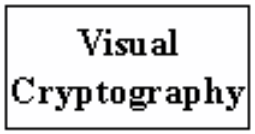
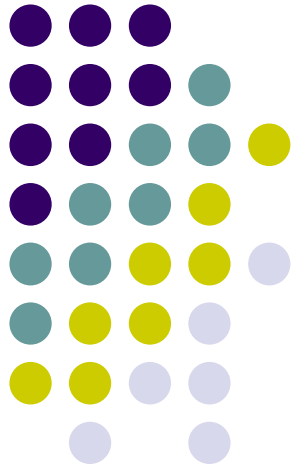
Kuliah Umum di Program Studi Teknik Informatika,
Universitas Kristen Satya Wacana, Salatiga,
Sabtu 26 November 2016

# Kriptografi Visual, Teori dan Aplikasinya

Dr. Rinaldi Munir *)



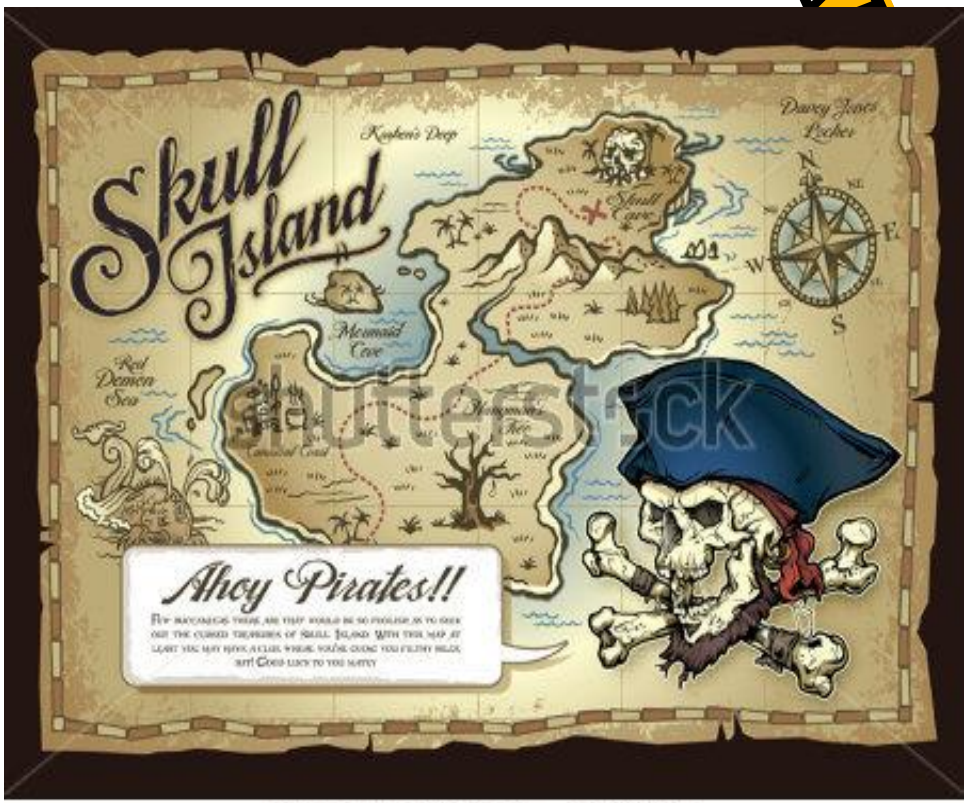
*) Kelompok Keahlian Informatika
Sekolah Teknik Elektro dan Informatika ITB


Universitas Kristen Satya Wacana Salatiga

Sekolah Teknik Informatika dan Elektro ITB

# Sebuah cerita…

Ada seorang kepala perompak. Dia mempunyai sebuah gambar peta rahasia yang berisi petunjuk harta karun. Dia ingin membagi gambar peta itu kepada 6 orang anak buahnya, namun untuk merekonstruksi gambar peta itu dibutuhkan sedikitnya 3 bagian gambar. Bagaimana caranya?




www.shutterstock.com · 90606391

Solusi: **Visual Cryptography**!!!!

# Visual

- Apapun yang dipersepsi oleh indra penglihatan

- Informasi visual: teks, gambar, video, animasi, object 3D

- Teks

A Quick Brown Fox Jumps Over The Lazy Dog 0123456789
A Quick Brown Fox Jumps Over The Lazy Dog 0123456789
A Quick Brown Fox Jumps Over The Lazy Dog 0123456789
A Quick Brown Fox Jumps Over The Lazy Dog 0123456789
A Quick Brown Fox Jumps Over The Lazy Dog 0123456789
A Quick Brown Fox Jumps Over The Lazy Dog 0123456789
A Quick Brown Fox Jumps Over The Lazy Dog 0123456789
A Quick Brown Fox Jumps Over The Lazy Dog 0123456789
A Quick Brown Fox Jumps Over The Lazy Dog 0123456789
A Quick Brown Fox Jumps Over The Lazy Dog 0123456789
A Quick Brown Fox Jumps Over The Lazy Dog 0123456789

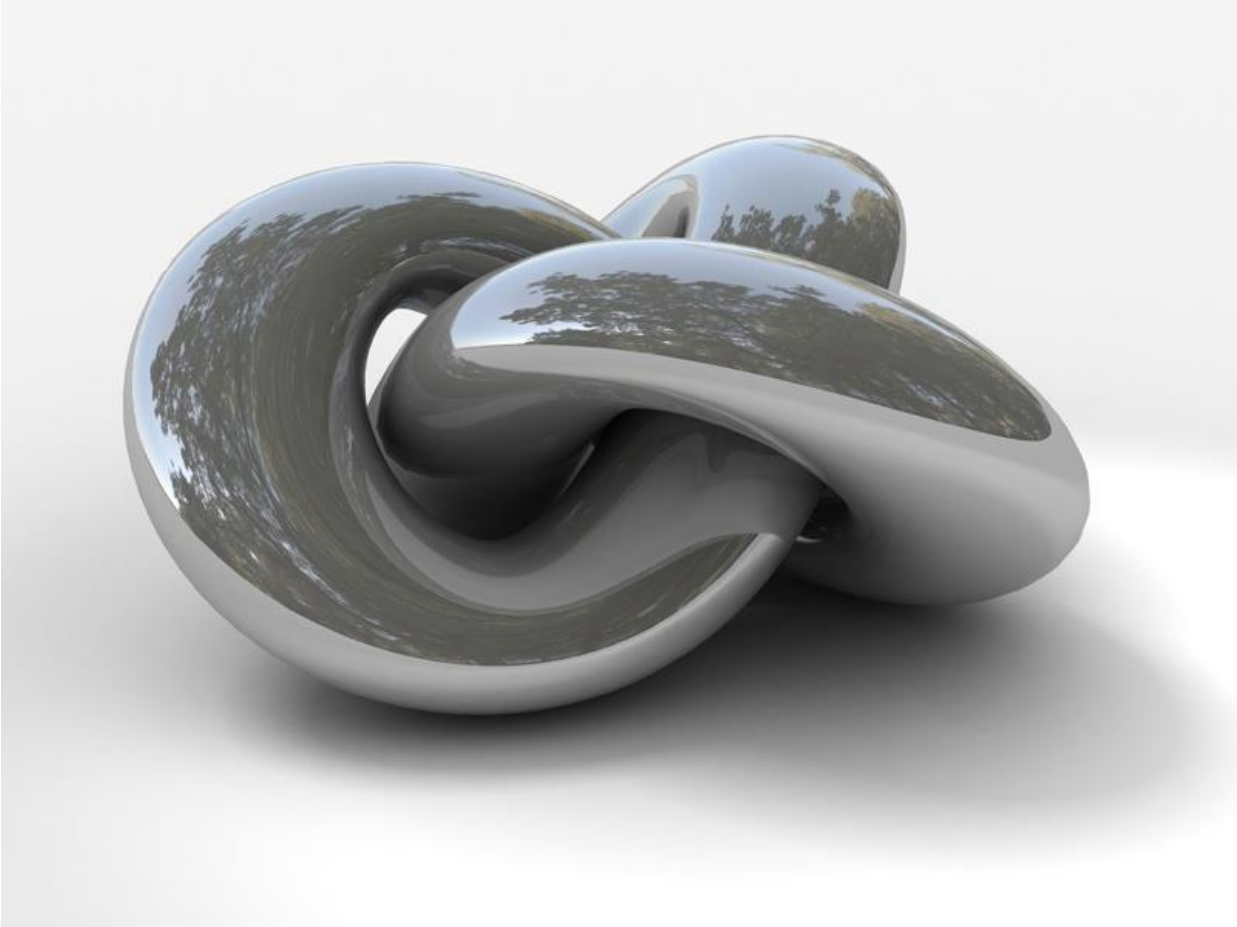
- Gambar (citra)

"Sebuah gambar bermakna lebih dari seribu kata"
(*A picture is more than a thousand words*)

- Video

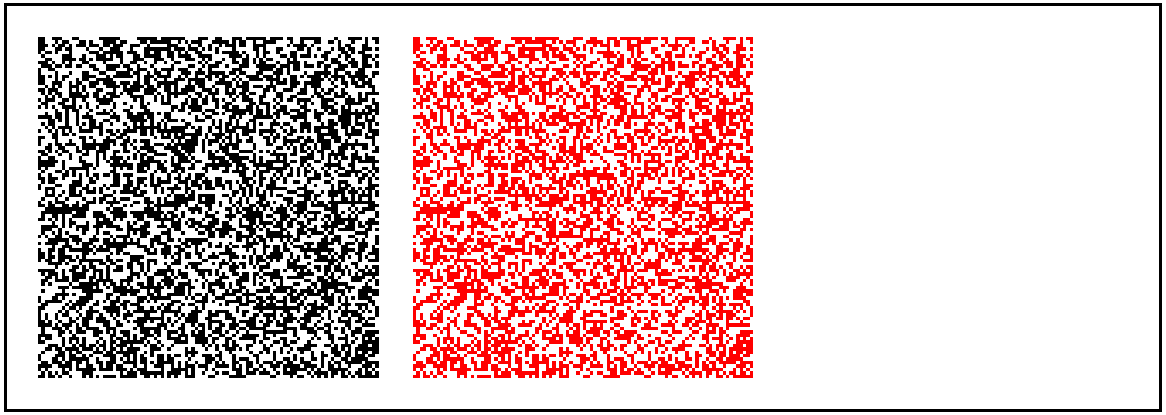
- Animasi

- Object 3D



# Visual Cryptography

- Teknik kriptografi yang *mengenkripsi* informasi visual dengan suatu cara sehingga *dekripsi* cukup dilakukan dengan mempersepsi informasi menggunakan indra penglihatan (mata).



- Diperkenalkan oleh Moni Naor dan Adi Shamir dalam makalah berjudul "*Visual Cryptography*" di dalam jurnal *Eurocrypt'94*

Visual Cryptography*

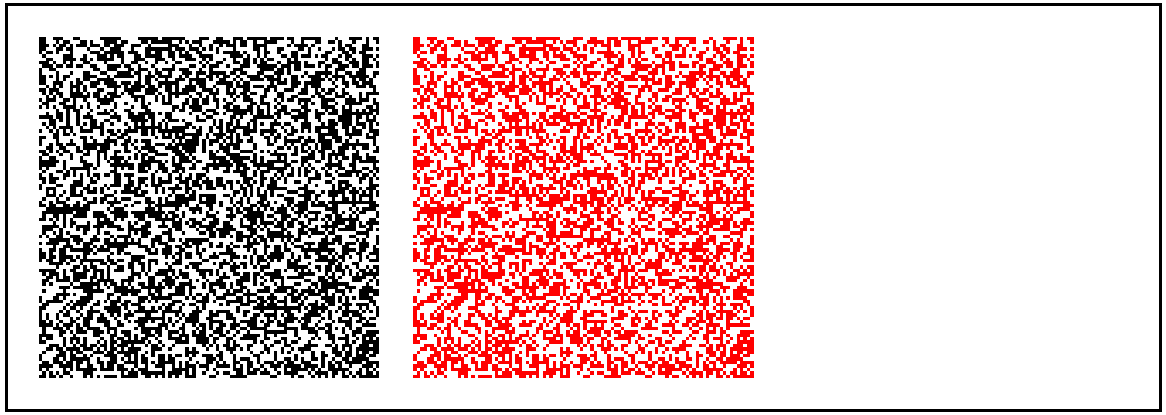
Moni Naor †  Adi Shamir ‡

**Abstract**

In this paper we consider a new type of cryptographic scheme, which can decode concealed images without any cryptographic computations. The scheme is perfectly secure and very easy to implement. We extend it into a visual variant of the $k$ out of $n$ secret sharing problem, in which a dealer provides a transparency to each one of the $n$ users; any $k$ of them can see the image by stacking their transparencies, but any $k-1$ of them gain no information about it.

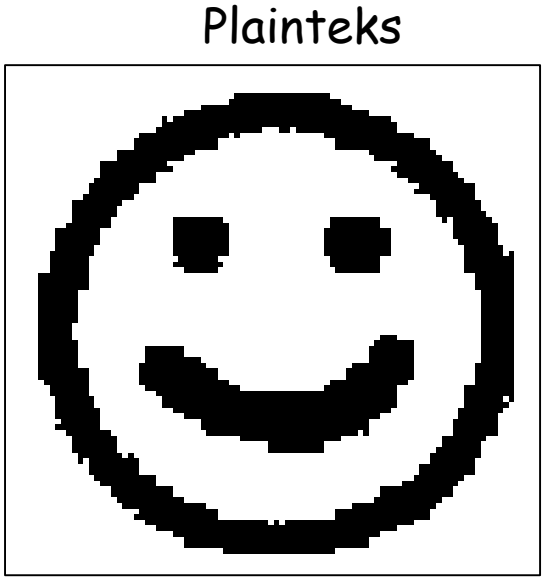
- Enkripsi dilakukan dengan membagi gambar menjadi sejumlah bagian yang disebut ***share***.

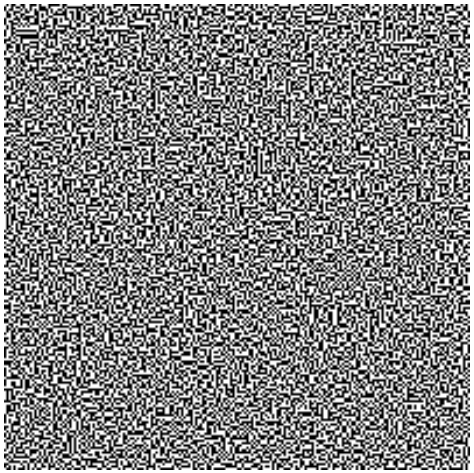
- Setiap *share* terlihat seperti citra acak yang tak bermakna sehingga disebut juga *shadow*.



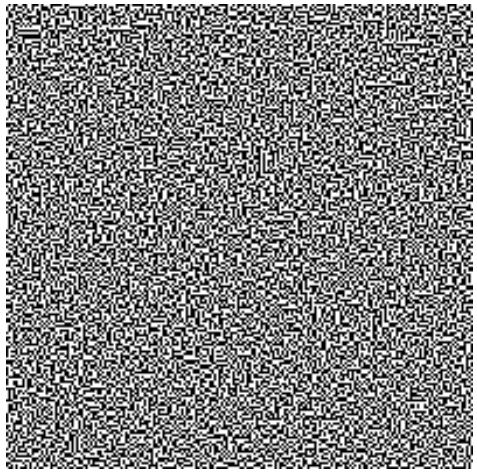
- Tidak membutuhkan komputasi untuk dekripsi citra. Dekripsi dilakukan dengan menumpuk sejumlah *share*.

# Contoh:



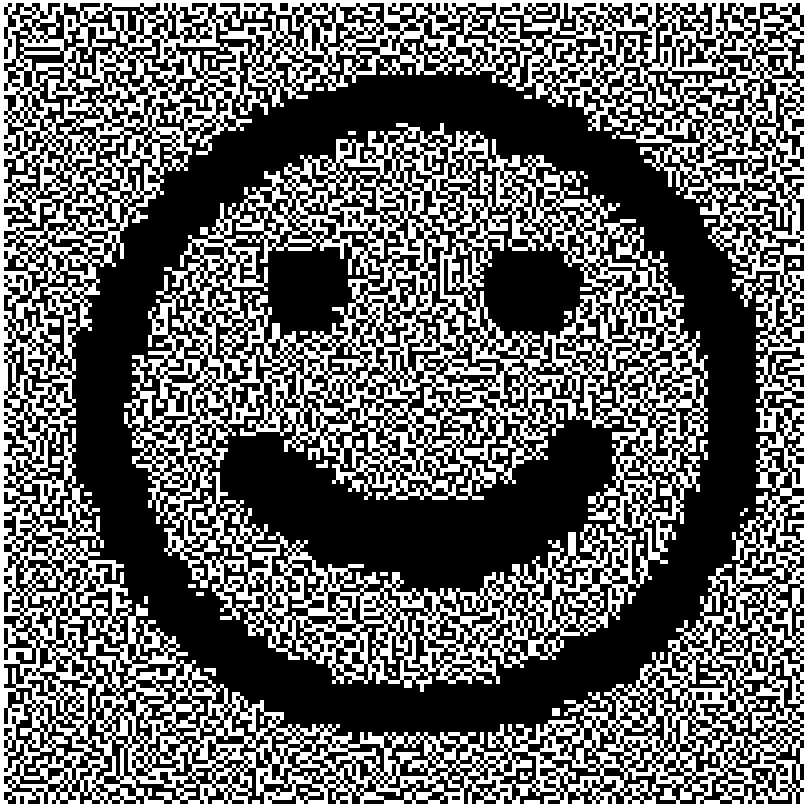
dekripsi



Share 1

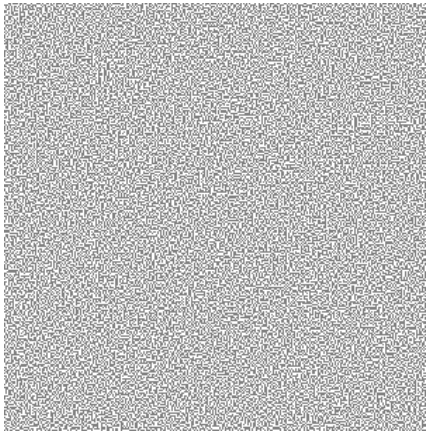
Share 2

Hasil dekripsi:

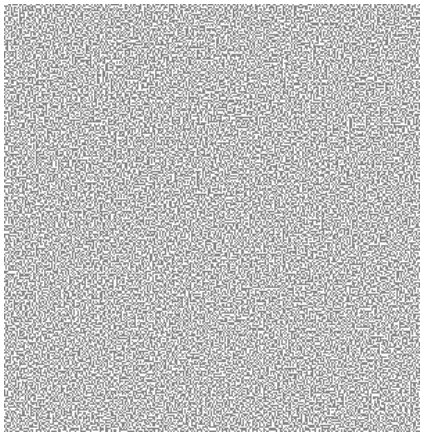


# Contoh lain:

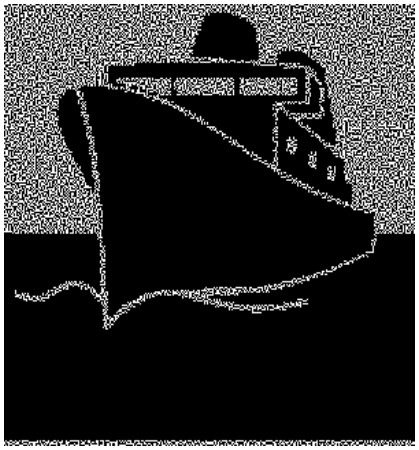
Plain-image



Share 1



Share 2



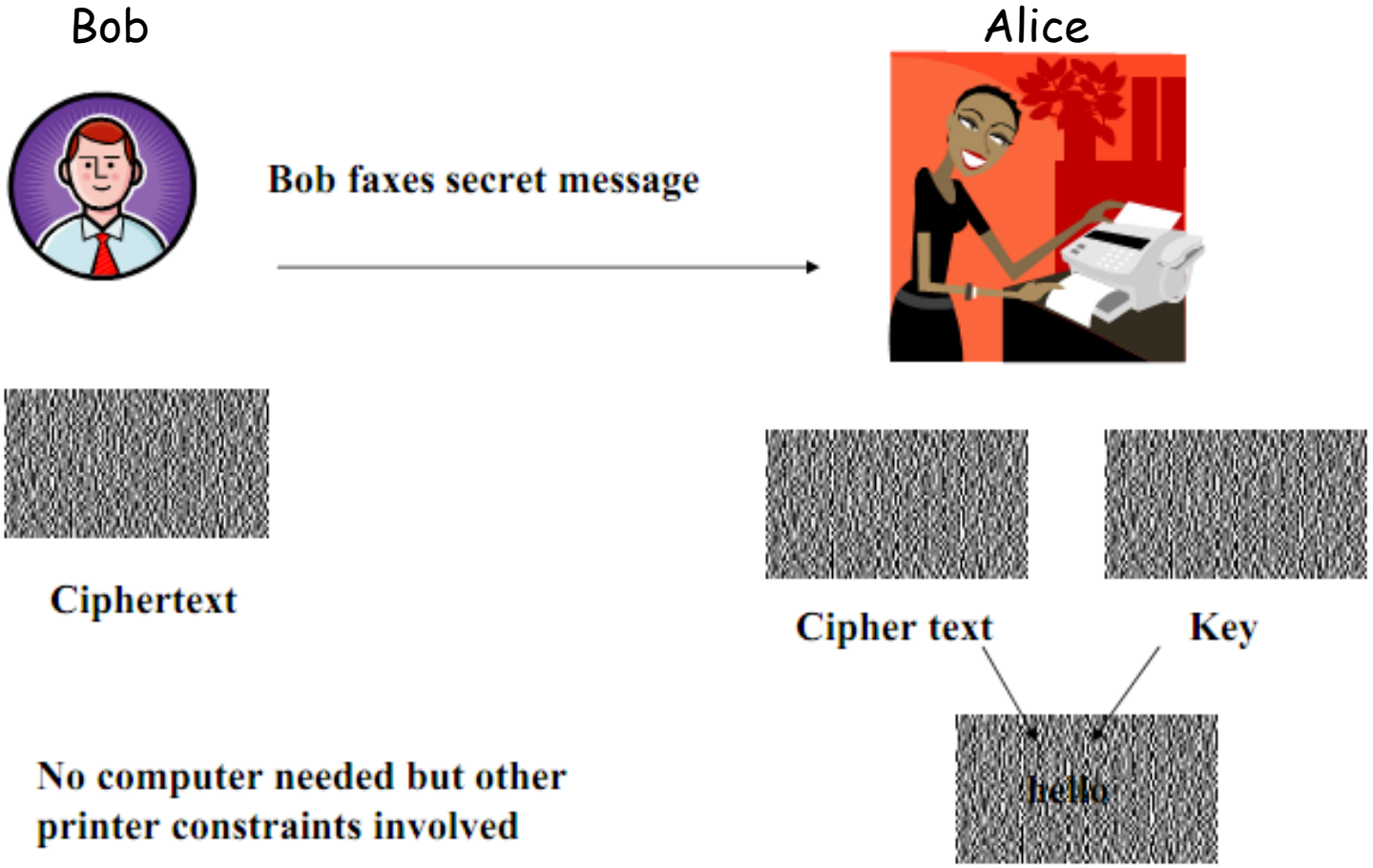
Share 1 + Share 2

- Untuk keamanan, maka dalam kriptografi visual, pembagian gambar menjadi sejumlah *share* dilakukan oleh pihak ketiga yang terpercaya, yang disebut ***dealer.***

- Sedangkan pihak yang menerima *share* diamakan ***partisipant***.

- Dekripsi dilakukan oleh *partisipant* dengan menumpuk *share* yang mereka miliki (misalnya setiap *share* dicetak pada plastik transparan)

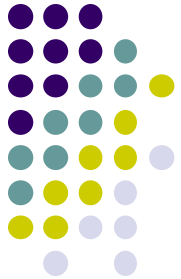
- Skenario penggunaan






Sumber: *www.cs.jhu.edu/~fabian/.../**VisualCrypto**.pdf*

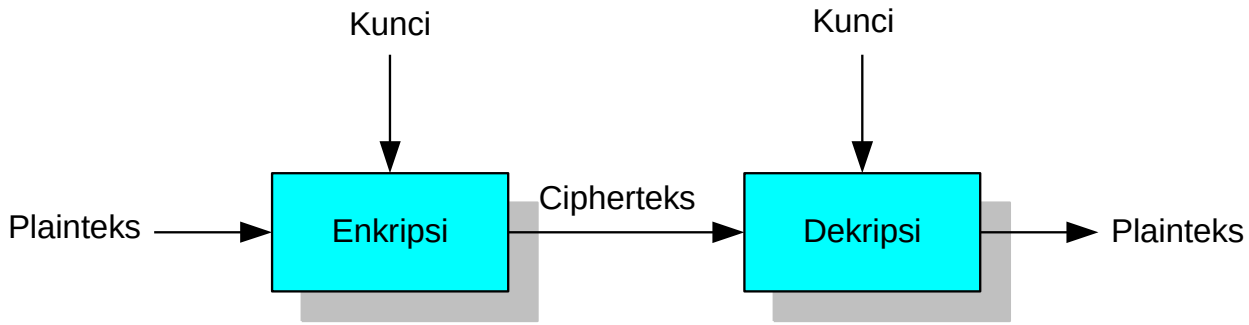
# Kriptografi *versus* Kriptografi Visual



- Kriptografi
  - Kriptografi tradisional
  - Simetri: DES, AES, RC4, Blowfish, dll
  - Nir-simetri: RSA, ElGamal, ECC, dll
    - Proses enkripsi dan dekripsi membutuhkan komputasi yang tinggi
    - Memerlukan kunci untuk enkripsi dan dekripsi

- Kriptografi Visual
  - Komputasi rendah
  - Dekripsi dilakukan tanpa komputasi, *fast decoding*
  - Tidak membutuhkan kunci untuk enkripsi dan dekripsi

- Kriptografi Tradisionil



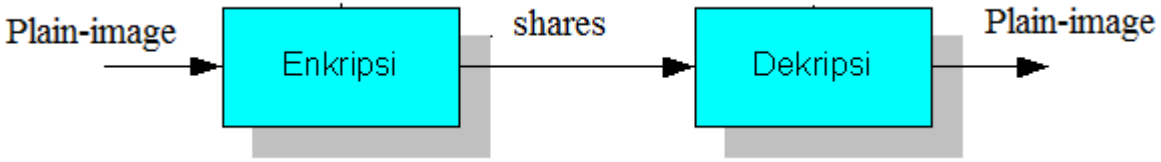

```
Ketika saya berjalan-jalan di
pantai, saya menemukan banyak
sekali kepiting yang merangkak
menuju laut. Mereka adalah
anak-anak kepiting yang baru
menetas dari dalam pasir.
Naluri mereka mengatakan bahwa
laut adalah tempat kehidupan
mereka.
```

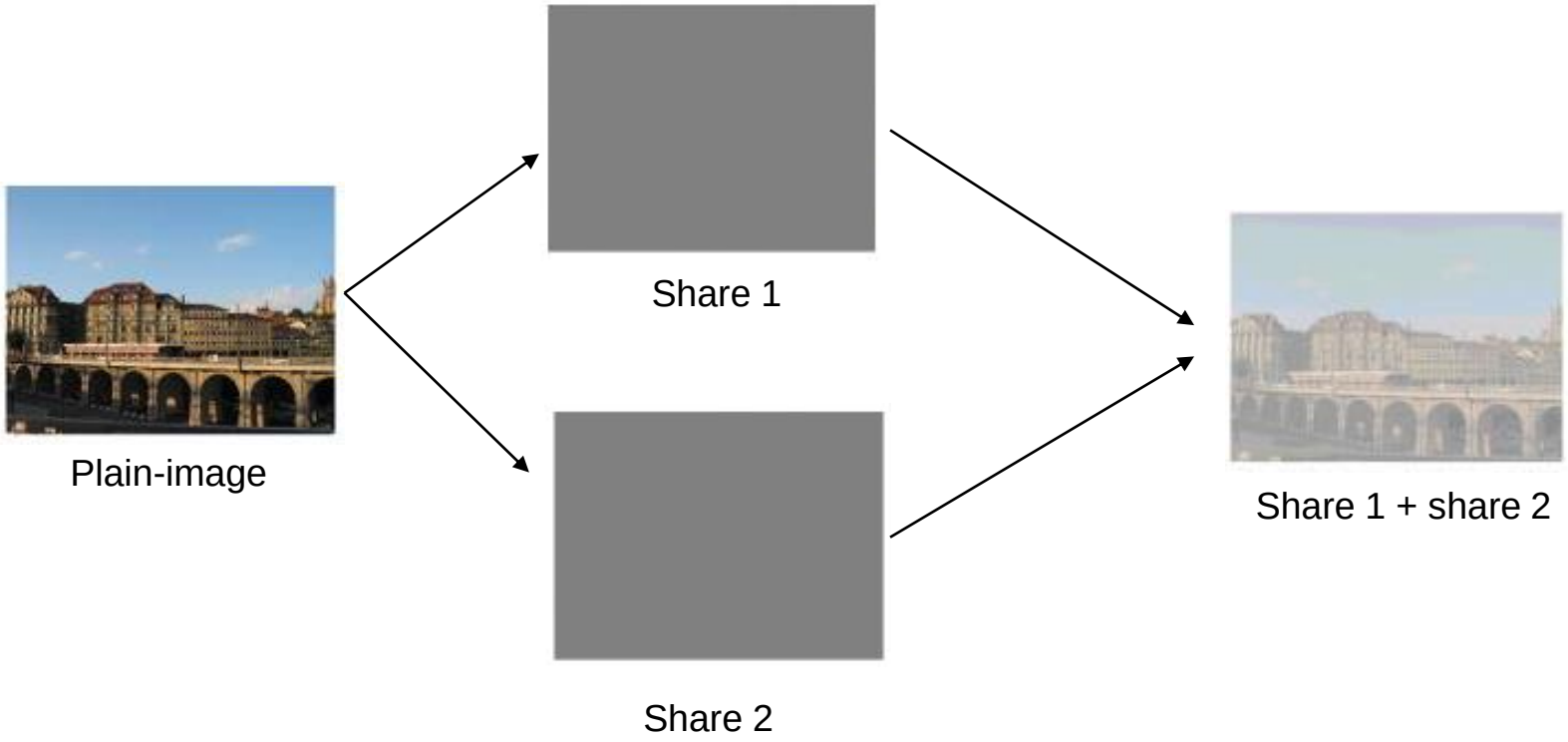
(a) Plainteks (teks)

```
Ztãxzp/épëp/qtüyp{p}<yp{p}/sx/□p}
âpx;pêp/|t}t|äzp}/qp}êpz/étzp{x/z
t□xâx}v□□êp}v/|tüp}vzpz/|t}äyä/{p
ääâ=/\tützp□□psp{pw/p}pz<p}pz/zt□x
âx}v/êp}v/qpüä□□|t}tâpé/spüx/sp{p
|/□péxü=/]p{äüx□□|ttüzp/|t}vpâpzp
}/qpwãp/{päâ/psp{pw□□ât|□pâ/ztwxs
ä□p}/|tützp=
```

(b) Cipherteks dari (a)

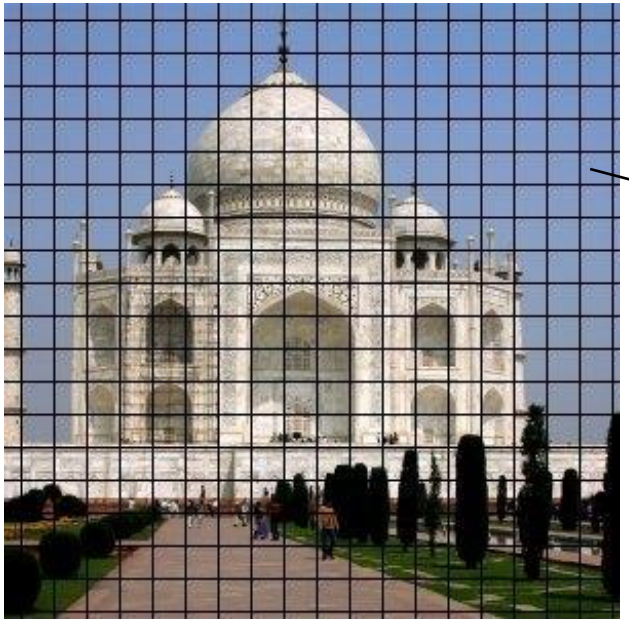
- Kriptografi Visual



# Konsep Citra Digital

- Citra terdiri dari sejumlah *pixel.* Citra 1200 x 1500 berarti memiliki 1200 x 1500 pixel = 1.800.000 pixel




- Setiap *pixel* panjangnya *n*-bit.

  Citra biner → 1 bit/pixel

  Citra *grayscale* → 8 bit/pixel

  Citra *true color* → 24 bit/pixel

# Citra Lenna

True color image
(24-bit)

Grayscale image
(8-bit)

Bimary image
(1-bit)

# Citra berwarna terdiri dari komponen *RGB* (*Red-Green-Blue*)

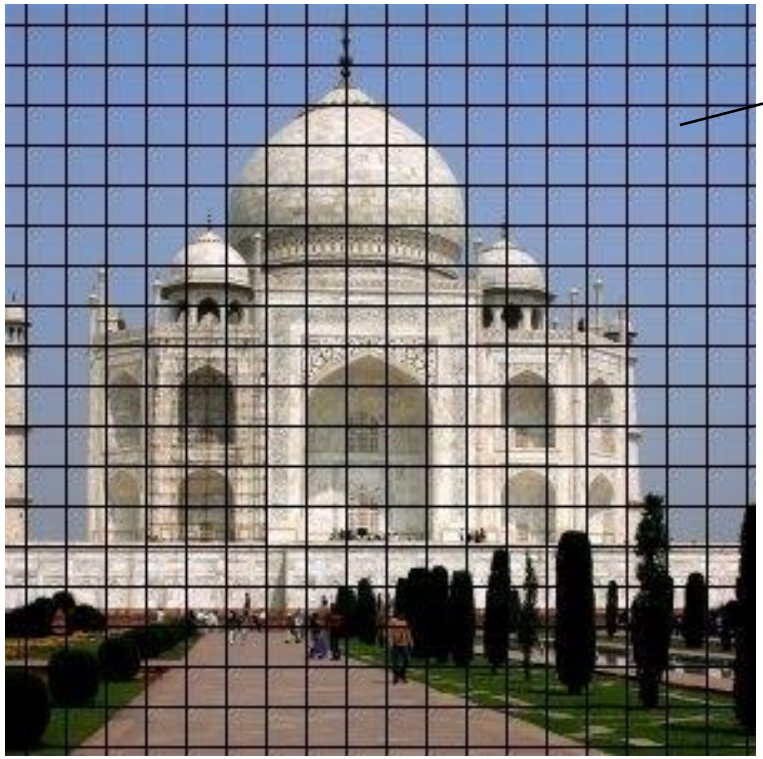
Original Image

Red

Green

Blue

Pada citra berwarna 24-bit (*real image*),
1 pixel = 24 bit,

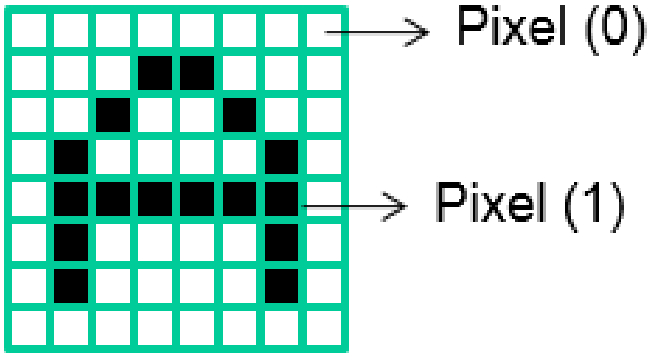


10010011100101001000101O

R G B

# Kriptografi Visual pada Citra Biner

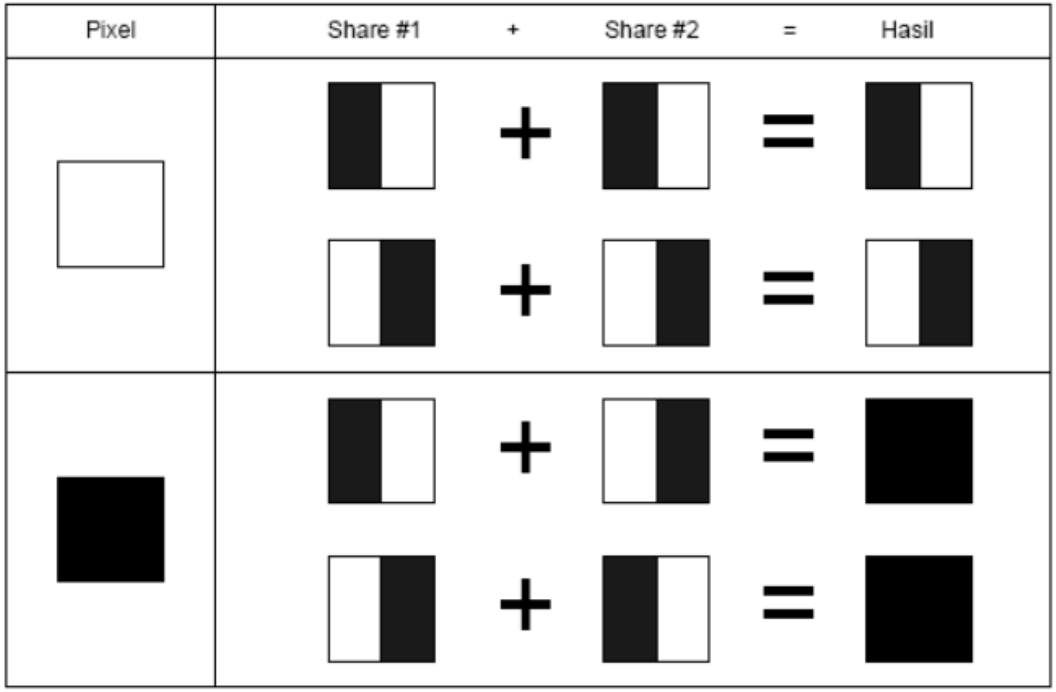
- Tinjau kriptografi visual untuk citra biner
- *Pixel* pada citra biner:
  - bernilai 1 jika hitam
  - bernilai 0 jika putih




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

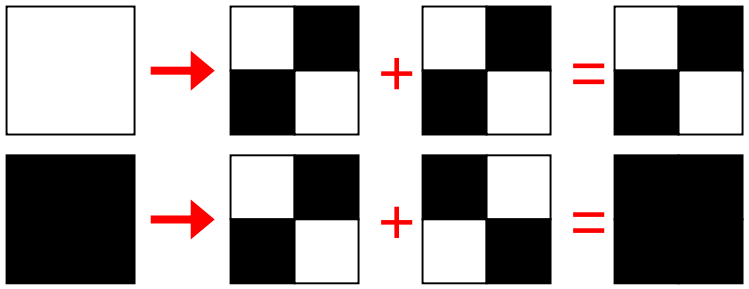
# Bagaimana cara kerja kriptografi visual?

- Setiap *pixel* dibagi menjadi sejumlah *sub-pixel.*
- Setiap *pixel* muncul pada setiap *share*
- Jika *sub-pixel* dari setiap *share* ditumpuk, hasilnya *pixel* yang dipersepsi sebagai “putih” atau “hitam”.

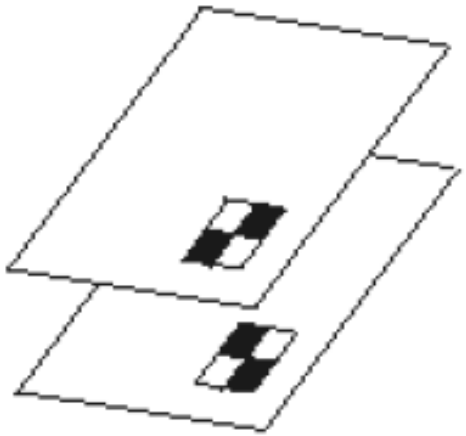


- Skema lainnya, satu *pixel* dibagi menjadi 4 buah *sub-pixel*


- Penumpukan:



- Satu *share* direpresentasikan sebagai satu transparansi.
- Jika dua buah *share* ditumpuk, maka mata manusia mempersepsi *pixel* yang terbentuk sebagai “hitam” atau “putih”
- Apa warna yang dipersepsi dari penumpukan di bawah ini?



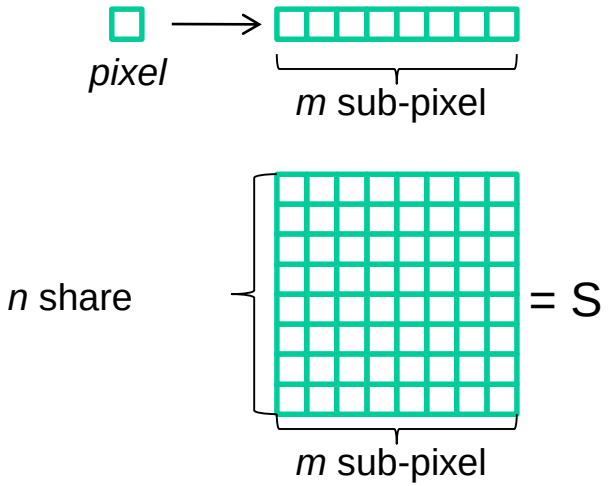
- Alternatif penumpukan lainnya:

| Secret pixel color / Share blocks | White | | | | | | Black | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2×2 block of the first share |  |  |  |  |  |  |  |  |  |  |  |  |
| 2×2 block of the second share |  |  |  |  |  |  |  |  |  |  |  |  |
| Stacked 2×2 block |  |  |  |  |  |  |  |  |  |  |  |  |

- *Pixel* hitam akan tampak hitam sempurna pada persepsi citra hasil penumpukan, sedangkan *pixel* putih akan terlihat mengandung *noise*, namun mata manusia masih dapat mempersepsi gambar semula.

# Kriptografi Visual untuk Citra Biner

- Tiap *pixel* muncul pada *n* buah *share*
- Tiap *share* terdiri dari *m* buah *sub-pixel* berwarna hitam dan putih.
- Dideskripsikan sebagai matriks *S* berukuran $n \times m$



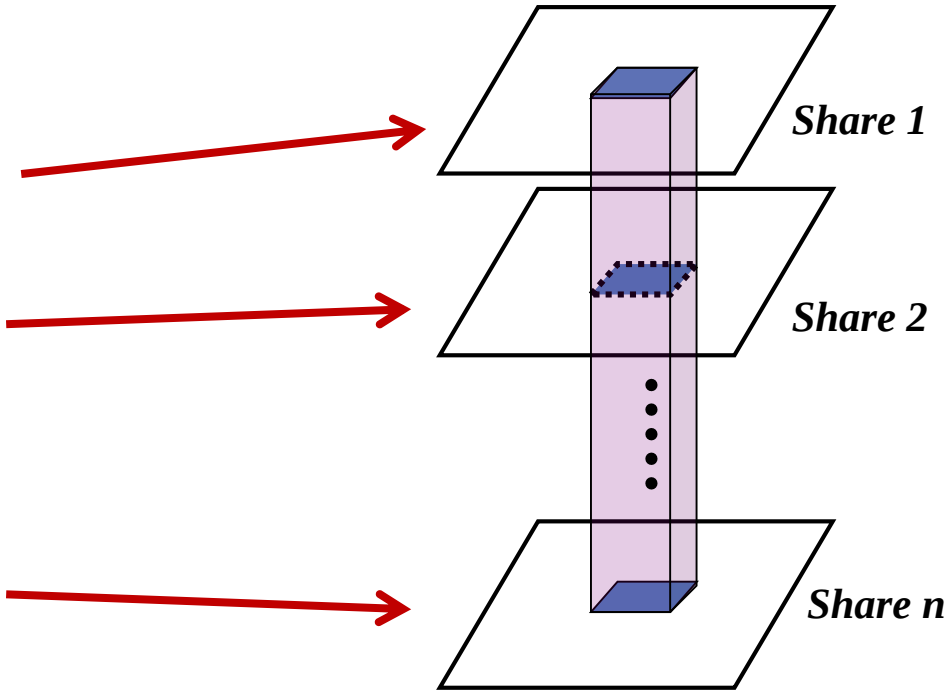

Contoh: $n = 2$, $m = 4$

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

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

- *S*[*i*,*j*] = 1 jika *sub-pixel* ke-*j* pada share ke-*i* berwarna hitam
- *S*[*i*,*j*] = 0 jika *sub-pixel* ke-*j* pada share ke-*i* bnerwarna putih

$$\begin{bmatrix} s_{11} & s_{12} & \cdots & s_{1m} \\ s_{21} & s_{22} & \cdots & s_{2m} \\ \vdots & \vdots & & \vdots \\ s_{n1} & s_{n2} & \cdots & s_{nm} \end{bmatrix}$$



- Penumpukan dua atau lebih *share* dapat dipandang sebagai operasi “OR”

$$\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

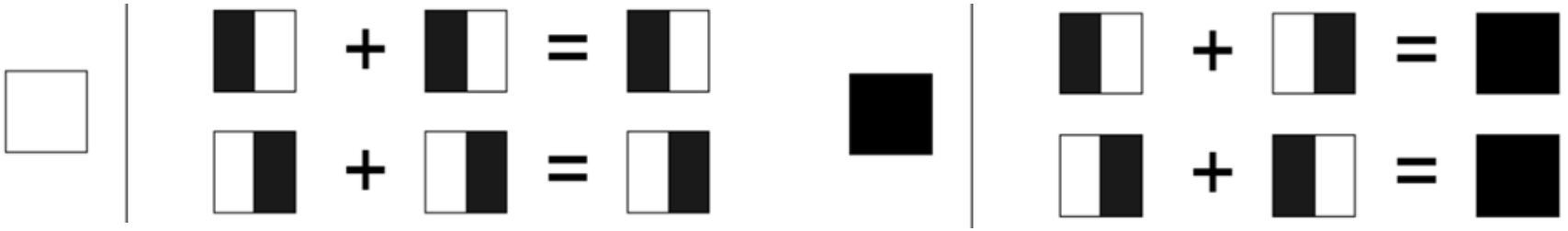
- **Bobot Hamming** ($H(V)$): Jumlah simbol tidak-nol dalam sebuah vektor dengan $m$-elemen.
- Level abu-abu hasil penumpukan *share* sebanding $H(V)$:

  - Dianggap hitam jika $H(V) \geq d$
  - Dianggap putih jika $H(V) < d - \alpha m$

    $d$ adalah *threshold,* $1 \leq d \leq m$

    $\alpha$ adalah level kontras, $\alpha > 0$

- Level kontras $\alpha$ dihitung dari persentase *sub-pixel* berwarna hitam dari *share*.
- Contoh: $\alpha = 0.5$

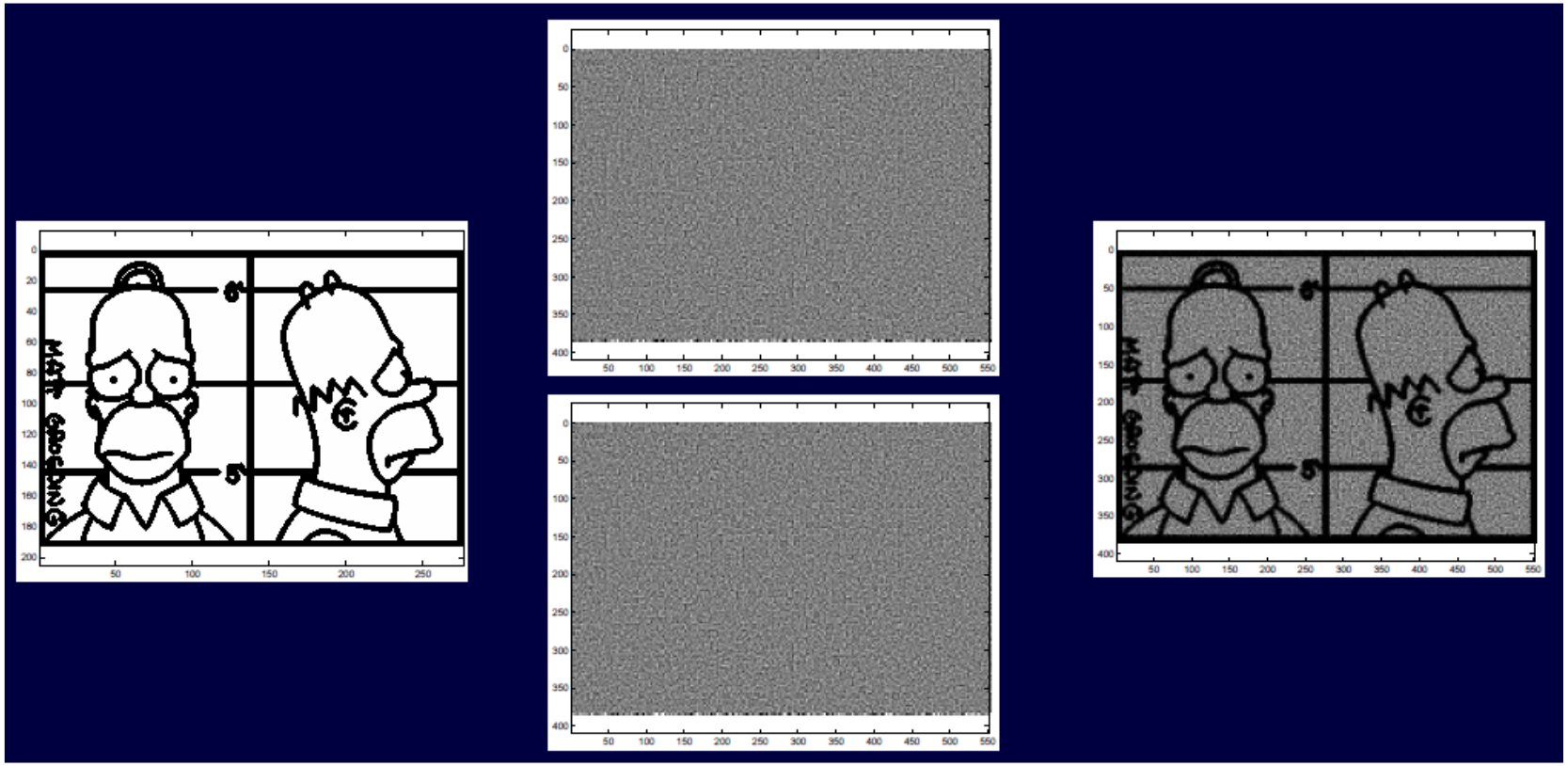


- Pada waktu dekripsi:

  - *pixel* putih dihasilkan dari *subpixel* putih dan *subpixel* hitam
  - *pixel* hitam dihasikan dari dua *subpixel* hitam tanpa *subpixel* putih

  Perbedaan tersebut menghasilkan kontras yang berbeda sehingga pandangan mata manusia menganggap setengah putih sebagai putih dan hitam sebagai hitam.

- Dalam implementasinya, membagi 1 *pixel* menjadi 2 *sub-pixel* dilakukan dengan meng-*extend* 1 *pixel* menjadi 2 *pixel*.
- Akibatnya, ukuran *share* menjadi dua kali ukuran gambar semula



# Solusi Kriptografi Visual

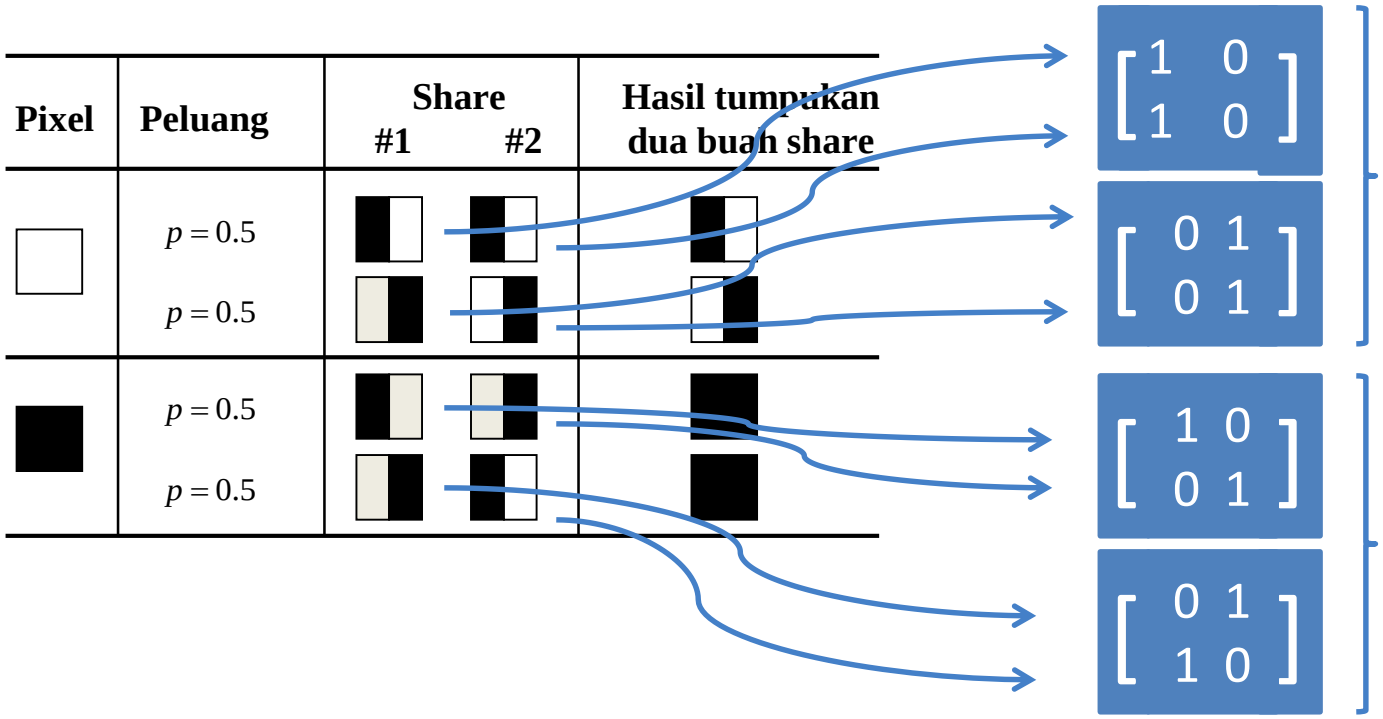
- Didefinisikan dua buah matriks $C_0$ dan $C_1$
- $C_0$ = semua matriks *S* yang merepresentasikan *pixel* putih
  = semua matriks hasil permutasi kolom dari 1 matriks

$$C_0 = \{\begin{bmatrix} & \end{bmatrix}, \begin{bmatrix} & \end{bmatrix}, \ldots, \begin{bmatrix} & \end{bmatrix}\}$$

- $C_1$ = semua matriks S yang merepresentasikan *pixel* hitam
  = semua matriks hasil permutasi kolom dari 1 matriks

$$C_1 = \{\begin{bmatrix} & \end{bmatrix}, \begin{bmatrix} & \end{bmatrix}, \ldots, \begin{bmatrix} & \end{bmatrix}\}$$

# Contoh:




$$C_0 = \left\{ \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \right\} \qquad C_1 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}$$

# Skema (2, 2)

- Satu gambar dibagi menjadi dua buah *share*
- Untuk mendekripsi, diperlukan dua buah *share*
- Algoritma enkripsi (membagi gambar menjadi dua *share*):

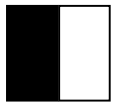
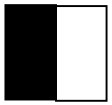
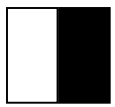
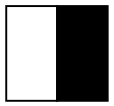
1. Ambil sebuah *pixel* dari gambar (*plain-image*), missal pixel *P*
2. Jika *P* berwarna putih, ambil secara acak sebuah matriks S pada $C_0$
   Jika P berwarna hitam, ambil secara acak sebuah matriks *S* pada $C_1$
3. Misalkan P berwarna hitam dan matriks yang diambil dari $C_1$ adalah sebagai berikut: $S = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
   maka *share* 1 adalah baris 1 dari *S* dan *share* 2 adalah baris 2 dari *S*



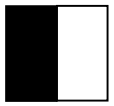
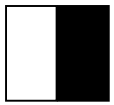
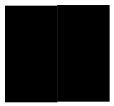
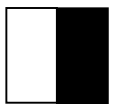
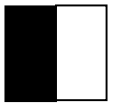

4. Ulangi langkah 2 dan 3 untuk *pixel-pixe*l lainnya

# Contoh:

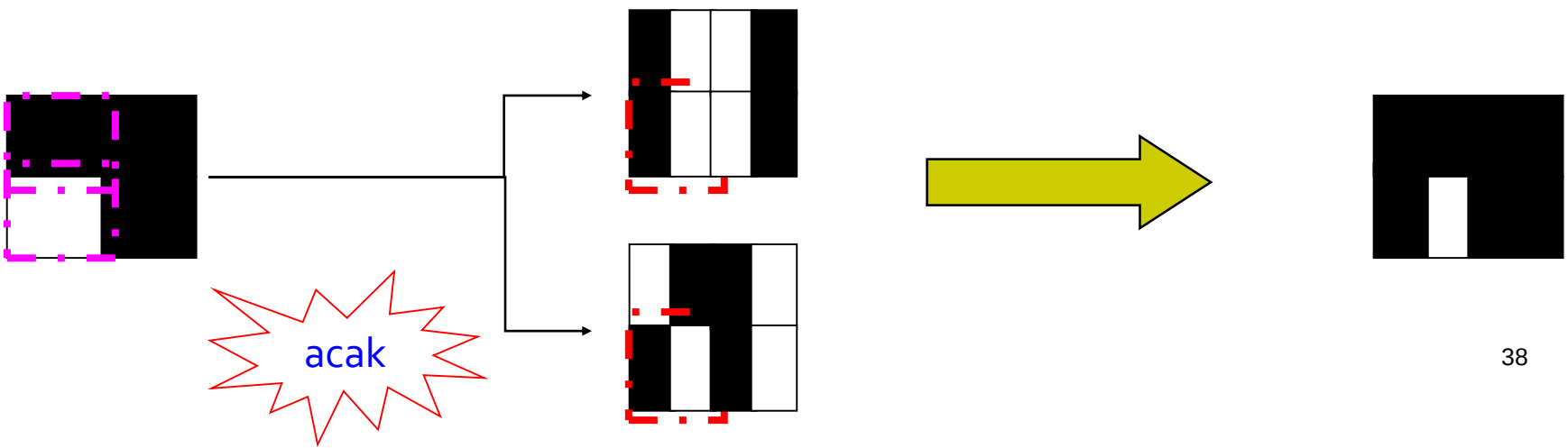
pixel

| | Share 1 | | Share2 | | Tumpukan |
|---|---|---|---|---|---|
| Alternatif 1 |  | + |  | = |  |
| Alternatif 2 |  | + |  | = |  |

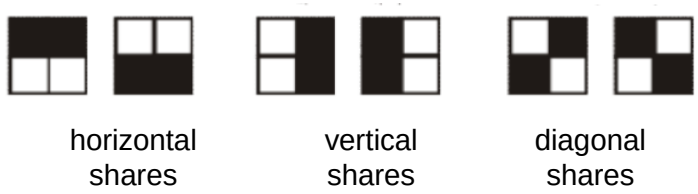
$$C_0 = \left\{ \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \right\}$$

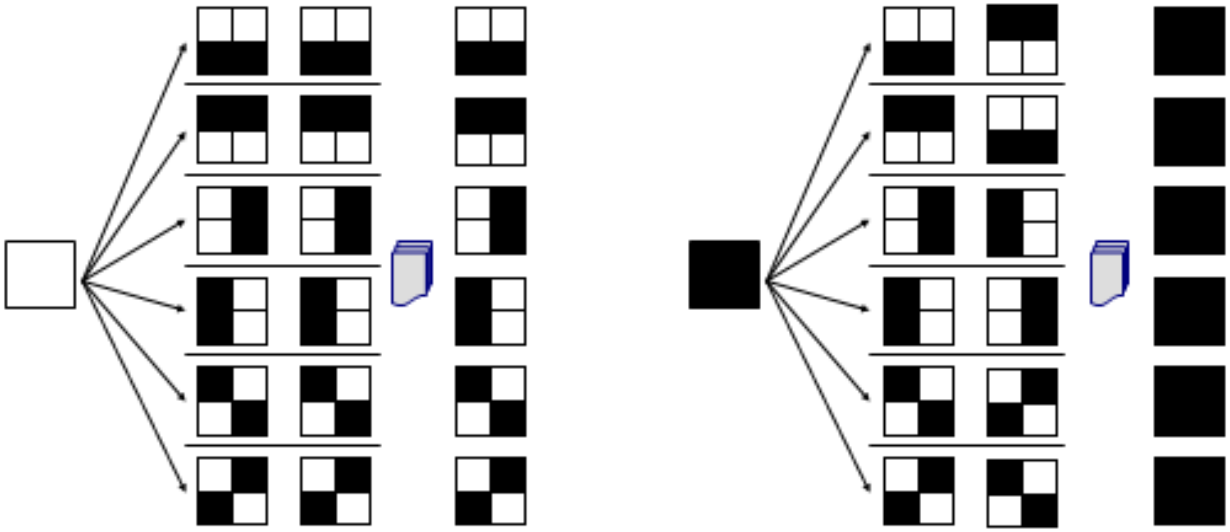
| | Share 1 | | Share2 | | Tumpukan |
|---|---|---|---|---|---|
| |  | + |  | = |  |
| |  | + |  | = |  |

$$C_1 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}$$



- Contoh skema (2, 2) lainnya:



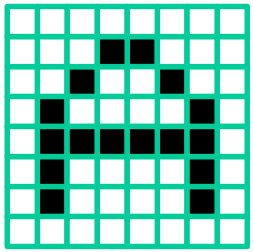
$$C_0 = \{\begin{bmatrix}0&0&1&1\\0&0&1&1\end{bmatrix},\begin{bmatrix}1&1&0&0\\1&1&0&0\end{bmatrix},\begin{bmatrix}1&0&1&0\\1&0&1&0\end{bmatrix},\begin{bmatrix}0&1&0&1\\0&1&0&1\end{bmatrix},\begin{bmatrix}1&0&0&1\\1&0&0&1\end{bmatrix},\begin{bmatrix}0&1&1&0\\0&1&1&0\end{bmatrix}\}$$

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

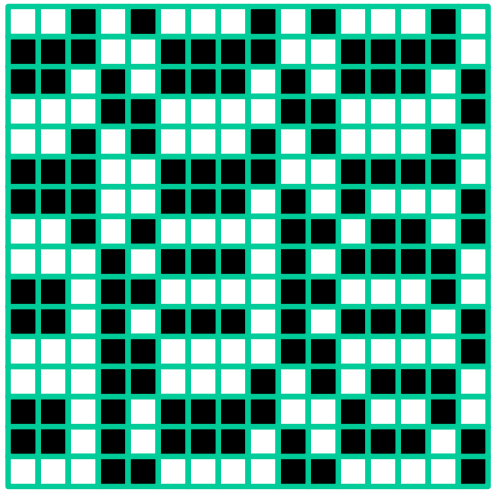
horizontal shares

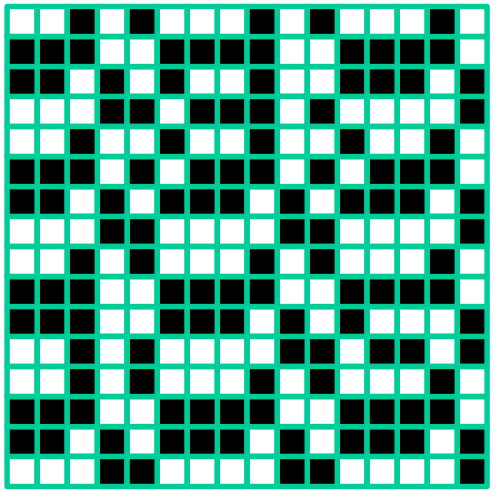
vertical shares

diagonal shares



Secret Image





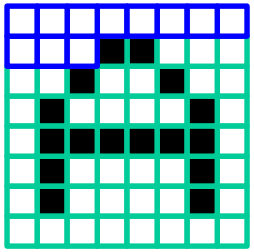
horizontal shares

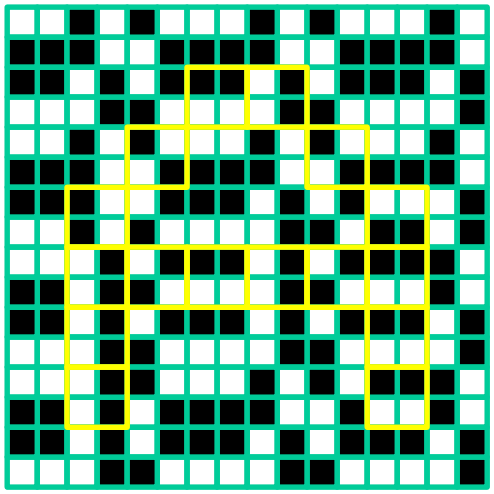


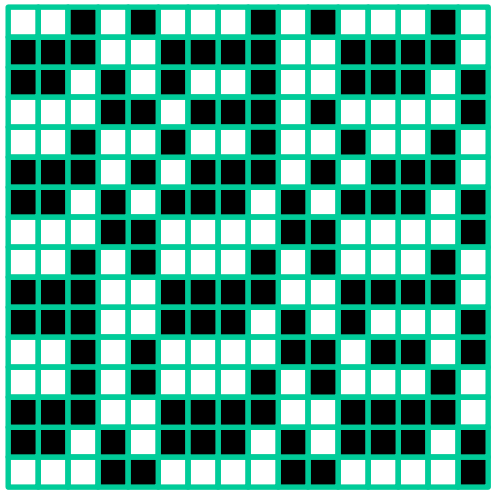
vertical shares



diagonal shares



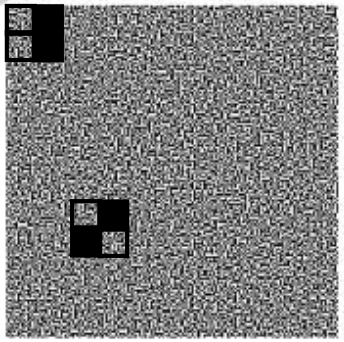




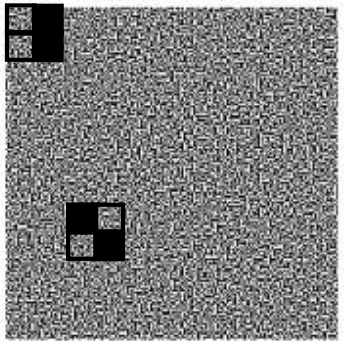
# Contoh lainnya:

| Secret pixel color / Share blocks | White | | | | | | Black | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2×2 block of the first share | ■□ | □■ | ■■ | □■ | ■□ | □■ | ■□ | ■□ | □■ | □■ | □■ | □■ |
| 2×2 block of the second share | ■□ | □■ | ■■ | □■ | ■□ | □■ | ■□ | □■ | □■ | □■ | □■ | □■ |
| Stacked 2×2 block | ■□ | □■ | ■■ | □■ | ■□ | □■ | ■■ | ■■ | ■■ | ■■ | ■■ | ■■ |

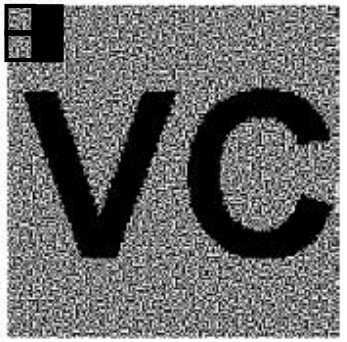

(a) Original secret image



(b) First share image

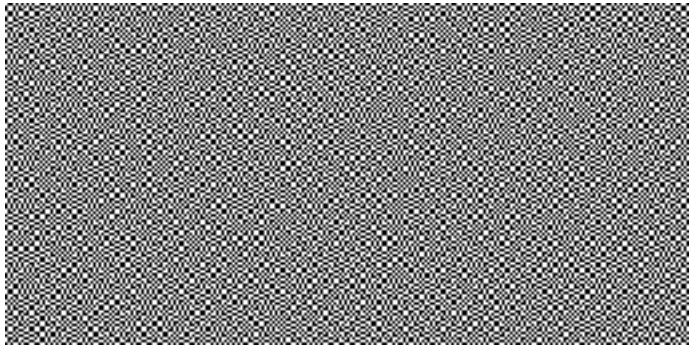


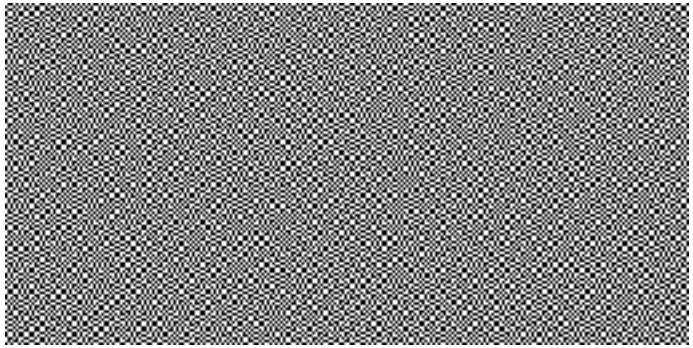
(c) Second share image

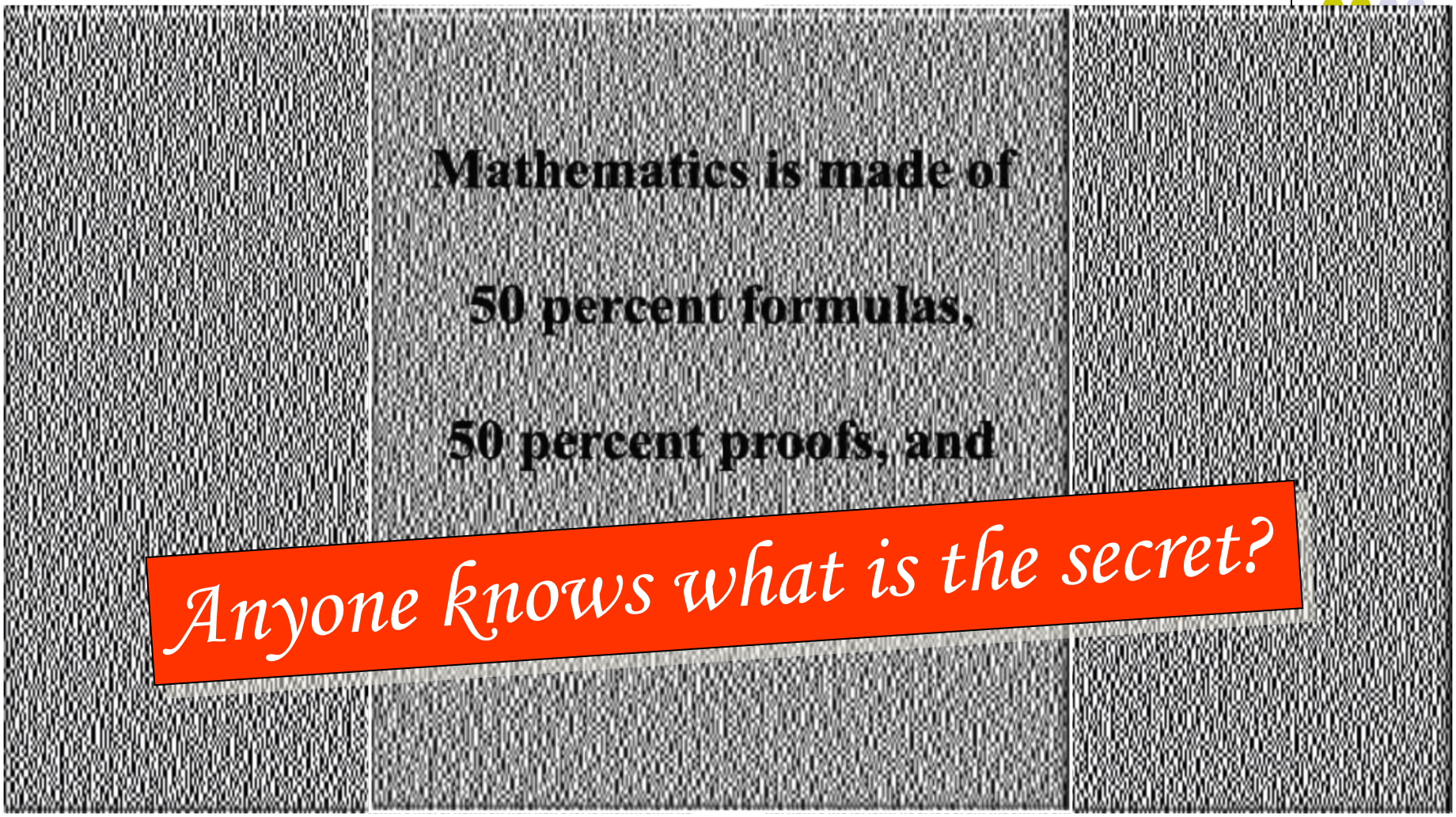



(d) Stacked result of (a) and (b)

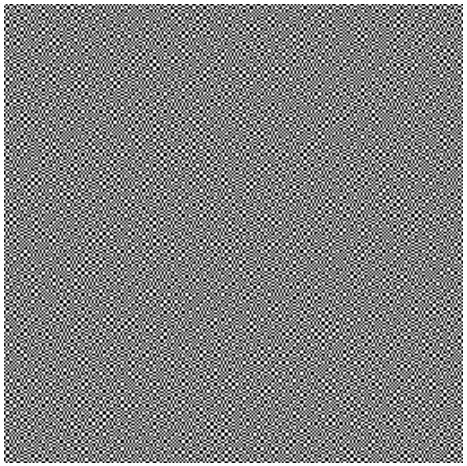
- Contoh-contoh kriptografi visual sederhana



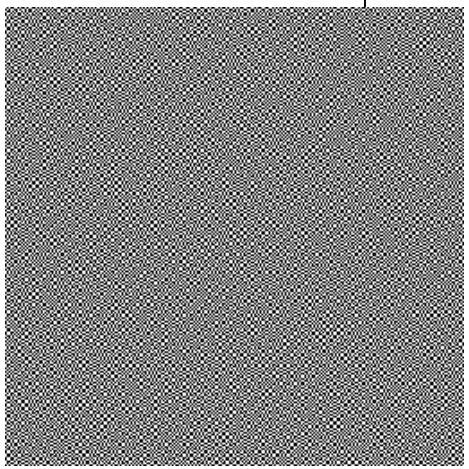



Mathematics is made of
50 percent formulas,
50 percent proofs, and
Anyone knows what is the secret?

**Original**



***Share* 1**



***Share* 2**

**Hasil penumpukan *share* 1 dan *share* 2**

# Skema (2, *n*)

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

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

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

# Skema (3, 3)

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

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

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

# Skema (3, *n*)

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

  *B* = matriks *n* x 1 yang bernilai 1 seluruhnya

  *I* = matriks identitas *n* x *n* (diagonal utama = 1)

  *BI* = matriks hasil penggabungan *B* dan *I*

  *c*(*BI*) = matriks komplemen dari *BI*

- Maka,

  $C_0$ = {seluruh matriks hasil permutasi kolom dari *c*(*BI*) }

  $C_1$ = {selurh matriks hasil permutasi kolom daro *BI* }

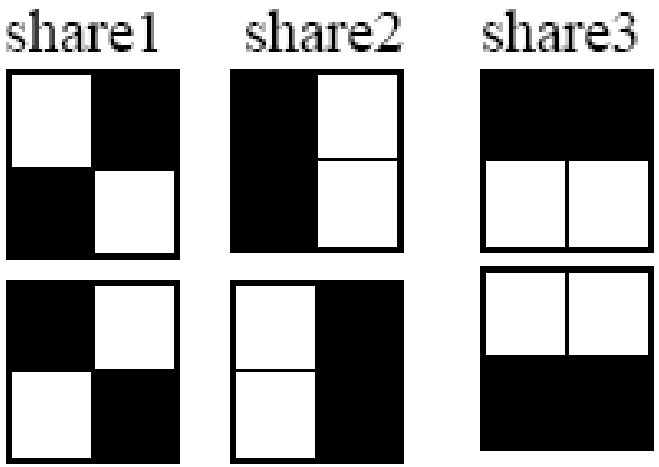
# Contoh: $n = 3$ → Skema (3, 3)

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

Misalkan [permutasinya adalah {2, 3, 4, 1 }

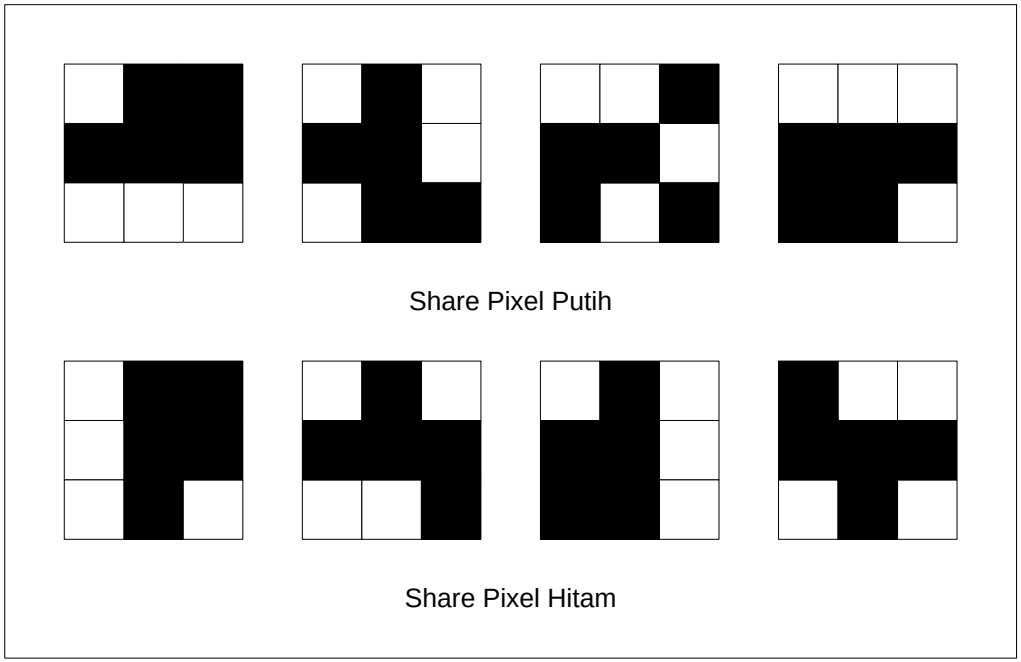
Shares

- White Pixel
- Black Pixel



# Skma(4, 4)

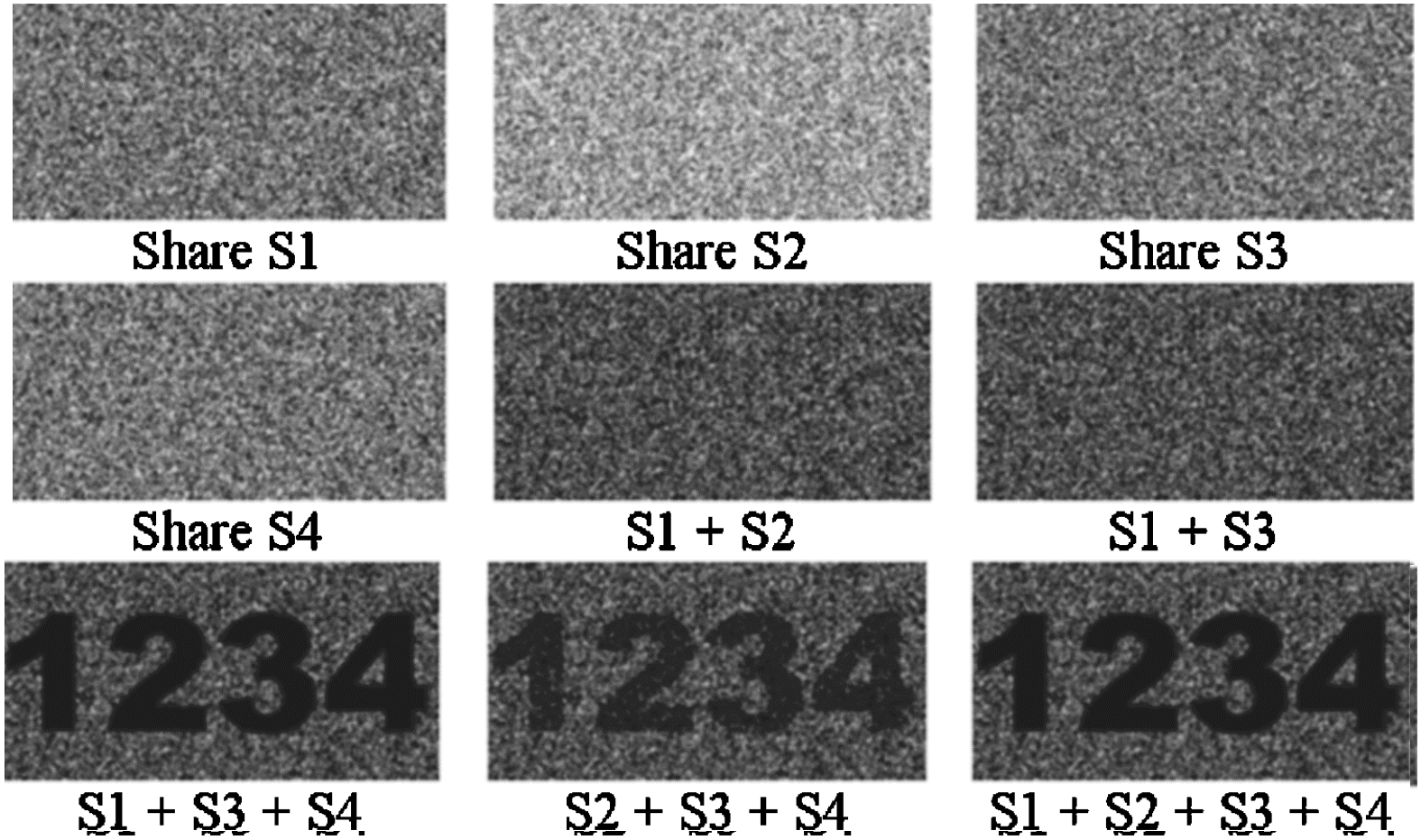
- Satu gambar dibagi menjadi 4 buah *share*
- Untuk mendekripsi, diperlukan 4 buah *share*



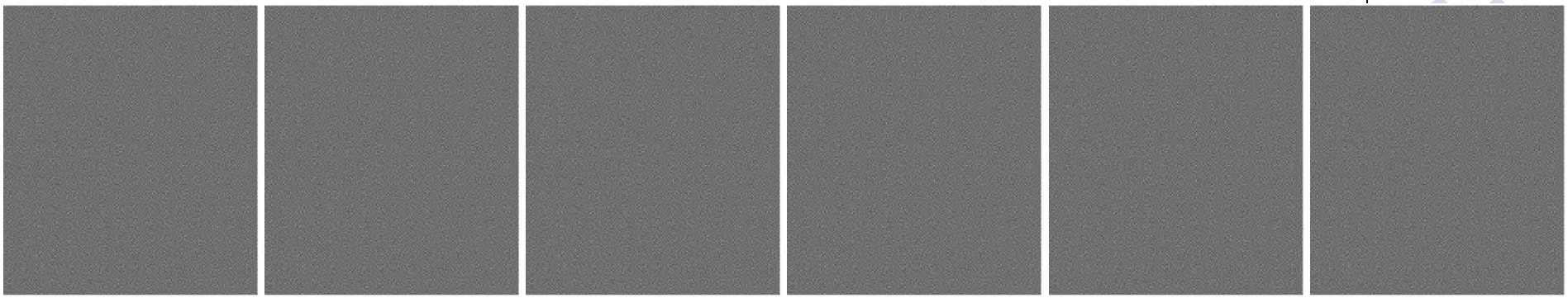
# Skema (*k*, *n*)

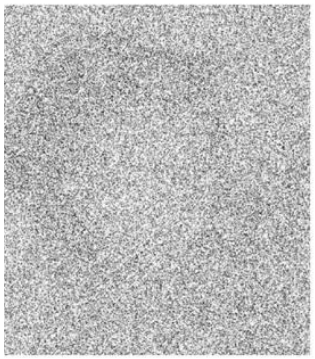
- Satu gambar dibagi menjadi *n* buah *share*
- Untuk mendekripsi gambar, diperlukan paling sedikit *k* buah *share*
- Jika jumlah *share* yang diumpuk kurang dari *k*, maka tidak dapat menghasilkan gambar semula

# Contoh: skema (3, 4)



# Hasil bermacam-macam Skema (*k*, 6)





(2, 6)

(3, 6)

(4, 6)

(5, 6)

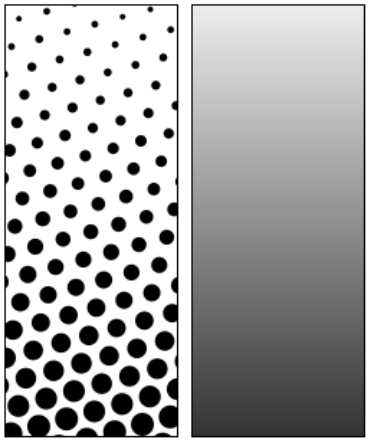
(6, 6)

- Solusi kriptografi visual skema ($k$, $n$) dinyatakan valid jika memenuhi 3 syarat berikut:
  1. Untuk sembarang matriks $S$ pada $C_0$, bobot Hamming untuk sejumlah $k$ dari $n$ baris memenuhi $H(V) \leq d - \alpha m$.
  2. Untuk sembarang matriks $S$ pada $C_1$, bobot Hamming untuk sejumlah $k$ dari $n$ baris memenuhi $H(V) \geq d$.
  3. Untuk sembarang *subset* $\{i_1, i_2, ..., i_q\}$ dari $\{1, 2, ..., n\}$, $q < k$, dua buah kumpulan matriks berukuran $q \times m$, yakni $D_0$ dan $D_1$, yang diperoleh dari hasil *restricting* masing-masing matriks berukuran $n \times m$ dari $C_0$ dan $C_1$ pada baris-baris $i_1, i_2, ..., i_q$ tidak dapat dibedakan satu sama lainnya karena memiliki matriks yang sama dengan frekuensi yang sama.

- Syarat ke-1 dan ke-2 menyatakan kontras, sedangkan syarat ke-3 menyatakan keamanan. Syarat 3 artinya dengan menumpuk *share* sejumlah kurang dari $k$ buah, citra semula tidak dapat didekripsi.

# Kriptografi Visual untuk Citra *Grayscale*

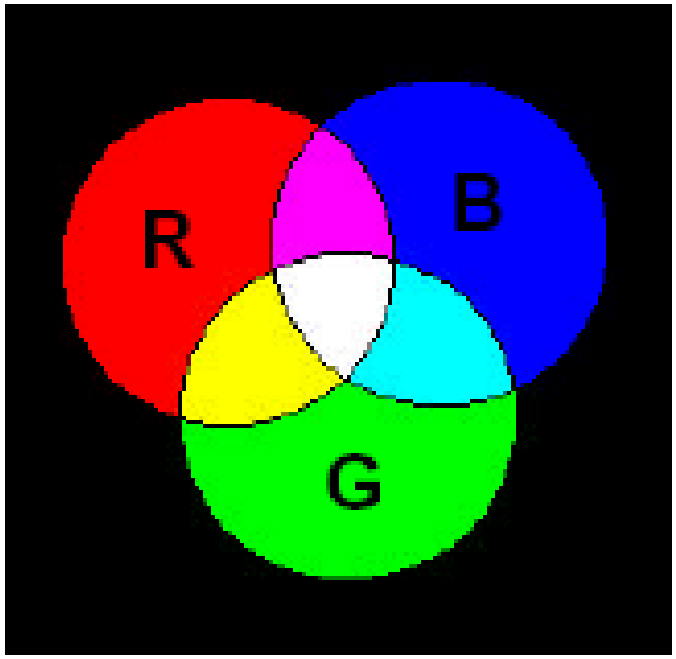
- Citra *grayscale* diubah terlih dahulu menjadi citra *halftone* (*halftone image*)
- *Halftone image:* teknik reproduksi citra yang mensimulasikan citra yang memiliki level keabuan yang kontinu dengan menggunakan titik-titik (*dot*) yang bervariasi ukuran dan jarak spasi antar titik.



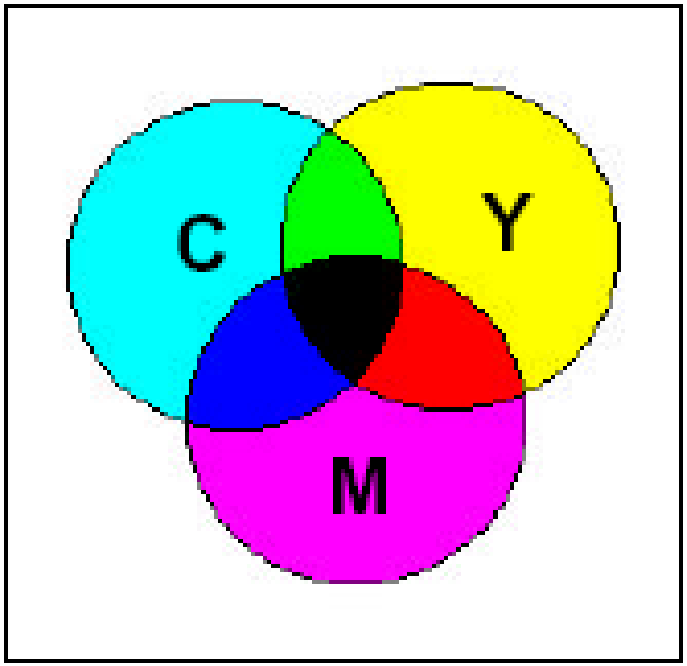
| Secret pixel color | White | Black |
|---|---|---|
| *Share blocks* | | |
| 2 × 2 block of the first share | | |
| 2 × 2 block of the second share | | |
| Stacked 2 × 2 block | | |

Share 1 Share 2

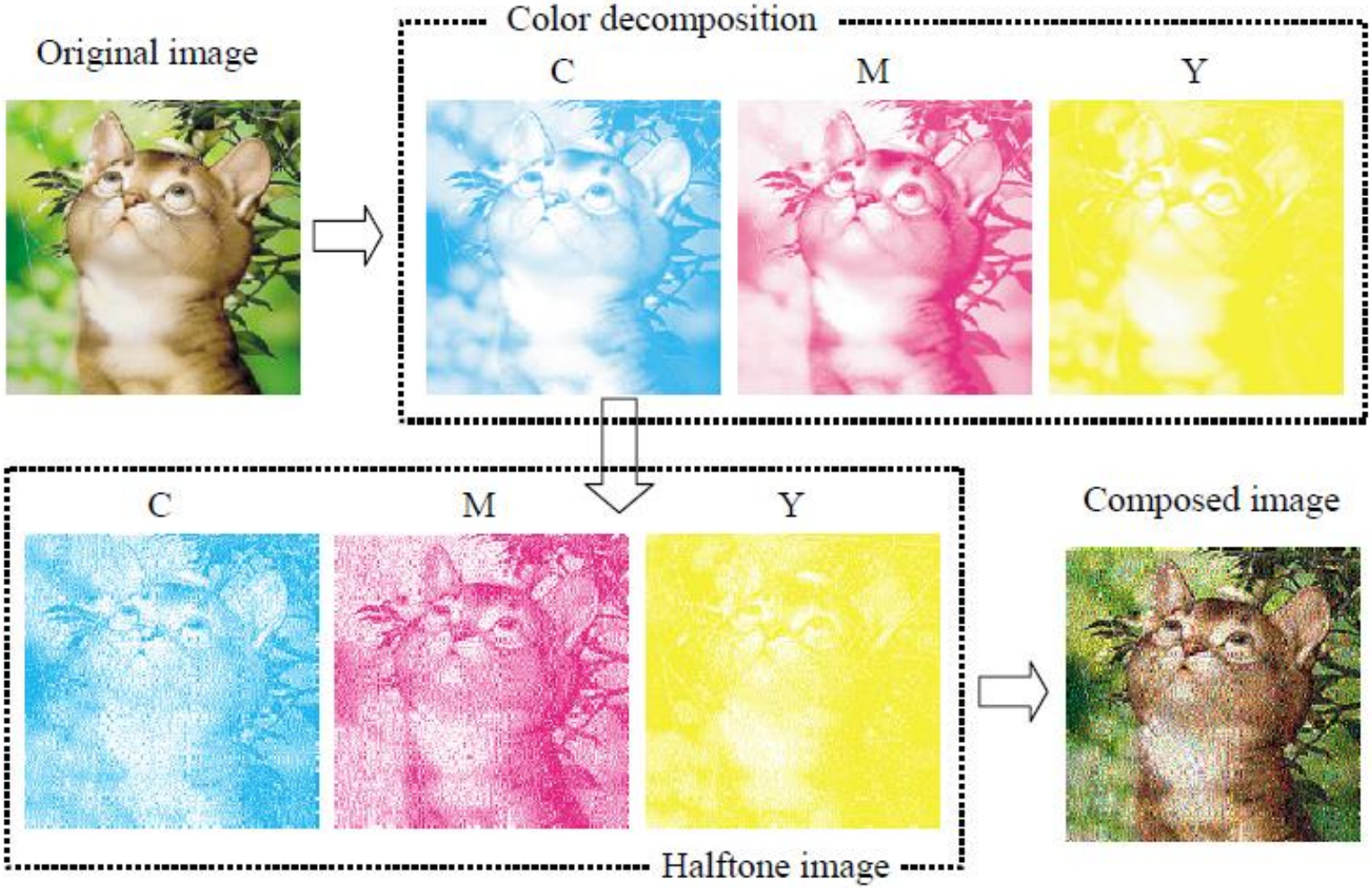
# Kriptografi visual untuk Citra Berwarna

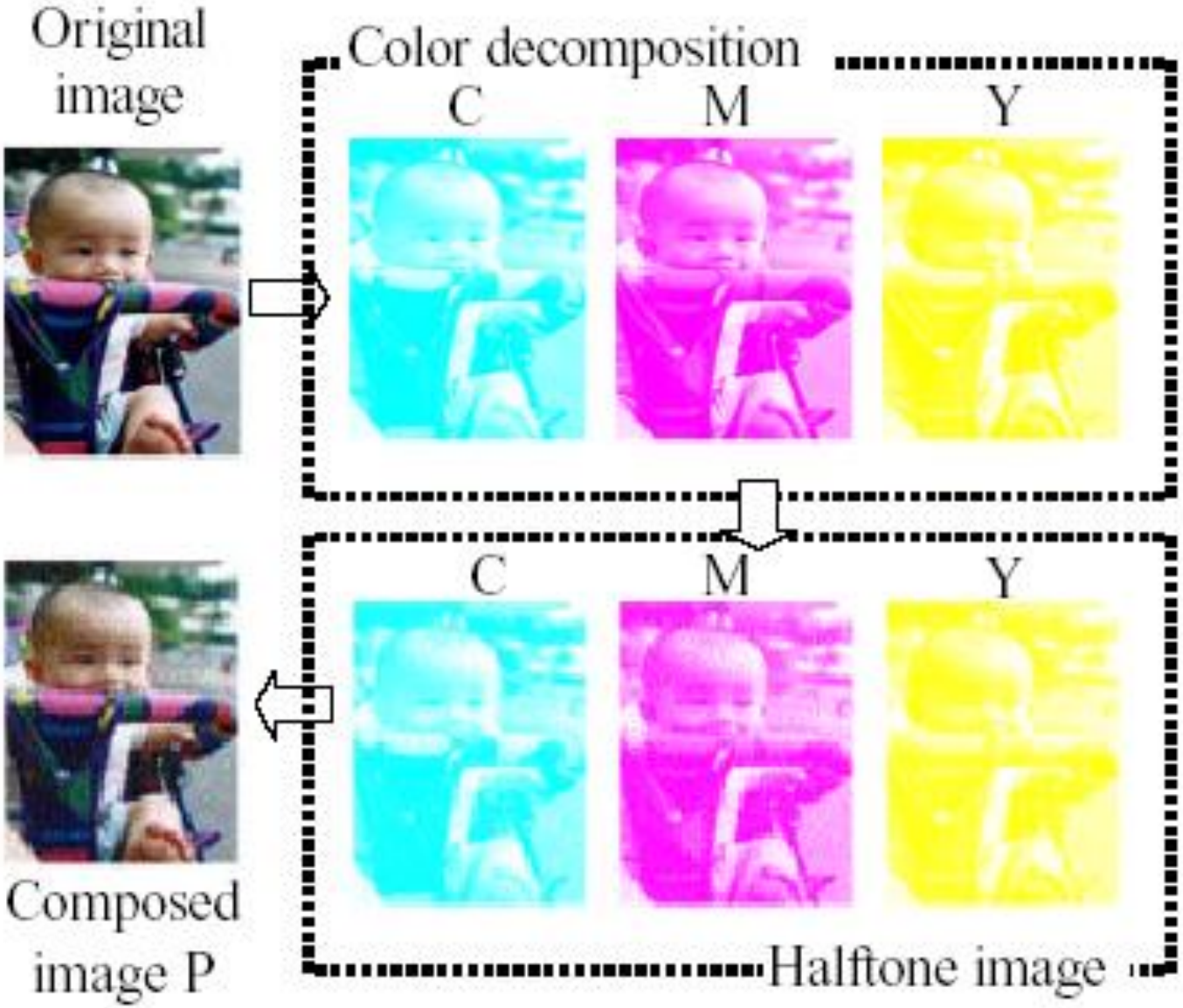


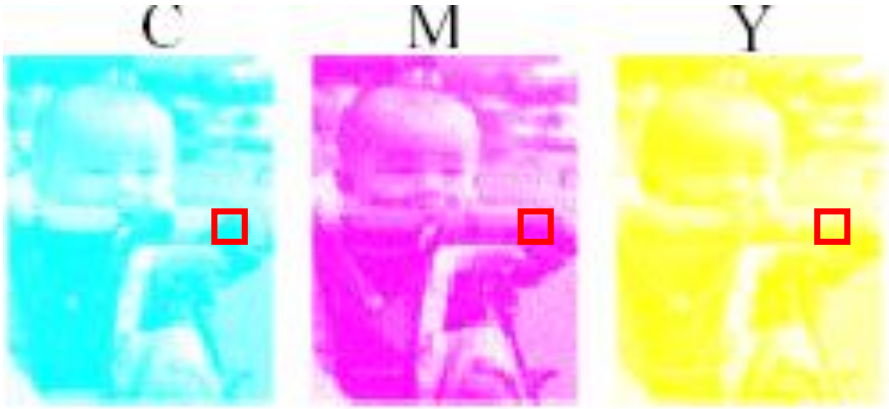

**RGB: TV dan monitor**

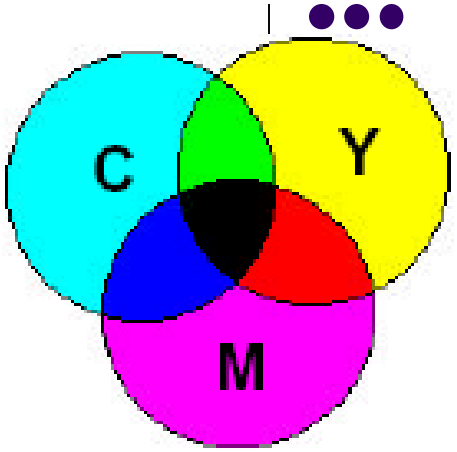


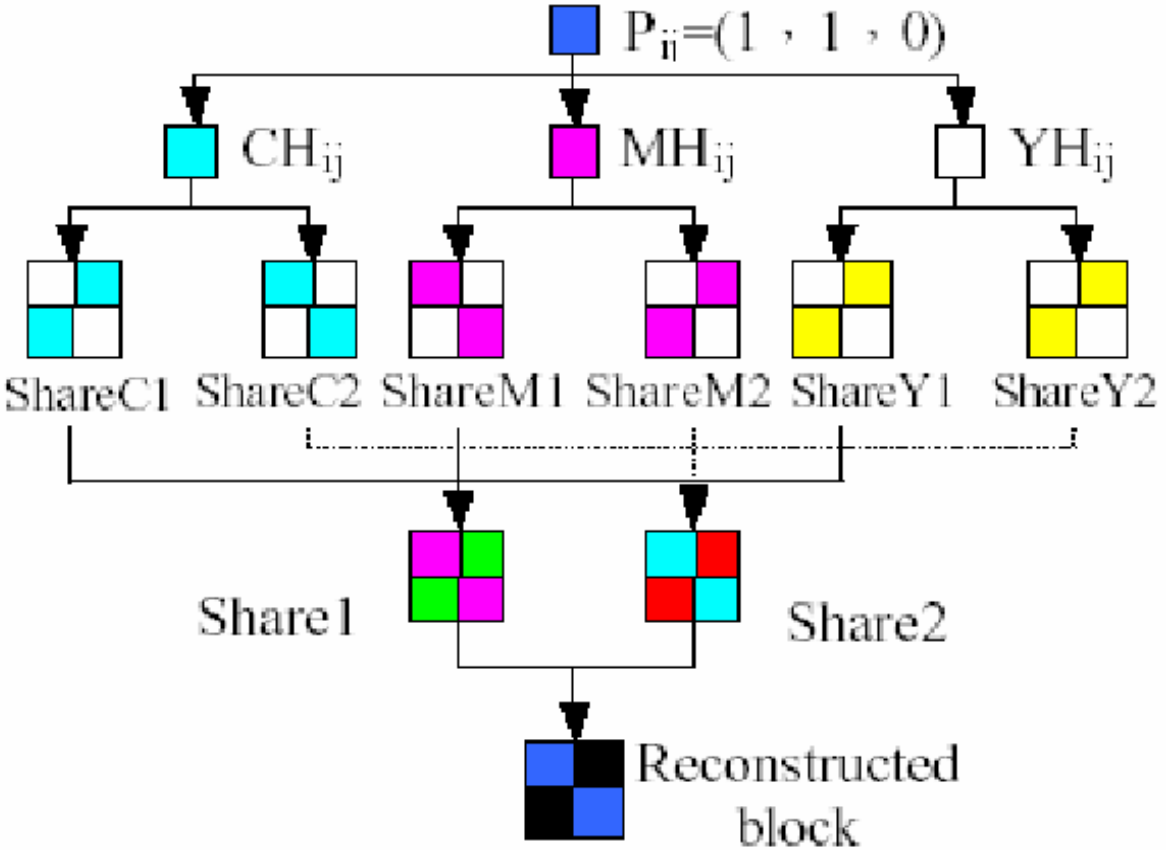

**CMY: Warna hasil cetakan**

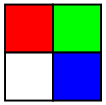
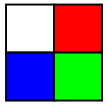
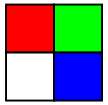
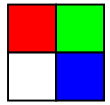
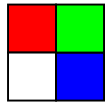
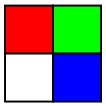
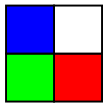
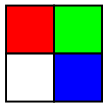
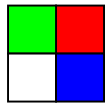
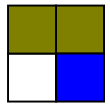
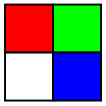
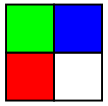
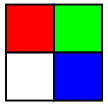
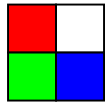
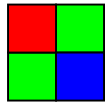

Original image
Color decomposition
C
M
Y
C
M
Y
Halftone image
Composed image


Original image
Color decomposition
C
M
Y
C
M
Y
Composed image P
Halftone image


C
M
Y


C
Y
M


$P_{ij}$=(1，1，0)
$CH_{ij}$
$MH_{ij}$
$YH_{ij}$
ShareC1
ShareC2
ShareM1
ShareM2
ShareY1
ShareY2
Share1
Share2
Reconstructed block

| Share 1 | Share 2 | Hasil tumpukan | Share 1 | Share 2 | Hasil tumpukan |
|---|---|---|---|---|---|
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Share 1

Share 2

Hasil tumpukan

Share 1

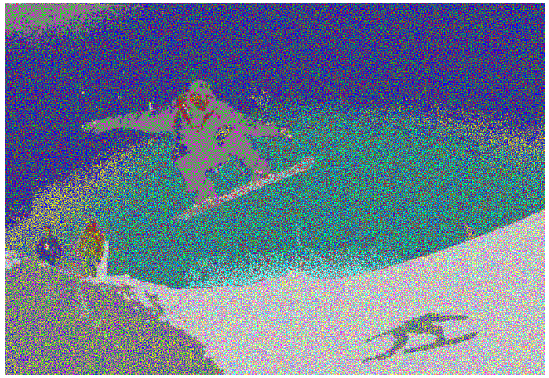
Share 2

Hasil tumpukan

Original image

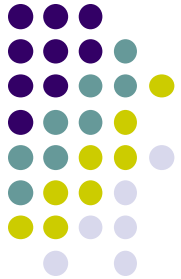
*Share 1*

*Share 2*



Hasil tumpukan

# Algoritma Kriptografi Visual dengan Fungsi XOR



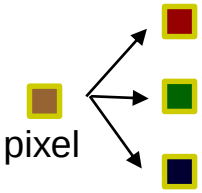
- Kriptografi visual untuk citra berwarna
- Tidak melakukan pembagian *pixel* menjadi *sub-pixel*.
- Ukuran *share* sama dengan ukuran citra semula
- Citra hasil dekripsi tepat sama dengan citra semula.
- Skema (*n*, *n*)
- Operator: XOR (dilambangkan dengan $\oplus$)

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

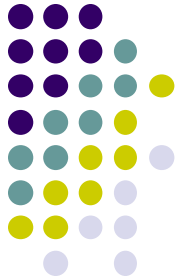
Contoh 2 buah share:

100 | 0 1 1 0 0 1 0 0

226 | 1 1 1 0 0 0 1 0

Perhatikan:

0 1 1 0 0 1 0 0 ⊕ 1 1 1 0 0 0 1 0 = 1 0 0 1 0 1 1 0



Algoritma enkripsi:

1. Misalkan *plain-image* adalah $P$, *share* yang dihasilkan adalah $A_1, ..., A_n$, dan matriks acak untuk membantu enkripsi, yakni $B_1, ..., B_{n-1}$. Semua matriks berukuran sama.
2. Skema $(n,n)$ dapat dihasilkan dengan urutan:

   $A_1 = B_1$

   $A_2 = B_1 \oplus B_2$

   ...

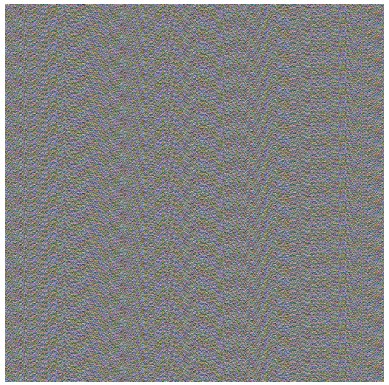
   $A_{n-1} = B_{n-2} \oplus B_{n-1}$

   $A_n = B_{n-1} \oplus P$
3. Seluruh citra *share* untuk skema $(n,n)$ telah dihasilkan.

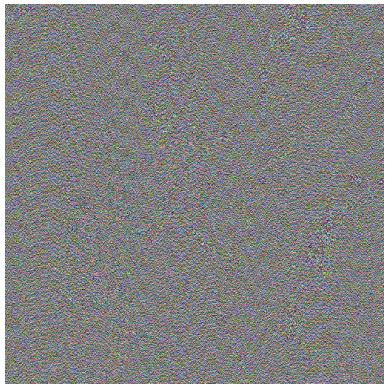
- Untuk merekonstruksi citra, dilakukan dengan meng-*XOR*-kan seluruh citra *share*, yang dijabarkan sebagai berikut:

$$A_1 \oplus A_2 \oplus A_3 \oplus \ldots \oplus A_{n-1} \oplus A_n$$
$$= B_1 \oplus (B_1 \oplus B_2) \oplus (B_2 \oplus B_3) \oplus \ldots \oplus (B_{n-2} \oplus B_{n-1}) \oplus B_{n-1} \oplus P$$
$$= (B_1 \oplus B_1) \oplus (B_2 \oplus B_2) \oplus B_3 \oplus \ldots \oplus B_{n-2} \oplus (B_{n-1} \oplus B_{n-1}) \oplus P$$
$$= (0 \oplus 0 \oplus \ldots \oplus 0) \oplus P$$
$$= 0 \oplus P$$
$$= P$$

Original
Image



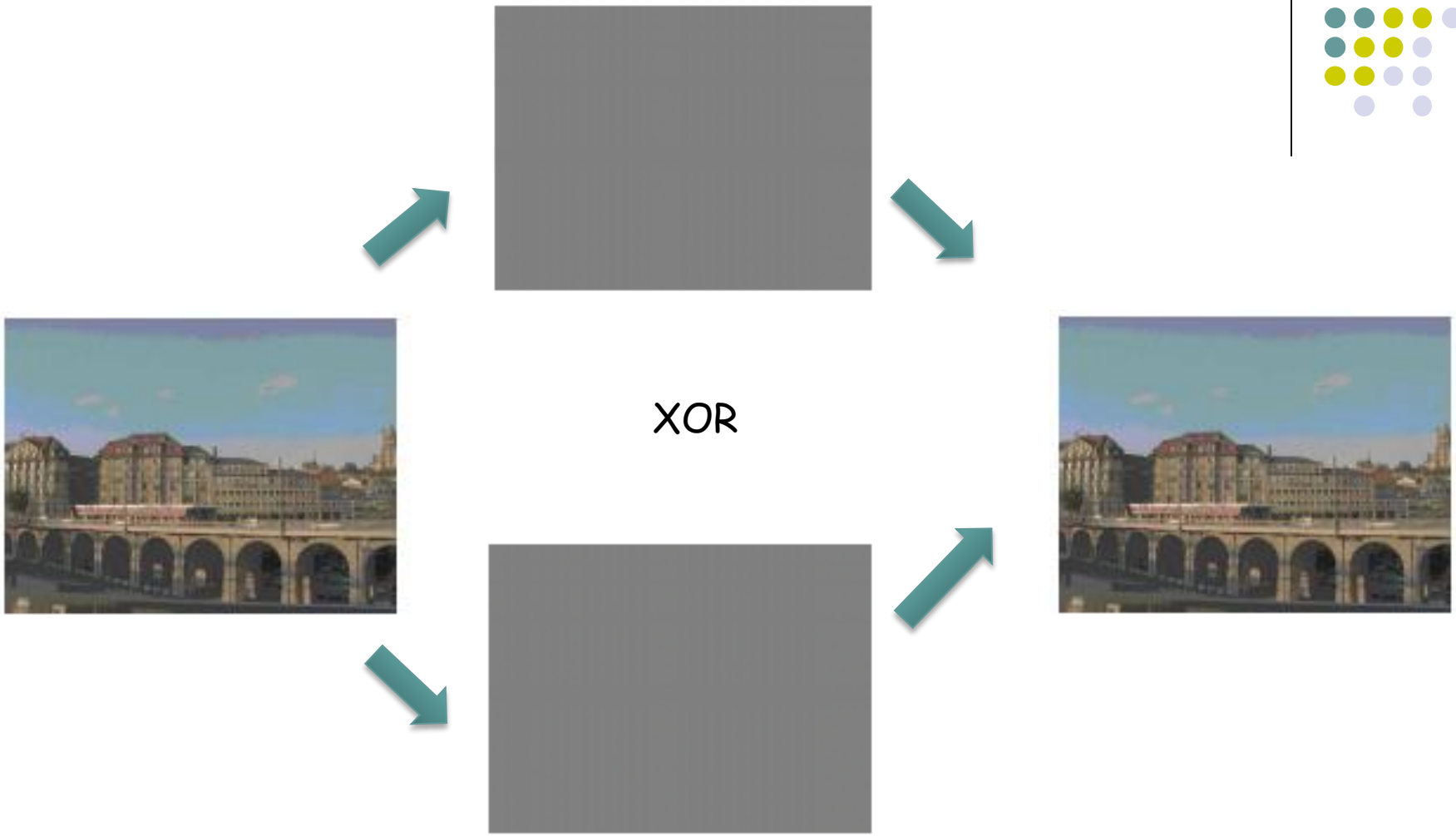
Share 1



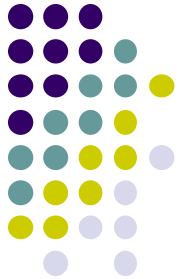
Share 2

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*

- Contoh steganografi:

```
#inlcude <stdio.h>

int main()
{
 printf("Hello world");

 return 0;
}
```

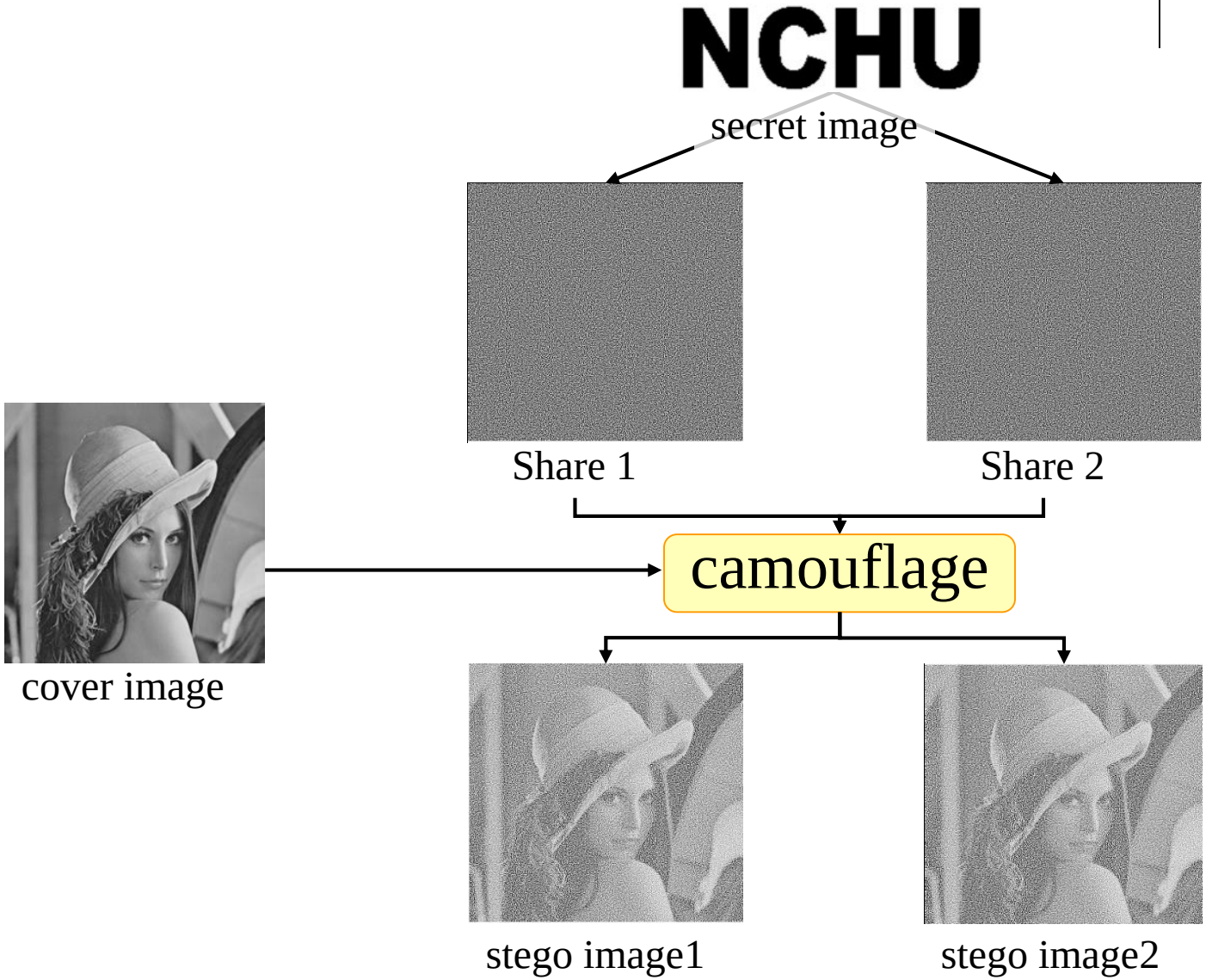
*Secret Message* *Cover-image* *Stego-image*

Secret image

Cover image

Stego-image

# Teknik Camouflage

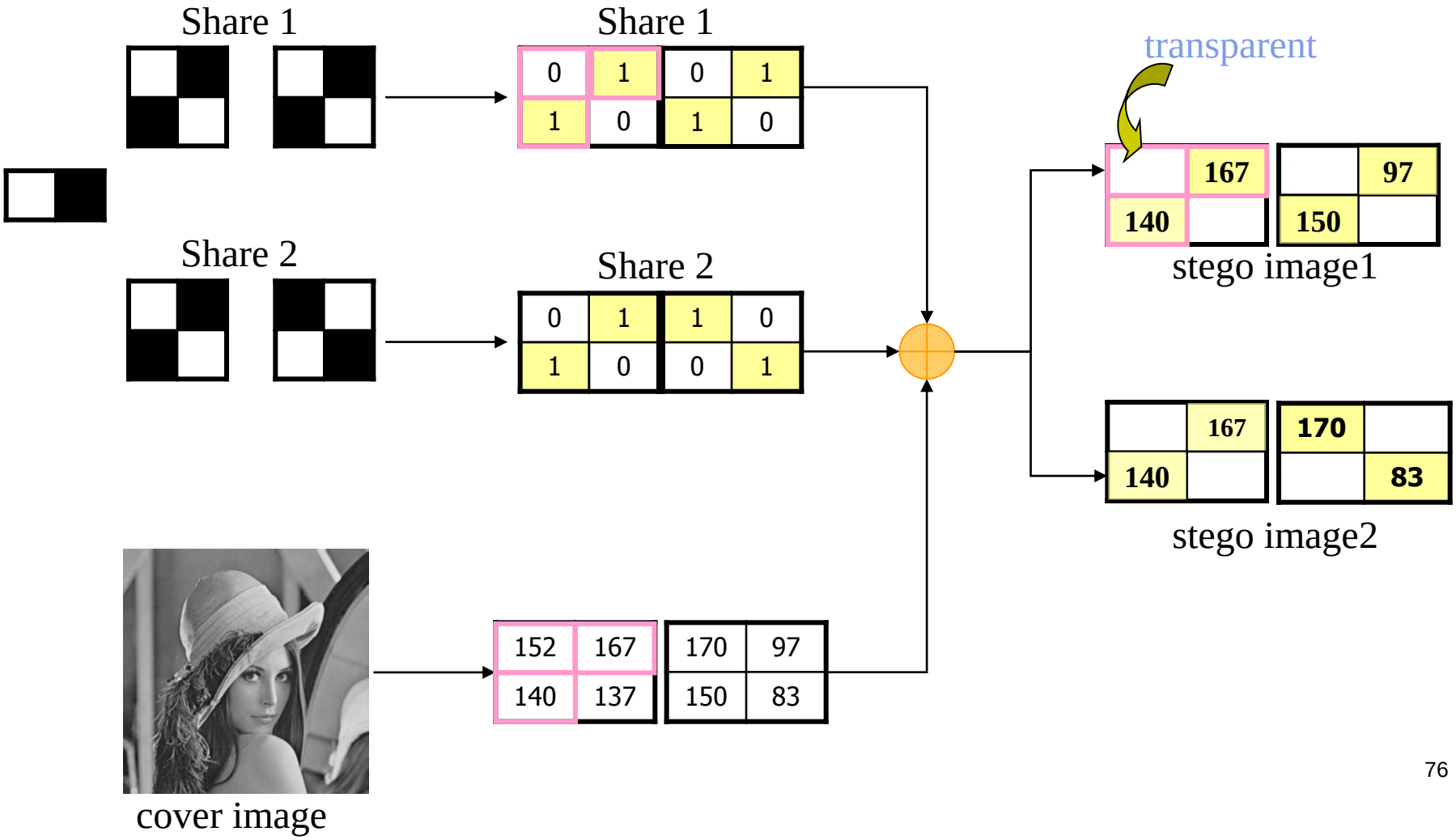


stego image1

stego image2


Stego image 1 + stego image 2

| Secret image | Share1 | Share2 | Stacked image |
|---|---|---|---|
| □ | ■□ / □■ | ■□ / □■ | ■□ / □■ |
| ■ | □■ / ■□ | □■ / ■□ | ■ / ■ |



stego image1

| | |
|---|---|
| | 167 |
| 140 | |

| | |
|---|---|
| | 97 |
| 150 | |

stego image2

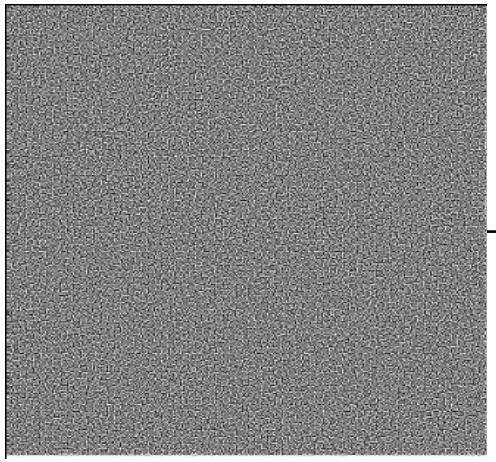
| | |
|---|---|
| | 167 |
| 140 | |

| | |
|---|---|
| 170 | |
| | 83 |

Stego image 1 + stego image 2

# Contoh hasil eksperimen:

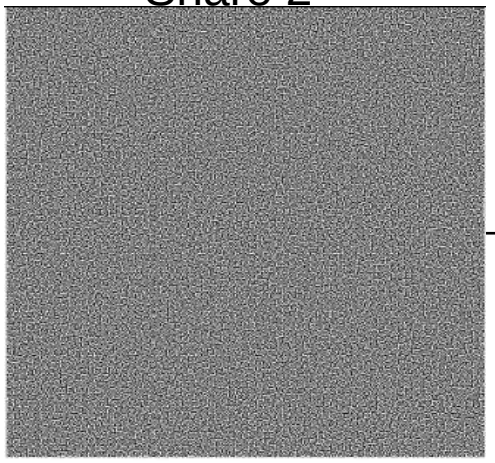
Share 1



cover image1

stego image1

Share 2



cover image2

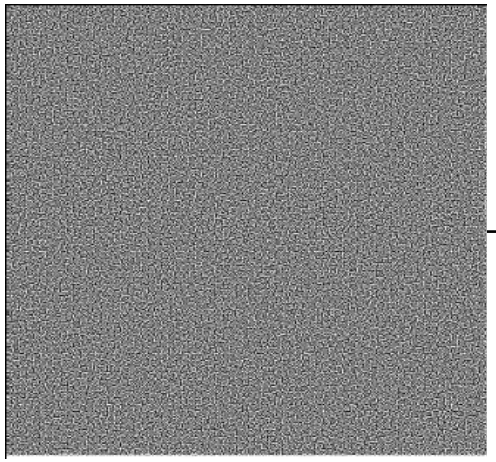
stego image2

stego image1

stego image2


Staego image 1 + stego image 2

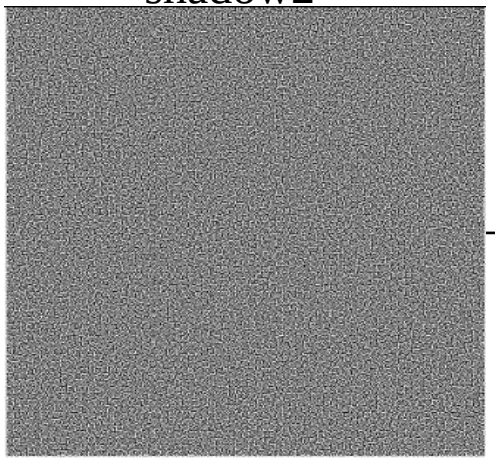
shadow1



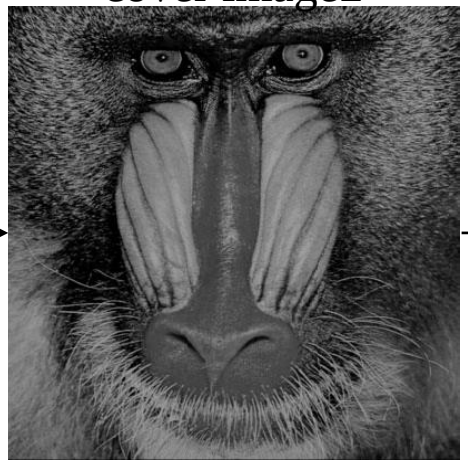
cover image1

stego image1

shadow2



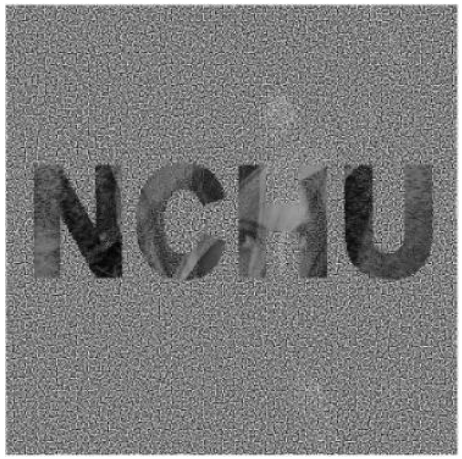
cover image2



stego image2

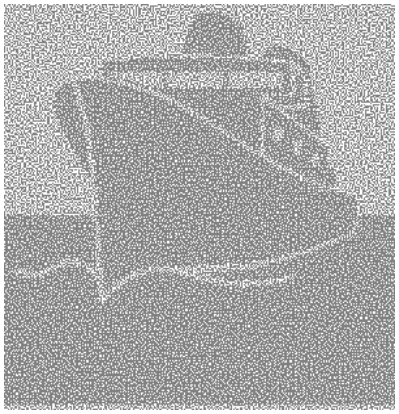
stego image1

stego image2



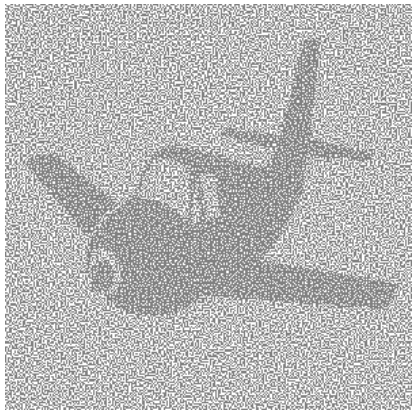

stacked result

- Contoh untuk citra biner



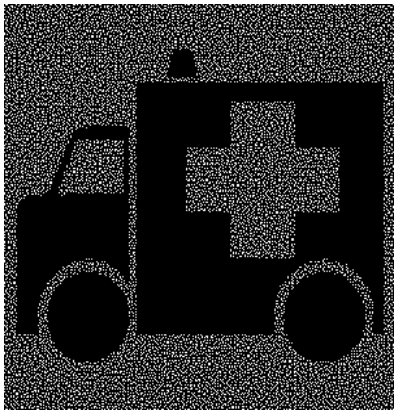
Stego image 1

+

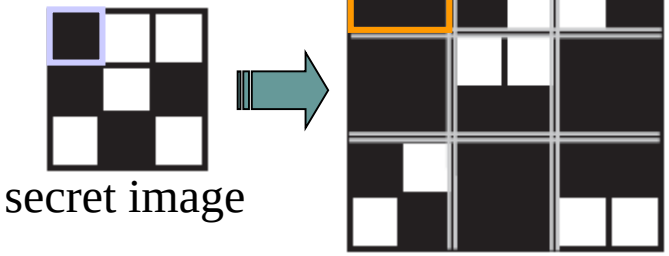


Stego image 2

=

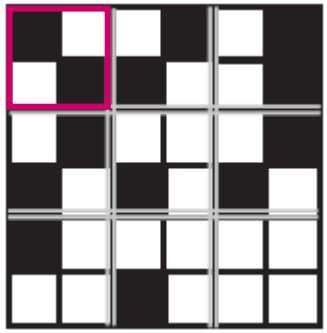


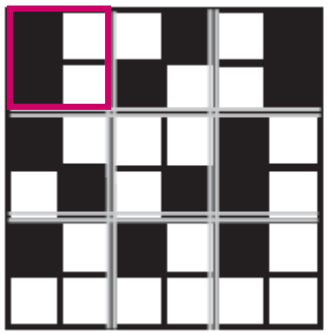
Stego image 1 + stego image2

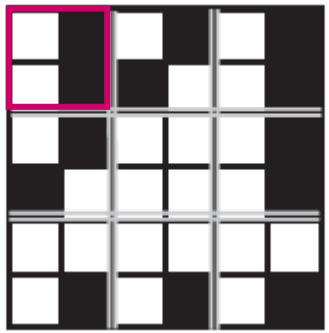


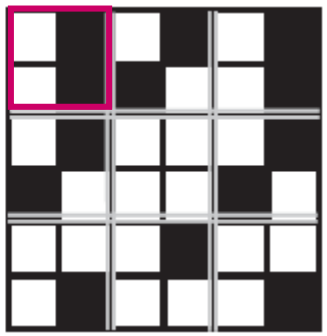




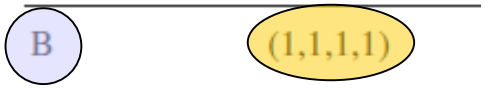








Stego image 1 Stego image 2 Stego image 3 Stego image 4




W

(1,1,0,0)

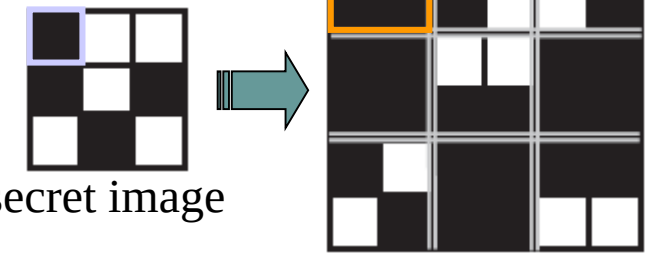
(1,0,1,0)

(1,0,0,1)

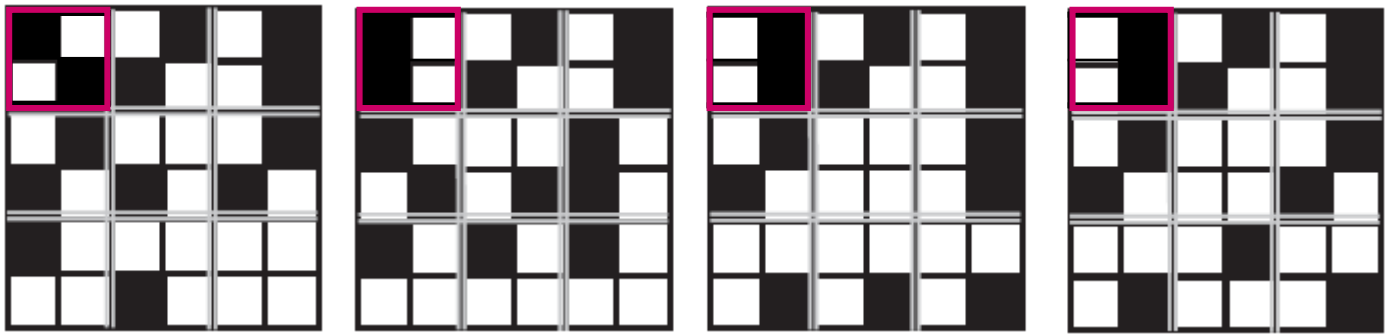
(0,1,1,0)

(0,1,0,1)

(0,0,1,1)



secret image

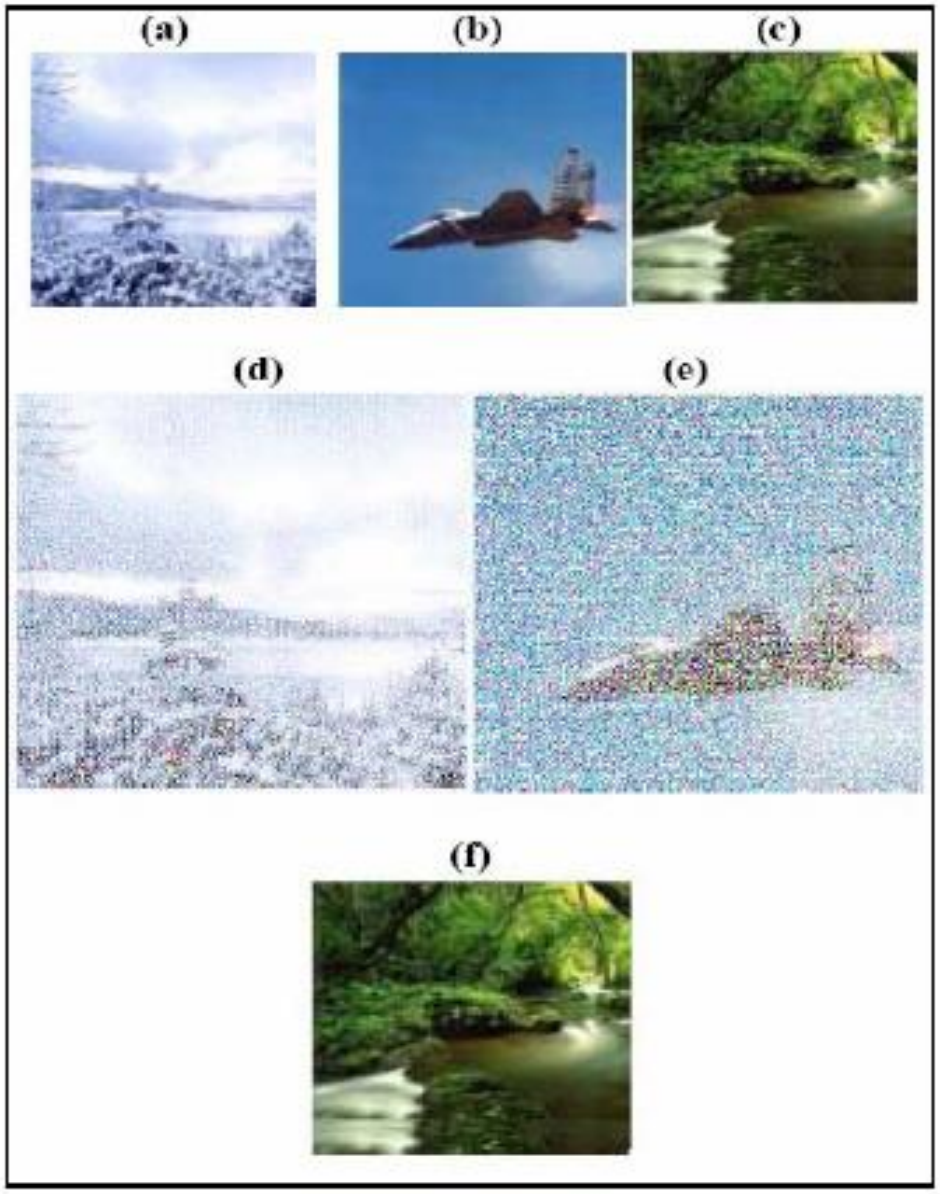


cover image

$k$=2

$k$ = 3

- Contoh untuk citra berwarna




Gambar 13 : Kriptografi Visual Chang dkk.

Keterangan:

(a) *cover 1*

(b) *cover 2*

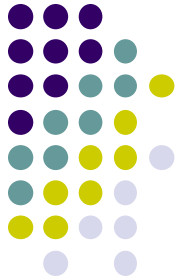
(c) *Secret image*

(d) *Share 1*

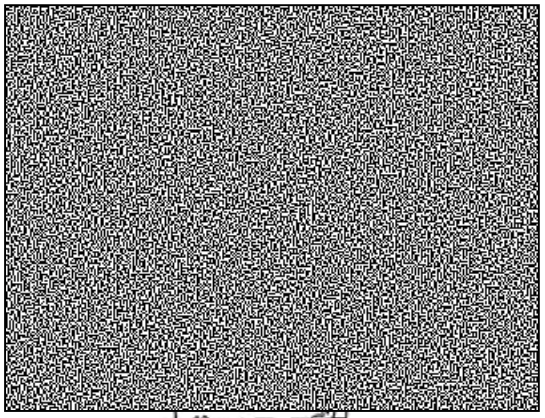
(e) *Share 2*

(f) Hasil dekripsi

# Aplikasi Kriptografi Visual

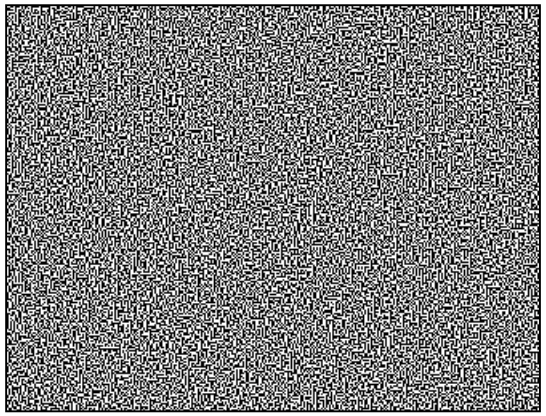


1. **Otentikasi (*authentication*)**
   - Misalkan Bank mengirim kepada nasabah $n - 1$ buah *share* sebagai *share* kunci
   - Situs bank menampilkan sebuah *share*
   - Nasabah melakukan penumpukan, membaca tulisan yang muncul pada hasil tumpukan (yang menyatakan kunci transaksi)
   - Selanjutnya nasabah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



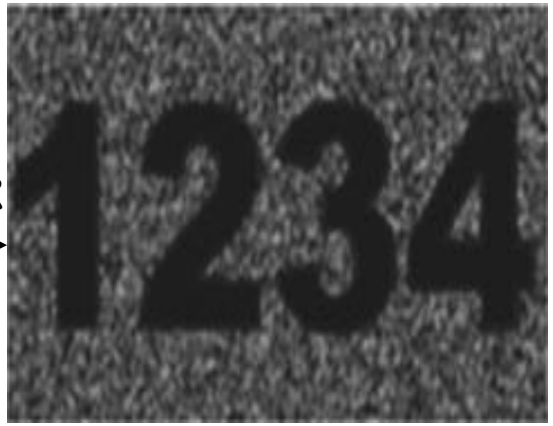
Hacker

Bank



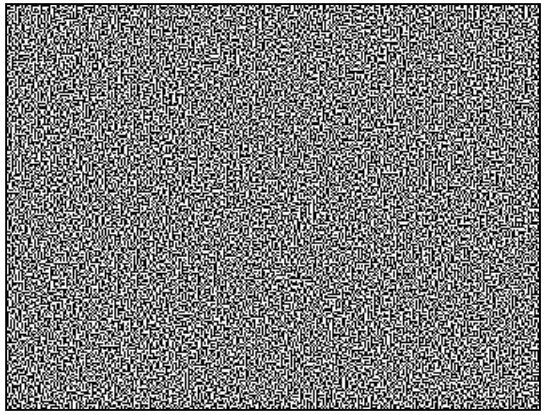
Share 1

Tumpuk




Recovered secret image

Nasabah



Share 2

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