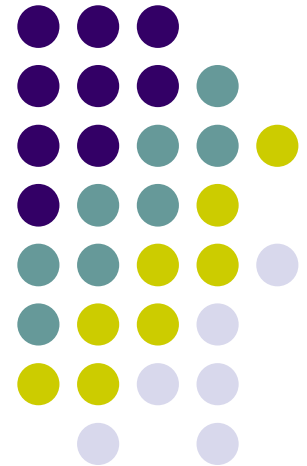


Bahan Kuliah IF4020 Kriptografi

Kriptografi Visual, Teori dan Aplikasinya (Bag. 2)

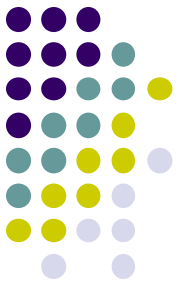
Visual
Cryptography

Oleh:
Rinaldi Munir



Program Studi Teknik Informatika
STEI - ITB





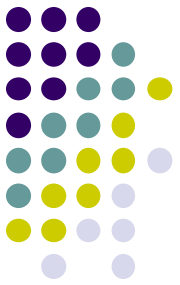
Skema (2, n)

- Satu gambar dibagi menjadi n buah *share*
- Untuk mendekripsi, diperlukan dua buah *share*

$$C_0 = \left\{ \text{seluruh matriks hasil permutasi kolom} \begin{bmatrix} 1 & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & 0 & \dots & 0 \end{bmatrix} \right\}$$

$$C_1 = \left\{ \text{seluruh matriks hasil permutasi kolom} \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix} \right\}$$





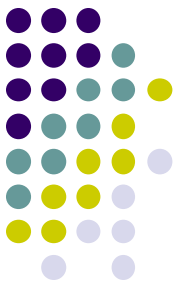
Skema (3, 3)

- Satu gambar dibagi menjadi 3 buah *share*
- Untuk mendekripsi, diperlukan 3 buah *share*

$$C_0 = \left\{ \text{seluruh matriks hasil permutasi kolom} \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \right\}$$

$$C_1 = \left\{ \text{seluruh matriks hasil permutasi kolom} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \right\}$$





Skema (3, n)

- Satu gambar dibagi menjadi n buah *share*
- Untuk mendekripsi, diperlukan 3 buah *share*
- Misalkan:

B = matriks $n \times 1$ yang bernilai 1 seluruhnya

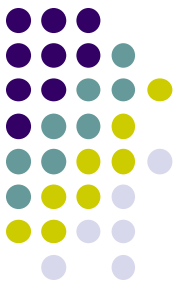
I = matriks identitas $n \times n$ (diagonal utama = 1)

BI = matriks hasil penggabungan B dan I

$c(BI)$ = matriks komplemen dari BI

- Maka,
 $C_0 = \{ \text{seluruh matriks hasil permutasi kolom dari } c(BI) \}$
 $C_1 = \{ \text{seluruh matriks hasil permutasi kolom dari } BI \}$





Contoh: $n = 3 \rightarrow$ Skema (3, 3)

$$\begin{array}{c}
 B: \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad I: \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad BI: \begin{array}{c} \text{BLACK} \\ \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \quad c(BI): \begin{array}{c} \text{WHITE} \\ \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}
 \end{array}
 \end{array}$$

Misalkan permutasinya adalah $\{2, 3, 4, 1\}$

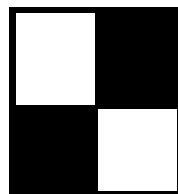
$$\text{putih} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \quad \text{hitam} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Shares

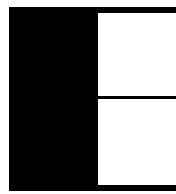
White Pixel

Black Pixel

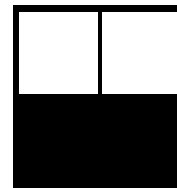
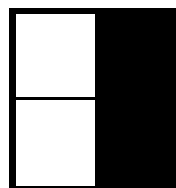
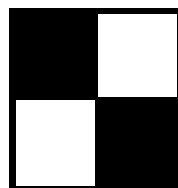
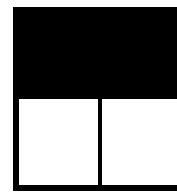
share1



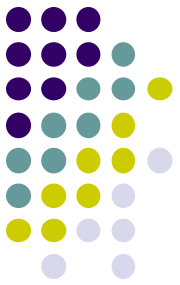
share2



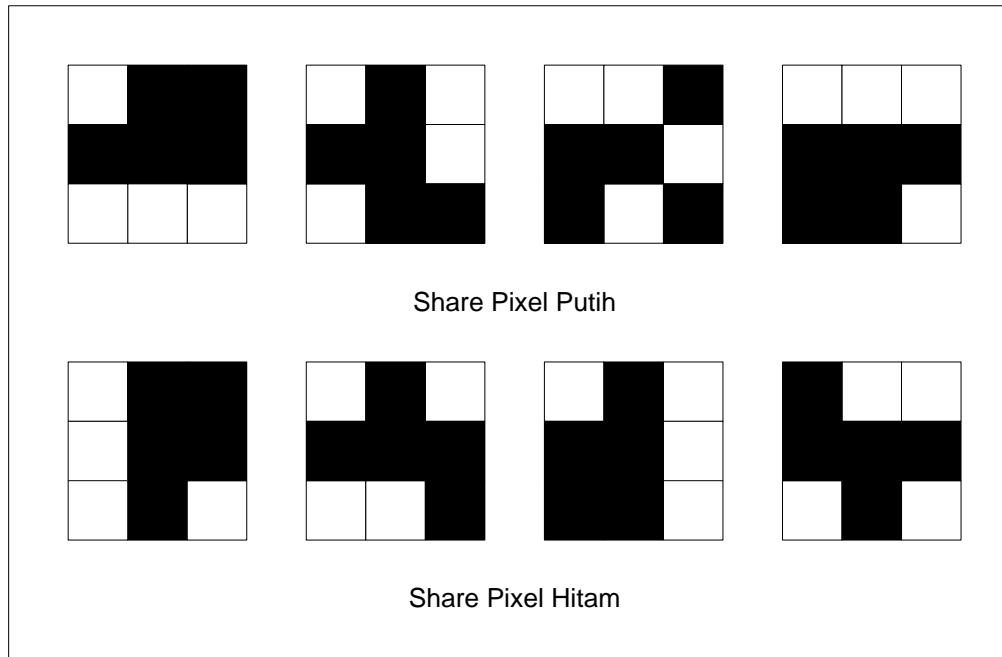
share3



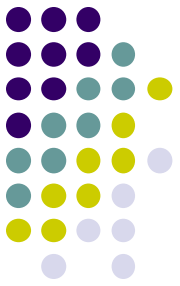
Skema(4, 4)



- Satu gambar dibagi menjadi 4 buah *share*
- Untuk mendekripsi, diperlukan 4 buah *share*

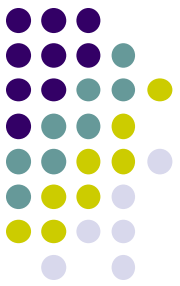


Skema (k, n)

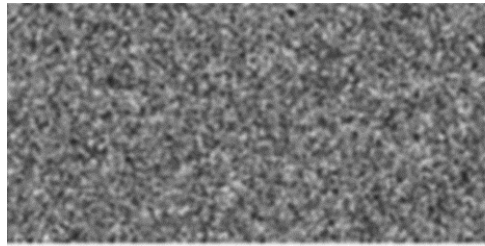


- Satu gambar dibagi menjadi n buah *share*
- Untuk mendekripsi gambar, diperlukan paling sedikit k buah *share*
- Jika jumlah *share* yang ditumpuk kurang dari k , maka tidak dapat menghasilkan gambar semula

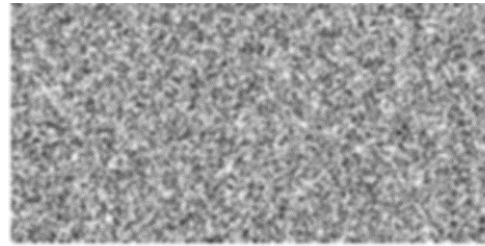




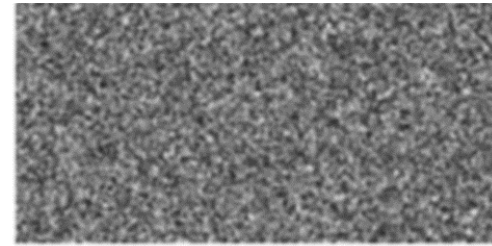
Contoh: skema (3, 4)



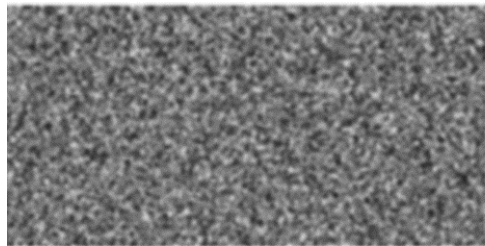
Share S1



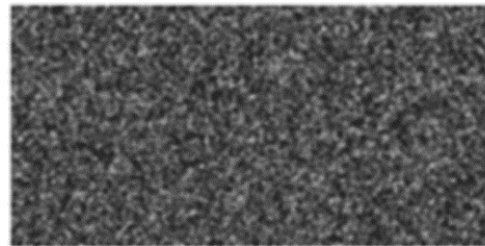
Share S2



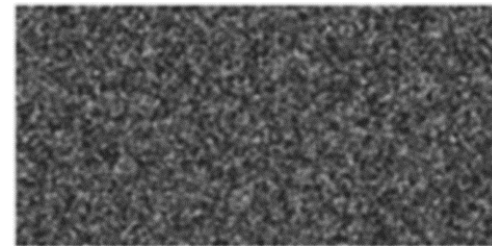
Share S3



Share S4



S1 + S2



S1 + S3



S1 + S3 + S4



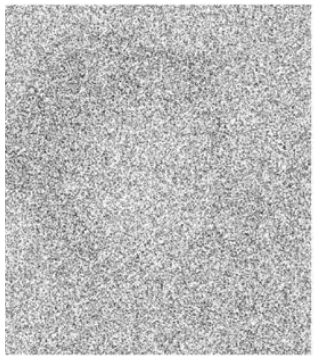
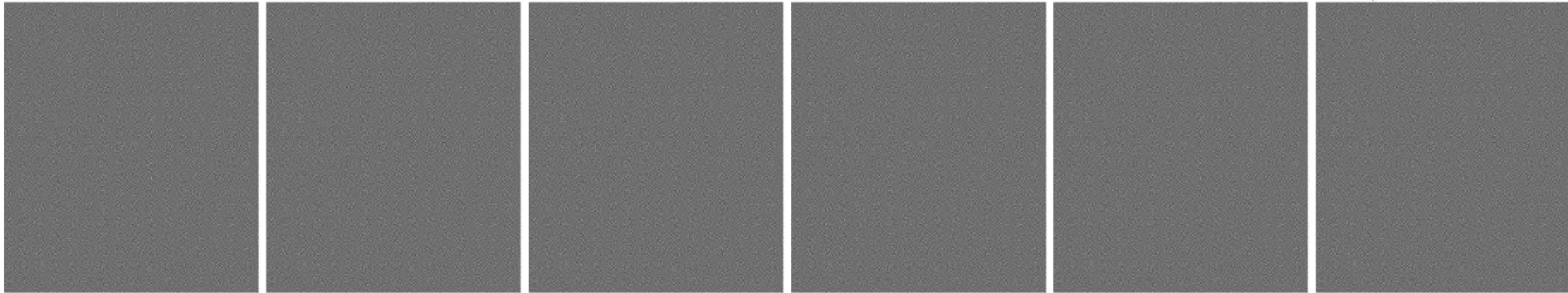
S2 + S3 + S4



S1 + S2 + S3 + S4



Hasil bermacam-macam Skema ($k, 6$)



(2, 6)



(3, 6)



(4, 6)

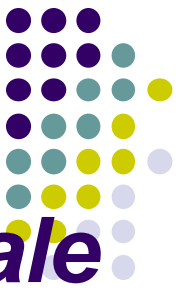


(5, 6)



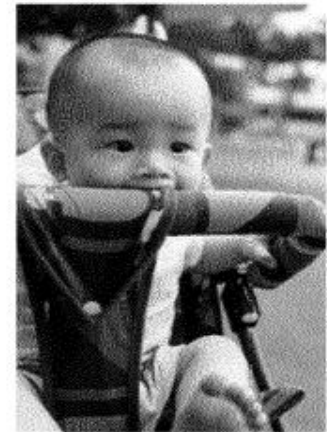
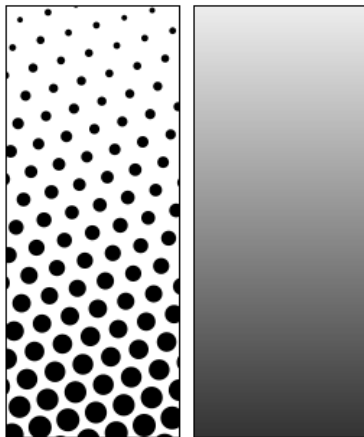
(6, 6)





Kriptografi Visual untuk Citra *Grayscale*

- Citra *grayscale* diubah terlebih dahulu menjadi citra *halftone* (*halftone image*)
- *Halftone image*: teknik reproduksi citra yang mensimulasikan citra yang memiliki level keabuan yang kontinu dengan menggunakan titik-titik (*dot*) yang bervariasi ukuran dan jarak spasi antar titik.

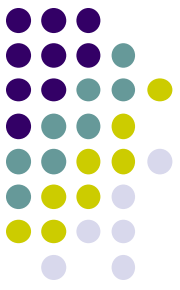


Secret pixel color	White						Black					
<i>Share blocks</i>												
2×2 block of the first share												
2×2 block of the second share												
Stacked 2×2 block												

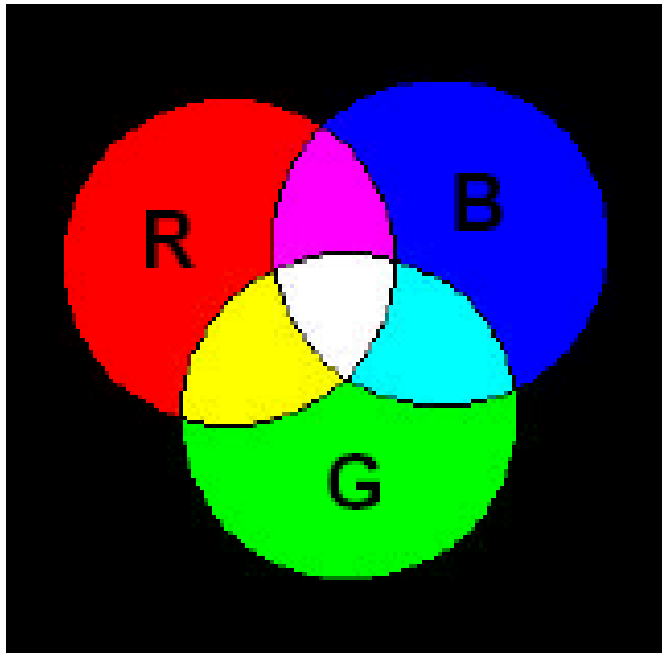


Share 1

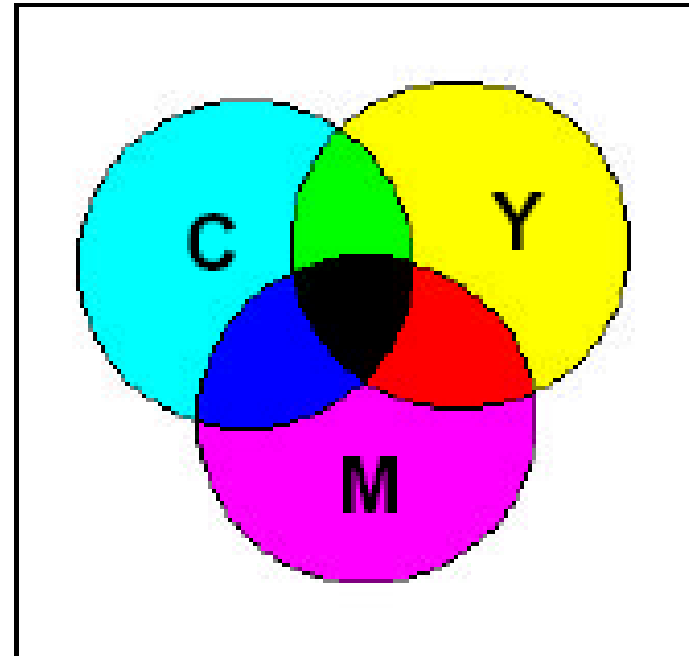
Share 2



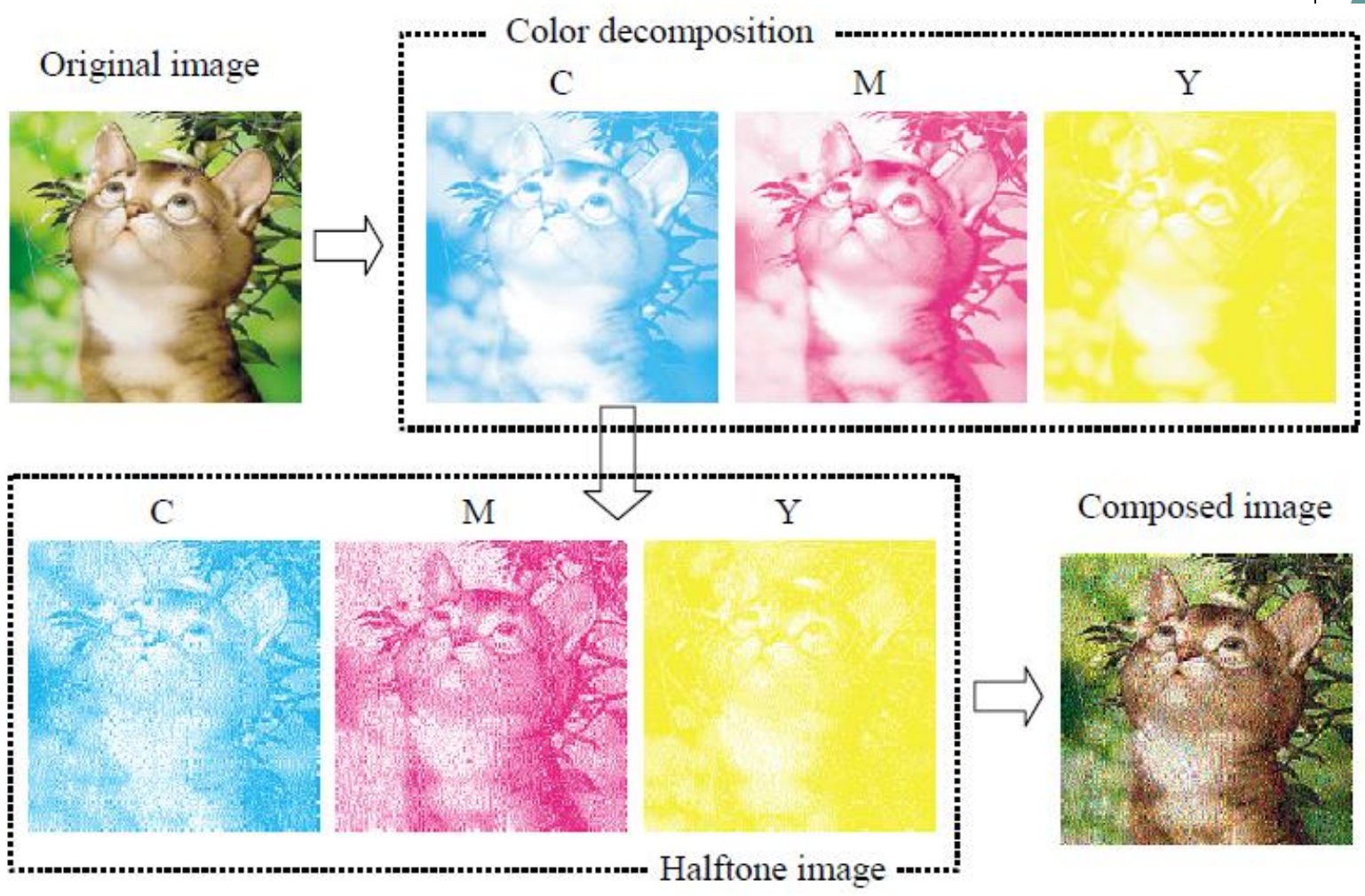
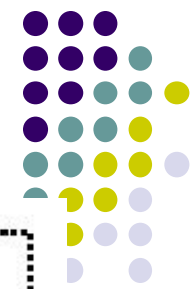
Kriptografi visual untuk Citra Berwarna

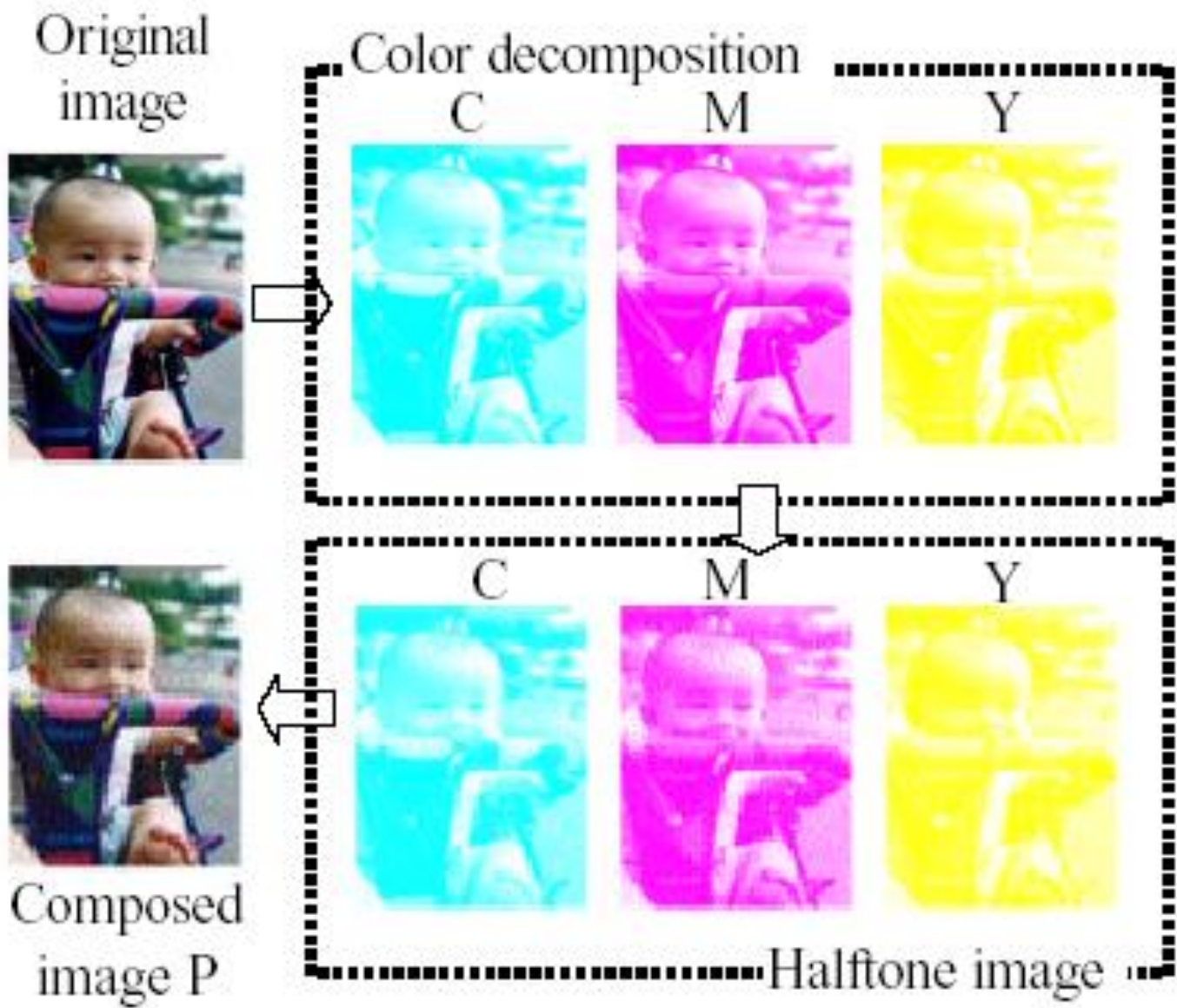


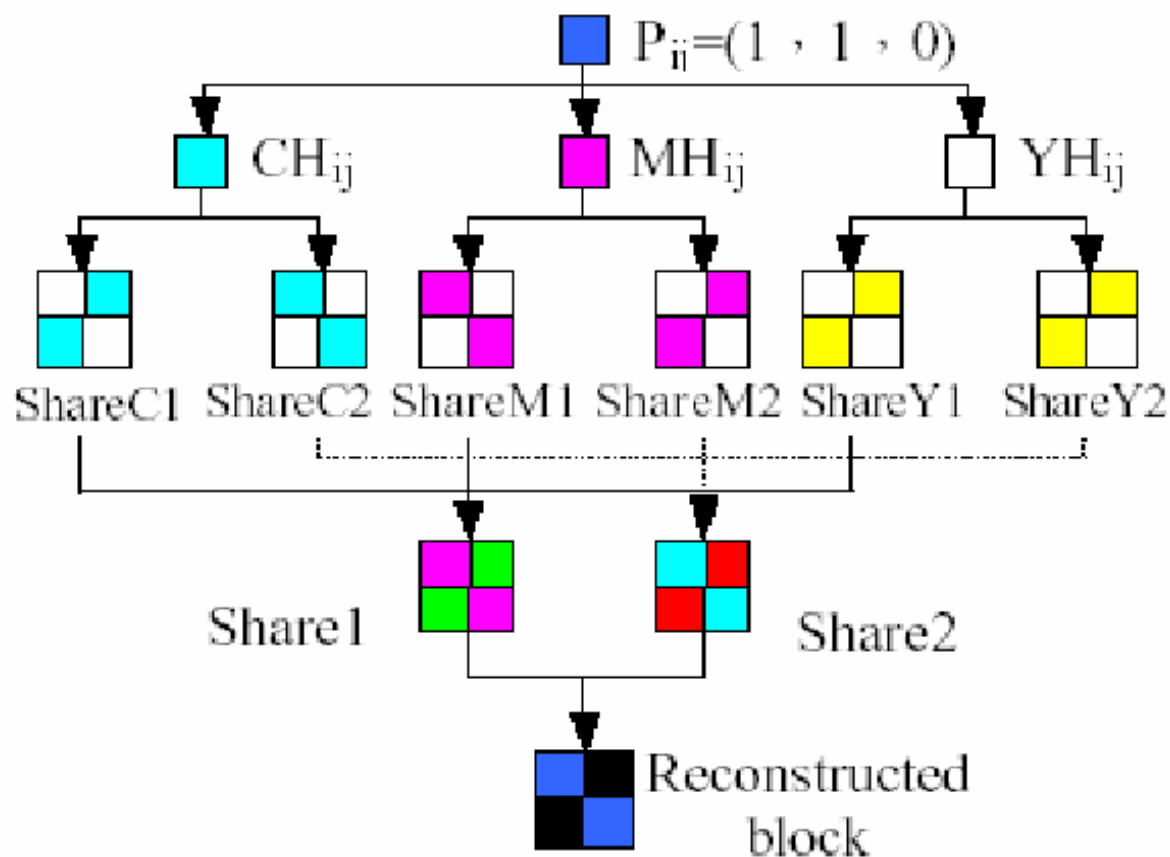
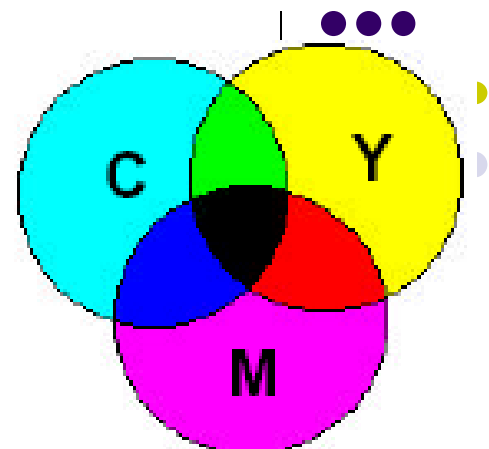
RGB: TV dan monitor

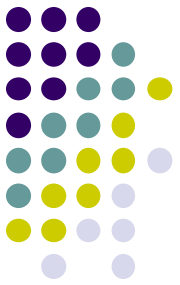


CMY: Warna hasil cetakan

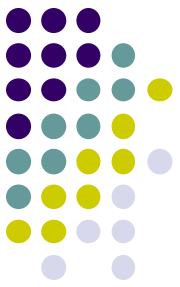








Share 1	Share 2	Hasil tumpukan	Share 1	Share 2	Hasil tumpukan



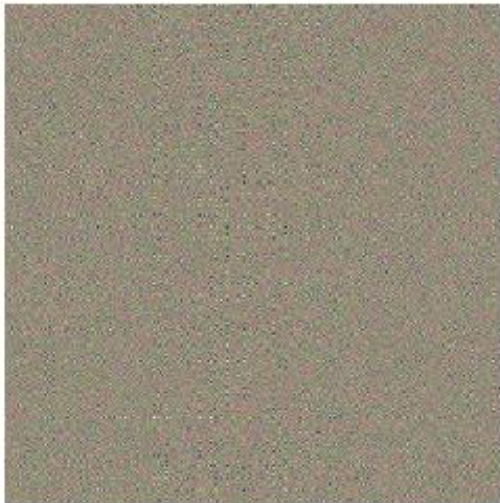
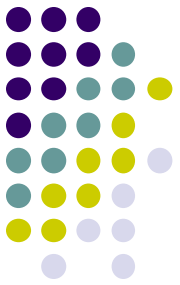
Share 1



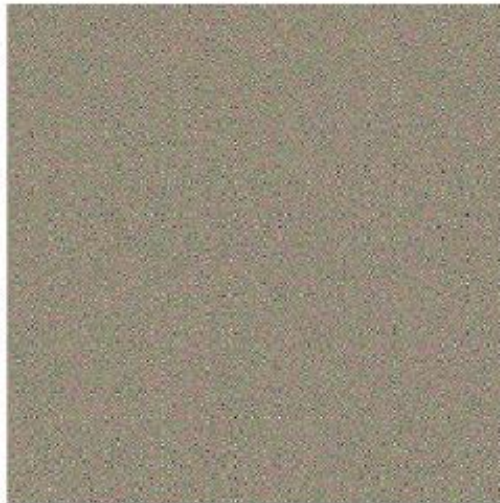
Share 2



Hasil tumpukan



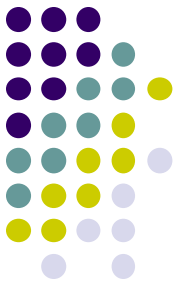
Share 1



Share 2



Hasil tumpukan



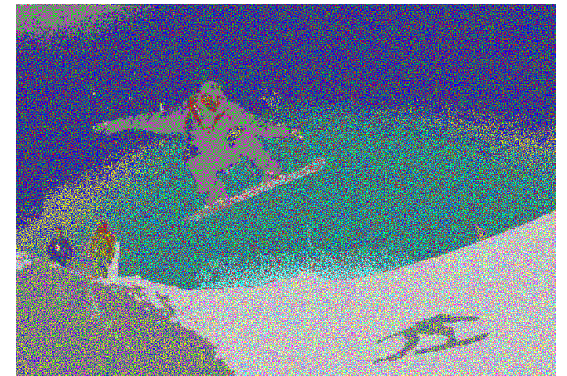
Original image



Share 1

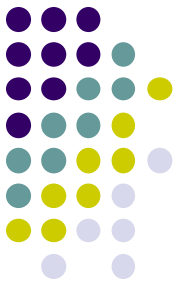


Share 2

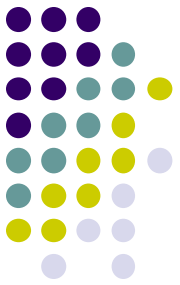


Hasil tumpukan

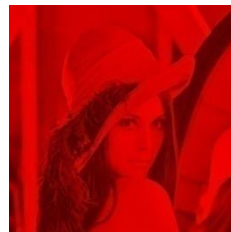
Algoritma Kriptografi Visual dengan Fungsi XOR



- Kriptografi visual untuk citra berwarna
- Tidak melakukan pembagian *pixel* menjadi *sub-pixel*.
- Ukuran *share* sama dengan ukuran citra semula
- Citra hasil dekripsi tepat sama dengan citra semula.
- Skema (n, n)
- Operator: XOR (dilambangkan dengan \oplus)



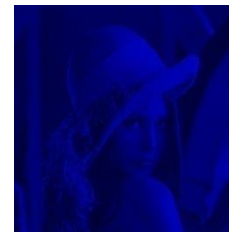
Original Image



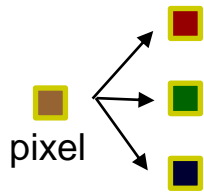
Red



Green



Blue



150		1 0 0 1 0 1 1 0
100		0 1 1 0 0 1 0 0
50		0 0 1 1 0 0 1 0

150		1 0 0 1 0 1 1 0
-----	--	-----------------

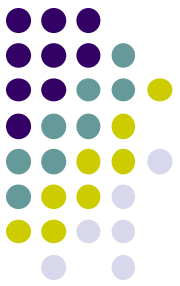
Contoh 2 buah share:

100		0 1 1 0 0 1 0 0
-----	--	-----------------

226		1 1 1 0 0 0 1 0
-----	--	-----------------

Perhatikan:

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



Algoritma enkripsi:

1. Misalkan *plain-image* adalah P , *share* yang dihasilkan adalah A_1, \dots, A_n , dan matriks acak untuk membantu enkripsi, yakni B_1, \dots, B_{n-1} . Semua matriks berukuran sama.

2. Skema (n,n) dapat dihasilkan dengan urutan:

$$A_1 = B_1$$

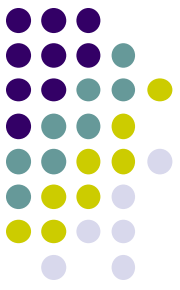
$$A_2 = B_1 \oplus B_2$$

...

$$A_{n-1} = B_{n-2} \oplus B_{n-1}$$

$$A_n = B_{n-1} \oplus P$$

3. Seluruh citra *share* untuk skema (n,n) telah dihasilkan.

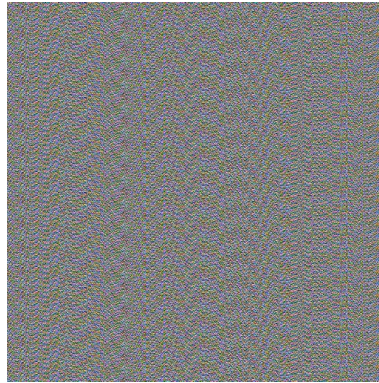


- Untuk merekonstruksi citra, dilakukan dengan meng-*XOR*-kan seluruh citra *share*, yang dijabarkan sebagai berikut:

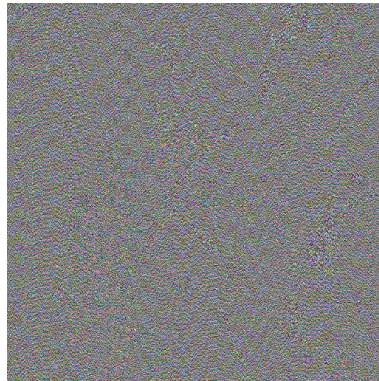
$$\begin{aligned} & A_1 \oplus A_2 \oplus A_3 \oplus \dots \oplus A_{n-1} \oplus A_n \\ &= B_1 \oplus (B_1 \oplus B_2) \oplus (B_2 \oplus B_3) \oplus \dots \oplus (B_{n-2} \oplus B_{n-1}) \oplus B_{n-1} \oplus P \\ &= (B_1 \oplus B_1) \oplus (B_2 \oplus B_2) \oplus B_3 \oplus \dots \oplus B_{n-2} \oplus (B_{n-1} \oplus B_{n-1}) \oplus P \\ &= (0 \oplus 0 \oplus \dots \oplus 0) \oplus P \\ &= 0 \oplus P \\ &= P \end{aligned}$$



Original Image



Share 1



Share 2



XOR



Recover Image





XOR

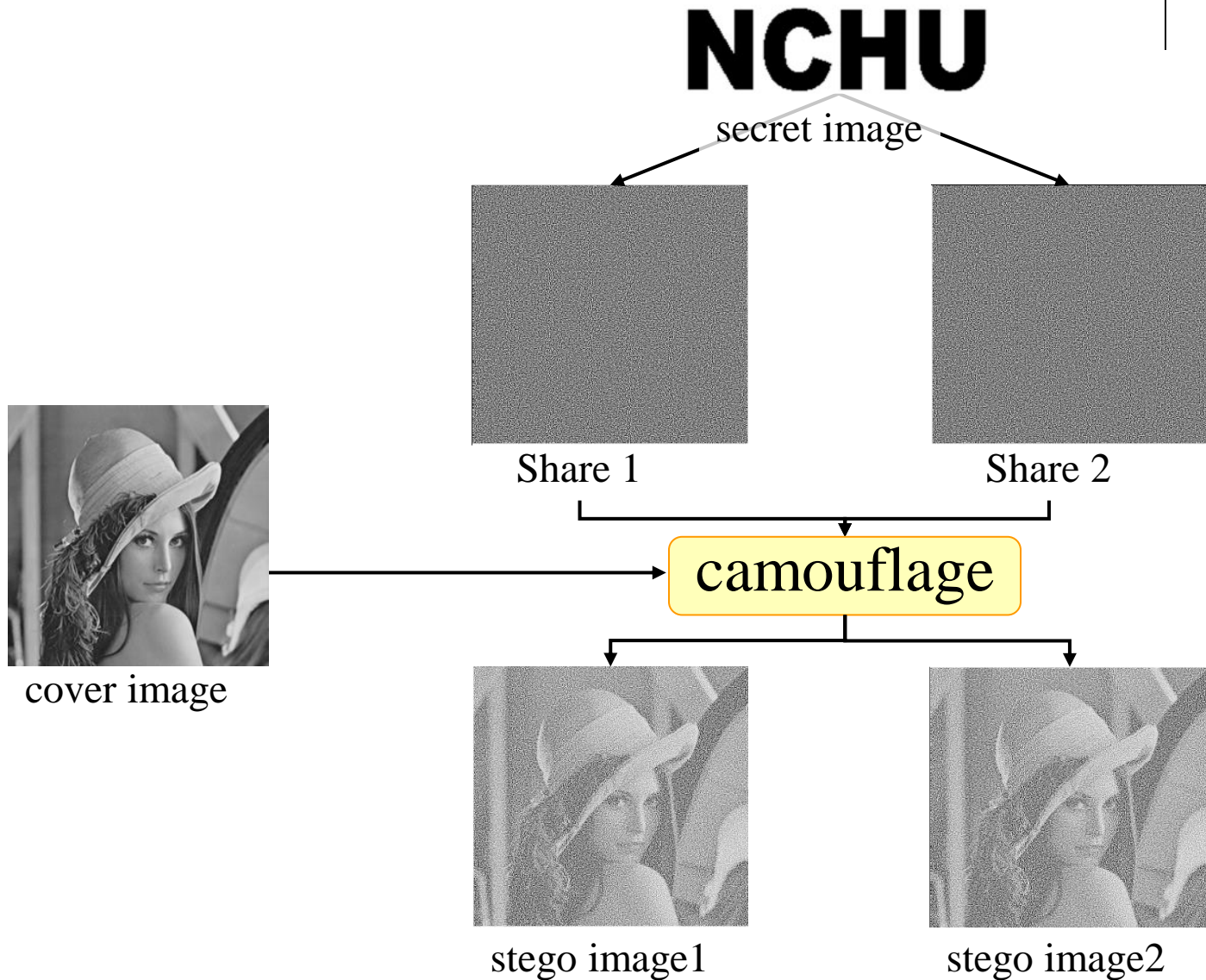
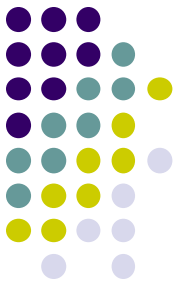


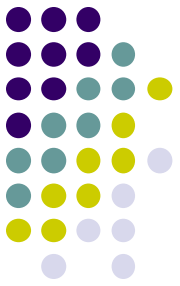
Kelemahan Kriptografi Visual



- Citra hasil dekripsi tidak tepat sama dengan citra asli.
- Citra hasil dekripsi mengandung *noise*.
- *Share* tidak memiliki makna → dapat menimbulkan kecurigaan bahwa gambar tsb merupakan pesan rahasia.
- Untuk menghilangkan kecurigaan, digunakan **steganografi** sebagai pelengkap kriptografi.
- Digunakan beberapa gambar lain sebagai *cover* untuk menyembunyikan *share*.
- *Share + cover = camouflage*

Teknik Camouflage

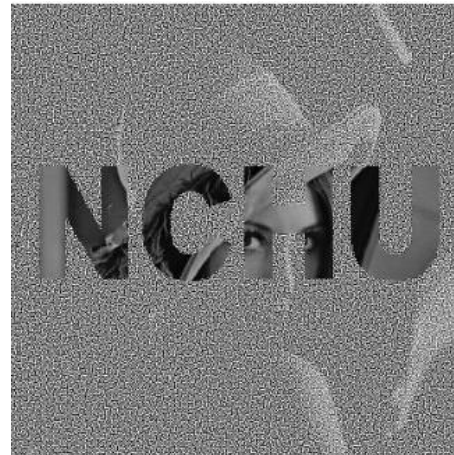












stego image1

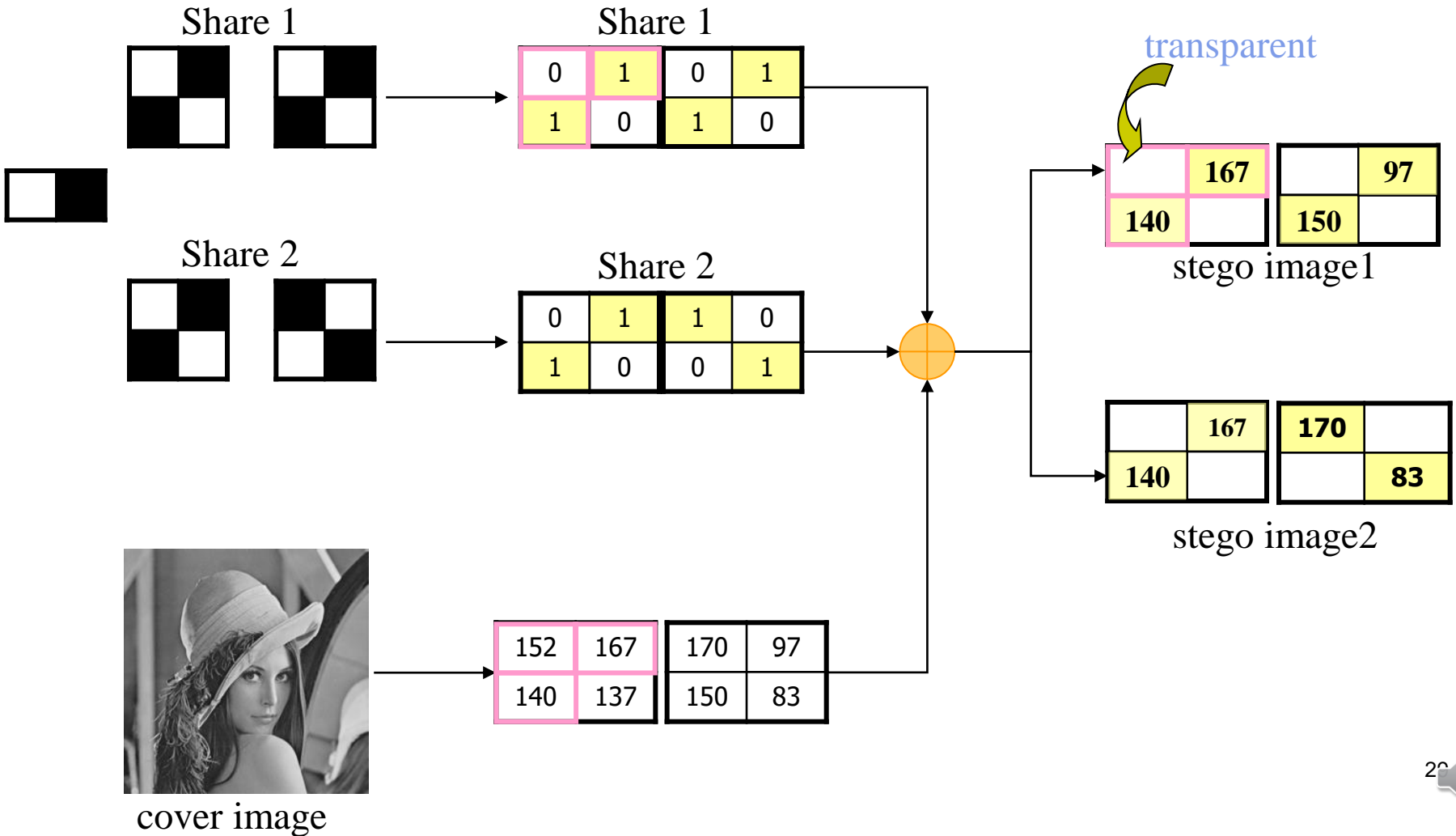


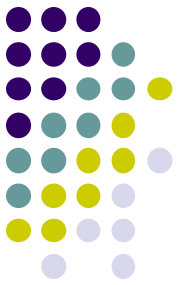
stego image2



Stego image 1 + stego image 2

Secret image	Share 1	Share 2	Stacked image
			
			





stego image 1

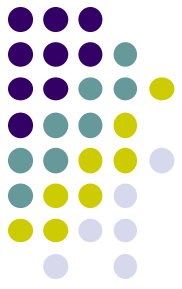
	167		97
140		150	



stego image 2

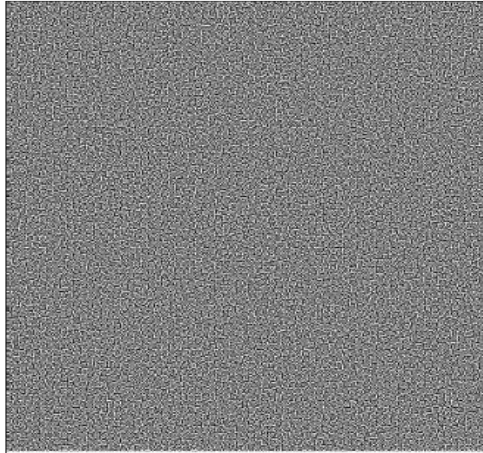
	167	170	
140			83

Stego image 1 + stego image 2



Contoh hasil eksperimen:

Share 1



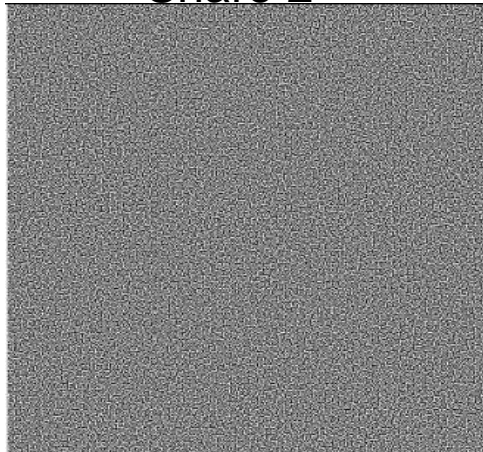
cover image1



stego image1



Share 2

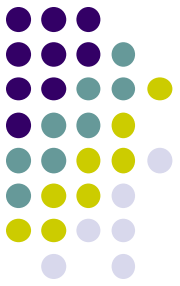


cover image2



stego image2

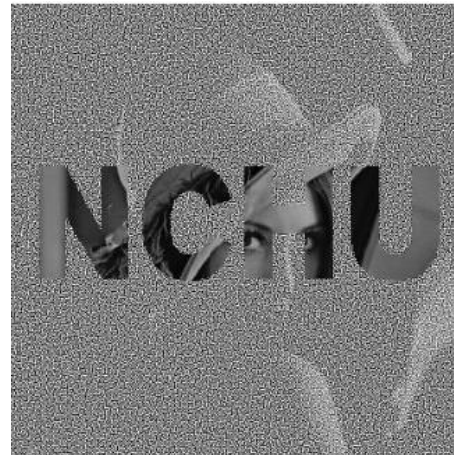




stego image1



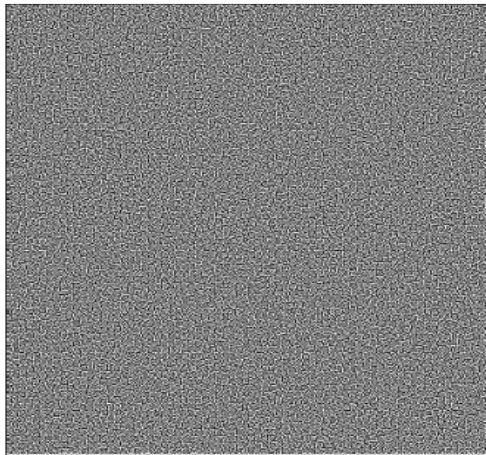
stego image2



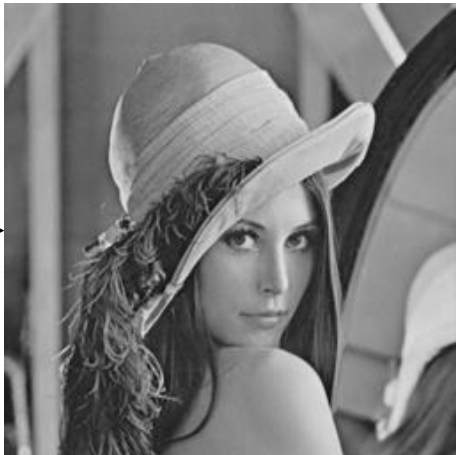
Staeo image 1 + stego image 2



shadow1



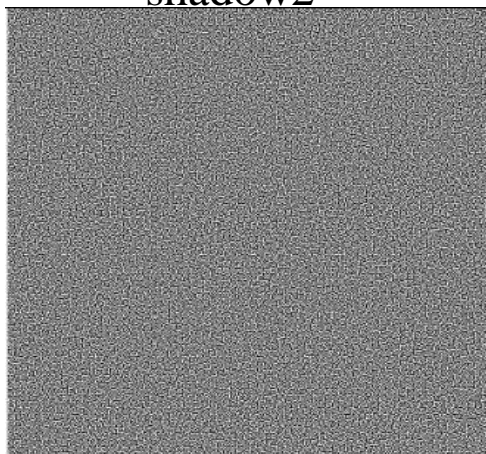
cover image1



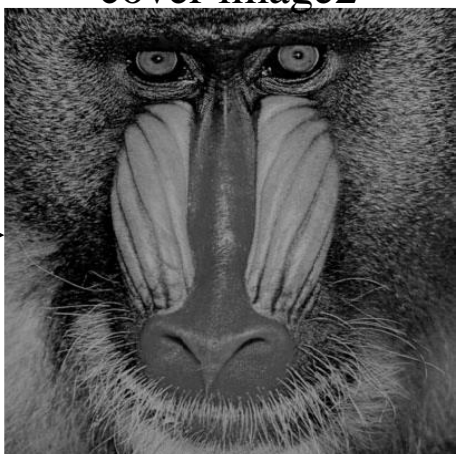
stego image1



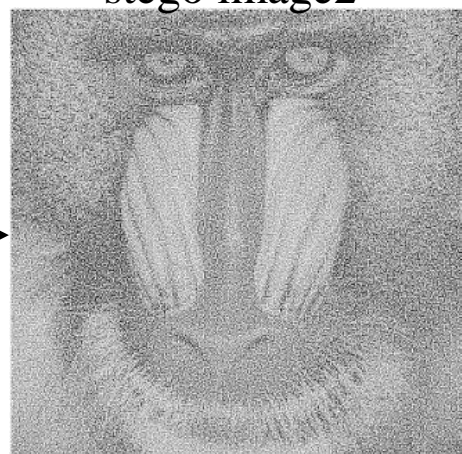
shadow2

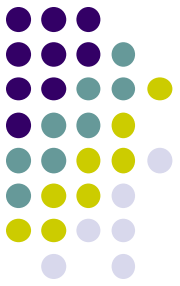


cover image2



stego image2

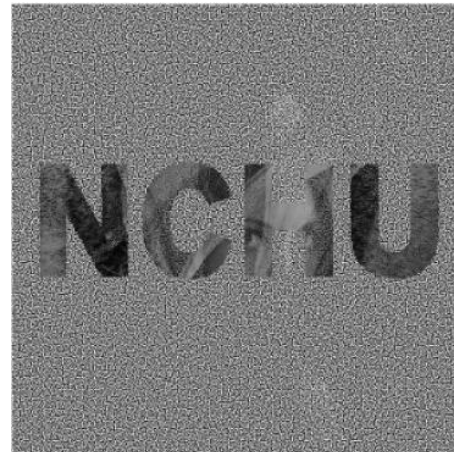
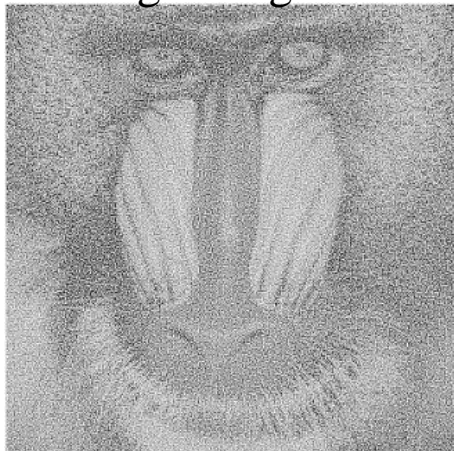




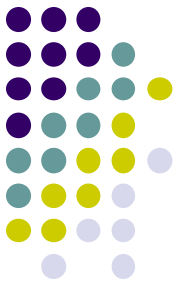
stego image1



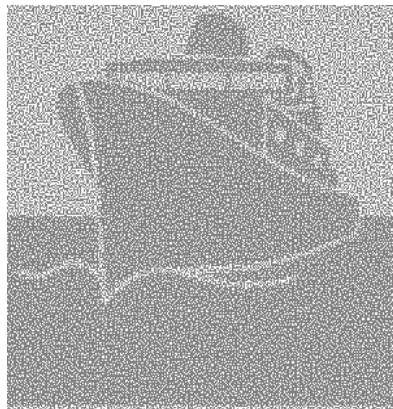
stego image2



stacked result

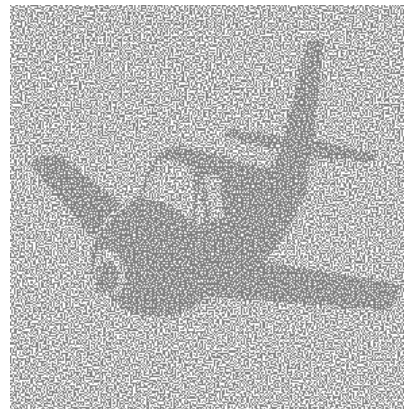


- Contoh untuk citra biner



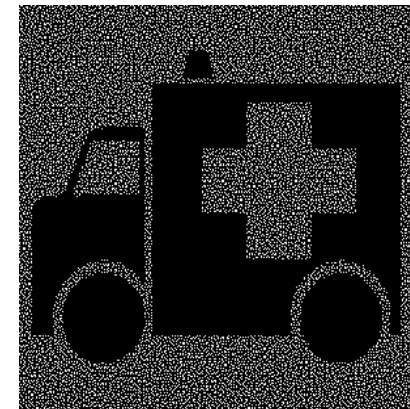
Stego image 1

+



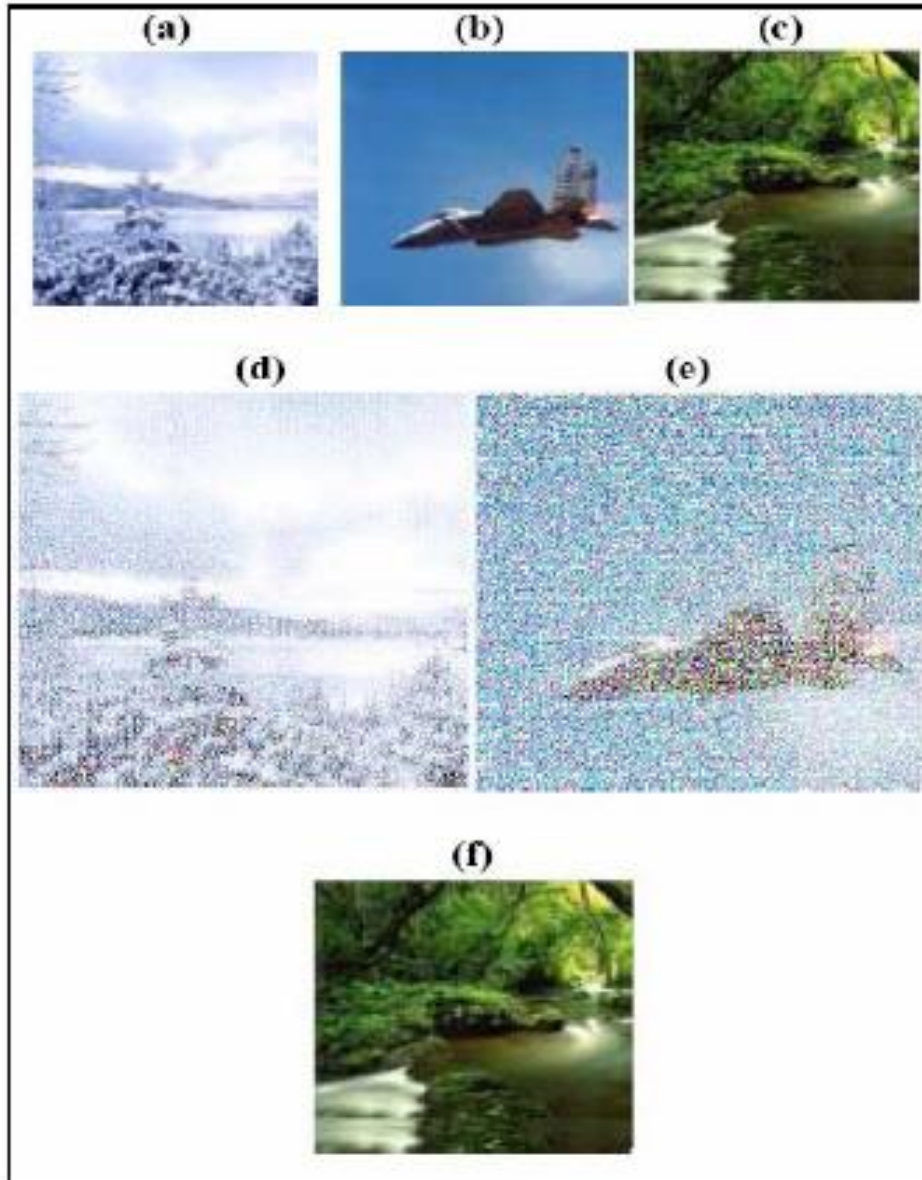
Stego image 2

=



Stego image 1 +
stego image 2

- Contoh untuk citra berwarna



Keterangan:

(a) *cover 1*

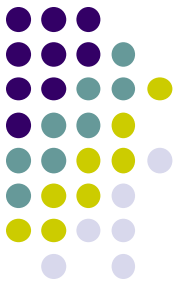
(b) *cover 2*

(c) *Secret image*

(d) *Share 1*

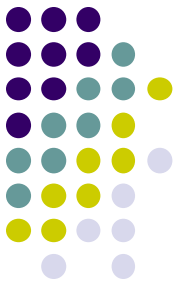
(e) *Share 2*

(f) Hasil dekripsi



Gambar 13 : Kriptografi Visual Chang dkk.

Aplikasi Kriptografi Visual

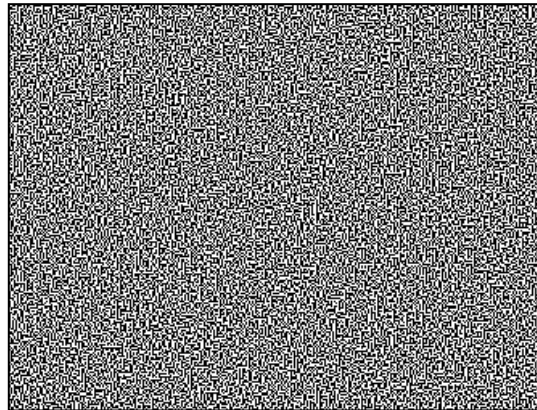


1. Otentikasi (*authentication*)

- Misalkan Bank mengirim kepada nasabah $n - 1$ buah *share* sebagai *share* kunci
- Situs bank menampilkan sebuah *share*
- Nasabah melakukan penumpukan, membaca tulisan yang muncul pada hasil tumpukan (yang menyatakan kunci transaksi)
- Selanjutnya nasabah memasukkan kunci transaksi



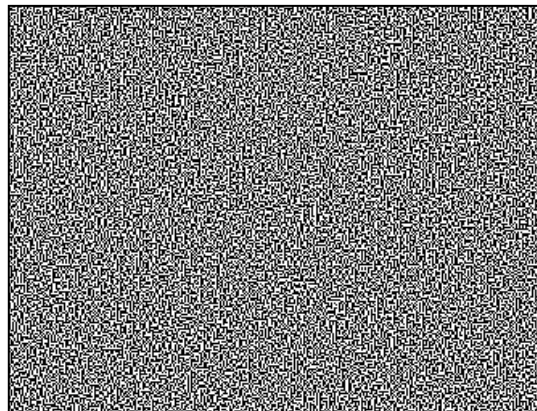
Bank



Share 1



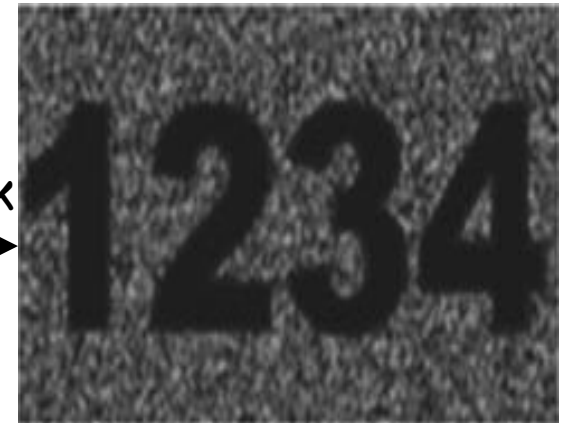
Nasabah



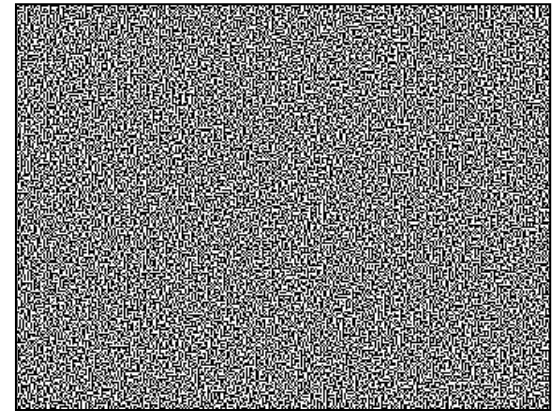
Share 2



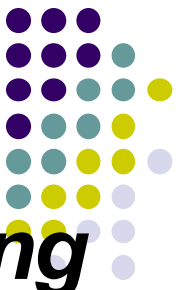
Tumpuk



Recovered secret image



Hacker

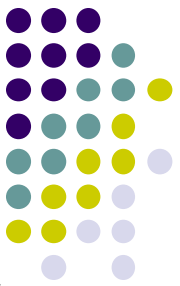


2. ***Verifiable Receipts in Electronic Voting***

Menggunakan dua buah *share* sebagai kunci, satu untuk *voter* dan satu lagi untuk sistem.

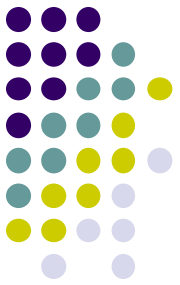
3. ***Sharing confidential documents or keys***

Dokumen rahasia dibagi kepada beberapa orang sebagai *share*. Untuk membacanya diperlukan beberapa *share*.

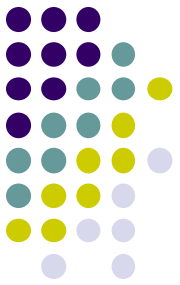


Referensi

1. Arif Ramdhoni, *Kriptografi Visual pada Citra Biner dan Berwarna serta Pengembangannya dengan Steganografi dan Fungsi XOR*, Tugas Akhir Informatika ITB, 2008.
2. Rinaldi Munir, *Bahan Kuliah IF4020 Kriptografi*, Program Studi Informatika STEI-ITB, 2014.
3. Semin Kim, *Visual Cryptography, Advanced Information Security*, Korea Advanced Institute of Science and Technology (KAIST), 2010.
4. Chin-Chen Chang, *Visual Cryptography*, National Tsing Hua University, Taiwan.
5. Kristin Burke, *Visual Cryptography*
6. Hossein Hajiabolhassan, *Visual Cryptography*, Department of of Mathematical Sciences Shahid Beheshti University, Tehran, Iran, 2009
7. Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo, *Halftone Visual Cryptography*, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 15, NO. 8, AUGUST 2006, pp. 2441-2453



8. Salik Jamal and Warsi, Siddharth Bora, *Visual Cryptography*.
9. Jiangyi Hu, *Visual Cryptography*
10. Frederik Vercauteren, *Visual Cryptography*, University of Bristol, 2001
11. Ricardo Martin, *Visual Cryptography: Secret Sharing without a Computer*, GWU Cryptography Group, 2005



TAMAT