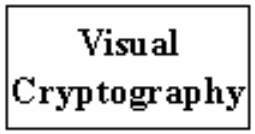
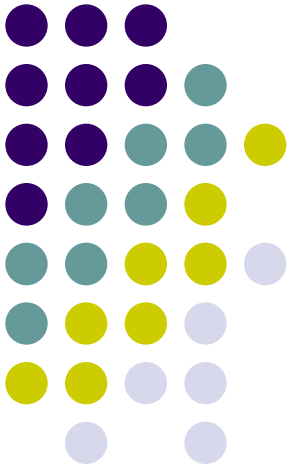
Bahan Kuliah IF4020 Kriptografi

Kriptografi Visual, Teori dan Aplikasinya (Bag. 1)

Oleh:

Dr. Ir. Rinaldi, M.T





Program Studi Teknik Informatika
STEI - 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
A Quick Brown Fox Jumps Over The Lazy Dog 0123456789

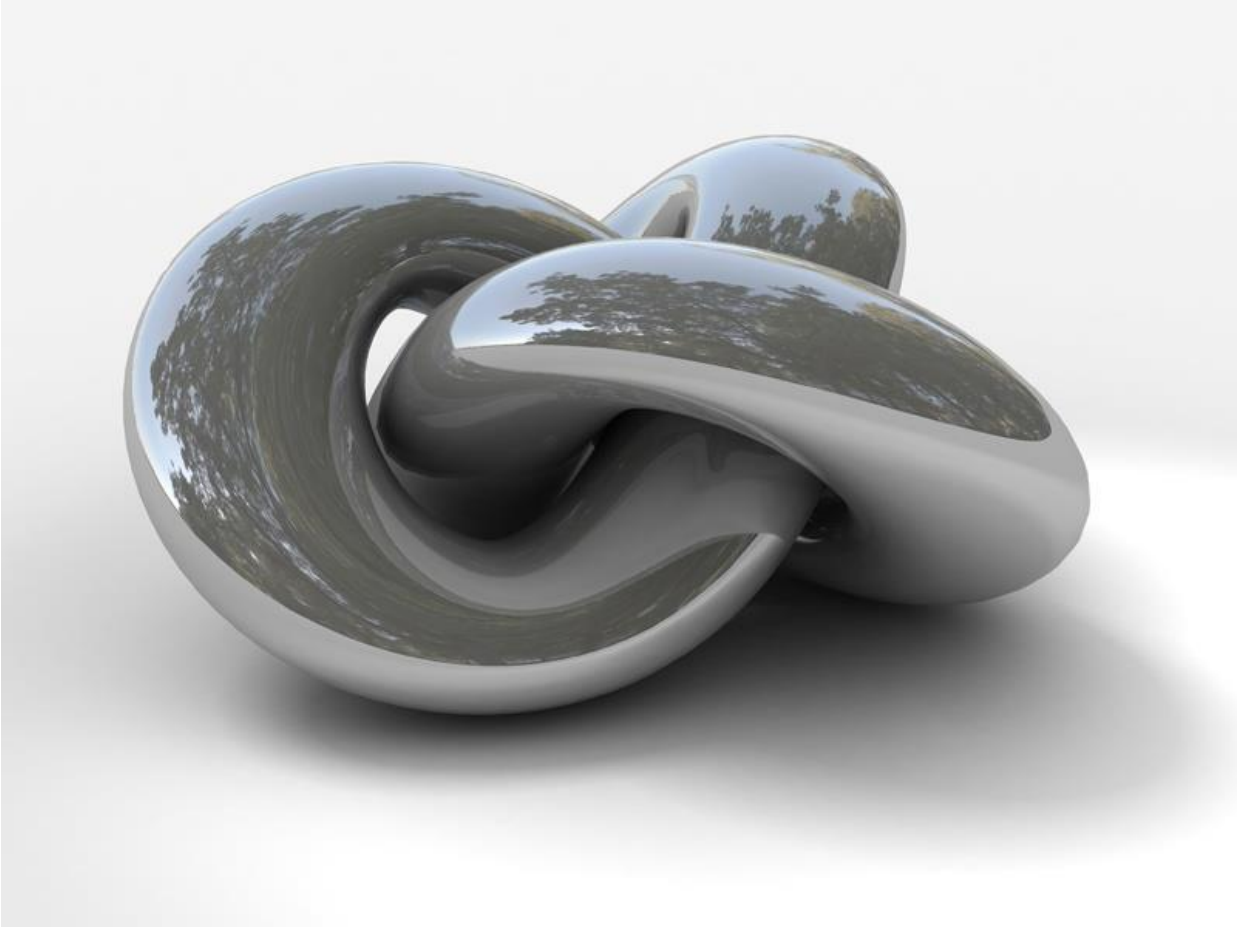
- Gambar (citra)

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

- Video

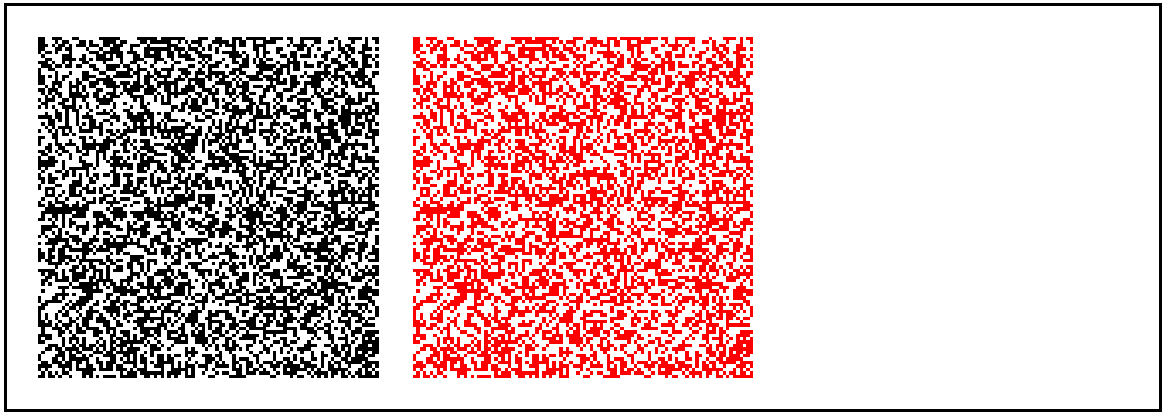
- Animasi

- 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*

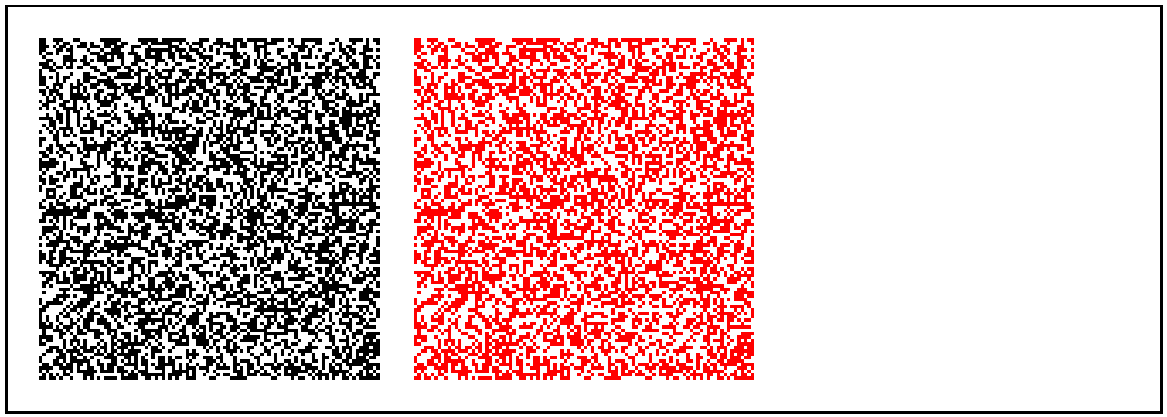
Moni Naor † Adi Shamir ‡

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.

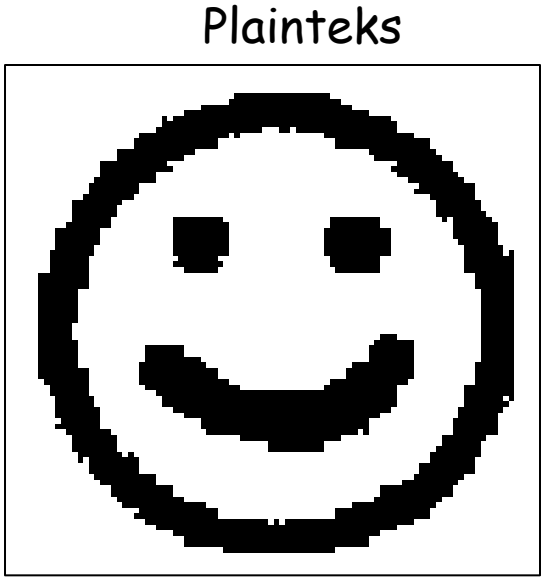
- Enkripsi dilakukan dengan membagi gambar menjadi sejumlah bagian yang disebut ***share***.

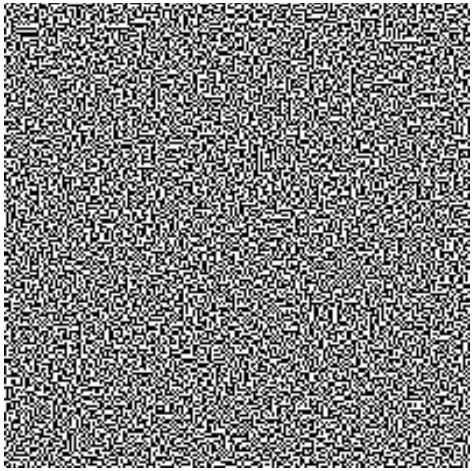
- Setiap *share* terlihat seperti citra acak yang tak bermakna sehingga disebut juga *shadow*.



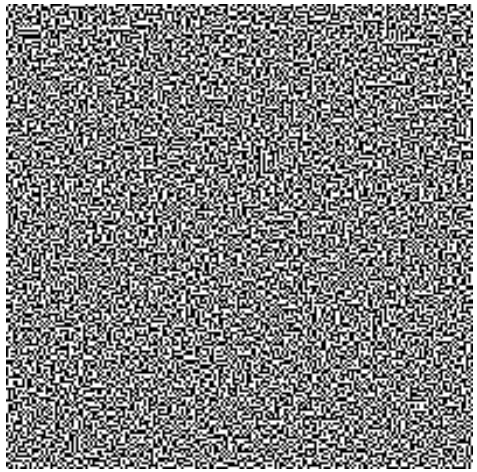
- Tidak membutuhkan komputasi untuk dekripsi citra. Dekripsi dilakukan dengan menumpuk sejumlah *share*.

Contoh:





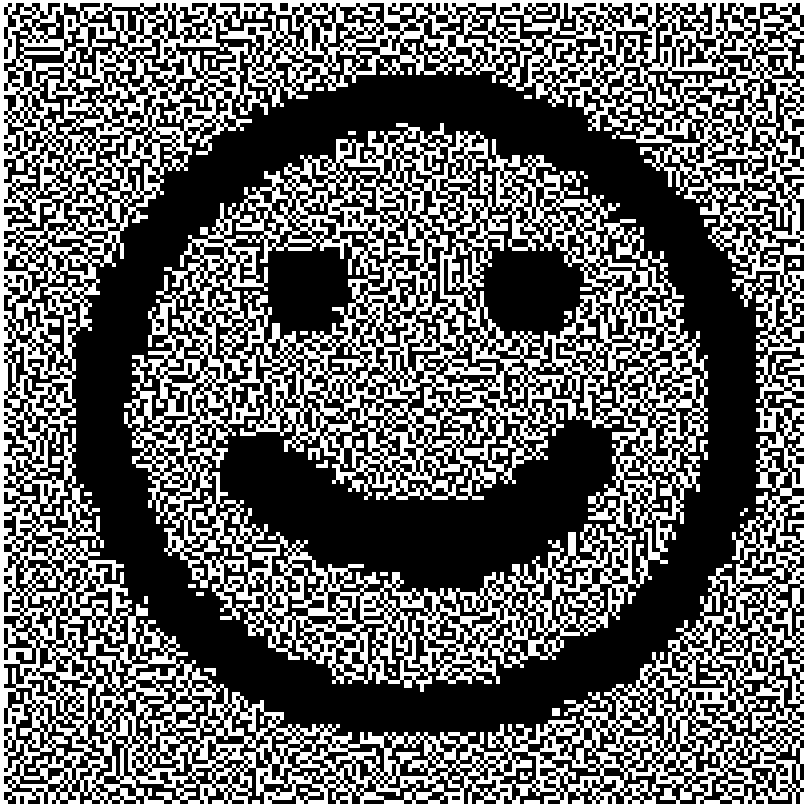
dekripsi



Share 1

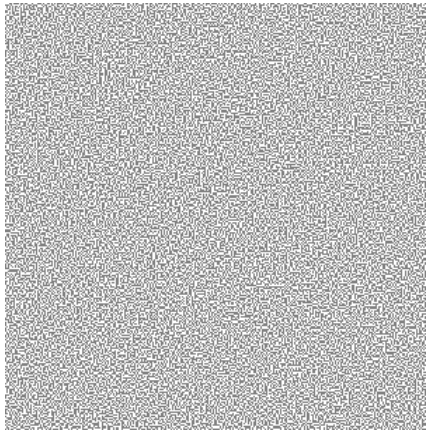
Share 2

Hasil dekripsi:

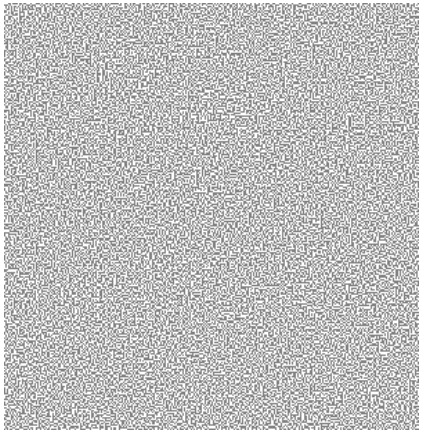


Contoh lain:

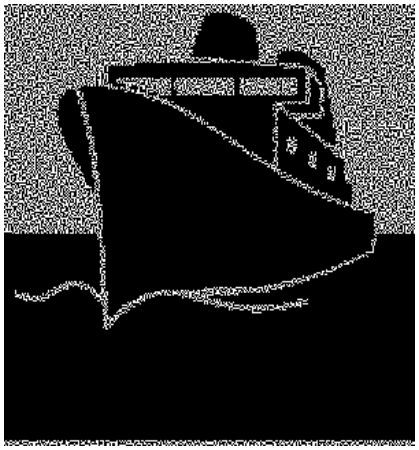
Plain-image



Share 1



Share 2



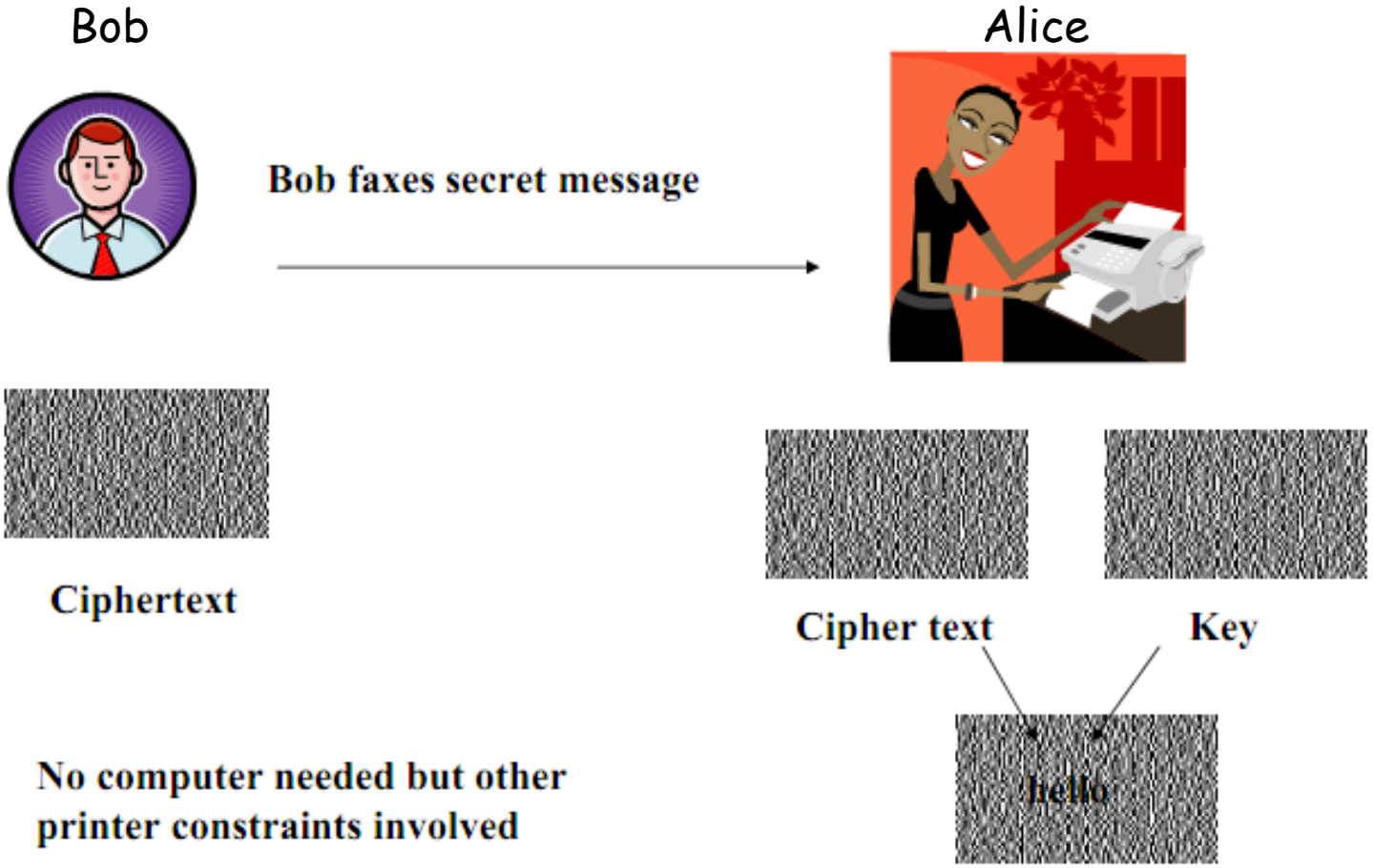
Share 1 + Share 2

- 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* dinamakan ***partisipant***.

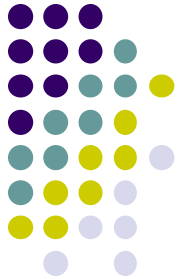
- Dekripsi dilakukan oleh *partisipant* dengan menumpuk *share* yang mereka miliki (misalnya setiap *share* dicetak pada plastik transparan)

- Skenario penggunaan



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

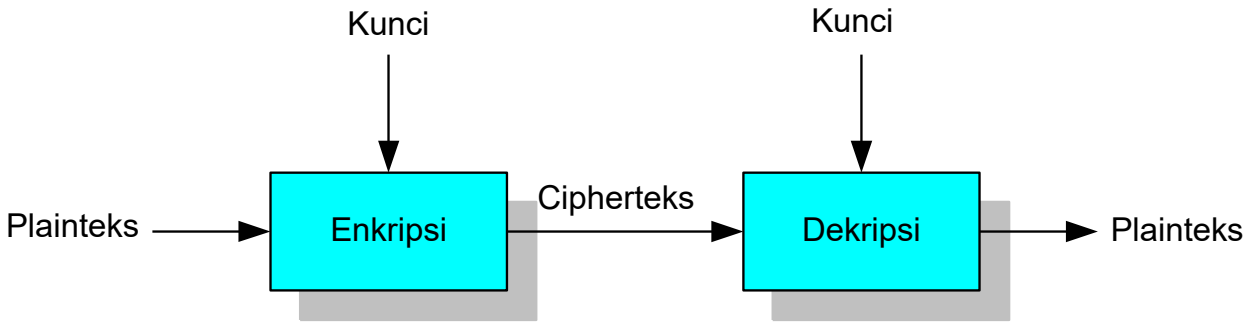
Kriptografi *versus* Kriptografi Visual



- 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
  - *Share* itu sendiri sudah berlaku sebagai kunci

- Kriptografi Tradisionil



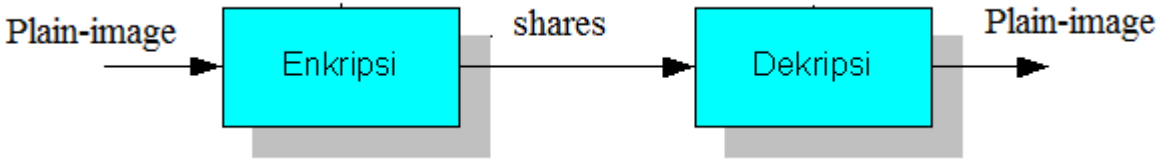

```
Ketika saya berjalan-jalan di
pantai, saya menemukan banyak
sekali kepiting yang merangkak
menuju laut. Mereka adalah
anak-anak kepiting yang baru
menetas dari dalam pasir.
Naluri mereka mengatakan bahwa
laut adalah tempat kehidupan
mereka.
```

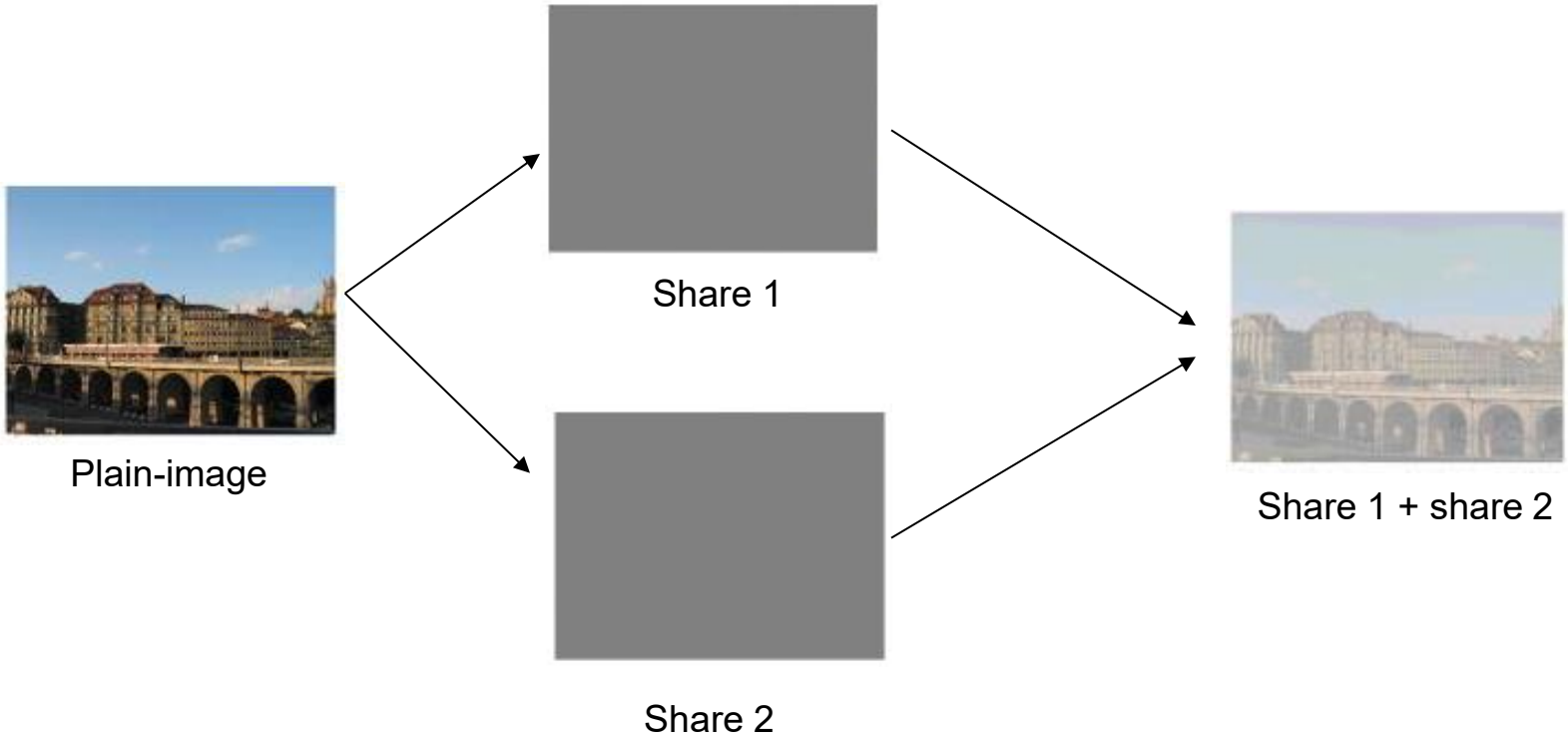
(a) Plainteks (teks)

```
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)

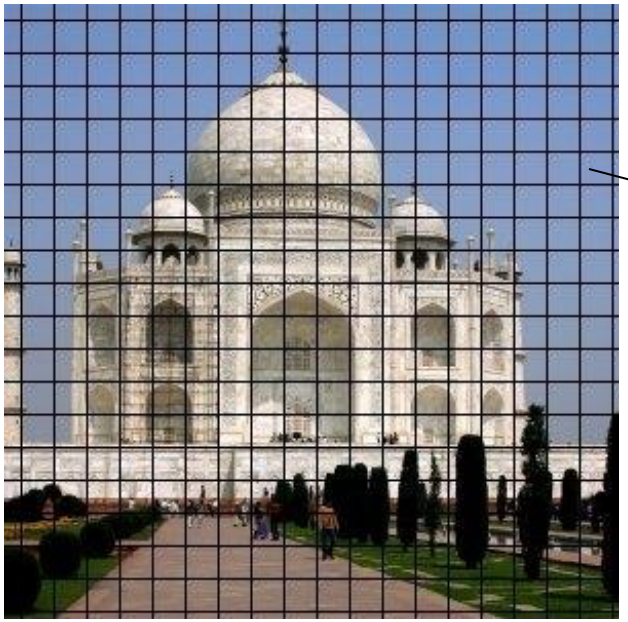
- Kriptografi Visual





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*)

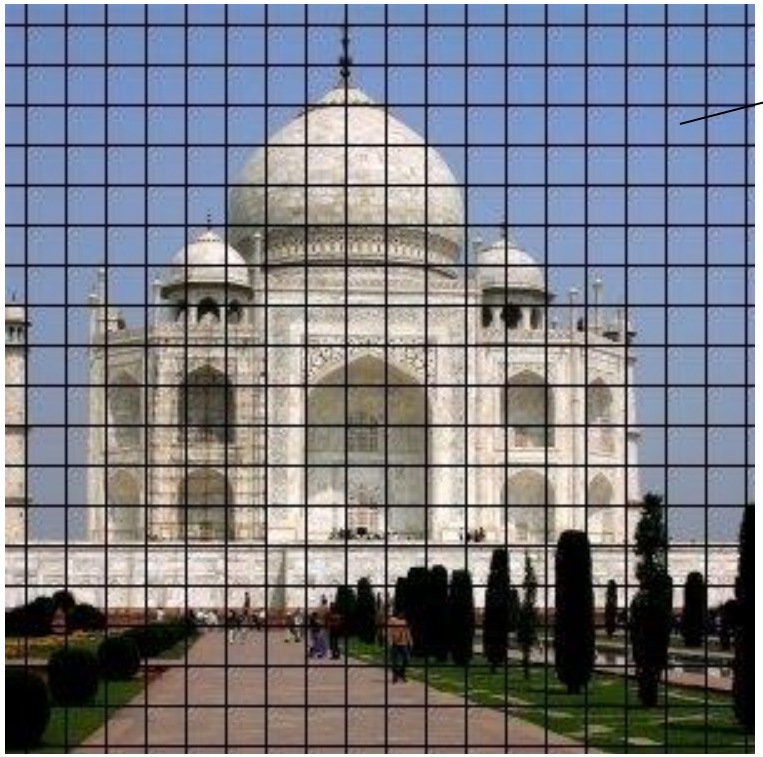
Original Image

Red

Green

Blue

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

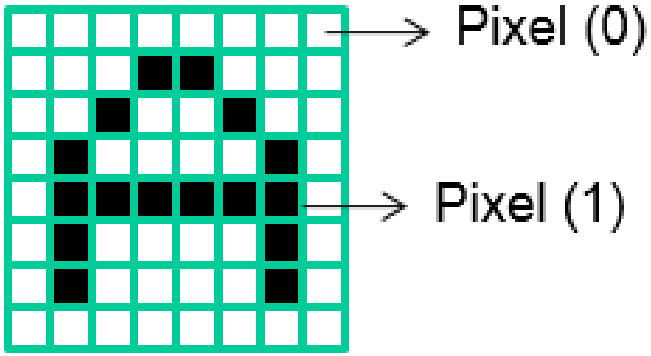


10010011100101001000101010

R G B

Kriptografi Visual pada Citra Biner

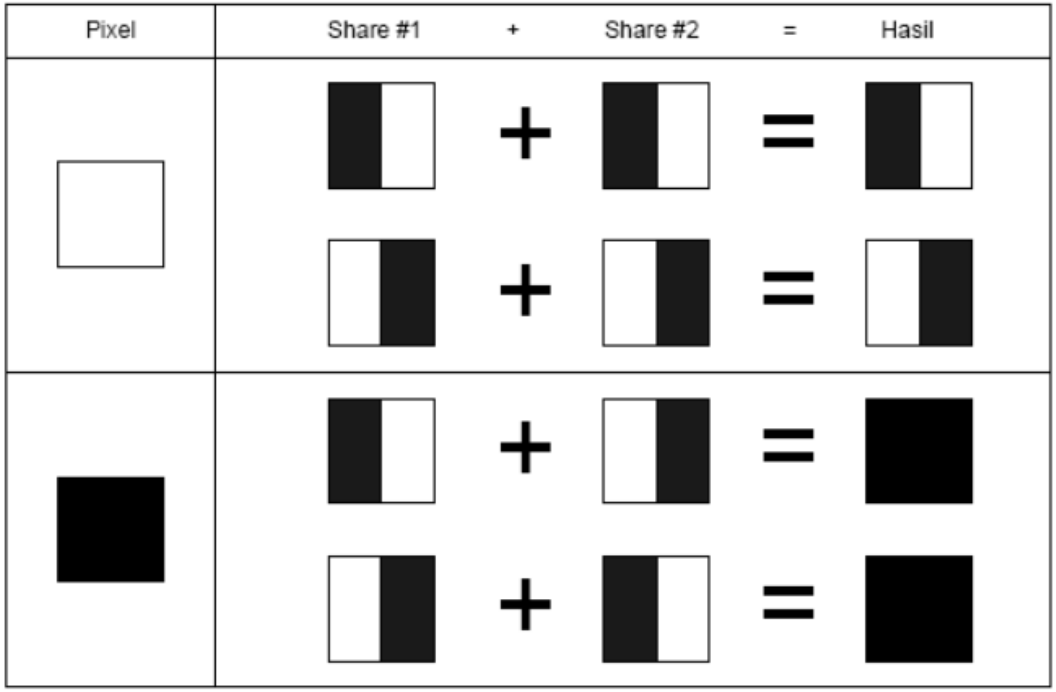
- Tinjau kriptografi visual untuk citra biner
- *Pixel* pada citra biner:
  - bernilai 1 jika hitam
  - bernilai 0 jika putih



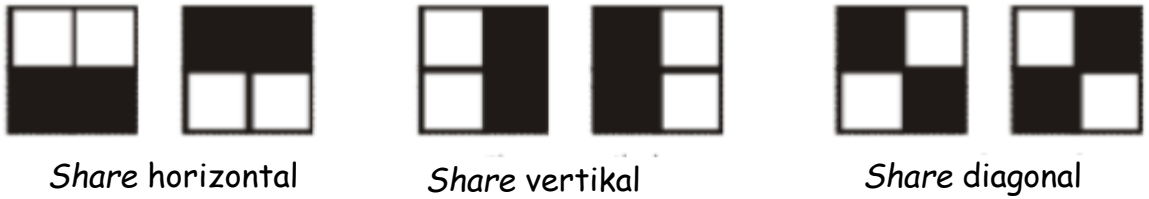
$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Bagaimana cara kerja kriptografi visual?

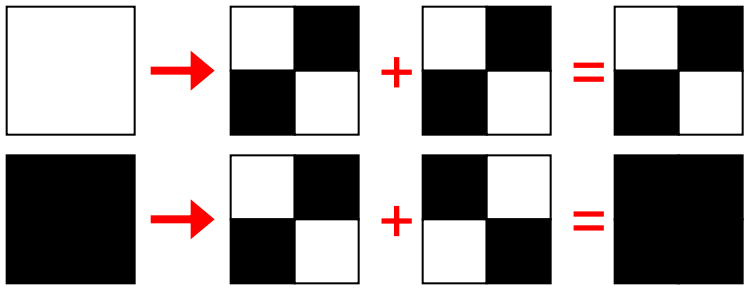
- Setiap *pixel* dibagi menjadi sejumlah *sub-pixel.*
- Setiap *pixel* muncul pada setiap *share*
- Jika *sub-pixel* dari setiap *share* ditumpuk, hasilnya *pixel* yang dipersepsi sebagai “putih” atau “hitam”.



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



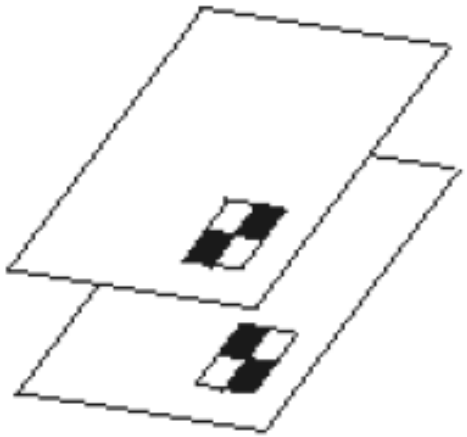
- Penumpukan:



- Setiap *share* dicetak pada plastik transparansi.

- Jika dua buah *share* ditumpuk, maka mata manusia mempersepsi *pixel* yang terbentuk sebagai “hitam” atau “putih”

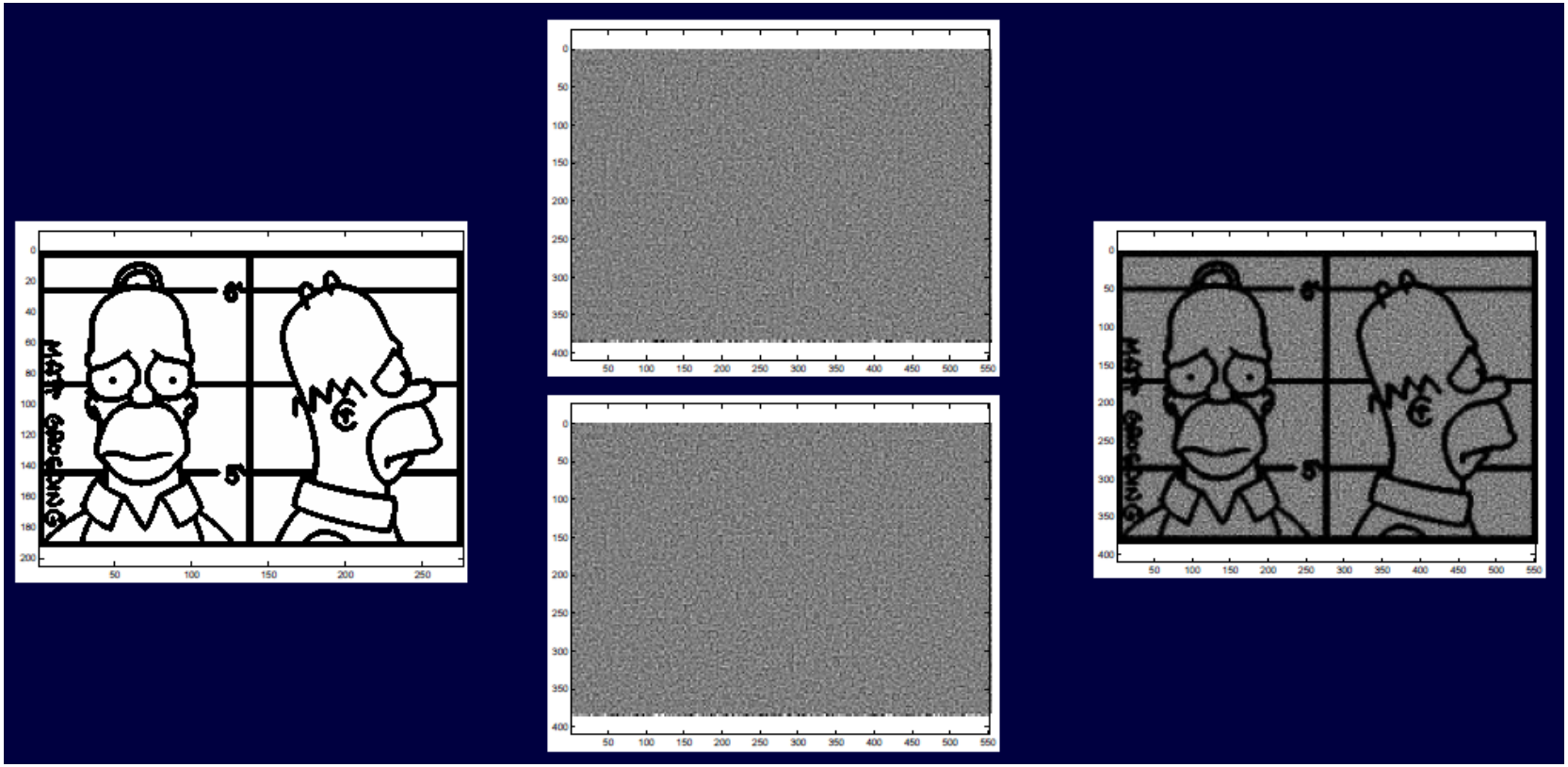
- Apa warna yang dipersepsi dari penumpukan di bawah ini?



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

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

- 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

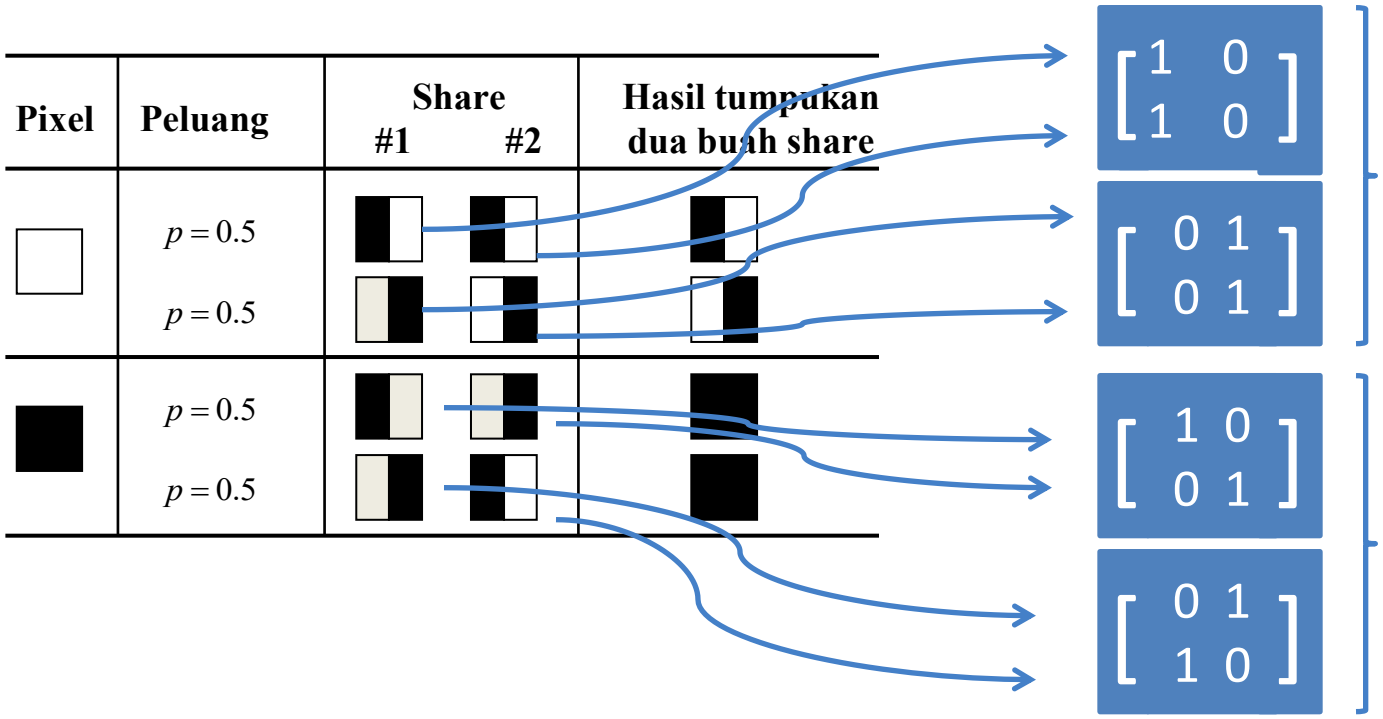
- Didefinisikan dua buah himpunan C_0 dan C_1
- C_0 = semua matriks *S* yang merepresentasikan *pixel* putih
  = semua matriks hasil permutasi kolom dari 1 matriks

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

- 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:

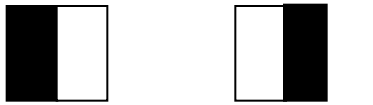


$$C_0 = \left\{ \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \right\} \qquad C_1 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}$$

Skema (2, 2)

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

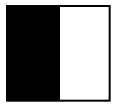
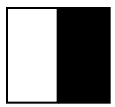
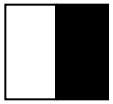
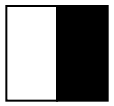
1. Ambil sebuah *pixel* dari gambar (*plain-image*), misal pixel *P*
2. Jika *P* berwarna putih, ambil secara acak sebuah matriks S pada C_0
   Jika P berwarna hitam, ambil secara acak sebuah matriks *S* pada C_1
   Misalkan P berwarna hitam dan matriks yang diambil dari C_1 adalah sebagai berikut: $S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



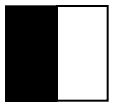
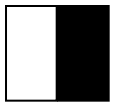
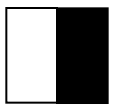
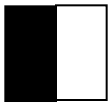
4. Ulangi langkah 2 dan 3 untuk *pixel-pixe*l lainnya

Contoh:

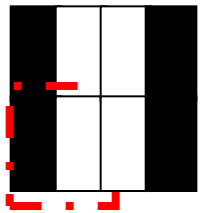
pixel

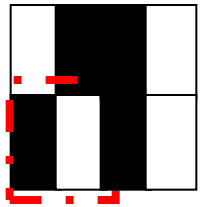
	Share 1		Share2		Tumpukan
Alternatif 1		+		=	
Alternatif 2		+		=	

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

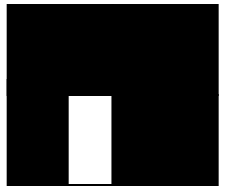
	Share 1		Share2		Tumpukan
Alternatif 1		+		=	
Alternatif 2		+		=	

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



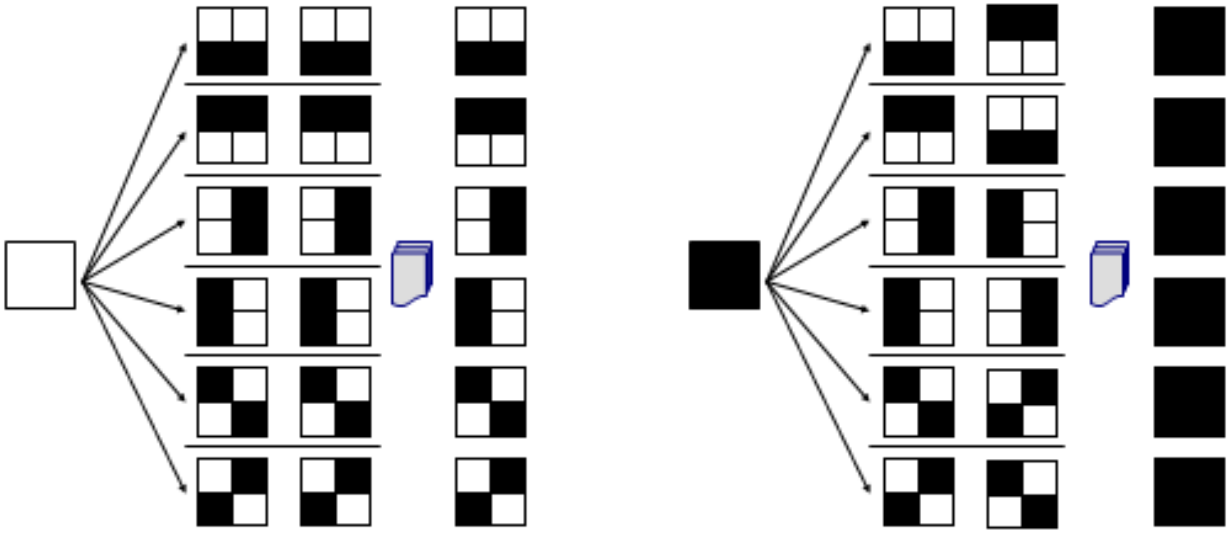


acak



- Contoh skema (2, 2) lainnya:

horizontal shares vertical shares diagonal shares



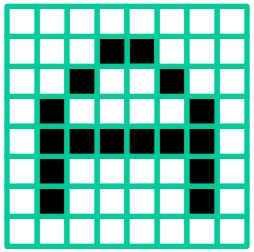
$$C_0 = \left\{ \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 &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

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

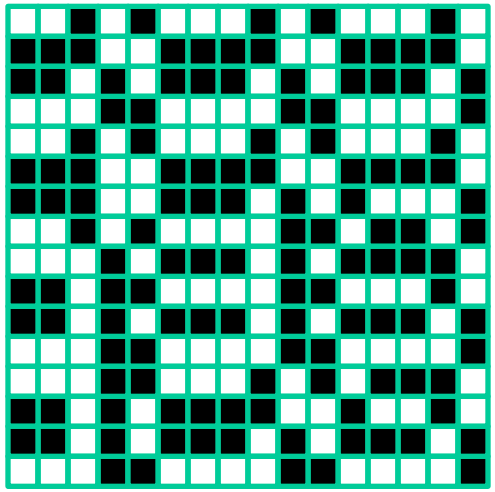
horizontal shares

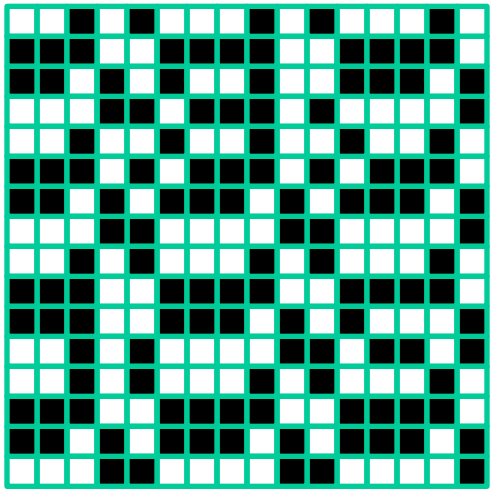
vertical shares

diagonal shares



Secret Image

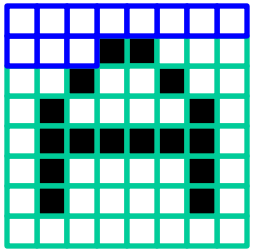


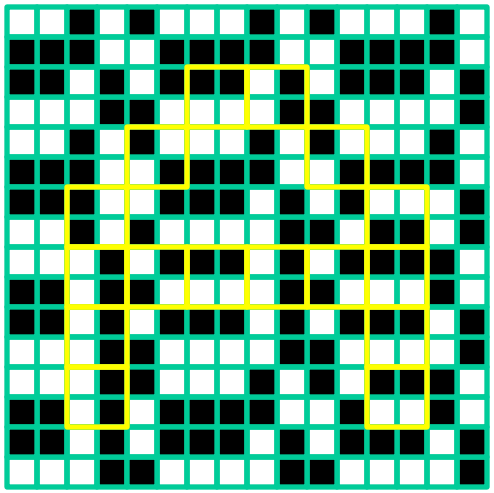


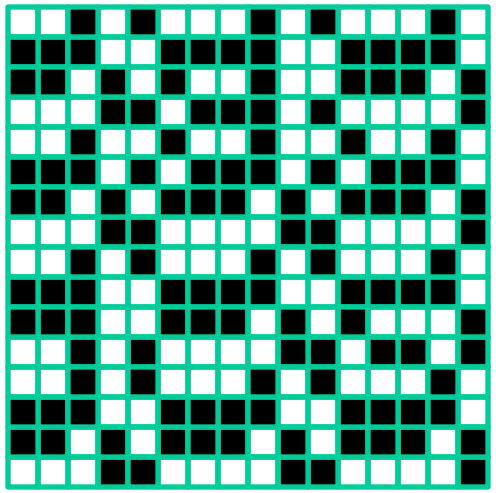
horizontal shares

vertical shares

diagonal shares



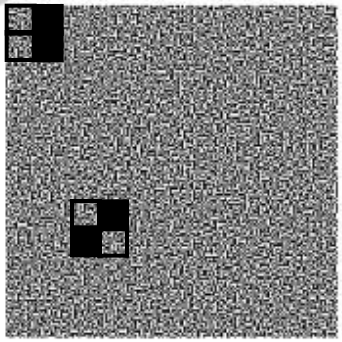




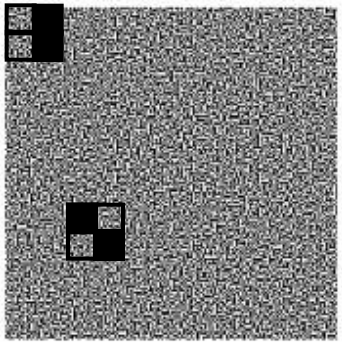
Contoh lainnya:

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	■□	□■	■■	□■	■□	□■	■■	■■	■■	■■	■■	■■

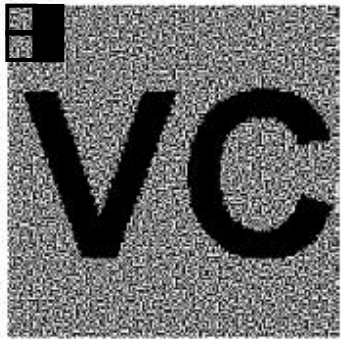
(a) Original secret image



(b) First share image

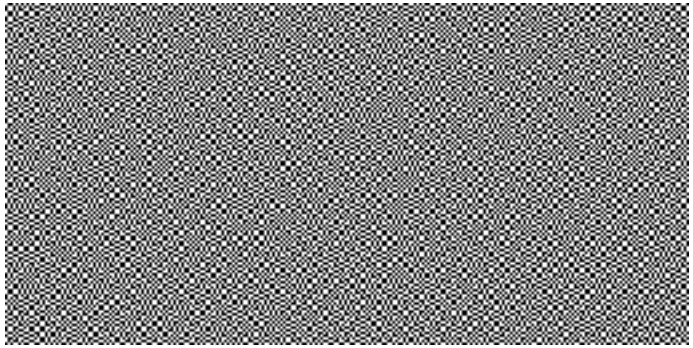


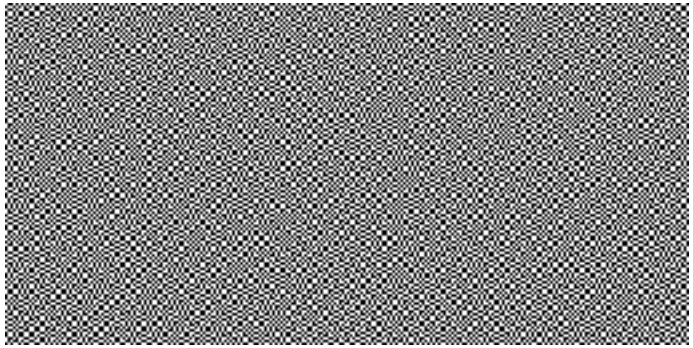
(c) Second share image

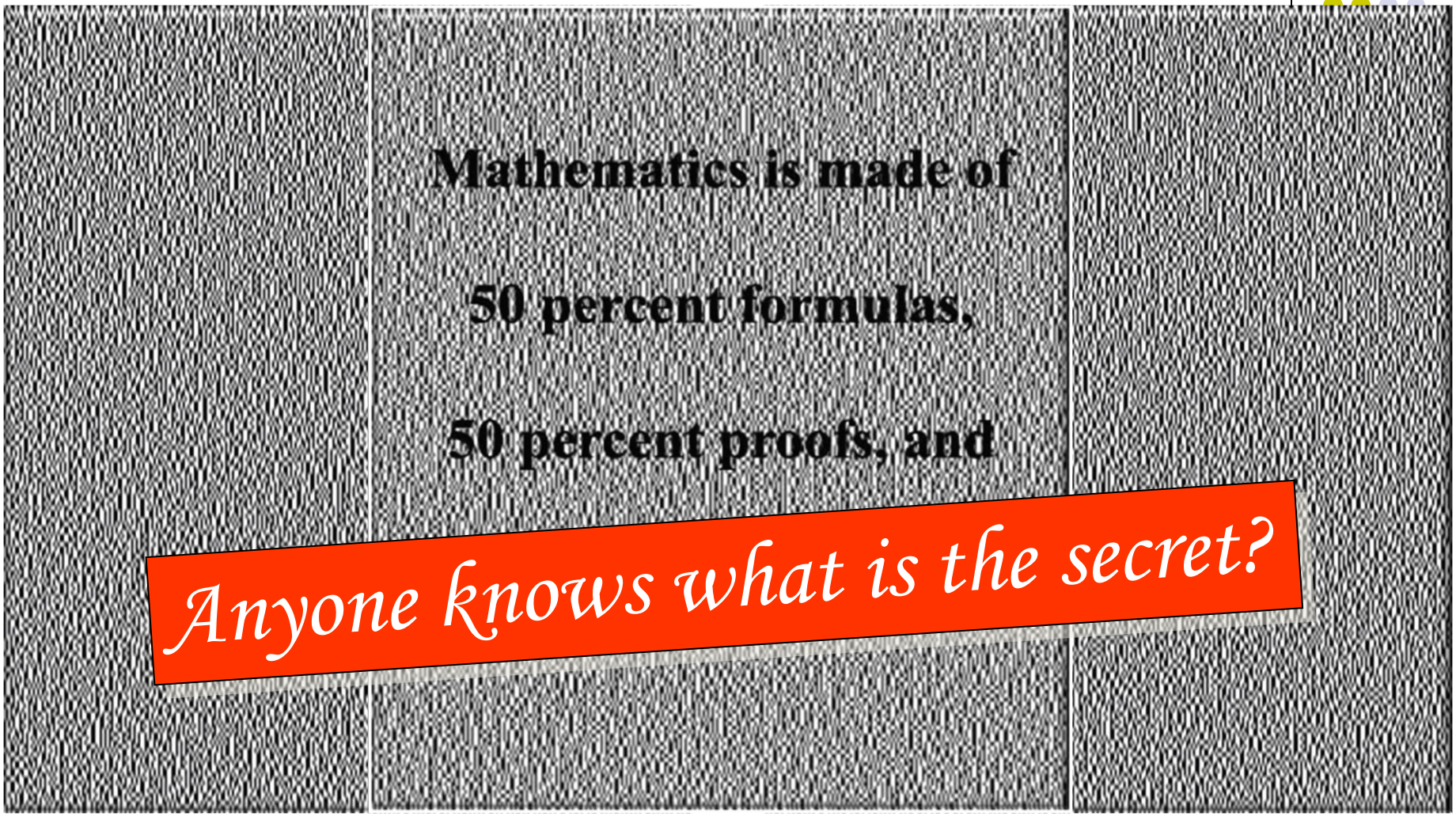


(d) Stacked result of (a) and (b)

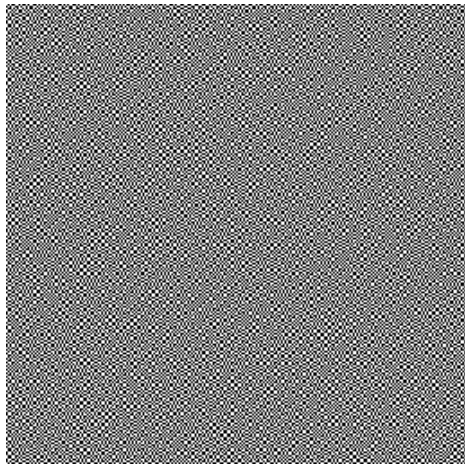
- Contoh-contoh kriptografi visual sederhana



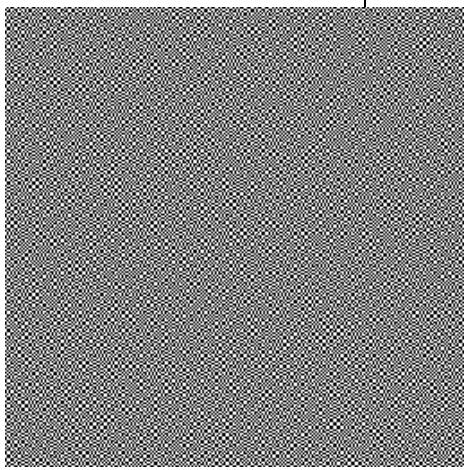



Mathematics is made of
50 percent formulas,
50 percent proofs, and
Anyone knows what is the secret?

Original



Share 1



Share 2

Hasil penumpukan *share* 1 dan *share* 2

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

BERSAMBUNG