

Steganografi

Bahan Kuliah Keamanan Data

Sevi Nurafni

Fakultas Sains dan Teknologi
Universitas Koperasi Indonesia 2025

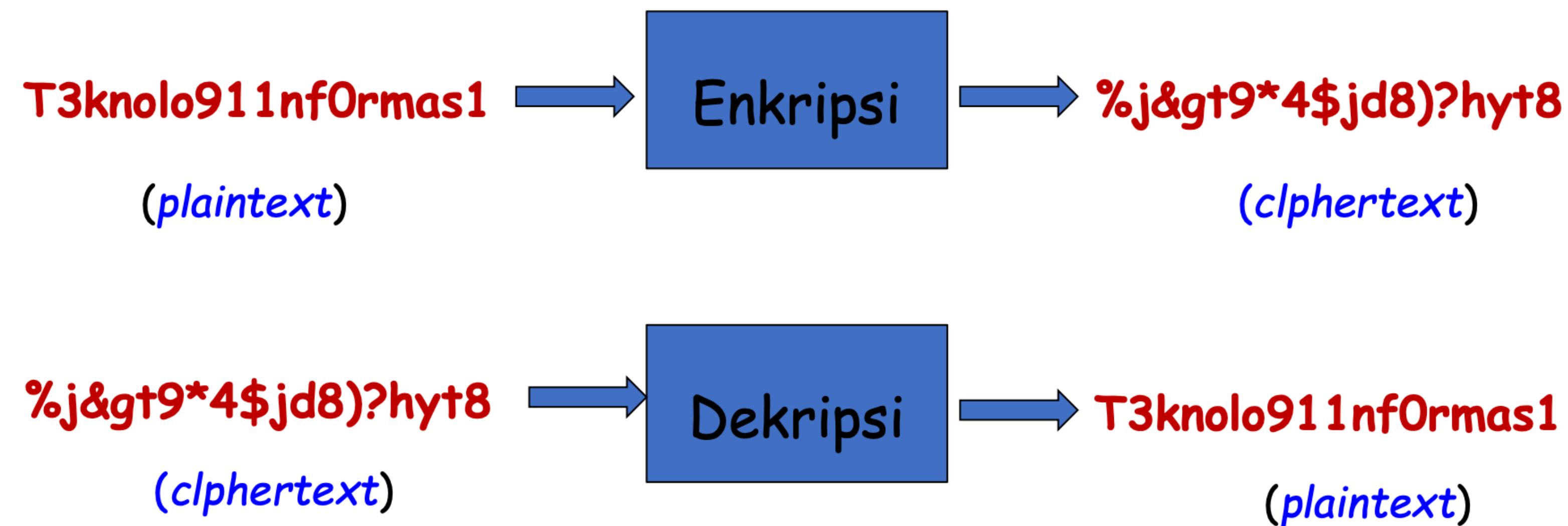
Get to Know

- Misalkan anda mempunyai data rahasia seperti *password*.

Password: **T3knolo911nf0rmas1**

- Anda ingin menyimpan *password* tersebut dengan aman (tidak bisa diketahui orang lain).
- Bagaimana caranya agar *password* tersebut dapat disimpan dengan aman?

Cara 1: Mengenkripsi



Cara 2: Menyembunyikan

T3knolo911nf0rmas1



Apa itu Steganografi?

- Dari Bahasa Yunani: steganos + graphien

“steganos” (στεγανός): tersembunyi

“graphien” (γραφία): tulisan

steganografi: tulisan tersembunyi (*covered writing*)

- *Steganography*: ilmu dan seni menyembunyikan pesan rahasia dengan suatu cara sedemikian sehingga tidak seorang pun yang mencurigai keberadaan pesan tersebut.

Tujuan steganografi: pesan tidak terdeteksi keberadaannya

Perbedaan Kriptografi dan Steganografi

- **Kriptografi**: menyembunyikan isi (*content*) pesan
Tujuan: agar pesan tidak dapat dibaca oleh pihak ketiga (lawan)
- **Steganografi**: menyembunyikan keberadaan (*existence*) pesan
Tujuan: untuk menghindari kecurigaan (*conspicuous*) dari pihak ketiga (lawan)

Kriptografi



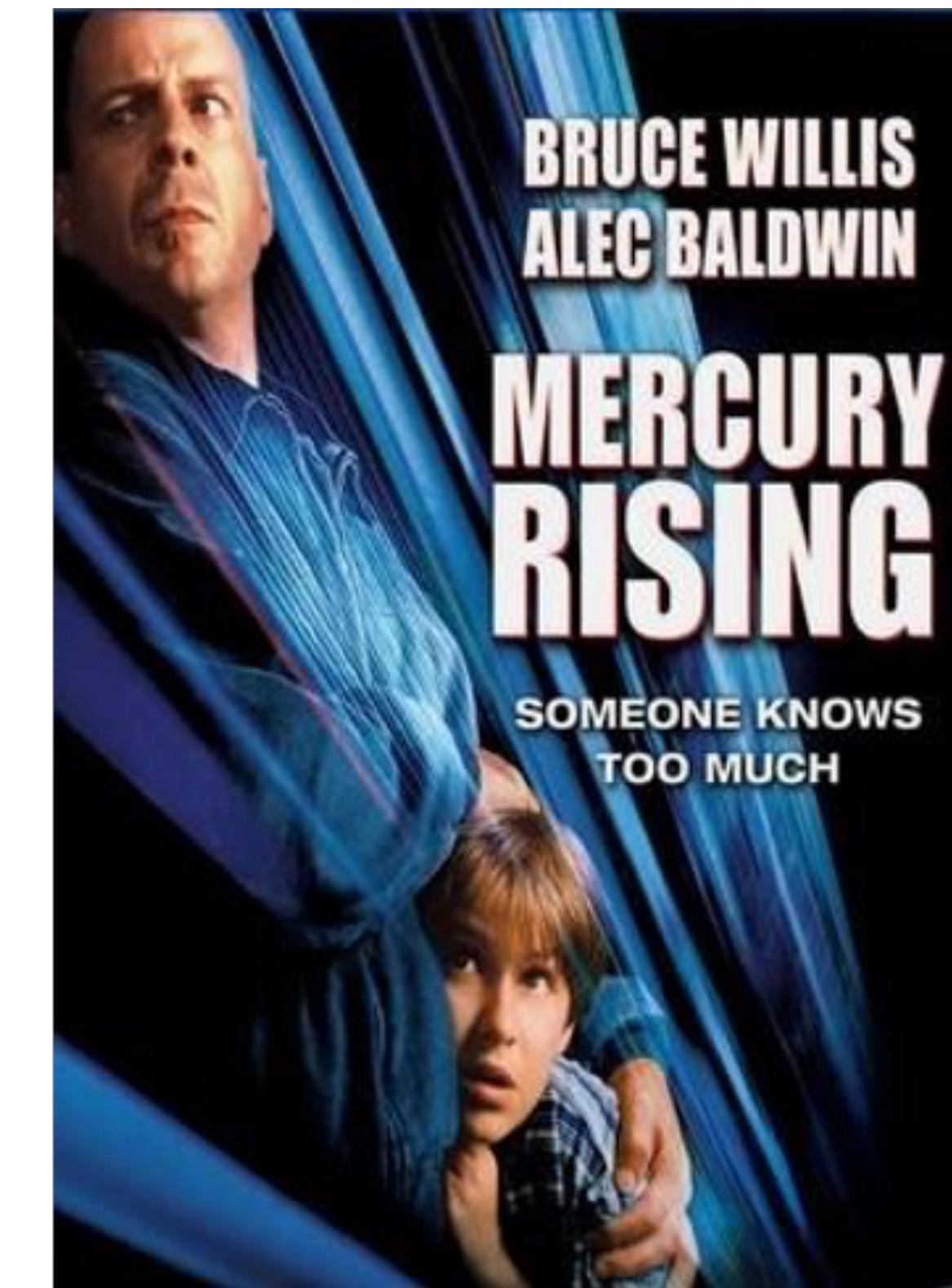
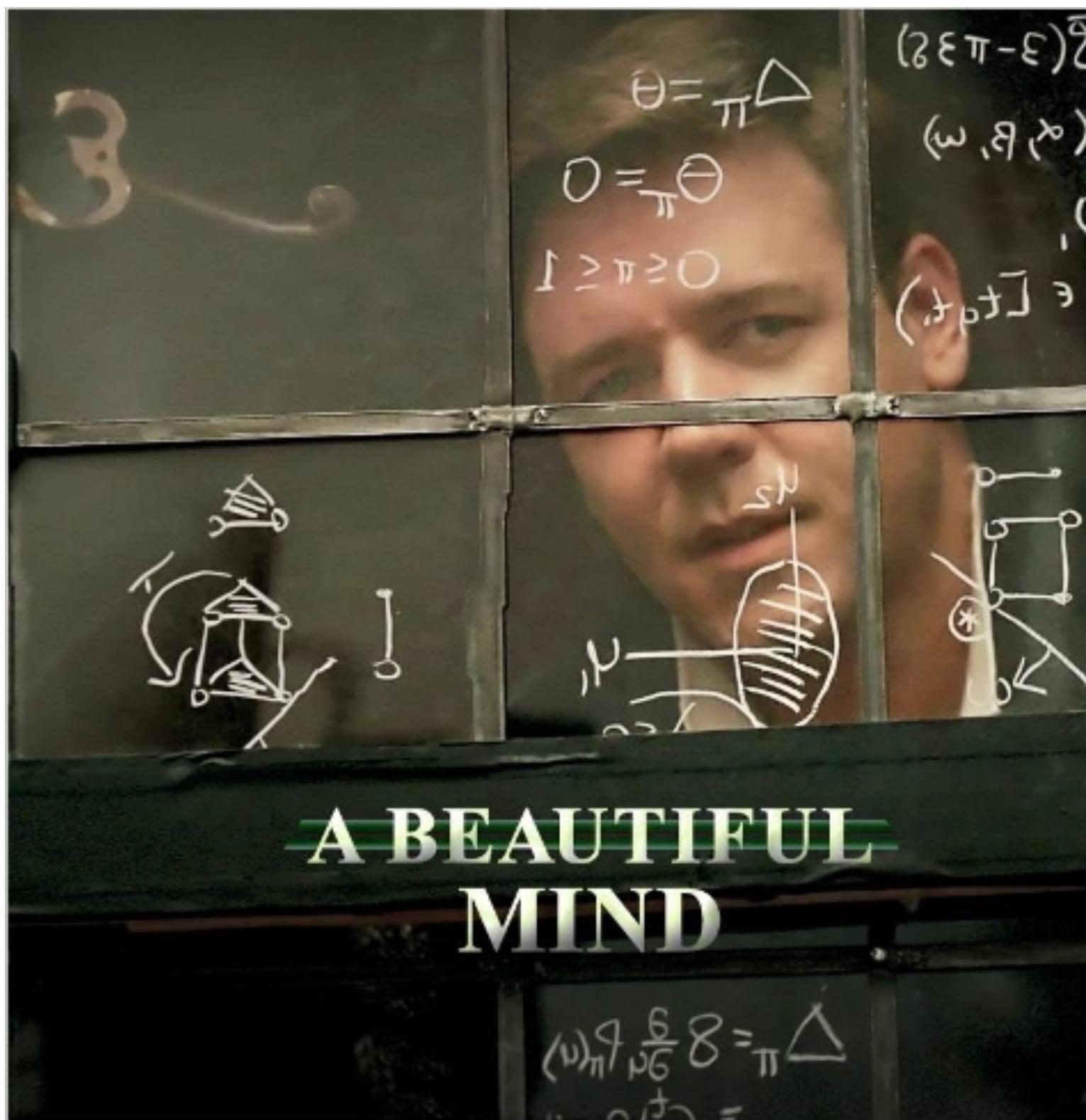
Pesan yang dienkripsi dengan kriptografi menimbulkan kecurigaan bagi pengamat.

Cipherteks dapat dideteksi keberadaannya.

Sejarah Steganografi

- Usia steganografi setua usia kriptografi, dan sejarah keduanya berjalan bersamaan.
- Periode sejarah steganografi dapat dibagi menjadi:
 1. Steganografi kuno (ancient steganography)
 2. Steganografi zaman renaisans (renaissance steganography).
 3. Steganografi zaman perang dunia
 4. Steganografi modern

Steganografi di dalam film



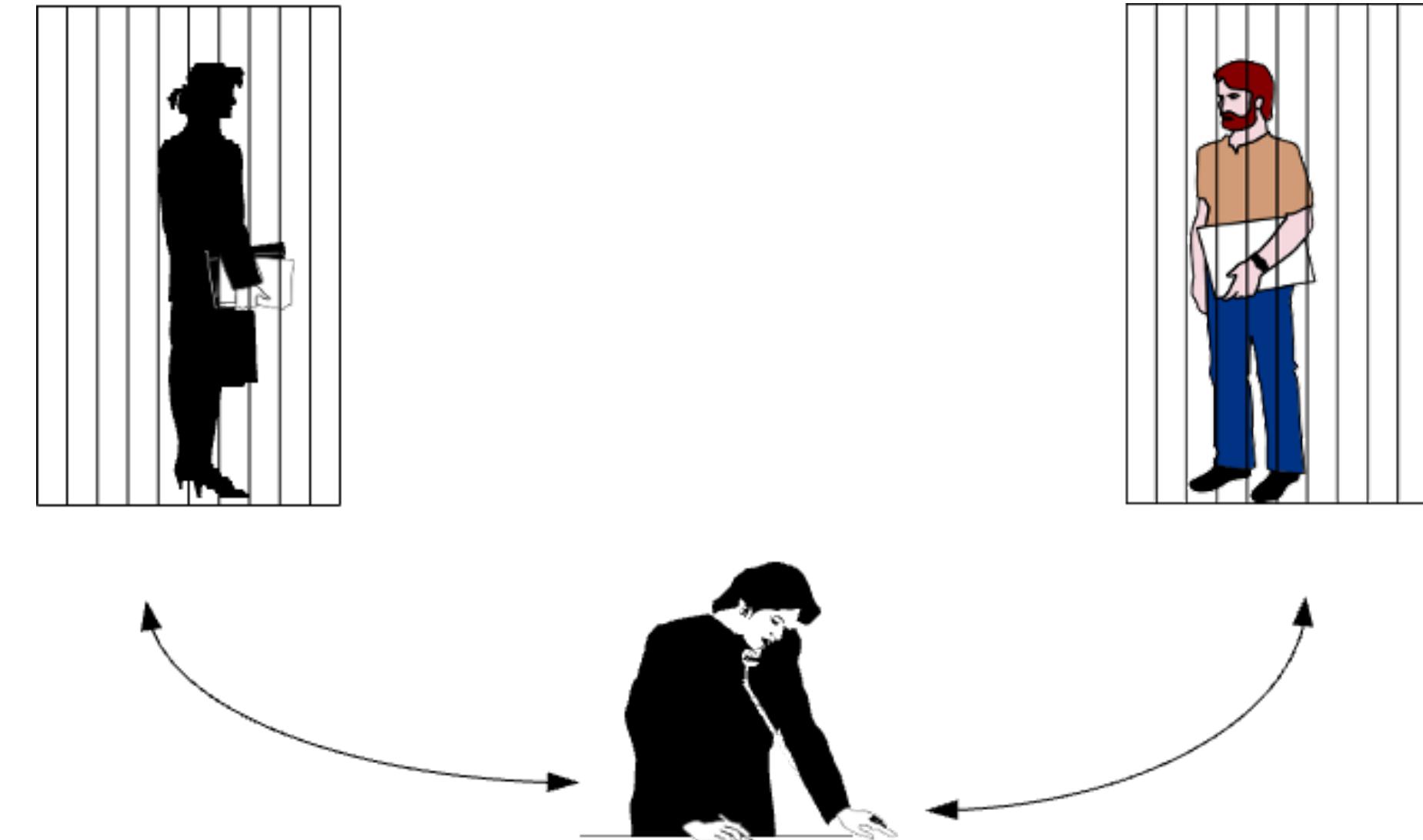
Steganografi dan terorisme

Ilmu steganografi mendadak naik daun ketika pasca 11 September 2001 pihak FBI menuduh Al-Qaidah menggunakan steganografi untuk menyisipkan pesan rahasia melalui video atau gambar yang mereka rilis secara teratur di Internet.



Steganografi Modern - The Prisoner's Problem

- Diperkenalkan oleh Simmons – 1983
- Dilakukan dalam konteks USA – USSR nuclear non-proliferation treaty compliance checking



Pesan rahasia: “ada mata-mata di team”

- Bagaimana cara Bob mengirim pesan rahasia kepada Alice tanpa diketahui oleh Wendy?
- Alternatif 1: mengenkripsinya `xjT#9uvmY!rc$7yt59hth@#`

Wendy pasti curiga!

- Alternatif 2: menyembunyikannya di dalam tulisan lain

masihkah **a**da lara **a**pabila **m**emoriku **i**ngat **n**estapa **i**tu. **k**ita **i**ngin **t**etap
abadikan **k**isah **a**smara. **b**ersamamu **u**siaku **r**enta.

Wendy tidak akan curiga!

Information hiding dengan steganografi!

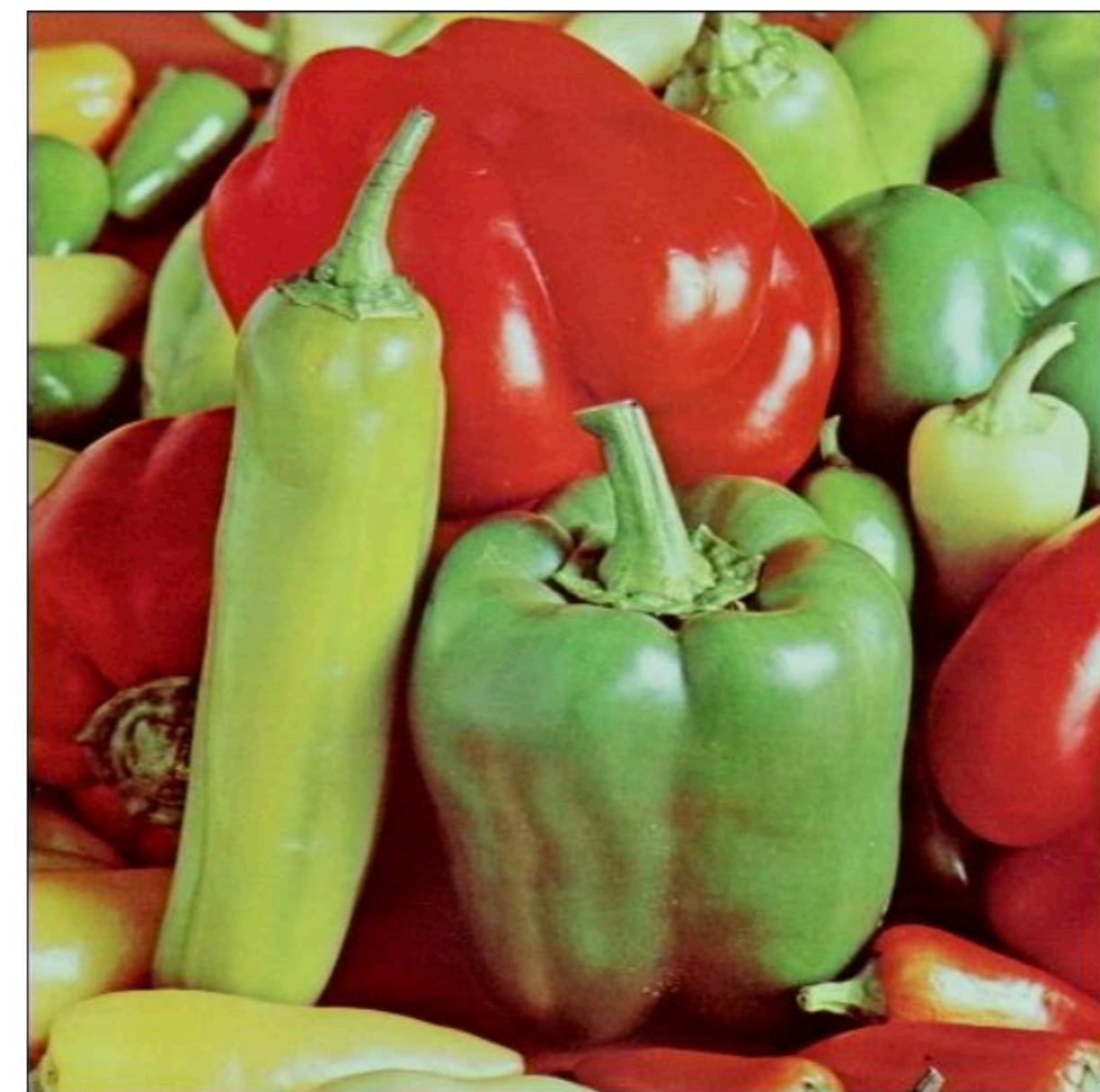
Steganografi Digital

- Steganografi digital: penyembunyian pesan digital di dalam dokumen digital lainnya.
- Carrier file: dokumen digital yang digunakan sebagai media untuk menyembunyikan pesan.

Terminologi Steganografi

1. *Embedded message (hidden text)* atau *secret message*: pesan yang disembunyikan.
Bisa berupa teks, gambar, audio, video, dll
2. *Cover-object (cover text)*: pesan yang digunakan untuk menyembunyikan *embedded message*.
Bisa berupa teks, gambar, audio, video, dll
3. *Stego-object (stego text)*: pesan yang sudah berisi pesan *embedded message*.
4. *Stego-key*: kunci yang digunakan untuk menyisipan pesan dan mengekstraksi pesan dari *stego text*.

Istilah keilmuan serumpun terasa memberikan distorsi persepsi pada maksud sebenarnya. Persepsi yang segera terbentuk dengan istilah tersebut adalah pertumbuhan dari akar-akar ilmu membentuk suatu rumpun, yang berarti bahwa nuansa historis organisasi/kelompok/unit yang mewadahinya.



Embedded message



Cover-image

Stego-image



Cover image

Embedded image



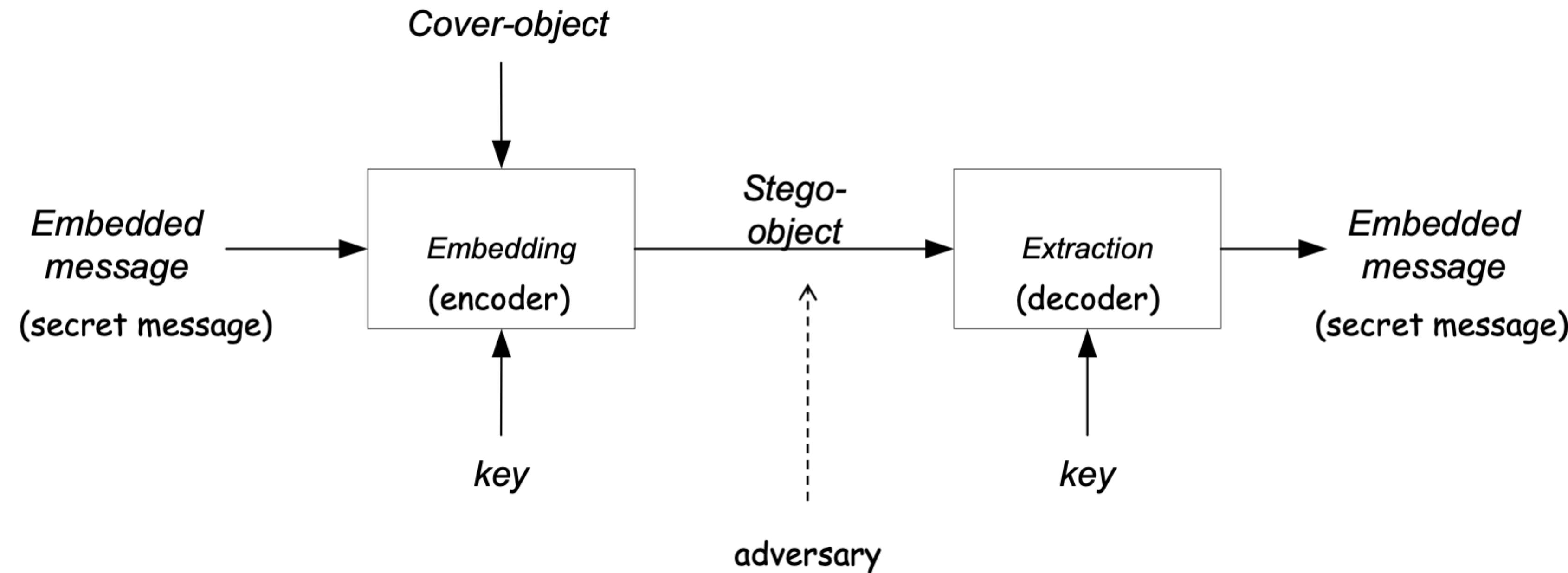


Stego-image

Extracted image



Diagram Proses Steganografi



Kriteria Steganografi yang Bagus

1. Imperceptible → Keberadaan pesan rahasia tidak dapat dipersepsi secara visual atau secara audial
2. Fidelity → Kualitas cover-object tidak jauh berubah akibat penyisipan pesan rahasia.
3. Recovery → Pesan yang disembunyikan harus dapat diekstraksi kembali.
4. Capacity → Ukuran pesan yang disembunyikan sedapat mungkin besar

Catatan: Robustnes bukan isu penting di dalam steganografi

Ranah Steganografi

Berdasarkan ranah operasinya, metode-metode steganografi dapat dibagi menjadi dua kelompok

- *Spatial (time) domain methods*

Memodifikasi langsung nilai byte dari cover-object (nilai byte merepresentasikan intensitas/warna pixel atau amplitudo)

Contoh: Metode LSB

- *Transform domain methods*

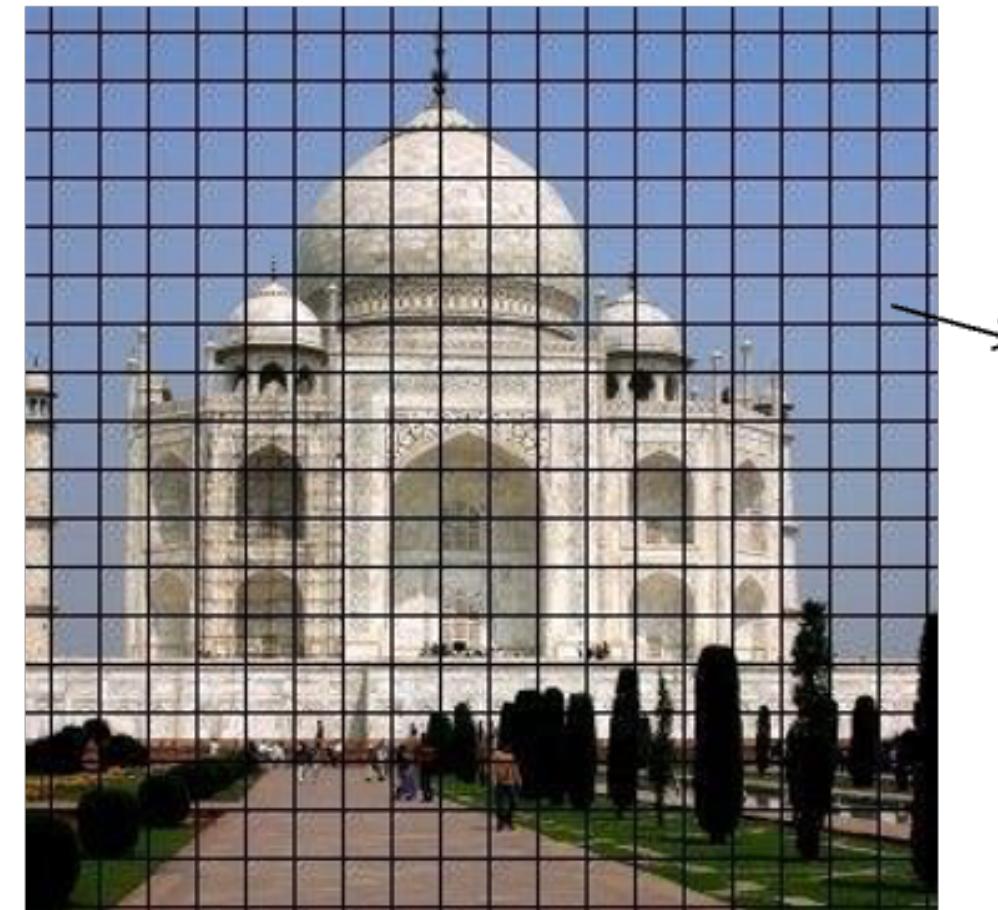
Memodifikasi hasil transformasi sinyal dalam ranah transform (hasil transformasi dari ranah spasial ke ranah lain (misalnya ranah frekuensi)).

Contoh: Metode Spread Spectrum

Metode LSB

Citra Digital

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

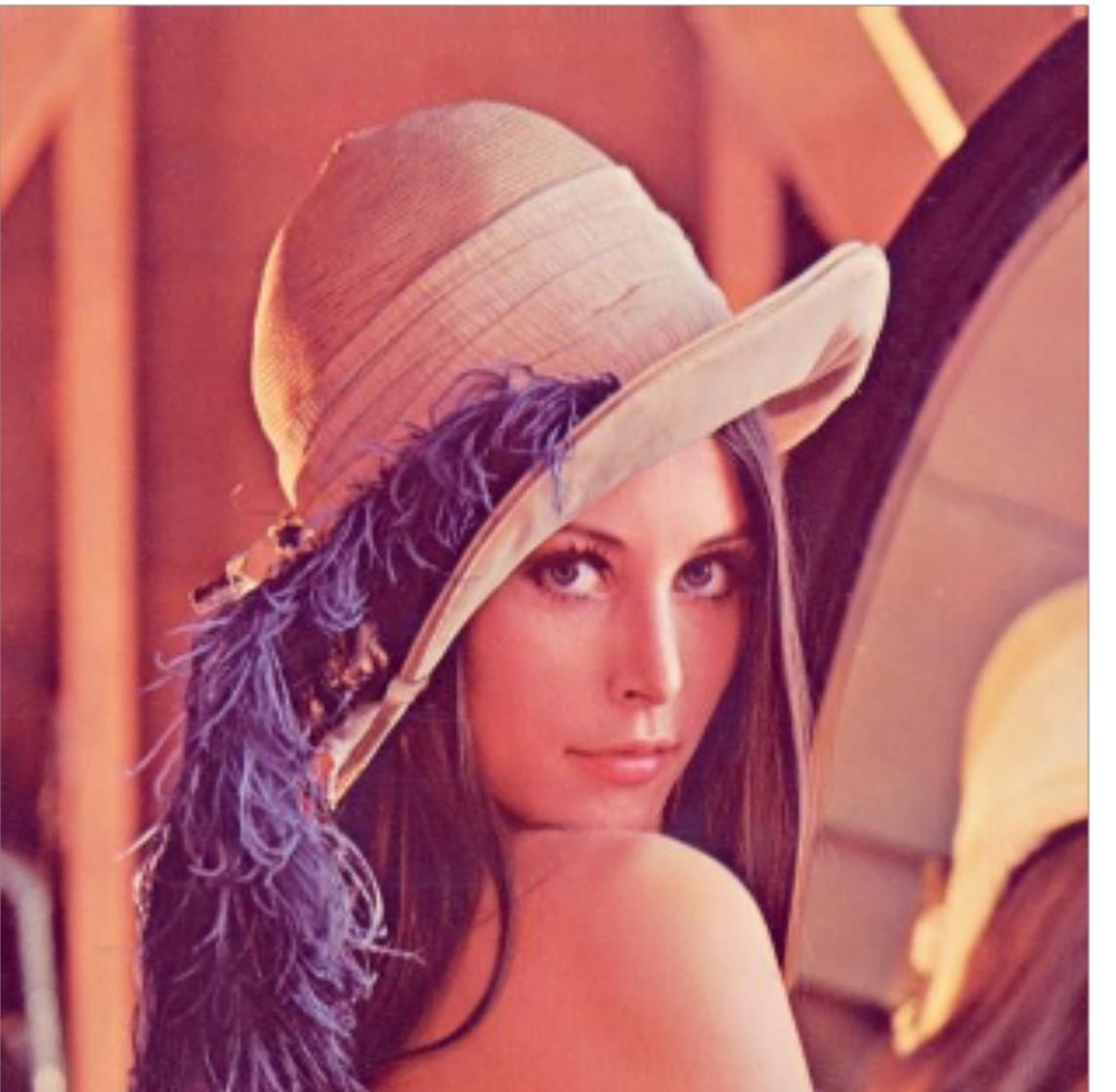


- Setiap pixel panjangnya n-bit.

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)

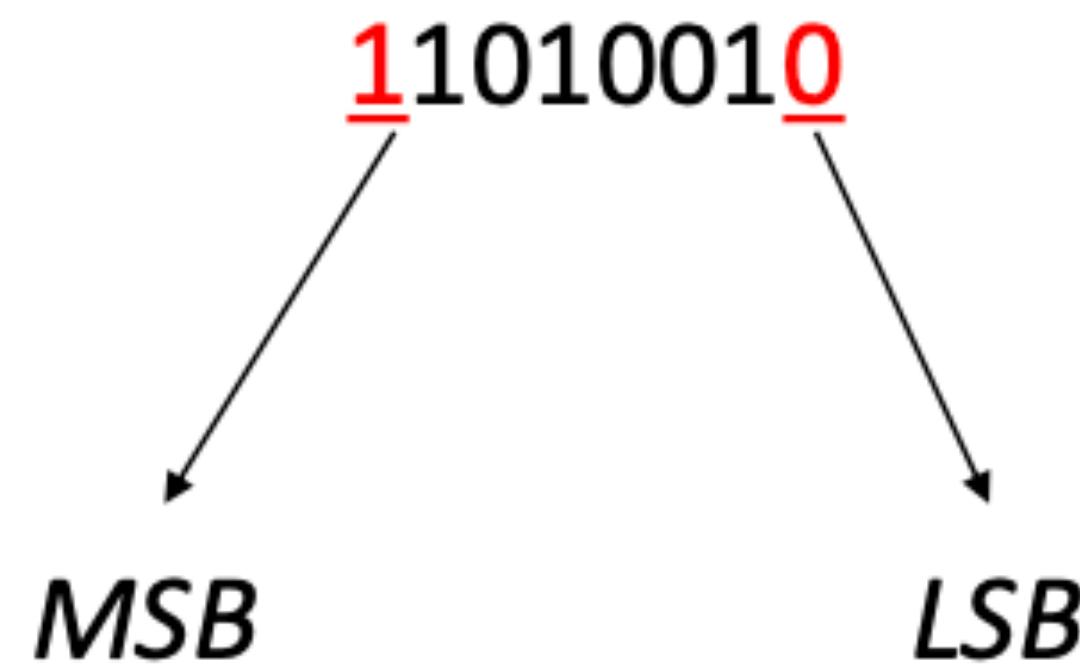


Binary image
(1-bit)

Bitplane pada Citra Digital

- Nilai pixel pada koordinat (x, y) menyatakan intensitas nilai keabuan pada posisi tersebut.
- Pada citra grayscale nilai keabuan itu dinyatakan dalam integer berukuran 1 byte sehingga rentang nilainya antara 0 sampai 255.
- Pada citra berwarna 24-bit setiap pixel tediri atas kanal red, green, dan blue (RGB) sehingga setiap pixel berukuran 3 byte (24 bit).

- Di dalam setiap byte bit-bitnya tersusun dari kiri ke kanan dalam urutan yang kurang berarti (least significant bits atau LSB) hingga bit-bit yang berarti (most significant bits atau MSB).
- Susunan bit pada setiap byte adalah $b_8b_7b_6b_5b_4b_3b_2b_1$. Contoh:



LSB = Least Significant Bit
MSB = Most Significant Bit

Jika setiap bit ke- i dari MSB ke LSB pada setiap *pixel* diekstrak dan diplot ke dalam setiap *bitplane image* maka diperoleh delapan buah citra biner.



Original image



Bitplane 7



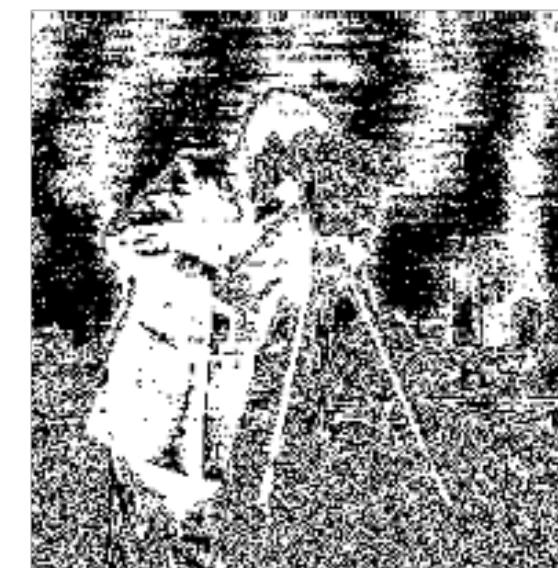
Bitplane 6



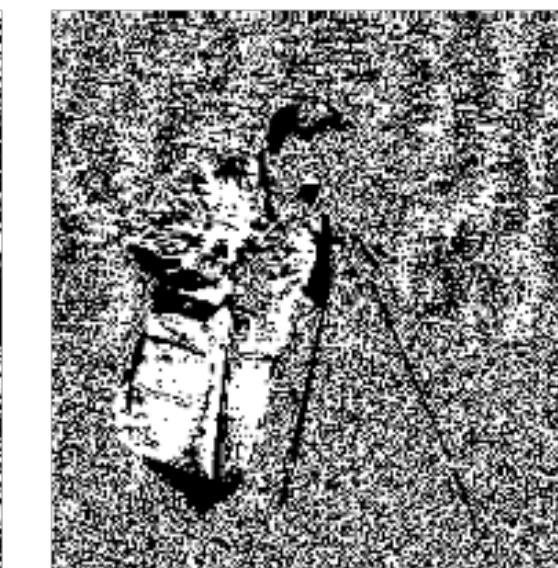
Bitplane 5



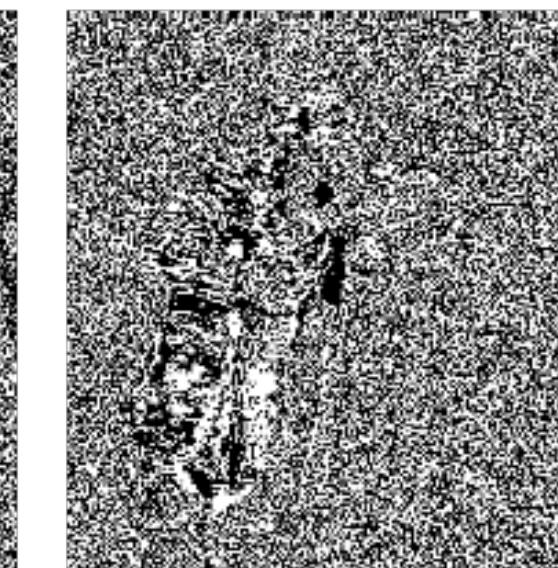
Bitplane 4



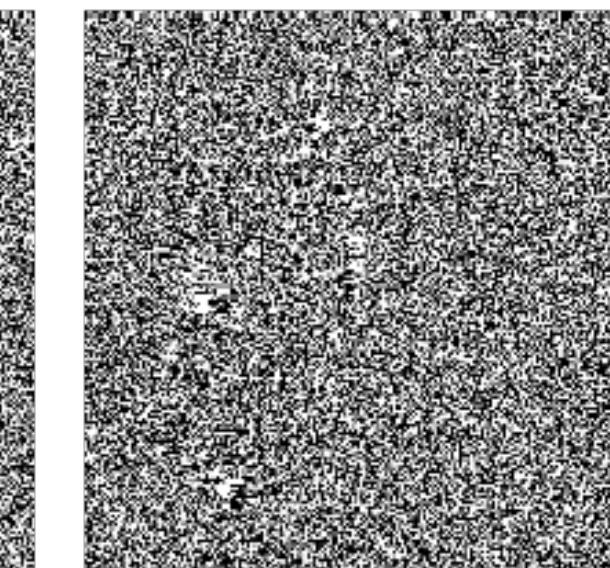
Bitplane 3



Bitplane 2



Bitplane 1



Bitplane 0

- Bitplane LSB, yaitu bitplane 0, terlihat seperti citra acak (random image).
- Bitplane LSB merupakan bagian yang redundan pada citra.
- Artinya, perubahan nilai bit pada bagian tersebut tidak mengubah persepsi citra secara keseluruhan.
- Inilah yang mendasari metode steganografi yang paling sederhana, yaitu metode LSB.

Metode LSB

- Merupakan metode steganografi yang paling populer.
- Memanfaatkan kelemahan indra visual manusia dalam mengamati perubahan sedikit pada gambar
- Caranya: Mengganti bit LSB dari pixel dengan bit pesan.

Mengubah bit LSB hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya → tidak berpengaruh terhadap persepsi visual/auditori

Misalkan semua bit LSB pada citra berwarna dibalikkan dari semula 0 menjadi 1; dari semula 1 menjadi 0



Sebelum



Sesudah

Adakah terlihat perbedaan?

Misalkan semua bit LSB pada citra grayscale dibalikkan Dari semula 0 menjadi 1; dari semula 1 menjadi 0



Adakah terlihat perbedaan?

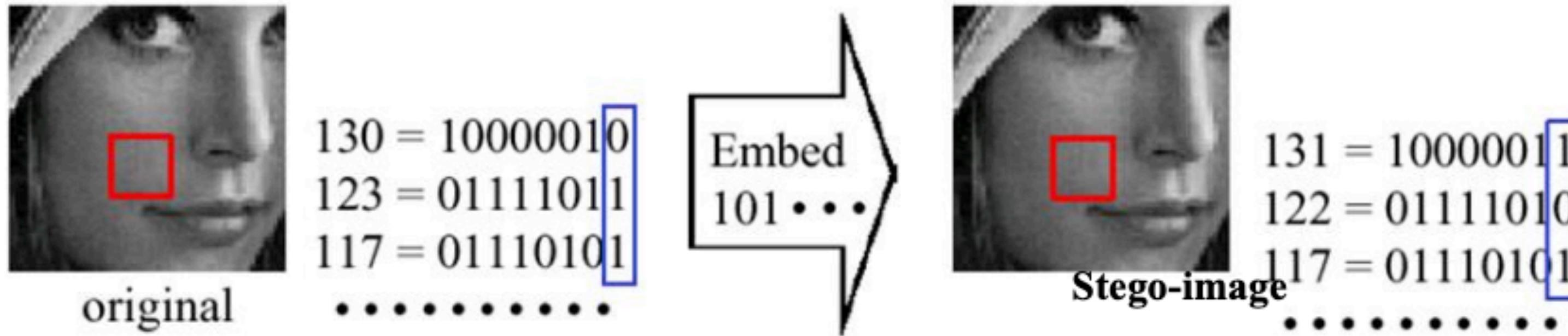
Contoh-1

- Tinjau 1 buah *pixel* dari citra 24-bit (3×8 bit):

10000010 (130)	0111011 (123)	01110101 (117)
---------------------	--------------------	---------------------

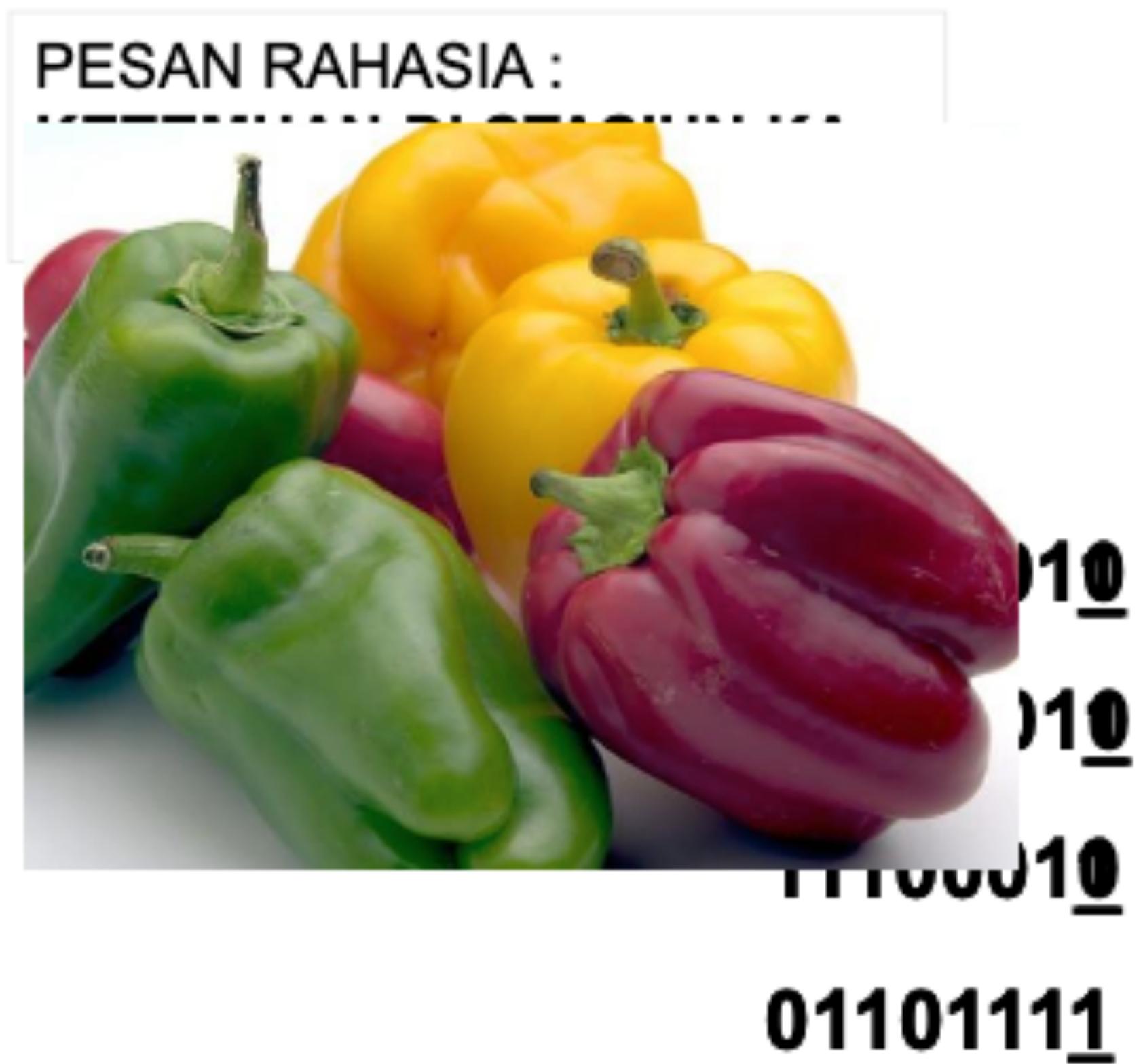
- Bit bit-bit *embedded message*: 101

- Embed*: 00110011 10100010 11100011



Original: misalkan *pixel* [130, 123, 117] berwarna "ungu"
 Stego-image: *pixel* [131, 122, 117] tetap "ungu" tapi berubah sangat sedikit.
 Mata manusia tidak dapat membedakan perubahan warna yang sangat kecil.

Pergeseran warna sebesar 1 dari 256 warna tidak dapat dilihat oleh manusia



Contoh-2

- Jika pesan = 10 bit, maka jumlah *byte* yang digunakan = 10 *byte*

- Contoh susunan *byte* yang lebih panjang:

00110011 10100010 11100010 10101011 00100110
10010110 11001001 11111001 10001000 10100011

- Pesan: 1110010111

- Hasil penyisipan pada bit *LSB*:

00110011 10100011 11100011 10101010 00100110
10010111 11001000 11111001 10001001 10100011

Ekstraksi Pesan dari Stego-image

Bit-bit pesan yang disembunyikan di dalam citra harus dapat diekstraksi kembali.

Caranya adalah dengan membaca byte-byte di dalam citra, mengambil bit LSB nya, dan merangkainya kembali menjadi bit-bit pesan

Contoh: misalkan stego-object sebagai berikut

```
00110011 10100011 11100011 10101010 00100110  
10010111 11001000 11111001 10001001 10100011
```

Ekstrak bit-bit LSB: 1110010111

Menghitung ukuran pesan yang dapat disembunyikan

- Ukuran pesan yang akan disembunyikan bergantung pada ukuran cover-object.
- Misalkan pada citra grayscale (1 byte/pixel) 256 x 256 pixel:
 - Jumlah pixel = jumlah byte = $256 \times 256 = 65536$
 - Setiap byte dapat menyembunyikan 1 bit pesan di LSB
 - Jadi ukuran maksimal pesan = 65536 bit = 8192 byte = 8 KB
- Pada citra berwarna 24-bit berukuran 256 x 256 pixel:
 - Jumlah pixel $256 \times 256 = 65536$
 - Setiap pixel = 3 byte berarti ada $65536 \times 3 = 196608$ byte
 - Setiap byte dapat menyembunyikan 1 bit pesan di LSB
 - jadi ukuran maksimal pesan = 196608 bit = 24576 byte = 24 KB

Beberapa Varian Metode SLB

1. Sequential

- Bit-bit pesan disembunyikan secara sekuensial pada pixel-pixel citra
- Misalkan ukuran pesan = 15 bit, maka urutan pixel-pixel yang digunakan untuk penyembunyian bit adalah

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	
						-	

Sequential - Ekstraksi pesan dari stego-image



- Pada proses ekstraksi pesan, pixel-pixel dibaca secara sekuensial mulai dari pixel pertama sampai pixel yang menyimpan bit pesan terakhir
- Ambil setiap byte dari pixel, ekstraksi bit LSB nya
- Rangkailah bit-bit LSB menjadi bit-bit pesan semula

2. Acak

- Untuk membuat penyembunyian pesan lebih aman, bit-bit pesan tidak disimpan pada pixel-pixel yang berurutan, namun dipilih secara acak
- Pembangkit generator bilangan acak-semu (PRNG: pseudo-random number generator) digunakan untuk membangkitkan bilangan acak.
- Umpan (seed) untuk pembangkit bilangan acak berlaku sebagai kunci (stego-key)
- Misalkan jika terdapat 64 byte dan 15 bit pesan yang akan disembunyikan. Pixel-pixel dipilih secara acak, seperti pada gambar berikut

			5			8
	10				4	
			13		2	
7						9
		1			12	
			15			
11					3	
			6			14

Acak - Ekstraksi pesan dari stego-image

- Posisi pixel yang menyimpan bit pesan dapat diketahui dari bilangan acak yang dibangkitkan oleh PRNG
- Jika kunci yang digunakan pada waktu ekstraksi sama dengan kunci pada waktu penyisipan, maka bilangan acak yang dibangkitkan juga sama
- Dengan demikian, bit-bit pesan yang bertaburan di dalam citra dapat dikumpulkan kembali

3. m-bit LSB

- Untuk meningkatkan ukuran pesan yang disembunyikan, maka digunakan lebih dari 1 bit LSB untuk setiap byte.
- Susunan bit pada setiap byte adalah $b_7b_6b_5b_4b_3b_2b_1b_0$. Jika diambil 2-bit LSB maka bit yang digunakan adalah bit b_1 dan b_0
- Contoh: 11010010 → 2 bit LSB terakhir dipakai untuk menyembunyikan pesan
- Trade-off: semakin banyak bit LSB yang digunakan, semakin besar ukuran pesan yang dapat disembunyikan, tetapi semakin turun kualitas stego-image
- Pesan dapat disembunyikan secara sekuensial atau secara acak pada pixel-pixel di dalam citra

4. Enkripsi

- Pesan dapat dienkripsi terlebih dahulu sebelum disembunyikan ke dalam citra.
- Teknik enkripsi yang sederhana misalnya dengan meng-XOR-kan bit-bit pesan dengan bit-bit kunci. Jumlah bit-bit kunci sama dengan jumlah bit pesan
- Bit-bit kunci dibangkitkan secara acak
- Kunci untuk pembangkitan bit-bit kunci menjadi stego-key
- Jika dipakai teknik acak dalam memilih pixel-pixel, maka dua stego-key: satu untuk pembangkitan bit-bit kunci, satu lagi untuk pembangkitan posisi pixel yang dipilih untuk menyembunyikan pesan

Daftar 100 tools steganografi

<https://www.jjtc.com/Steganography/toolmatrix.htm>

**SELAMAT
BELAJAR**