

資訊隱藏技術與其應用
Data Hiding Technique and Its
Application

周永振

亞洲大學 資訊工程學系

Web: <http://120.108.116.237/~jackjow>

E-mail: yungchen@gmail.com

Introduction

- ✓ 小明暗戀隔壁班的女同學阿花，一天小明終於鼓起勇氣寫信給阿花
- ✓ 請選擇以下其中一樣在其中打勾：

愛情； 友情

- ✓ 阿花回送給他一首詩：

願君多諒知識淺，選題未答繳白卷
愛莫能助實有愧，情願送詩供君覽

Introduction (Cont.)

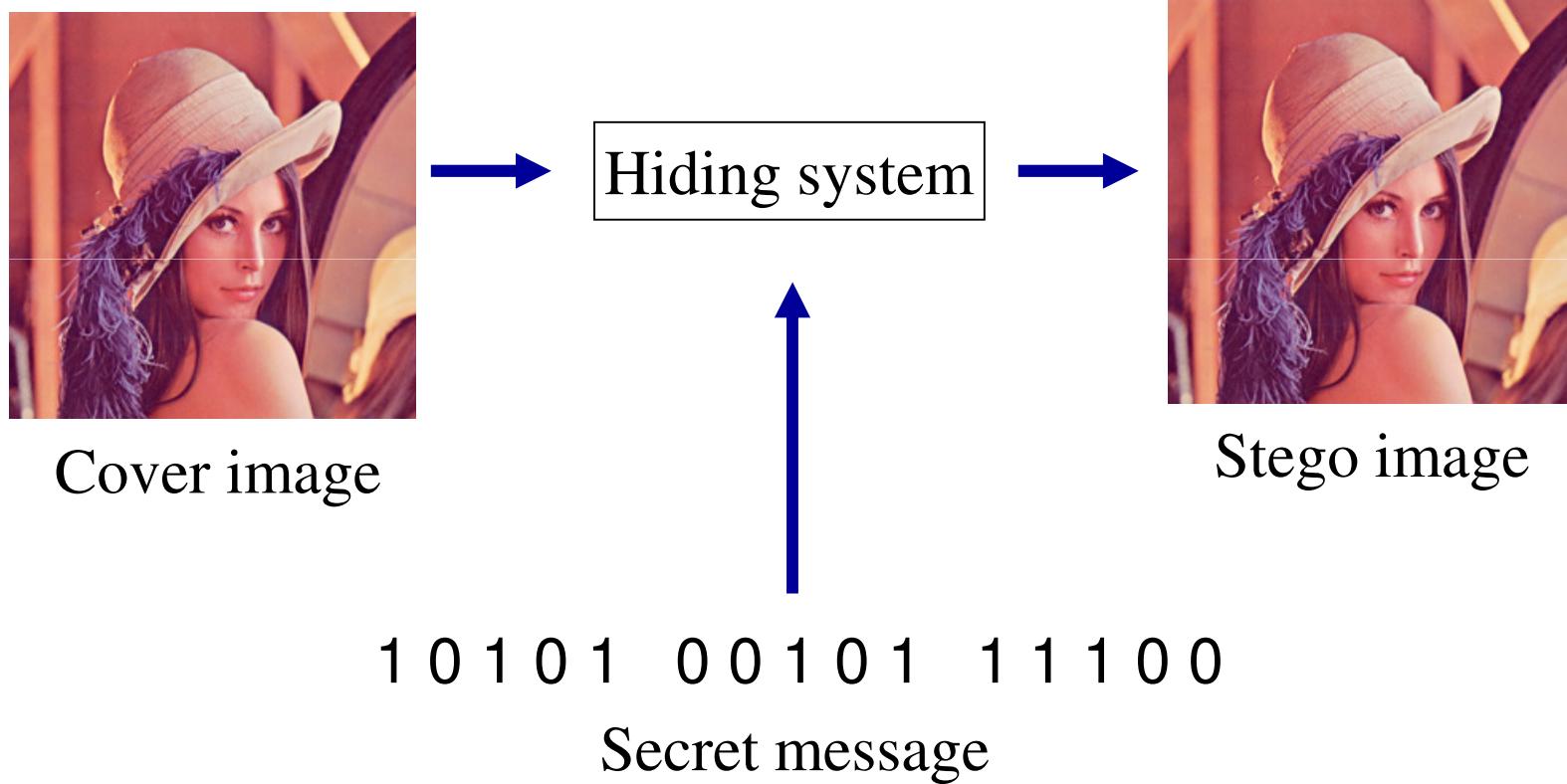
345	相思苦
1573	一往情深
5646	無聊死了
53406	我想死你了
53770	我想親親你
075、9125、184	你親我就要愛我一輩子
0800-956-956	恁別贏贏-救摸聊-救摸聊

Introduction (Cont.)

- Cryptography
 - RSA (Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman, 1977)
 - DES (**D**ata **E**ntryption **S**tandard, 1976)
 - AES (**A**dvance **E**ntryption **S**tandard, 2001/11/26)
- Steganography
 - Secret data delivery
 - Visual quality vs. embedding capacity
 - Categories:
 - Compression domain
 - Spatial domain
 - Frequency domain
 - Grayscale image/color image
- Digital Watermarking

Introduction (Cont.)

- Information hiding (Data hiding)



VQ domain data hiding

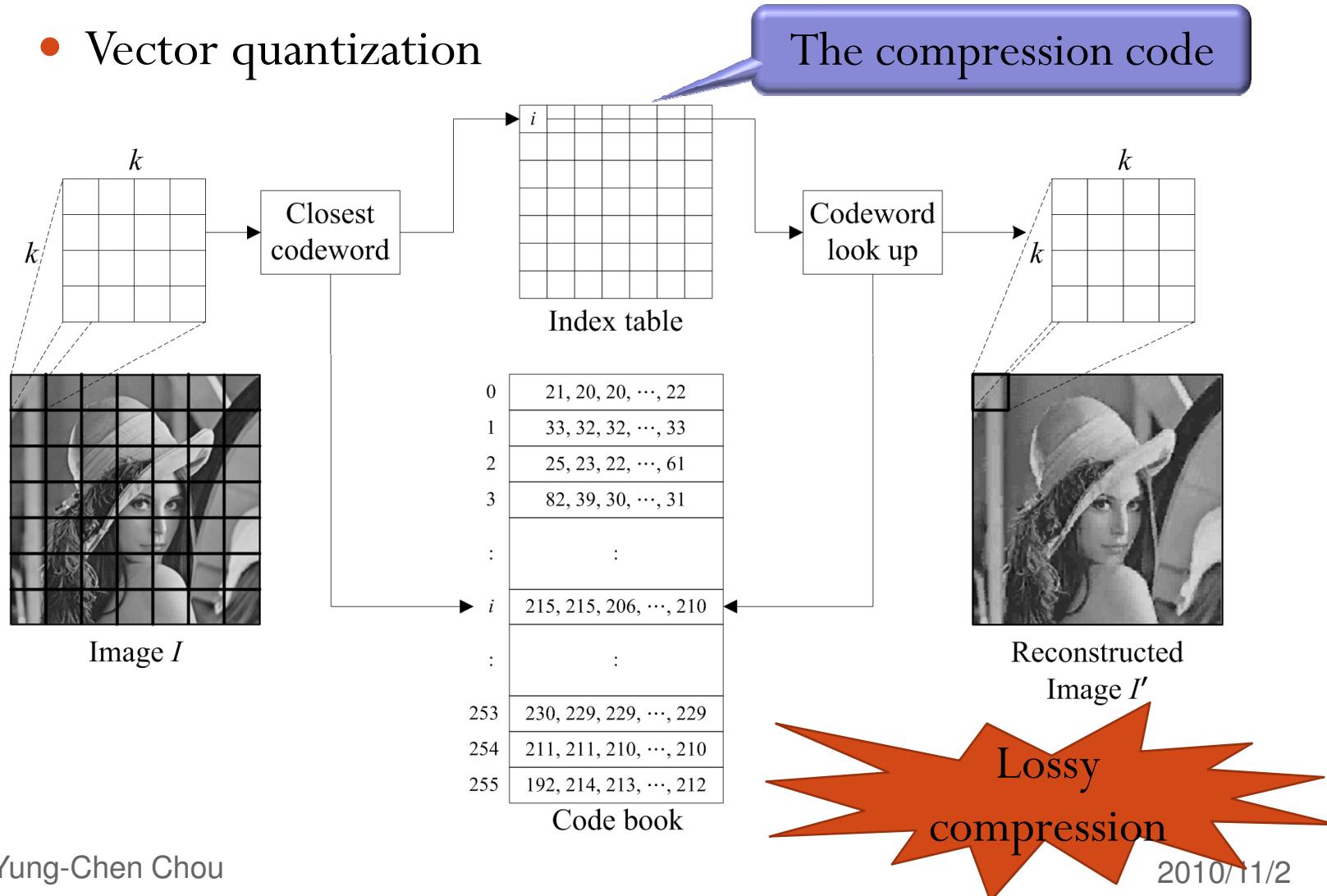


資料來源：<http://www.peopo.org/kcl137/post/27265>

Yung-Chen Chou

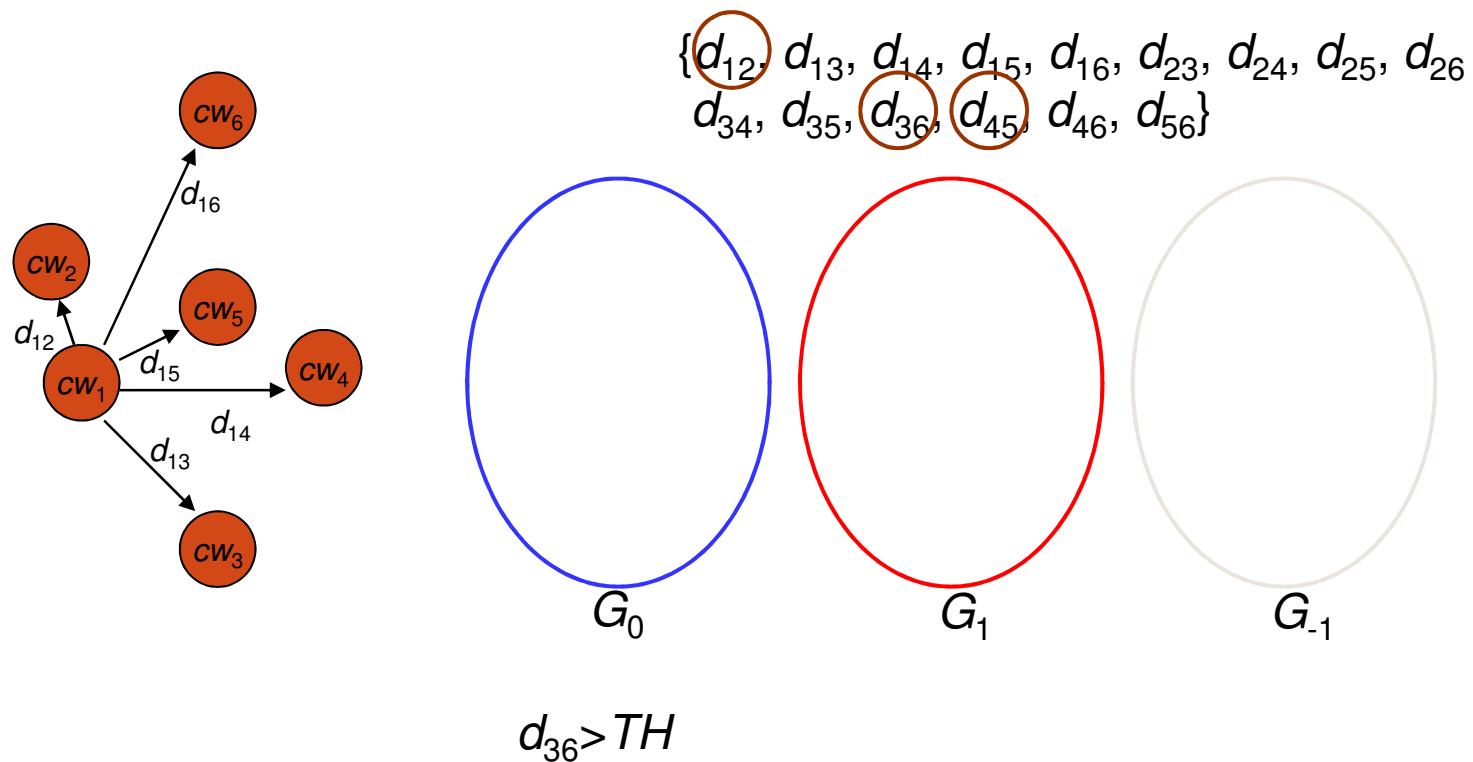
VQ domain data hiding (Cont.)

- Vector quantization



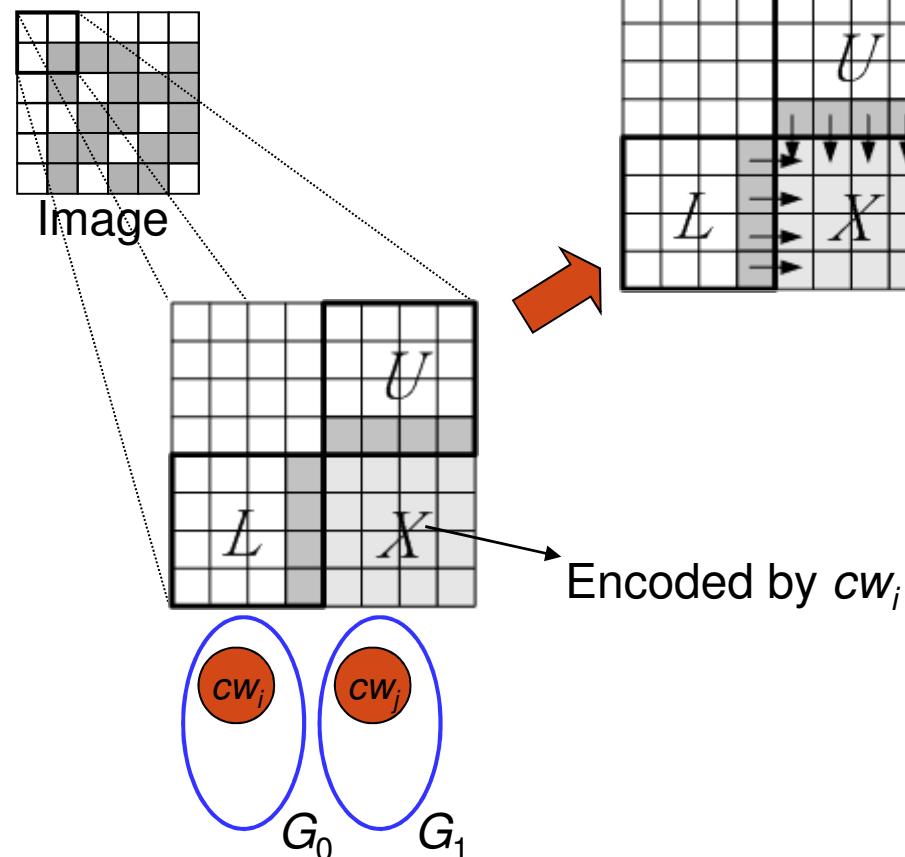
VQ domain data hiding (Cont.)

- Codeword pairing



VQ domain data hiding (Cont.)

- Data hiding



$$SMD(cw_x, NBV_{B_i}) = \sqrt{\sum_{j=0,1,2,3,4,8,12} (cw_x(j) - NBV_{B_i}(j))^2}$$

$$NBV_X = \{x_0, x_1, x_3, x_4, X, X, X, x_8, X, X, X, x_{12}, X, X, X\}$$

Indicator = '0'

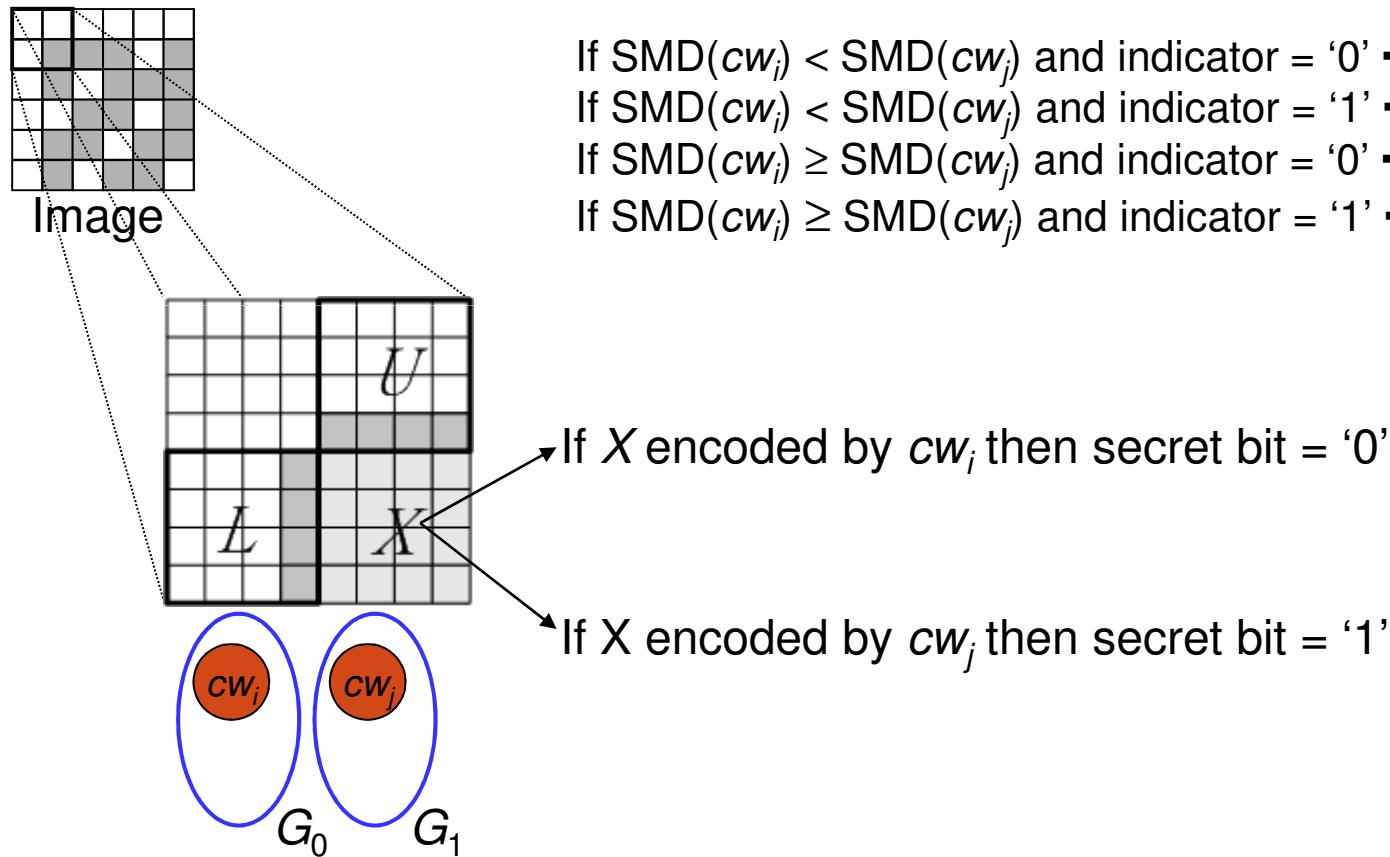
If $SMD(cw_i, NBV_X) < SMD(cw_j, NBV_X)$ then X is replaceable
Else X is non-replaceable

Indicator = '1'

If secret bit = '0' then encode X by cw_i
else encode X by cw_j

VQ domain data hiding (Cont.)

- Data extracting and restoring



VQ domain data hiding (Cont.)

- Experimental results

Images	Size of Codebook	Stego image quality (PSNR)	Payload (bits)	Restoration information (bits)	Available embedding capacity (bits)
Baboon	256	24.16	8512	1562	6950
	512	24.43	9824	1766	8058
	1024	24.80	9782	1740	8042
Jet(F16)	256	30.12	11154	1786	9368
	512	30.98	13665	2228	11437
	1024	31.62	13702	2308	11394
Lena	256	30.54	12947	2174	10773
	512	31.31	13922	2310	11612
	1024	32.32	14014	2343	11671
Pepper	256	30.00	12285	2023	10262
	512	30.65	13507	2236	11271
	1024	31.22	14504	2403	12101
Sailboat	256	26.47	10773	1789	8984
	512	26.95	12323	2080	10243
	1024	27.58	11314	1955	9359
Toys	256	29.28	8115	1292	6823
	512	30.41	8795	1412	7383
	1024	31.66	13546	2099	11447

VQ domain data hiding (Cont.)

- Experimental results

The comparison using Lena as the cover image				
Methods	Stego image quality (PSNR)	Recovered image quality (PSNR)	Embedding time (sec)	Available embedding capacity (bits)
Jo and Kim's				
($TH = 40$)	30.74	30.74	0.17	14,510
Chang and Lin's	30.23	32.24	22.59	8,098
Proposed				
($TH = 40$)	31.31	32.24	0.23	11,646

The comparison using Baboon as the cover image				
Methods	Stego image quality (PSNR)	Recovered image quality (PSNR)	Embedding time (sec)	Available embedding capacity (bits)
Jo and Kim's				
($TH = 40$)	24.32	24.32	0.21	10,946
Chang and Lin's	24.04	24.70	22.94	2,814
Proposed				
($TH = 40$)	24.43	24.70	0.25	8,096

Data hiding using Sudoku (Cont.)

- Spatial domain data embedding
- Sudoku
 - A logic-based number placement puzzle

5	3			7					
6				1	9	5			
	9	8					6		
8				6					3
4			8		3				1
7				2				6	
	6				2	8			
			4	1	9				5
			8			7	9		



5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

Data hiding using Sudoku (Cont.)

- Property

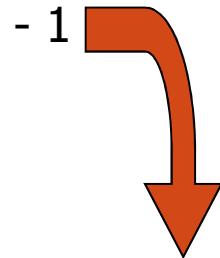
5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

- A Sudoku grid contains nine 3×3 matrices, each contains different digits from 1 to 9.
- Each row and each column of a Sudoku grid also contain different digits from 1 to 9.

Possible solutions:
6,670,903,752,021,072,936,960
(i.e. $\approx 6.671 \times 10^{21}$)

Data hiding using Sudoku (Cont.)

6	5	1	7	4	8	2	3	9
9	3	8	2	5	6	1	7	4
2	4	7	3	1	9	8	6	5
3	2	4	1	9	7	6	5	8
5	7	6	4	8	3	9	2	1
8	1	9	5	6	2	3	4	7
4	6	2	8	7	1	5	9	3
7	8	3	9	2	5	4	1	6
1	9	5	6	3	4	7	8	2



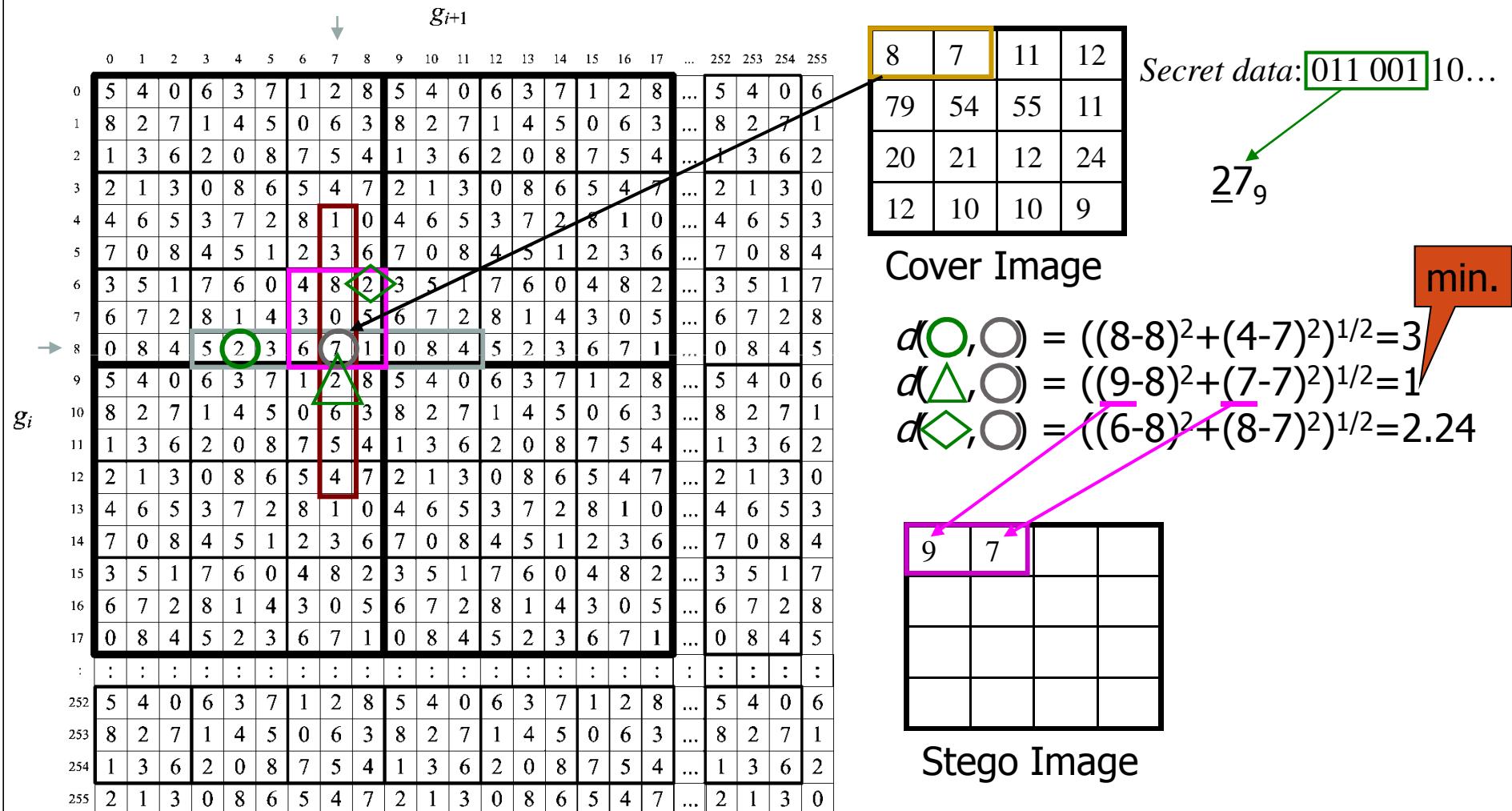
5	4	0	6	3	7	1	2	8
8	2	7	1	4	5	0	6	3
1	3	6	2	0	8	7	5	4
2	1	3	0	8	6	5	4	7
4	6	5	3	7	2	8	1	0
7	0	8	4	5	1	2	3	6
3	5	1	7	6	0	4	8	2
6	7	2	8	1	4	3	0	5
0	8	4	5	2	3	6	7	1



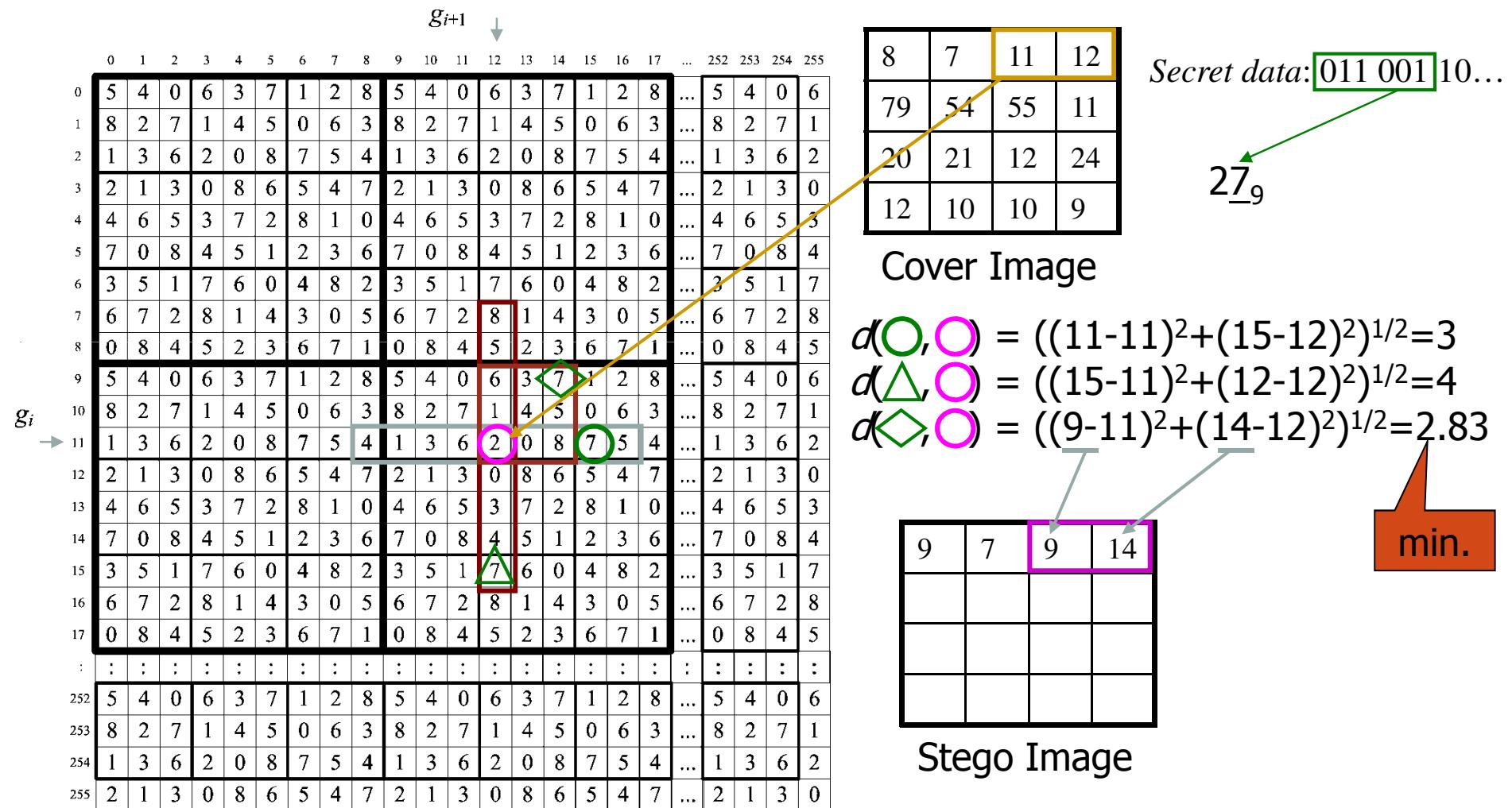
g_i

	g_{i+1}																		...	252	253	254	255
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	...	5	4	0	6
0	5	4	0	6	3	7	1	2	8	5	4	0	6	3	7	1	2	8	...	5	4	0	6
1	8	2	7	1	4	5	0	6	3	8	2	7	1	4	5	0	6	3	...	8	2	7	1
2	1	3	6	2	0	8	7	5	4	1	3	6	2	0	8	7	5	4	...	1	3	6	2
3	2	1	3	0	8	6	5	4	7	2	1	3	0	8	6	5	4	7	...	2	1	3	0
4	4	6	5	3	7	2	8	1	0	4	6	5	3	7	2	8	1	0	...	4	6	5	3
5	7	0	8	4	5	1	2	3	6	7	0	8	4	5	1	2	3	6	...	7	0	8	4
6	3	5	1	7	6	0	4	8	2	3	5	1	7	6	0	4	8	2	...	3	5	1	7
7	6	7	2	8	1	4	3	0	5	6	7	2	8	1	4	3	0	5	...	6	7	2	8
8	0	8	4	5	2	3	6	7	1	0	8	4	5	2	3	6	7	1	...	0	8	4	5
9	5	4	0	6	3	7	1	2	8	5	4	0	6	3	7	1	2	8	...	5	4	0	6
10	8	2	7	1	4	5	0	6	3	8	2	7	1	4	5	0	6	3	...	8	2	7	1
11	1	3	6	2	0	8	7	5	4	1	3	6	2	0	8	7	5	4	...	1	3	6	2
12	2	1	3	0	8	6	5	4	7	2	1	3	0	8	6	5	4	7	...	2	1	3	0
13	4	6	5	3	7	2	8	1	0	4	6	5	3	7	2	8	1	0	...	4	6	5	3
14	7	0	8	4	5	1	2	3	6	7	0	8	4	5	1	2	3	6	...	7	0	8	4
15	3	5	1	7	6	0	4	8	2	3	5	1	7	6	0	4	8	2	...	3	5	1	7
16	6	7	2	8	1	4	3	0	5	6	7	2	8	1	4	3	0	5	...	6	7	2	8
17	0	8	4	5	2	3	6	7	1	0	8	4	5	2	3	6	7	1	...	0	8	4	5
:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	
252	5	4	0	6	3	7	1	2	8	5	4	0	6	3	7	1	2	8	...	5	4	0	6
253	8	2	7	1	4	5	0	6	3	8	2	7	1	4	5	0	6	3	...	8	2	7	1
254	1	3	6	2	0	8	7	5	4	1	3	6	2	0	8	7	5	4	...	1	3	6	2
255	2	1	3	0	8	6	5	4	7	2	1	3	0	8	6	5	4	7	...	2	1	3	0

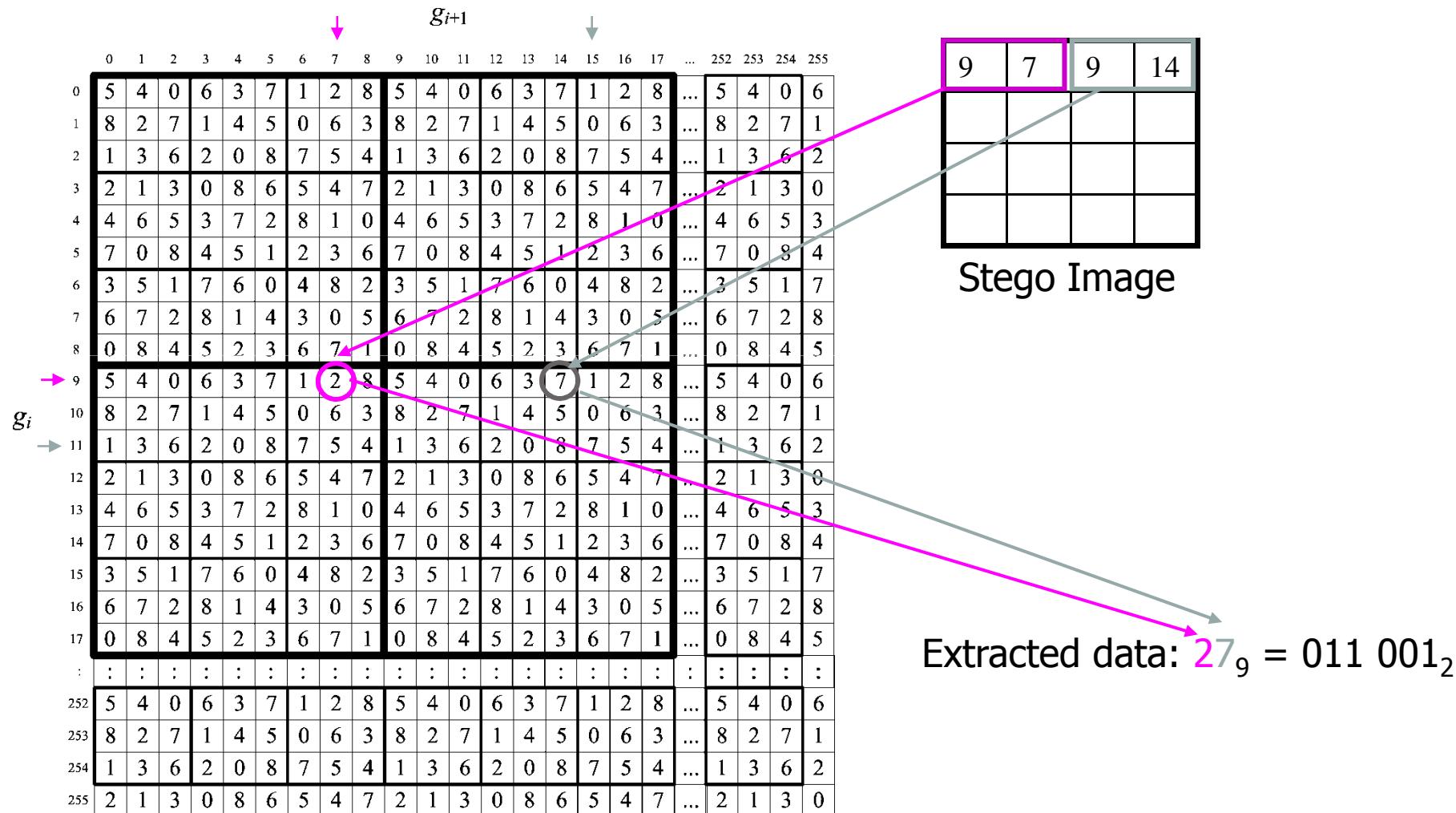
Data hiding using Sudoku (Embedding) (Cont.)



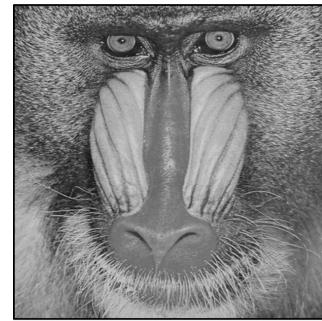
Data hiding using Sudoku (Embedding) (Cont.)



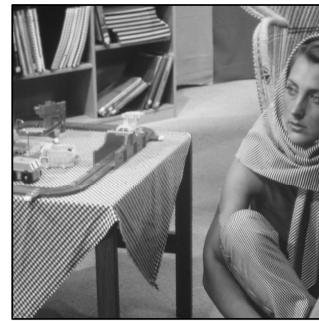
Data hiding using Sudoku (Extracting) (Cont.)



Experimental results



(a) Baboon ($PSNR = 44.68$ dB)



(b) Barbara ($PSNR = 44.77$ dB)



(c) Boat ($PSNR = 44.94$ dB)



(d) Goldhill ($PSNR = 44.84$ dB)



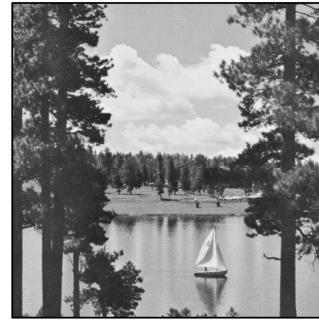
(e) Jet(F16) ($PSNR = 45.02$ dB)



(f) Lena ($PSNR = 44.97$ dB)



(g) Pepper ($PSNR = 44.67$ dB)



(h) Sailboat ($PSNR = 44.67$ dB)



(i) Tiffany ($PSNR = 45.02$ dB)

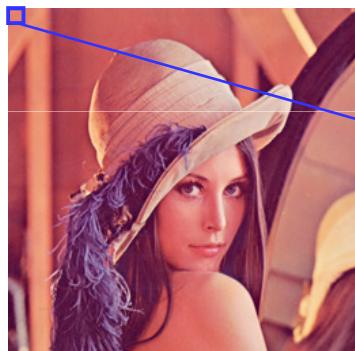
Experimental results (Cont.)

TABLE I
THE RESULTS OF VISUAL QUALITY AND EMBEDDING CAPACITY
COMPARISONS

Images	Zhang and Wang		Mielikainen		Proposed	
	<i>PSNR</i>	<i>C</i>	<i>PSNR</i>	<i>C</i>	<i>PSNR</i>	<i>C</i>
Baboon	52.11	1	52.76	1	44.68	1.5
Barbara	52.11	1	52.77	1	44.77	1.5
Boats	52.11	1	52.78	1	44.94	1.5
Goldhill	52.11	1	52.77	1	44.84	1.5
Jet(F16)	52.11	1	52.77	1	45.02	1.5
Lena	52.12	1	52.77	1	44.97	1.5
Pepper	52.12	1	52.77	1	44.67	1.5
Sailboat	52.11	1	52.75	1	44.67	1.5
Tiffany	52.11	1	52.77	1	45.02	1.5
Average	52.11	1	52.77	1	44.88	1.5

Data hiding for color images

- True color and color palette image
- Color pixel (Red, Green, Blue)
- Reversibility
- Review Fridrich's method



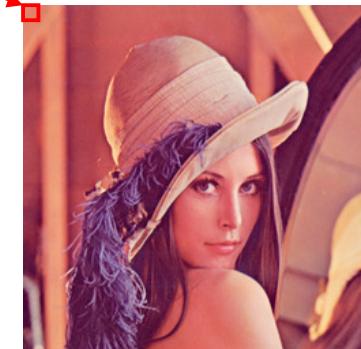
Image

0	(15, 16, 13)
1	(35, 26, 42)
:	:
127	(115, 216, 112)
128	(105, 146, 193)
:	:
254	(223, 216, 232)
255	(250, 252, 248)

Sorted color palette

$$R+G+B \bmod 2 = (115 + 216 + 112) \bmod 2 = 1$$
$$R+G+B \bmod 2 = (105 + 146 + 193) \bmod 2 = 0$$

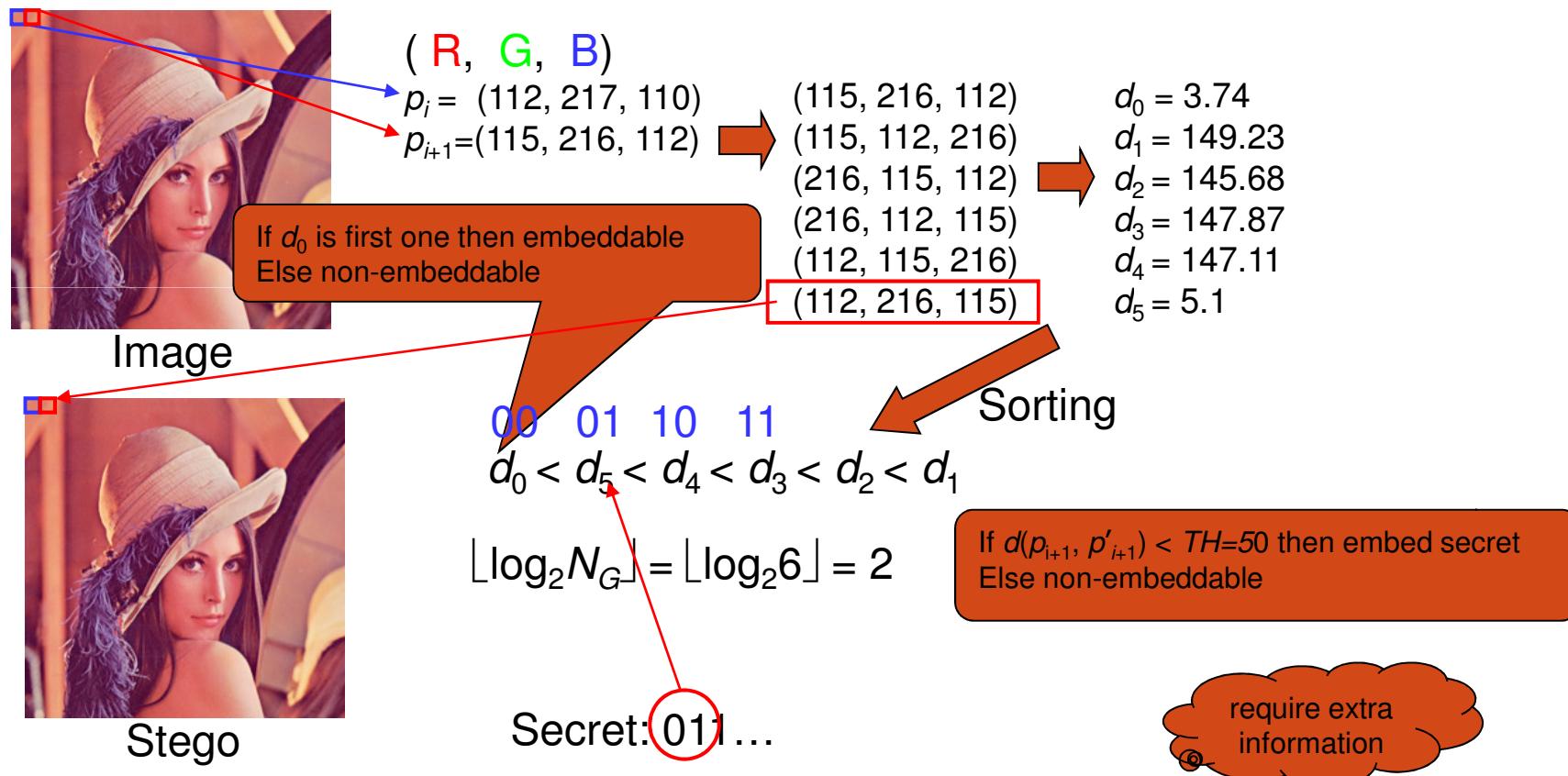
Secret: 010...



Stego 2010/11/2

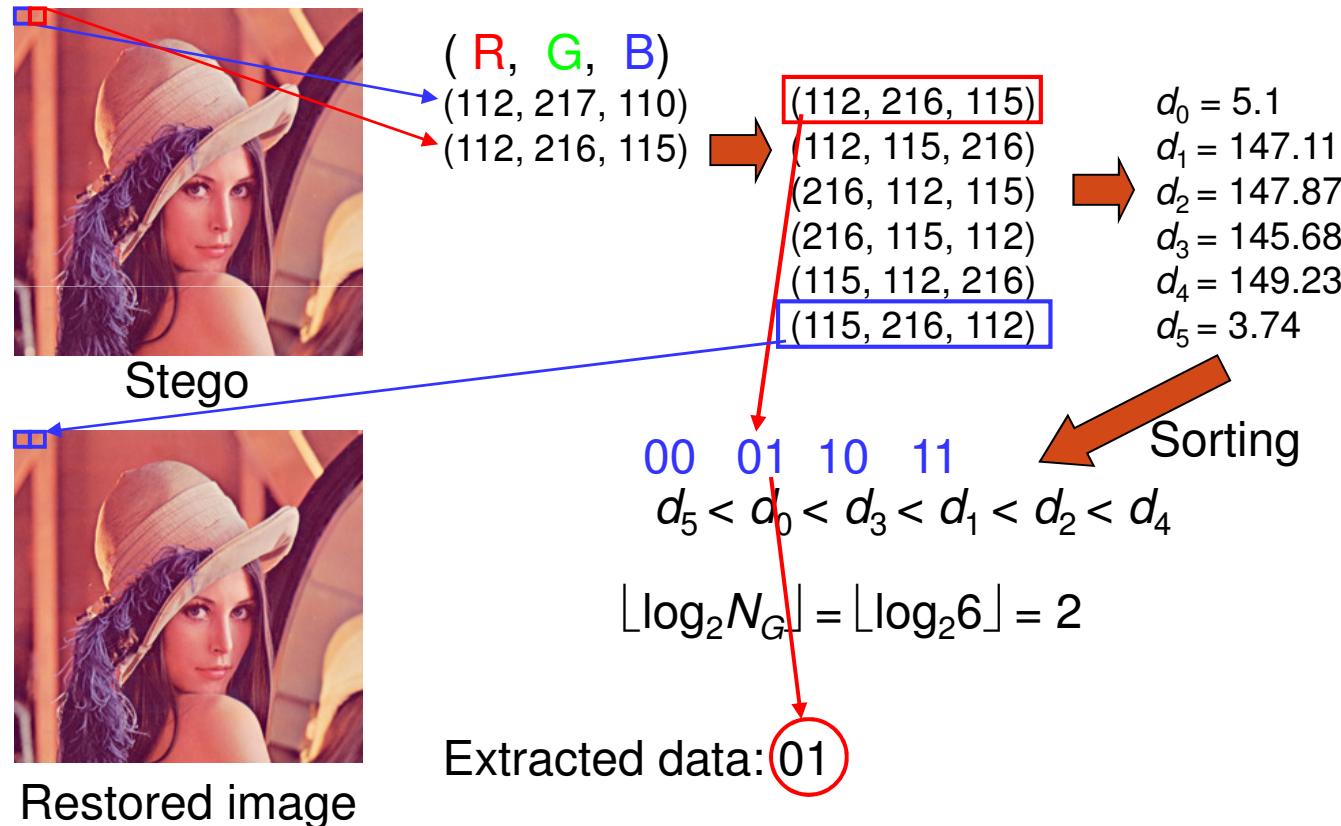
Data hiding for color images (Cont.)

- Proposed method (Embedding)



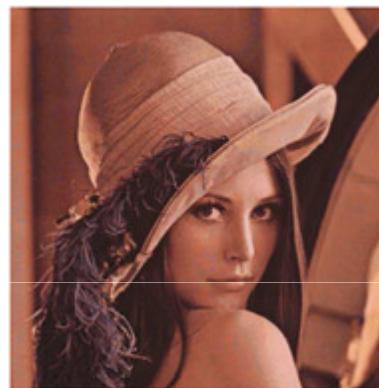
Data hiding for color images (Cont.)

- Proposed method (Extracting and restoring)



Data hiding for color images (Cont.)

- Experimental results



(a) EZ-stego



(b) Fridrich's method



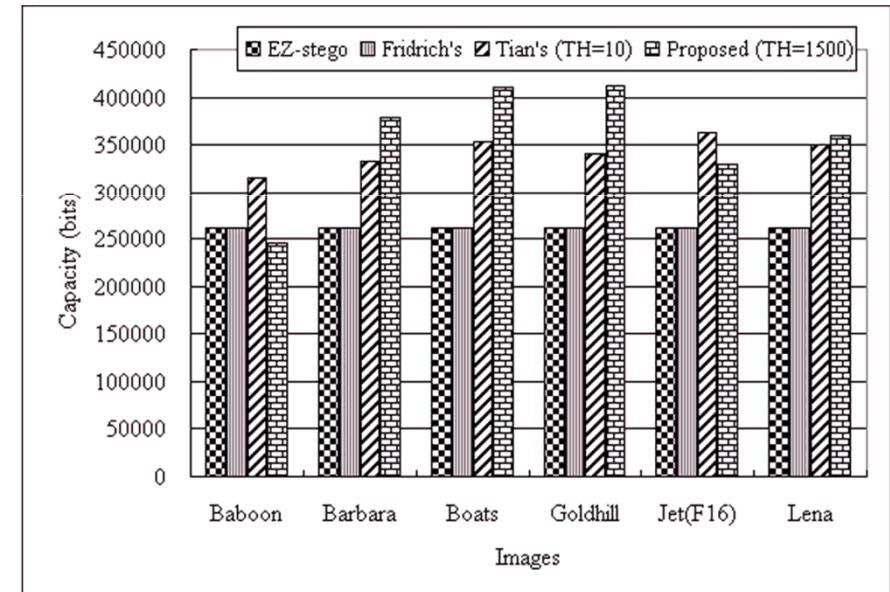
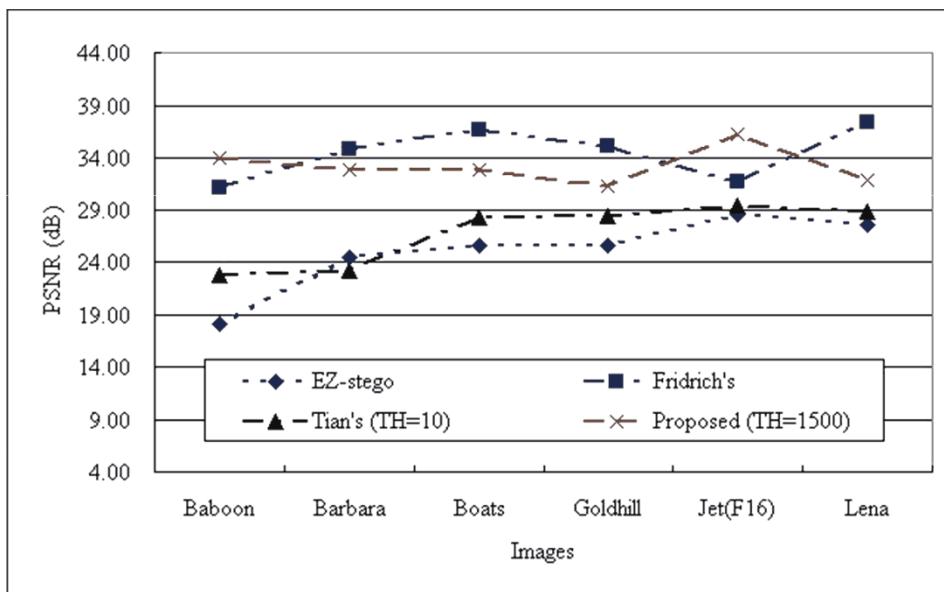
(c) Tian's method ($TH=10$)



(d) Proposed method ($TH=1500$)

Data hiding for color images (Cont.)

- Experimental results



High payload data hiding for color images

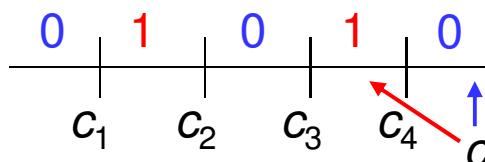
- Review Tzeng's method

(10, 20, 15)	(6, 8, 15)	(10, 10, 12)	...
(12, 18, 9)	(16, 18, 25)
:	:		

Image

$$\begin{aligned}v &= 0.3 \times r + 0.59 \times g + 0.11 \times b \\v_1 &= 0.3 \times 10 + 0.59 \times 20 + 0.11 \times 15 = 16.45 \\v_2 &= 8.17 \\v_3 &= 10.22 \\v_4 &= 15.21 \\v_c &= 18.17\end{aligned}$$

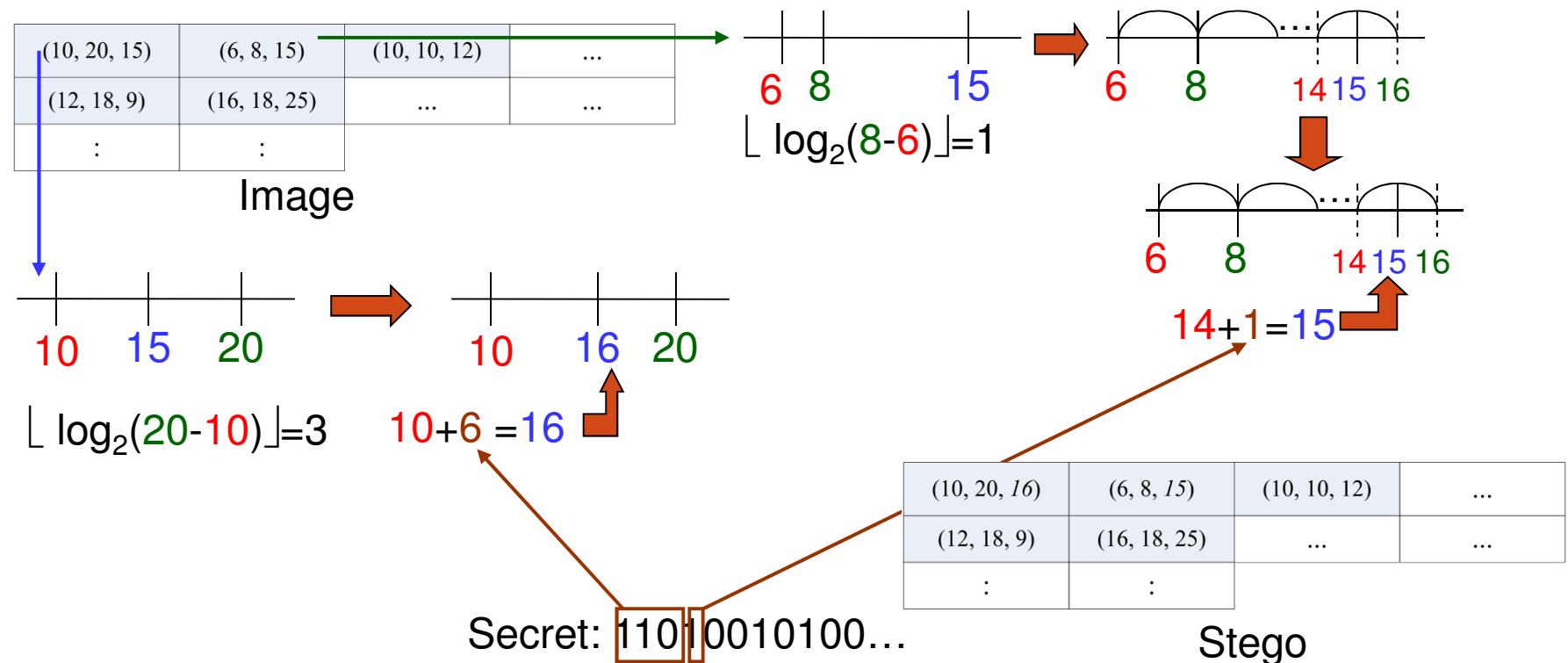
$$\left\{ \begin{array}{l} c_1 > c_2, \text{ if } (v_1 > v_2) \text{ or} \\ \quad (v_1 = v_2 \text{ and } r_1 > r_2) \text{ or} \\ \quad (v_1 = v_2 \text{ and } r_1 = r_2 \text{ and } g_1 > g_2) \\ c_1 = c_2, \text{ if } (r_1 = r_2 \text{ and } g_1 = g_2 \text{ and } b_1 = b_2) \\ c_1 < c_2, \text{ otherwise} \end{array} \right.$$



Secret: 101...

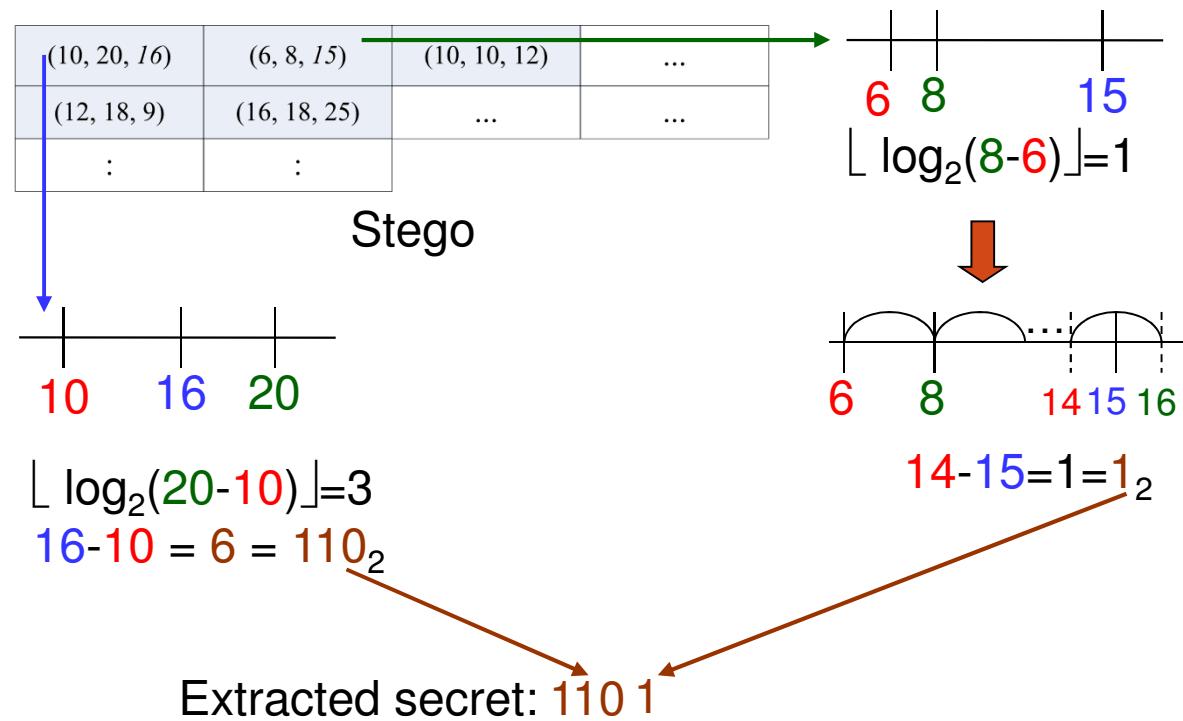
High payload data hiding for color images (Cont.)

- The proposed (Embedding)



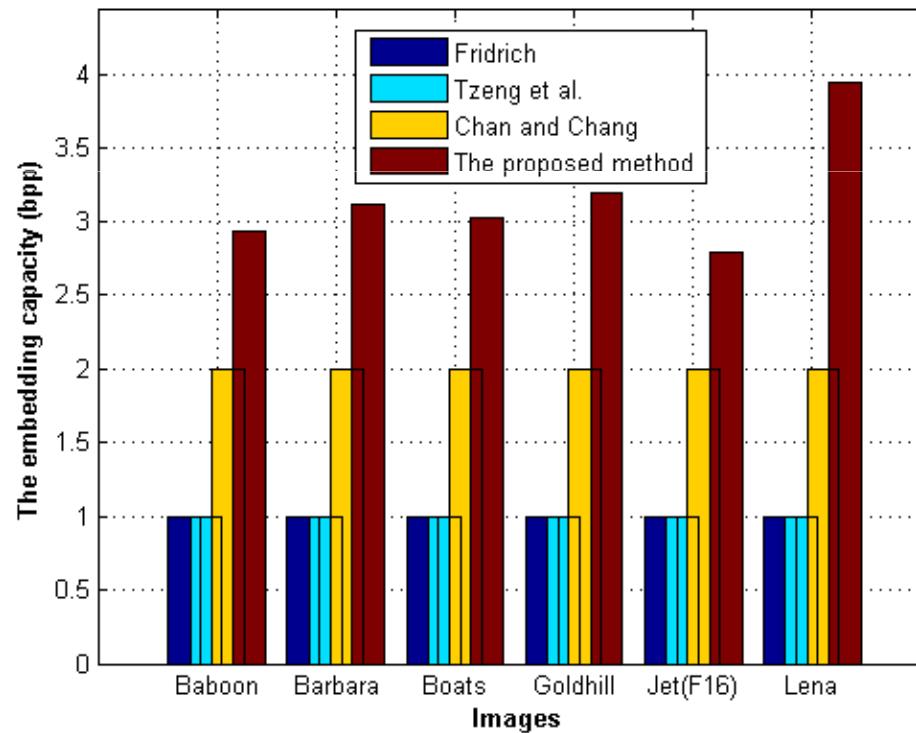
High payload data hiding for color images (Cont.)

- The proposed (Extracting)



High payload data hiding for color images (Cont.)

- Experimental results



High payload data hiding for color images (Cont.)



(a) Original Lena image



(b) The proposed Method
(TH = 100), PSNR =
76.486 dB, C = 3.949 bpp



(c) Fridrich's method
PSNR= 31.826 dB, C = 1
bpp



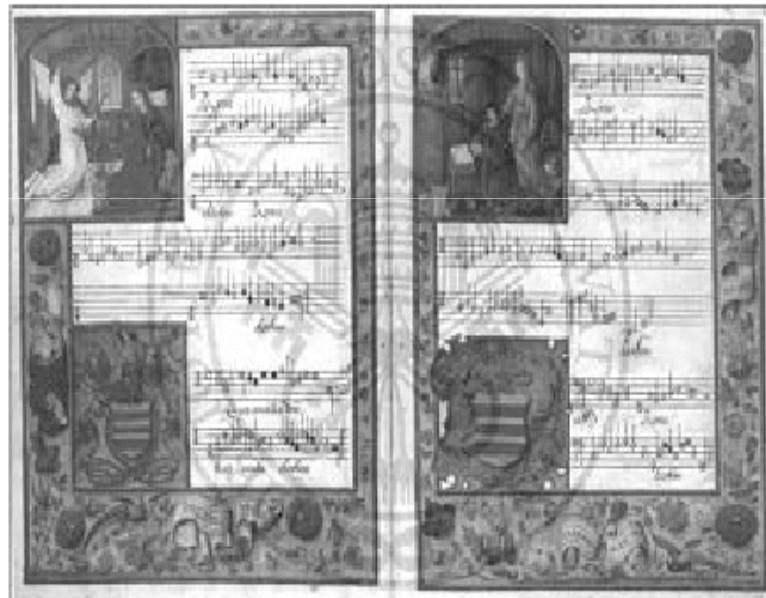
(d) Tzeng et al.'s method, PSNR= 33.283
dB, C = 0.996 bpp



(e) Chan and Chang's method, PSNR=
28.346 dB, C = 1.992 bpp

Digital Image Copyright Protection

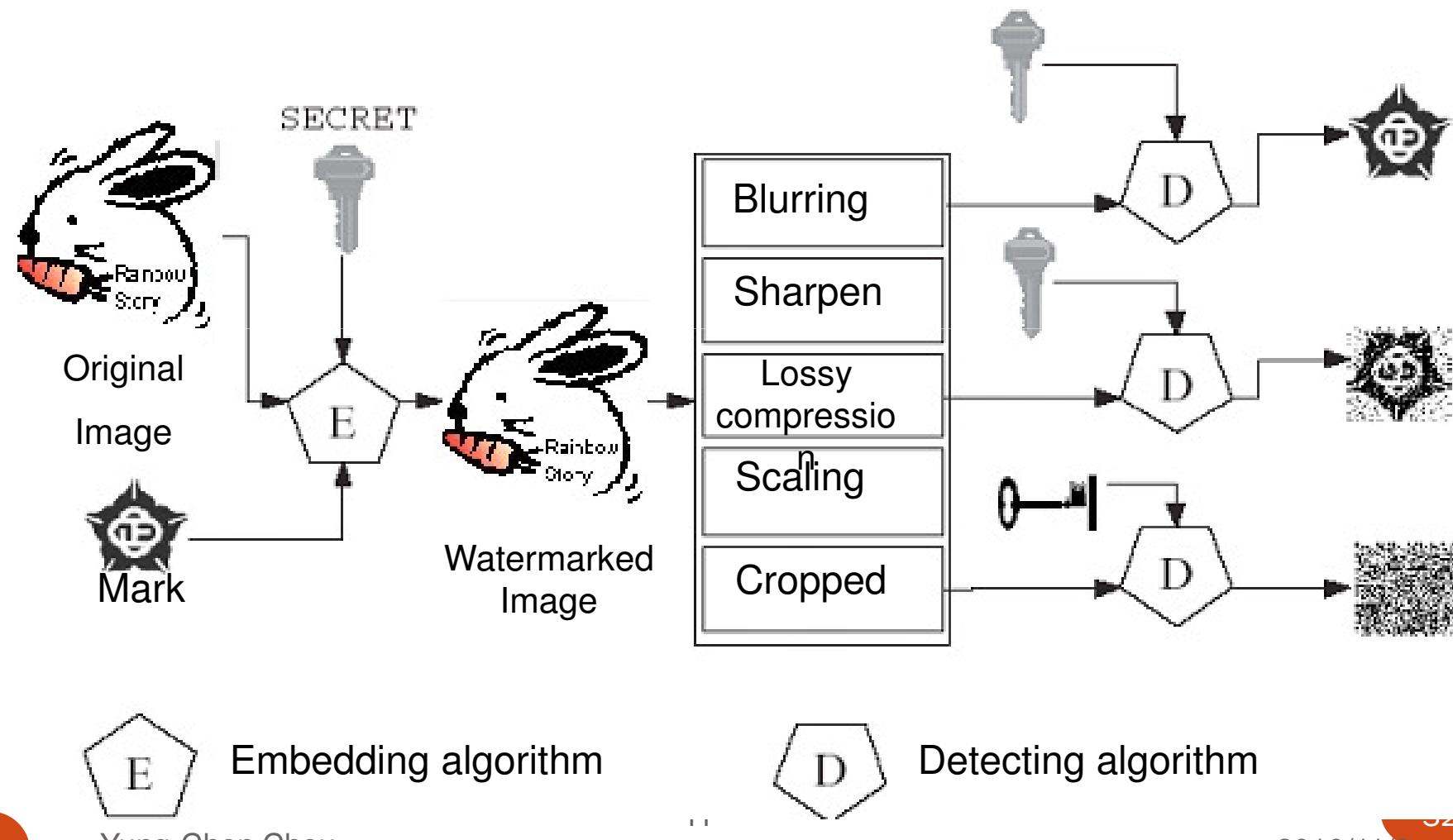
Visible



Invisible



Digital Image Copyright Protection (Cont.)

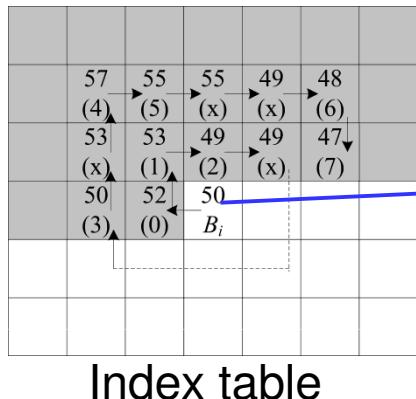


Digital Image Copyright Protection (Cont.)

- Watermarking characteristics:
 - Invisibility
 - Security
 - Blindness
 - Multiple Watermarks
 - Robustness

SOC improvement

- Scan-order coding (SOC)



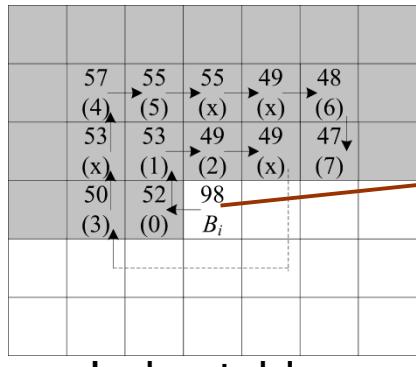
Index table

0	52
1	53
2	49
3	50
4	57
5	55
6	48
7	47

State codebook

Compression code: ...1 011...

Indicator



Index table

0	52
1	53
2	49
3	50
4	57
5	55
6	48
7	47

State codebook

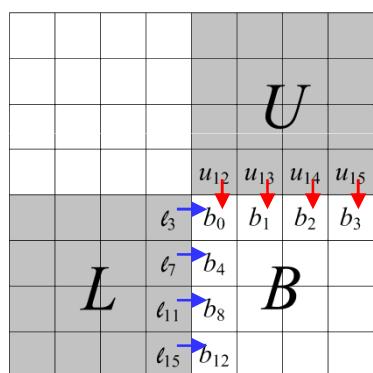
Compression code: ...0 01100010...

Indicator

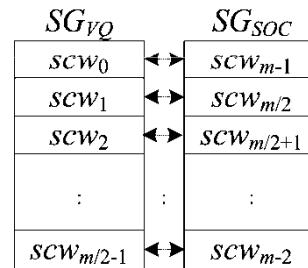
SOC improvement (Cont.)

- Review Lin and Chang's method

$$SMD(cw_x, NBV_{B_i}) = \sqrt{\sum_{j=0,1,2,3,4,8,12} (cw_x(j) - NBV_{B_i}(j))^2}$$



$$NBV_B = \{b_0, b_1, b_3, b_4, X, X, X, b_8, X, X, X, b_{12}, X, X, X\}$$



If $SMD(\alpha, NBV_B) < SMD(\bar{\alpha}, NBV_B)$

- Secret = 0 → α
- Secret = 1 → $\bar{\alpha}$
- Secret = 0 → 000 || α
- Secret = 1 → 111 || α

If $SMD(\alpha, NBV_B) \geq SMD(\bar{\alpha}, NBV_B)$

SOC improvement (Cont.)

- The proposed method (Encoding)

	57	55	55	49	48		
	(5)	(6)					
	53	53	49	49	47		
	(x)	(2)	(3)	(x)			
	50	52(1)	50	49			
	(4)	B_{i-1}	B_i				

Index table

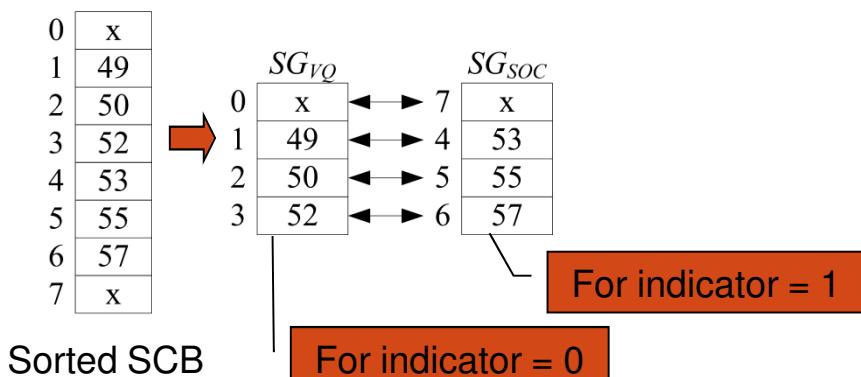
	57	55	55	49	48		
	(6)						
	53	53	49	49	47		
	(5)	(2)	(x)	(3)			
	50	52	50(1)	49			
	(4)	B_i	B_{i+1}				

Index table

0	x
1	47
2	49
3	50
4	52
5	53
6	55
7	x

Sorted SCB

Can be compressed by
SOC (i.e. indicator = 1)



If $SMD(cw_{50}, NBV_{B_i}) < SMD(cw_{55}, NBV_{B_i})$
Compression code: ...101
Else Compression code: ... 111 010

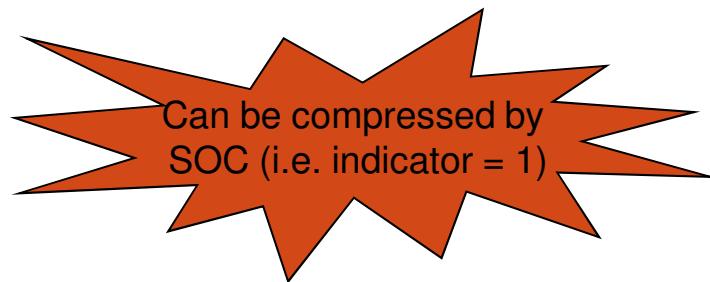
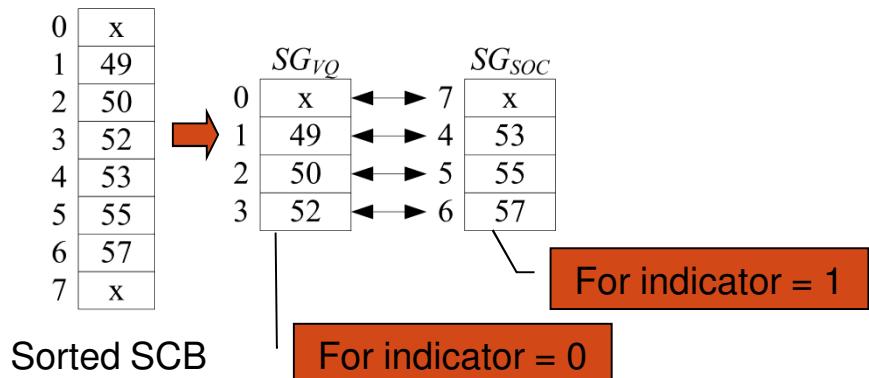
SOC improvement (Cont.)

		57	55	55	49	48		
		(5)	(6)					
		53	53	49	50	47		
		(x)	(2)	(3)	(4)			
		50	52(1)	130	50			
		(x)	B_{i-1}	B_i				

Index table

		57	55	55	49	48		
		53	53	49	50	47		
		(6)	(2)	(3)	(4)			
		50	52	130(1)	50			
		(5)	B_i	B_{i+1}				

Index table



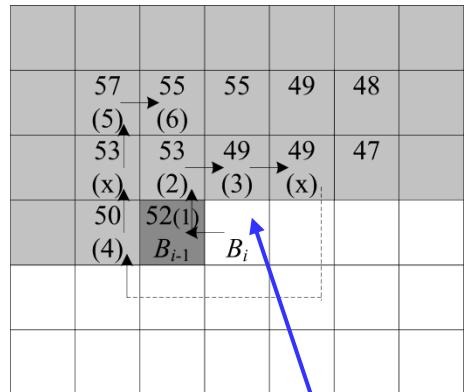
MG_{VQ}	MG_{SOC}
0	255
1	128
2	129
3	130
:	:
127	254

For indicator = 1
For indicator = 0

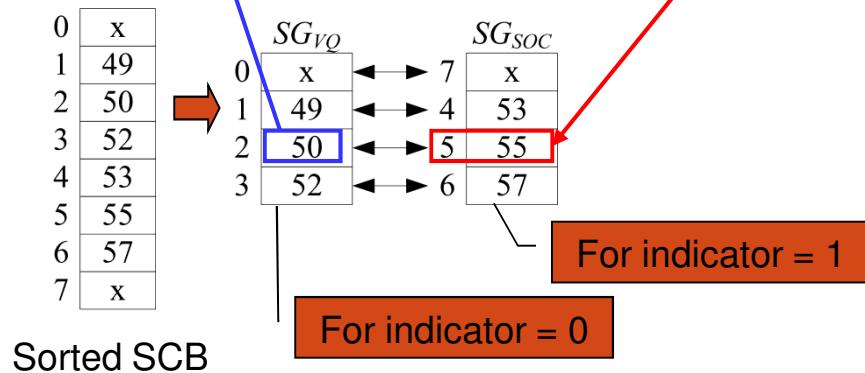
If $SMD(cw_{130}, NBV_{B'}) < SMD(cw_3, NBV_{B'})$
Compression code: ... 10000010
Else Compression code: ... 11111111 10000010

SOC improvement (Cont.)

- The proposed method (Decoding)



Index table



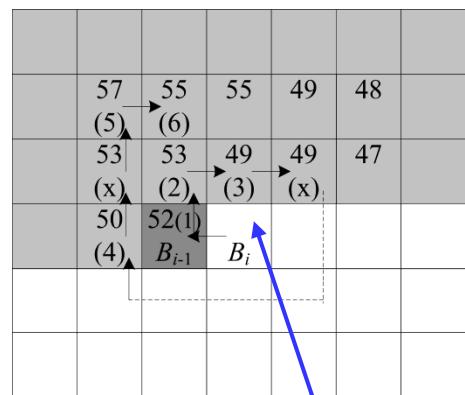
Compression code: ...**101**...

The indicator for next block is '1'

$SMD(cw_{55}, NBV_{B_i}) \geq SMD(cw_{50}, NBV_{B_i})$

Using cw_{50} to decode B_i

SOC improvement (Cont.)



Index table

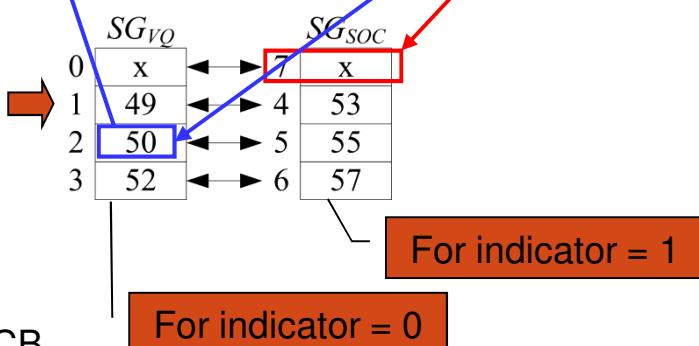
0	x
1	49
2	50
3	52
4	53
5	55
6	57
7	x

Sorted SCB

Compression code: ...111010...

The indicator for next block is '1'

Using cw_{50} to decode B_i



SOC improvement (Cont.)

SMD function			
	$SMD(t_i, NBV_{B_i}) <$	$SMD(t_i, NBV_{B_i}) \geq$	
Relationship	$SMD(\bar{t}_i, NBV_{B_i})$	$SMD(\bar{t}_i, NBV_{B_i})$	
$t_i \in G_{VQ}$	$p_{i+1} = 0$	t_i	$0 t_i$
	$p_{i+1} = 1$	\bar{t}_i	$n - 1 t_i$
$t_i \in G_{SOC}$	$p_{i+1} = 0$	\bar{t}_i	$0 t_i$
	$p_{i+1} = 1$	t_i	$n - 1 t_i$

SMD function			
	$SMD(SCB(t_i), NBV_{B_i}) <$	$SMD(SCB(t_i), NBV_{B_i}) \geq$	
Relationship	$SMD(SCB(\bar{t}_i), NBV_{B_i})$	$SMD(SCB(\bar{t}_i), NBV_{B_i})$	
$t_i \in SG_{VQ}$	$p_{i+1} = 0$	t_i	$0 t_i$
	$p_{i+1} = 1$	\bar{t}_i	$m - 1 t_i$
$t_i \in SG_{SOC}$	$p_{i+1} = 0$	\bar{t}_i	$0 t_i$
	$p_{i+1} = 1$	t_i	$m - 1 t_i$

SOC improvement (Cont.)

- Experimental results

		Codebook size		
Images		$m = 4$	$m = 8$	$m = 16$
Baboon	RBR(%)	3.62	6.66	9.28
	Time(sec.)	0.031	0.047	0.109
	PSNR (dB)	24.7	24.7	24.7
Jet(F16)	RBR (%)	23.39	29.87	30.82
	Time (sec.)	0.015	0.078	0.125
	PSNR (dB)	31.58	31.58	31.58
Lena	RBR (%)	20.92	27.53	29.44
	Time (sec.)	0.031	0.078	0.141
	PSNR (dB)	32.24	32.24	32.24
Pepper	RBR (%)	22.46	28.33	29.41
	Time (sec.)	0.032	0.078	0.141
	PSNR (dB)	30.47	30.47	30.47
Sailboat	RBR (%)	18.38	24.33	25.24
	Time (sec.)	0.015	0.062	0.141
	PSNR (dB)	27.15	27.15	27.15
Tiffany	RBR (%)	35.37	43.17	40.37
	Time (sec.)	0.032	0.094	0.156
	PSNR (dB)	29.57	29.57	29.57
Average RBR (%)		20.69	26.65	27.43
Average time (sec.)		0.03	0.07	0.14
Average PSNR (dB)		29.29	29.29	29.29

		Conditions			
Images		IESOC	SOC	LAS	SMVQ
Baboon	RBR (%)	9.28	4.15	-2.37	10.79
	Time (sec.)	0.109	0.093	3.719	7.969
	PSNR (dB)	24.7	24.7	24.7	24.7
Jet(F16)	RBR (%)	30.82	22.5	18.17	31.89
	Time (sec.)	0.125	0.094	2.406	12.265
	PSNR (dB)	31.58	31.58	31.58	31.57
Lena	RBR (%)	29.44	21.39	13.73	32.3
	Time (sec.)	0.141	0.109	2.547	7.547
	PSNR (dB)	32.24	32.24	32.24	32.23
Pepper	RBR (%)	29.41	20.85	15.79	33.45
	Time (sec.)	0.141	0.11	2.484	7.156
	PSNR (dB)	30.47	30.47	30.47	30.46
Sailboat	RBR (%)	25.24	18.4	14.9	27.53
	Time (sec.)	0.141	0.093	2.156	7.609
	PSNR (dB)	27.15	27.15	27.15	27.15
Tiffany	RBR (%)	40.37	31.63	34.68	36.41
	Time (sec.)	0.156	0.109	1.875	13.609
	PSNR (dB)	29.57	29.57	29.57	29.57
Average RBR (%)		27.43	19.82	15.82	28.73
Average time (sec.)		0.14	0.1	2.53	9.36
Average PSNR (dB)		29.29	29.29	29.29	29.28