
	1/2	■	■	■	
■	1/2	□	■	■	0
	1/2	■	□	■	

S: secret; G_1: share 1; G_2: share 2; $\otimes$: or; $T(G_1 \otimes G_2)$: Transmittance

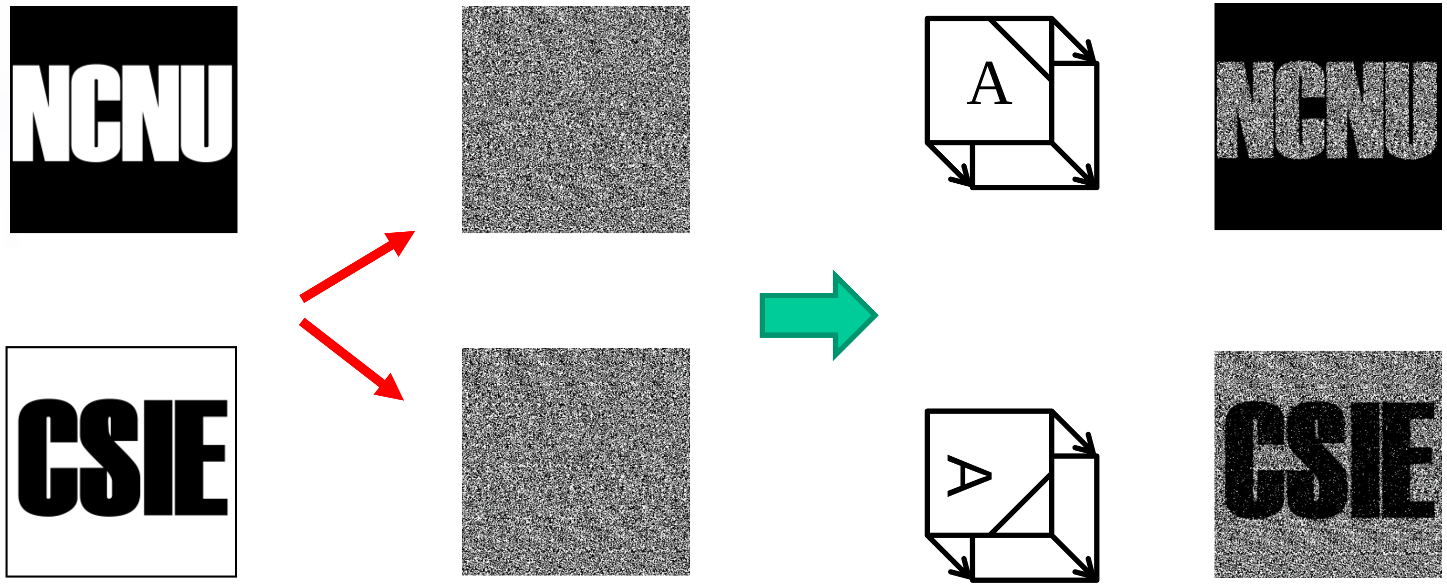
§ 7.1 RG-based Multi-VSS Scheme

- **<u>Def</u>: Random Grid (RG) based VSS**
  - Three encryption algorithms for black and white images.
  - KK1:



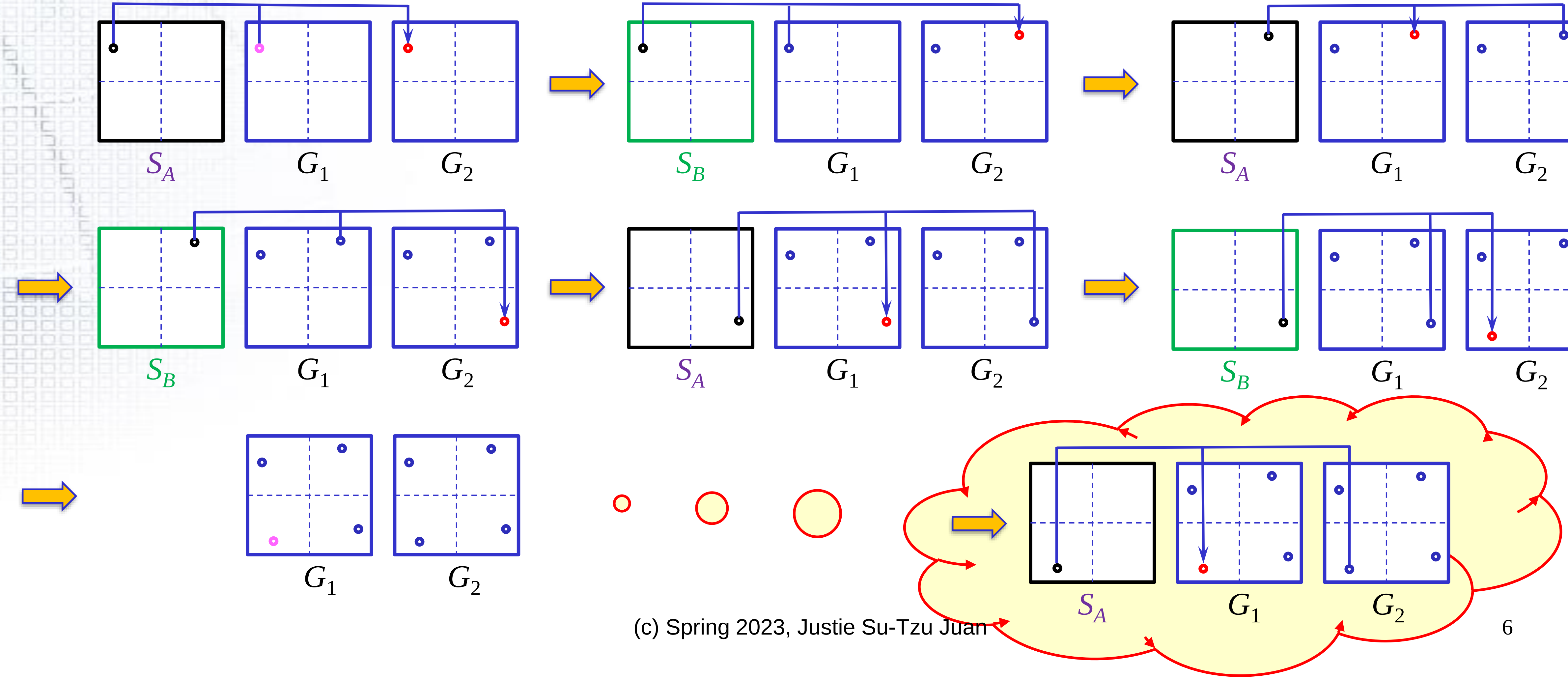
§ 7.1 RG-based Multi-VSS Scheme

- **RG-based Multi-VSS Scheme by Rotating**
  – T.-H. Chen, K.-H. Tsao, and K.-C. Wei, “Multiple-image encryption by rotating random grids,” in Proceedings of ISDA, vol. 3, 2008, pp. 252-256.



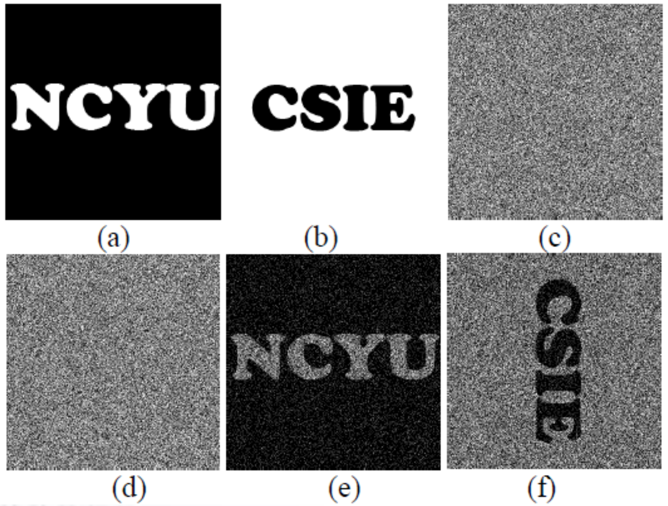
§ 7.1 RG-based Multi-VSS Scheme

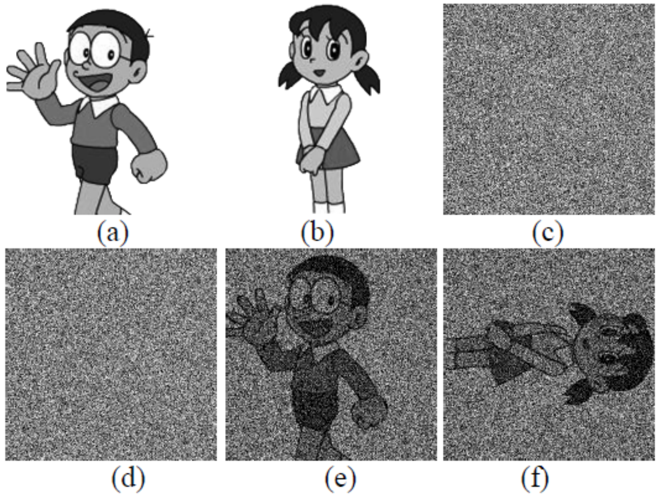
- **RG-based Multi-VSS Scheme by Rotating**

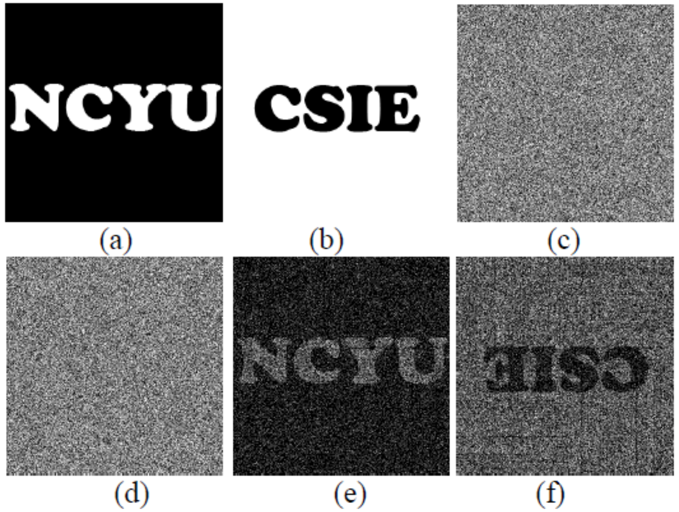


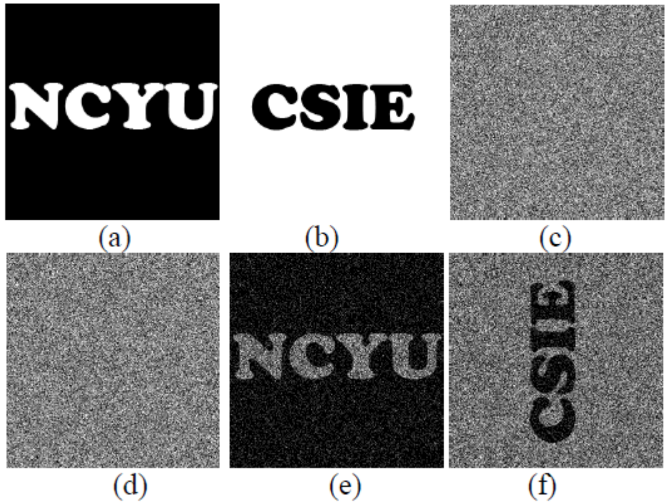
§ 7.1 RG-based Multi-VSS Scheme

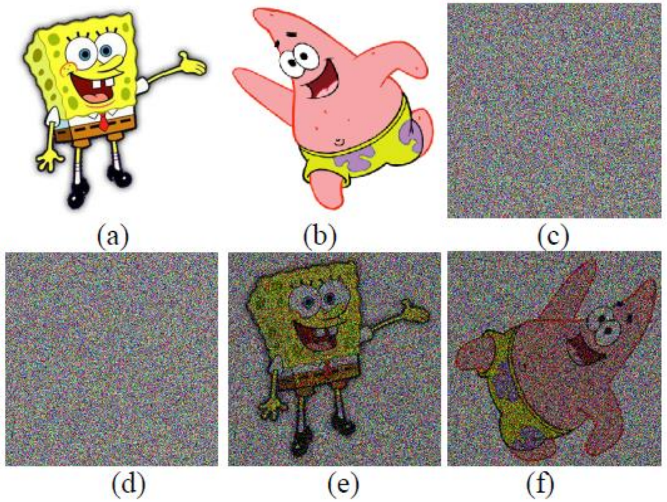
- **RG-based Multi-VSS Scheme by Rotating (512 × 512)**











§ 7.1 RG-based Multi-VSS Scheme

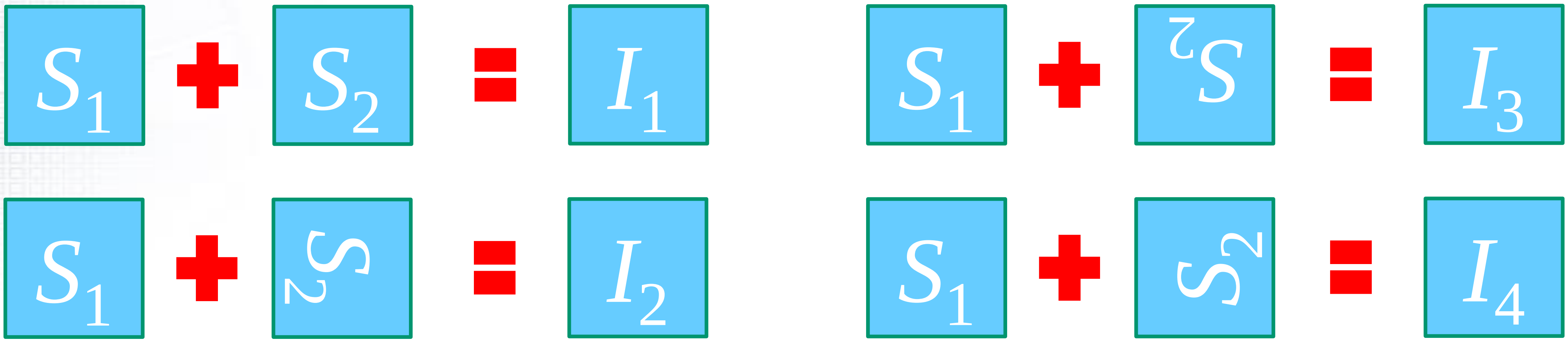
- **The drawbacks of RG-based Multi-VSS Scheme by Rotating**
  - Secret image must be square.
  - Distortion = 1 / 4 is large.

- **Def. The Quantity of *Distortion* of Algorithm *A*, *D(A)*:**

$$D(A) = \frac{\text{pixels not be encrypted in } A}{\text{all pixels of secret images in } A}$$

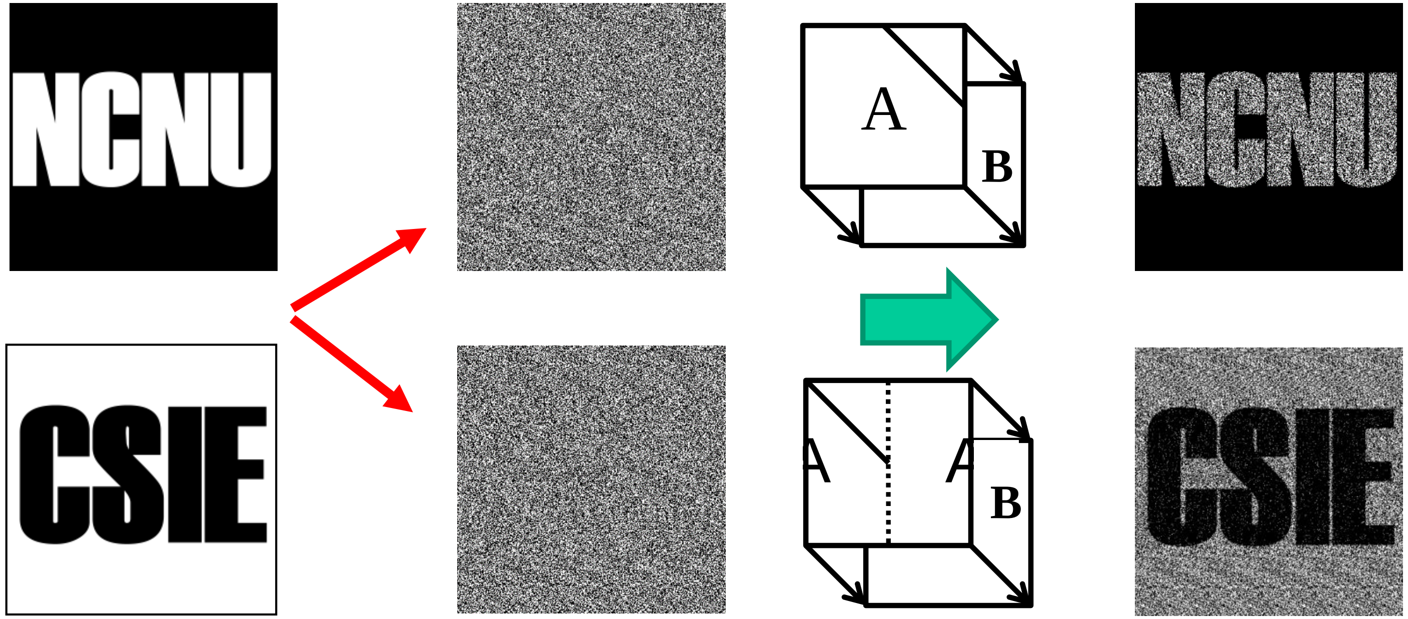
§ 7.1 RG-based Multi-VSS Scheme

- **RG-based Multi-VSS Scheme by Rotating**
  - T. H. Chen and K. H. Tsao, (2011) "Yet another multiple-image encryption by rotating random grids," *Journal of Signal Processing*, Vol.92, pp. 2229-2237, 2012.



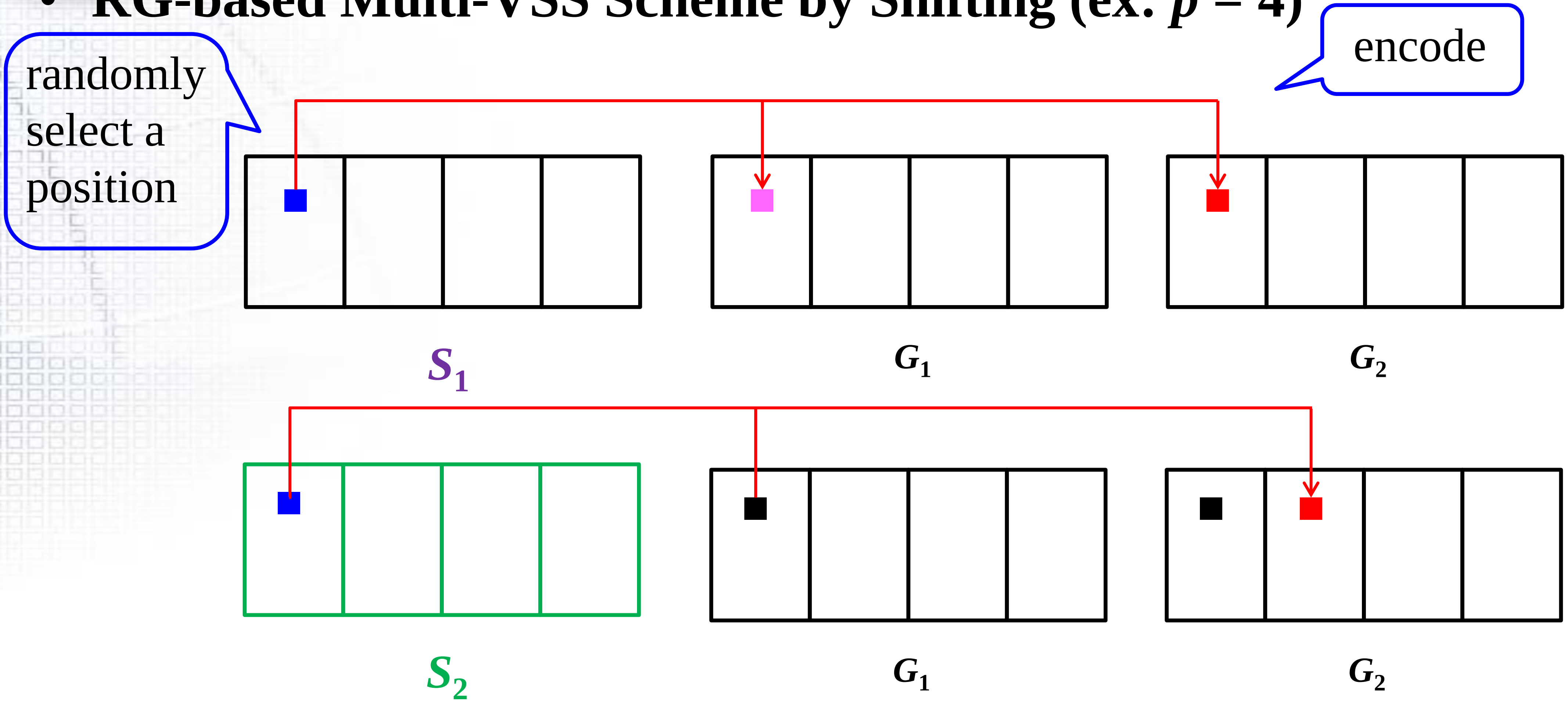
§ 7.1 RG-based Multi-VSS Scheme

- **RG-based Multi-VSS Scheme by Shifting**
  - Joy Jo-Yi Chang and Justie Su-Tzu Juan*, "Multi-VSS Scheme by Shifting Random Grids," Proc. of *WASET*, Vol. 65, Tokyo, 2012. pp. 1277-1283.



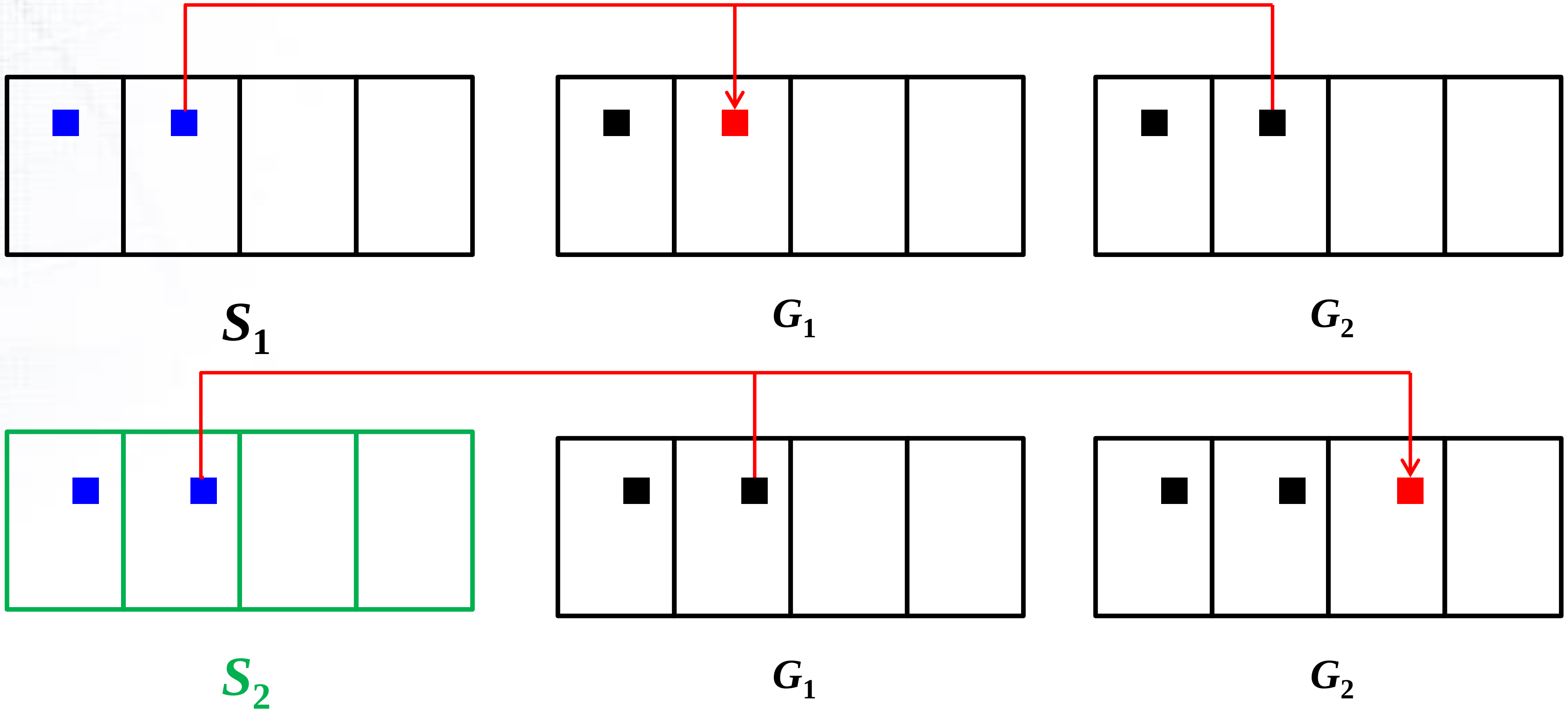
§ 7.1 RG-based Multi-VSS Scheme

- **RG-based Multi-VSS Scheme by Shifting (ex: p = 4)**



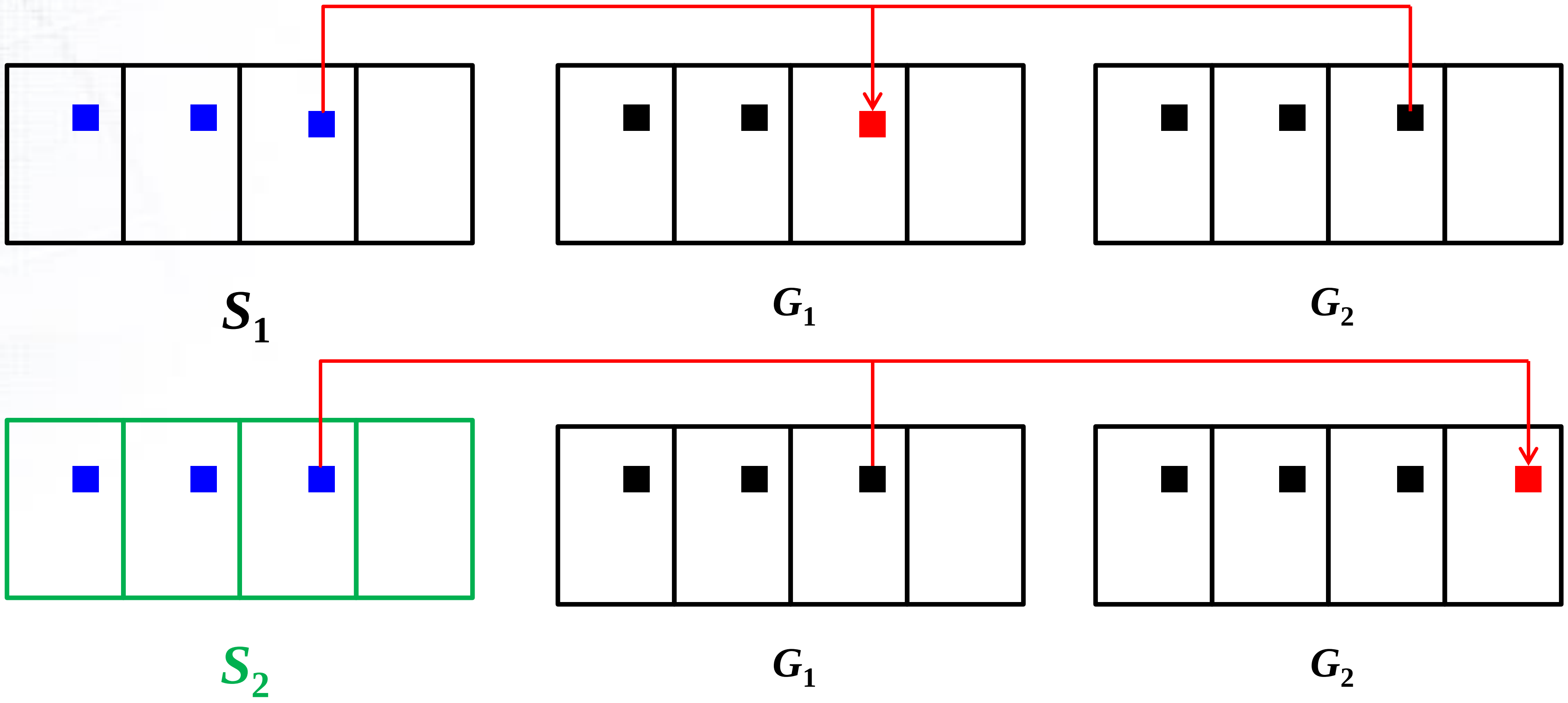
§ 7.1 RG-based Multi-VSS Scheme

- **RG-based Multi-VSS Scheme by Shifting (ex: *p* = 4)**



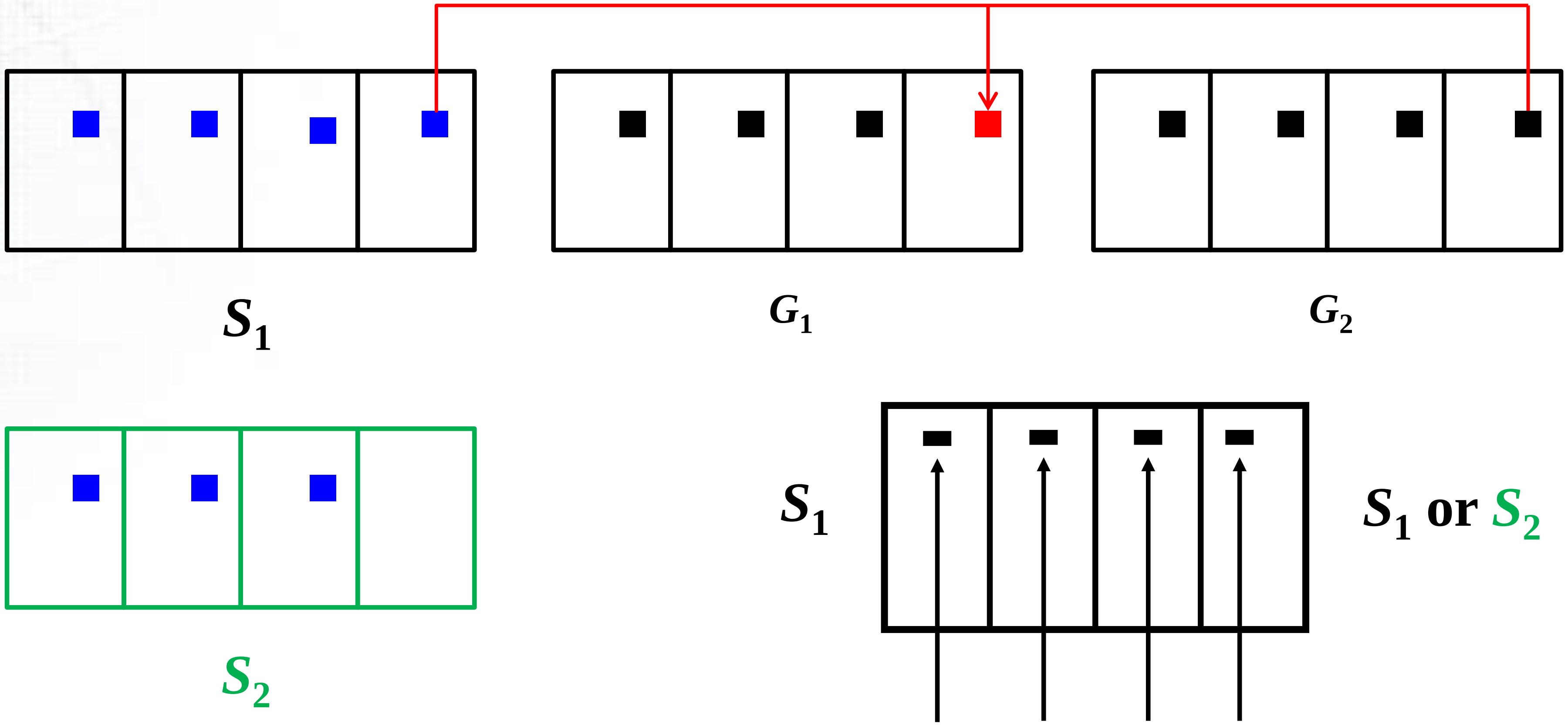
§ 7.1 RG-based Multi-VSS Scheme

- **RG-based Multi-VSS Scheme by Shifting (ex: p = 4)**



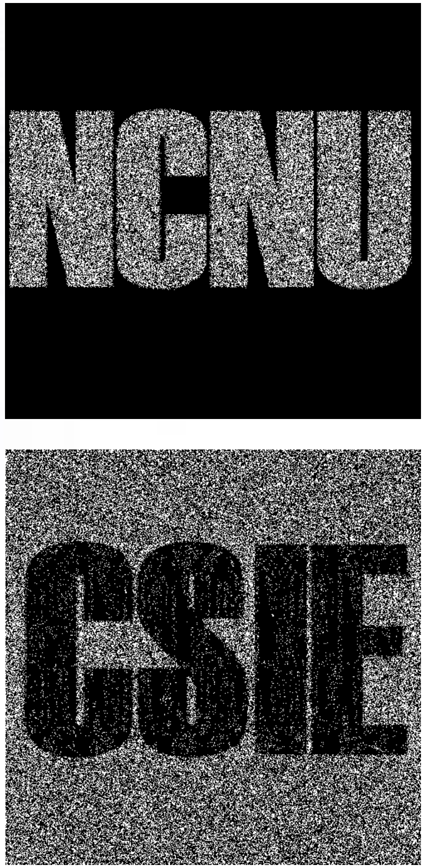
§ 7.1 RG-based Multi-VSS Scheme

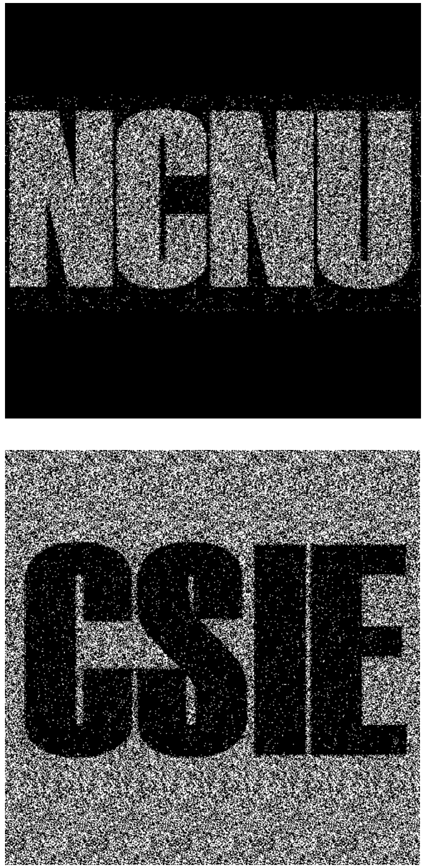
- RG-based Multi-VSS Scheme by Shifting (ex: p = 4)



§ 7.1 RG-based Multi-VSS Scheme

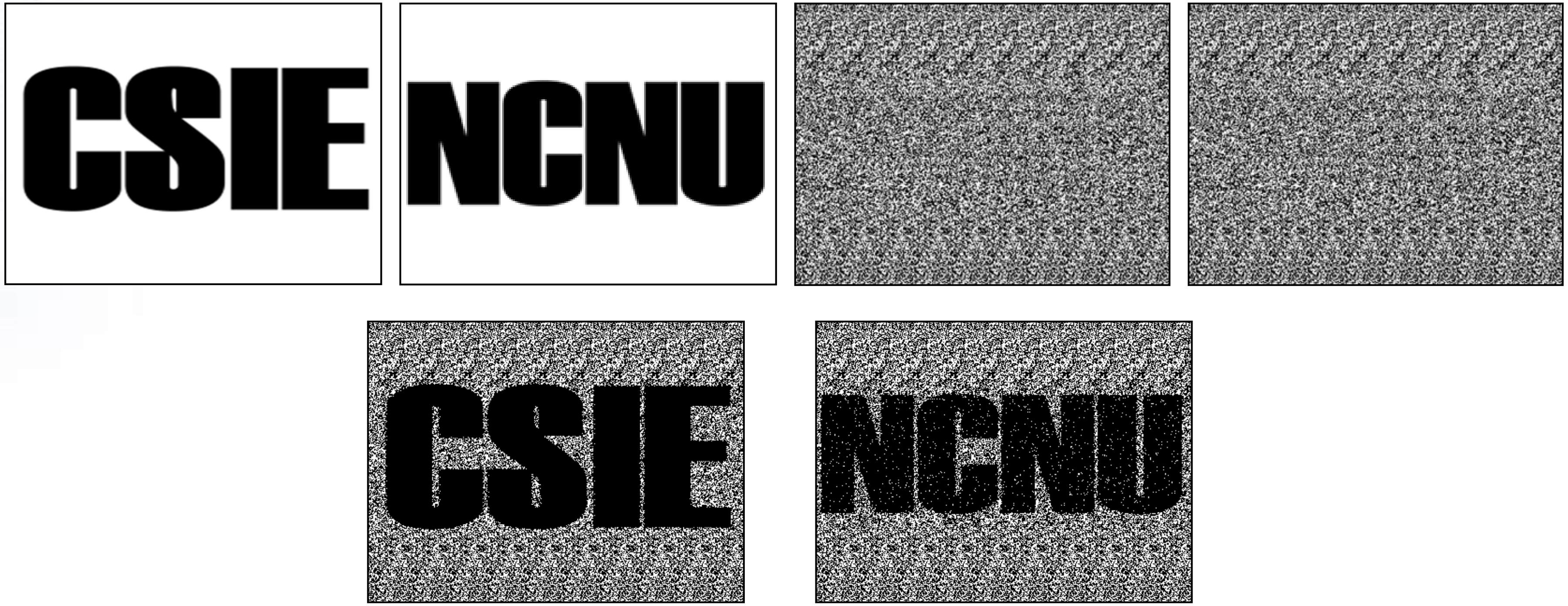
- **RG-based Multi-VSS Scheme by Shifting**





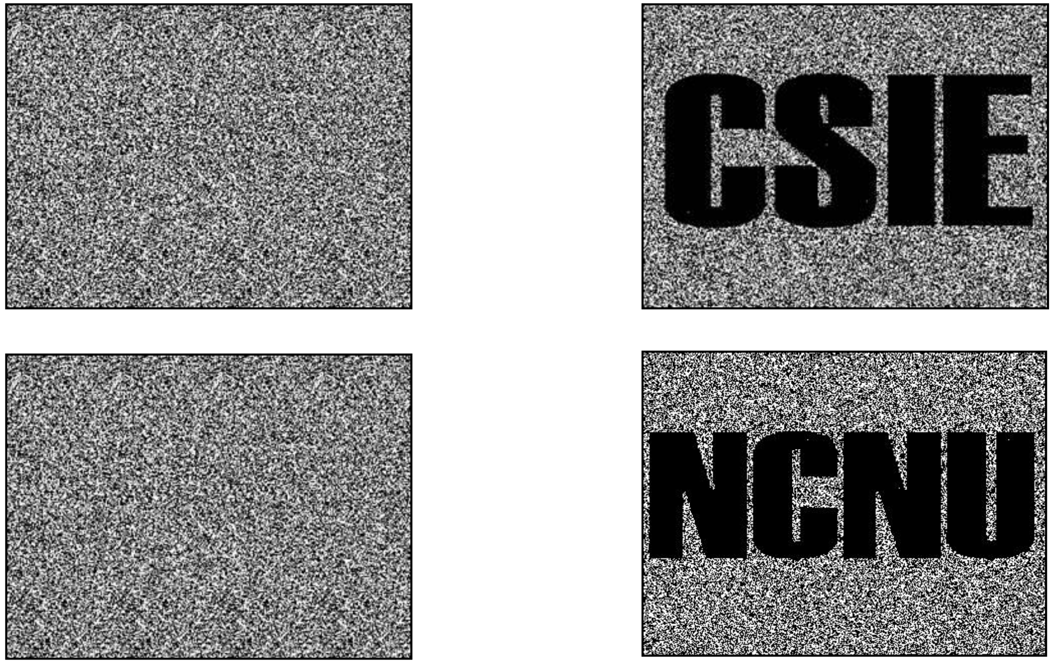
§ 7.1 RG-based Multi-VSS Scheme

- **RG-based Multi-VSS Scheme by Shifting**
  - Experimental result - Algorithm 1: Two secret images S_A and S_B with the size of 400×300, $p = 10$.



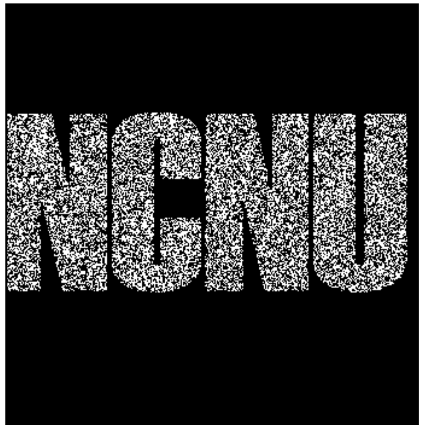
§ 7.1 RG-based Multi-VSS Scheme

- **RG-based Multi-VSS Scheme by Shifting**
  - Experimental result - Algorithm 2: Two secret images S_A and S_B with the size of 400×300, p = 50.



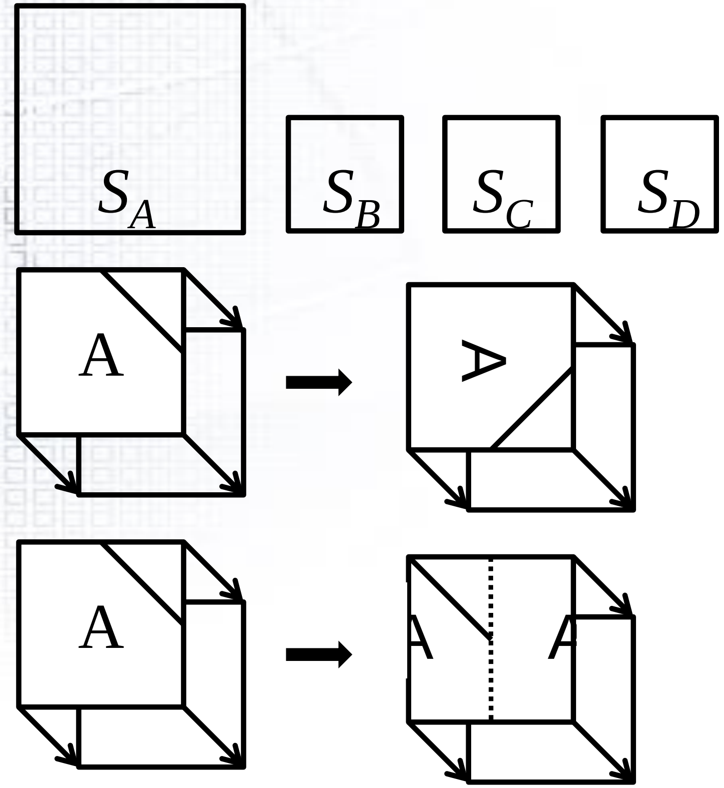
§ 7.1 RG-based Multi-VSS Scheme

- **RG-based Multi-VSS Scheme by Shifting**
  - Experimental result - Algorithm 3: Two secret images S_A and S_B with the size of 500×500, p = 50.



§ 7.1 RG-based Multi-VSS Scheme

- **Comparison**

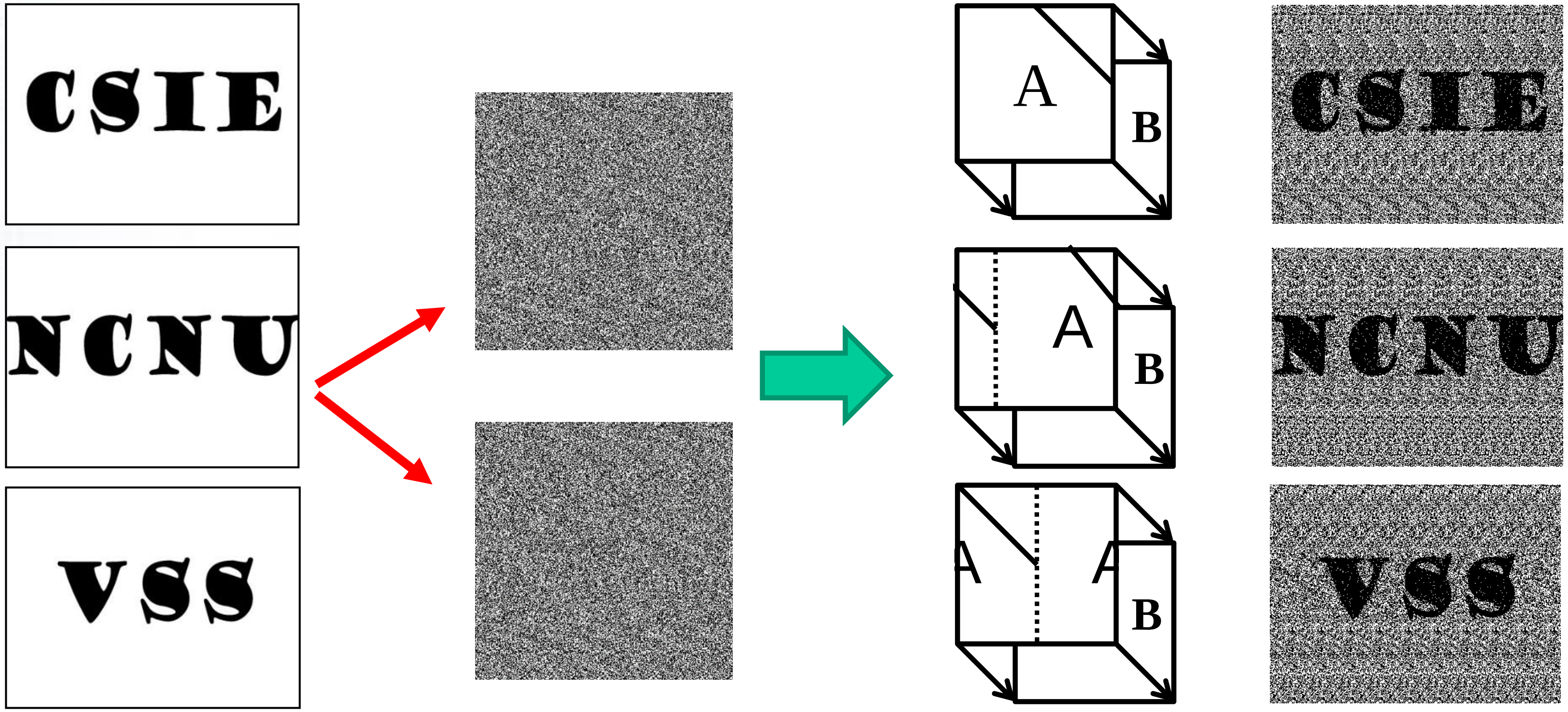


	Chen et .al [ISC 2008]	Chen et .al [ISDA 2008]	Alg. 1, 2	Alg. 3
Data Quantity	1.75	2	2	$(2 - 1/p)$
Distortion	0	1/4	$1/2p$	0
Any Rectangle	Yes	No	Yes	Yes

- T.-H. Chen, G.-Z. Wei, and K.-X. Taso, "An multi-secret image scheme by using random grids," *in Proceedings of 18th Information Security Conference*, Hualien, May 29-30, 2008.
- T.-H. Chen, K.-H. Tsao, and K.-C. Wei, "Multiple-image encryption by rotating random grids," *in Proceedings of The 8th International Conference on Intelligent System Design and Applications (ISDA 2008)*, vol. 3, 2008, pp. 252-256.

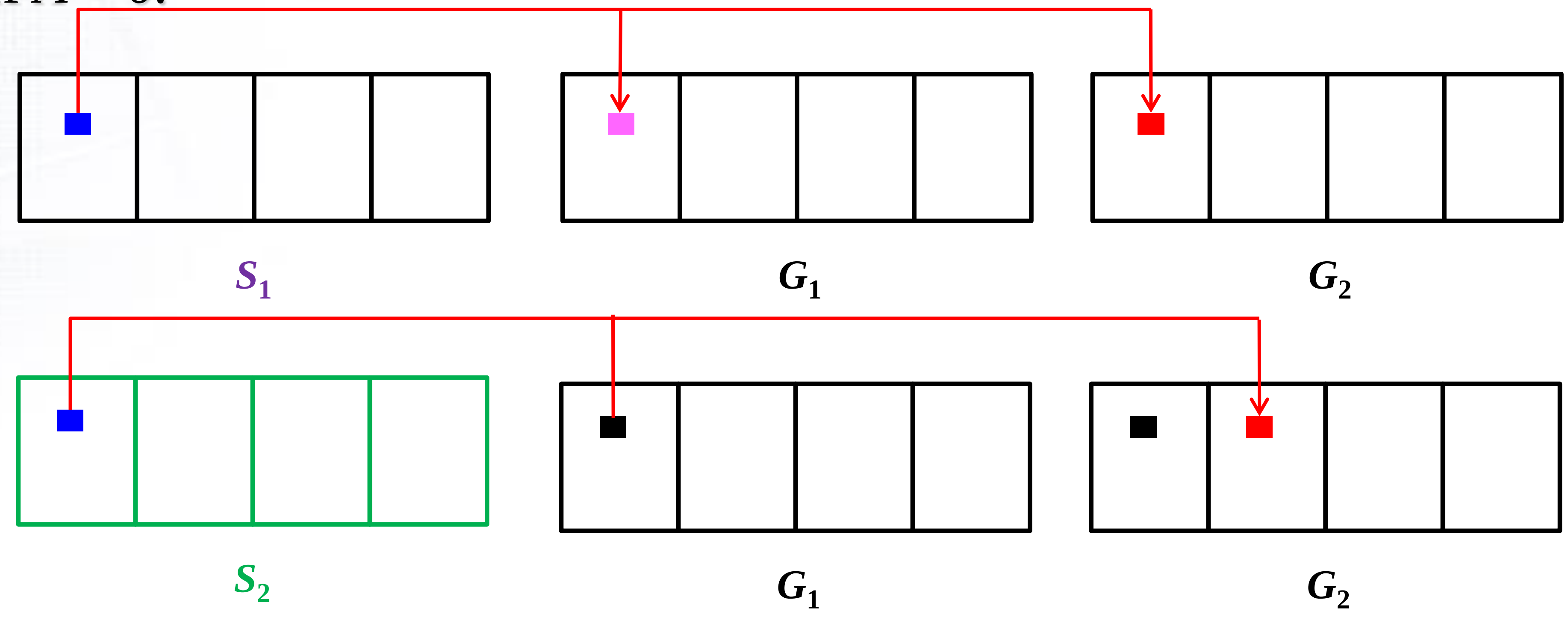
§ 7.1 RG-based Multi-VSS Scheme

- **RG-based Multi-VSS Scheme by Shifting**
  – Joy Jo-Yi Chang, Bo-Yuan Huang and Justie Su-Tzu Juan*, "A New Visual Multi-Secrets Sharing Scheme by Random Grids," *Cryptography*, Vol. 2, Iss. 3, 2018, 24.



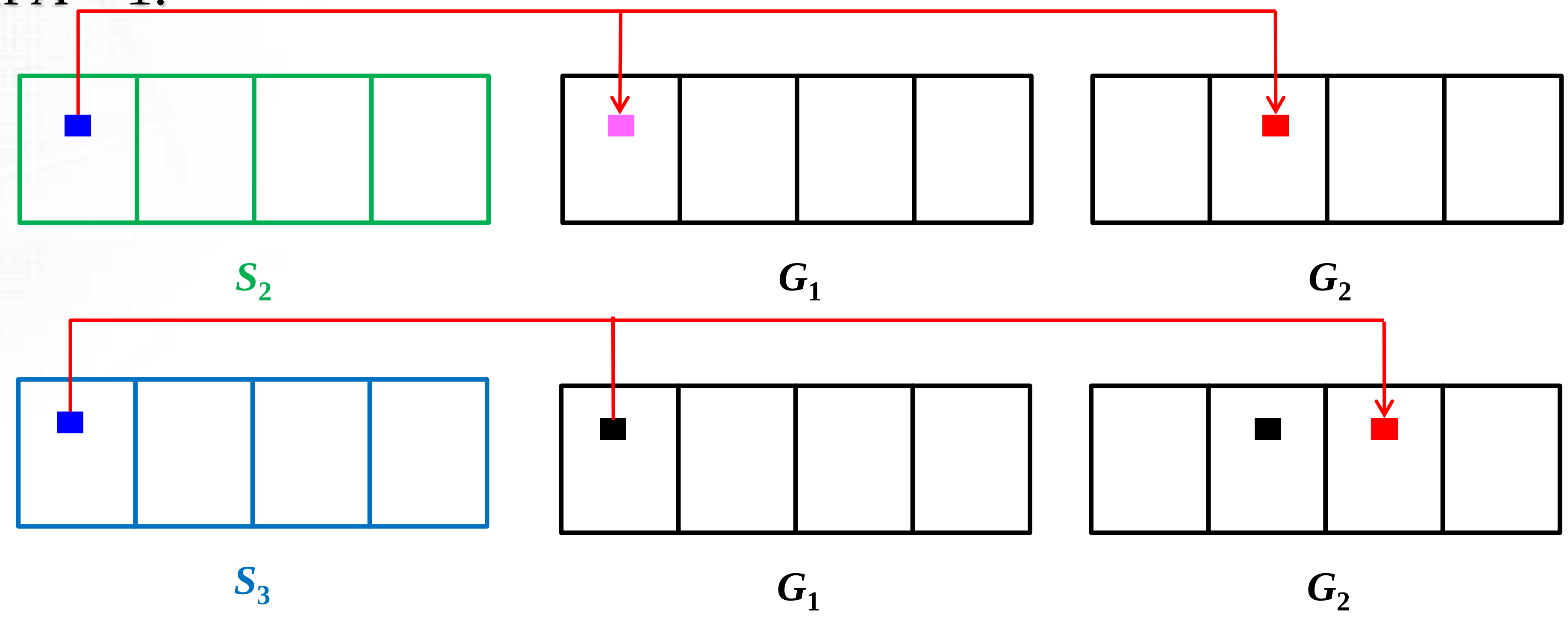
§ 7.1 RG-based Multi-VSS Scheme

- **RG-based Multi-VSS Scheme by Shifting**
  - **Ex**: n = 3, randomly select A = 0, 1, or 2. (for encrypting (S_0, S_1), (S_1, S_2), or (S_2, S_0))
    - If A = 0:



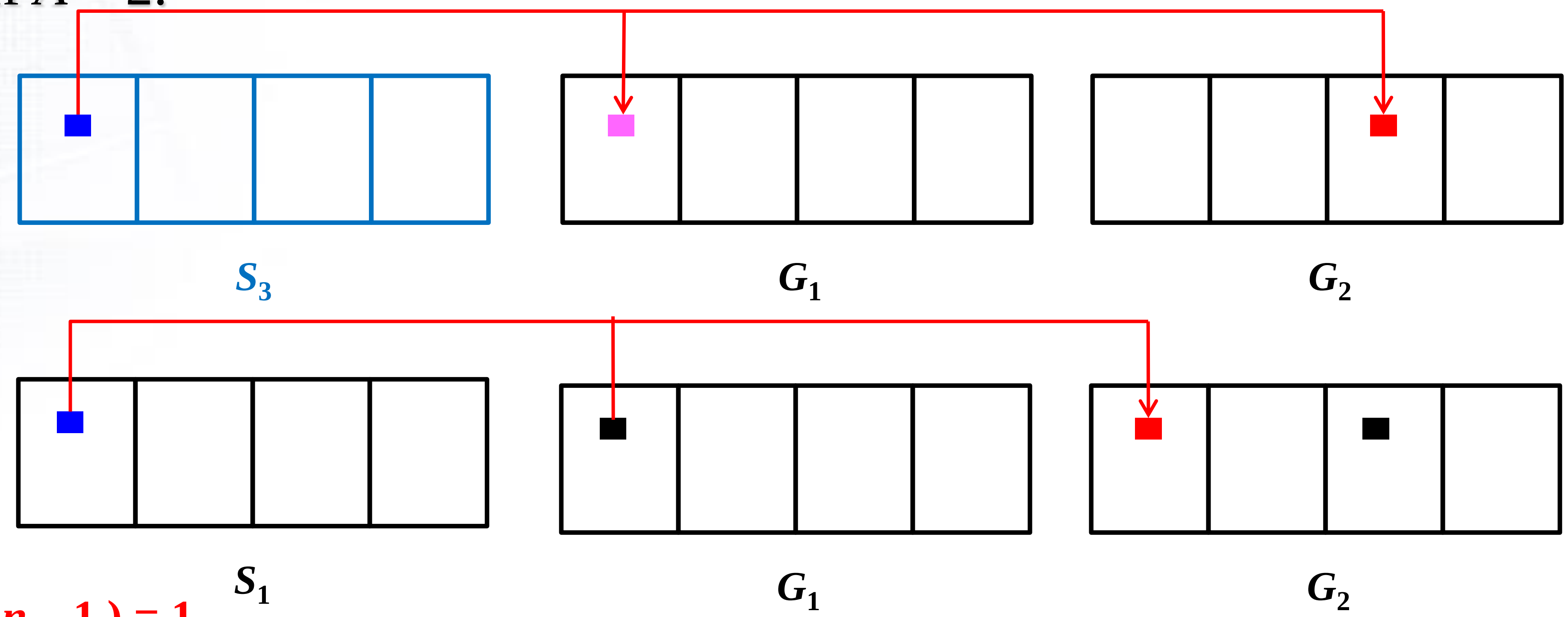
§ 7.1 RG-based Multi-VSS Scheme

- **RG-based Multi-VSS Scheme by Shifting**
  - <u>**Ex**</u>: n = 3, randomly select A = 0, 1, or 2. (for encrypting (S_0, S_1), (S_1, S_2), or (S_2, S_0))
    - If A = 1:



§ 7.1 RG-based Multi-VSS Scheme

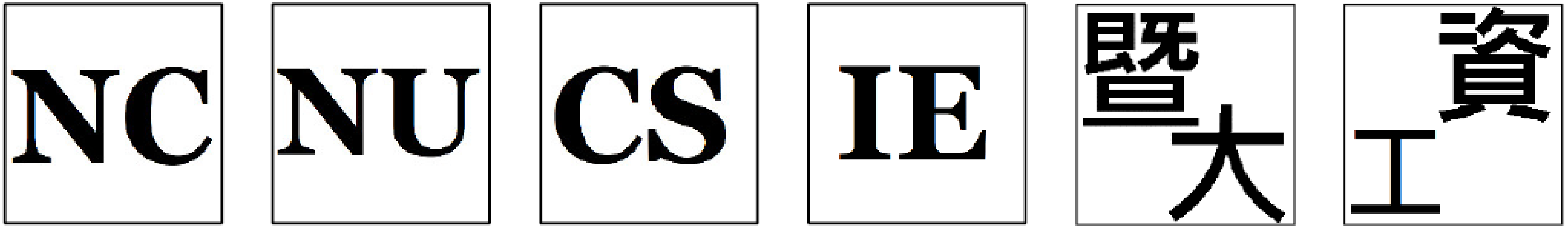
- **RG-based Multi-VSS Scheme by Shifting**
  - **Ex**: n = 3, randomly select A = 0, 1, or 2. (for encrypting (S_0, S_1), (S_1, S_2), or (S_2, S_0))
    - If A = 2:



- **GCD(p, n – 1) = 1**

§ 7.1 RG-based Multi-VSS Scheme

- **RG-based Multi-VSS Scheme by Shifting**



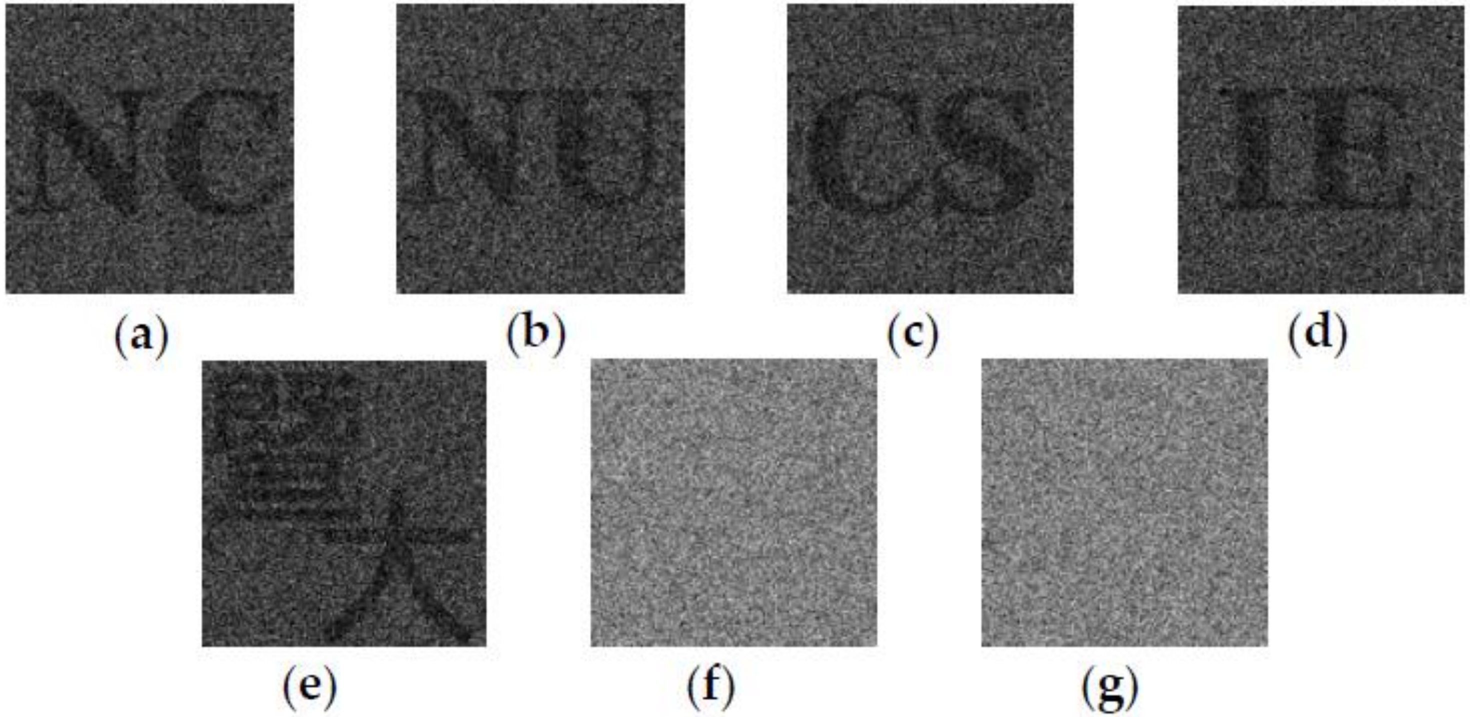
(a) (b) (c) (d) (e) (f)

  - Experimental result 1: n = 4 secret images with the size of 540 × 540, p = 10.

(a) (b) (c) (d) (e) (f)

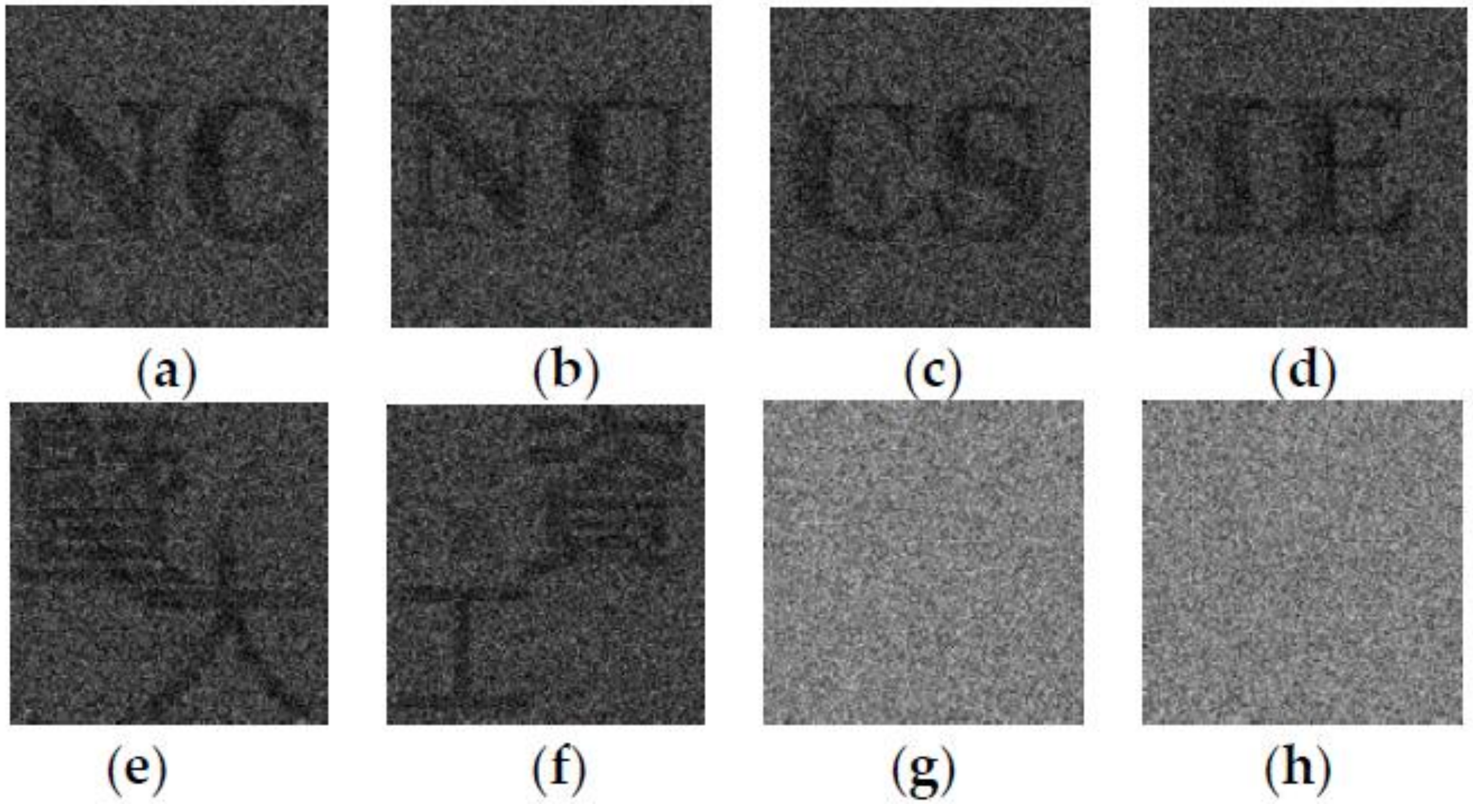
§ 7.1 RG-based Multi-VSS Scheme

- **RG-based Multi-VSS Scheme by Shifting**
  - Experimental result 2: n = 5 secret images with the size of 540 $\times$ 540, p = 9.



§ 7.1 RG-based Multi-VSS Scheme

- **RG-based Multi-VSS Scheme by Shifting**
  - Experimental result 3: n = 6 secret images with the size of 540 $\times$ 540, p = 27.



§ 7.1 RG-based Multi-VSS Scheme

- **Comparison**

Scheme	Number of Secret Images	Number of Shares	Quality Adjustable	Any Rectangle Secret Images	Direct Recovery Operation
The proposed scheme	$s \geq 2$	2	Yes	Yes	Yes
Reddy et al., 2016 [12]	$s \geq 2$	$3s$	No	Yes	No
Tsao et al., 2015 [11]	$2^n - n - 1 \geq s \geq 1$	n	No	Yes	Yes
Salehi et al., 2014 [10]	$s \geq 2$	n	No	Yes	Yes/No
Chang et al., 2012 [9]	3	2	Yes	Yes	Yes
Chen et al., 2012 [8]	4	2	No	No	Yes
Chang et al., 2010 [7]	2	2	Yes	Yes	Yes
Chen et al., 2008 [6]	2	2	No	No	Yes

  – Distortion = $((N - 2)p + 1) / Np$

- **Analysis**

$$\sigma = \frac{T(R[S_{i,0}]) - T(R[S_{i,1}])}{1 + T(R[S_{i,1}])} = \frac{4p - 2}{4Np + Np - 2p + 1} = \frac{2(2p-1)}{5Np - 2p + 1} = \frac{2(2p-1)}{(5N-2)p + 1}$$

Computer Science and Information Engineering
National Chi Nan University

The Principle and Application of Secret Sharing

Dr. Justie Su-Tzu Juan

Lecture 7. Visual Cryptography with Various Functions

§ 7.2 Fault-Tolerant VSS Scheme

Slides for a Course Based on

Justie Su-Tzu Juan* and Yung-Chang Chen, "Extended Fault-Tolerant Visual Secret Sharing Scheme without Pixel Expansion," *Proc. of Int. Conf. on Security and Management* (SAM'18), Luxor, Las Vegas, Nevada, USA, 2018, pp. 61-67.

Outline

- **INTRODUCTION**
- **RELATED WORKS**
  - *Random Grid Encryption Algorithm*
  - *The MTVSS Scheme*
  - *The FTVSS Scheme*
- **THE PROPOSED SCHEME**
  - *The Main Idea and Algorithm*
  - *The Experimental Results*
- **ANALYSIS AND COMPARISON**
- **CONCLUSIONS**

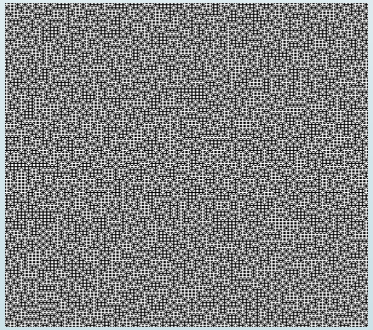
Introduction (1/2)

- In 1987, Kafri and Keren proposed the *visual secret sharing schemes* (VSSS for short).
- In 1995, Noar and Shamir proposed *visual cryptography* (VC for short), which is a way to encrypt one secret image and it can be decoded by human vision without any calculation.

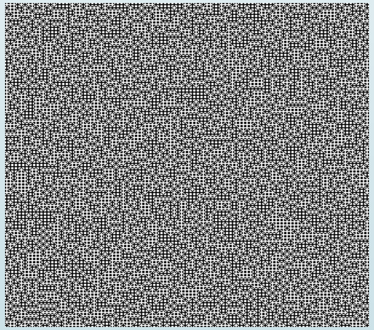
	Encryption	(k, n)-threshold	Pixel Expansion
Kafri and Keren	random gird	(2, 2)	No
Noar and Shamir	code book	(k, n)	Yes

Introduction (2/2)

- In practical, a slight misalignment between the shares could dramatically degrade the visual quality of the reconstructed image. If the size of one-pixel which be printed on the transparencies is small, the alignment will be difficult.



share 1

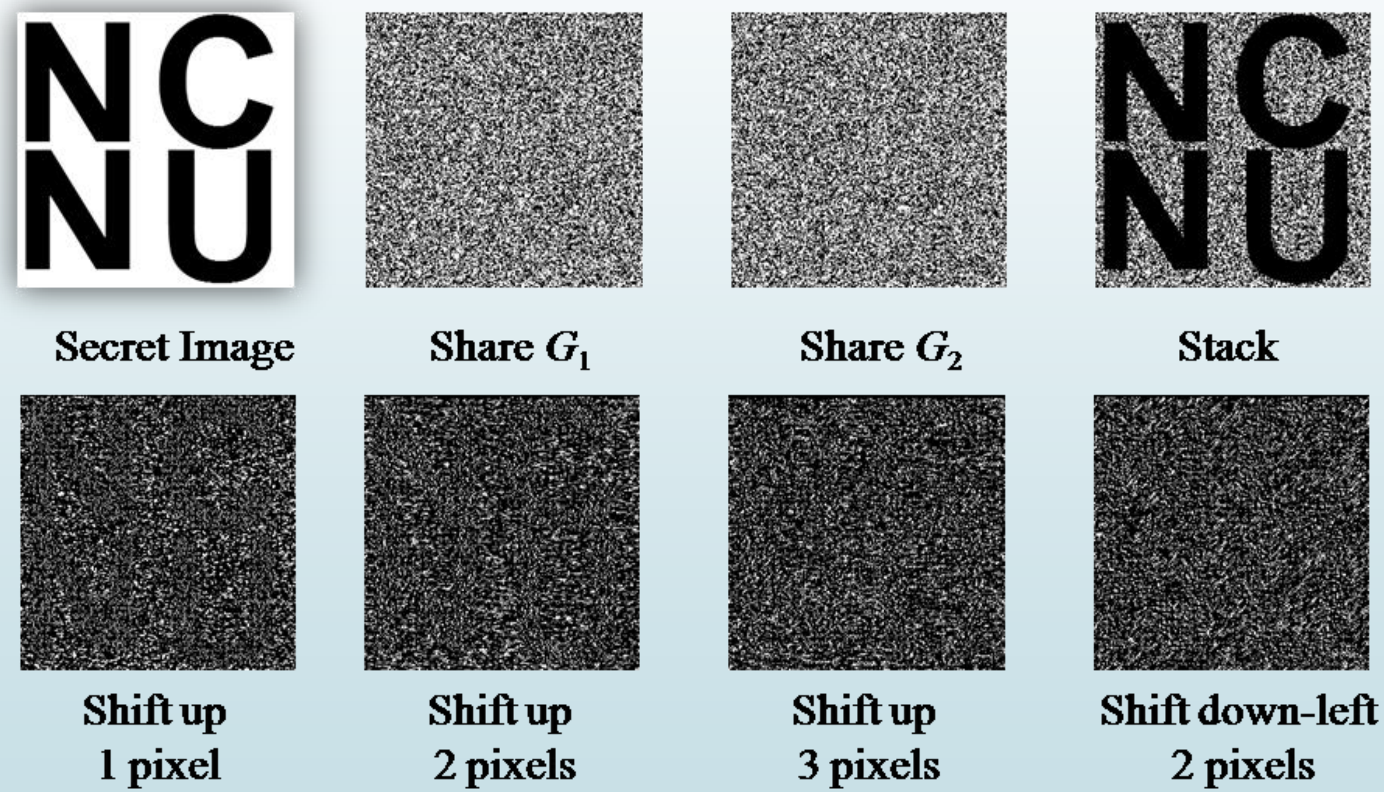


share 2

Related Work (1/3)

- *Random Grid Encryption Algorithm*

In KK1:

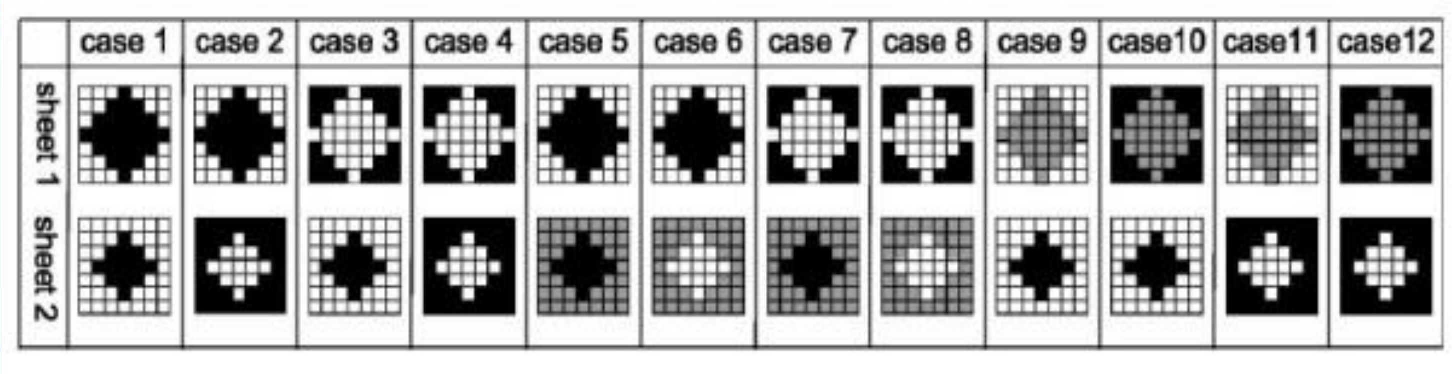


Related Work (2/3)

➨*The MTVSS Scheme*

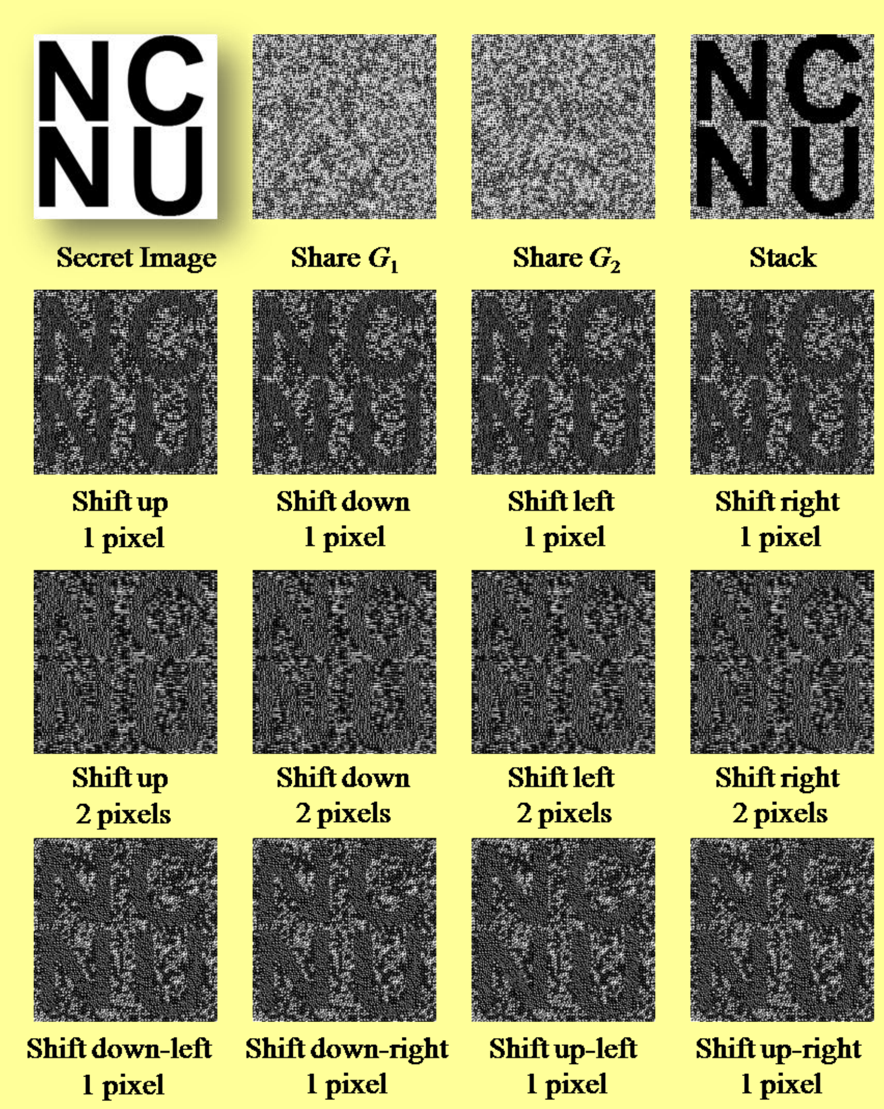
In 2004, Nakajima and Yamaguchi proposed:

- Shift-Tolerant
- Pixel Expansion



M. Nakajima and Y. Yamaguchi, “Enhancing registration tolerance of extended visual cryptography for natural images,” *Journal of Electronic Imaging* 13(3), pp. 654-662 (July 2004).

Related Work (3/3)



proposed these schemes.

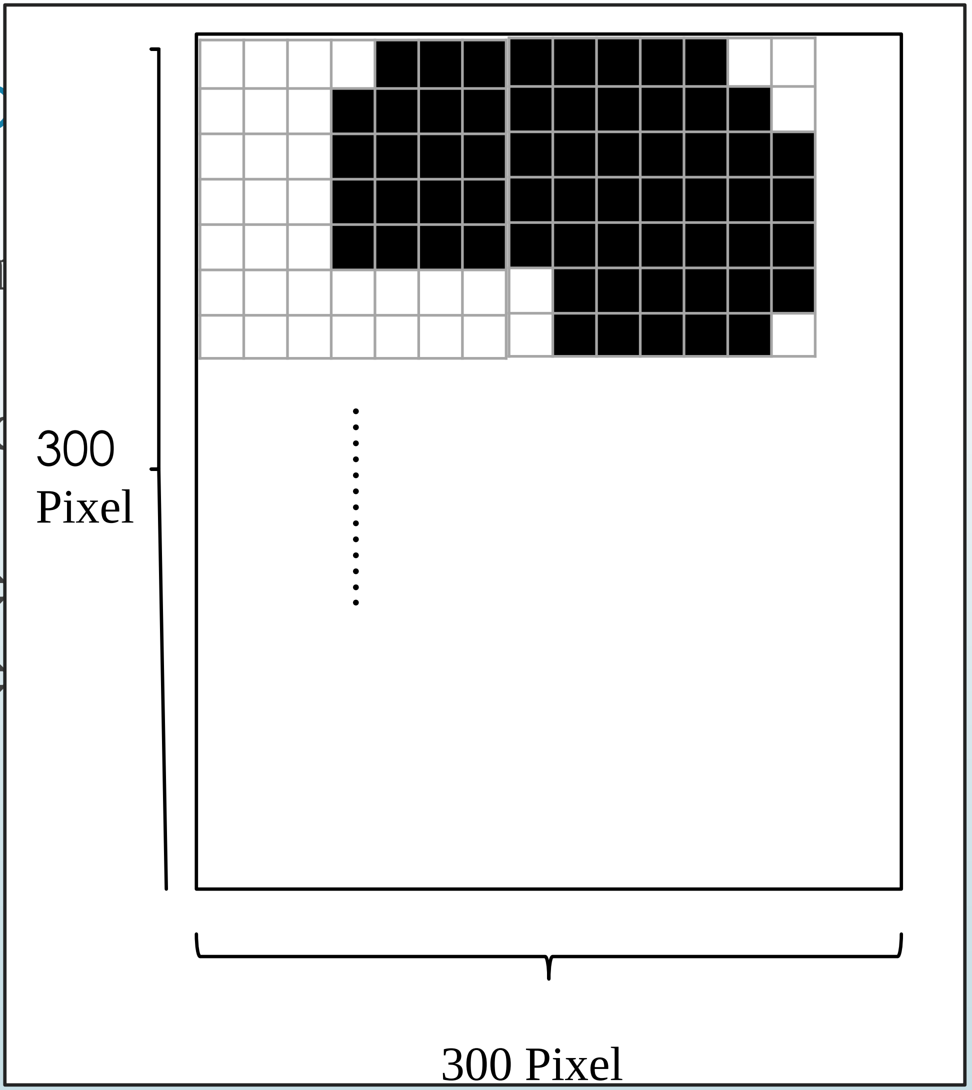
out

5 × 5	Stack	Shift 1 pixel
□	1/2	31/100
■	0	19/100
	Shift 2 pixels	Diagonal shift one pixel
□	26/100	721/3200
■	23/100	465/3200

The Proposed Scheme –

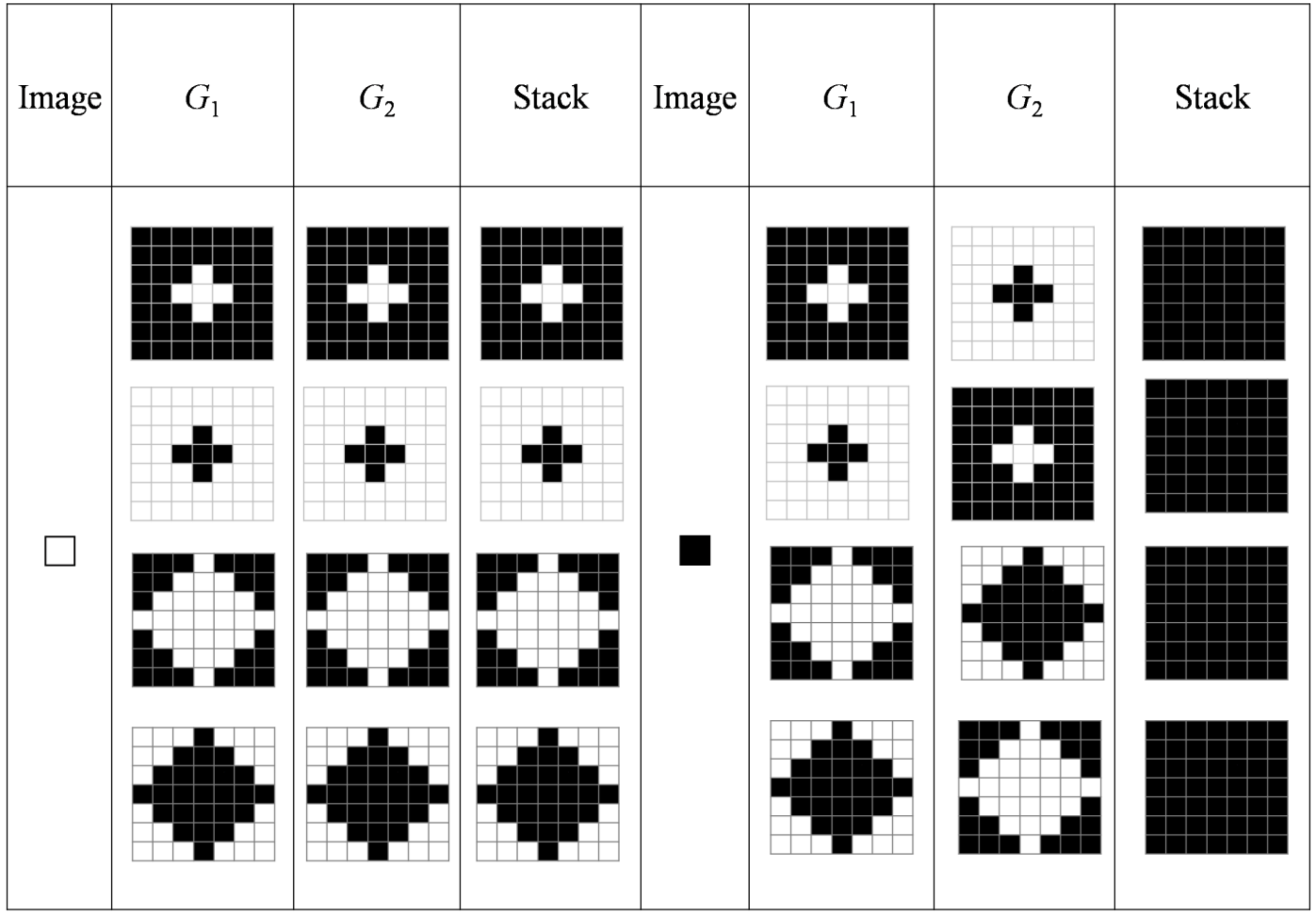
The Main Idea and Algo

- Taking $n \times n$ grid as a unit, the in units, for $n = 7$.
- Counting the number of black and the secret image.
  - the black pixels > white pixels ⇒
  - the black pixels < white pixels ⇒

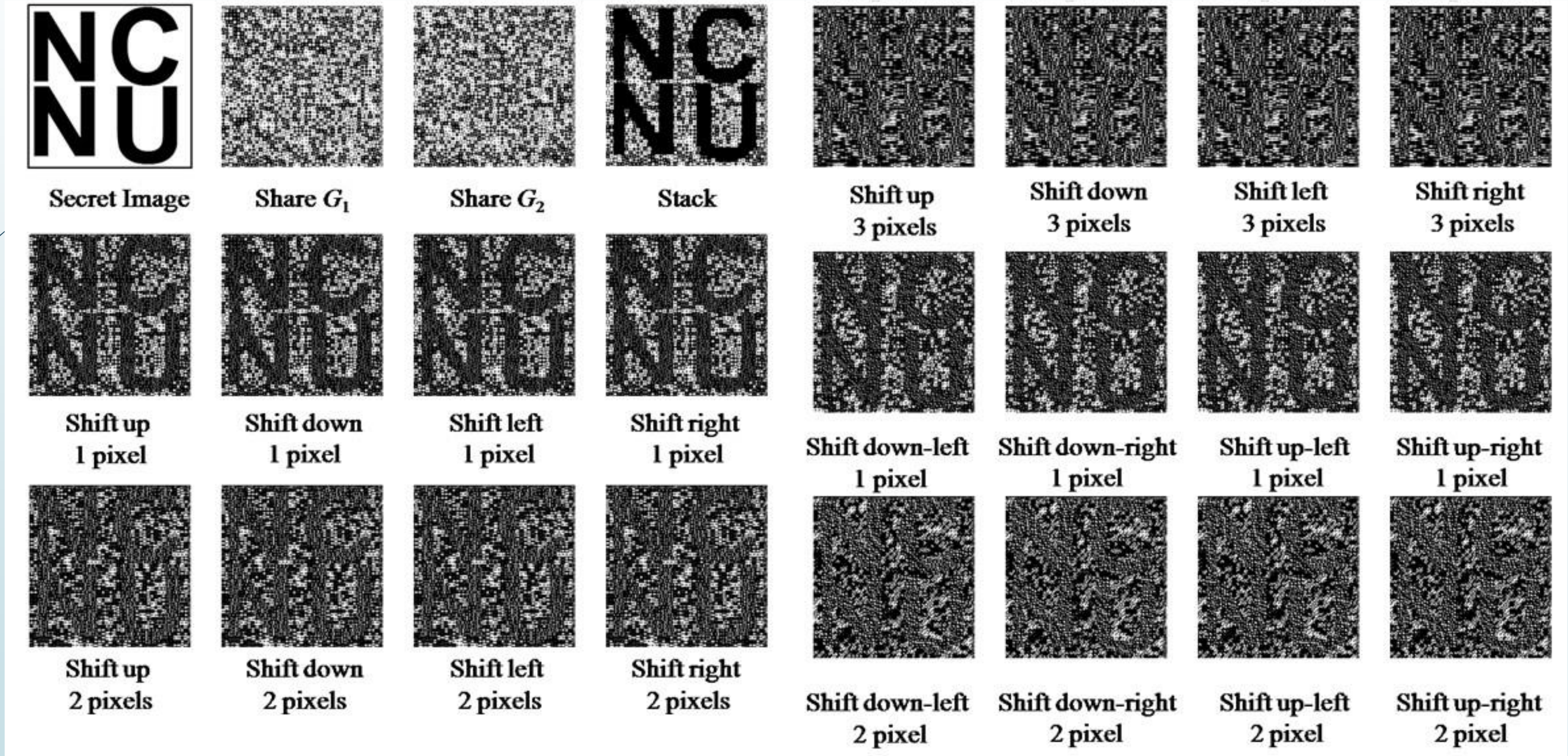


The Proposed Scheme – *The Main Idea and Algorithm (2/2)*

- **First share**: rand
  we designed.
- **Second share**: the
  Algorithm KK ac
  the same unit, and
  unit in the secret i



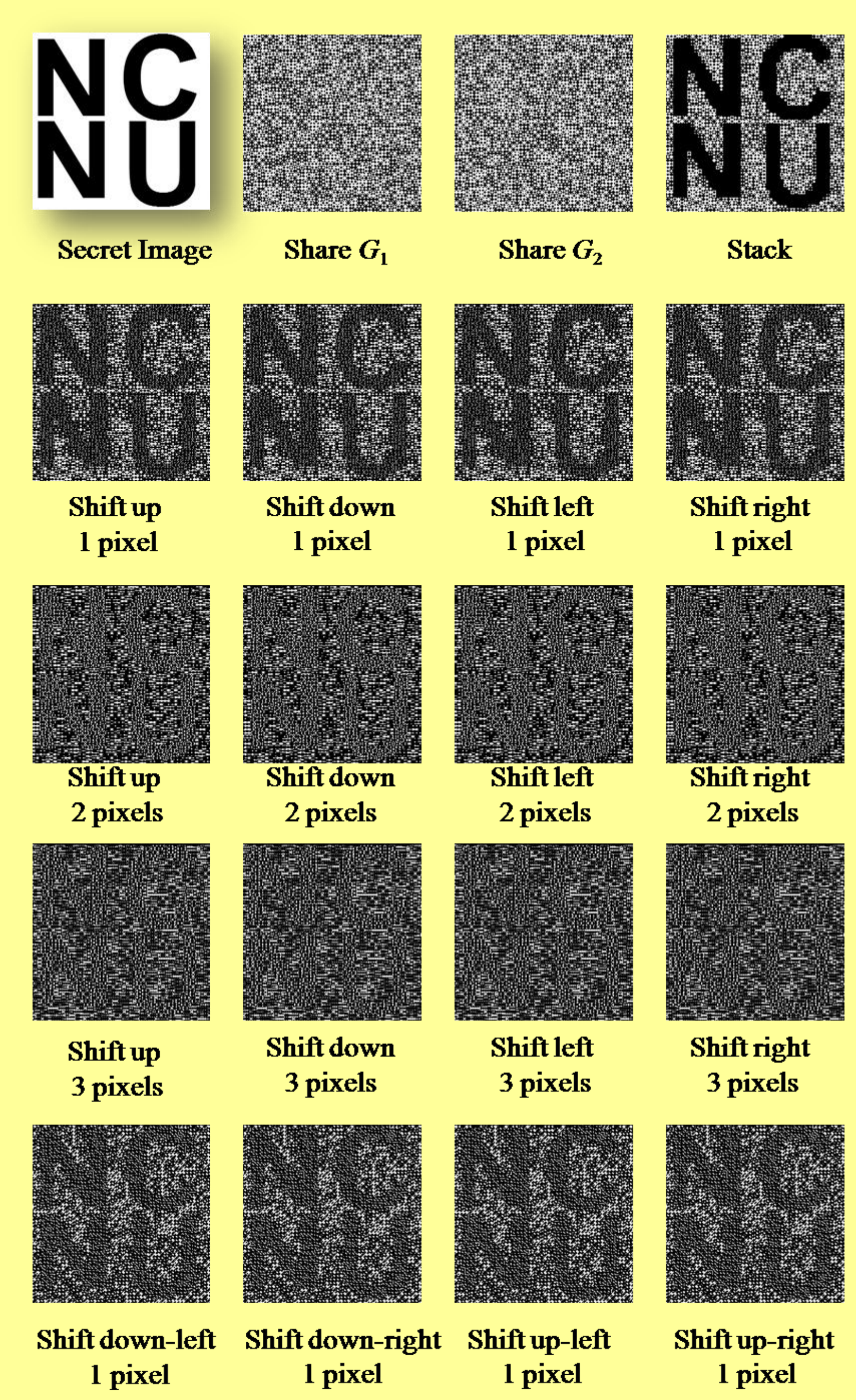
The Proposed Scheme – *The Experimental Results (1/2)*



國立暨南國際大學
National Chi Nan University

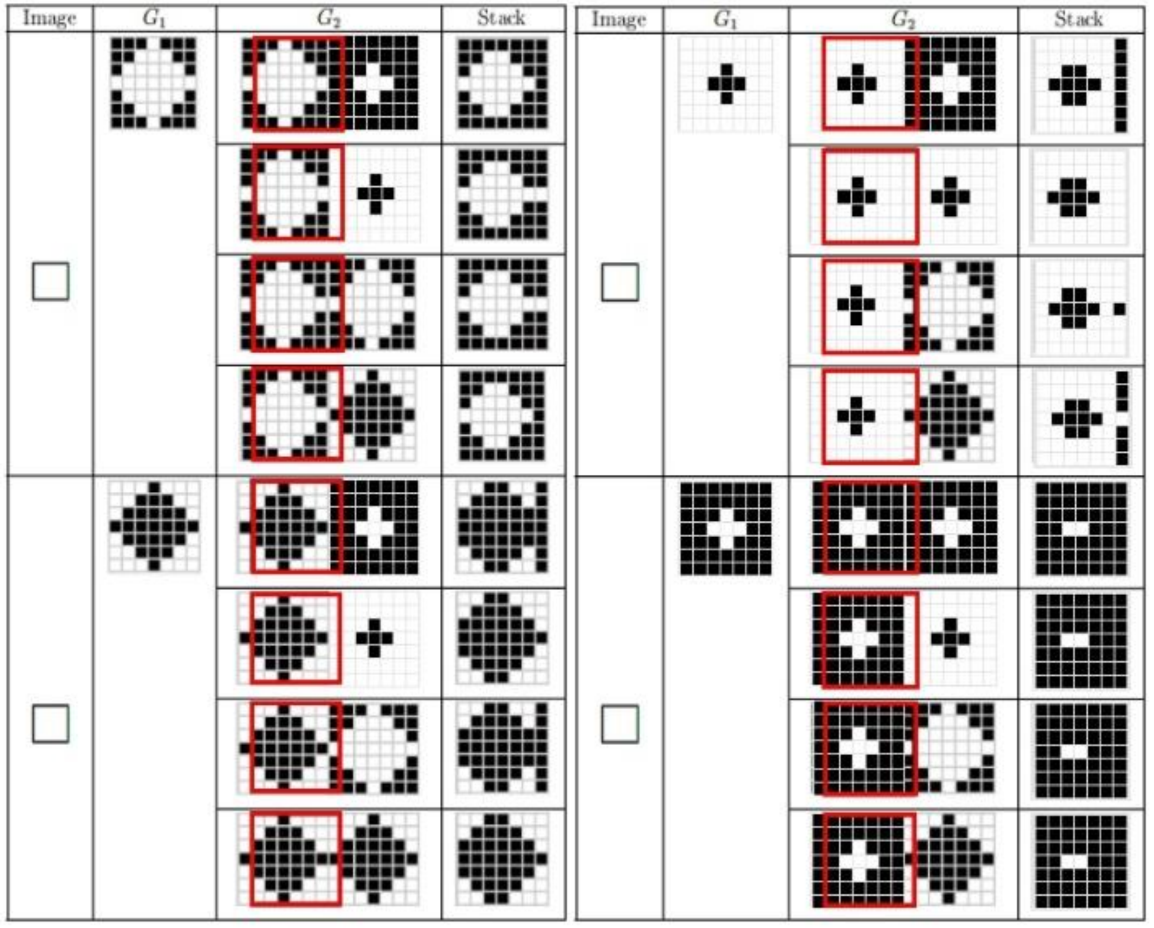
T… …ults (2/2)

- …we us…
…e.



6 × 6	Stack	Shift 1 pixel
□	1/2	50/144
■	0	25/144
	Shift 2 pixel	Shift 3 pixel
□	42/144	38/144
■	36/144	33/144
	Diagonal shift one pixel	
□	1189/4608	
■	422/4608	

ANALYSIS AND COMPARISON (1/7)



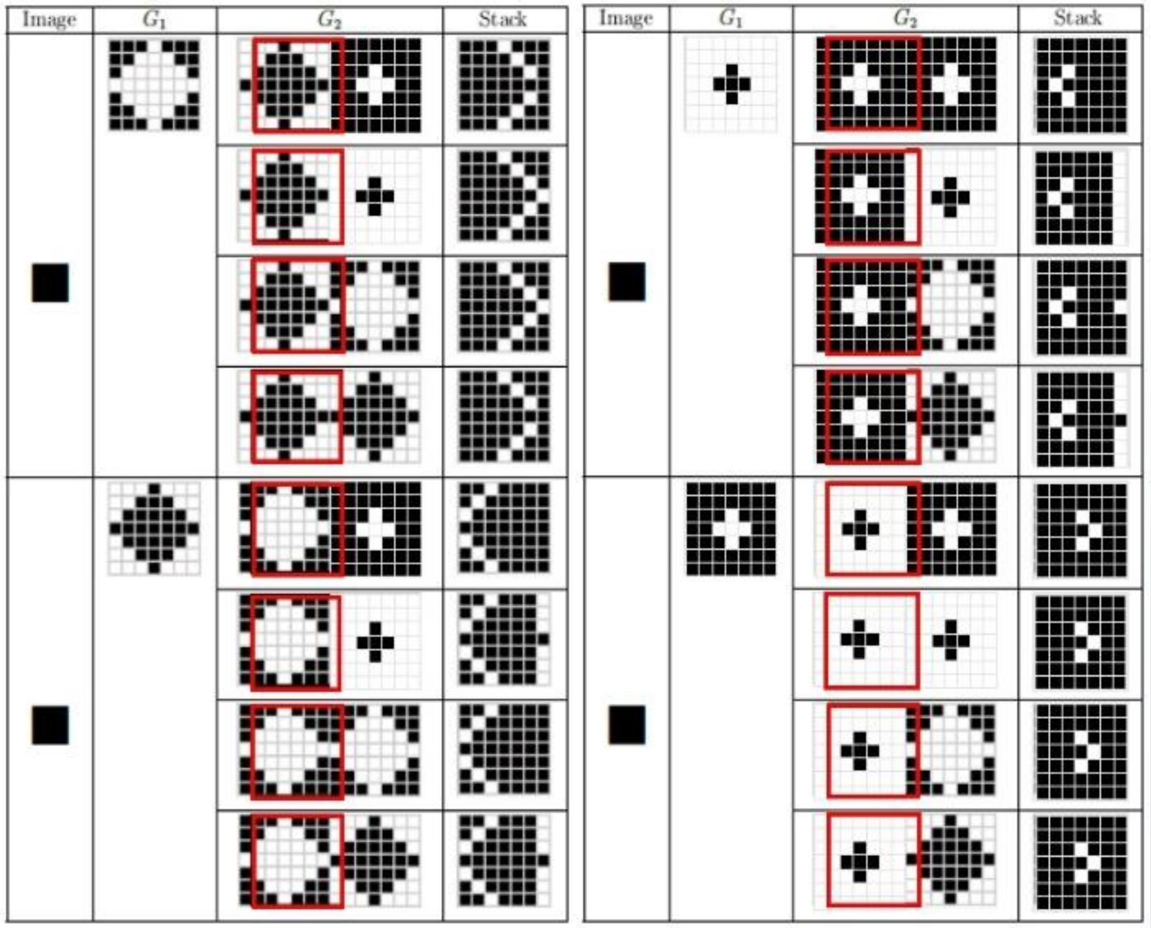
- The Transmittance for a white pixel in secret image =

  (74 + 60 + 150 + 8) / 784

  = 292 / 784

  = 73/196.

ANALYSIS AND COMPARISON (2/7)



- The Transmittance for a white pixel in secret image =

  (26 + 36 + 26 + 12) / 784

  = 100 / 784

  = 25/196.

ANALYSIS AND COMPARISON (3/7)

- The transmittance analysis for stacking two units for *n* = 7, compare with for *n* = 5, and 6 (FTVSS).

***n* = 7**	**Stack**	**Shift 1 pixel**	**Shift 2 pixels**	**Shift 3 pixels**
□	1/2	73/196	62/196	53/196
■	0	25/196	37/196	45/196
***n* = 6**	Stack	Shift 1 pixel	Shift 2 pixels	Shift 3 pixels
□	1/2	50/144	42/144	38/144
■	0	25/144	36/144	33/144
***n* = 5**	Stack	Shift 1 pixel	Shift 2 pixels	
□	1/2	31/100	26/100	
■	0	19/100	23/100	

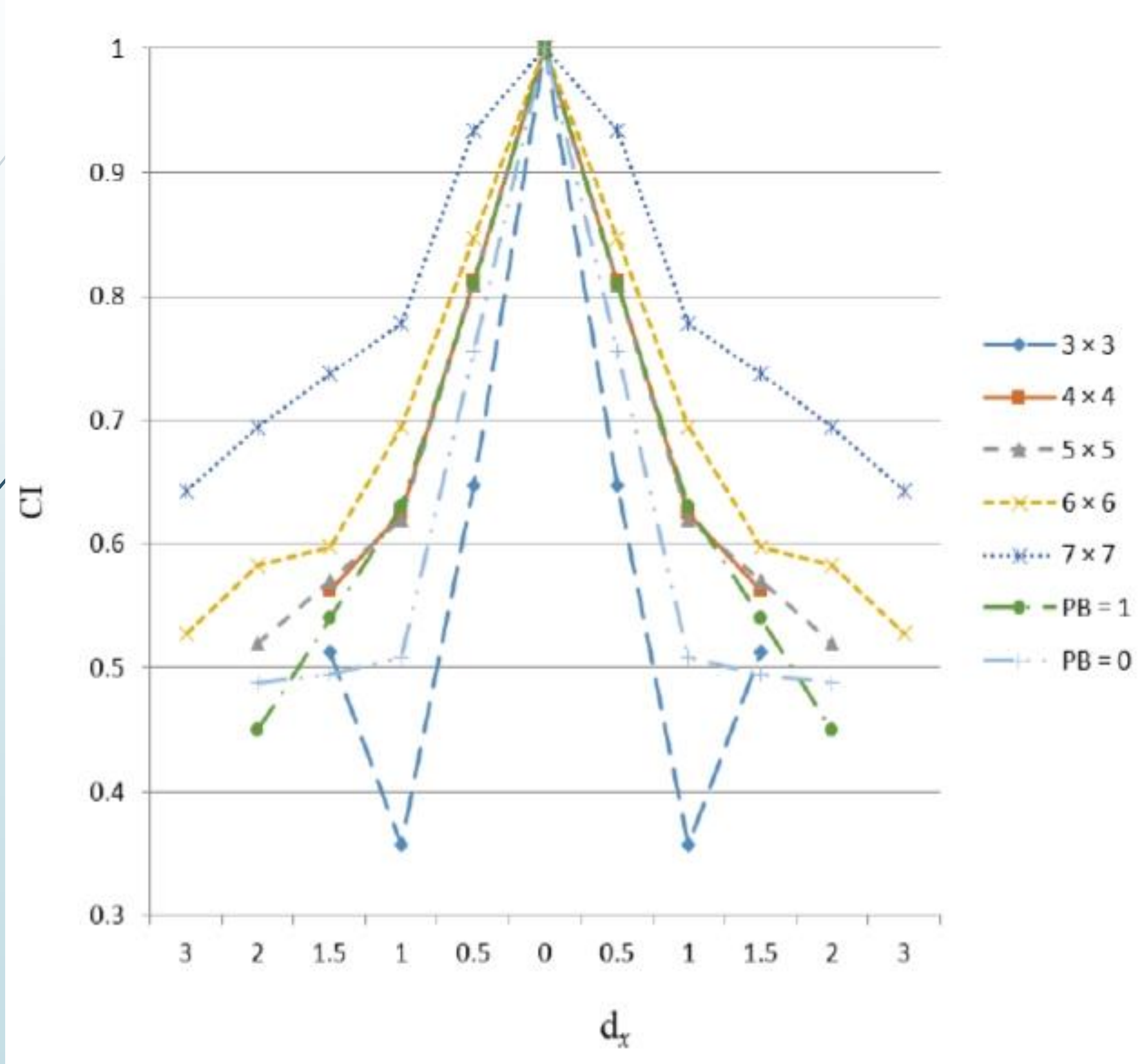
ANALYSIS AND COMPARISON (4/7)

- The transmittance analysis for stacking two resulting units for one pixel diagonal-shift for n = 7, compare with for n = 4, 5, and 6 (FTVSS).

Diagonal-shift one pixel	$n = 4$	$n = 5$	$n = 6$	$n = 7$
□	381/2048	721/3200	1189/4608	1893/6272
■	173/2048	465/3200	422/4608	613/6272

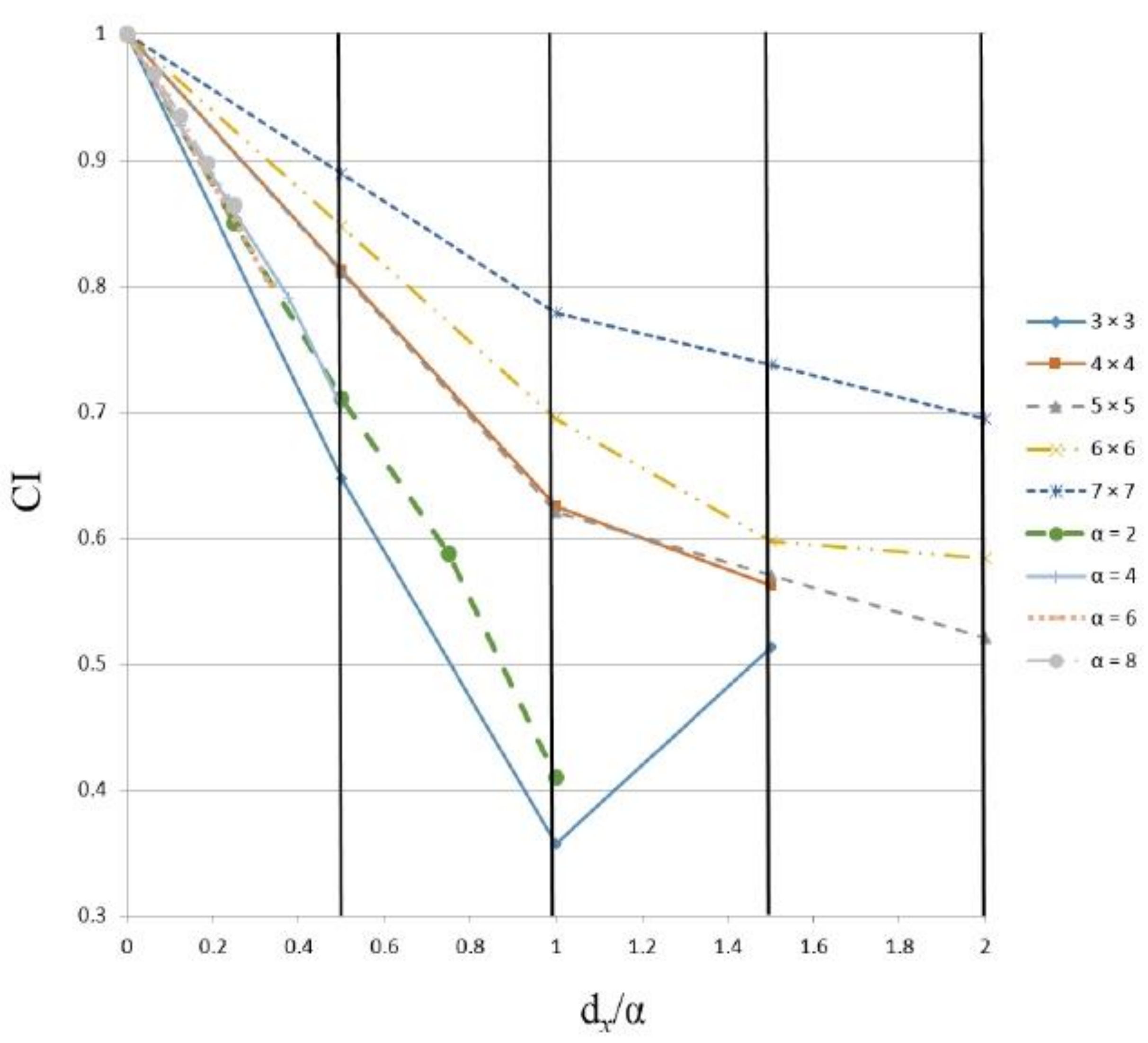
- **Theorem 1.** The proposed scheme are the fault-tolerant VSS scheme.

ANALYSIS AND COMPARISON (5/7)



- Compare CI with MTVSS and FTVSS. (1/2)

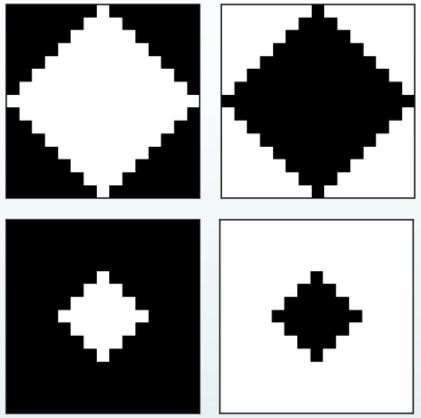
ANALYSIS AND COMPARISON (6/7)

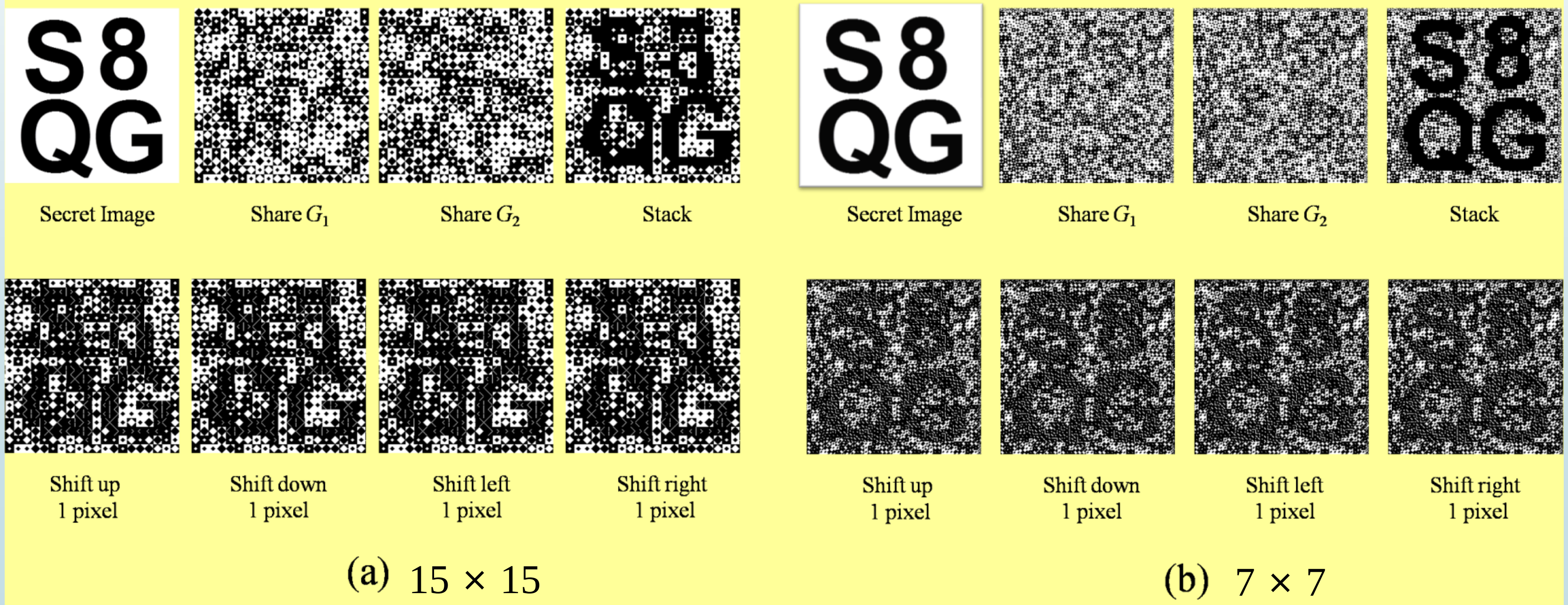


- Compare CI with MTVSS and FTVSS. (2/2)

ANALYSIS AND COMPARISON (7/7)

- If n is greater, will the performance of tolerance be better ?

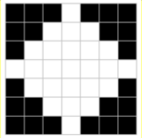
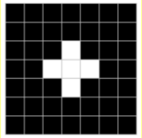
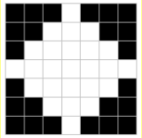
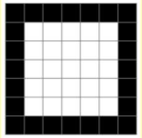
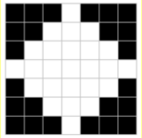
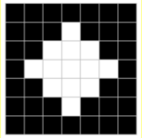




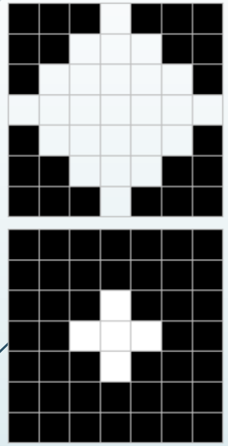
CONCLUSIONS

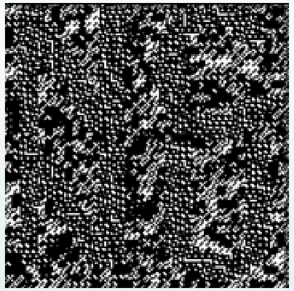
- This paper presents a visual secret sharing scheme that are fault tolerant without pixel expansion; which is an extended scheme of FTVSS.
- This paper also discusses the limits of this technique.
- Future works:
  - Improving the existing algorithms.
  - Round sharp?
  - Design a (k, n)-threshold VSS scheme that addresses the misalignment problem without pixel expansion.

APPENDIX (1/2)

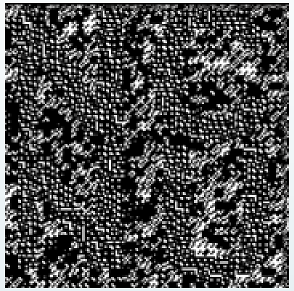
7 × 7		Shift 1 pixel	Shift 2 pixels	Shift 3 pixels	Diagonal shift one pixel	Diagonal shift two pixels
	□	73/196	62/196	53/196	3786/12544	2040/12544
	■	25/196	37/196	45/196	1226/12544	1656/12544
	□	69/196	58/196	51/196	3146/12544	2516/12544
	■	29/196	40/196	46/196	1866/12544	1108/12544
	□	69/196	54/196	47/196	3530/12544	1656/12544
	■	29/196	44/196	51/196	1482/12544	2040/12544

APPENDIX (2/2)

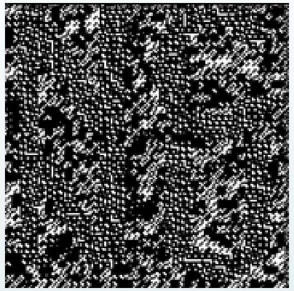




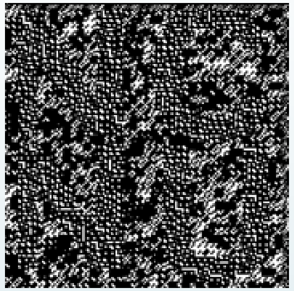
Shift down-left
2 pixel



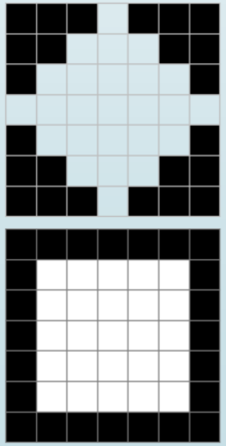
Shift down-right
2 pixel

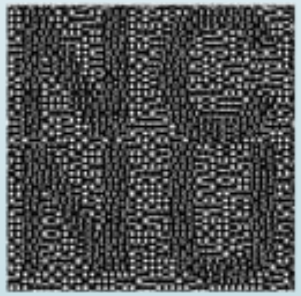


Shift up-left
2 pixel

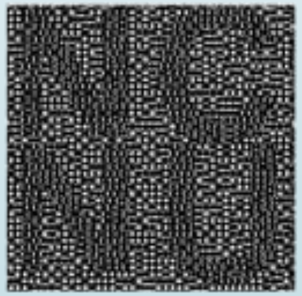


Shift up-right
2 pixel



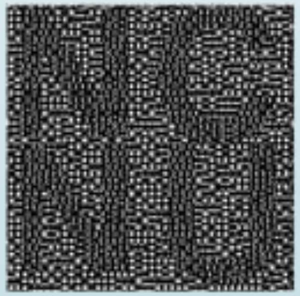


Shift down-left
2 pixels



Shift down-right
2 pixels

Shift up-left
2 pixels



Shift up-right
2 pixels

Computer Science and Information Engineering
National Chi Nan University

The Principle and Application of Secret Sharing

Dr. Justie Su-Tzu Juan

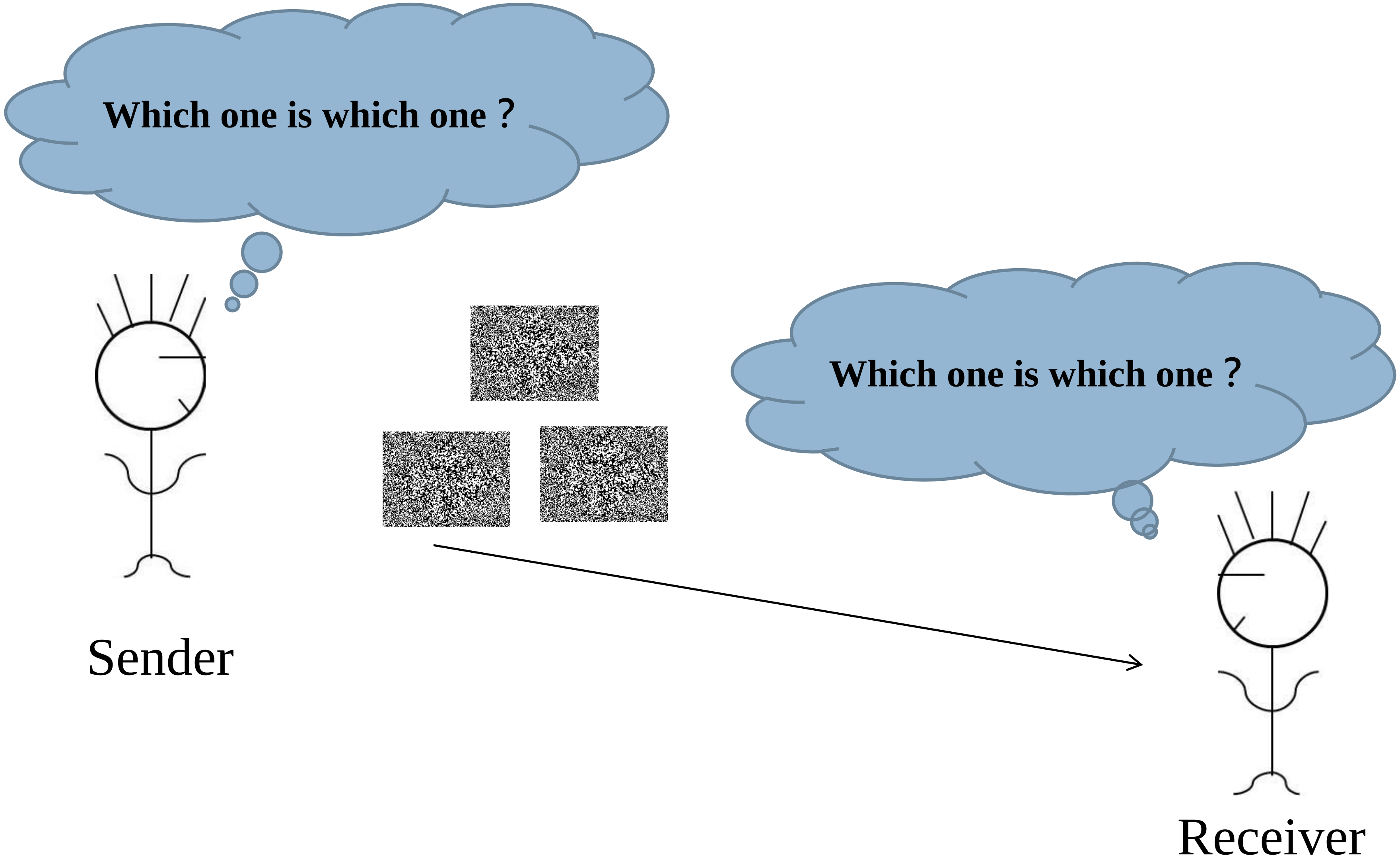
Lecture 7. Visual Cryptography with Various Functions

§ 7.3 Meaningful VSS Scheme

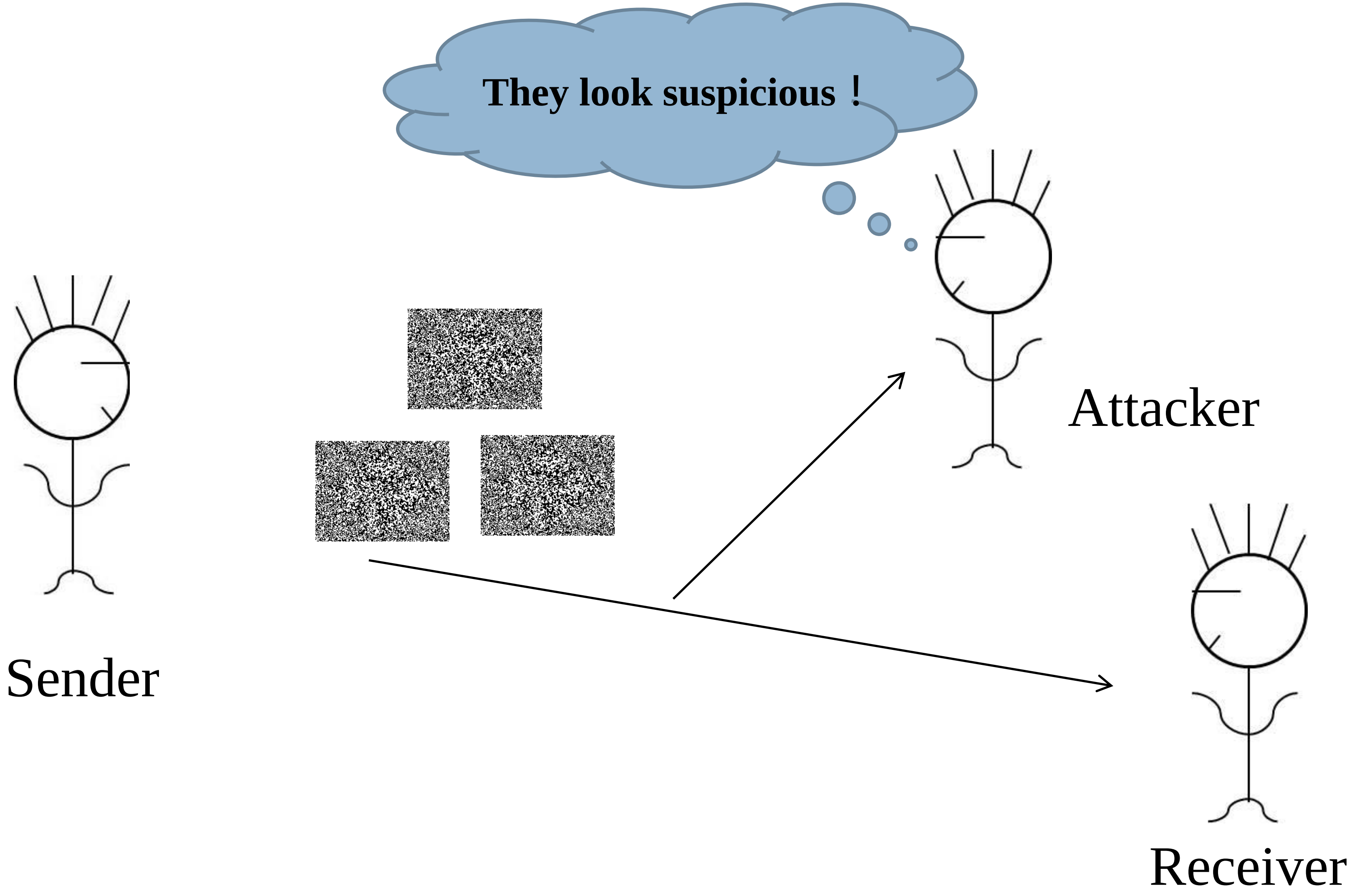
Slides for a Course Based on

Bo-Yuan Huang and Justie Su-Tzu Juan[*], "A Meaningful Visual Multi-Secret Sharing Scheme by Random Grids," *Proc. of GCEAS 2017*, Okinawa Convention Center, Okinawa, Japan, July 25-27, 2017, pp. 244-255.

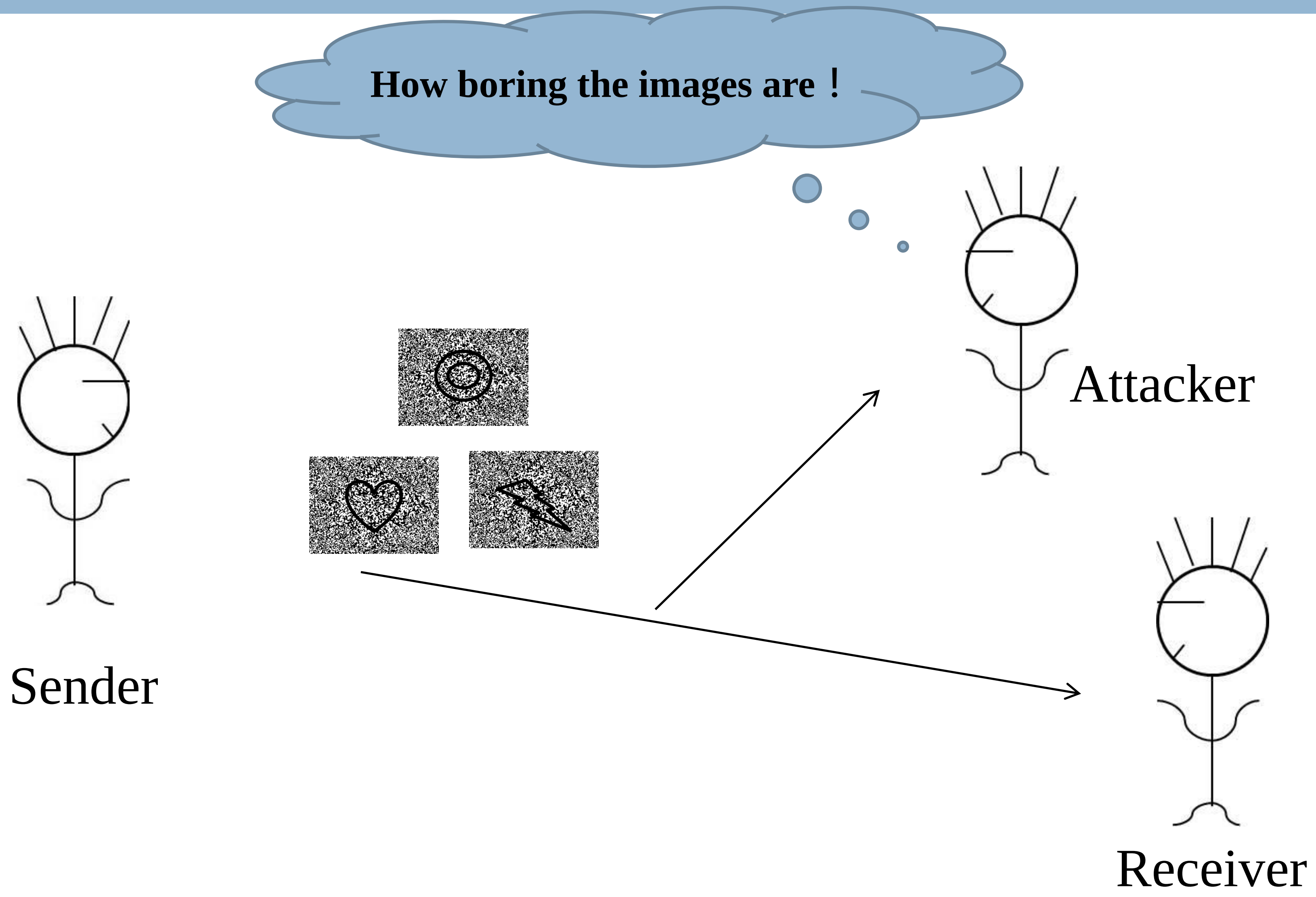
Image management ?



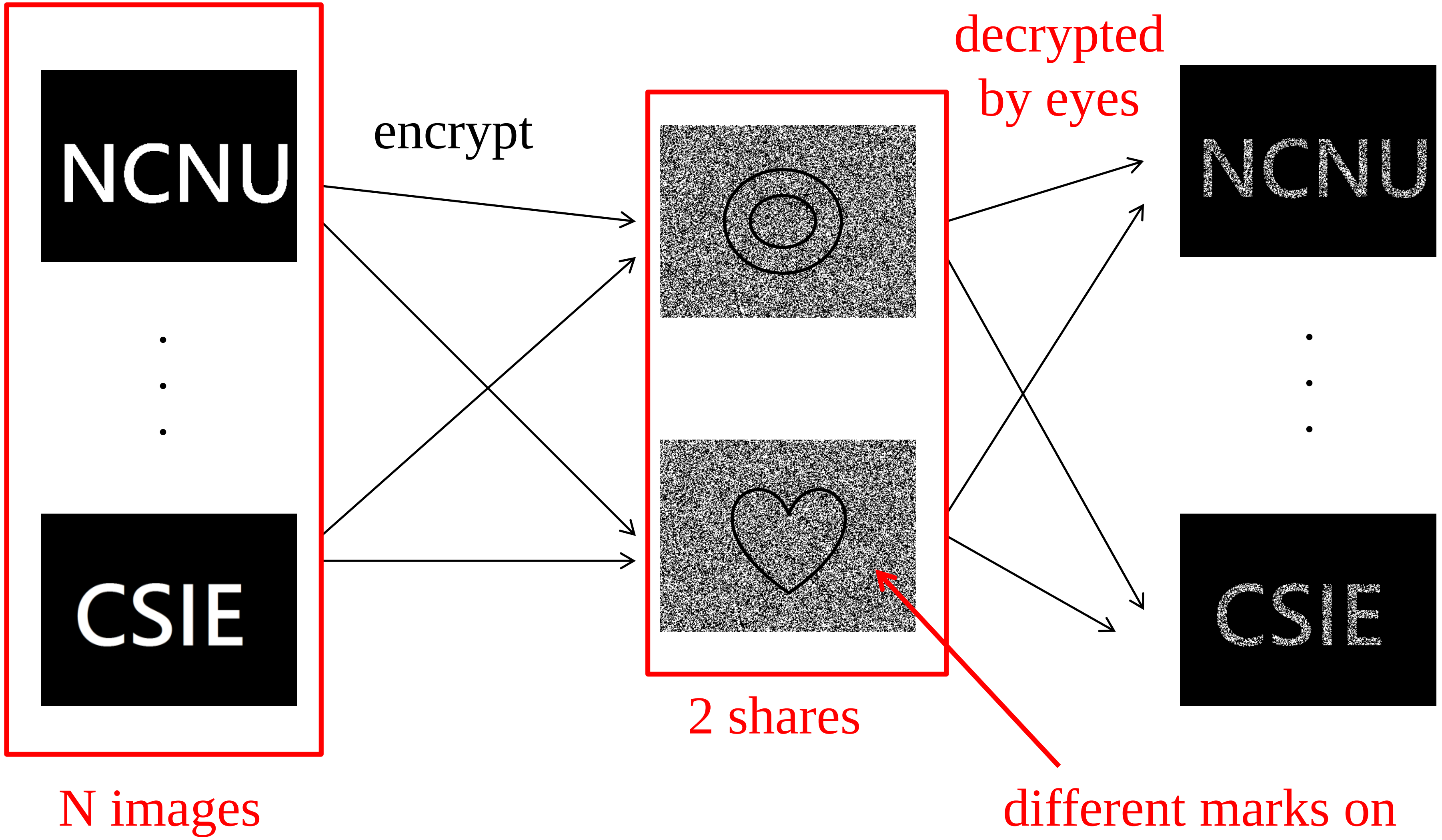
Suspicious ?



Meaningful VMSSS (MVMSSS)

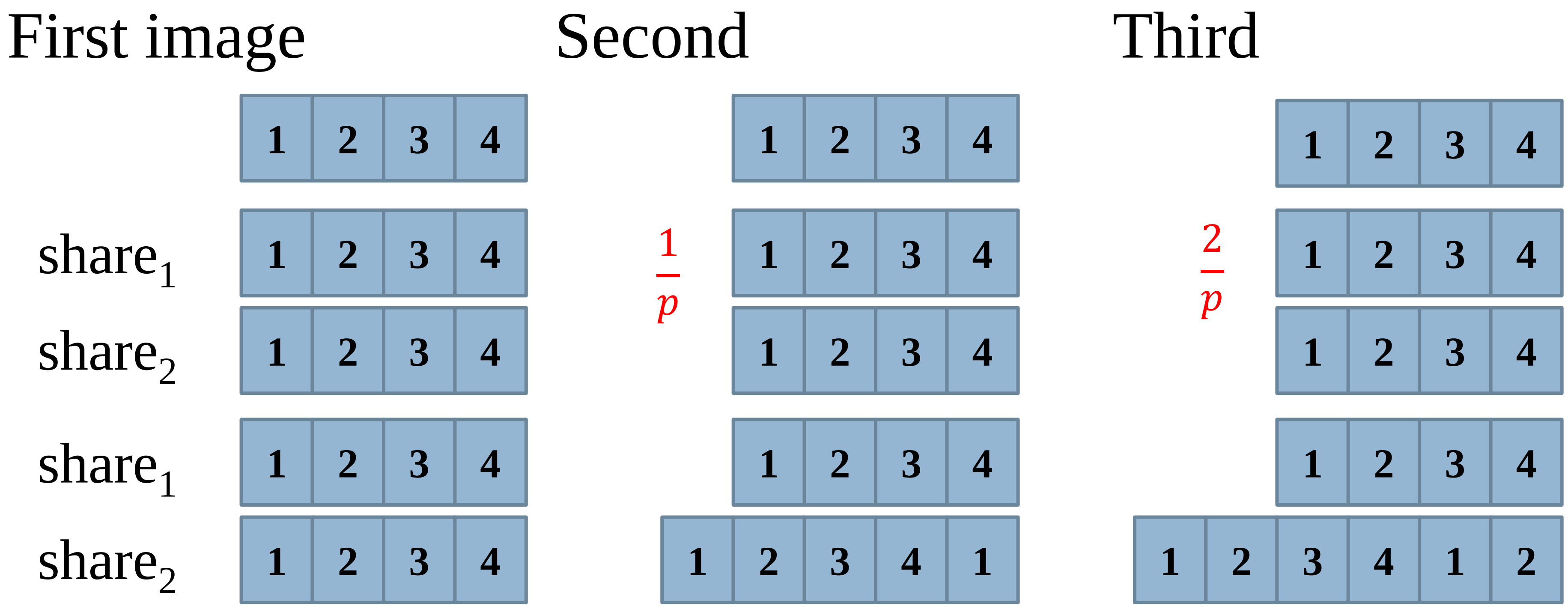


Our main achievement



How we decrypt & encrypt ?

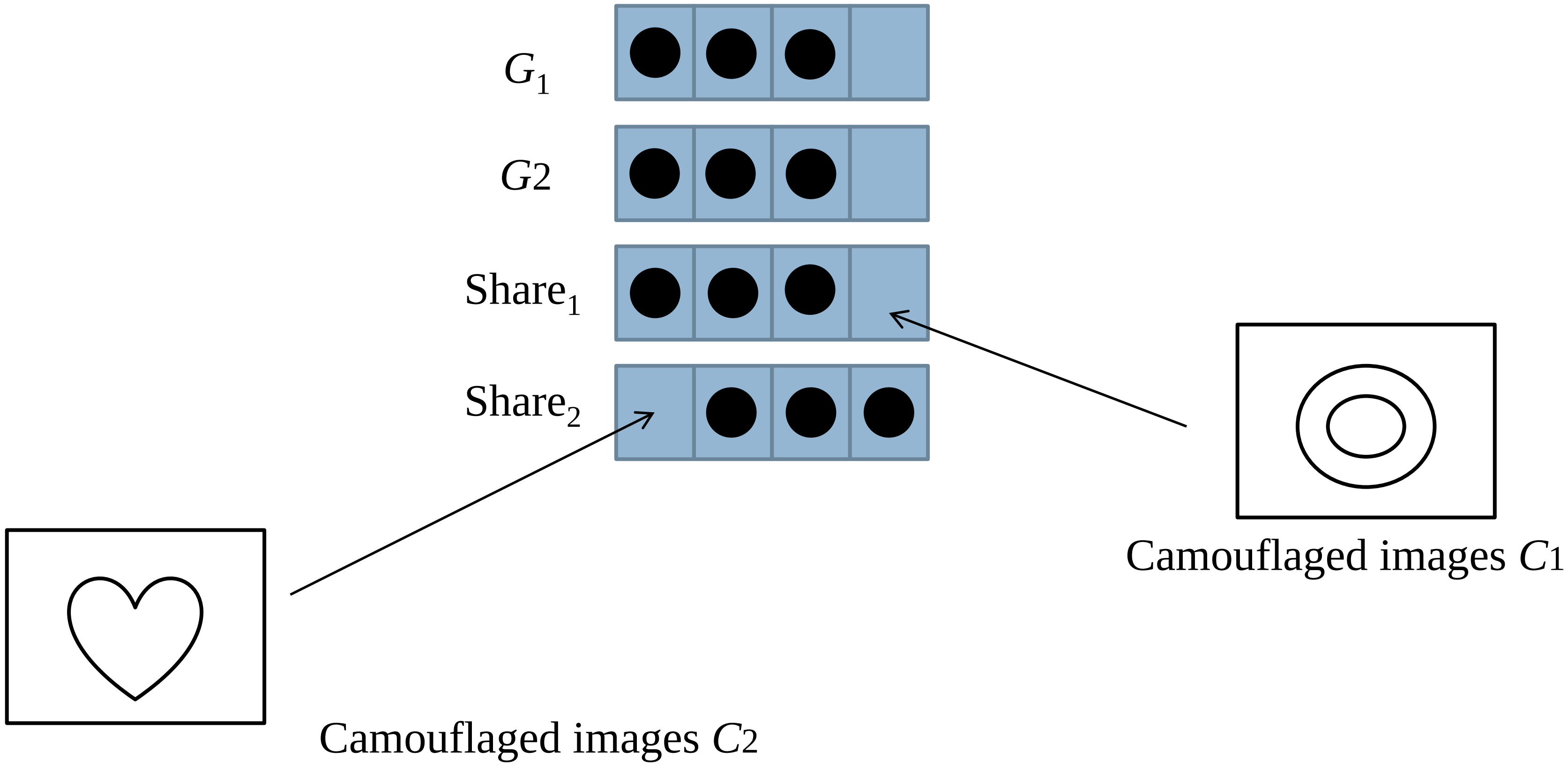
- Shifting random grids
- For example $N = 3$, $p = 4$



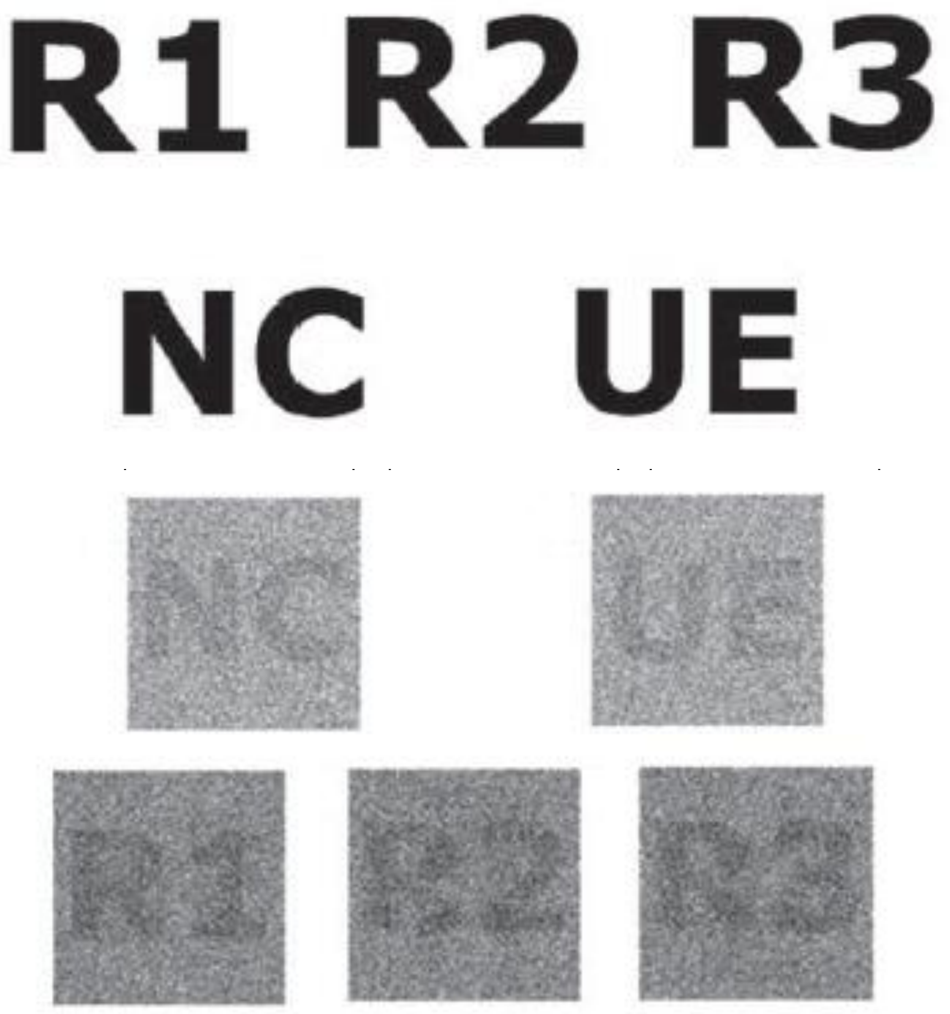
How we make them meaningful?

- $Share_1(a, b) = C1(a, b)$
- $Share_2(c, d) = C2(c, d)$

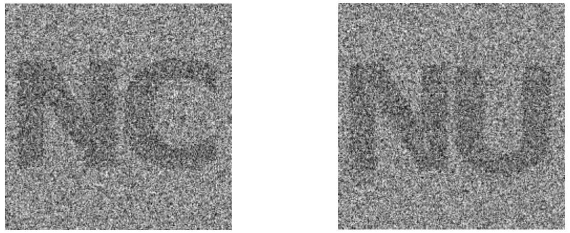
this two pixels are according to the first pixels you randomly select



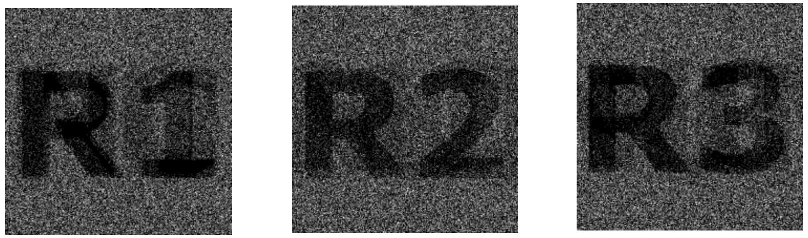
s (540×540 p =10)



Liu et al., Computer Journal, 2015.

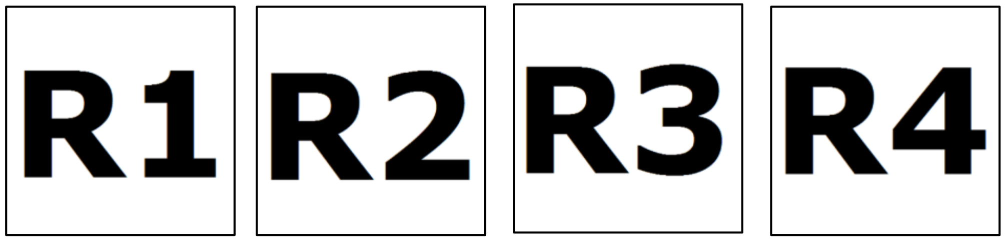


Shares

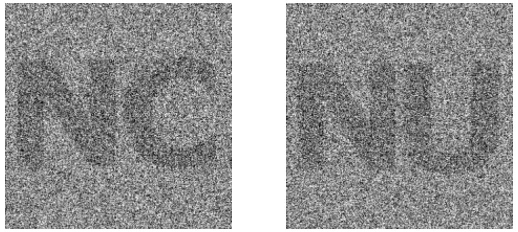


Restored images

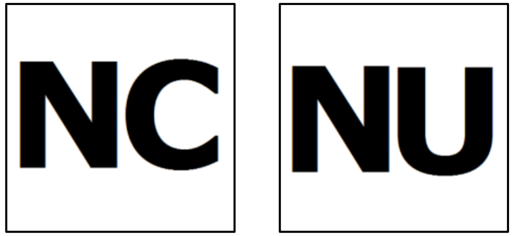
Experiment results (cont’d) (540×540 p =10)



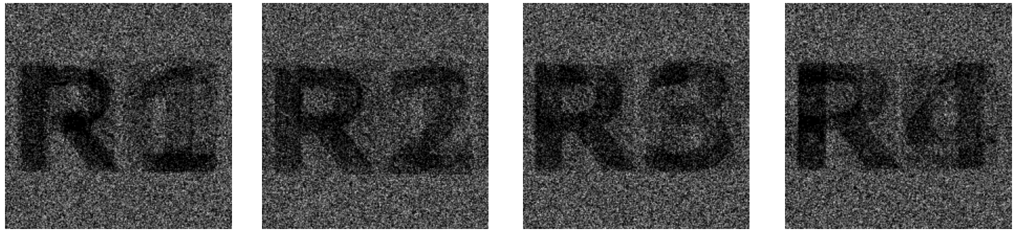
Secret images



Shares

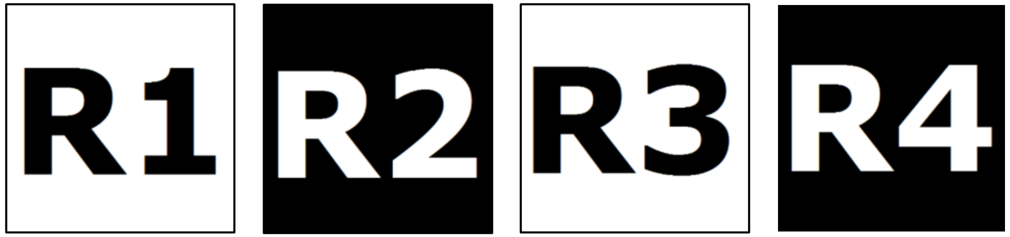


Camouflaged images

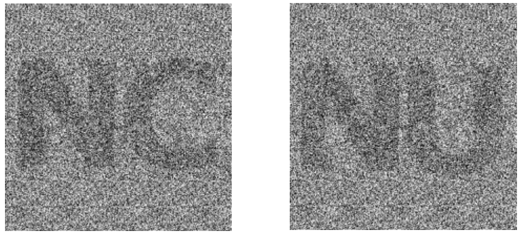


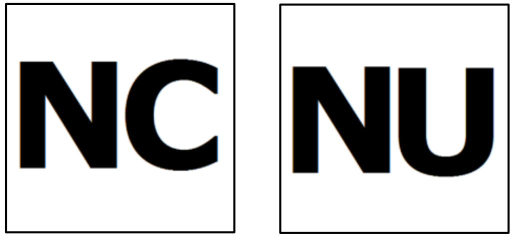
Restored images

Experiment results (cont'd) (540×540 p =20)

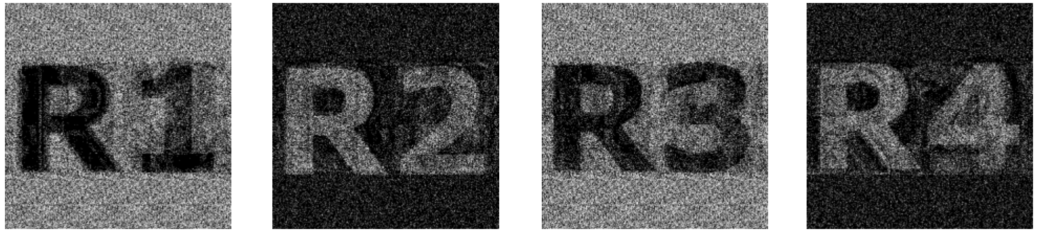


Secret images


Shares

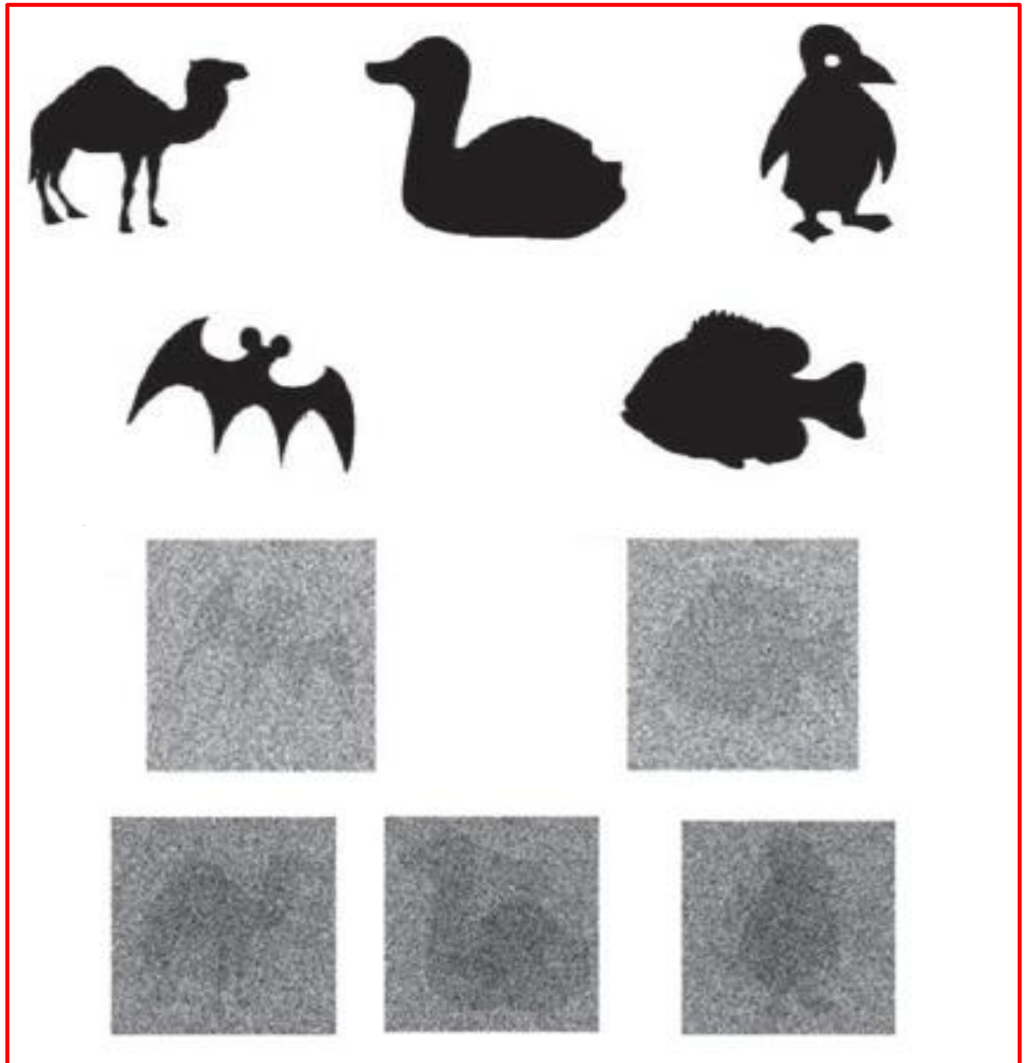


Camouflaged images

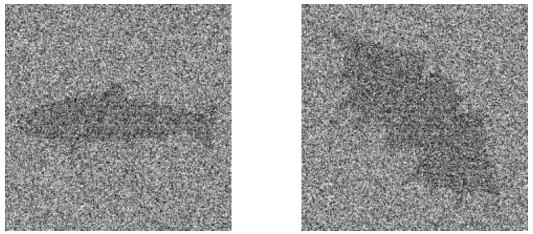


Restored images

Ex… nt’d) (540×540 p =10)



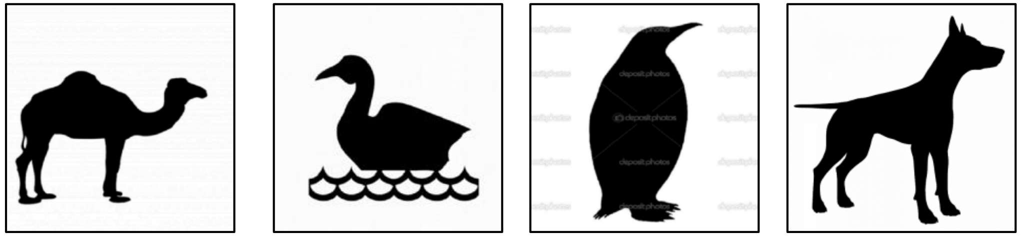
Liu et al., Computer Journal, 2015.



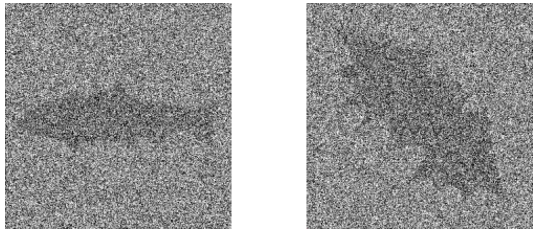
Shares

Restored images

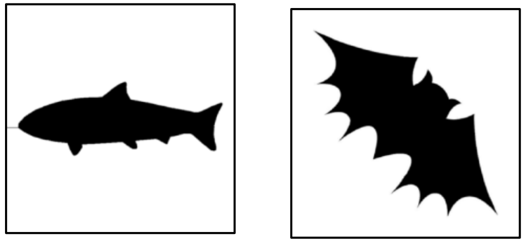
Experiment results (cont'd) (540×540 p =10)



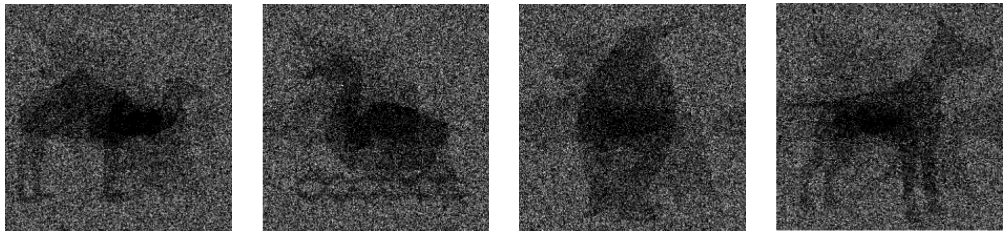
Secret images



Shares

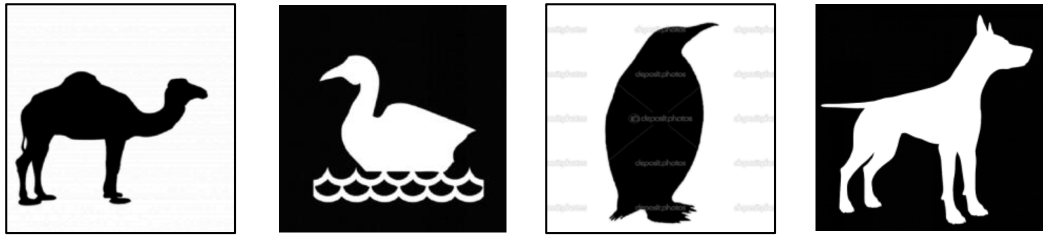


Camouflaged images

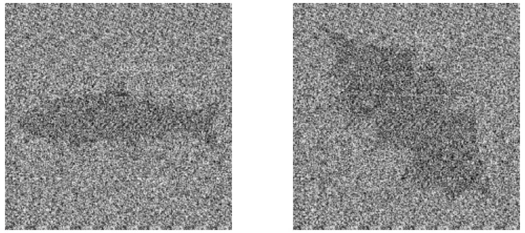


Restored images

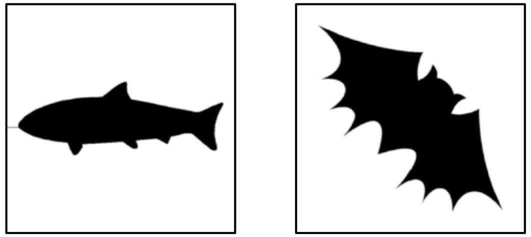
Experiment results (cont’d) (540×540 p =20)



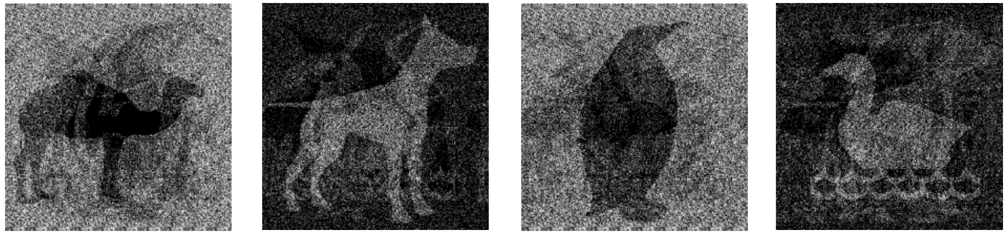
Secret images



Shares



Camouflaged images



Restored images

Comparison

	Number of secret images	Meaningful shares	Quality of shares	Any secret rectangle images
The proposed scheme	More than 2	Yes	High	Yes
Chen et al. (2012)	4	No	Low	No (Square only)
Liu et al. (2015)	3	Yes	Low	No (Square only)
Chang et al. (2010)	More than 2	No	High	Yes

Conclusion

- With the Meaningful Shares
  - efficiency on image management
  - more secure when transmission
- With the Shifting Random Grid
  - flexibility on the number of the secret images
  - any rectangle secret image allowed