



視覺密碼

# Visual Cryptography

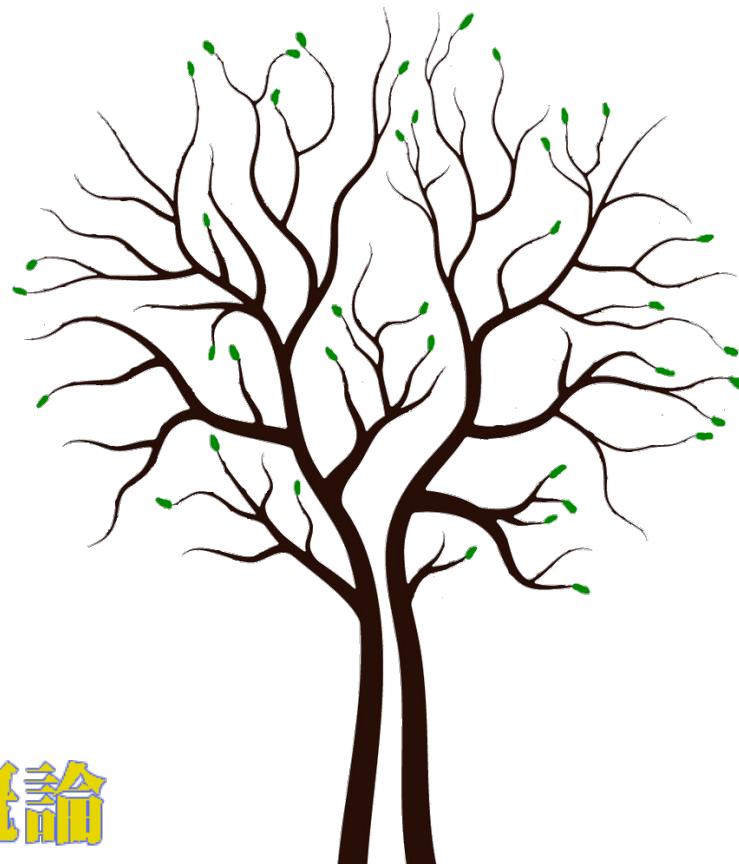
陳琨

[kchen@csie.org](mailto:kchen@csie.org)



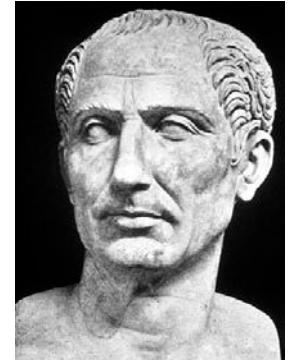
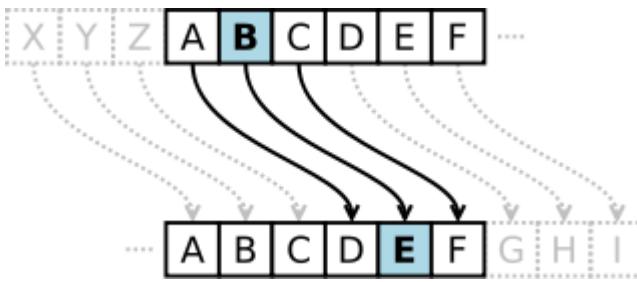
# 密碼學 Cryptography

- 源於希臘文“kryptós”「隱藏」，和“gráphein”「寫字」組成，表示隱藏的字



# 凱撒(Caesar)密碼

- 於西元前50年羅馬皇帝 Julius Caesar 使用
- 將每個字母用其後的第三個字母來取代。
  - 明文：i love you
  - 密文：l oryh brx

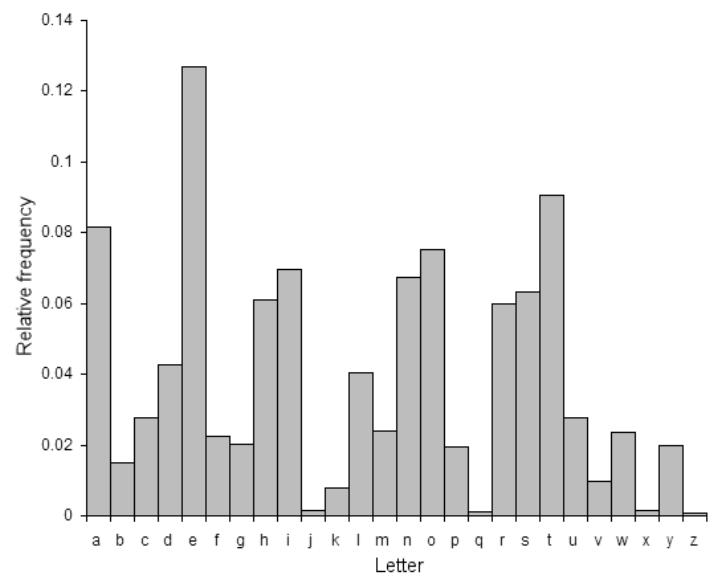
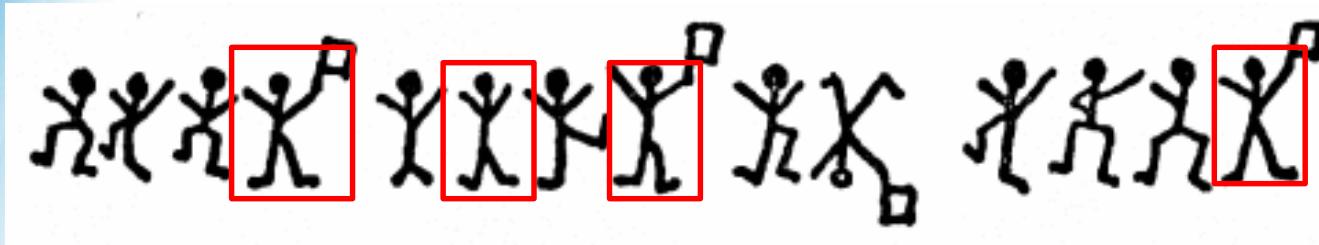


$$C = E_n(P) = (P + n) \bmod 26$$

$$P = D_n(C) = (C - n) \bmod 26$$



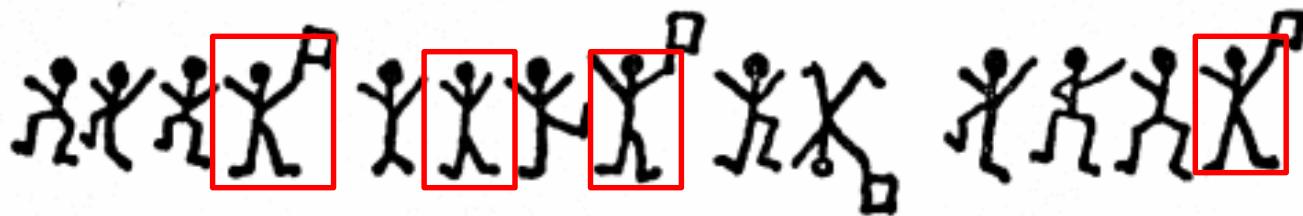
# 福爾摩斯與跳舞的人



計算機概論

[http://ebooks.adelaide.edu.au/d/doyle/arthur\\_conan/d75  
re/chapter4.html](http://ebooks.adelaide.edu.au/d/doyle/arthur_conan/d75/re/chapter4.html)

# 福爾摩斯與跳舞的人



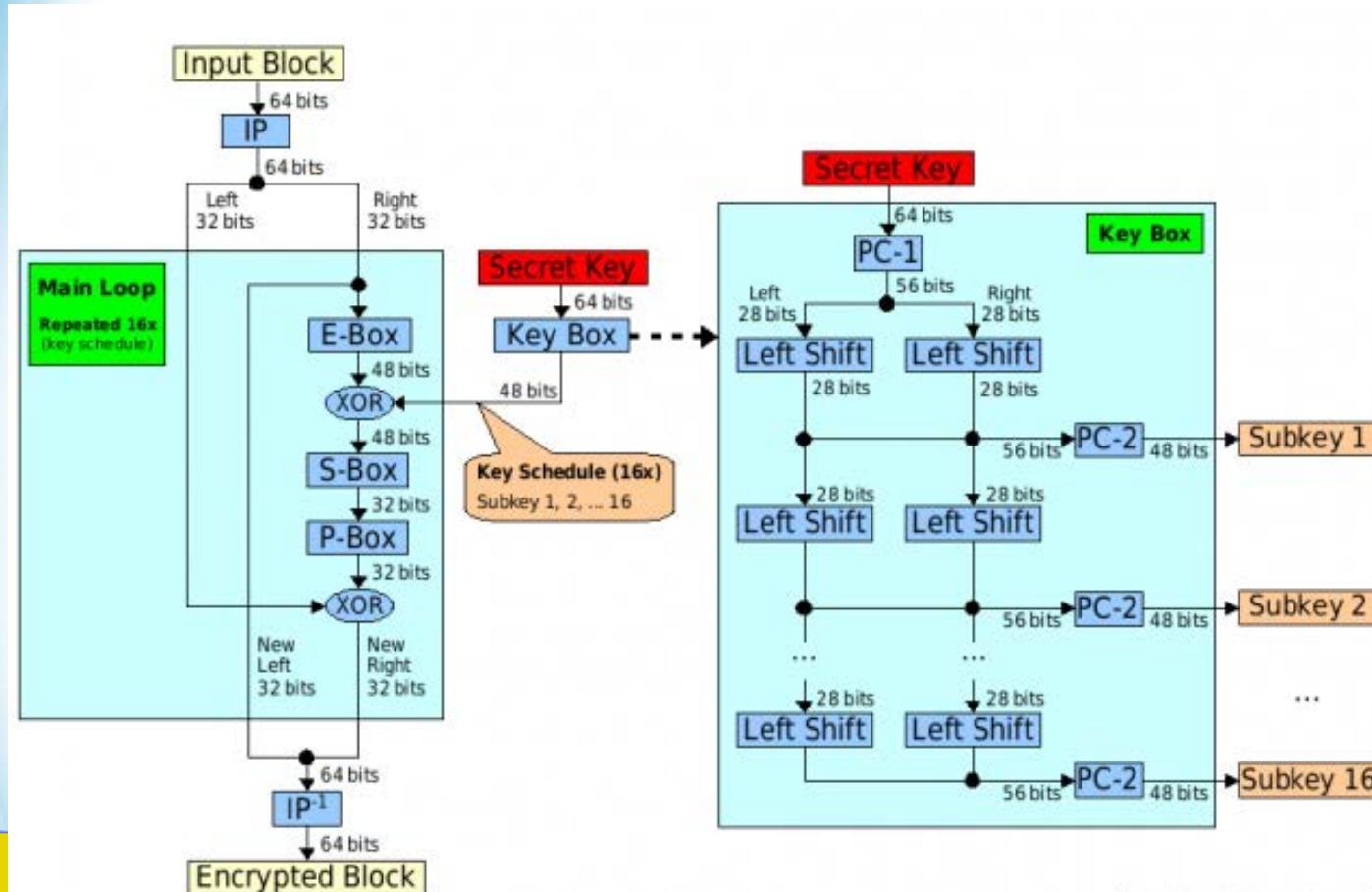
C O M E   H E R E   A T   O N C E

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z



# 資料加密標準 (DES)

- DES : Data Encryption Standard



# 現今密碼應用



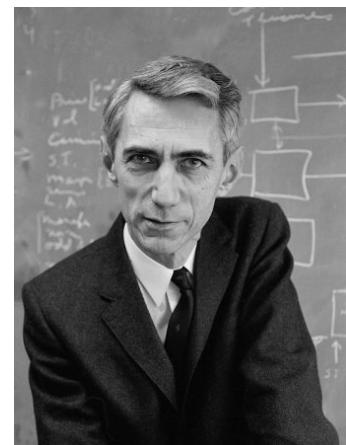
計算機概論



# One-time pad

- 稱一次性密碼本，是一種加密的演算法
- 特性：金鑰是**隨機產生且只用一次**
- 夏農 (Shannon)於1948年證明此種加密是俱有完美的安全性(perfect security)，亦即猜金鑰的機率和猜明文的機率是一樣。

明文 : 01101001 01110110  
金鑰 : 01100101 01111000 → XOR  
密文 : 00001100 00001110



1916-2001



# XOR 的秘密

XOR	0	1
0	0	1
1	1	0

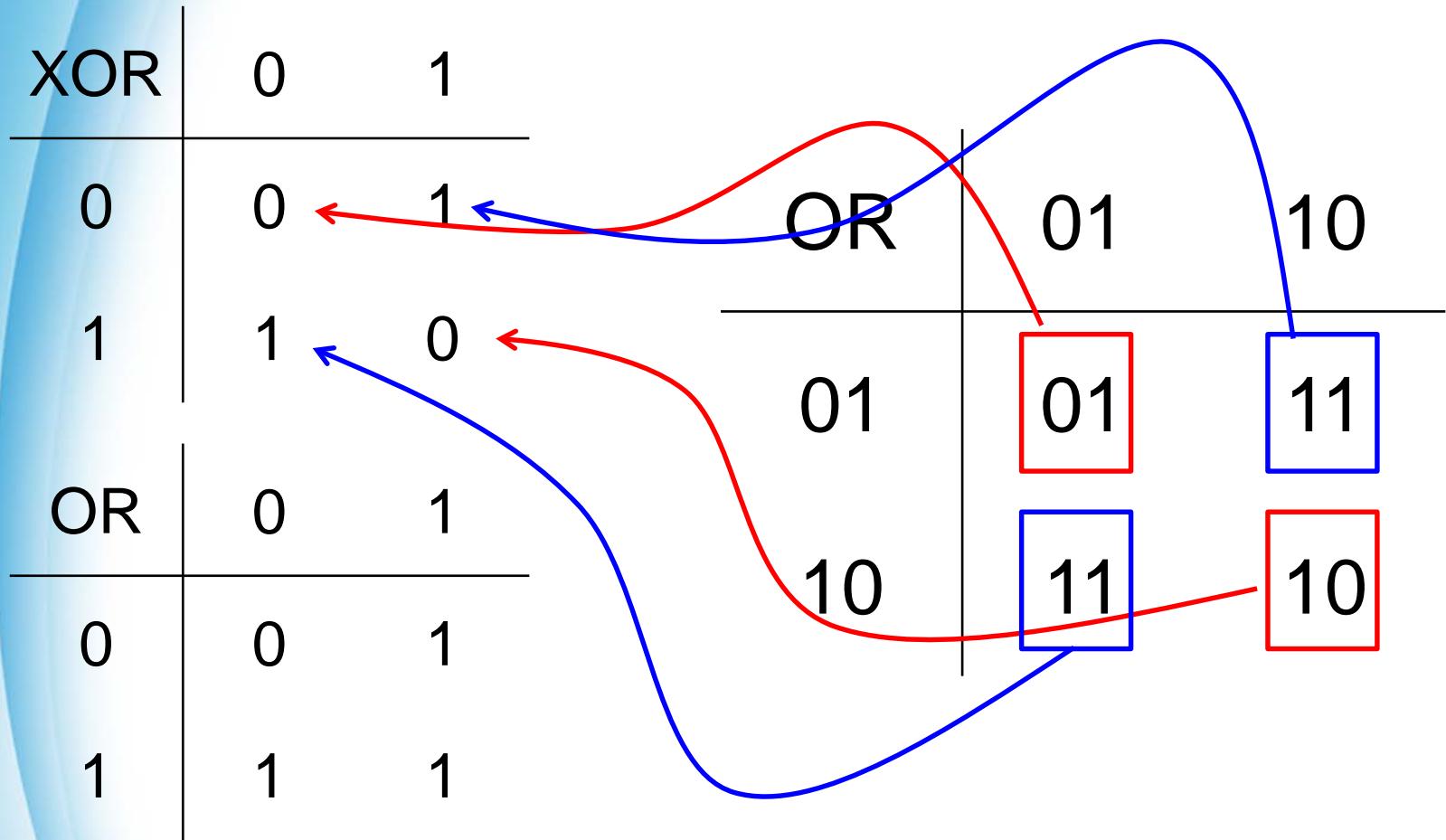
OR	0	1
0	0	1
1	1	1

AND	0	1
0	0	0
1	0	1

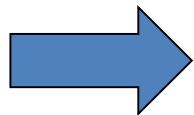


# 用OR模擬XOR

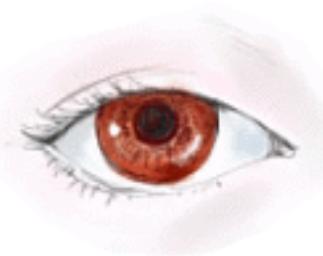


# 視覺密碼

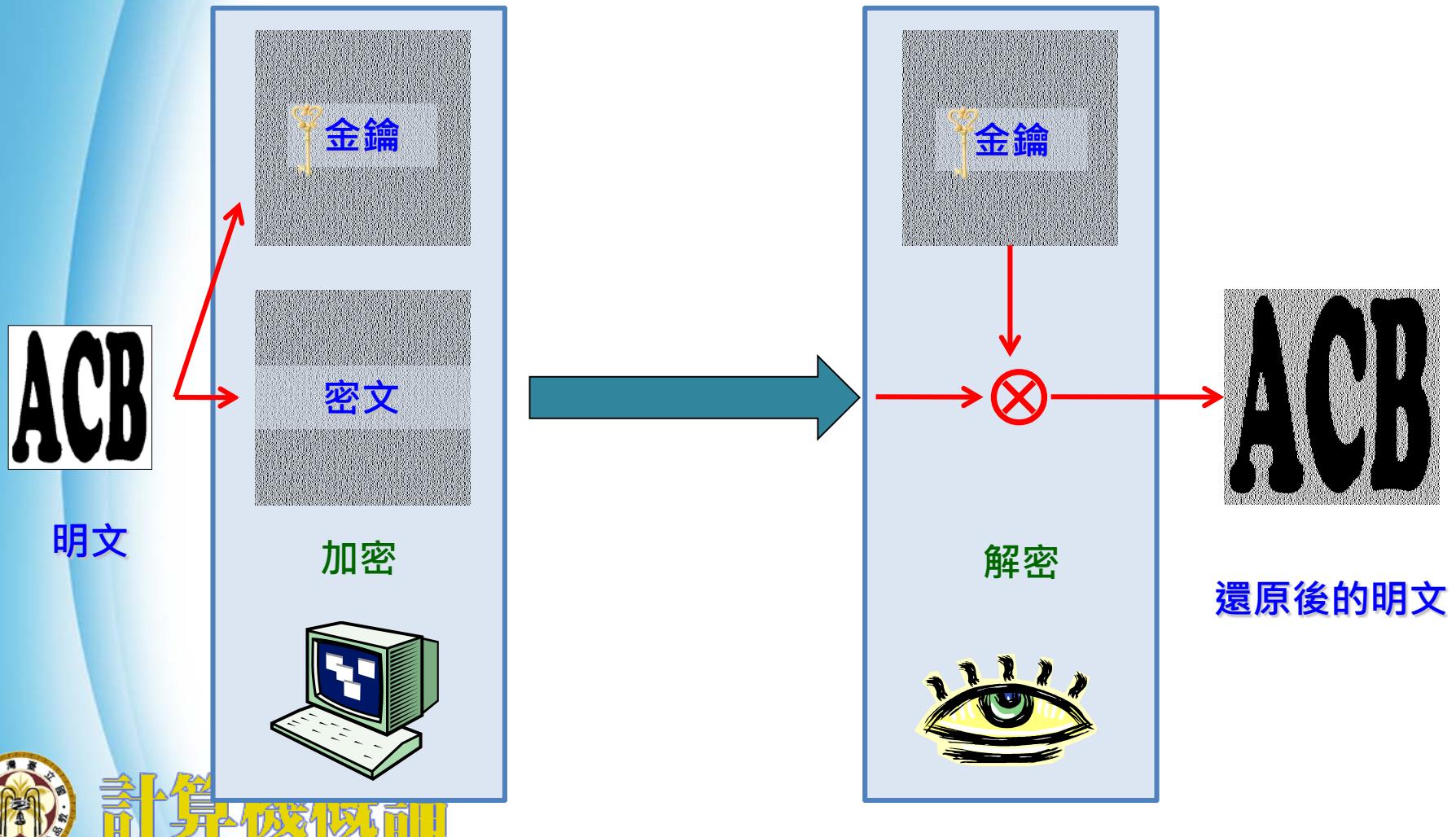
- 1995年由 Naor 和 Shamir 所提出
- 不同於傳統的密碼學，在於解密時不需要任何的計算，直接利用人的眼睛即可看出機密



解密

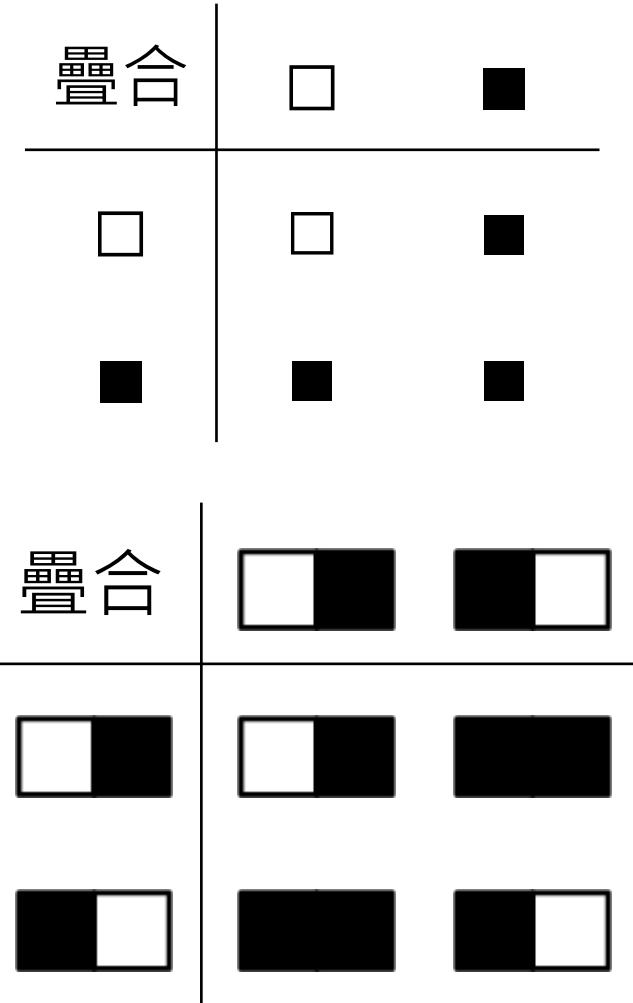


# 視覺密碼的流程

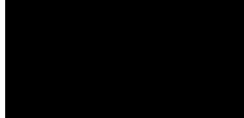
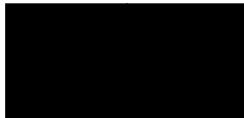


# 投影片的效果

OR	0	1
0	0	1
1	1	1



# 編碼表

$p$	$s_1$	$s_2$	$s_1+s_2$
			
			
			
			

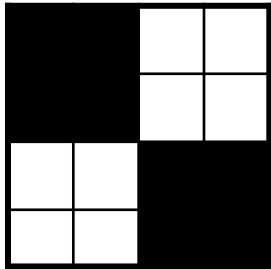


# 視覺密碼的例子

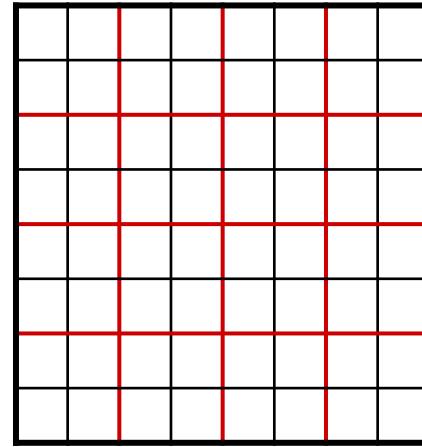
$p$	$s_1$	$s_2$	$s_1+s_2$
□			
■			

codebook

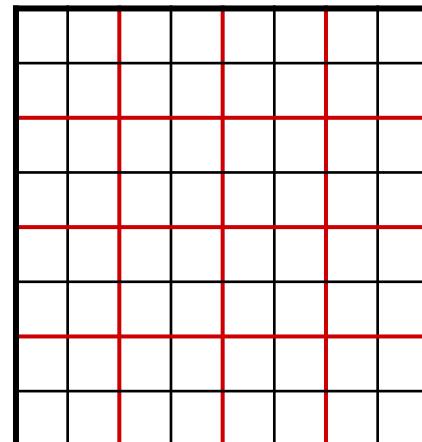
機密影像



計算機概論



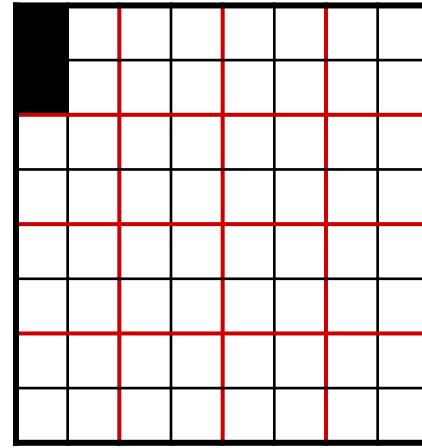
$S_1$



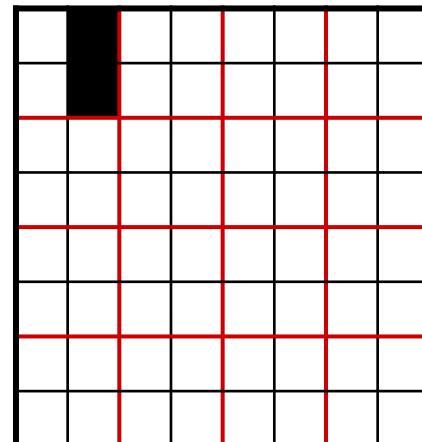
$S_2$

# 視覺密碼的例子

$p$	$s_1$	$s_2$	$s_1+s_2$
□			
			
■			
	 codebook		

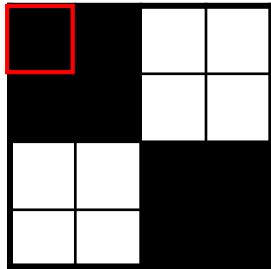


$S_1$



$S_2$

機密影像



計算機概論

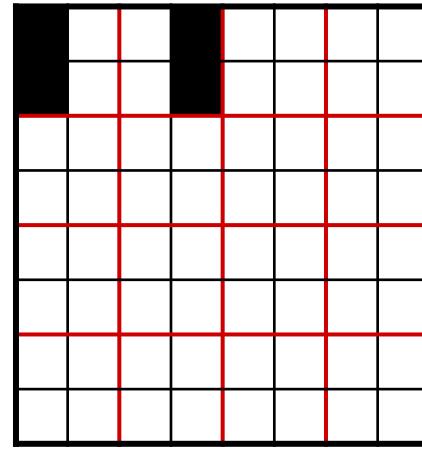
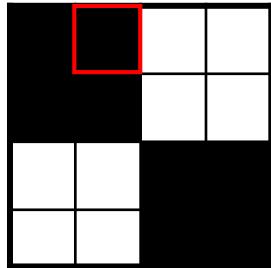


# 視覺密碼的例子

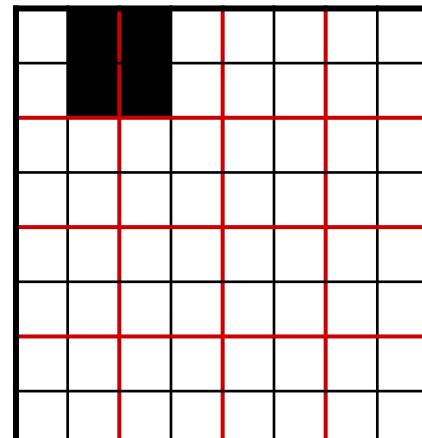
$p$	$s_1$	$s_2$	$s_1+s_2$
□			
■			
□			
■			

codebook

機密影像



$S_1$



$S_2$

計算機概論

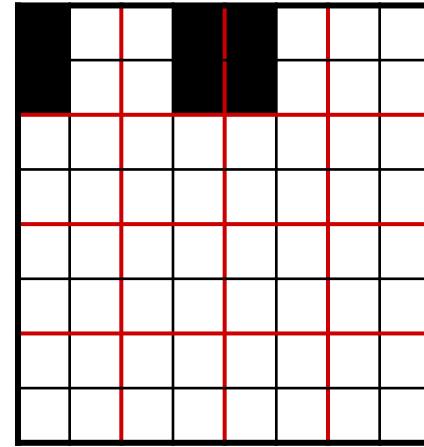
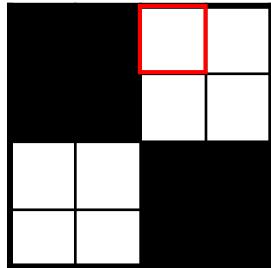


# 視覺密碼的例子

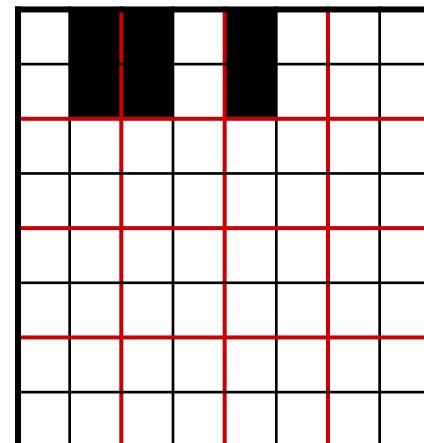
$p$	$s_1$	$s_2$	$s_1+s_2$
□			
			

codebook

機密影像



$S_1$



$S_2$

計算機概論

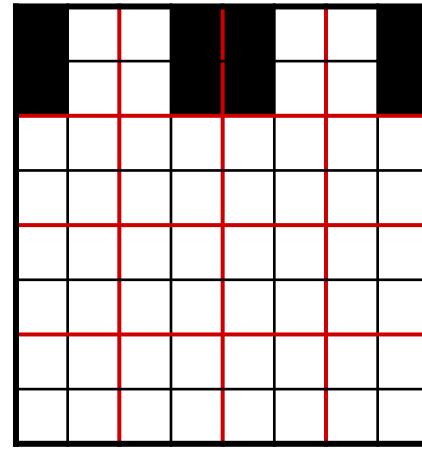
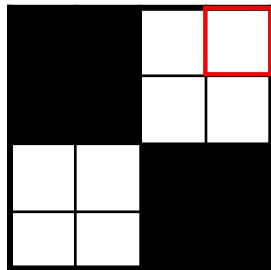


# 視覺密碼的例子

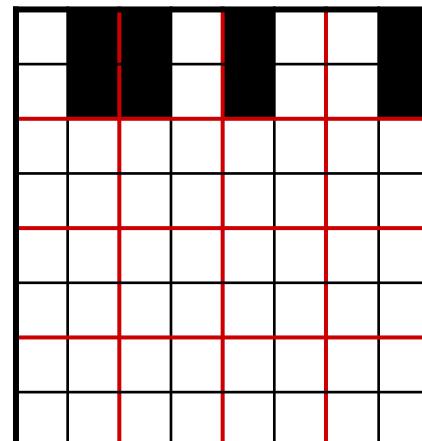
$p$	$s_1$	$s_2$	$s_1+s_2$
□			
□			
■			
■			

codebook

機密影像



$S_1$



$S_2$

計算機概論

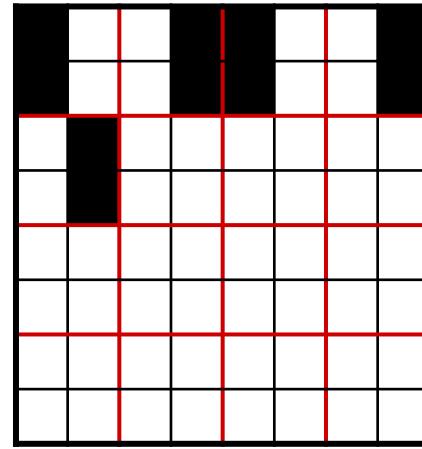
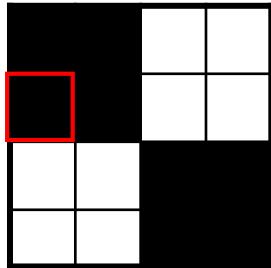


# 視覺密碼的例子

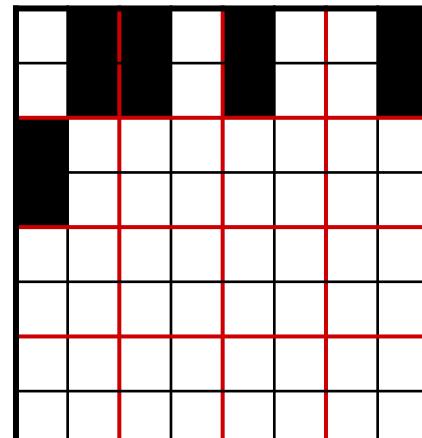
$p$	$s_1$	$s_2$	$s_1+s_2$
□			
■			
□			
■			

codebook

機密影像



$S_1$



$S_2$

計算機概論

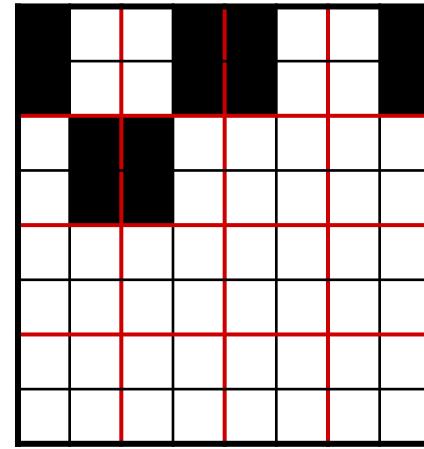
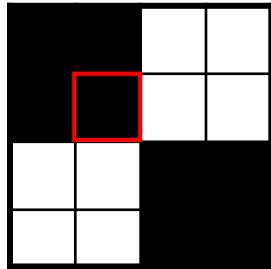


# 視覺密碼的例子

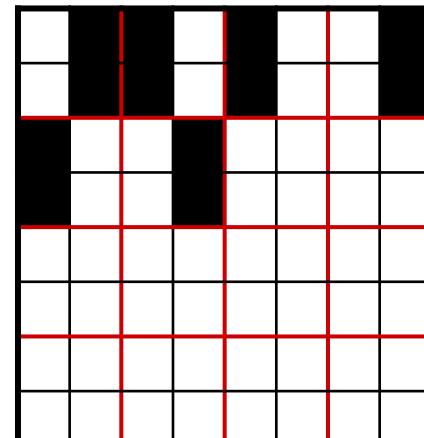
$p$	$s_1$	$s_2$	$s_1+s_2$
□			
■			

codebook

機密影像



$S_1$



$S_2$

計算機概論

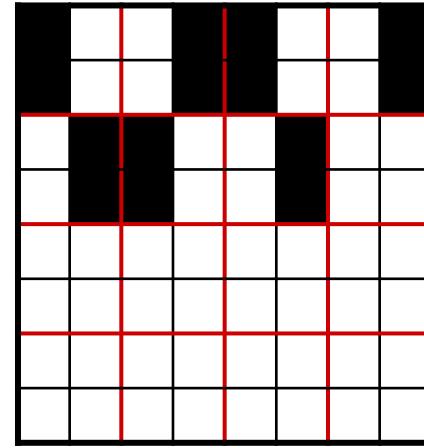
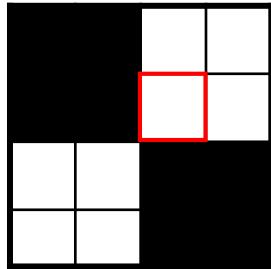


# 視覺密碼的例子

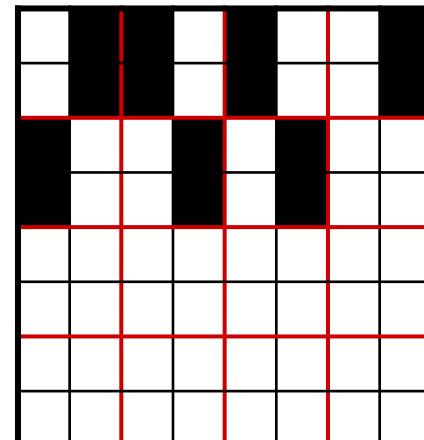
$p$	$s_1$	$s_2$	$s_1+s_2$
□			
□			
■			
■			

codebook

機密影像



$S_1$



$S_2$

計算機概論

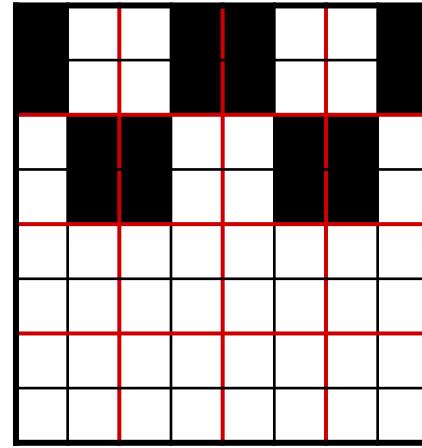
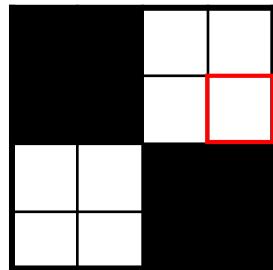


# 視覺密碼的例子

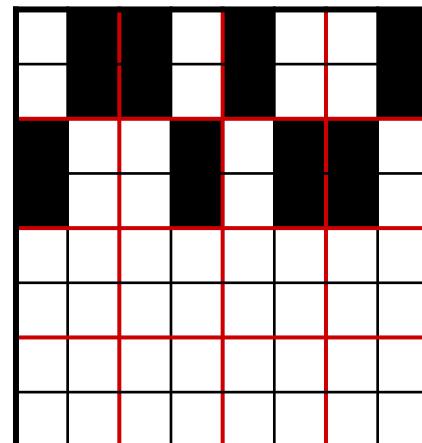
$p$	$s_1$	$s_2$	$s_1+s_2$
□			

codebook

機密影像



$S_1$



$S_2$

計算機概論

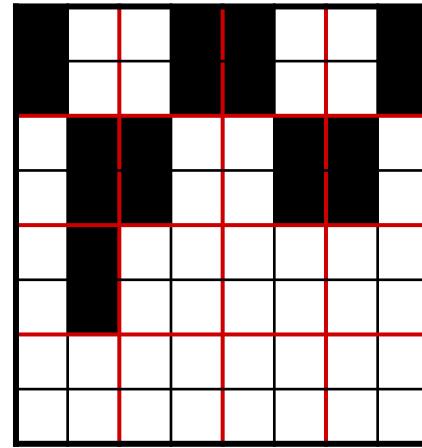
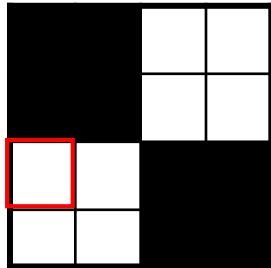


# 視覺密碼的例子

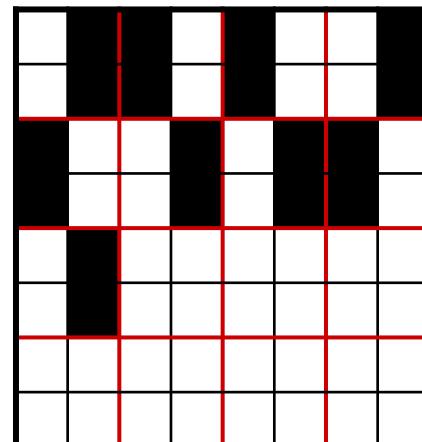
$p$	$s_1$	$s_2$	$s_1+s_2$
□			
□			
■			
■			

codebook

機密影像



$S_1$



$S_2$

計算機概論

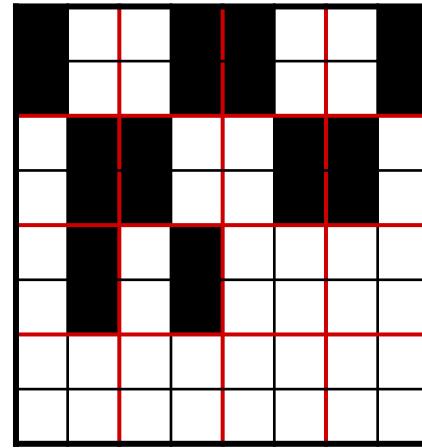
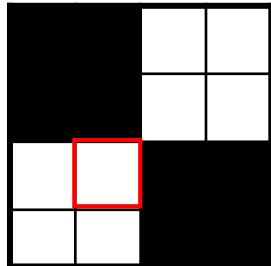


# 視覺密碼的例子

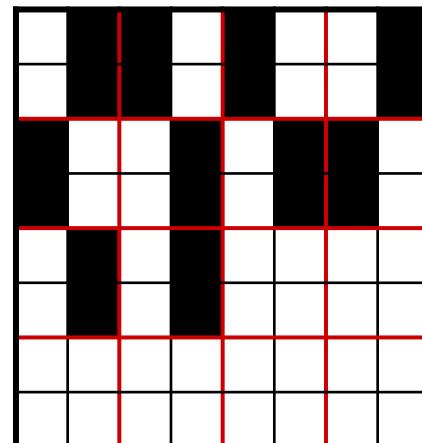
$p$	$s_1$	$s_2$	$s_1+s_2$
□			
□			
■			
■			

codebook

機密影像



$S_1$



$S_2$

計算機概論

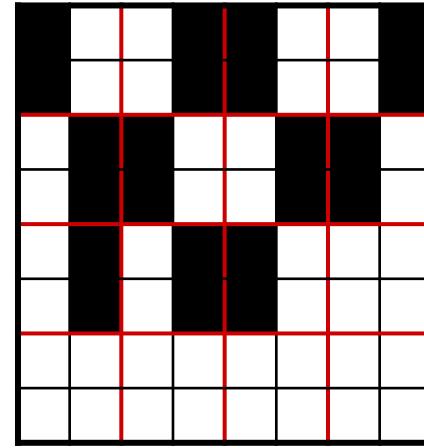
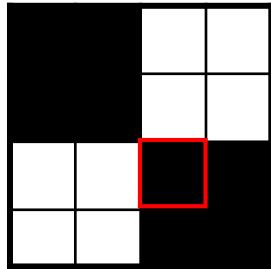


# 視覺密碼的例子

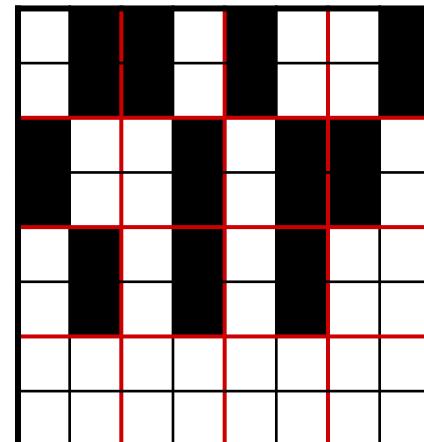
$p$	$s_1$	$s_2$	$s_1+s_2$
□			
■			

codebook

機密影像



$S_1$



$S_2$

計算機概論

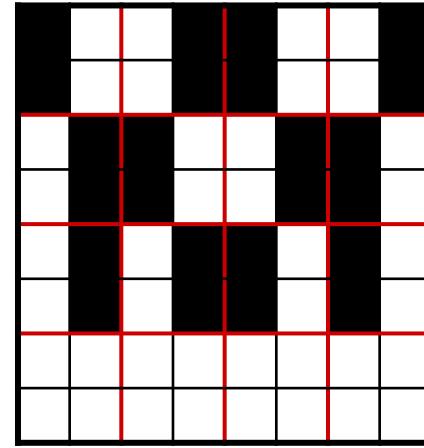
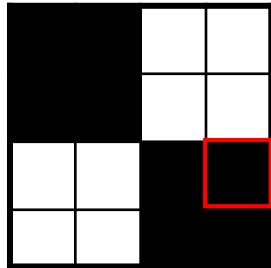


# 視覺密碼的例子

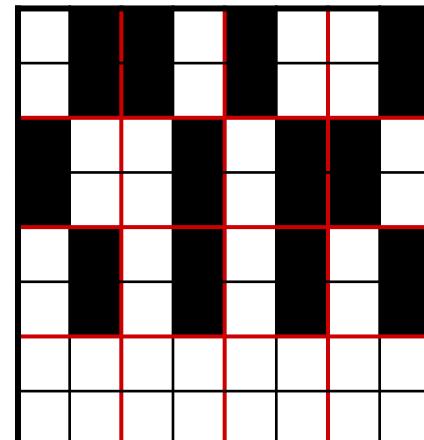
$p$	$s_1$	$s_2$	$s_1+s_2$
□			
■			

codebook

機密影像



$S_1$



$S_2$



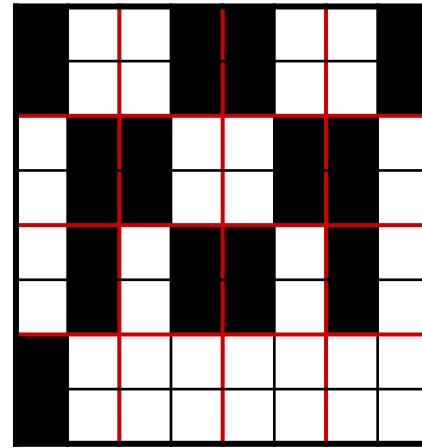
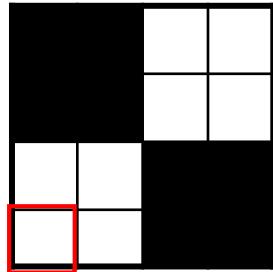
計算機概論

# 視覺密碼的例子

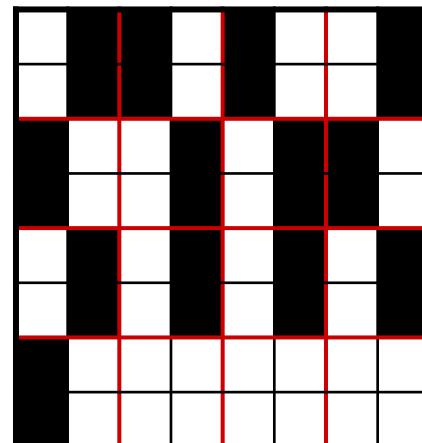
$p$	$s_1$	$s_2$	$s_1+s_2$
□			

codebook

機密影像



$S_1$



$S_2$

計算機概論

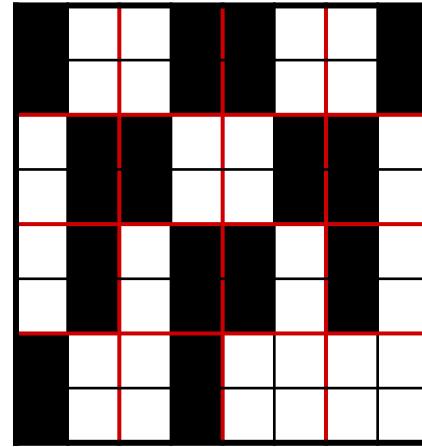
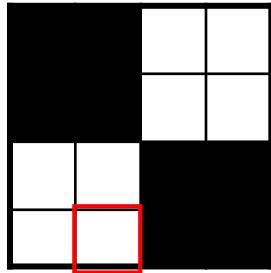


# 視覺密碼的例子

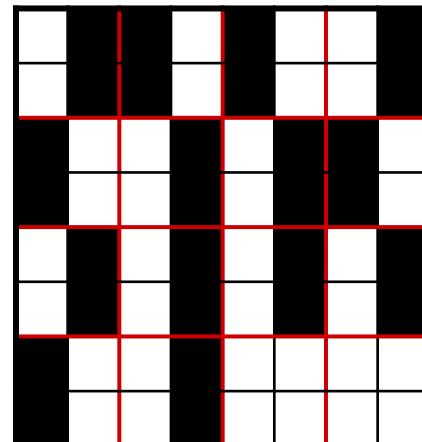
$p$	$s_1$	$s_2$	$s_1+s_2$
□			
■			
□			
■			

codebook

機密影像



$S_1$



$S_2$

計算機概論

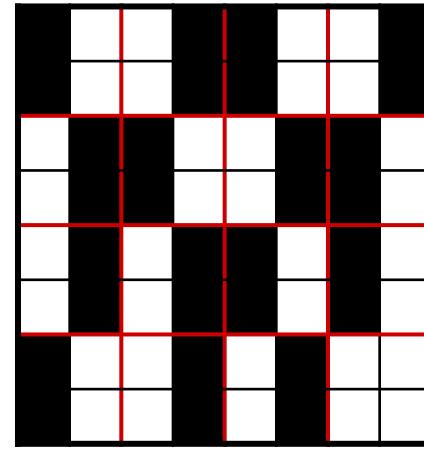
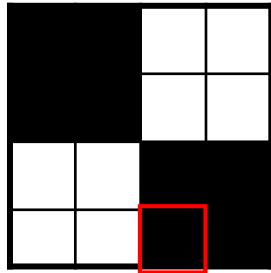


# 視覺密碼的例子

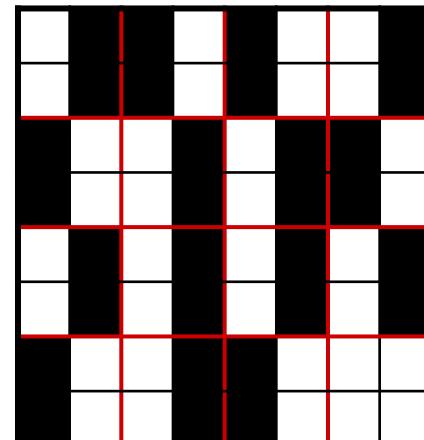
$p$	$s_1$	$s_2$	$s_1+s_2$
□			
■			

codebook

機密影像



$S_1$



$S_2$

計算機概論

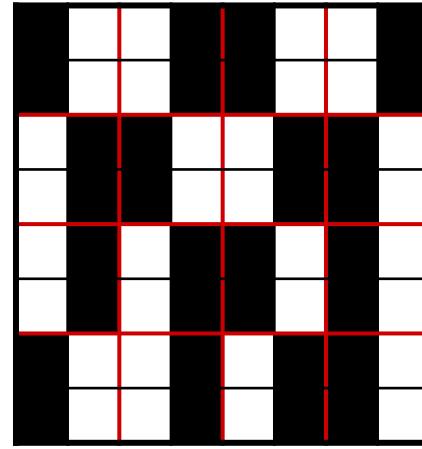
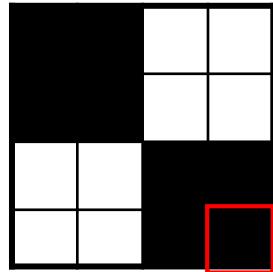


# 視覺密碼的例子

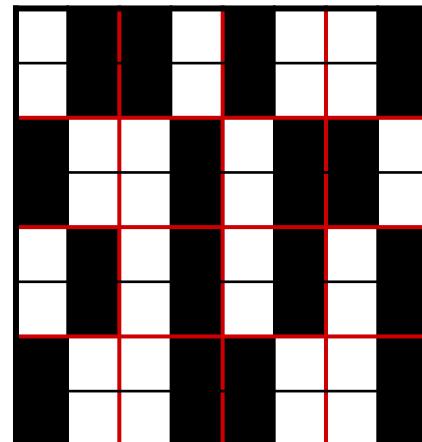
$p$	$s_1$	$s_2$	$s_1+s_2$
□			
■			
	(highlighted by red box)		

codebook

機密影像



$S_1$



$S_2$

計算機概論

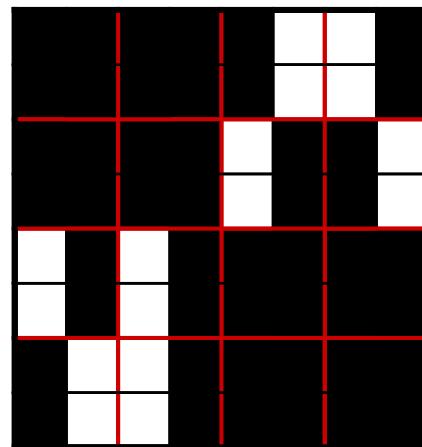
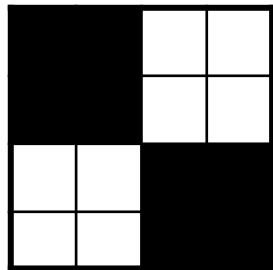


# 視覺密碼的例子

$p$	$s_1$	$s_2$	$s_1+s_2$
□			
■			

codebook

機密影像



$s_1$



$s_2$



計算機概論

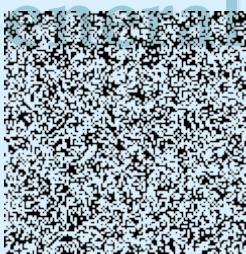
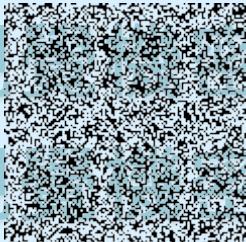
# 視覺機密分享

- $(2, 2)$  視覺機密分享機制
- $(n, n)$  視覺機密分享機制
- $(k, n)$  視覺機密分享機制
- GAS(General Access Structure)視覺機密分享機制



# 視覺機密分享

- $(2, 2)$  視覺機密分享機制
- $(n, n)$  視覺機密分享機制
- $(k, n)$  視覺機密分享機制
- GAS(General Access Structure) 視覺機密分享機制



Access Structure

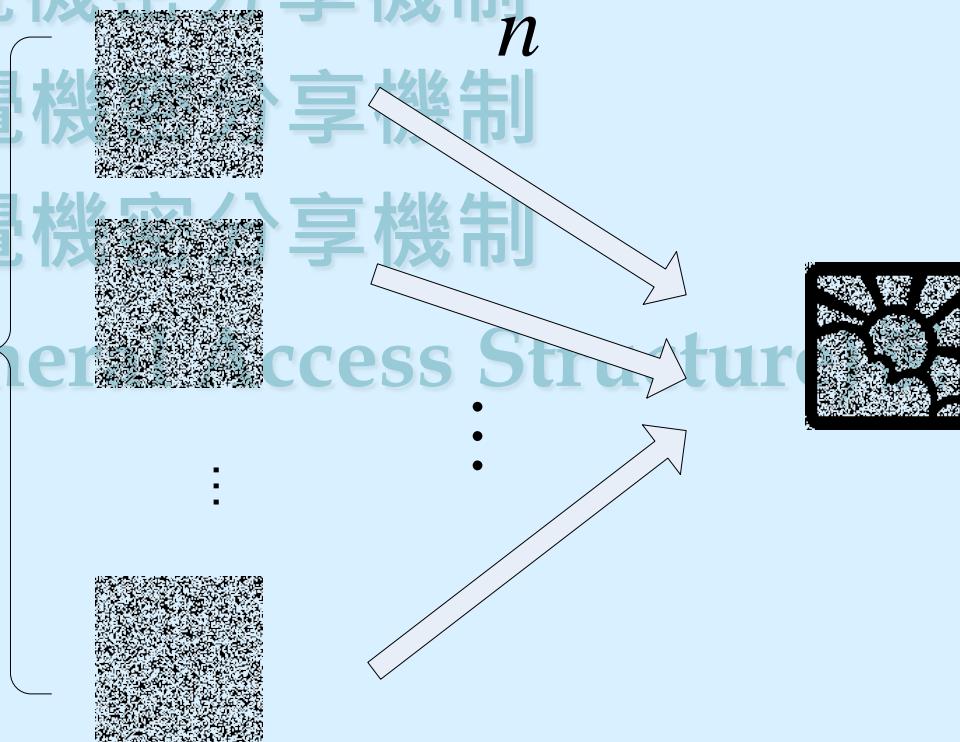


視覺機密分



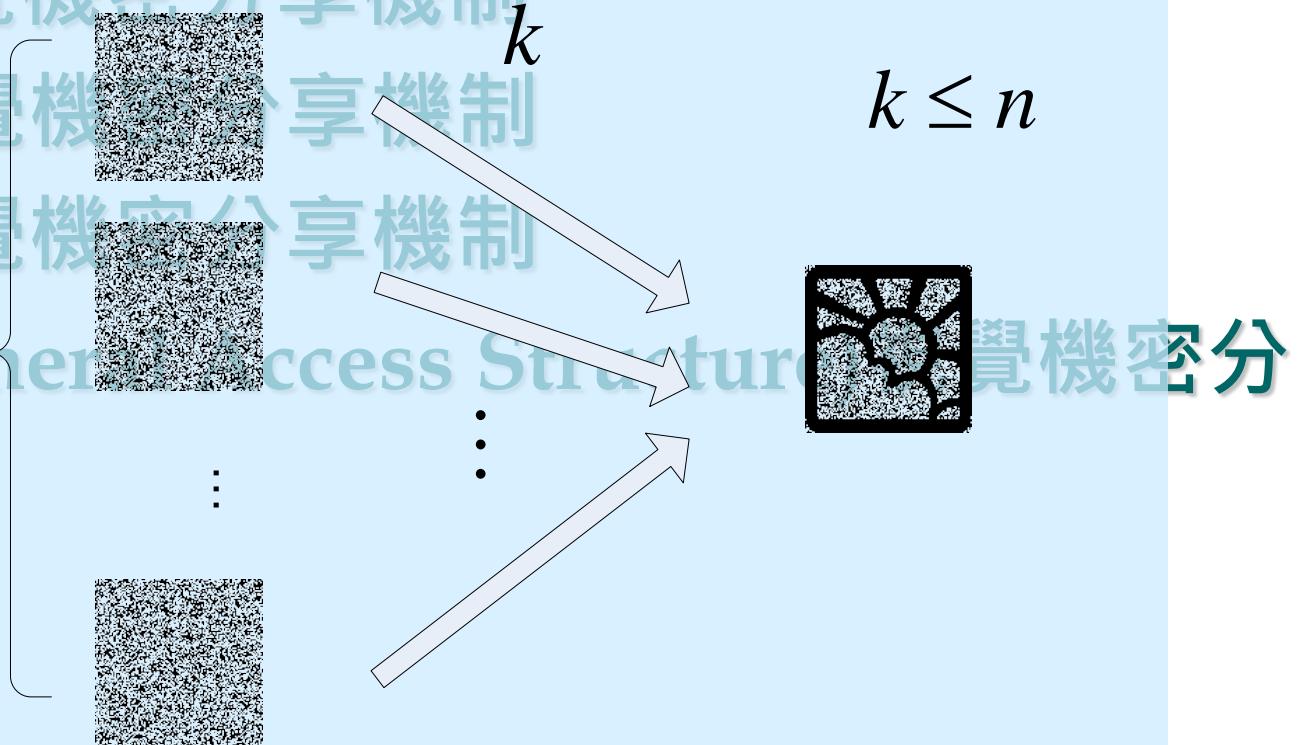
# 視覺機密分享

- $(2, 2)$  視覺機密分享機制
- $(n, n)$  視覺機密分享機制
- $(k, n)$  視覺機密分享機制
- GAS(General Access Structure) 視覺機密分享機制



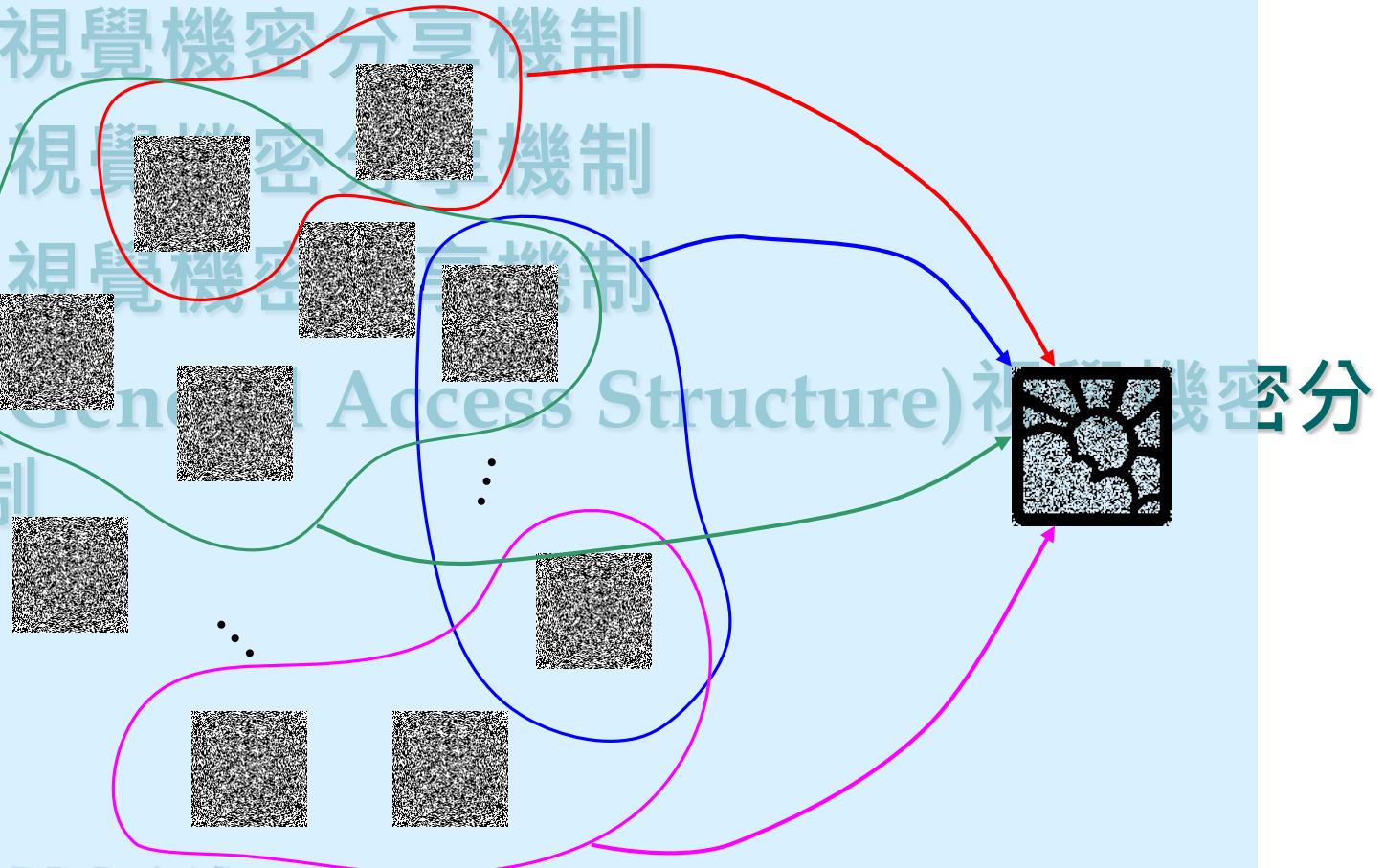
# 視覺機密分享

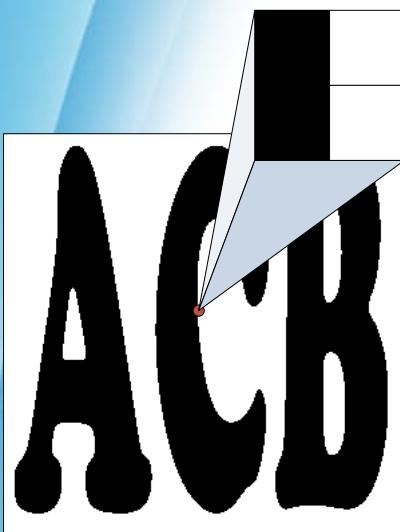
- $(2, 2)$  視覺機密分享機制
- $(n, n)$  視覺機密分享機制
- $(k, n)$  視覺機密分享機制
- GAS(General Access Structure) 視覺機密分享機制



# 視覺機密分享

- $(2, 2)$  視覺機密分享機制
- $(n, n)$  視覺機密分享機制
- $(k, n)$  視覺機密分享機制
- GAS(General Access Structure)視覺機密分享機制





機密影像

$$S_0 \in C_0 \quad \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$
$$S_1 \in C_1 \quad \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

計算機概論

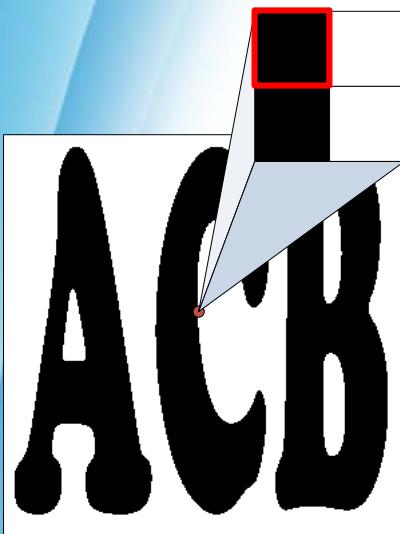










機密影像

$$S_0 \in C_0 \quad \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

$$S_1 \in C_1 \quad \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$



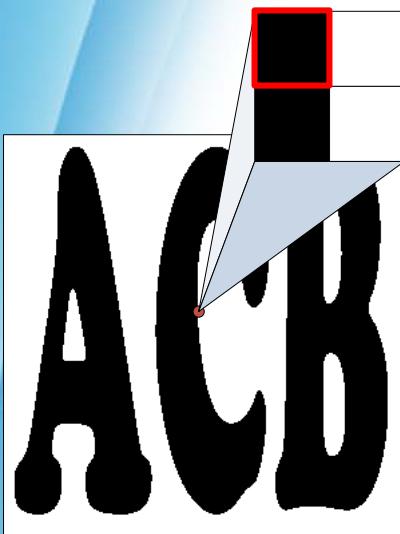
計算機概論









機密影像

$$S_0 \in C_0 \quad \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

$$S_1 \in C_1 \quad \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

計算機概論

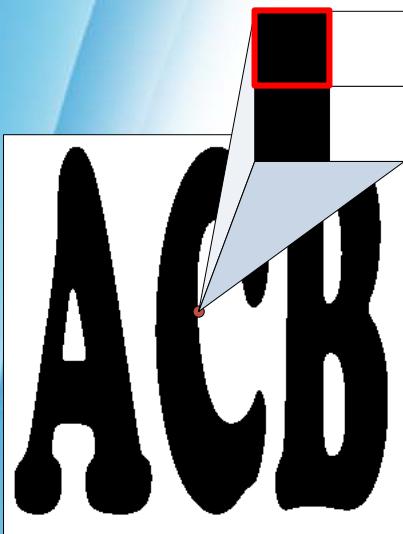










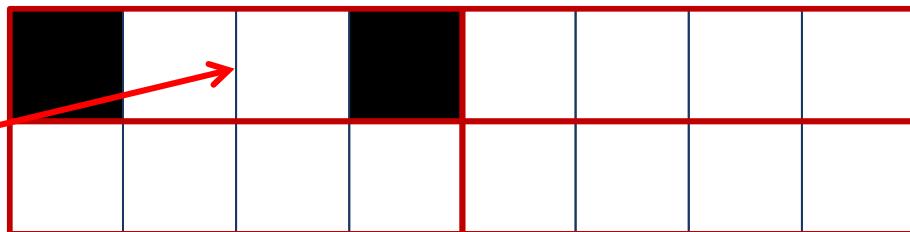
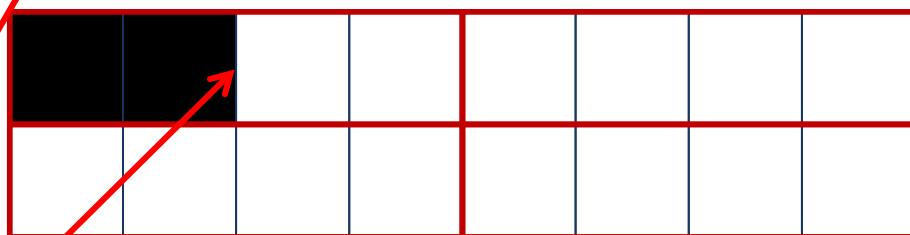
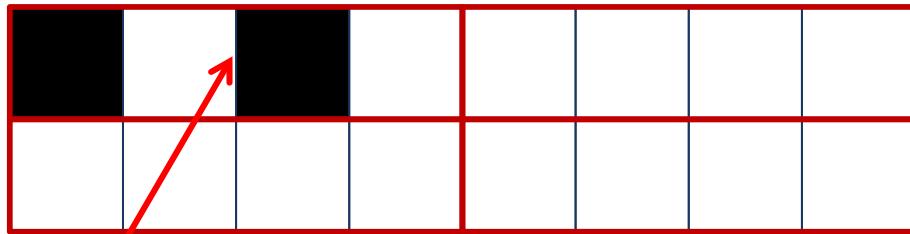
機密影像

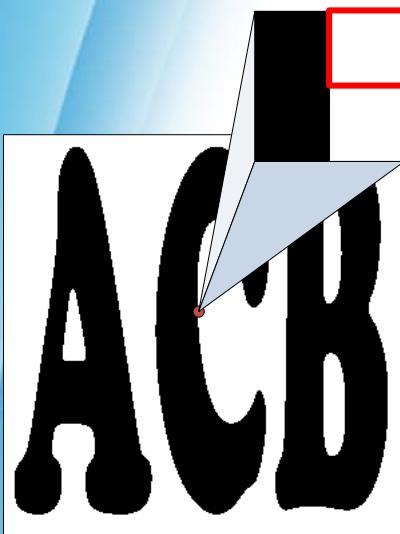
$$S_0 \in C_0$$

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



計算機概論





機密影像

$$S_0 \in C_0 \quad \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

$$S_1 \in C_1 \quad \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

計算機概論



Black	White	Black	White				
White							

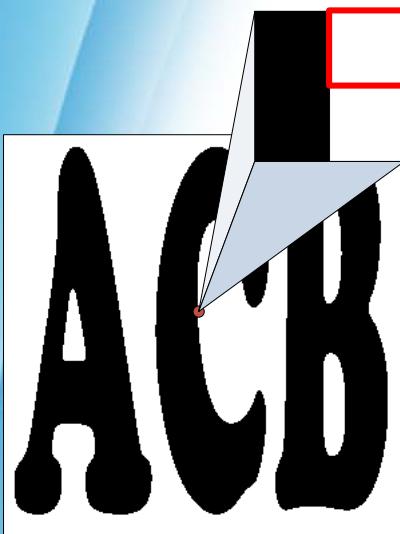


Black	Black						
White							



Black			Black				
White			White				





機密影像

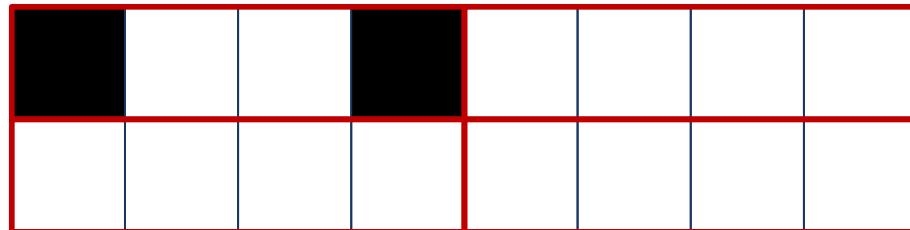
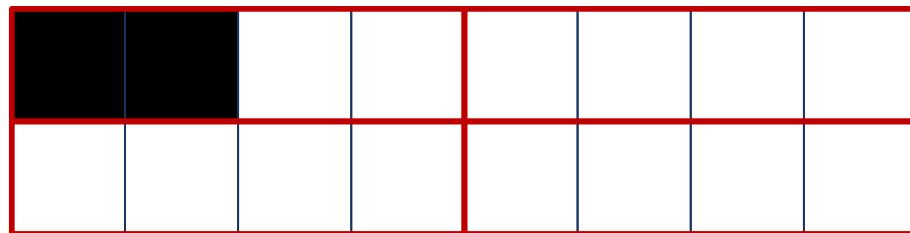
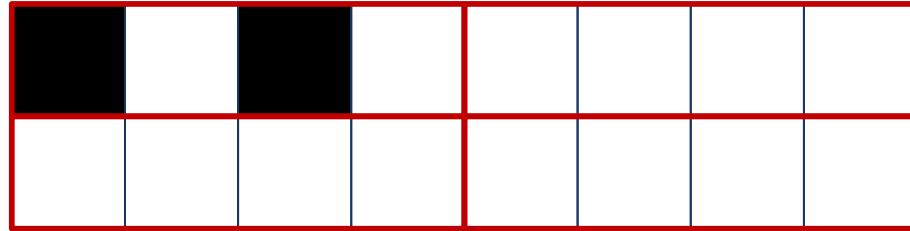
$$S_0 \in C_0$$

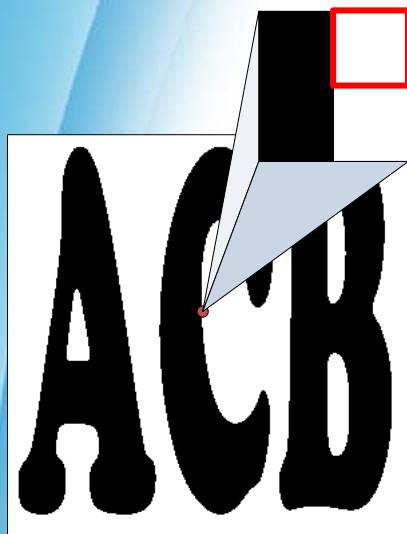
$$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$S_1 \in C_1$$

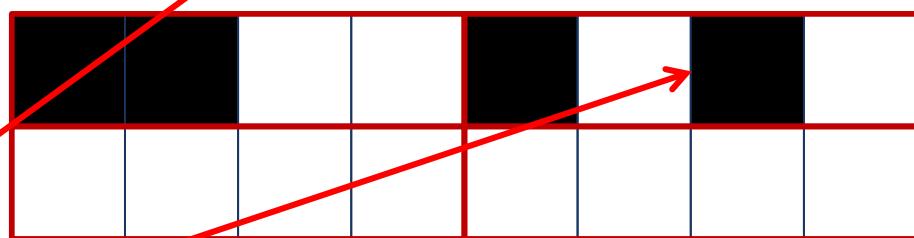
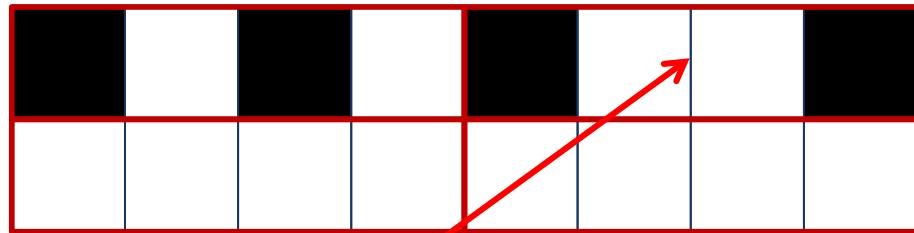
$$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

計算機概論





機密影像



$1$	$0$	$0$	$1$
$1$	$0$	$1$	$0$
$0$	$0$	$1$	$1$
$1$	$0$	$1$	$0$
$1$	$1$	$0$	$0$
$1$	$0$	$0$	$1$

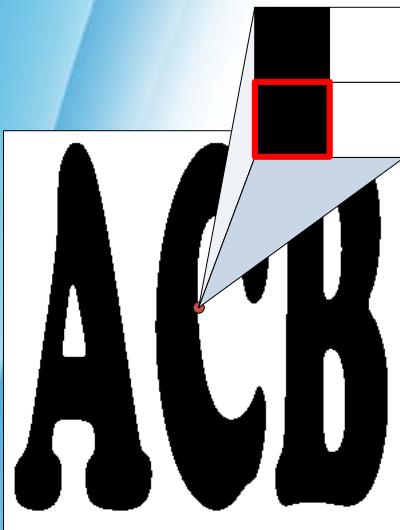
$S_0 \in C_0$

$S_1 \in C_1$



計算機概論





機密影像

$$S_0 \in C_0 \quad \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

$$S_1 \in C_1 \quad \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

計算機概論



Black	White	Black	White	Black	White	Black
White						

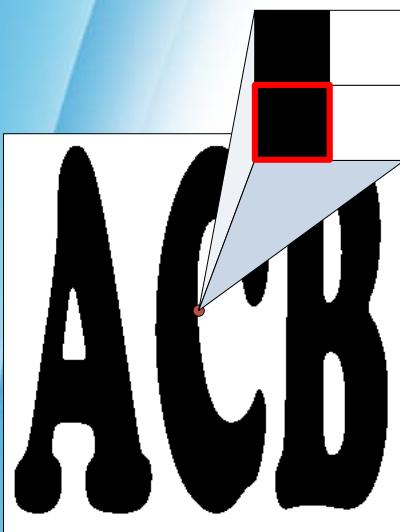


Black	Black	White	White	Black	Black
White	White	White	White	White	White



Black	White	White	Black	White	Black	Black
White						



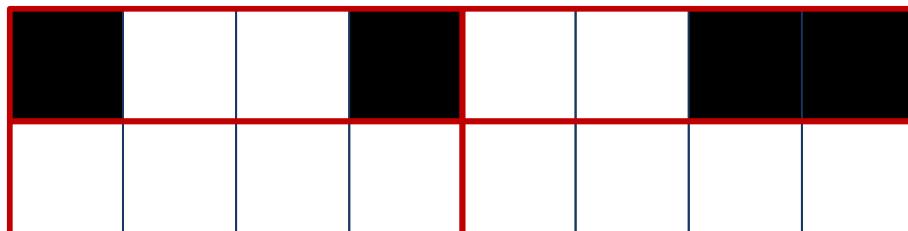
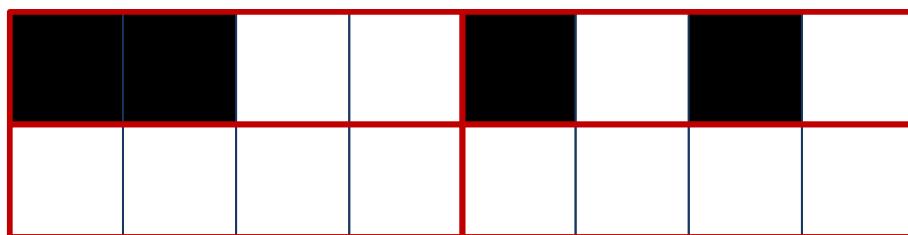
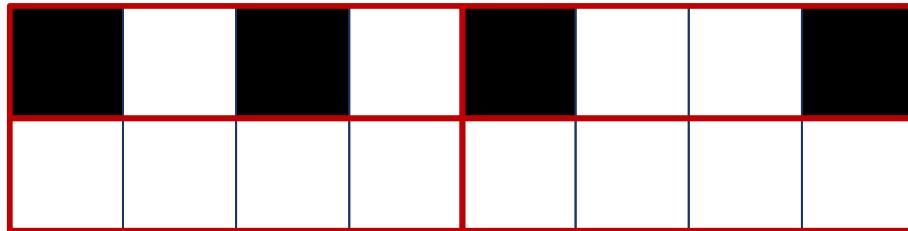


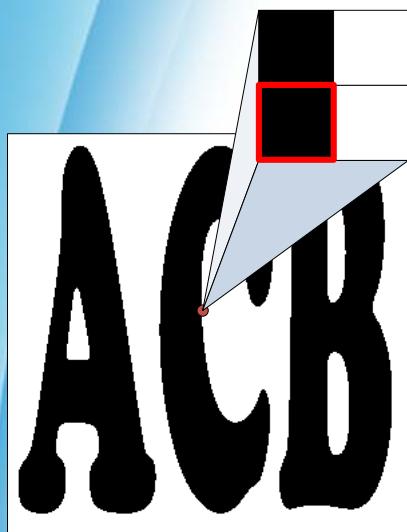
機密影像

$$S_0 \in C_0 \quad \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

$$S_1 \in C_1 \quad \boxed{\begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}}$$

計算機概論





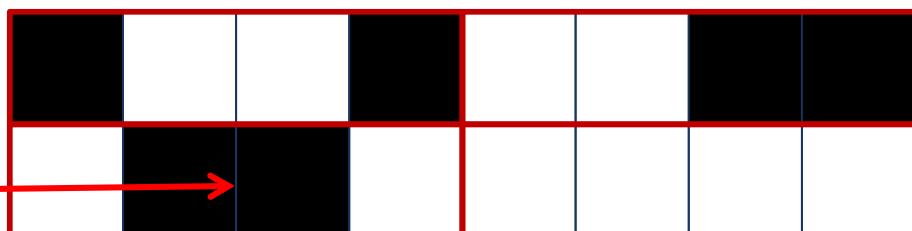
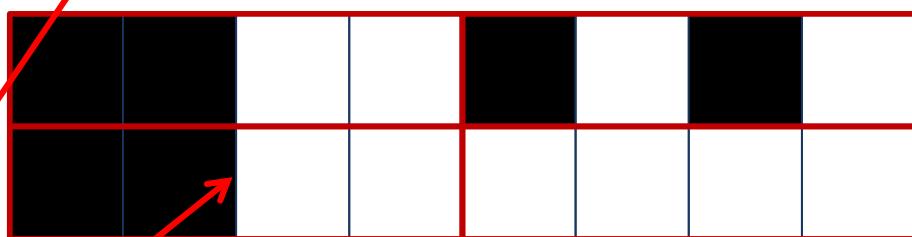
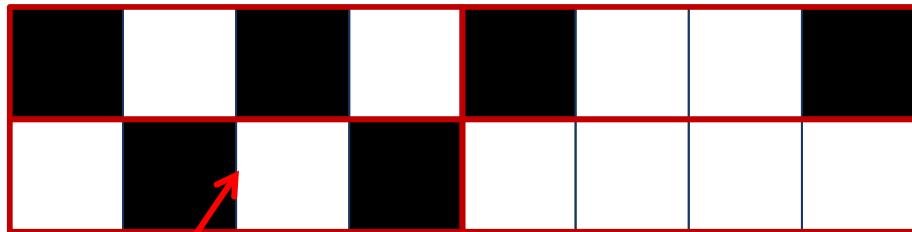
機密影像

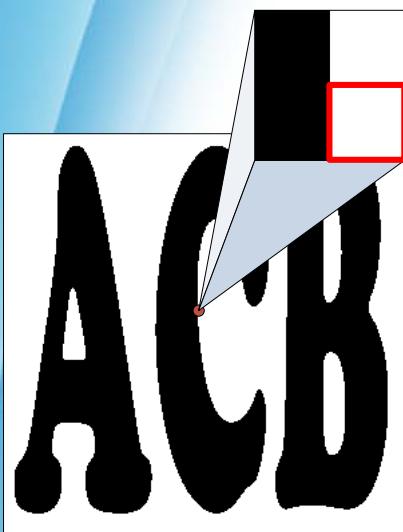
$$S_0 \in C_0$$

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



計算機概論



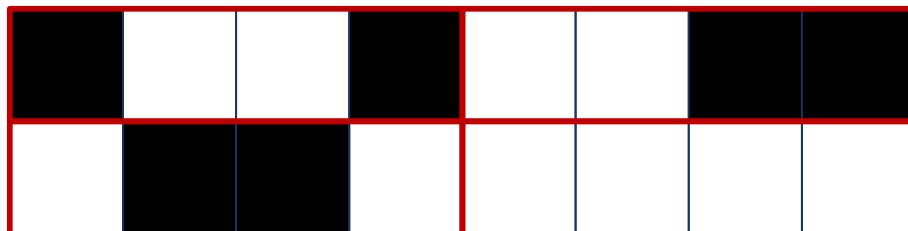
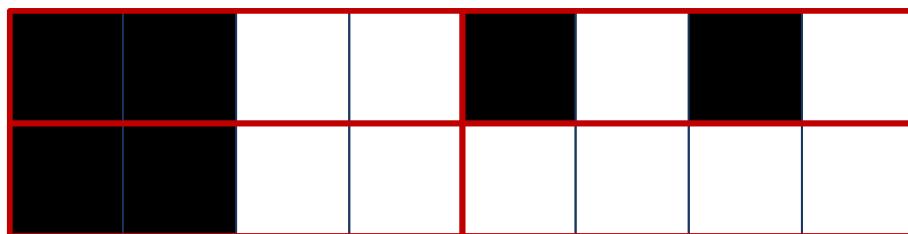
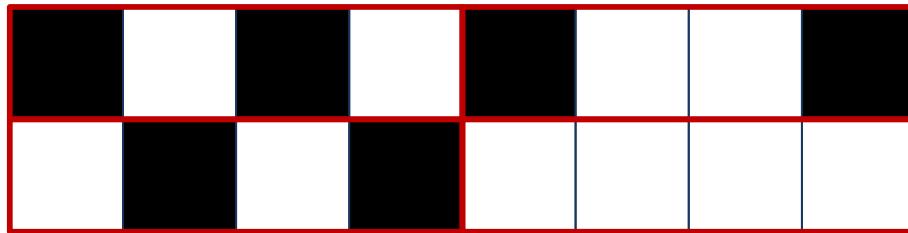


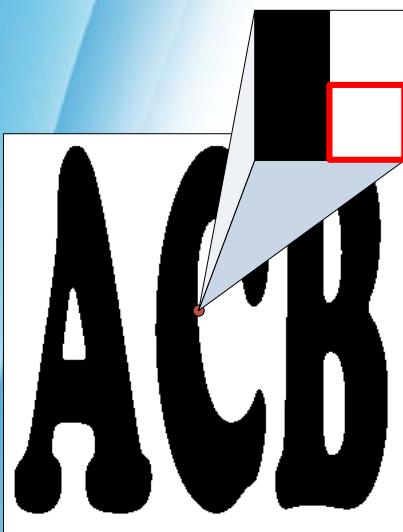
機密影像

$$S_0 \in C_0 \quad \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

$$S_1 \in C_1 \quad \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

計算機概論





機密影像

$S_0 \in C_0$

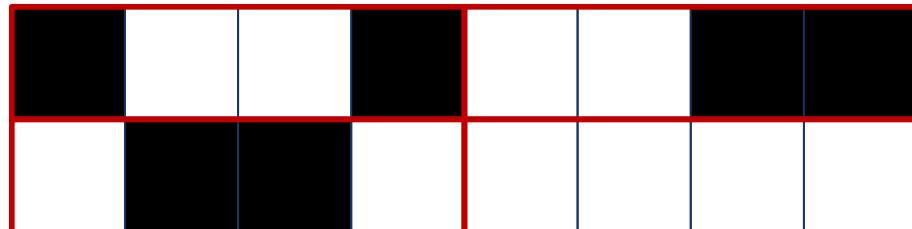
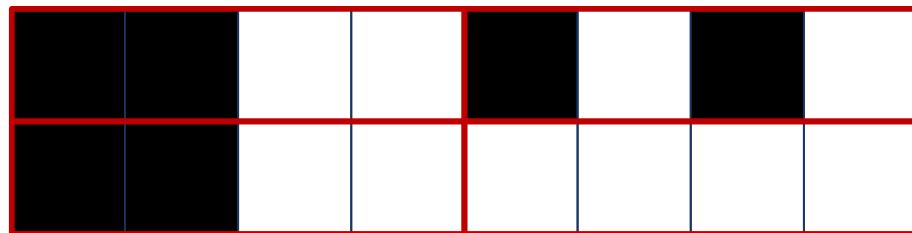
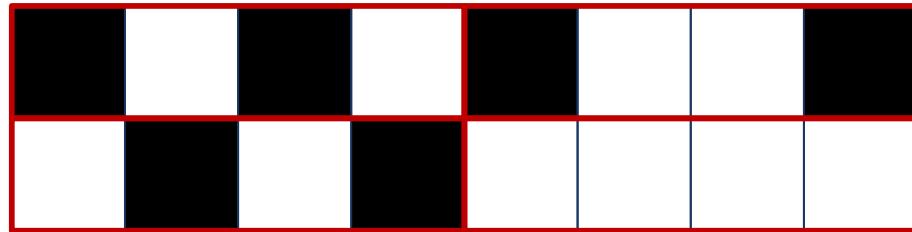
$$\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

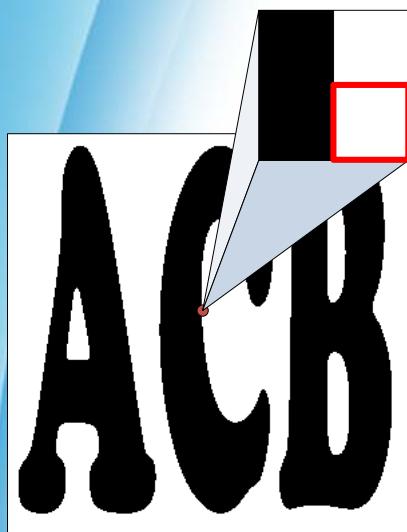
$S_1 \in C_1$

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

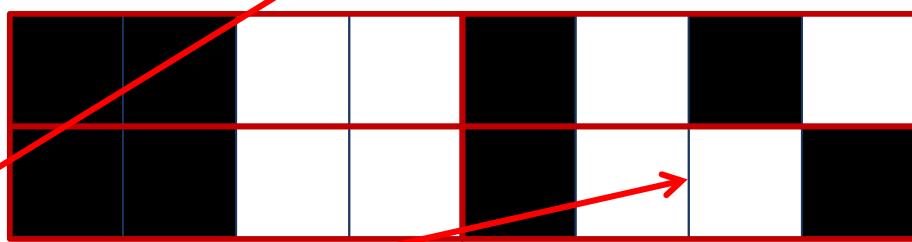
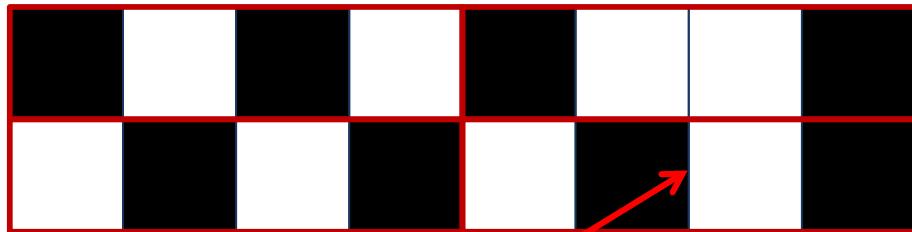


# 計算機概論





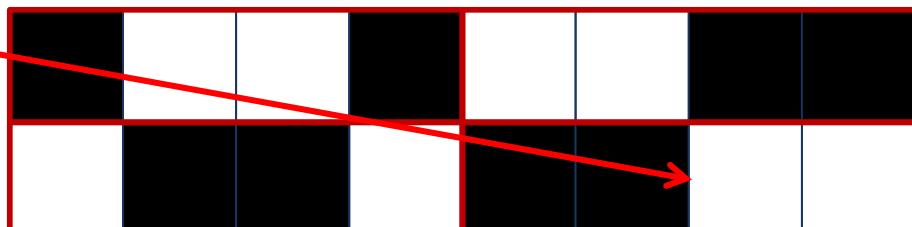
機密影像



0	1	0	1
1	0	0	1
1	1	0	0
0	1	0	1
1	1	0	0
0	1	1	0

$S_0 \in C_0$

$S_1 \in C_1$



計算機概論

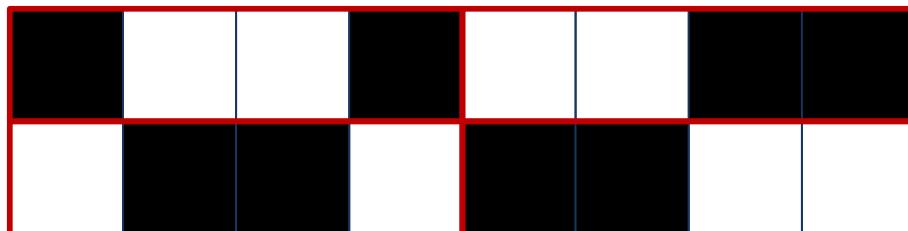
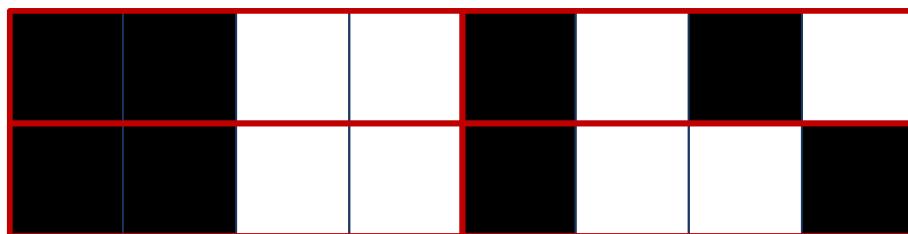
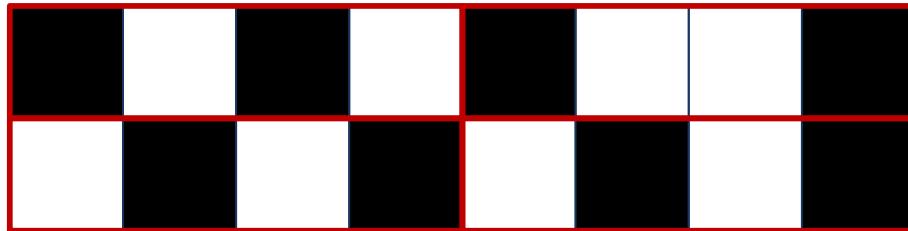


機密影像

$$S_0 \in C_0 \quad \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

$$S_1 \in C_1 \quad \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

計算機概論

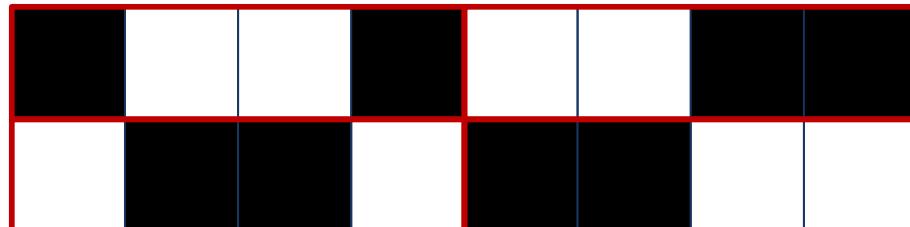
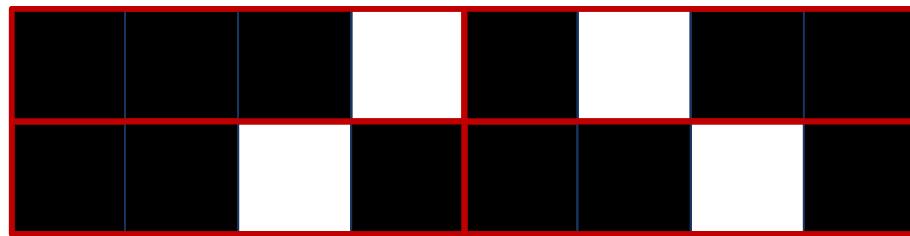


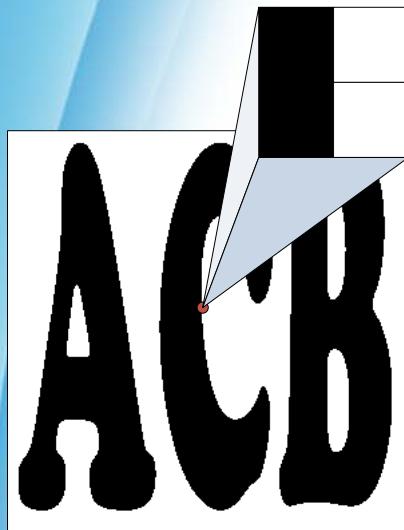


機密影像

$$S_0 \in C_0 \quad \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$
$$S_1 \in C_1 \quad \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

計算機概論





機密影像

$$S_0 \in C_0 \quad \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$
$$S_1 \in C_1 \quad \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

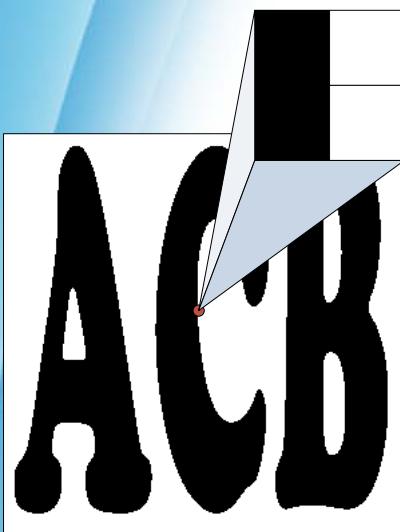
計算機概論



■	■	■	■	■	■	■
■	■	■	■	■	■	■



■	■	■	■	■	■	■
■	■	■	■	■	■	■



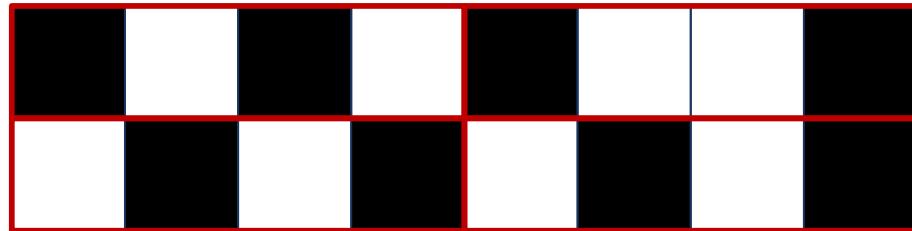
機密影像

$$S_0 \in C_0 \quad \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

$$S_1 \in C_1 \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$



計算機概論



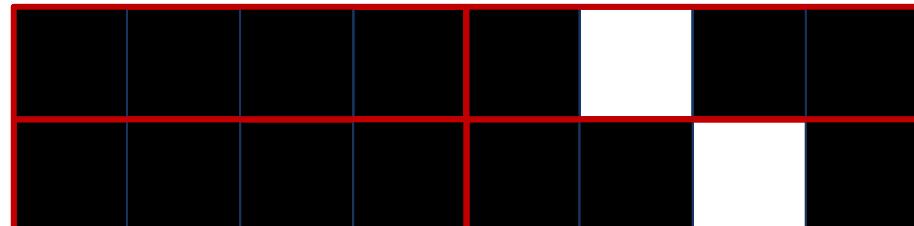


機密影像

$$S_0 \in C_0 \quad \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$
$$S_1 \in C_1 \quad \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$



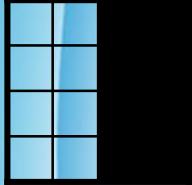
計算機概論



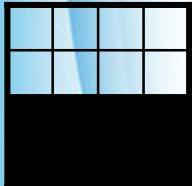
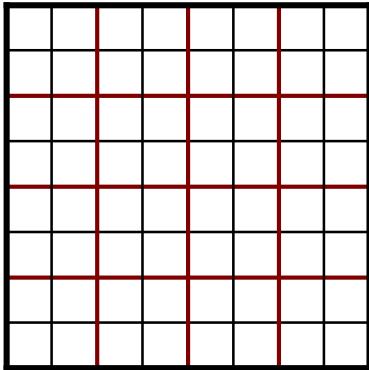
# 旋轉式視覺密碼

(Wu and Chen, 1998)

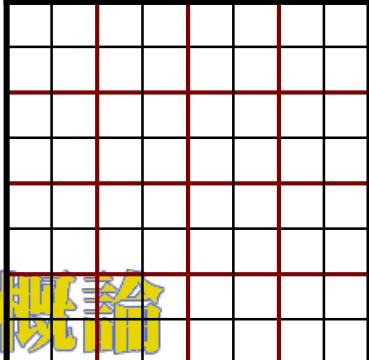
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



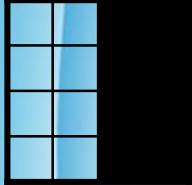
計算機視聽



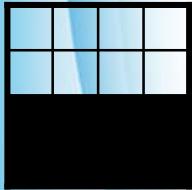
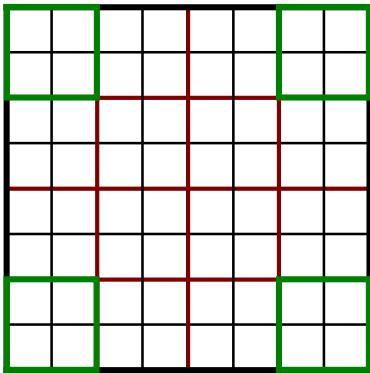
# 旋轉式視覺密碼

(Wu and Chen, 1998)

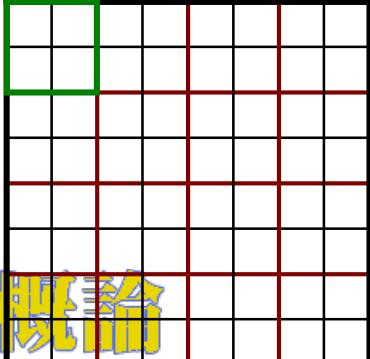
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



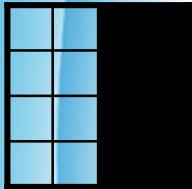
計算機視聽



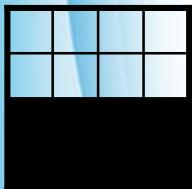
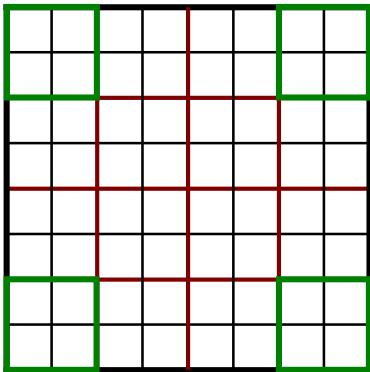
# 旋轉式視覺密碼

(Wu and Chen, 1998)

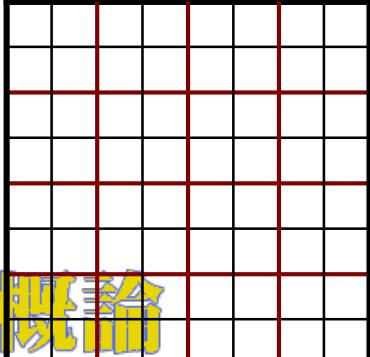
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	□	□	■	□	■	□	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



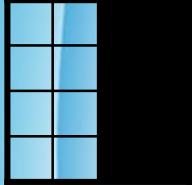
計算機視聽



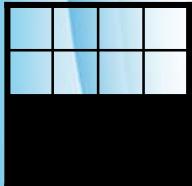
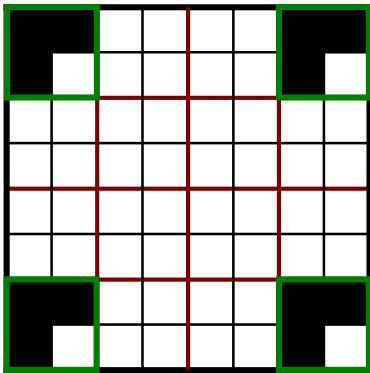
# 旋轉式視覺密碼

(Wu and Chen, 1998)

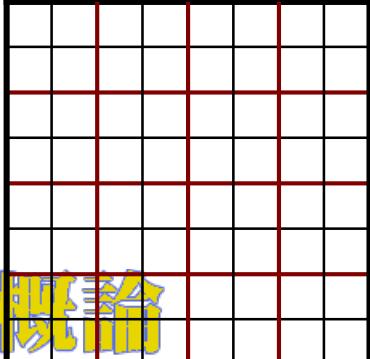
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	□	□	■	□	■	□	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



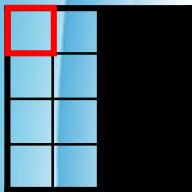
計算機視聽



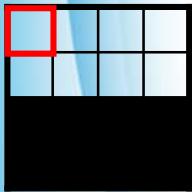
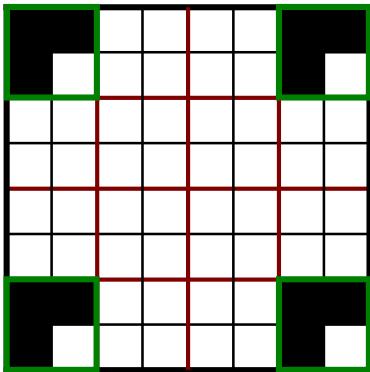
# 旋轉式視覺密碼

(Wu and Chen, 1998)

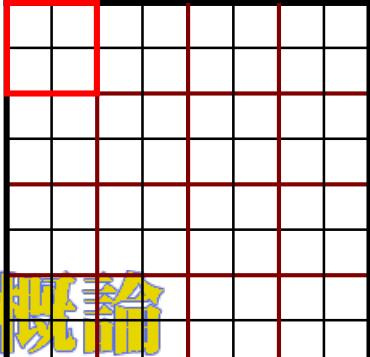
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	□	□	■	□	■	□	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



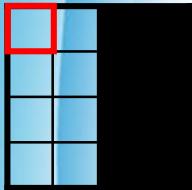
計算機視聽



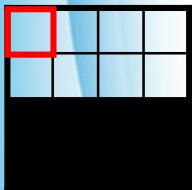
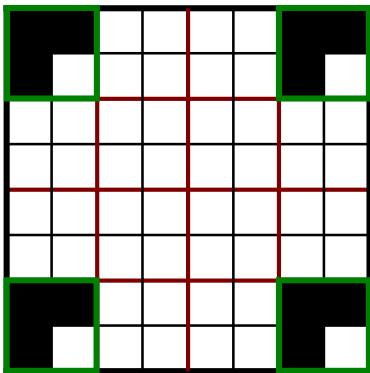
# 旋轉式視覺密碼

(Wu and Chen, 1998)

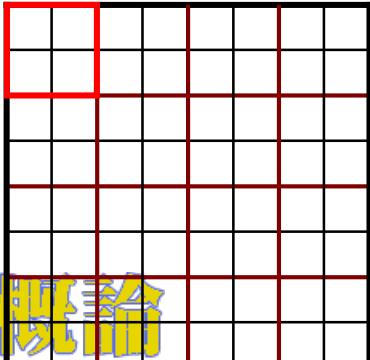
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	□	□	■	■	□	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



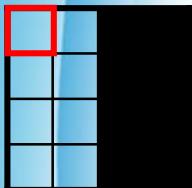
計算機視聽



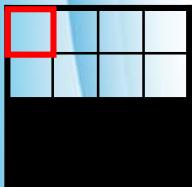
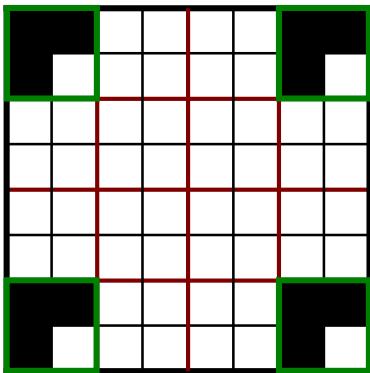
# 旋轉式視覺密碼

(Wu and Chen, 1998)

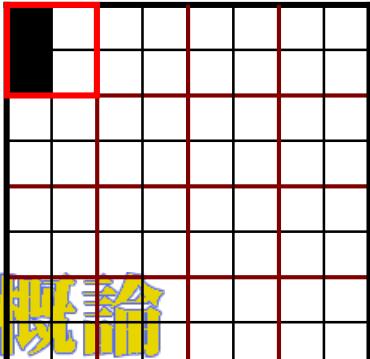
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	□	□	■	■	□	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



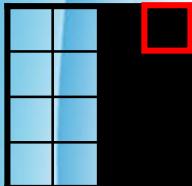
計算機視聽



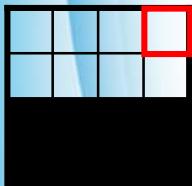
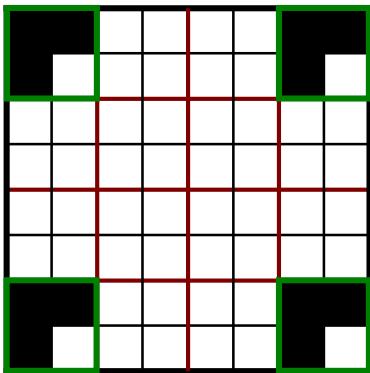
# 旋轉式視覺密碼

(Wu and Chen, 1998)

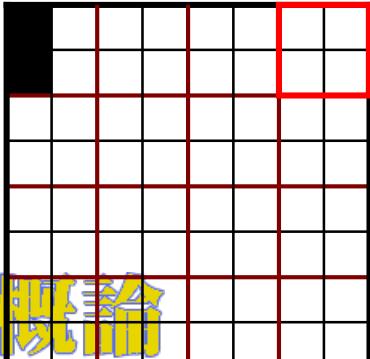
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	□	□	■	□	■	□	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



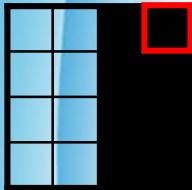
計算機視聽



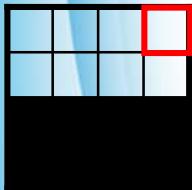
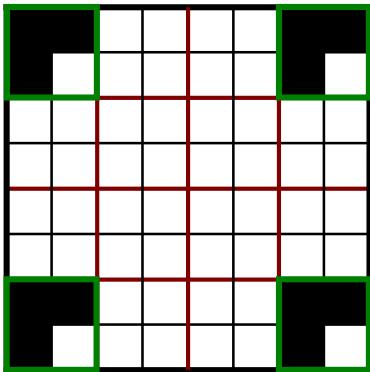
# 旋轉式視覺密碼

(Wu and Chen, 1998)

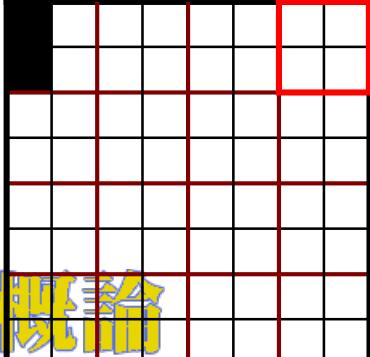
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	■	□	□	■	■	□	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



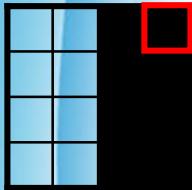
計算機視聽



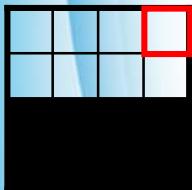
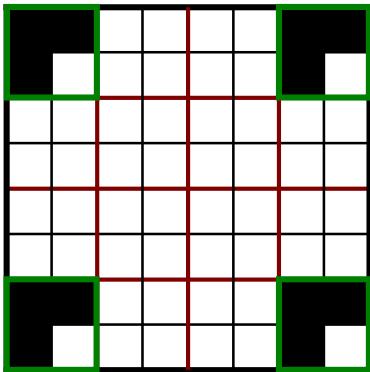
# 旋轉式視覺密碼

(Wu and Chen, 1998)

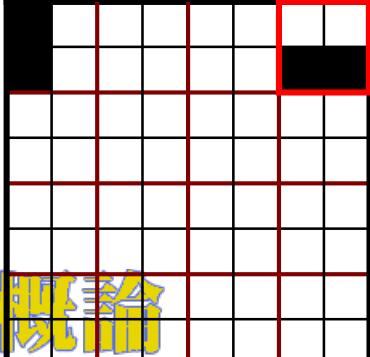
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	□	□	■	□	■	□	□	■	■
$s_1$	■	□	■	□	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



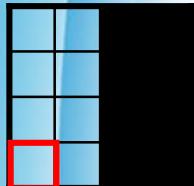
計算機視聽



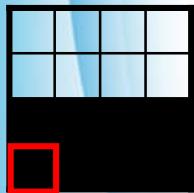
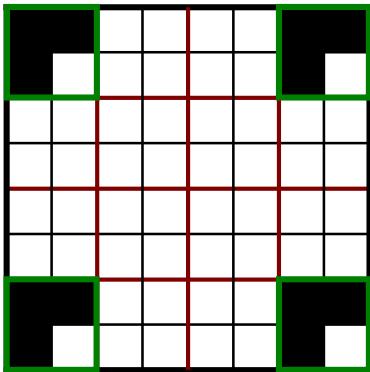
# 旋轉式視覺密碼

(Wu and Chen, 1998)

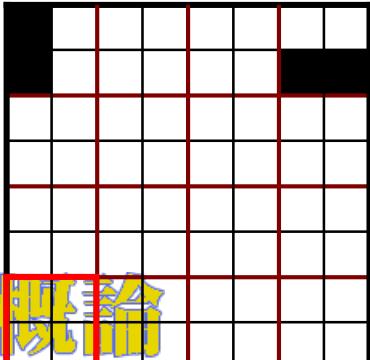
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	□	□	■	□	■	□	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



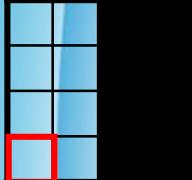
計算機概論



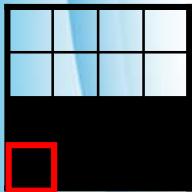
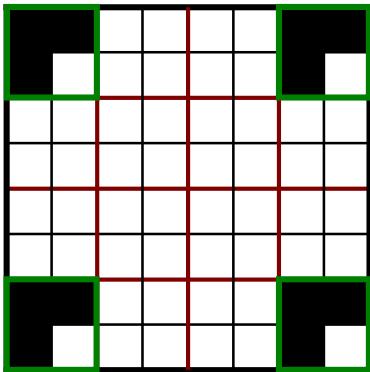
# 旋轉式視覺密碼

(Wu and Chen, 1998)

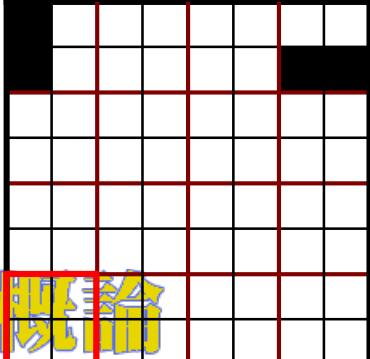
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	□	□	■	■	□	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



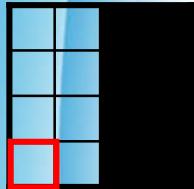
計算機概論



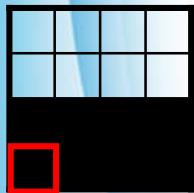
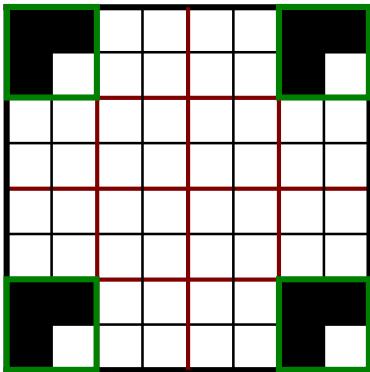
# 旋轉式視覺密碼

(Wu and Chen, 1998)

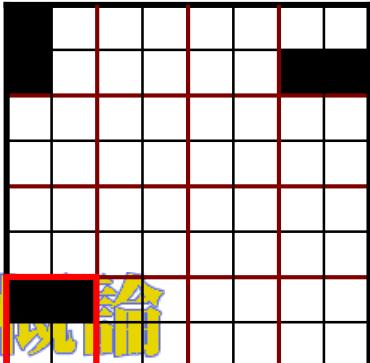
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	□	□	■	■	□	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



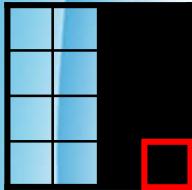
計算機系  
部



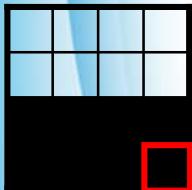
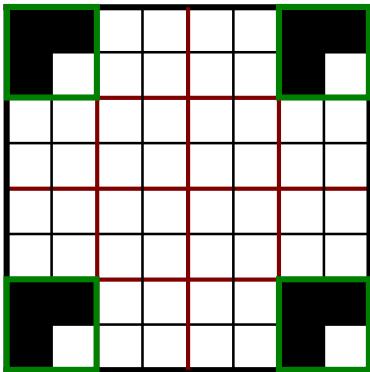
# 旋轉式視覺密碼

(Wu and Chen, 1998)

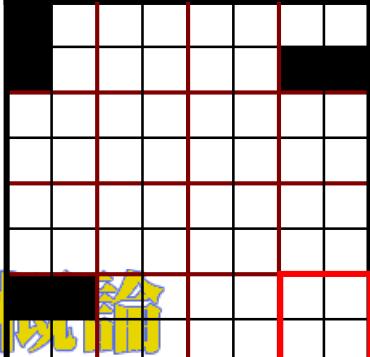
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	□	□	■	□	■	□	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



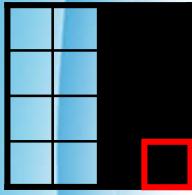
計算機視覺



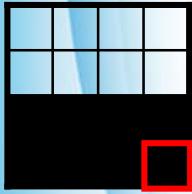
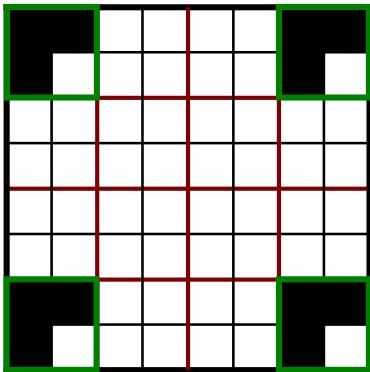
# 旋轉式視覺密碼

(Wu and Chen, 1998)

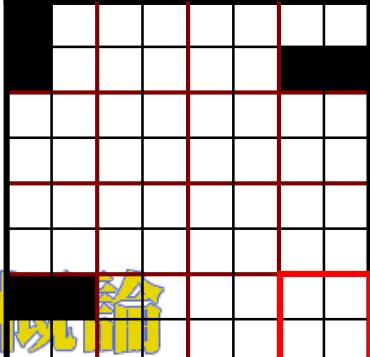
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	□	□	■	■	□	□	■	□	■
$s_1$	■	□	■	□	■	■	■	■	□	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



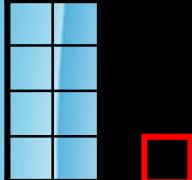
計算機視覺



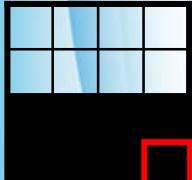
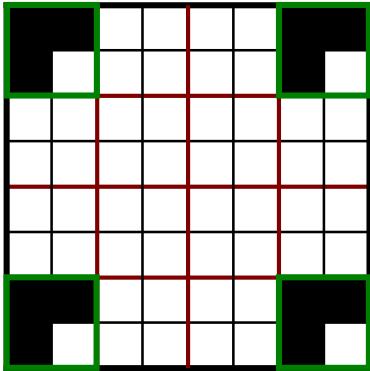
# 旋轉式視覺密碼

(Wu and Chen, 1998)

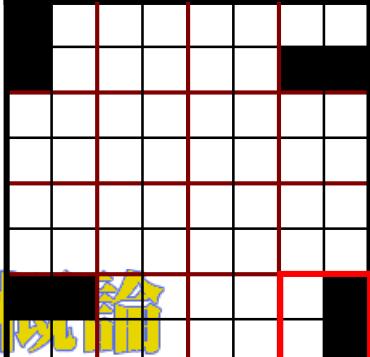
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	□	□	■	■	□	□	■	□	■
$s_1$	■	□	■	□	■	■	■	□	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



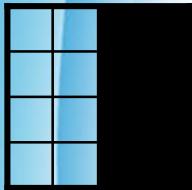
計算機視覺



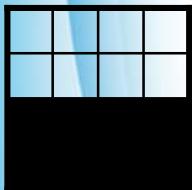
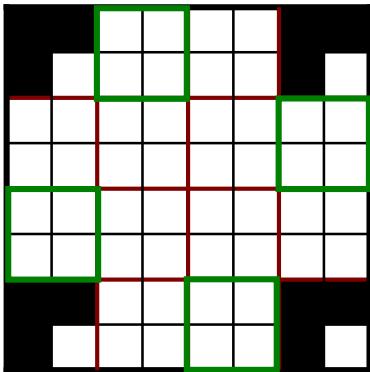
# 旋轉式視覺密碼

(Wu and Chen, 1998)

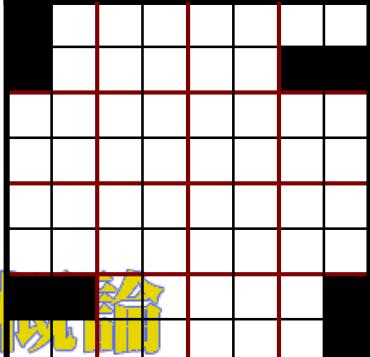
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



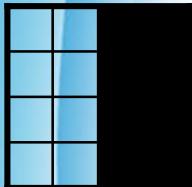
計算機概論



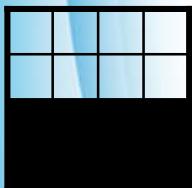
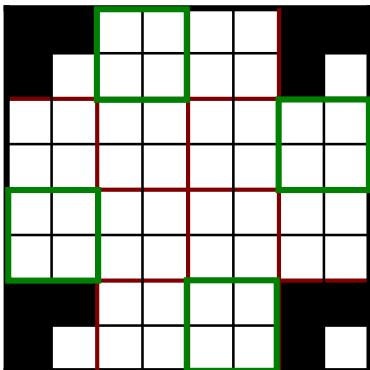
# 旋轉式視覺密碼

(Wu and Chen, 1998)

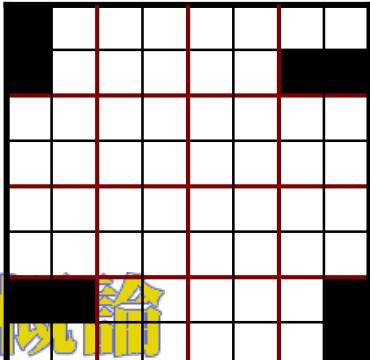
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	□	■	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



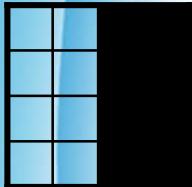
計算機概論



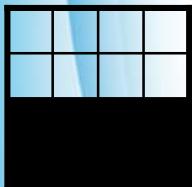
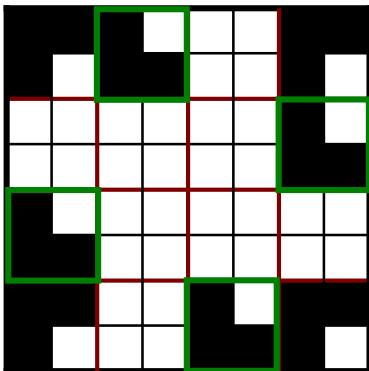
# 旋轉式視覺密碼

(Wu and Chen, 1998)

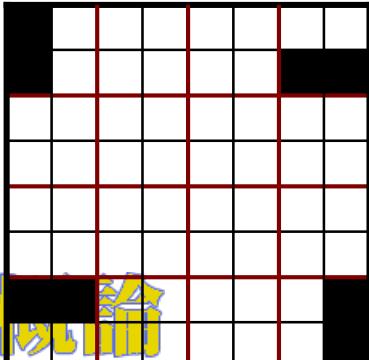
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□	■
$s_1$	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□
$s_2$	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□



$P_1$



$P_2$



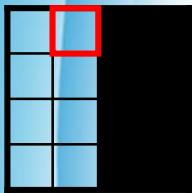
計算機系  
討論



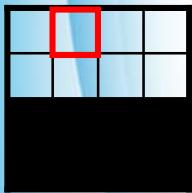
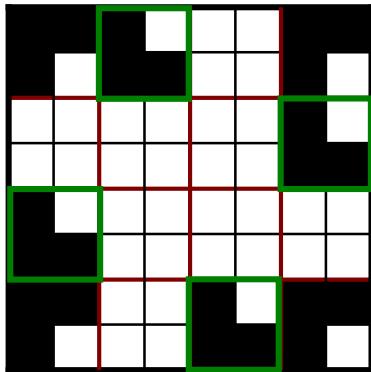
# 旋轉式視覺密碼

(Wu and Chen, 1998)

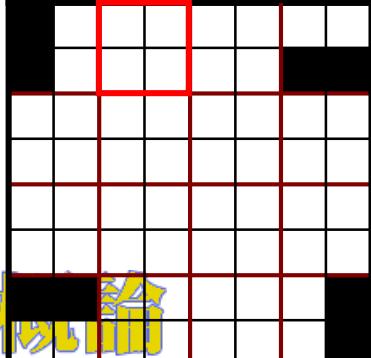
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



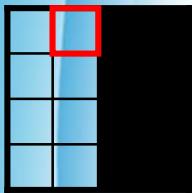
計算機系  
討論



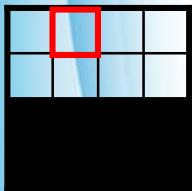
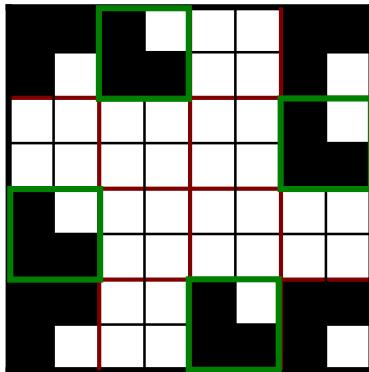
# 旋轉式視覺密碼

(Wu and Chen, 1998)

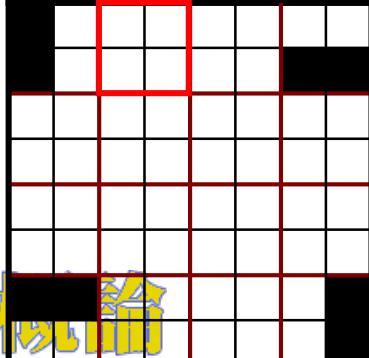
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	■	□	□	■	■	□	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



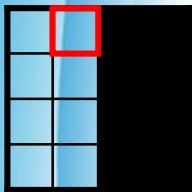
計算機系  
討論



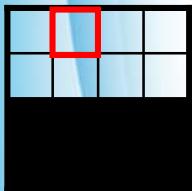
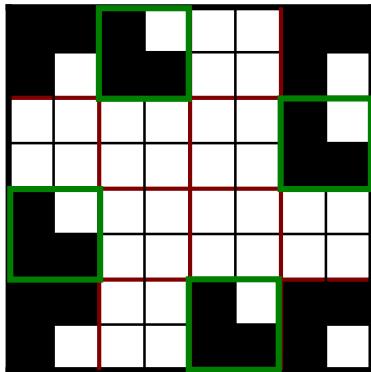
# 旋轉式視覺密碼

(Wu and Chen, 1998)

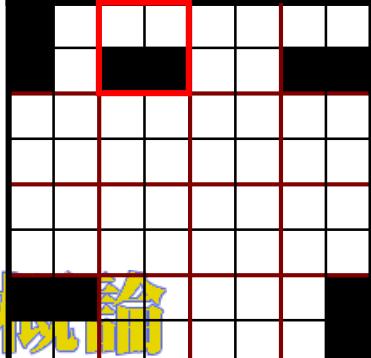
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	■	□	□	■	■	□	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



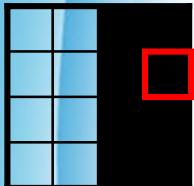
計算機概論



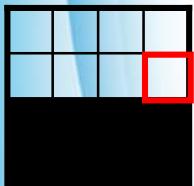
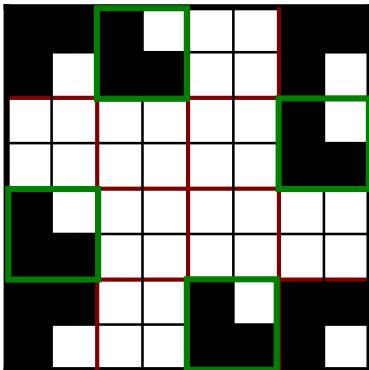
# 旋轉式視覺密碼

(Wu and Chen, 1998)

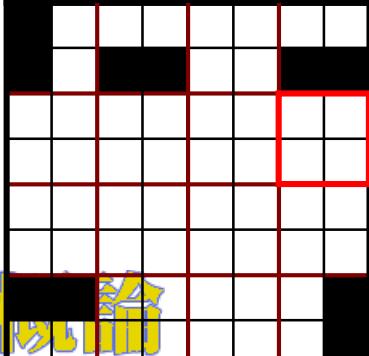
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



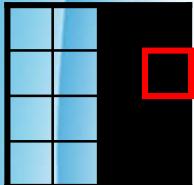
計算機視聽



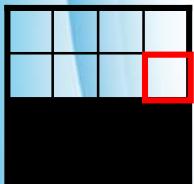
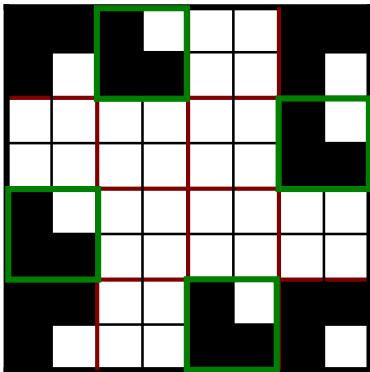
# 旋轉式視覺密碼

(Wu and Chen, 1998)

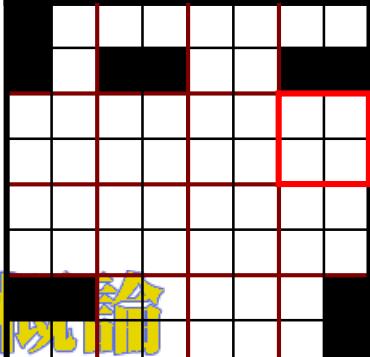
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



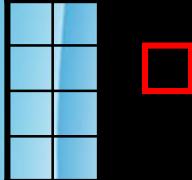
計算機視聽



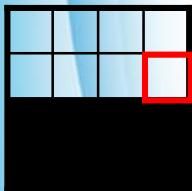
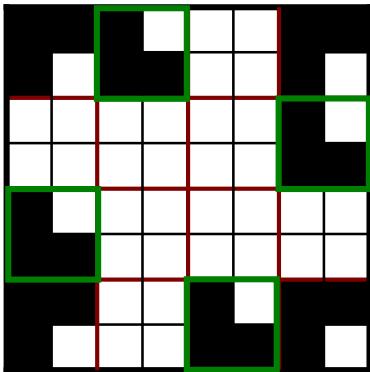
# 旋轉式視覺密碼

(Wu and Chen, 1998)

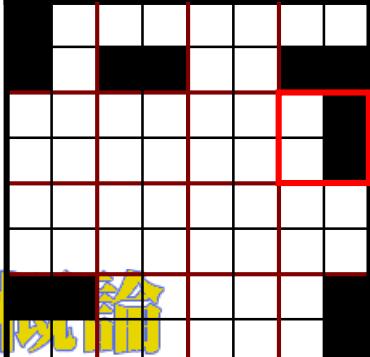
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



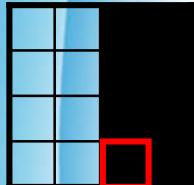
計算機系  
討論



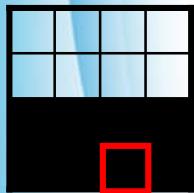
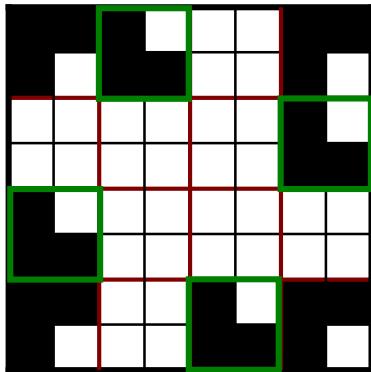
# 旋轉式視覺密碼

(Wu and Chen, 1998)

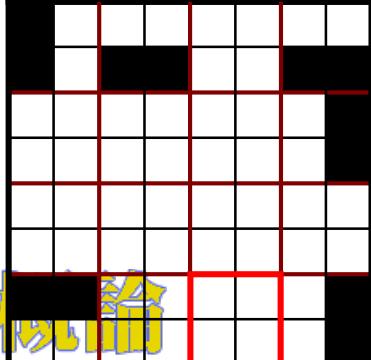
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



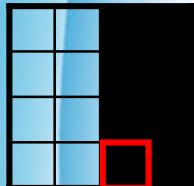
計算機系  
部



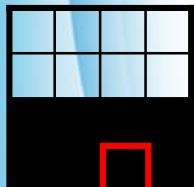
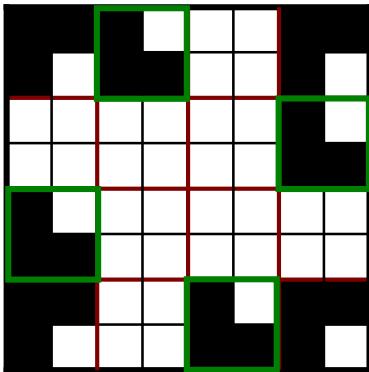
# 旋轉式視覺密碼

(Wu and Chen, 1998)

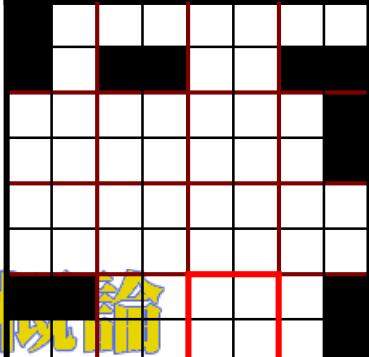
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	■	□	□	■	■	□	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



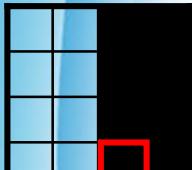
計算機系  
部



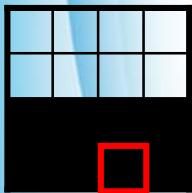
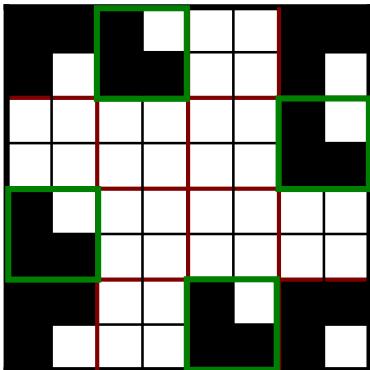
# 旋轉式視覺密碼

(Wu and Chen, 1998)

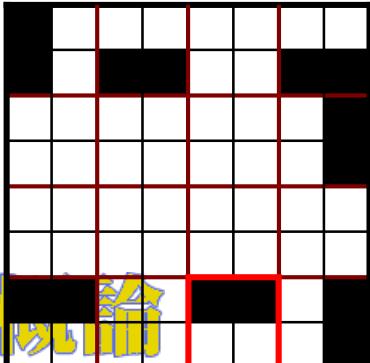
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	■	□	□	■	■	□	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



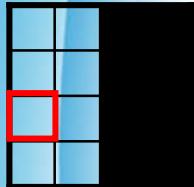
計算機系  
部



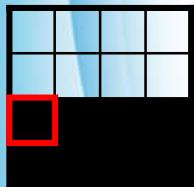
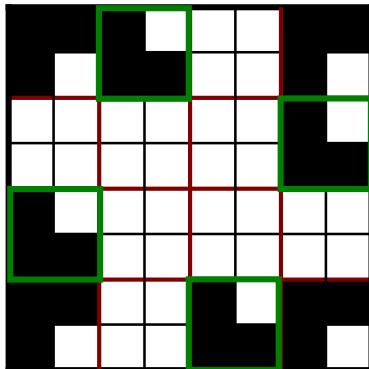
# 旋轉式視覺密碼

(Wu and Chen, 1998)

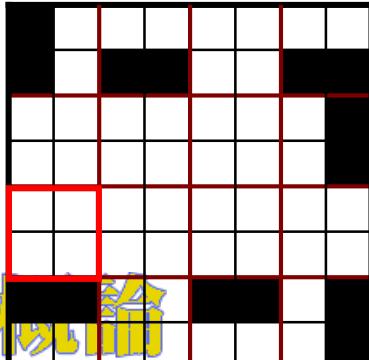
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



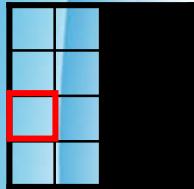
計算機系  
討論



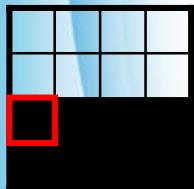
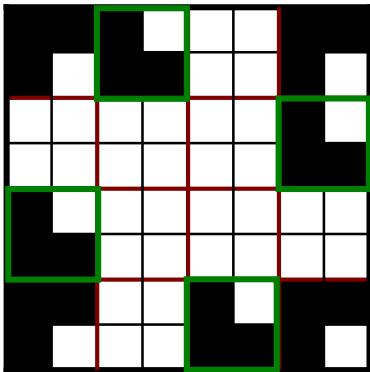
# 旋轉式視覺密碼

(Wu and Chen, 1998)

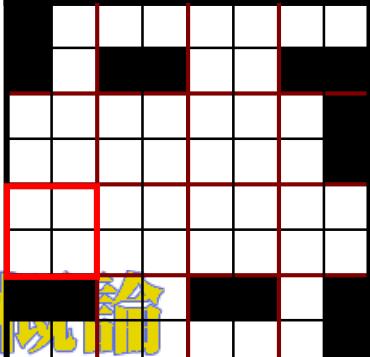
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	□	■	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



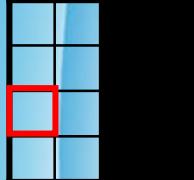
計算機系  
部



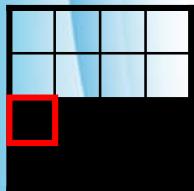
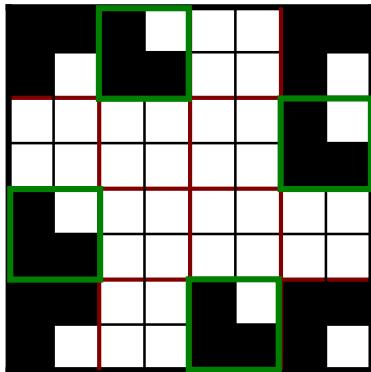
# 旋轉式視覺密碼

(Wu and Chen, 1998)

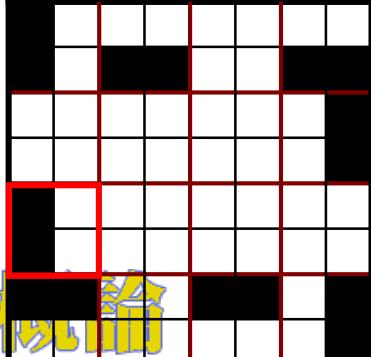
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	■	□	□	■	■	□	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



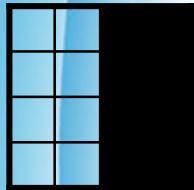
計算機系  
討論會



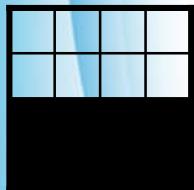
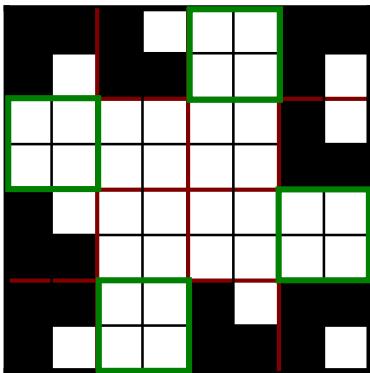
# 旋轉式視覺密碼

(Wu and Chen, 1998)

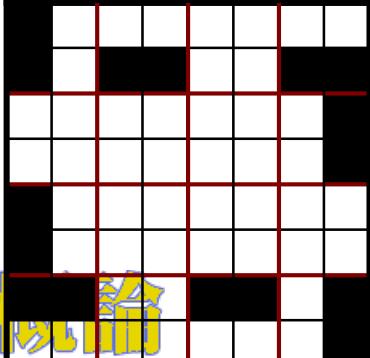
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	□	■	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



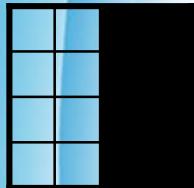
計算機概論



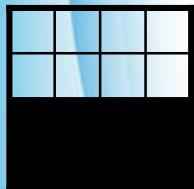
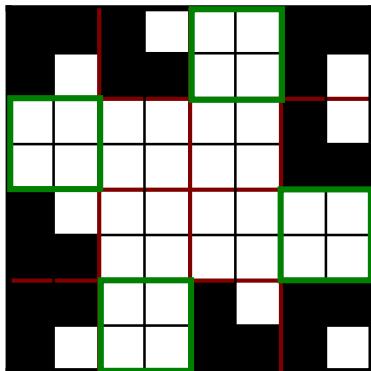
# 旋轉式視覺密碼

(Wu and Chen, 1998)

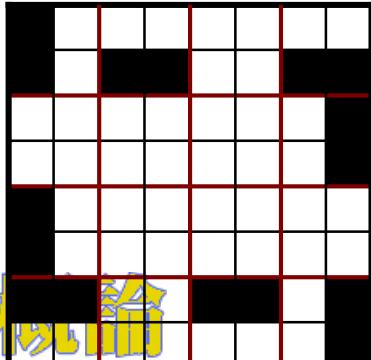
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



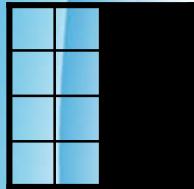
計算機概論



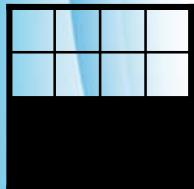
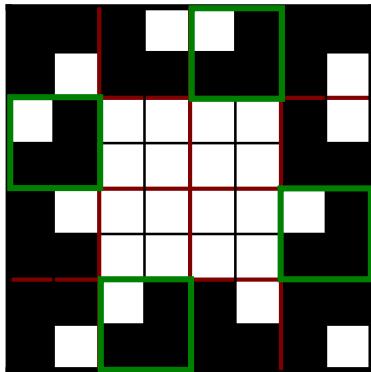
# 旋轉式視覺密碼

(Wu and Chen, 1998)

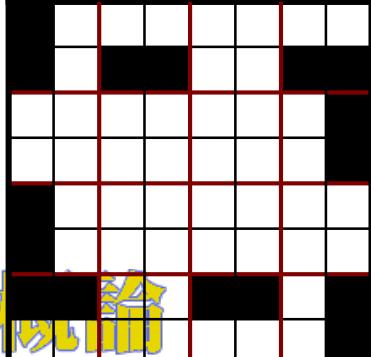
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



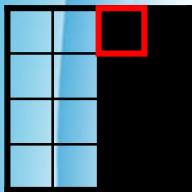
計算機概論



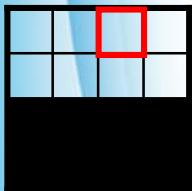
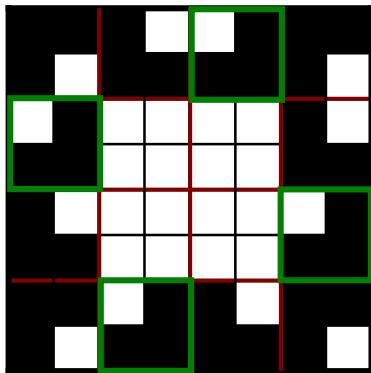
# 旋轉式視覺密碼

(Wu and Chen, 1998)

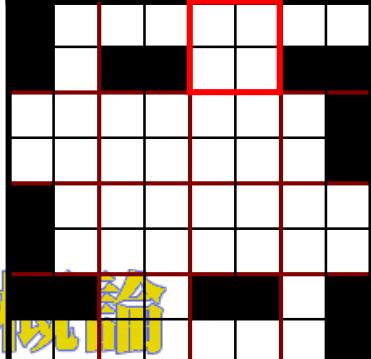
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



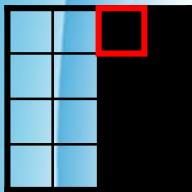
計算機概論



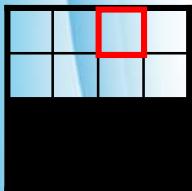
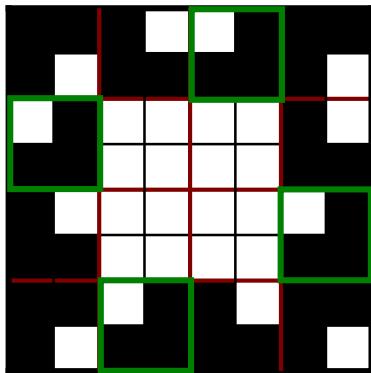
# 旋轉式視覺密碼

(Wu and Chen, 1998)

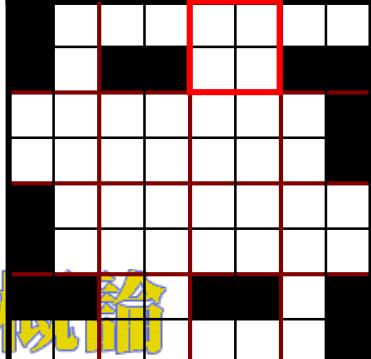
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



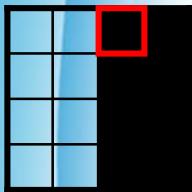
計算機概論



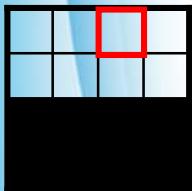
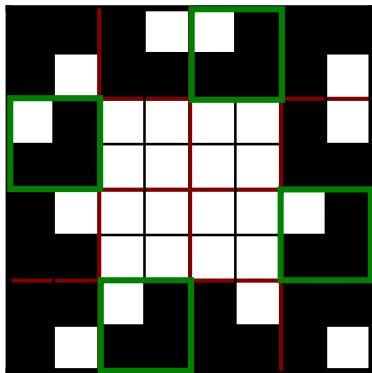
# 旋轉式視覺密碼

(Wu and Chen, 1998)

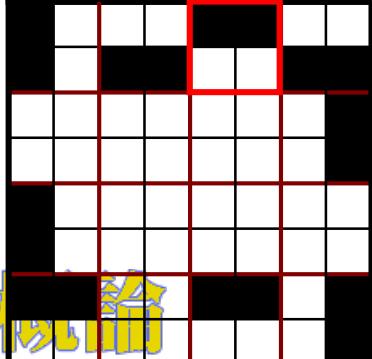
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



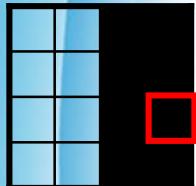
計算機概論



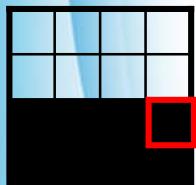
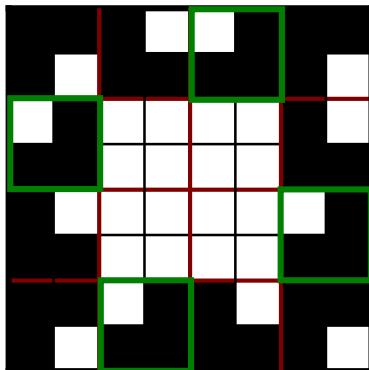
# 旋轉式視覺密碼

(Wu and Chen, 1998)

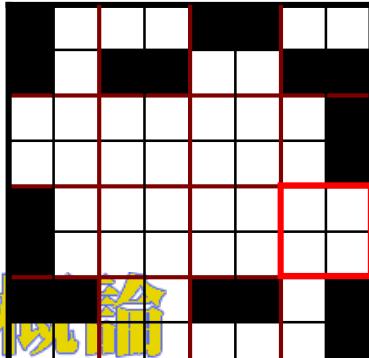
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



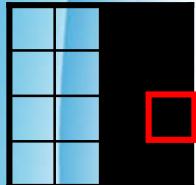
計算機概論



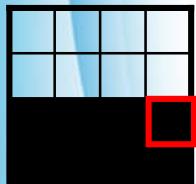
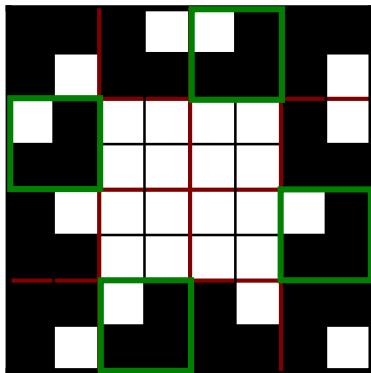
# 旋轉式視覺密碼

(Wu and Chen, 1998)

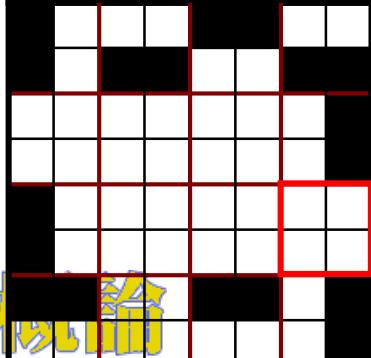
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



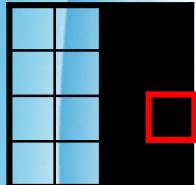
計算機概論



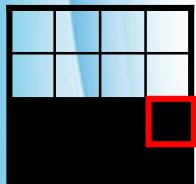
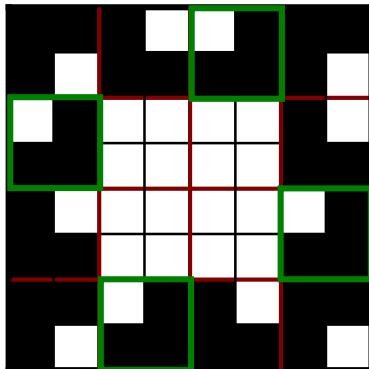
# 旋轉式視覺密碼

(Wu and Chen, 1998)

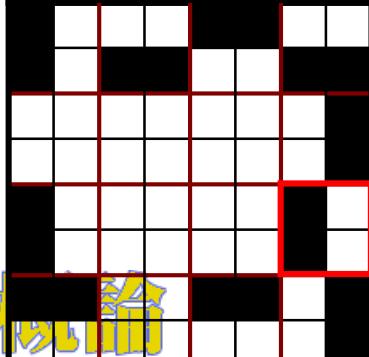
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



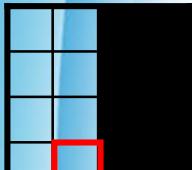
計算機概論



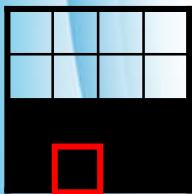
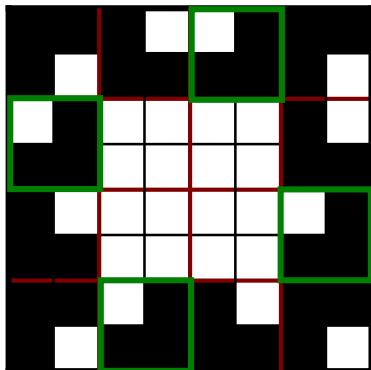
# 旋轉式視覺密碼

(Wu and Chen, 1998)

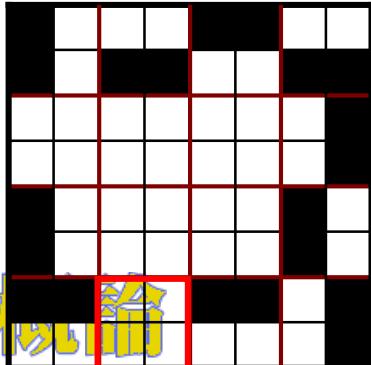
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



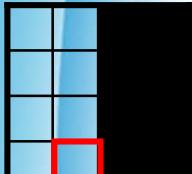
計算機概論



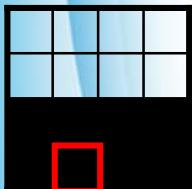
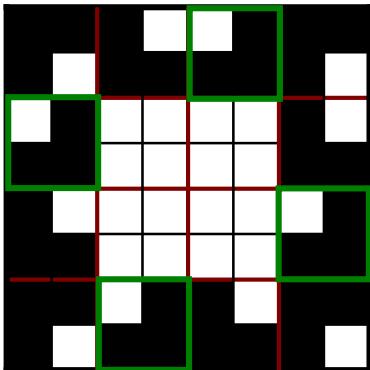
# 旋轉式視覺密碼

(Wu and Chen, 1998)

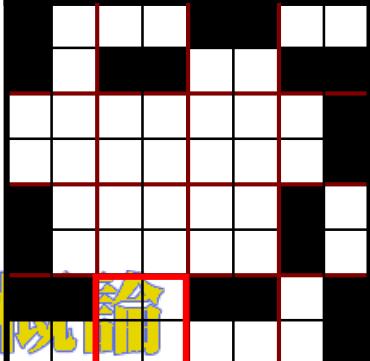
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$

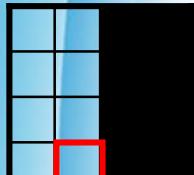


計算機系  
論

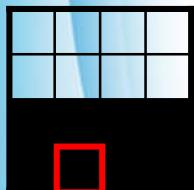
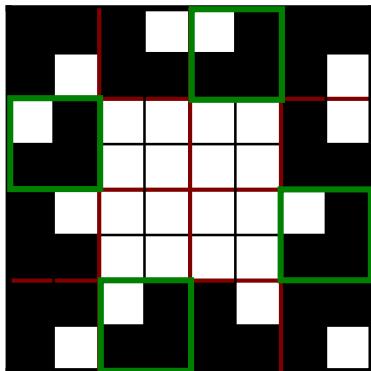
# 旋轉式視覺密碼

(Wu and Chen, 1998)

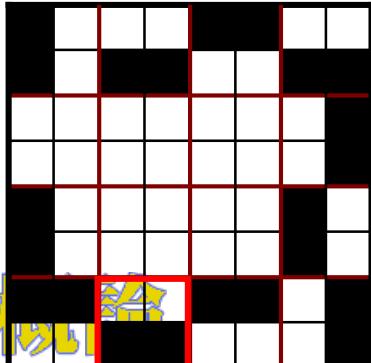
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



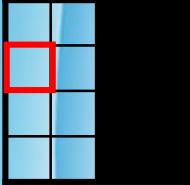
計算機系



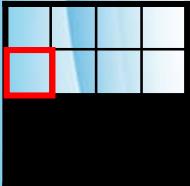
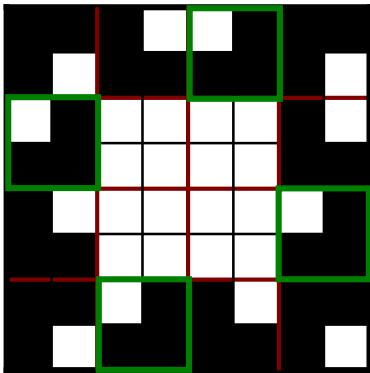
# 旋轉式視覺密碼

(Wu and Chen, 1998)

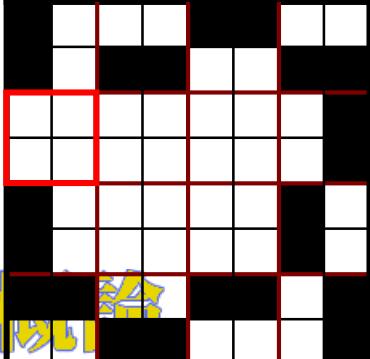
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



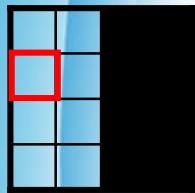
計算機  
系



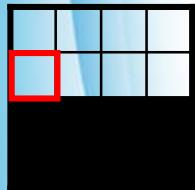
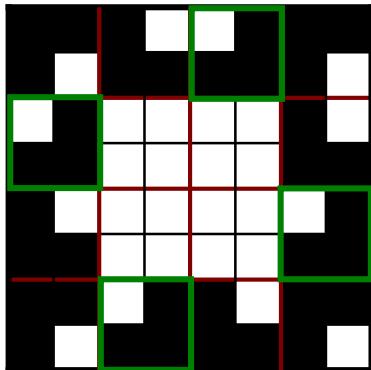
# 旋轉式視覺密碼

(Wu and Chen, 1998)

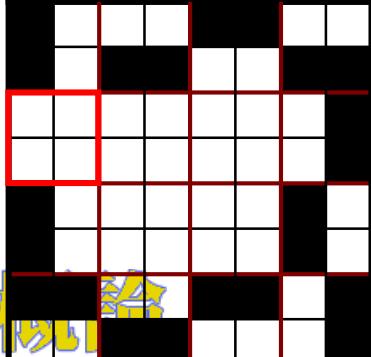
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	■	□	□	■	■	□	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



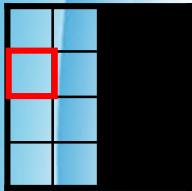
計算機  
系



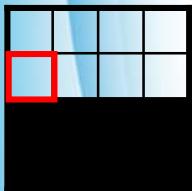
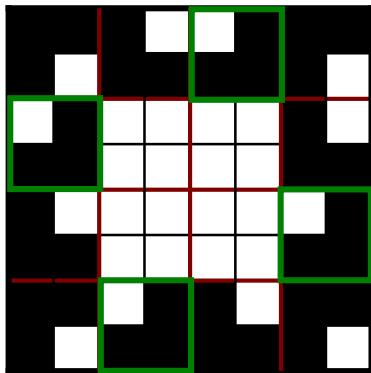
# 旋轉式視覺密碼

(Wu and Chen, 1998)

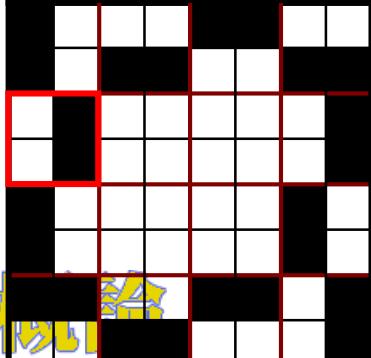
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	■	□	□	■	■	□	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



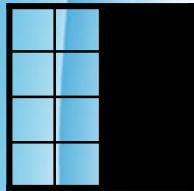
計算機  
系



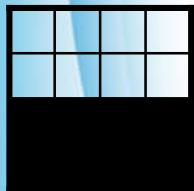
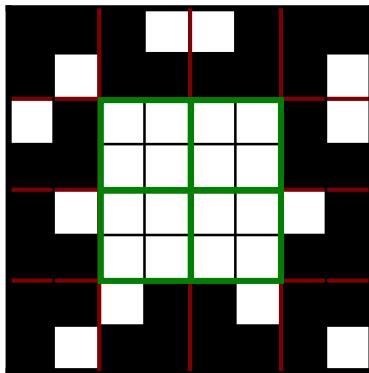
# 旋轉式視覺密碼

(Wu and Chen, 1998)

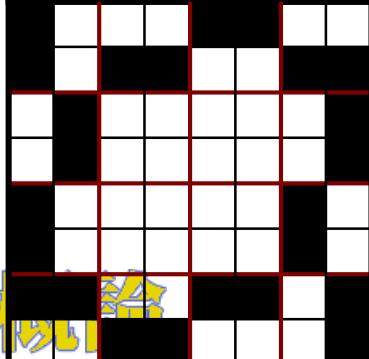
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



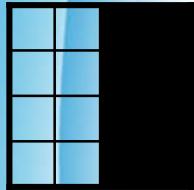
計算機  
系



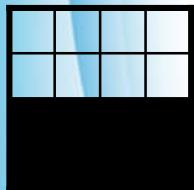
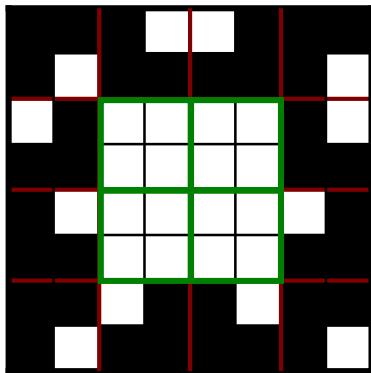
# 旋轉式視覺密碼

(Wu and Chen, 1998)

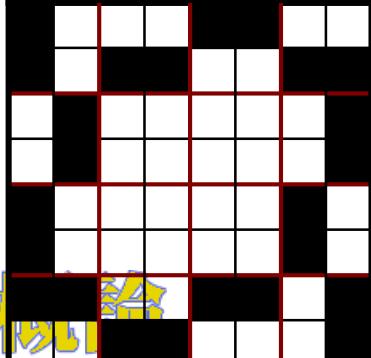
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	■	□	□	■	■	□	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



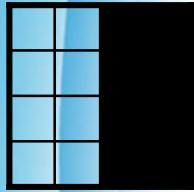
計算機  
系



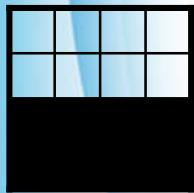
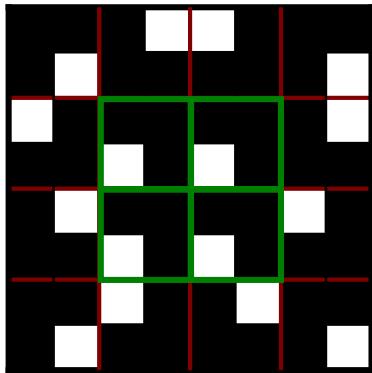
# 旋轉式視覺密碼

(Wu and Chen, 1998)

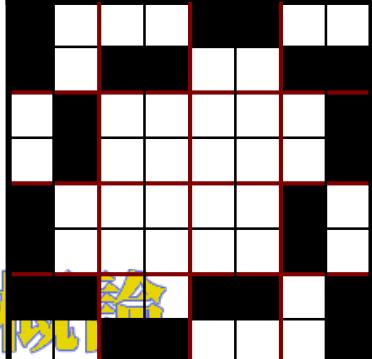
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	■	□	□	■	■	□	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



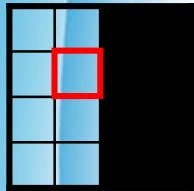
計算機  
系



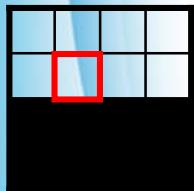
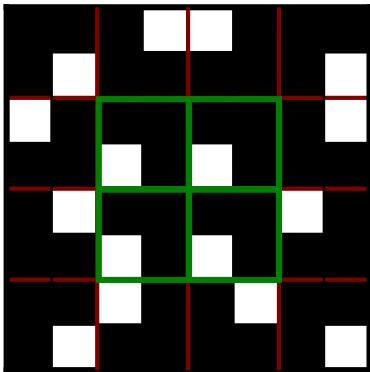
# 旋轉式視覺密碼

(Wu and Chen, 1998)

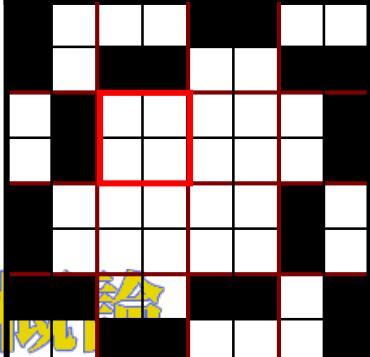
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	■	□	□	■	■	□	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



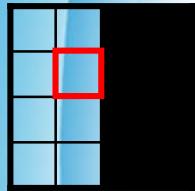
計算機  
系



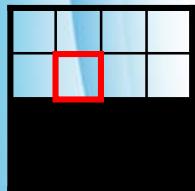
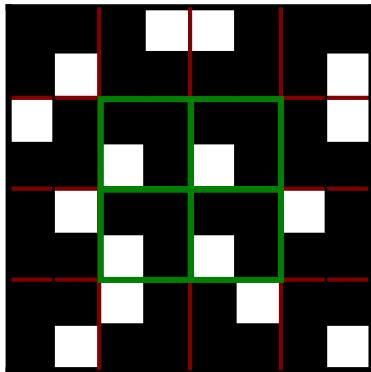
# 旋轉式視覺密碼

(Wu and Chen, 1998)

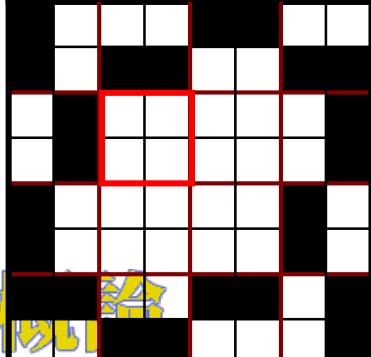
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	■	□	□	■	■	□	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



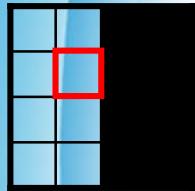
計算機  
系



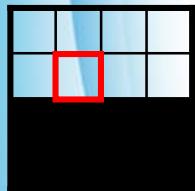
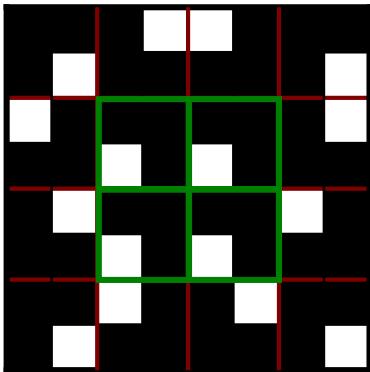
# 旋轉式視覺密碼

(Wu and Chen, 1998)

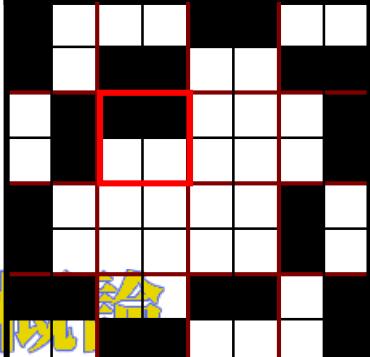
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	■	□	□	■	■	□	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



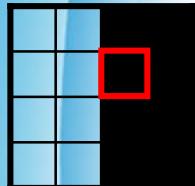
計算機  
系



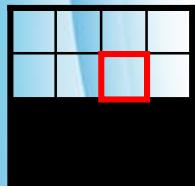
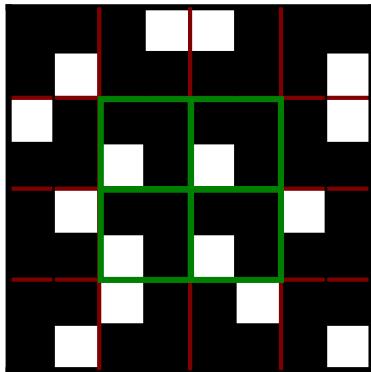
# 旋轉式視覺密碼

(Wu and Chen, 1998)

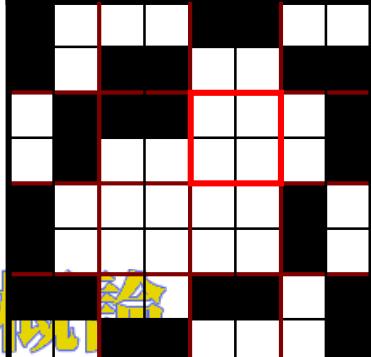
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	■	□	□	■	■	□	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$

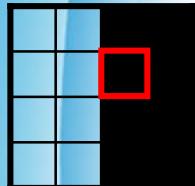


計算機系

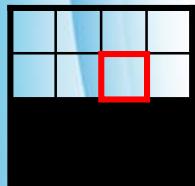
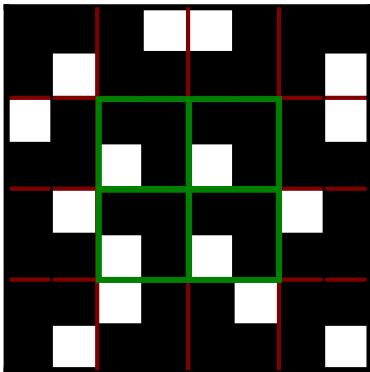
# 旋轉式視覺密碼

(Wu and Chen, 1998)

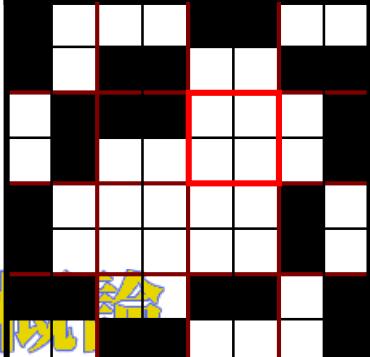
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	■	■
$p_2$	□	■	□	■	□	□	■	□	□	■	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



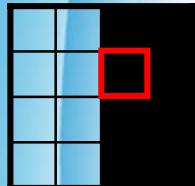
計算機  
系



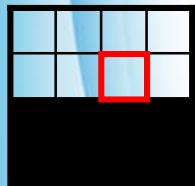
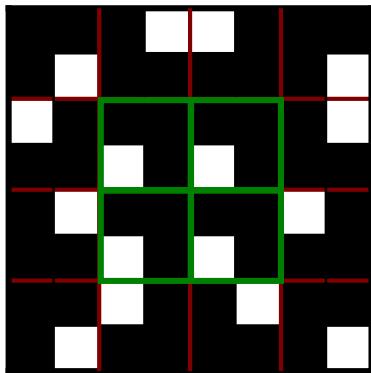
# 旋轉式視覺密碼

(Wu and Chen, 1998)

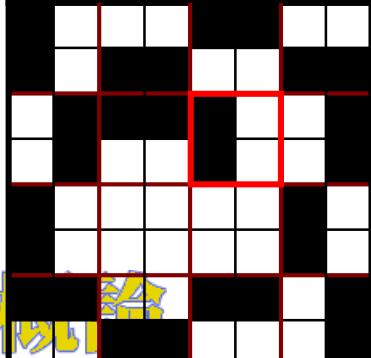
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	■	■
$p_2$	□	■	□	■	□	□	■	□	□	■	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$

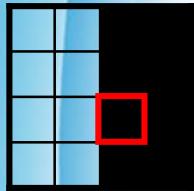


計算機  
系

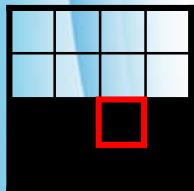
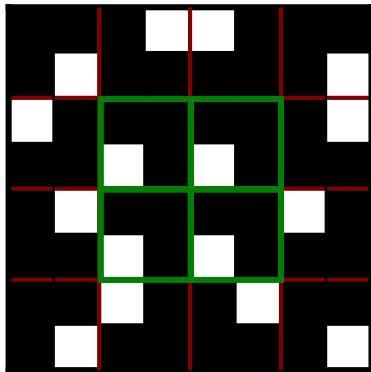
# 旋轉式視覺密碼

(Wu and Chen, 1998)

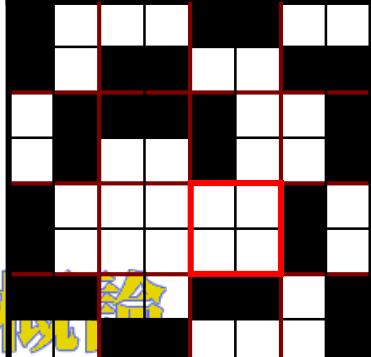
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	■	□	□	■	■	□	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



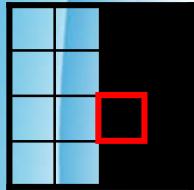
計算機  
系



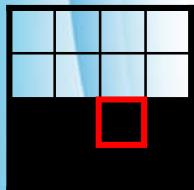
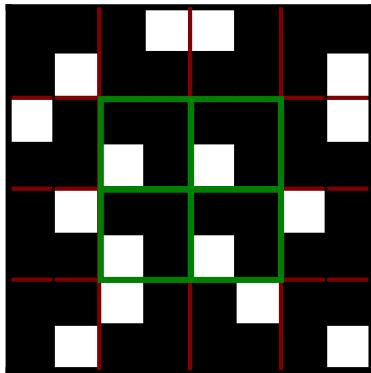
# 旋轉式視覺密碼

(Wu and Chen, 1998)

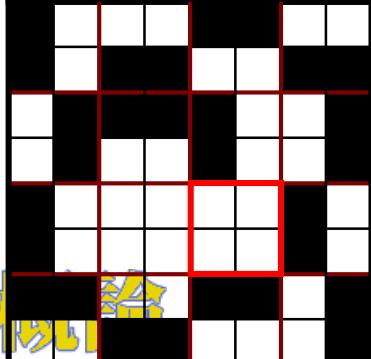
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	□	□	■	■	□	■	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



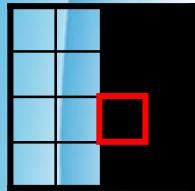
計算機  
系



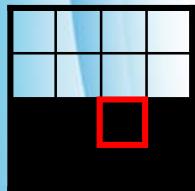
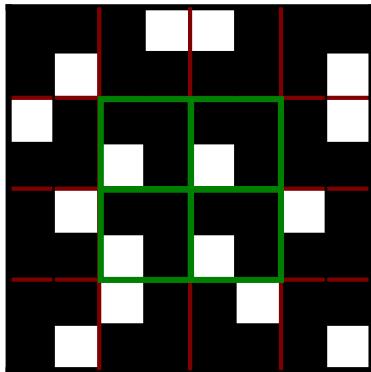
# 旋轉式視覺密碼

(Wu and Chen, 1998)

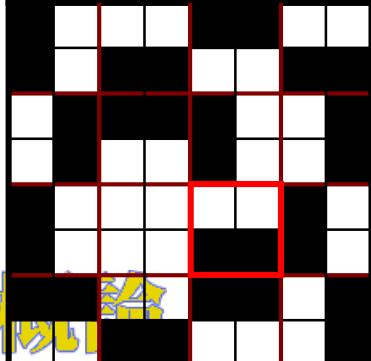
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	□	□	■	□	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



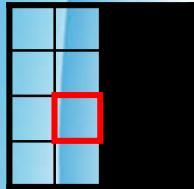
計算機  
系



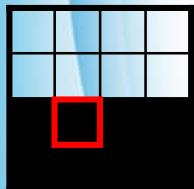
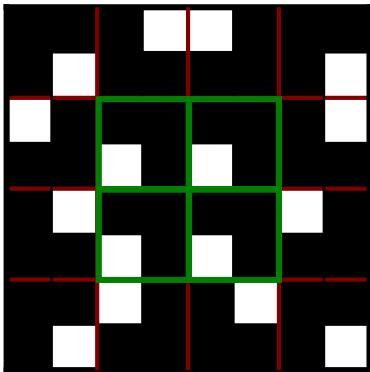
# 旋轉式視覺密碼

(Wu and Chen, 1998)

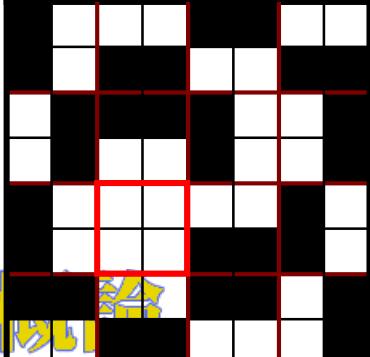
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	□	■	■	□	□	■	■	□	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



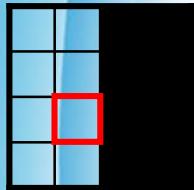
計算機  
系



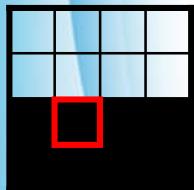
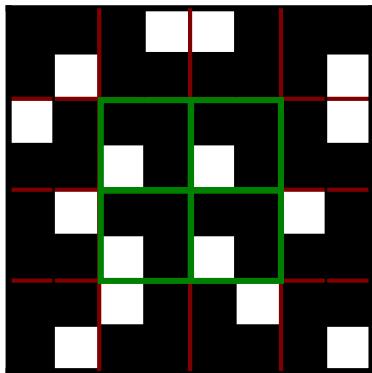
# 旋轉式視覺密碼

(Wu and Chen, 1998)

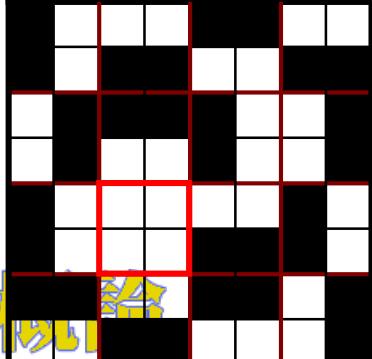
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	■	■
$p_2$	□	■	□	■	□	□	■	■	□	□	■	■	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



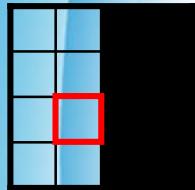
計算機  
系



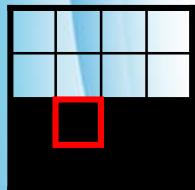
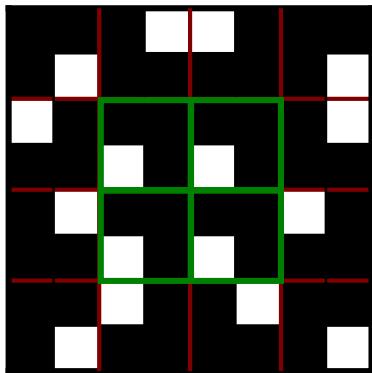
# 旋轉式視覺密碼

(Wu and Chen, 1998)

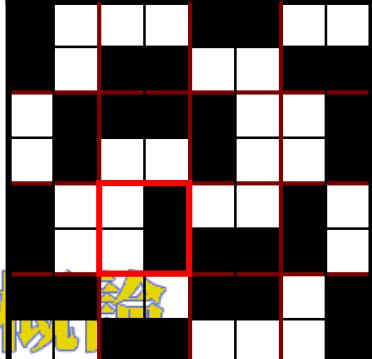
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	■	■
$p_2$	□	■	□	■	□	□	■	■	□	□	■	■	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



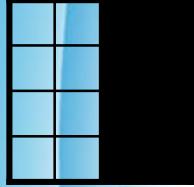
計算機  
視覺密碼



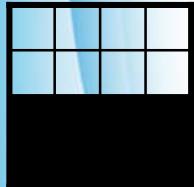
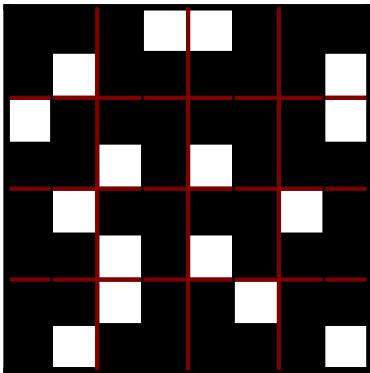
# 旋轉式視覺密碼

(Wu and Chen, 1998)

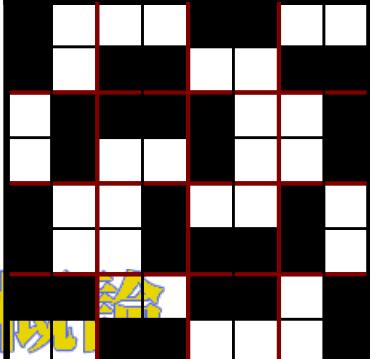
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



計算機  
系



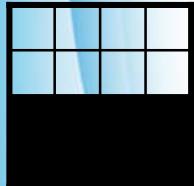
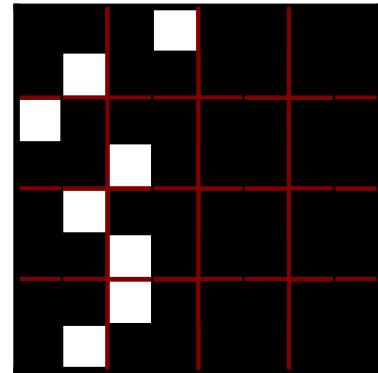
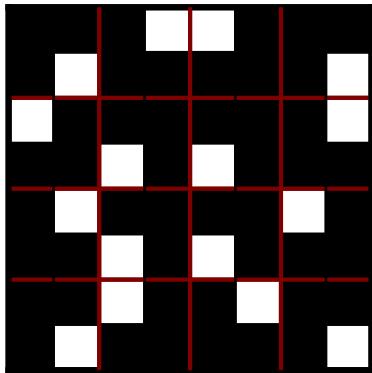
# 旋轉式視覺密碼

(Wu and Chen, 1998)

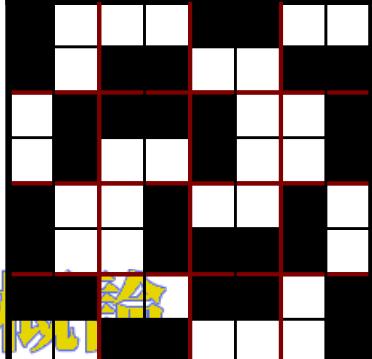
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	□	■	■	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$



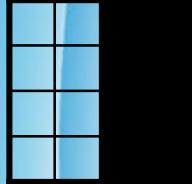
計算機  
系



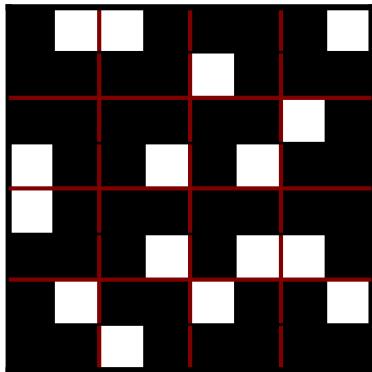
# 旋轉式視覺密碼

(Wu and Chen, 1998)

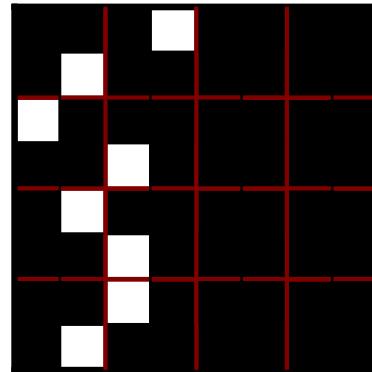
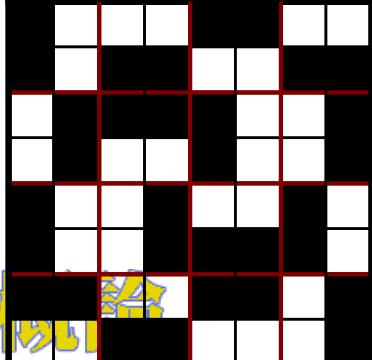
$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	□	■	■	□	■	■
$s_1$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
$s_2$	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■



$P_1$



$P_2$

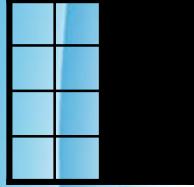


計算機系

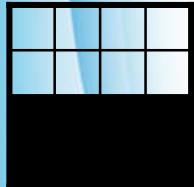
# 旋轉式視覺密碼

(Wu and Chen, 1998)

$p_1$	□	□	■	■	□	□	■	■	□	□	■	■	□	■	■
$p_2$	□	■	□	■	□	■	□	■	□	■	□	■	□	■	■
$s_1$	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□
$s_2$	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□	■□



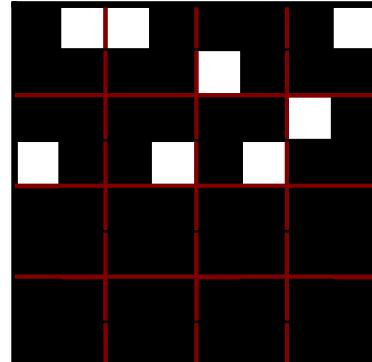
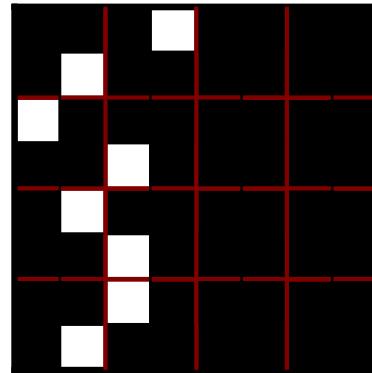
$P_1$



$P_2$



計算機概論



# 平移式視覺密碼

(Wu and Yang, 2001)

$S_1$


$S_2$

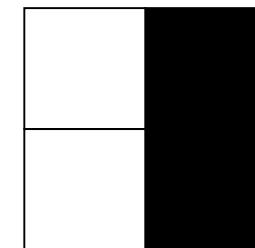

$P_1$


$S_1$


$S_2$

$P_2$



# 平移式視覺密碼

(Wu and Yang, 2001)

$S_1$


$S_2$


$P_1$


$S_1$


計算機概論

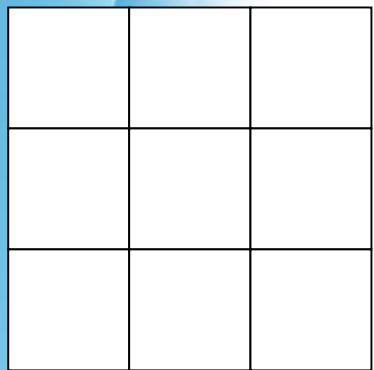
$S_2$



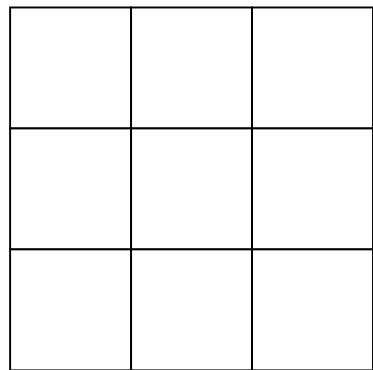

# 平移式視覺密碼

(Wu and Yang, 2001)

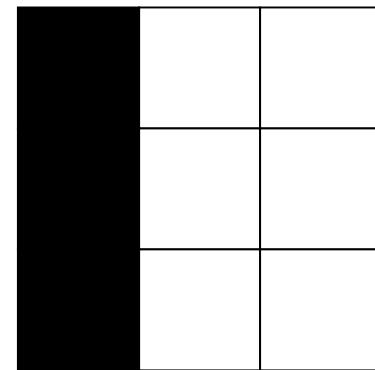
$S_1$



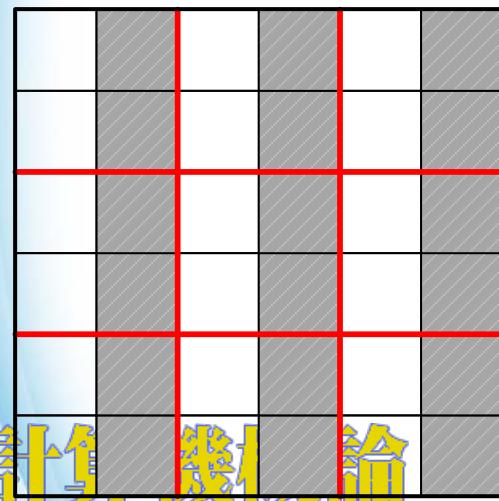
$S_2$



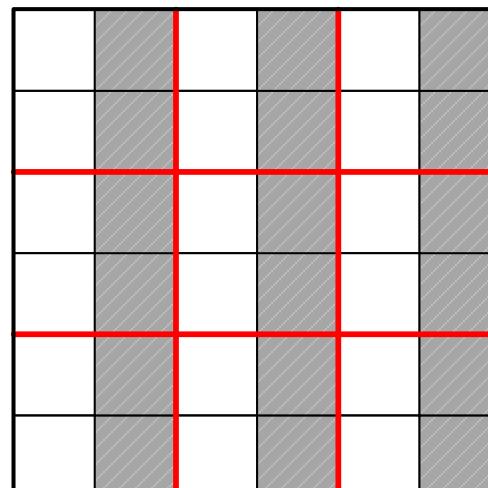
$P_1$



$S_1$



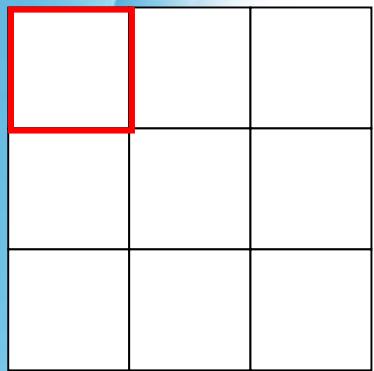
$S_2$



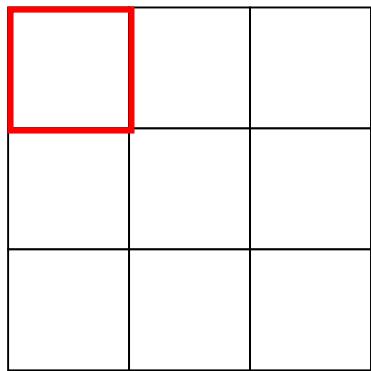
# 平移式視覺密碼

(Wu and Yang, 2001)

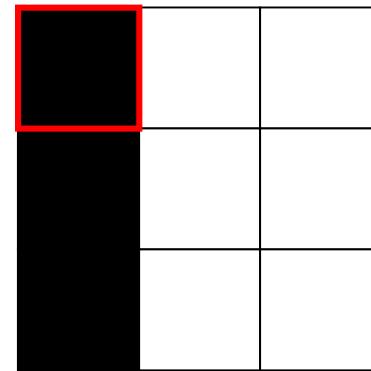
$S_1$



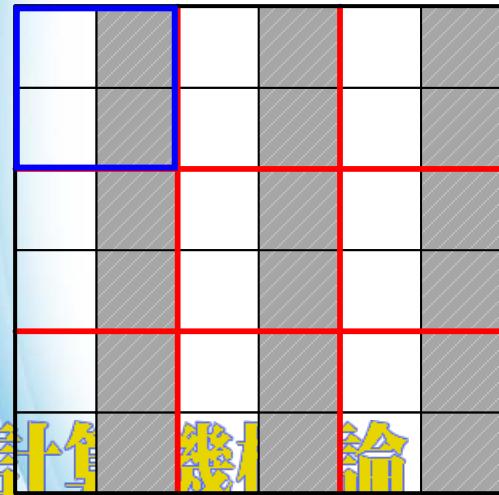
$S_2$



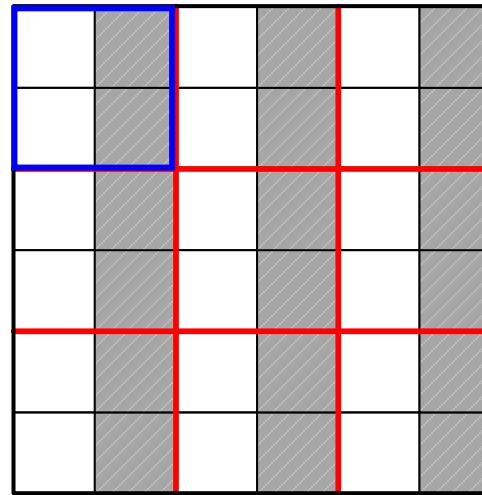
$P_1$



$S_1$



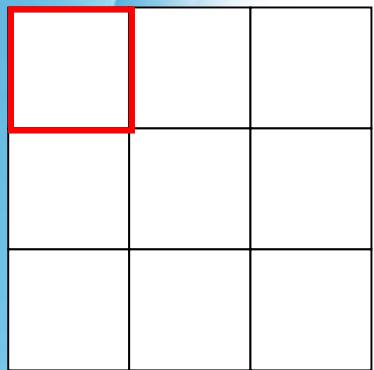
$S_2$



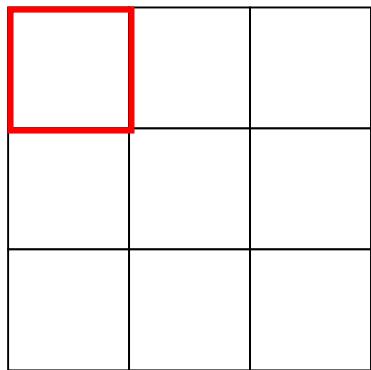
# 平移式視覺密碼

(Wu and Yang, 2001)

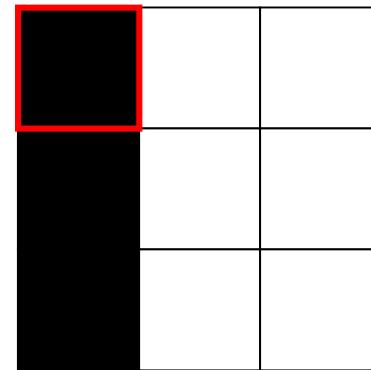
$S_1$



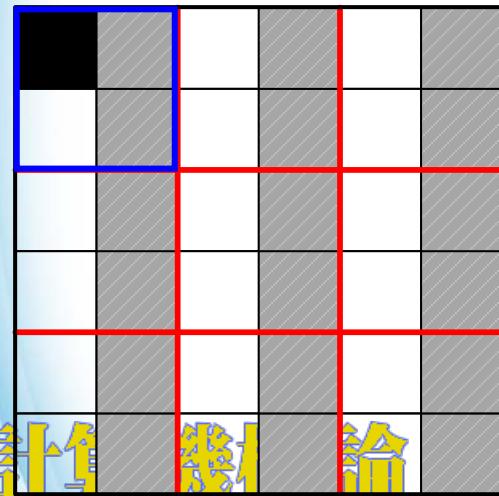
$S_2$



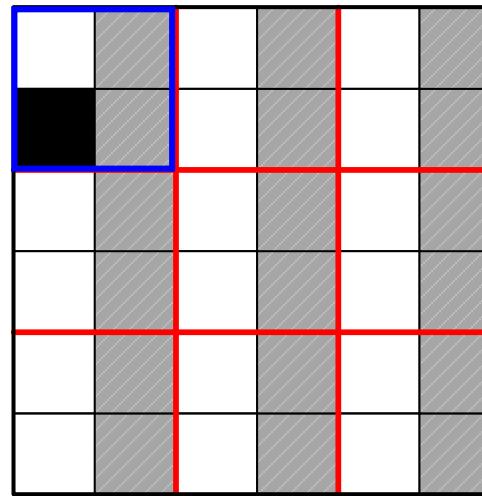
$P_1$



$S_1$



$S_2$

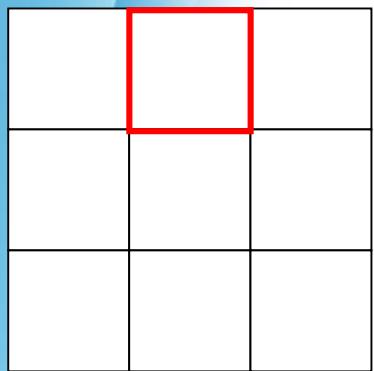


計算機系  
論

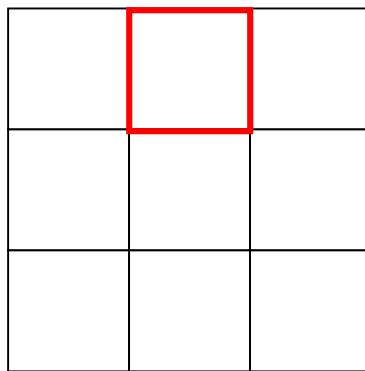
# 平移式視覺密碼

(Wu and Yang, 2001)

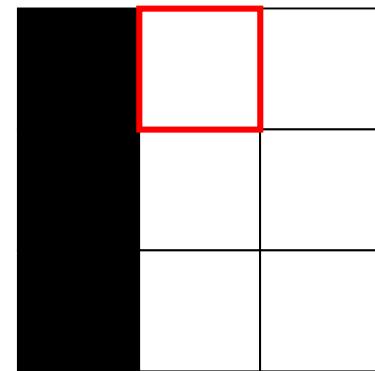
$S_1$



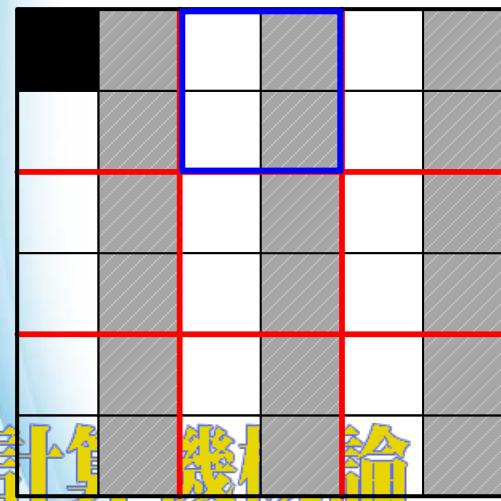
$S_2$



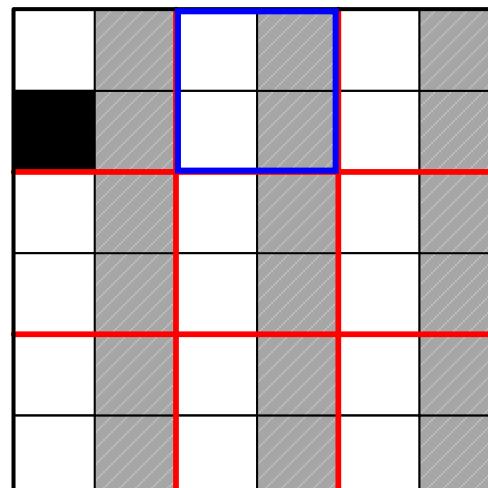
$P_1$



$S_1$



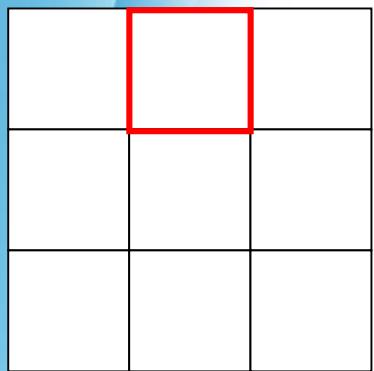
$S_2$



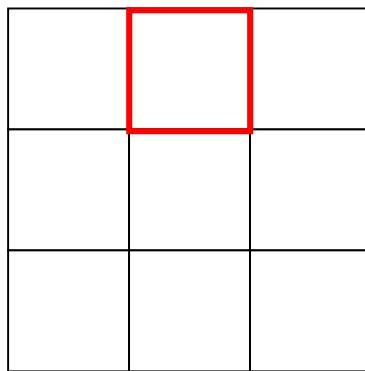
# 平移式視覺密碼

(Wu and Yang, 2001)

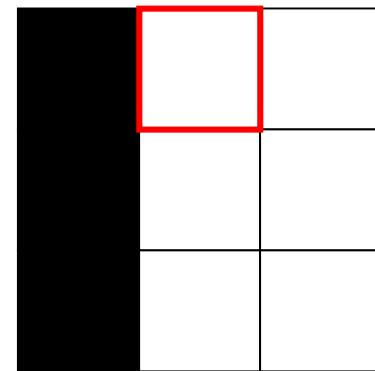
$S_1$



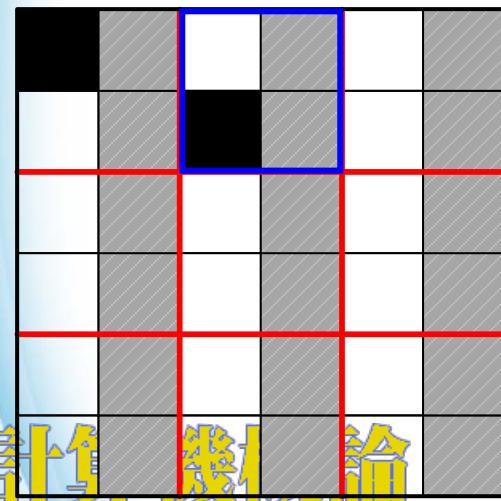
$S_2$



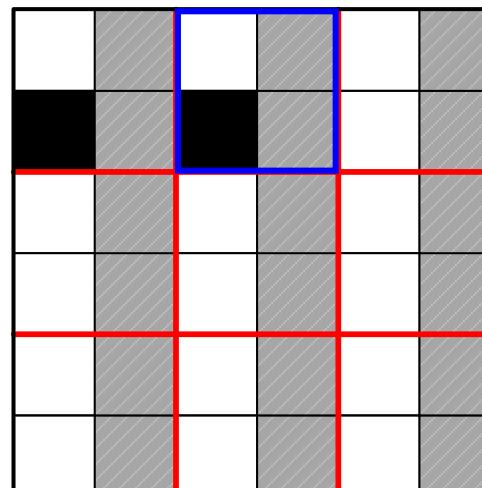
$P_1$



$S_1$



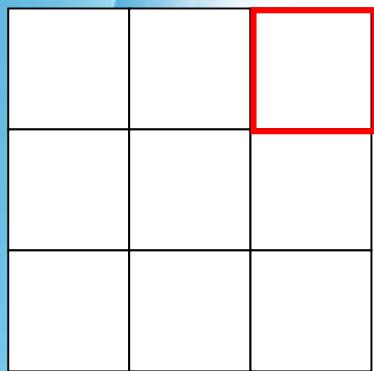
$S_2$



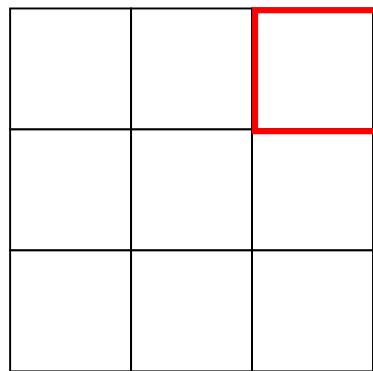
# 平移式視覺密碼

(Wu and Yang, 2001)

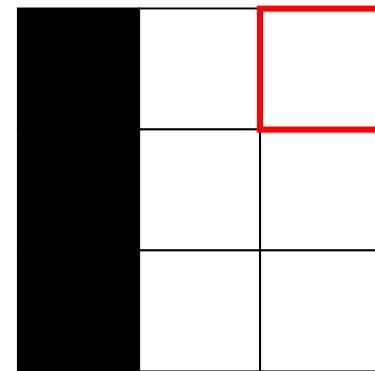
$S_1$



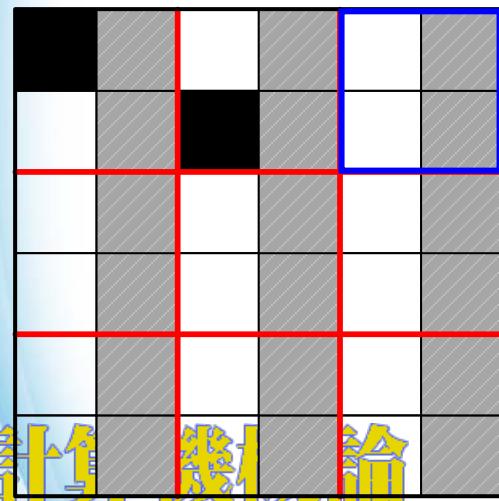
$S_2$



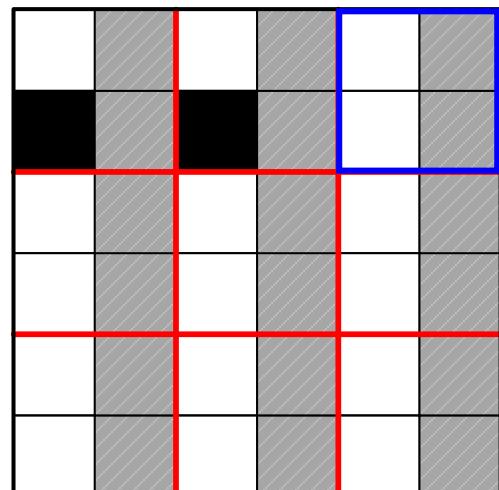
$P_1$



$S_1$



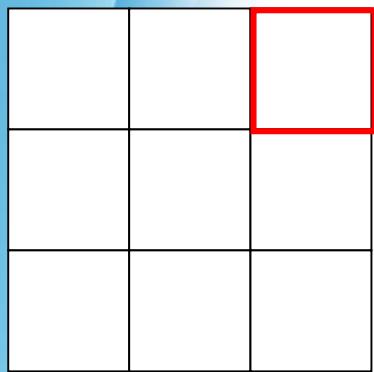
$S_2$



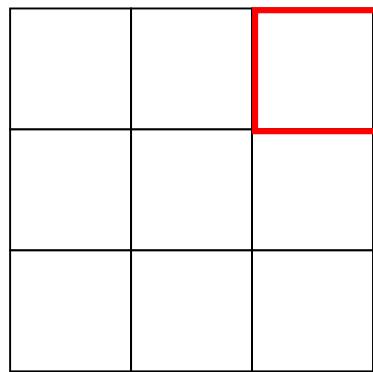
# 平移式視覺密碼

(Wu and Yang, 2001)

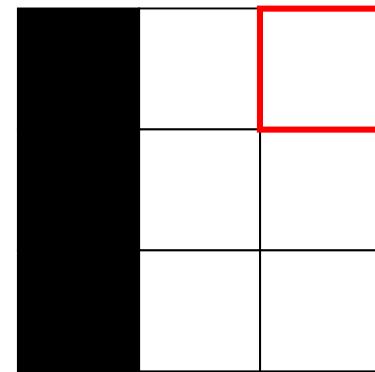
$S_1$



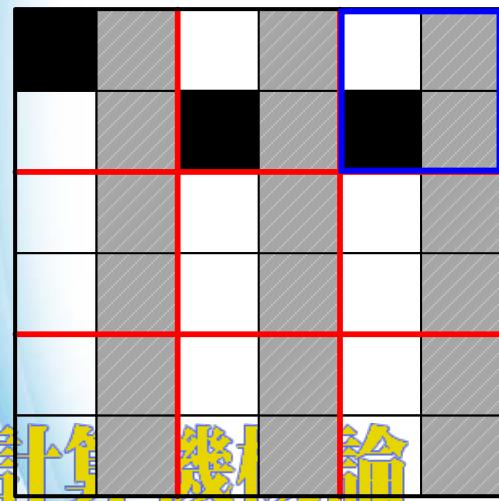
$S_2$



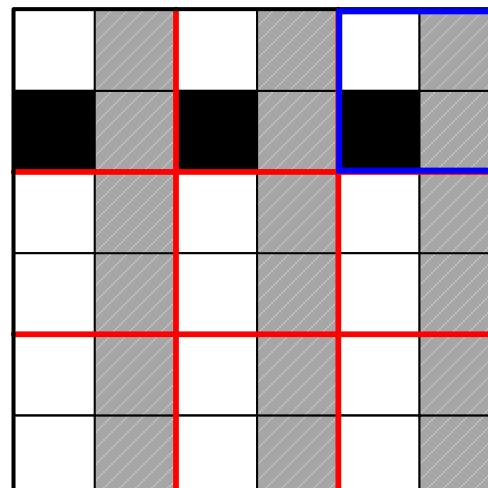
$P_1$



$S_1$



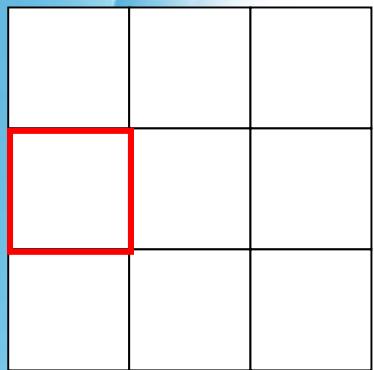
$S_2$



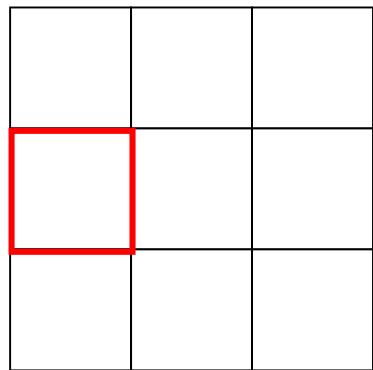
# 平移式視覺密碼

(Wu and Yang, 2001)

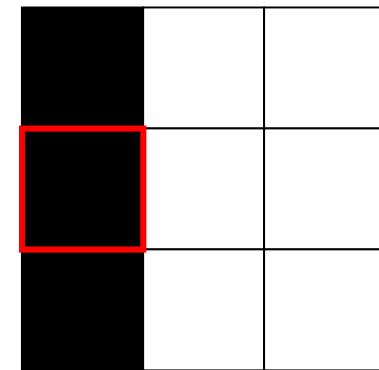
$S_1$



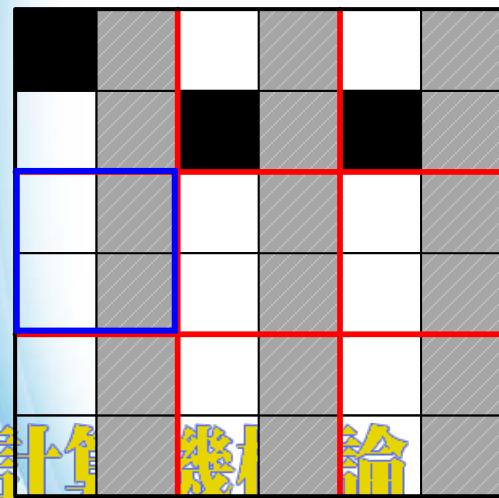
$S_2$



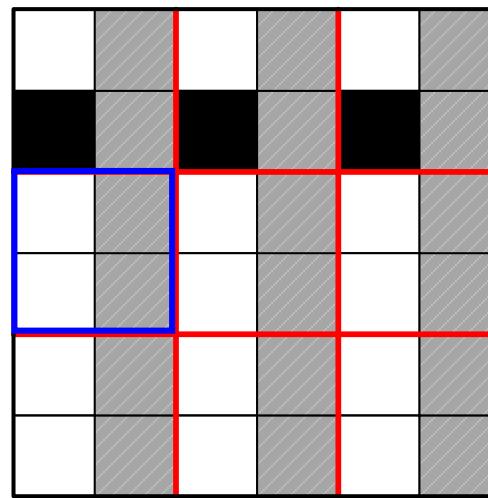
$P_1$



$S_1$



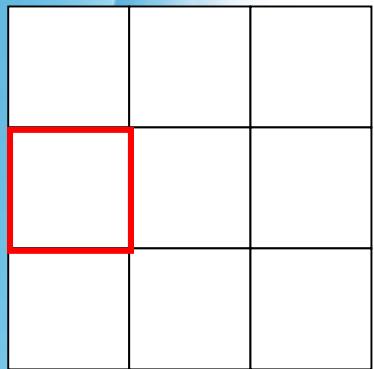
$S_2$



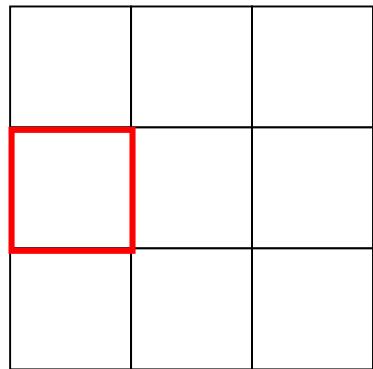
# 平移式視覺密碼

(Wu and Yang, 2001)

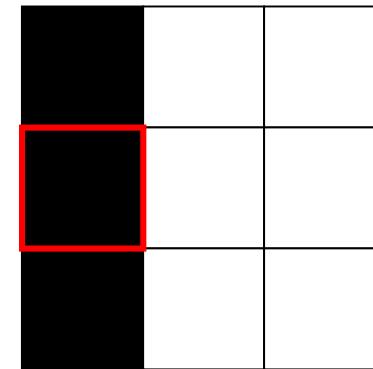
$S_1$



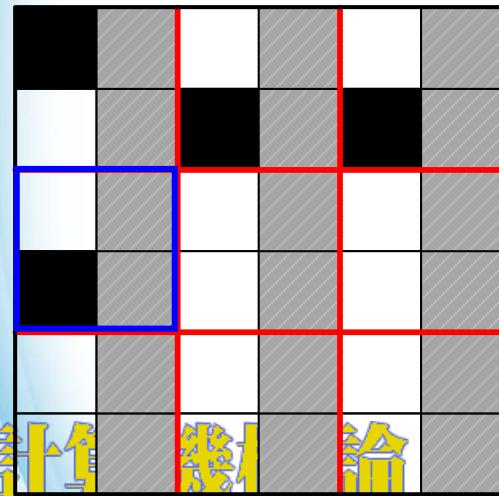
$S_2$



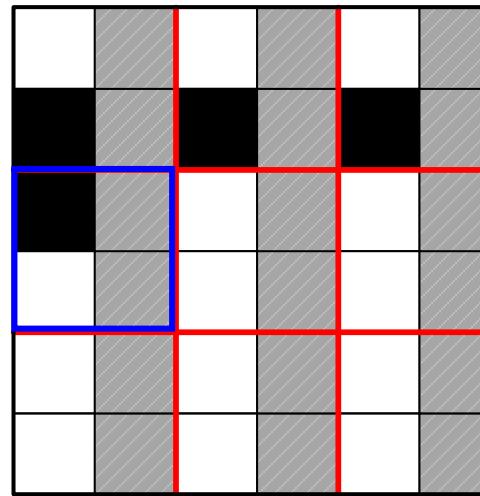
$P_1$



$S_1$



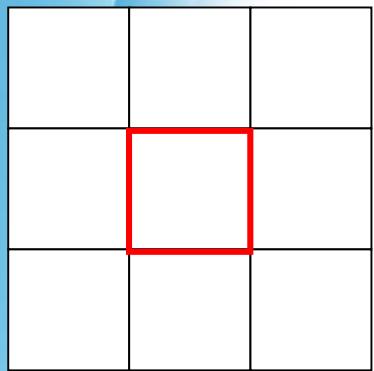
$S_2$



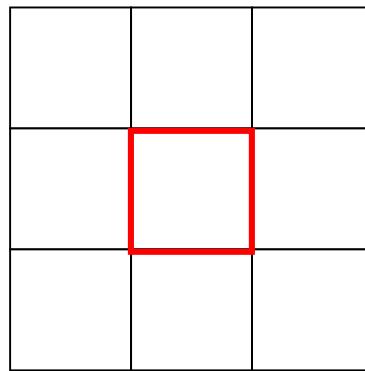
# 平移式視覺密碼

(Wu and Yang, 2001)

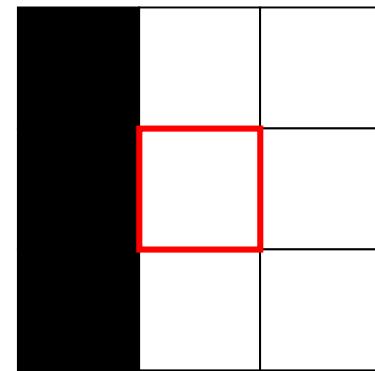
$S_1$



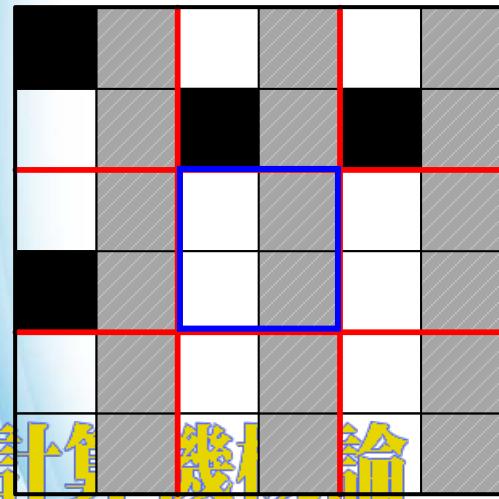
$S_2$



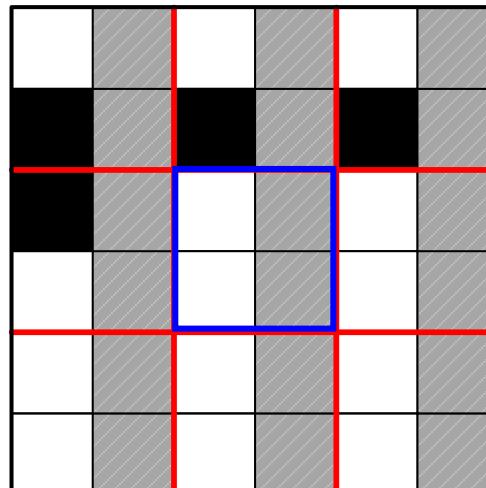
$P_1$



$S_1$



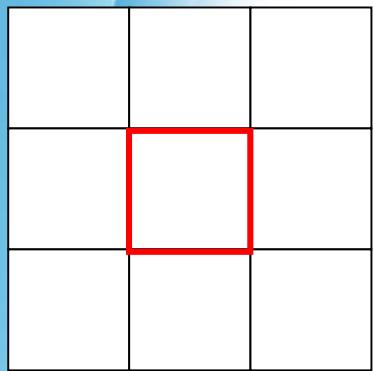
$S_2$



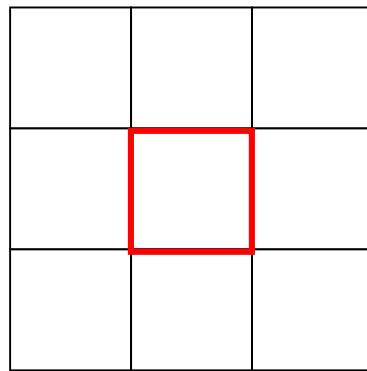
# 平移式視覺密碼

(Wu and Yang, 2001)

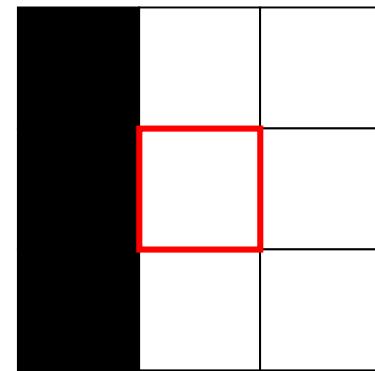
$S_1$



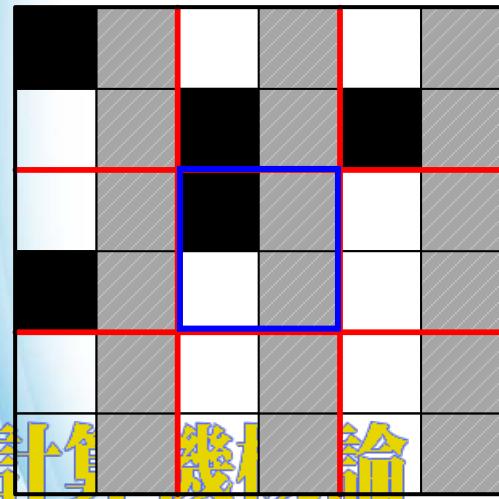
$S_2$



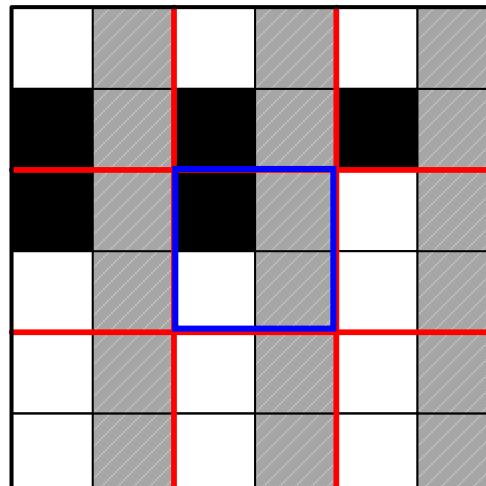
$P_1$



$S_1$



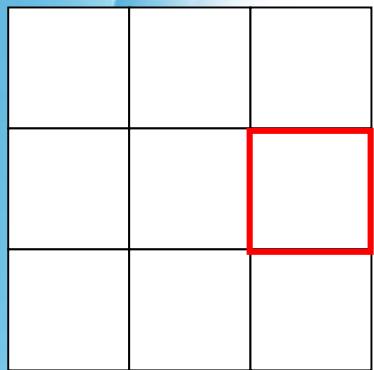
$S_2$



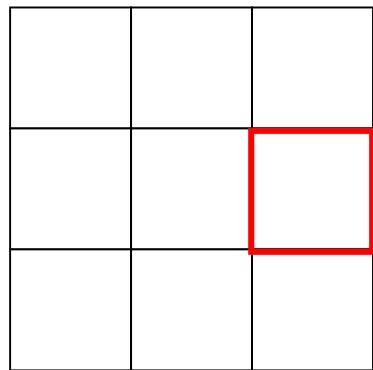
# 平移式視覺密碼

(Wu and Yang, 2001)

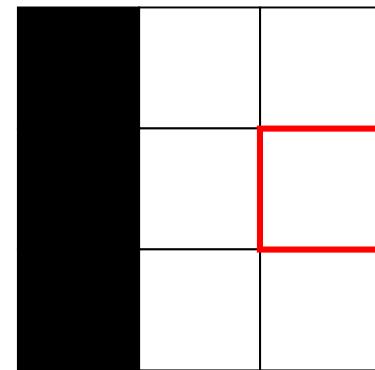
$S_1$



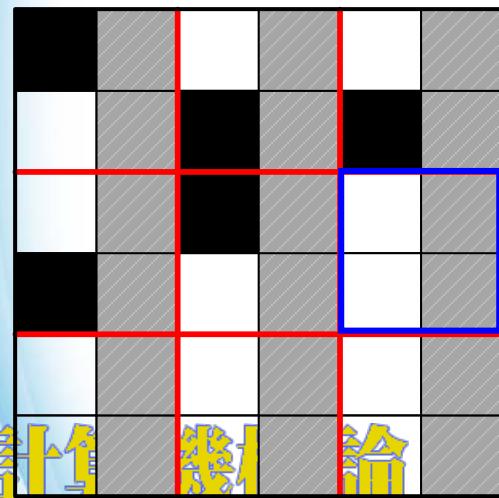
$S_2$



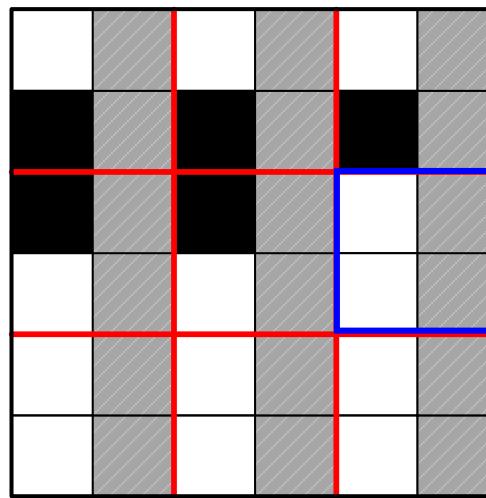
$P_1$



$S_1$



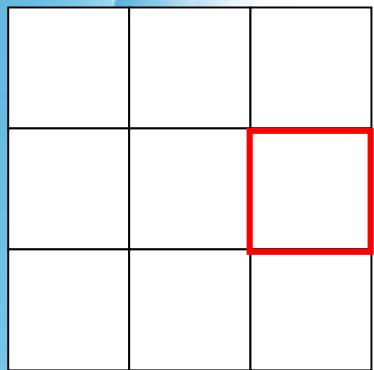
$S_2$



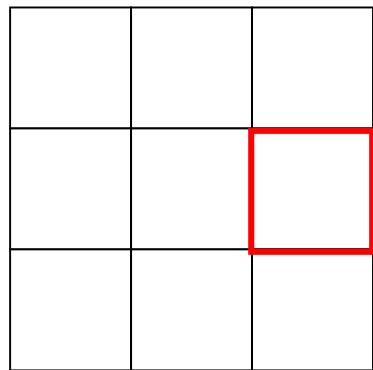
# 平移式視覺密碼

(Wu and Yang, 2001)

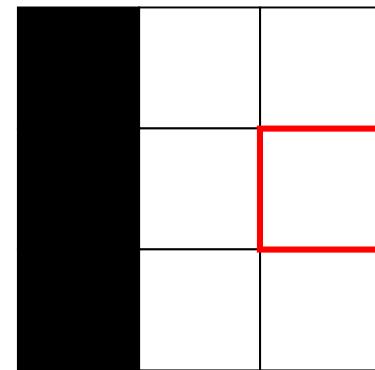
$S_1$



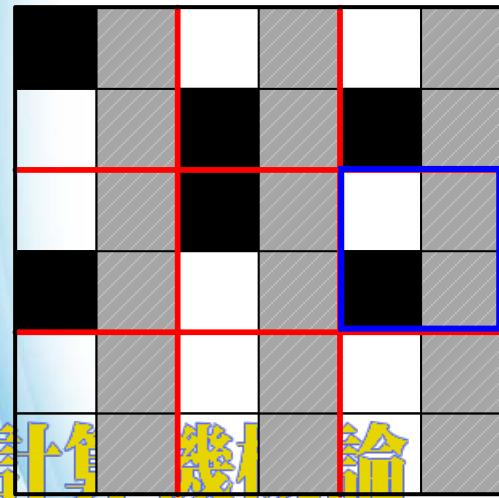
$S_2$



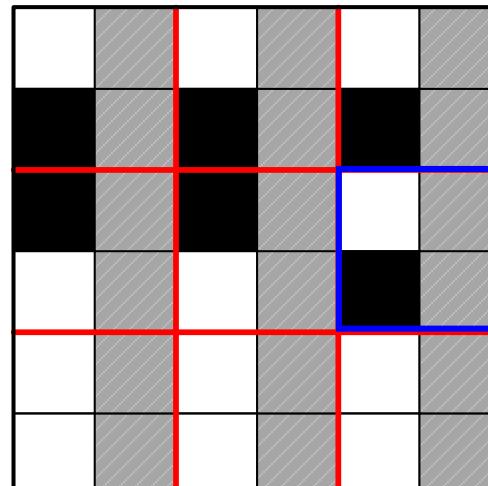
$P_1$



$S_1$



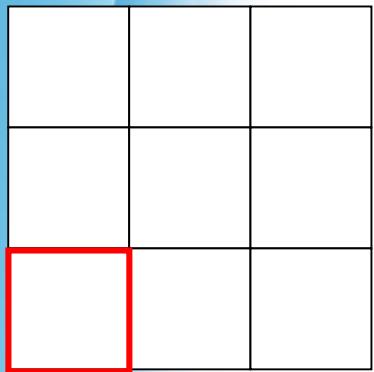
$S_2$



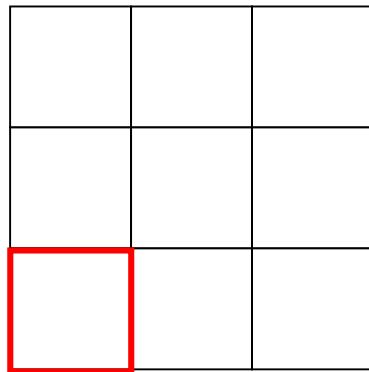
# 平移式視覺密碼

(Wu and Yang, 2001)

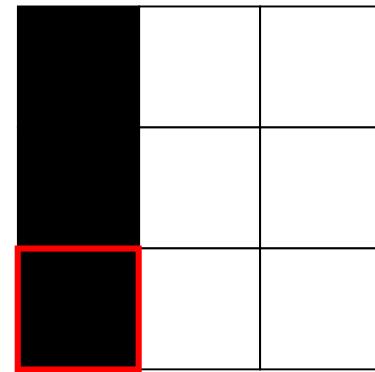
$S_1$



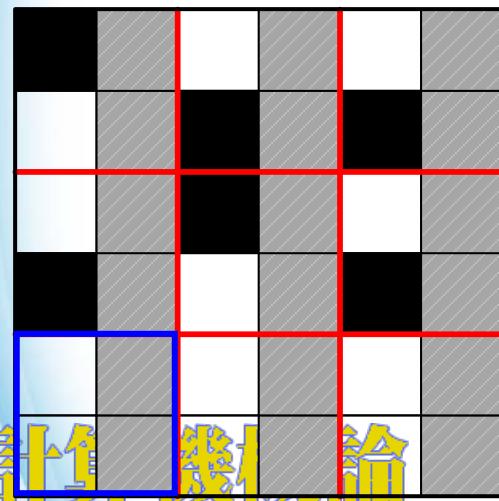
$S_2$



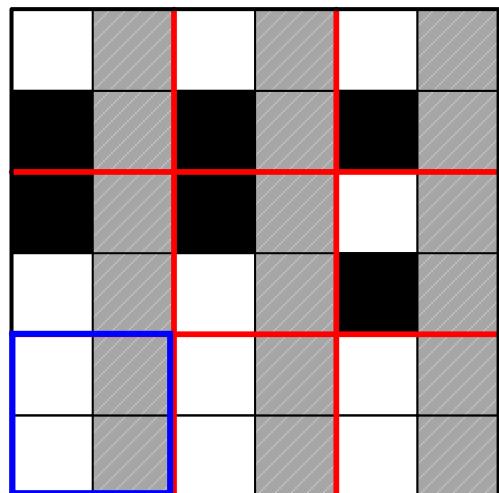
$P_1$



$S_1$



$S_2$

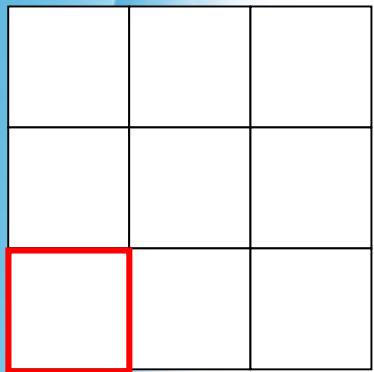


計算機理論

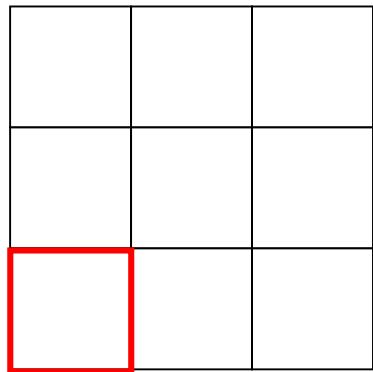
# 平移式視覺密碼

(Wu and Yang, 2001)

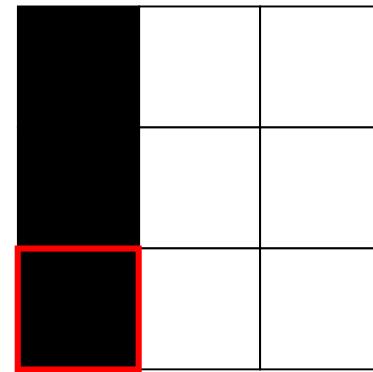
$S_1$



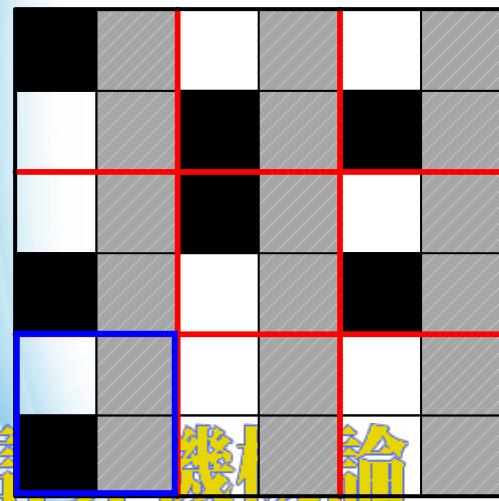
$S_2$



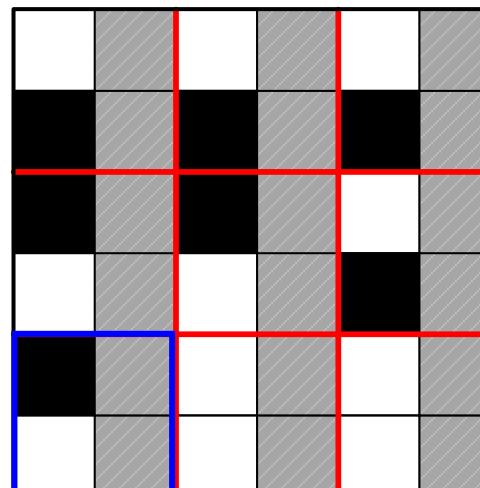
$P_1$



$S_1$



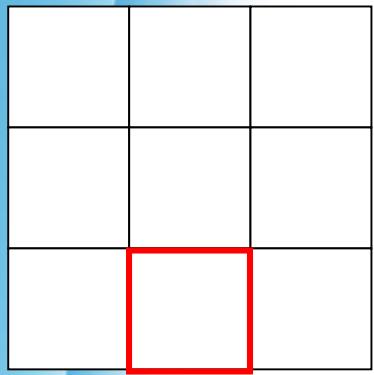
$S_2$



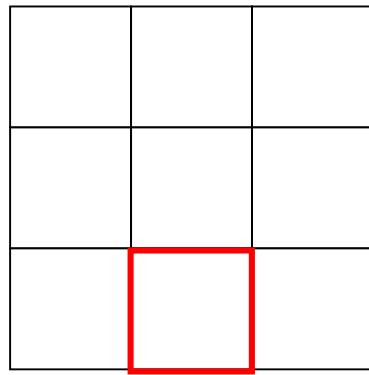
# 平移式視覺密碼

(Wu and Yang, 2001)

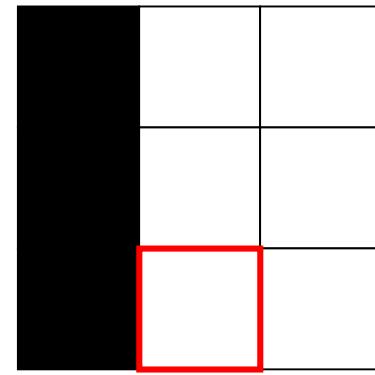
$S_1$



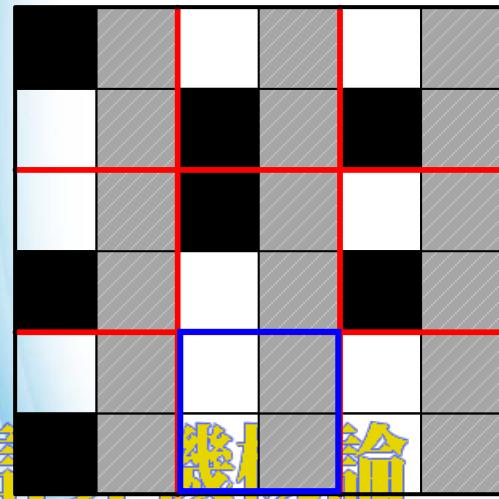
$S_2$



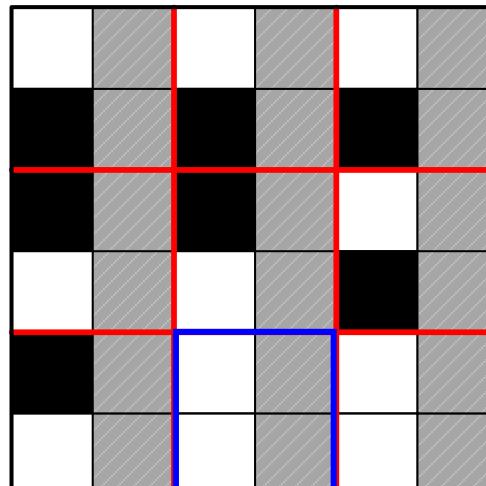
$P_1$



$S_1$



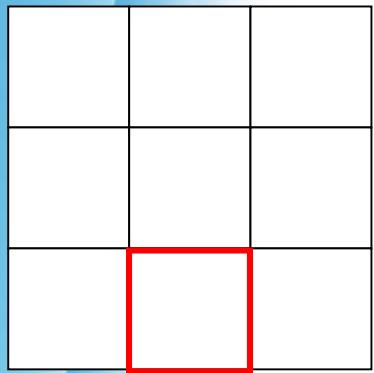
$S_2$



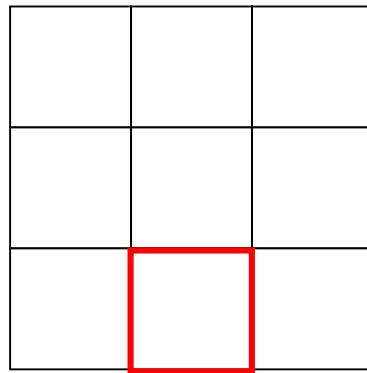
# 平移式視覺密碼

(Wu and Yang, 2001)

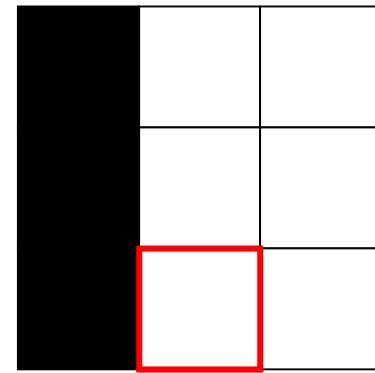
$S_1$



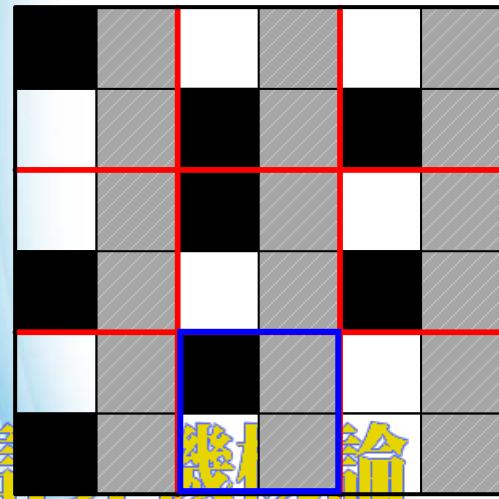
$S_2$



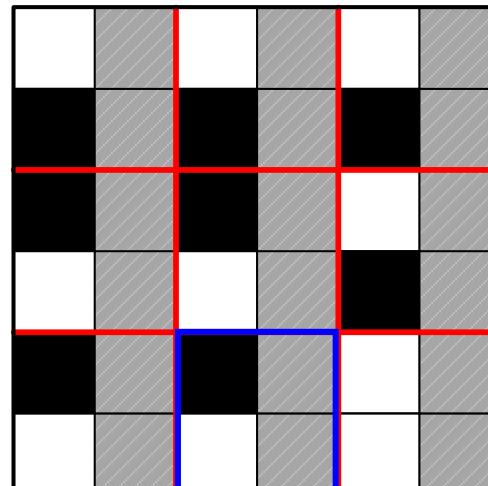
$P_1$



$S_1$



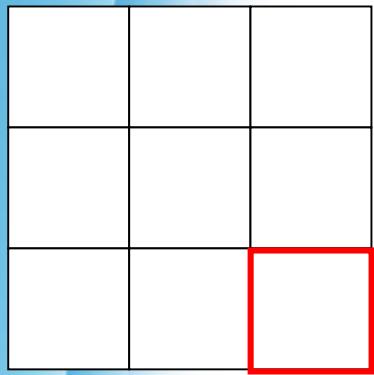
$S_2$



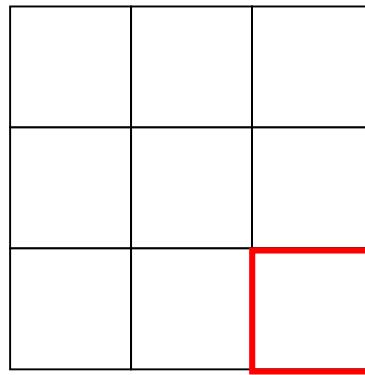
# 平移式視覺密碼

(Wu and Yang, 2001)

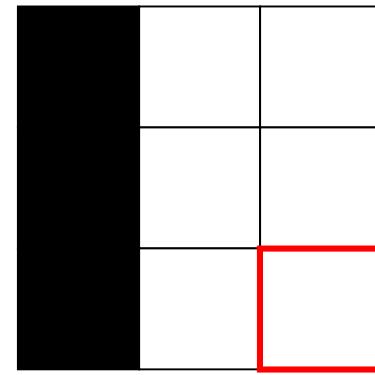
$S_1$



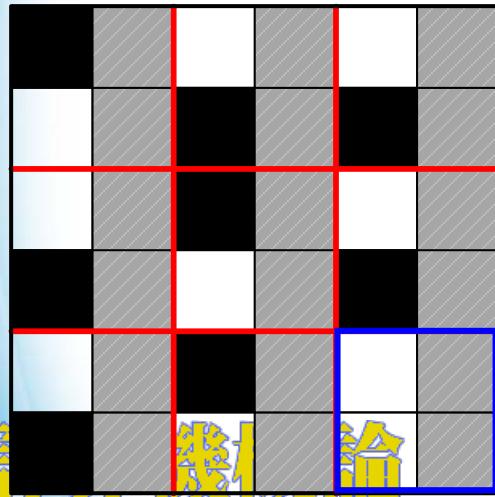
$S_2$



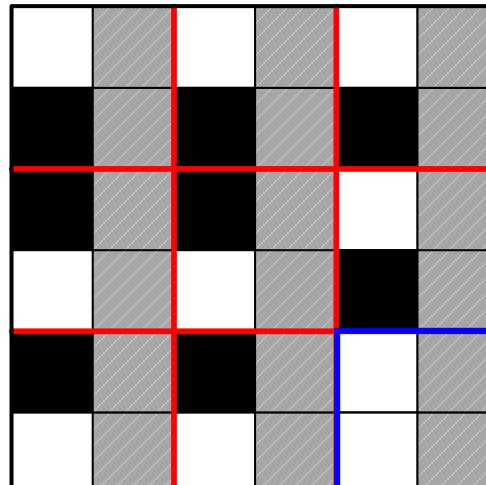
$P_1$



$S_1$



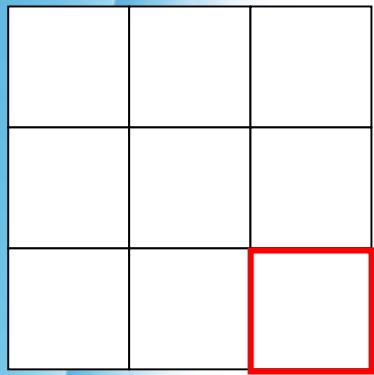
$S_2$



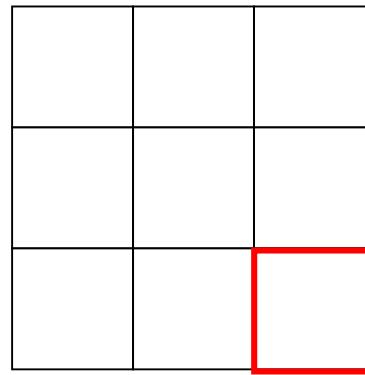
# 平移式視覺密碼

(Wu and Yang, 2001)

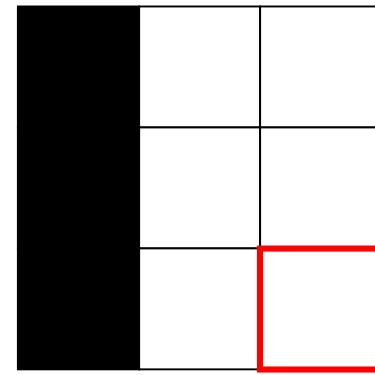
$S_1$



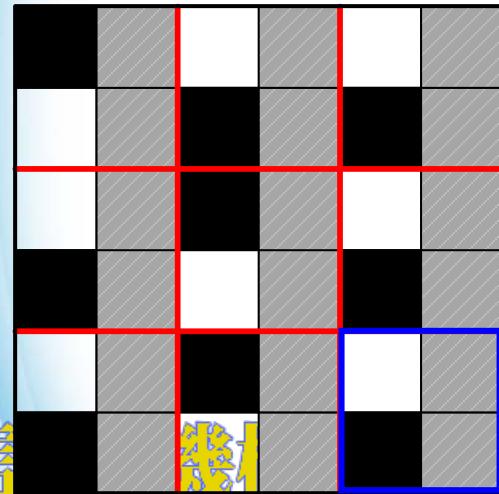
$S_2$



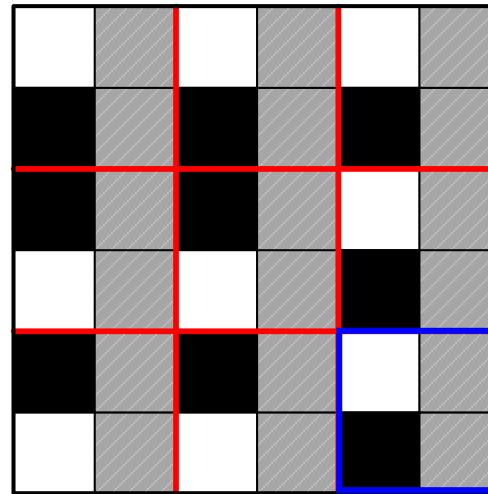
$P_1$



$S_1$

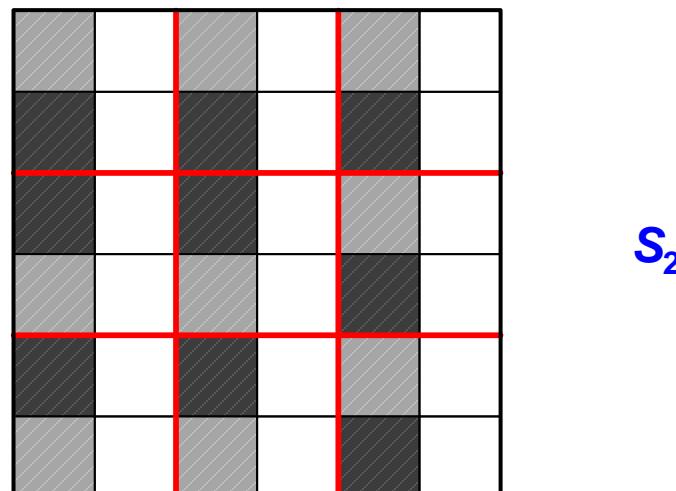
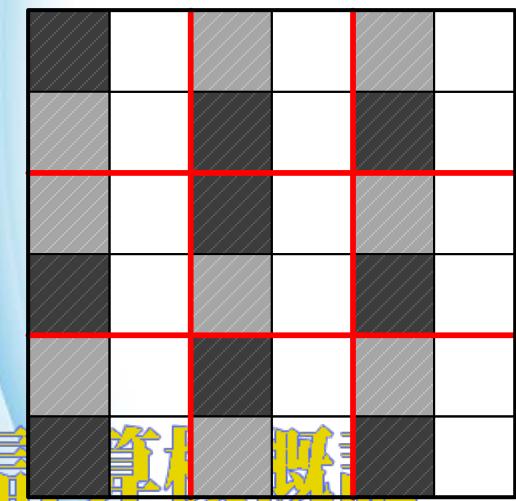
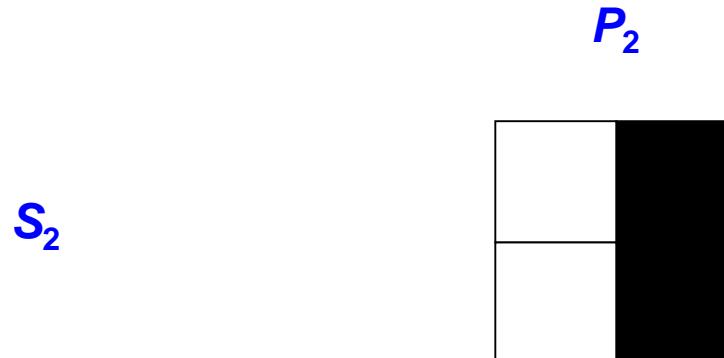
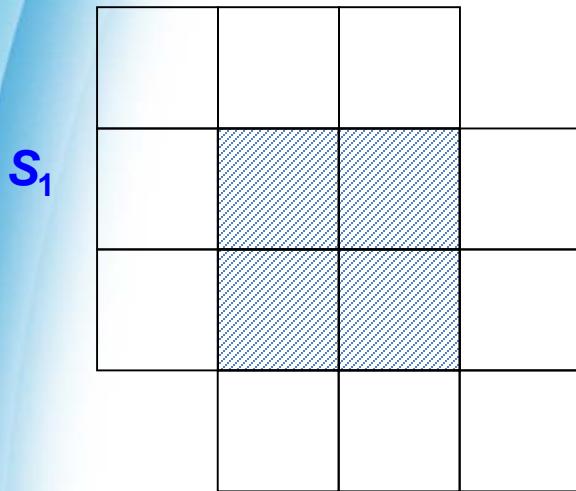


$S_2$



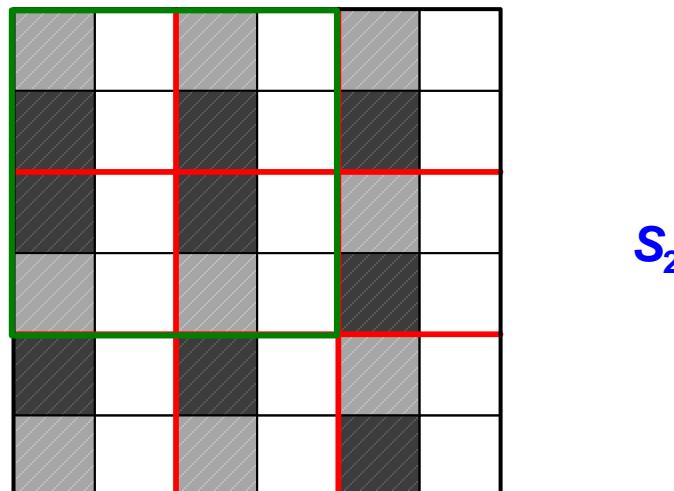
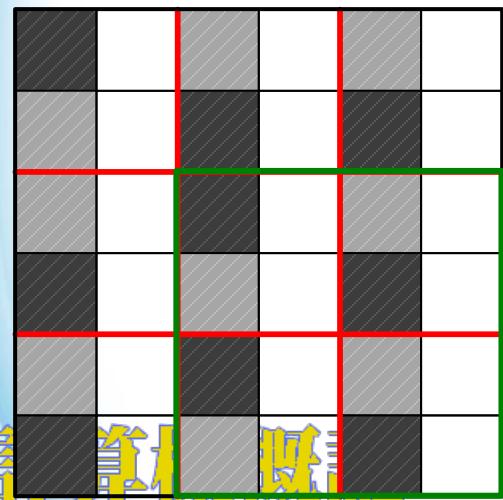
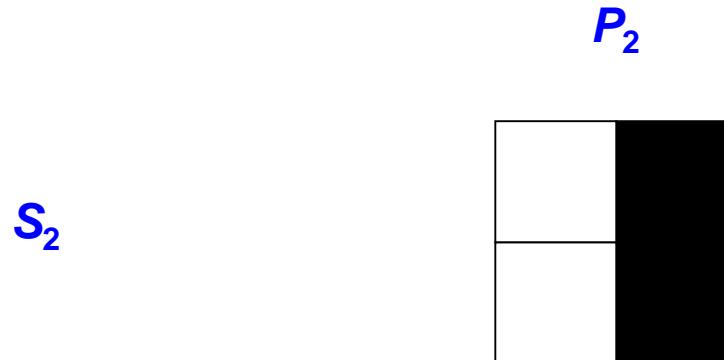
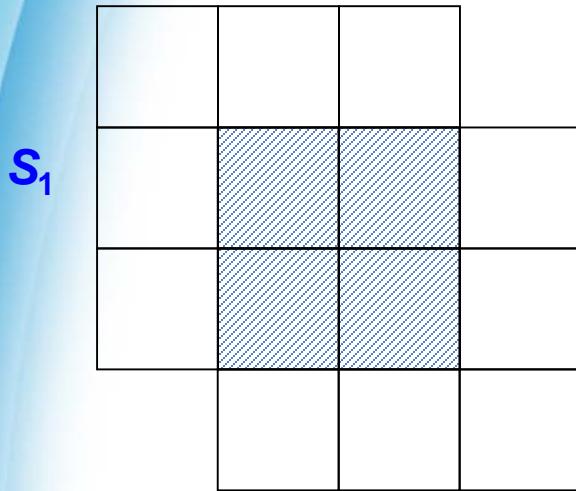
# 平移式視覺密碼

(Wu and Yang, 2001)



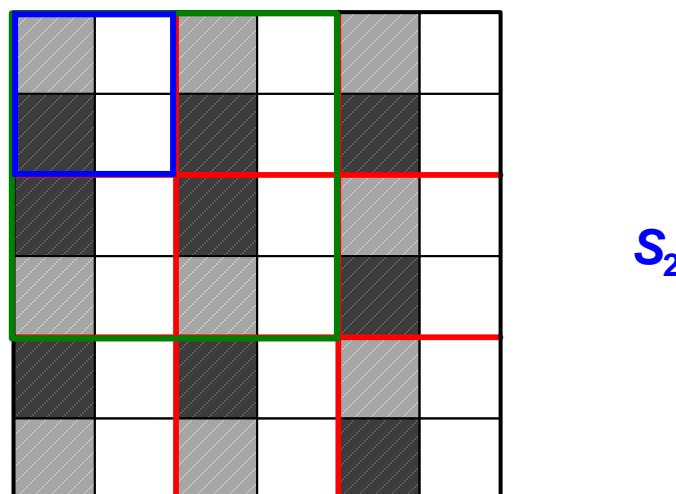
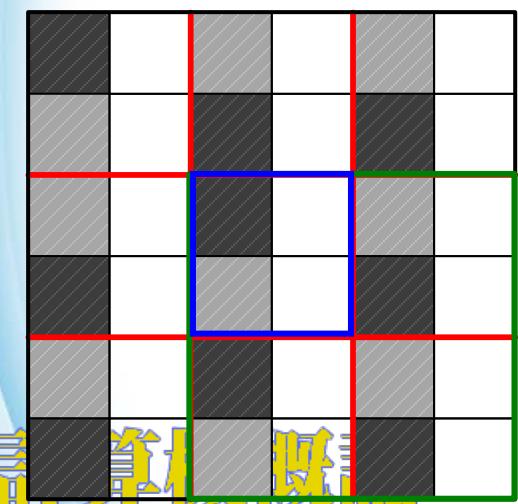
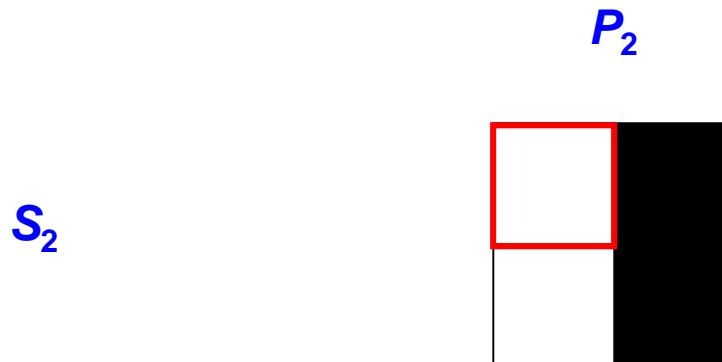
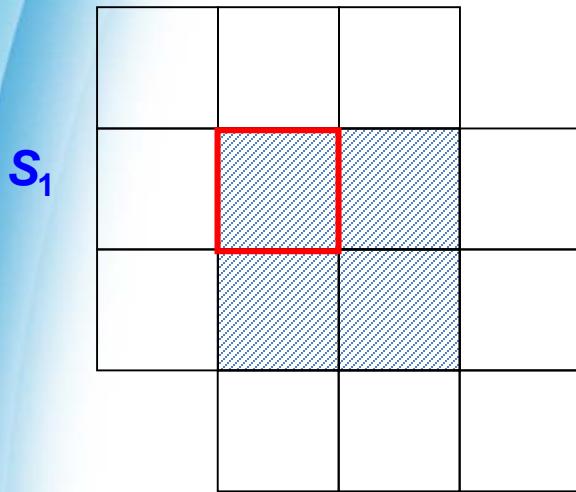
# 平移式視覺密碼

(Wu and Yang, 2001)



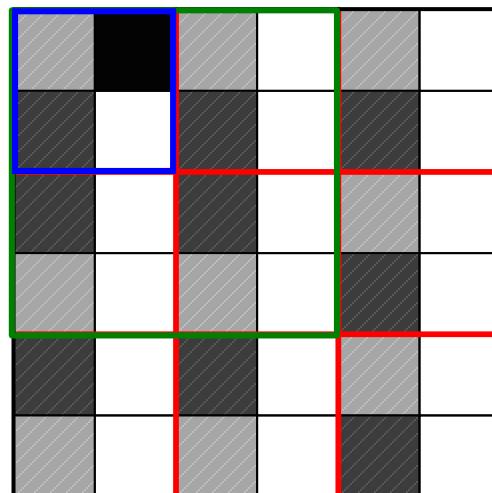
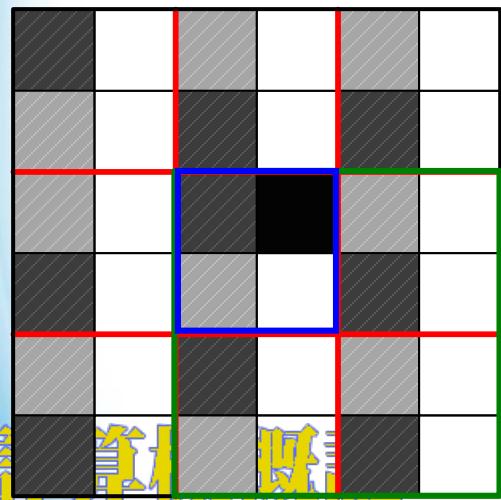
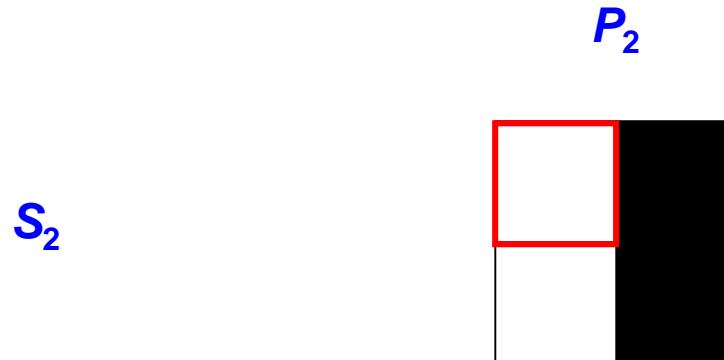
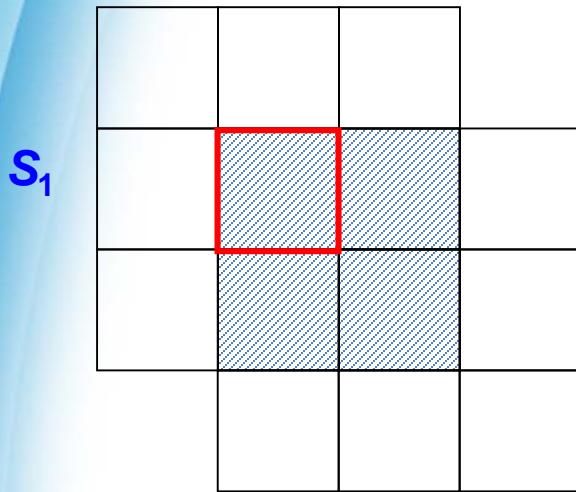
# 平移式視覺密碼

(Wu and Yang, 2001)



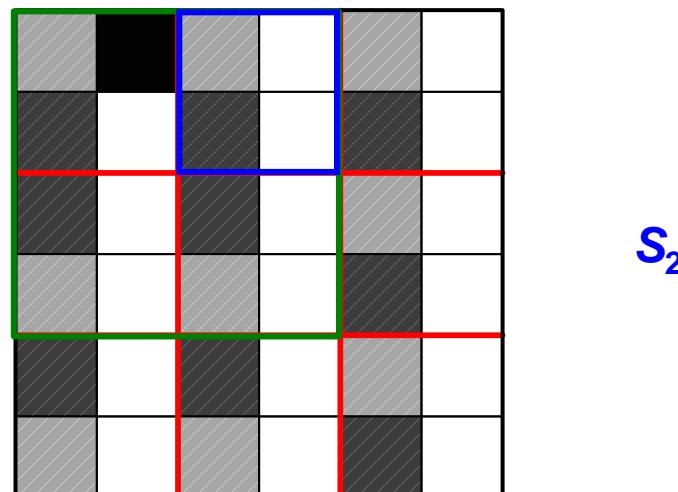
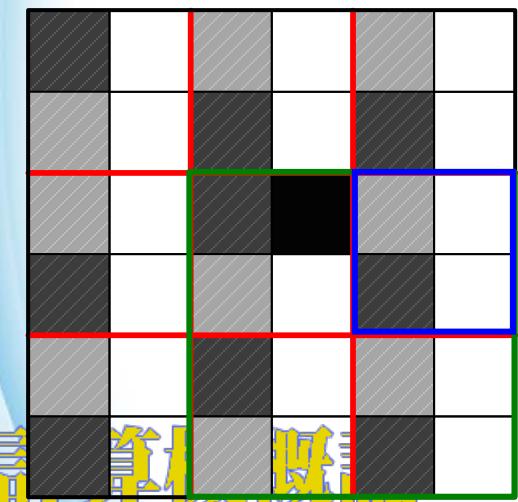
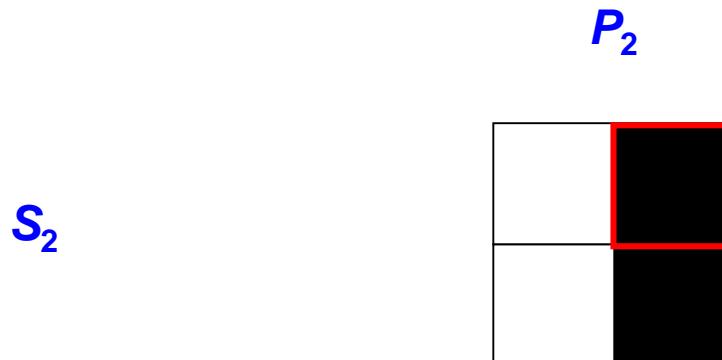
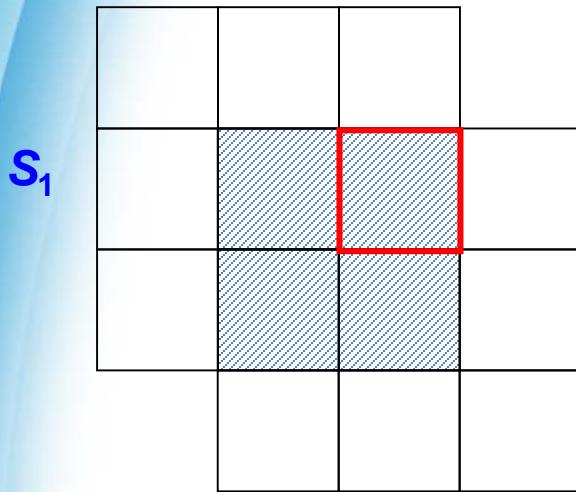
# 平移式視覺密碼

(Wu and Yang, 2001)



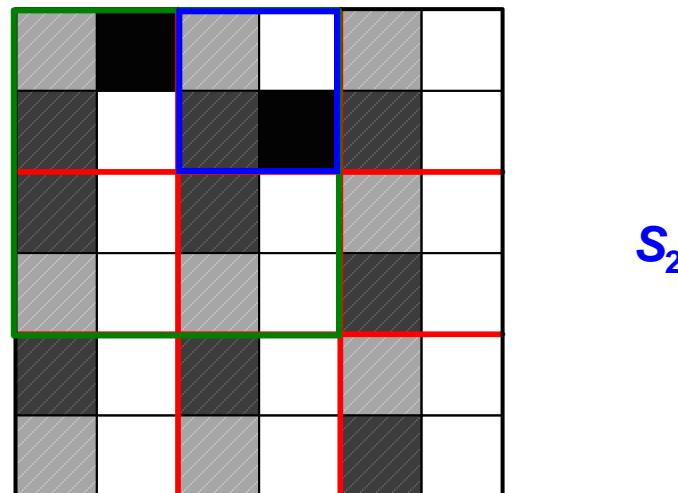
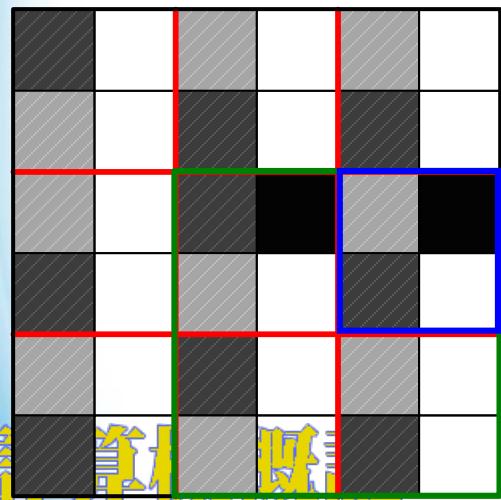
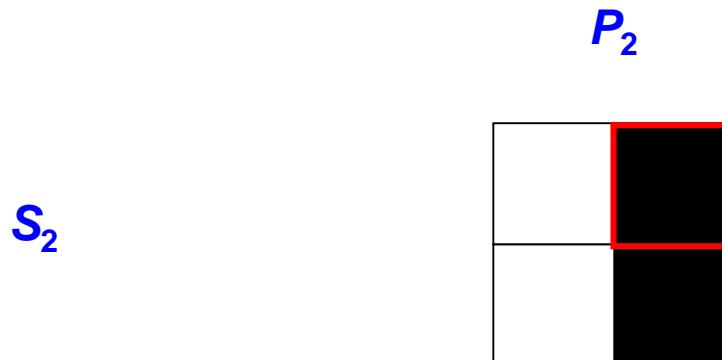
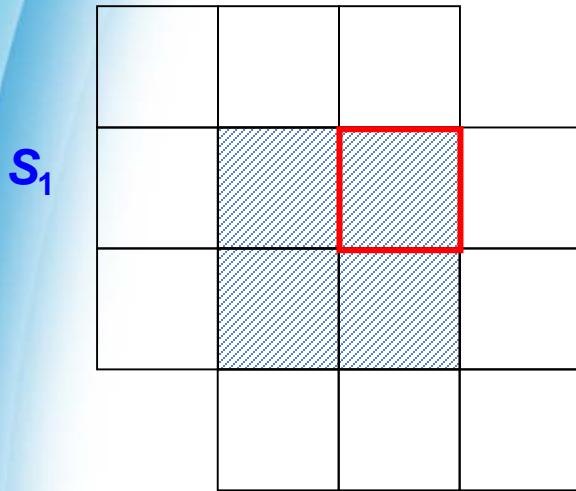
# 平移式視覺密碼

(Wu and Yang, 2001)



# 平移式視覺密碼

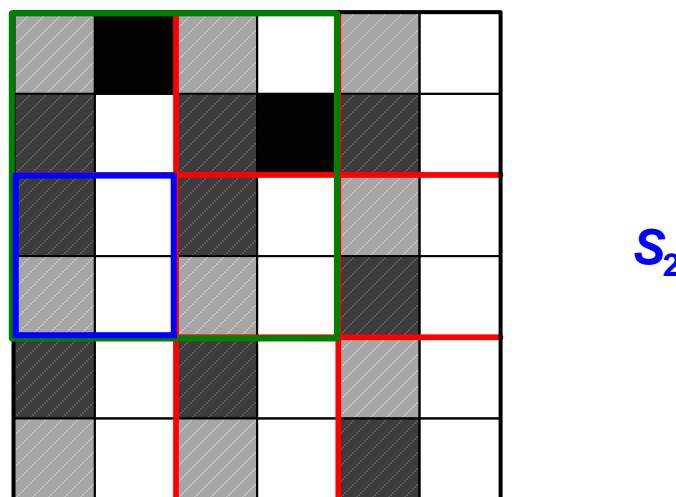
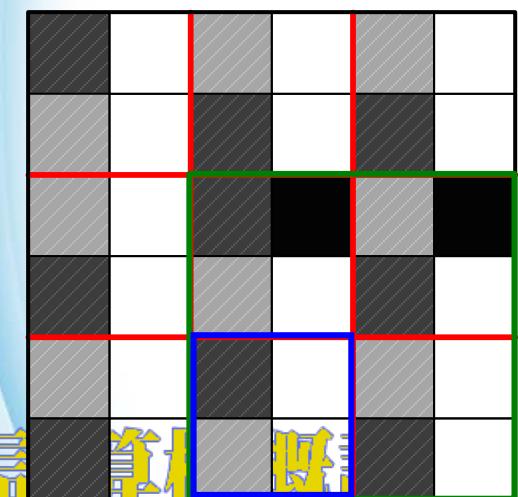
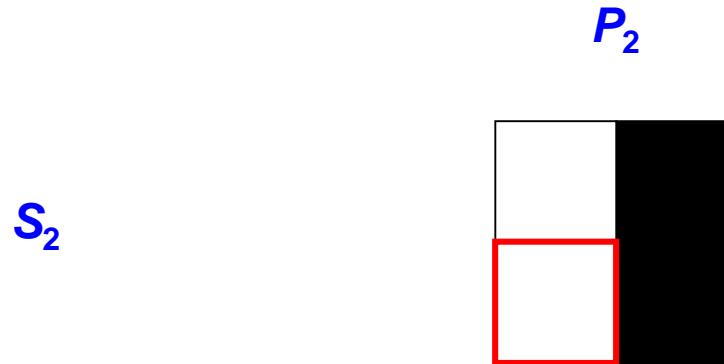
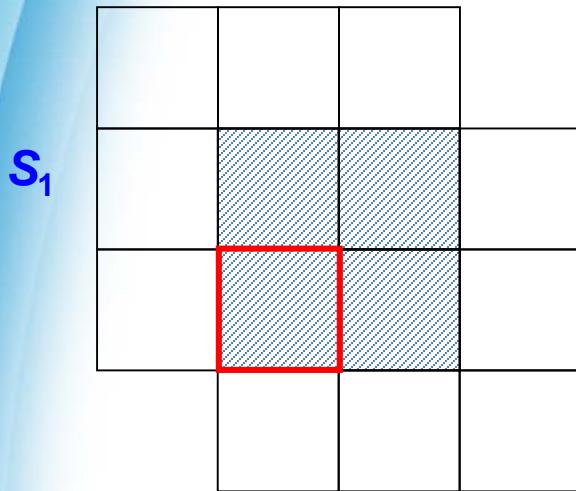
(Wu and Yang, 2001)



清华大学  
计算机系  
视觉组

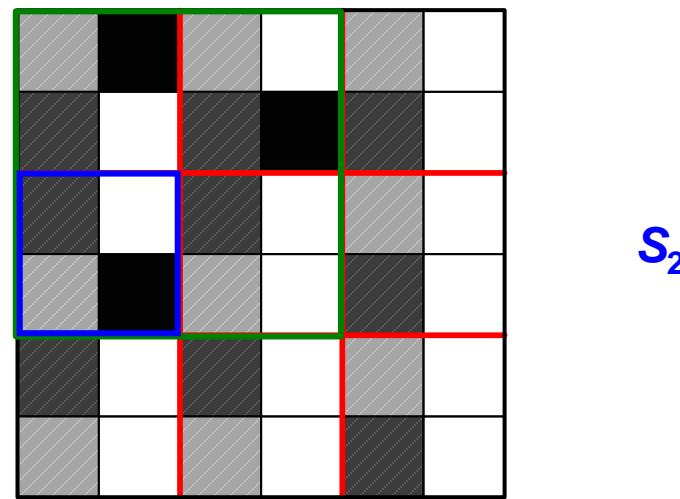
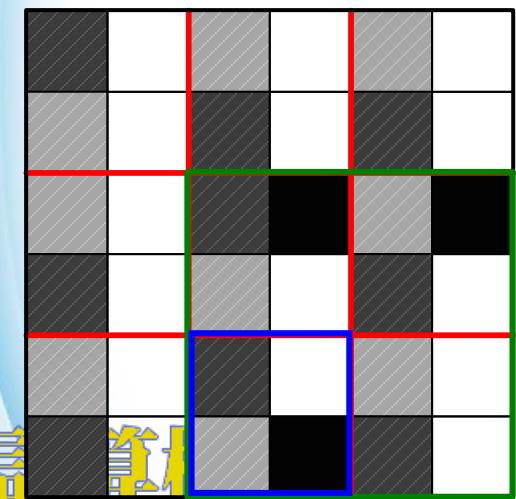
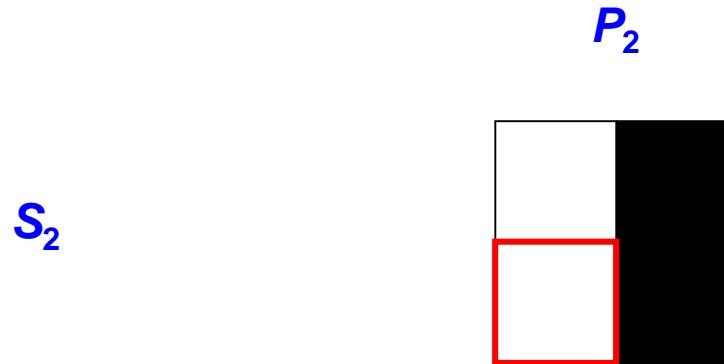
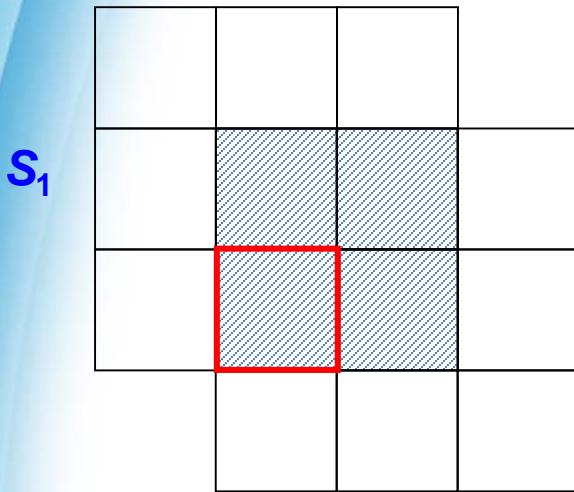
# 平移式視覺密碼

(Wu and Yang, 2001)



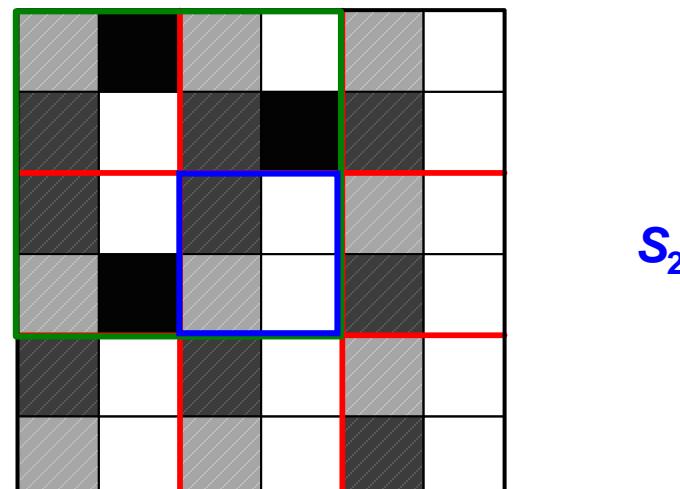
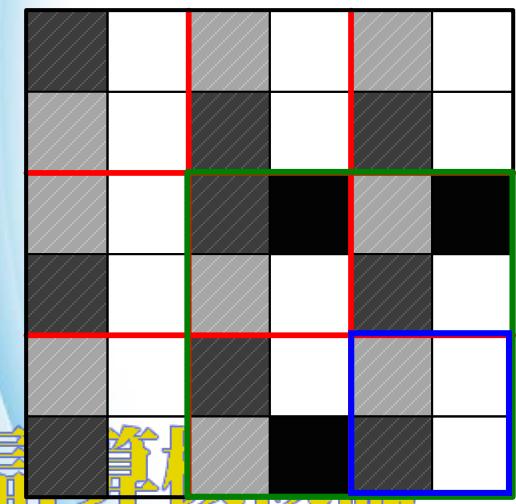
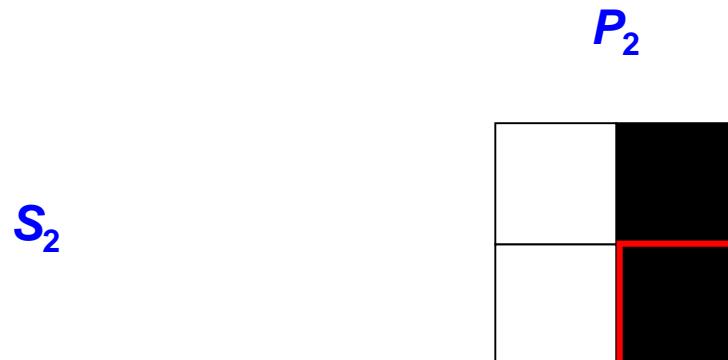
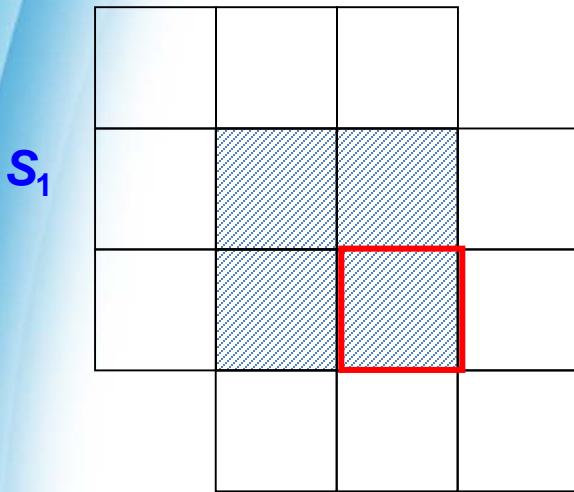
# 平移式視覺密碼

(Wu and Yang, 2001)



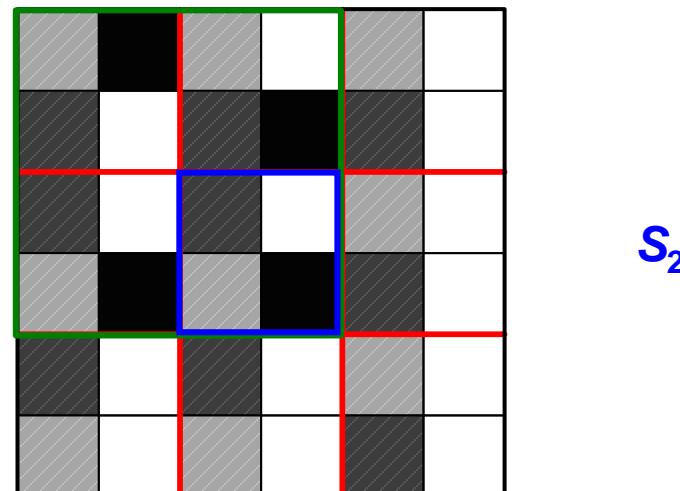
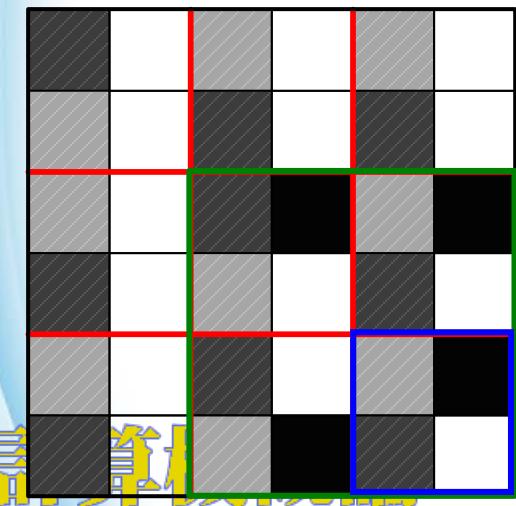
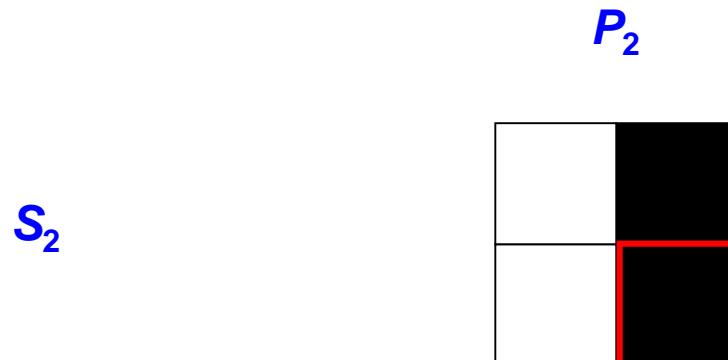
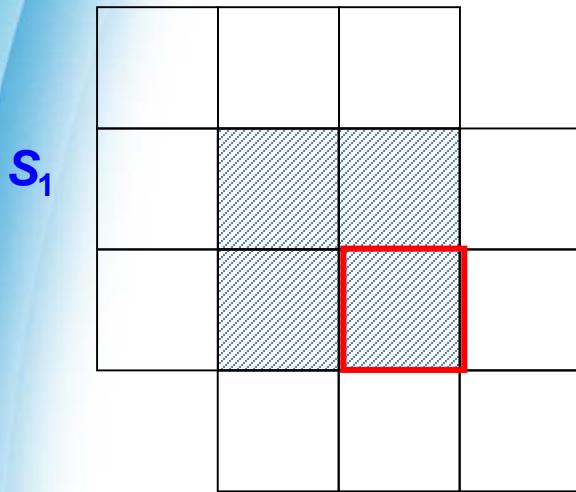
# 平移式視覺密碼

(Wu and Yang, 2001)



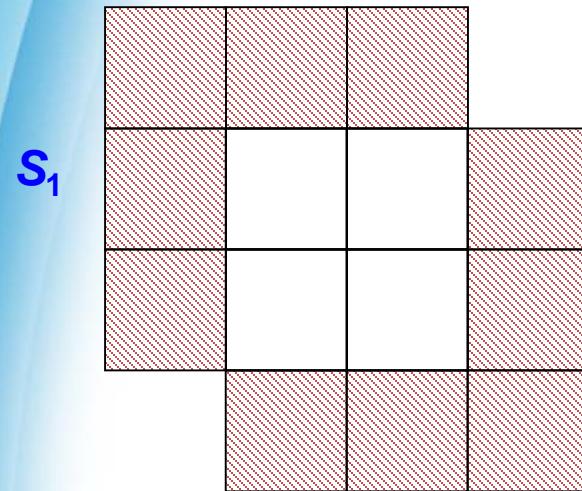
# 平移式視覺密碼

(Wu and Yang, 2001)



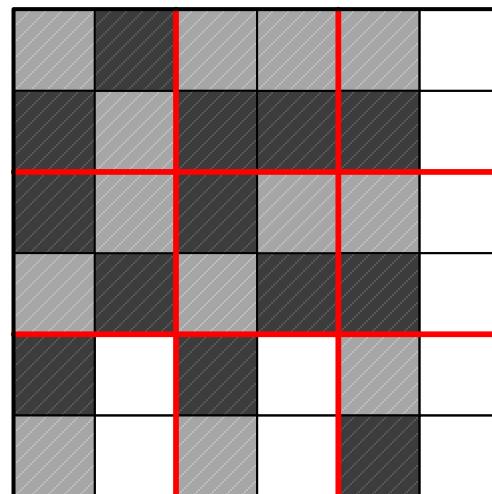
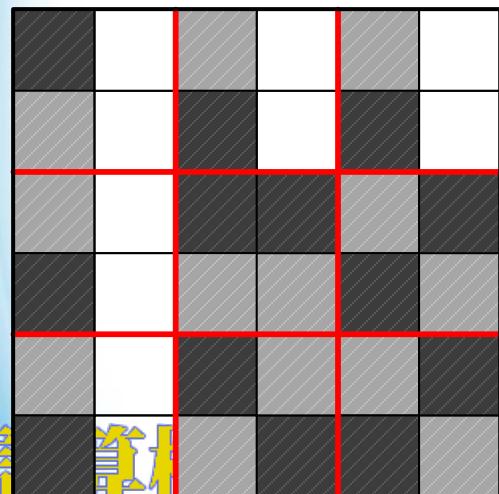
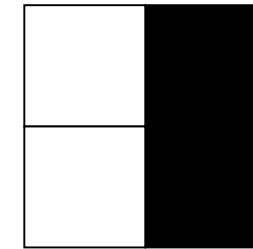
# 平移式視覺密碼

(Wu and Yang, 2001)



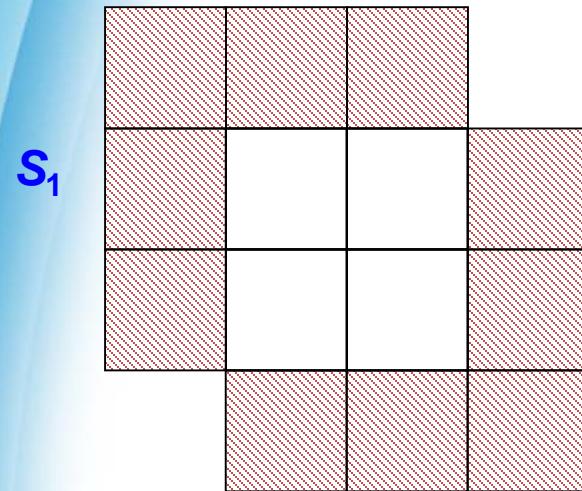
$S_2$

$P_2$



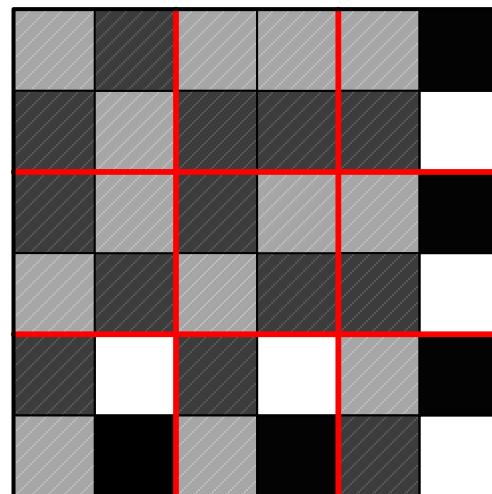
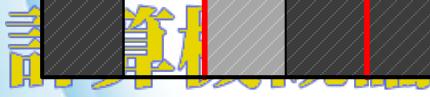
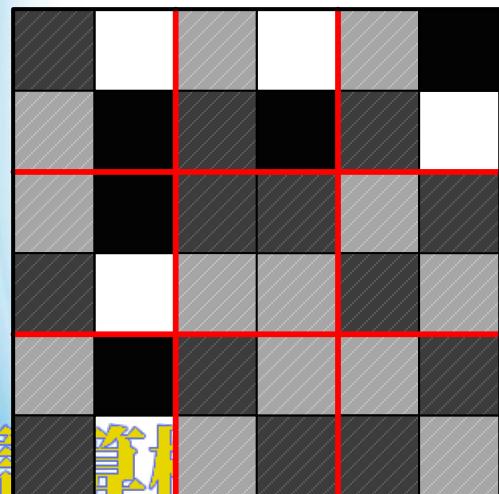
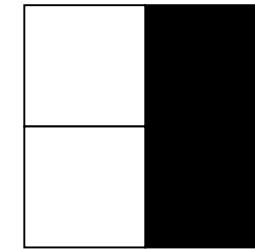
# 平移式視覺密碼

(Wu and Yang, 2001)



$S_2$

$P_2$

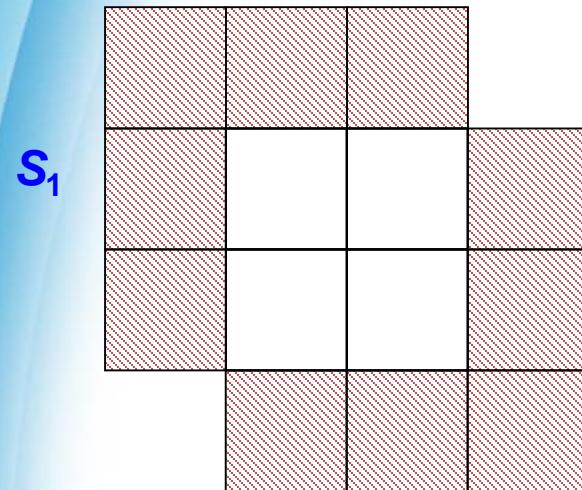


$S_2$



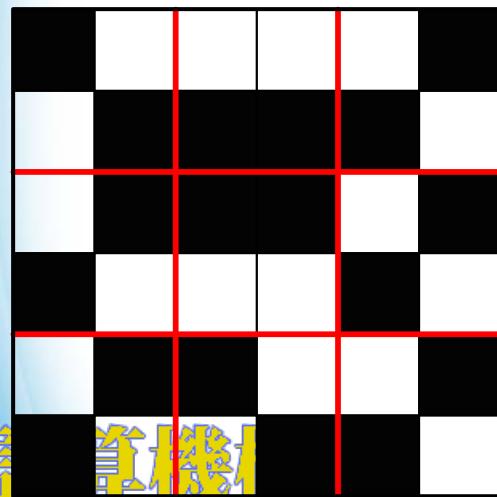
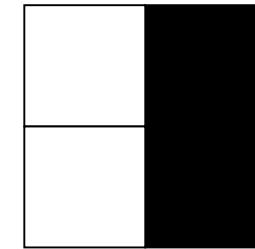
# 平移式視覺密碼

(Wu and Yang, 2001)

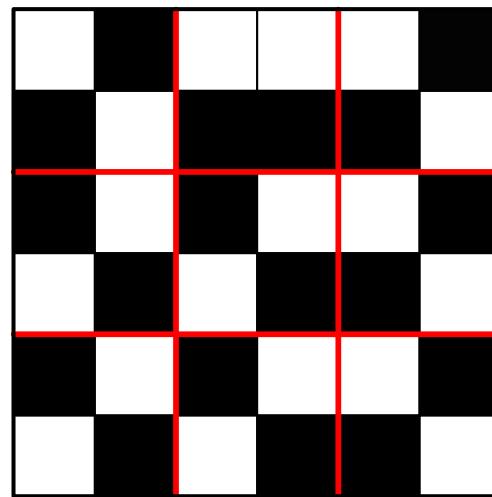


$S_2$

$P_2$



$S_1$



$S_2$

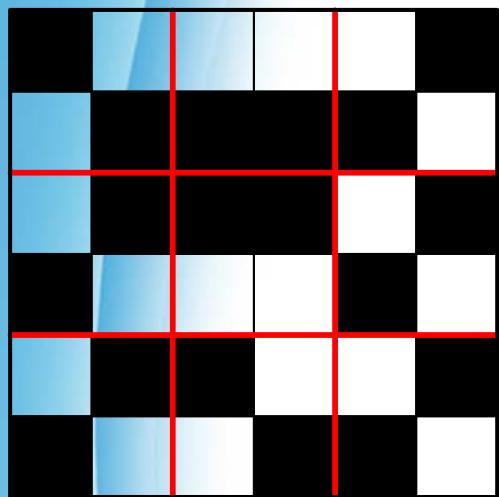


視覺密碼

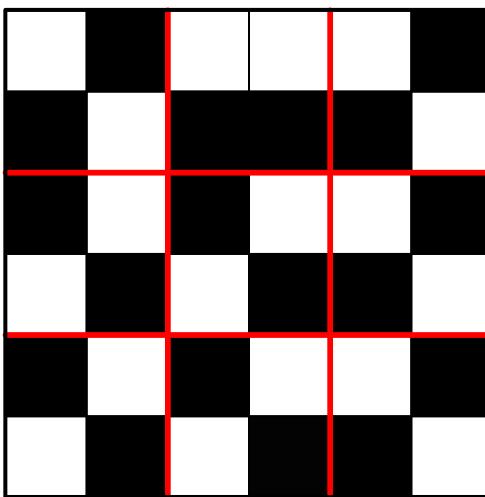
# 平移式視覺密碼

(Wu and Yang, 2001)

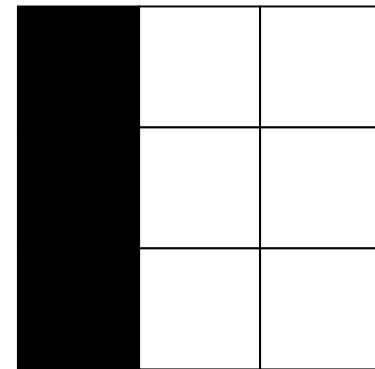
$S_1$



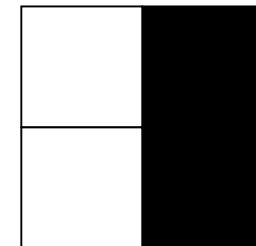
$S_2$



$P_1$



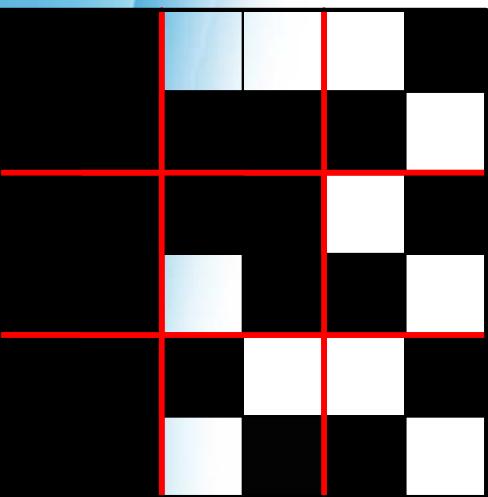
$P_2$



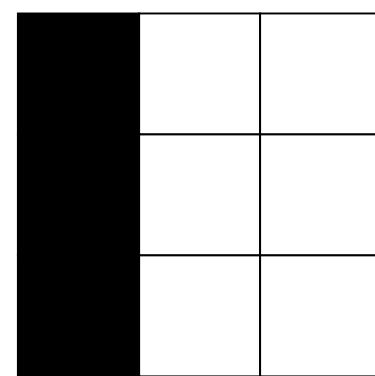
# 平移式視覺密碼

(Wu and Yang, 2001)

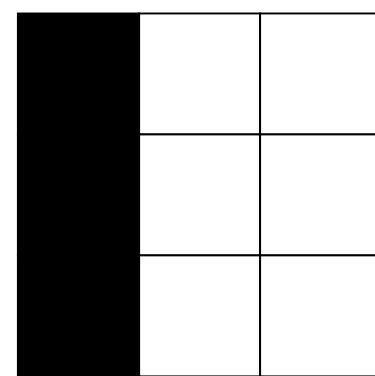
$S_1$



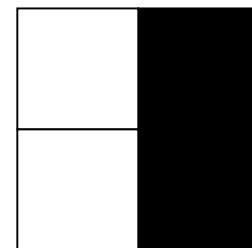
$S_2$



$P_1$



$P_2$



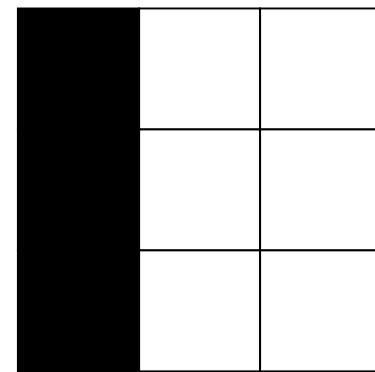
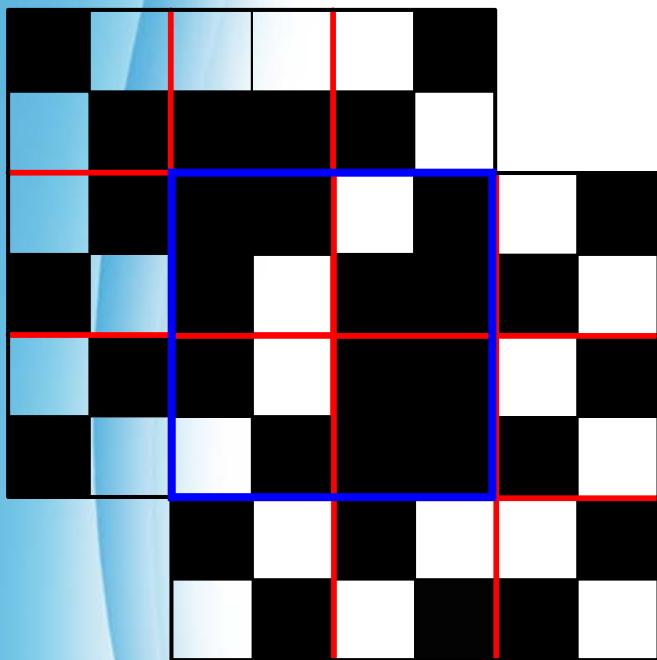
# 平移式視覺密碼

(Wu and Yang, 2001)

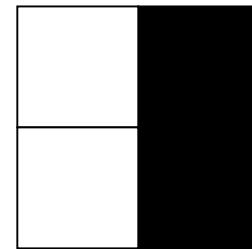
$S_1$

$S_2$

$P_1$



$P_2$



# Related Work

	Shadow shape	Number of secrets	Operator	Pixel expansion	Contrast
Wu & Chen (1998)	square	2	rotation (90°)	4	1/4
Wu, Chang (2005)	circular	2	rotation ( $\theta$ )	4	1/4, 1/2
Shyu et. al. (2007)	circular	$x \geq 2$	rotation ( $\theta=360^\circ/x$ )	$2x$	$1/2x, 1/2$
Feng et. al. (2008)	cylinder	$x \geq 2$	rotation ( $\theta=360^\circ/x$ )	$3x$	$1/3x, 1/3x$
Chen et. al. (2009)	cylinder	4	rotation & flipping	9	2/9
Shyu & Chen (2010)	circular & cylinder	$x \geq 2$	rotation (any $\theta$ )	1	$1/2^x$
Wu et. al. (2006)	rectangle	2	flipping	8	color
Shyu & Chen (2010)	square	2, 4, 8	flipping	4, 9, 16 (2x)	1/4, 1/9, 1/16



# Related Work

	Shadow shape	Number of secrets	Operator	Pixel expansion	Contrast
Wu & Chen (1998)	square	2	rotation (90°)	4	1/4
Wu, Chang (2005)	circular	2	rotation ( $\theta$ )	4	1/4, 1/2
Shyu et. al. (2007)	circular	$x \geq 2$	$S_1$	2	1/2
Feng et. al. (2008)	cylinder	$x \geq 2$		3	1/3x
Chen et. al. (2009)	cylinder	4	rotation &	9	2/9
Shyu & Chen (2010)	circular & cylinder	$x \geq 2$	$S_2$	2	$2^x$
Wu et. al. (2006)	rectangle	2		4, 9,	or
Shyu & Chen (2010)	square	2, 4, 8		16, 25,	1/16



# Related Work

	Shadow shape	Number of secrets	Operator	Pixel expansion	Contrast
Wu & Chen (1998)	square	2	rotation (90°)	4	1/4
Wu, Chang (2005)	circular	2	rotation ( $\theta$ )	4	1/4, 1/2
Shyu et al. (2009)	cylindrical	4	rotation ( $\theta = 30^\circ$ ) rotation ( $\theta = 30^\circ$ ) rotation ( $\theta = 30^\circ$ ) rotation ( $\theta = 30^\circ$ )	9	1/2
Feng et al. (2010)	circular	2, 4	rotation flipping flipping	4, 9	1/2 <sup>x</sup>
Shyu et al. (2010)	cylindrical	2, 4	rotation flipping flipping	4, 9	1/2 <sup>x</sup>



# Related Work

	Shadow shape	Number of secrets	Operator	Pixel expansion	Contrast
Wu & Chen (1998)	square	2	rotation (90°)	4	1/4
Wu, Chang (2005)	circular	2	rotation ( $\theta$ )	4	1/4, 1/2
Shyu et. al. (2007)	circular	$x \geq 2$	rotation ( $\theta=360^\circ/x$ )	$2x$	$1/2x, 1/2$

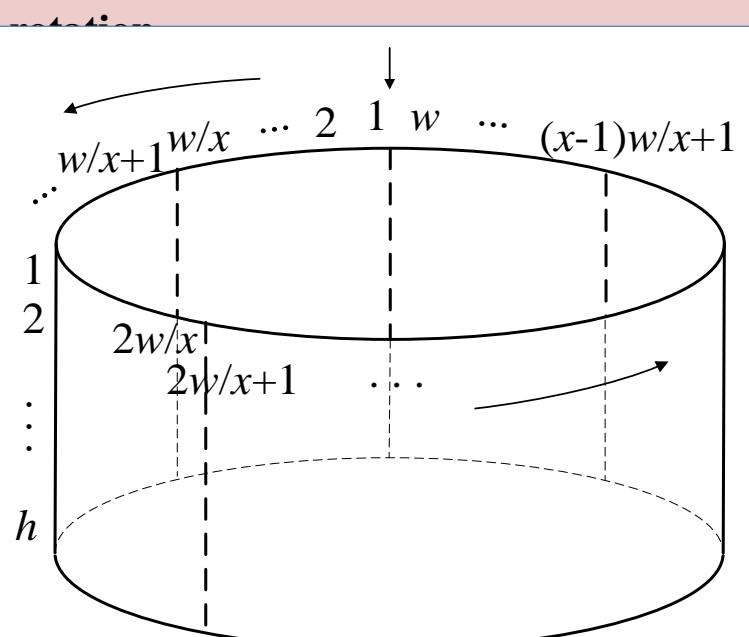
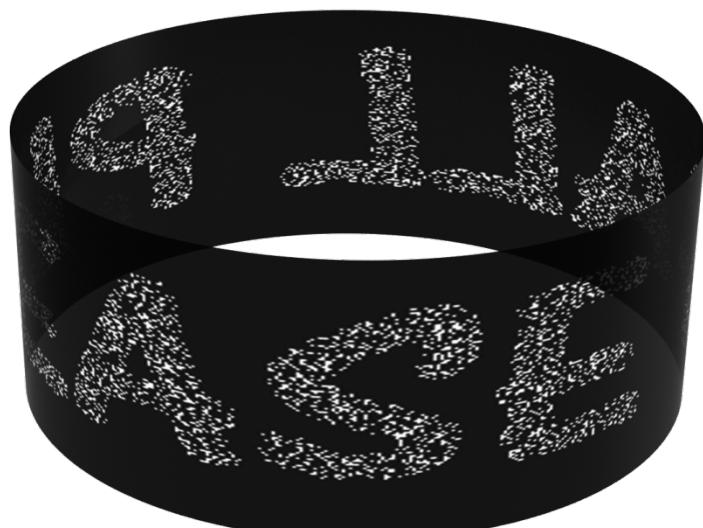
Feng et. al.

Chen et. al.

Shyu & Chen

Wu et. al.

Shyu & Chen



計

# Related Work

	Shadow shape	Number of secrets	Operator	Pixel expansion	Contrast
Wu & Chen (1998)	square	2	rotation (90°)	4	1/4
Wu, Chang (2005)	circular	2	rotation ( $\theta$ )	4	1/4, 1/2
Shyu et. al. (2007)	circular	$x \geq 2$	rotation ( $\theta=360^\circ/x$ )	$2x$	$1/2x, 1/2$
Feng et. al. (2008)	cylinder	$x \geq 2$	rotation ( $\theta=360^\circ/x$ )	$3x$	$1/3x, 1/3x$
Chen et. al. (2009)	cylinder	4	rotation & flipping	9	2/9
Shyu & Chen (2010)	circular cylinder	$x \geq 2$	rotation	1	$1/2^x$
Wu et. al. (2006)	rectangle	2		8	color
Shyu & Chen (2010)	square	4, 8		16	$1/9, 1/16$

計算機概論



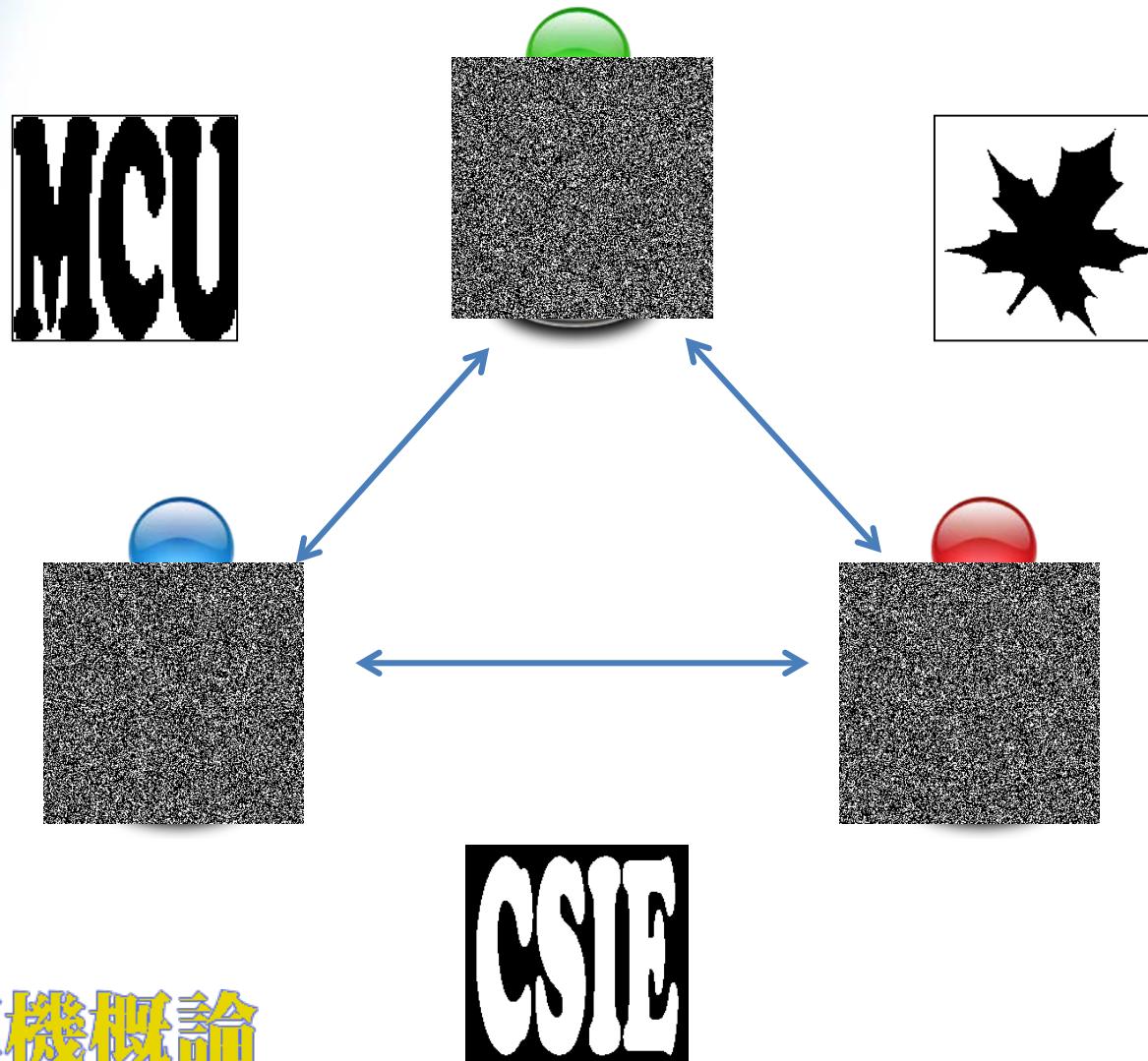
# Related Work



	Number of secrets	Operator	Pixel expansion	Contrast
	2	rotation ( $90^\circ$ )	4	$1/4$
	2	rotation ( $\theta$ )	4	$1/4, 1/2$
	$x \geq 2$	rotation ( $\theta=360^\circ/x$ )	$2x$	$1/2x, 1/2$
	$x \geq 2$	rotation ( $\theta=360^\circ/x$ )	$3x$	$1/3x, 1/3x$
Chen et. al. (2009)	cylinder	4	rotation & flipping	9
Shyu & Chen (2010)	circular & cylinder	$x \geq 2$	rotation (any $\theta$ )	$1$
Wu et. al. (2006)	rectangle	2	flipping	8
Shyu & Chen (2010)	square	2, 4, 8	flipping	4, 9, 16 ( $2x$ )
				$1/4, 1/9, 1/16$



# (2,3,3) Visual Cryptography



# (2,3,3) Visual Cryptography



$S_1$

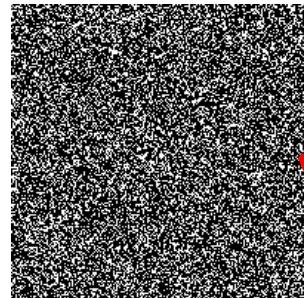


$S_2$

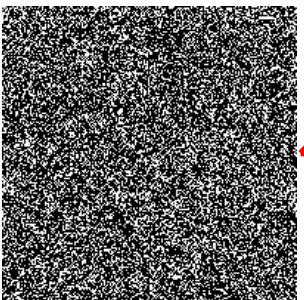


計算機概論  
 $S_3$

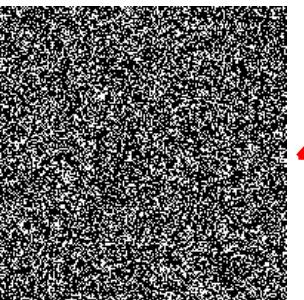
sharing



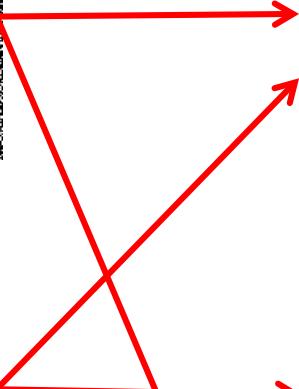
$R_1$



$R_2$



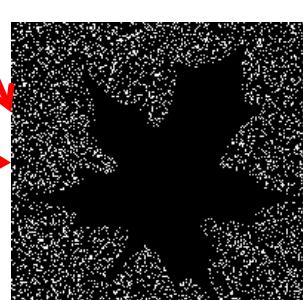
$R_3$



$R_1 \otimes R_2$



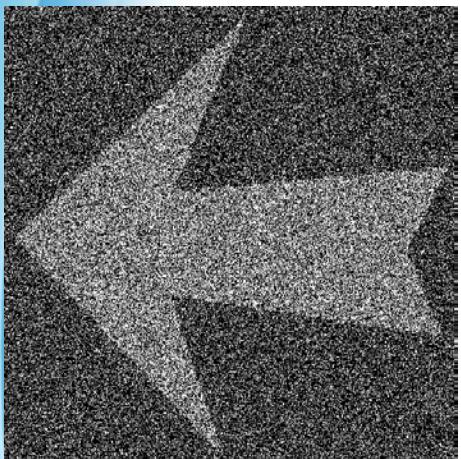
$R_2 \otimes R_3$



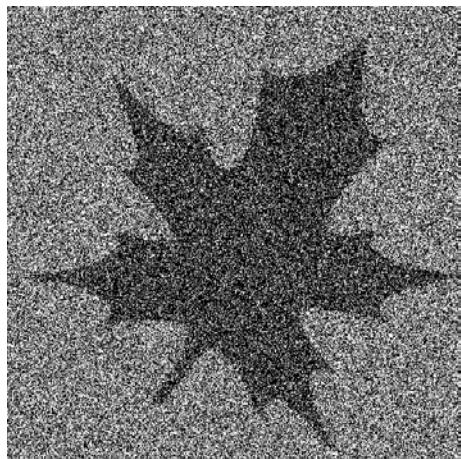
$R_3 \otimes R_1$



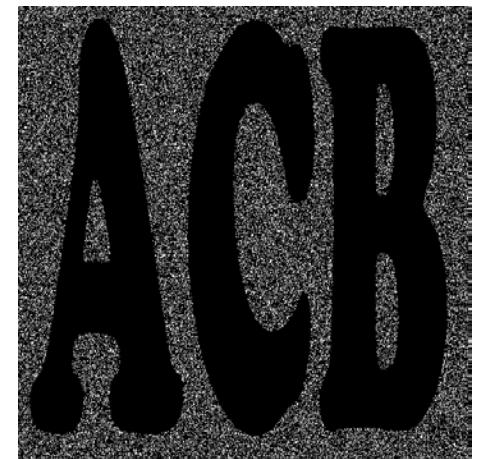
# Extended VC



**Share A**



**Share B**



**$A \otimes B$**

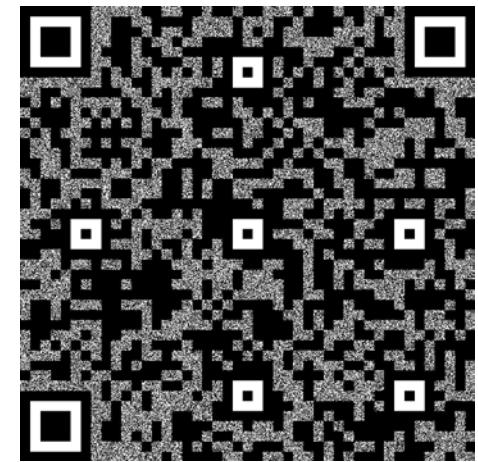
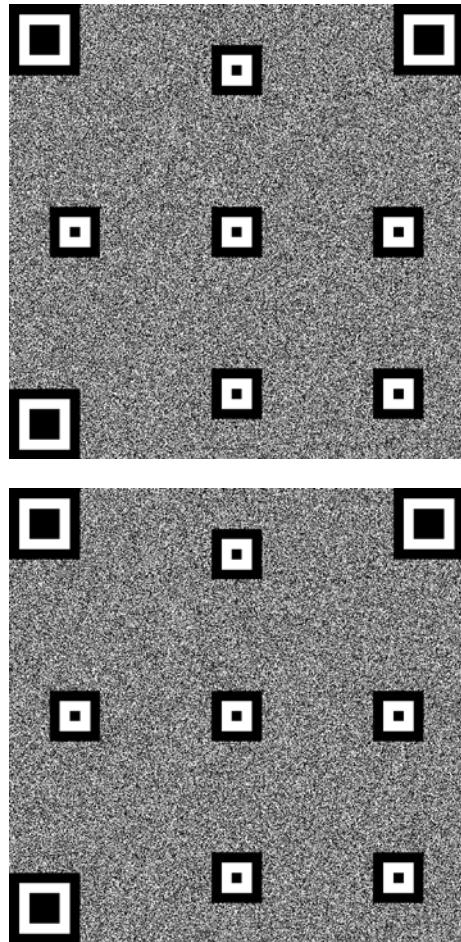


# 視覺密碼與QR-Code (1)



計算機概論

# 視覺密碼與QR-Code (2)

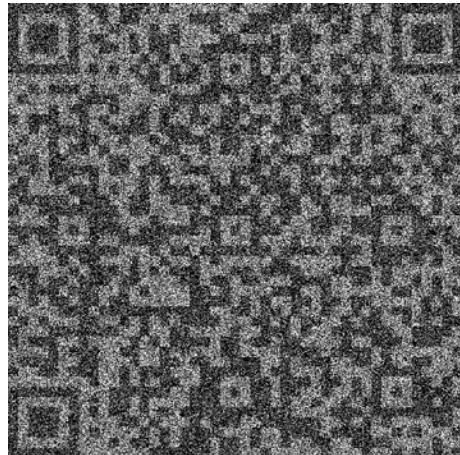


計算機概論

# 視覺密碼與QR-Code (3)



$QR_1$

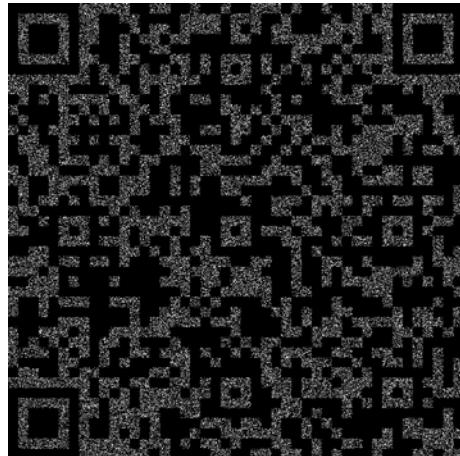


$QR_2$

計算機概論



$QR_3$



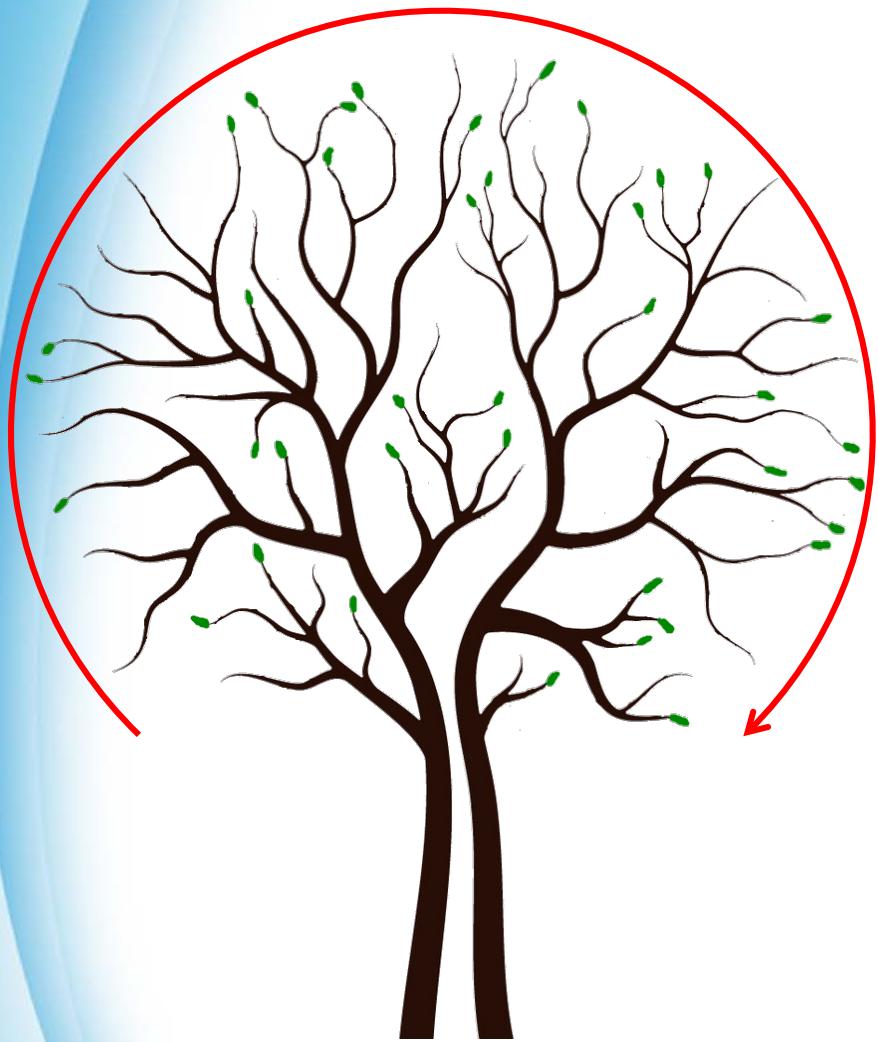
# 作業二

- 請利用視覺密碼的編碼技巧，實作出兩張投影片，當兩張投影片疊合後可看到一張機密影像。
  - 可手工繪製或利用電腦繪圖後再輸出
- 評分標準：
  - 疊合後的辨識程度
  - 單張投影片的安全性
- 額外加分：特別的疊合方式或其它創意
- 繳交方式：
  - 收件人：[kchen@csie.org](mailto:kchen@csie.org)
  - 主旨：**[bcc13spr][hw][2]** 學號 - 姓名
- **Deadline:** 2013年5月27日 23:59

計算機概論



# 愛情樹



計算機概論



金鑰：  
有葉為壹，無葉為零，  
順時旋轉，ASCII。

01101001	i
01101100	l
01101111	o
01110110	v
01100101	e
01111001	y
01101111	o
01110101	u

# Reference

- [1] M. Naor, A. Shamir, Visual Cryptography, *Advances in Cryptology: Eurocrypt'94*, LNCS 950, 1-12, 1995.
- [2] C.C. Wu and L.H. Chen, A Study on Visual Cryptography, *Master thesis*, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C, 1998.
- [3] H.-C. Wu and C.-C. Chang, Sharing visual multi-secrets using circle shares, *Computer Standards & Interfaces*, 134(28), 123-135, 2005.
- [4] A. H. C. Wu, H. C. Wang and C. S. Tsai, Multiple image sharing based on colour visual cryptography, *The Imaging Science Journal*, 54(3), 164-177, 2006.
- [5] S. J. Shyu, S.-Y. Huang, Y.-K. Lee, R.-Z. Wang, K. Chen, Sharing multiple secrets in visual cryptography, *Pattern Recognition*, 40, 3633-3651, 2007
- [6] B. J. B. Feng, H. C. Wu, C. S. Tsai, Y. F. Chang and Y. P. Chu, Visual secret sharing for multiple secrets, *Pattern Recognition*, 41, 3572-3581, 2008.
- [7] J.Chen, T.S. Chen, H. C. Hsu, Y. H. Lin, Using multi-ringed shadow image of visual cryptography to hide more secret messages, *The Image Science Journal*, 57, 101-108, 2009
- [8] S. J. Shyu, K. Chen, Visual multiple secrets sharing by circle random grids, to appear in *SIAM Journal on Imaging Sciences*, 2010.

