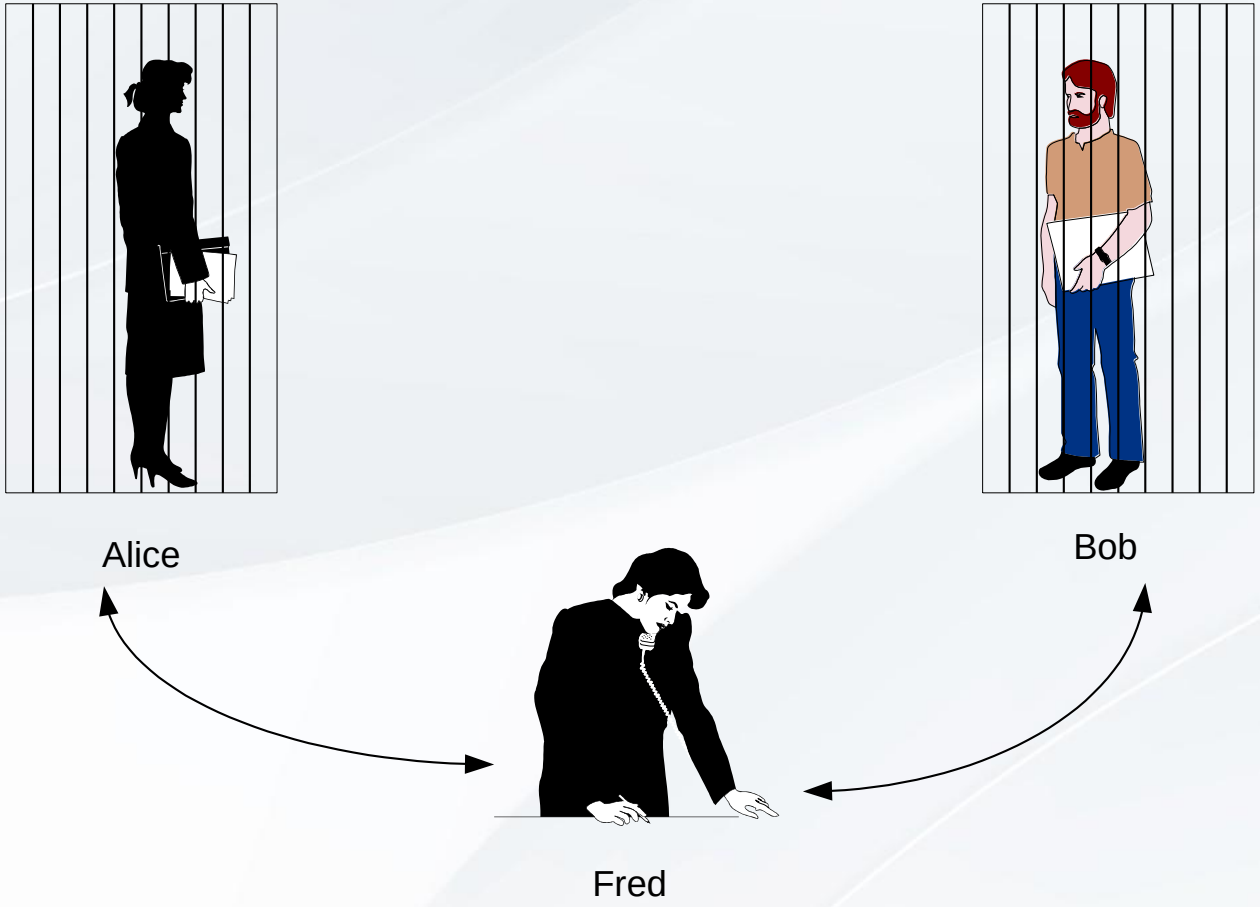
Network Security

Chapter #03

Steganografi

Pengantar: *Prisoner's Problem*



Pesan rahasia: "Lari jam satu"

- Bagaimana Bob mengirim pesan rahasia kepada Alice tanpa diketahui oleh Fred?

- Alternatif 1: mengenkripsinya

xjT#9uvmY!rc$

Fred pasti curiga!

- Alternatif 2: menyembunyikannya di dalam pesan lain

  Lupakan asal rumor itu, jaga agar matamu sehat atau turunkan ubanmu

  Fred tidak akan curiga!

  Information hiding dengan steganografi!

Apa Steganografi itu?

- “steganos” (B.Yunani) ➔ tulisan tersembunyi
  (*covered writing*)

Steganography: ilmu dan seni menyembunyikan (*embedded*) informasi dengan cara menyisipkan pesan rahasia di dalam pesan lain [1].

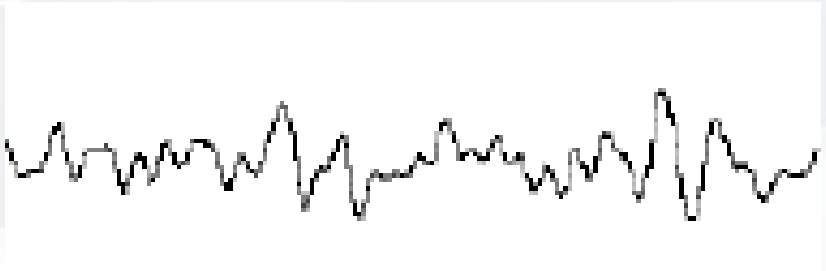
Steganografi digital: steganografi pada data digital dengan menggunakan komputer digital

Pesan (*message*)

1. Teks

   “Kita semua bersaudara”

2. Audio



3. Gambar (*image*)

4. Video

Contoh: Pesan (teks) disembunyikan ke dalam gambar (citra)

PESAN RAHASIA :
LEDAKAN BOM PUKUL 13.00!

Contoh: Pesan (citra) disembunyikan ke dalam citra

Properti Steganografi

1. *Embedded message* (*hiddentext)*: pesan yang disembunyikan.

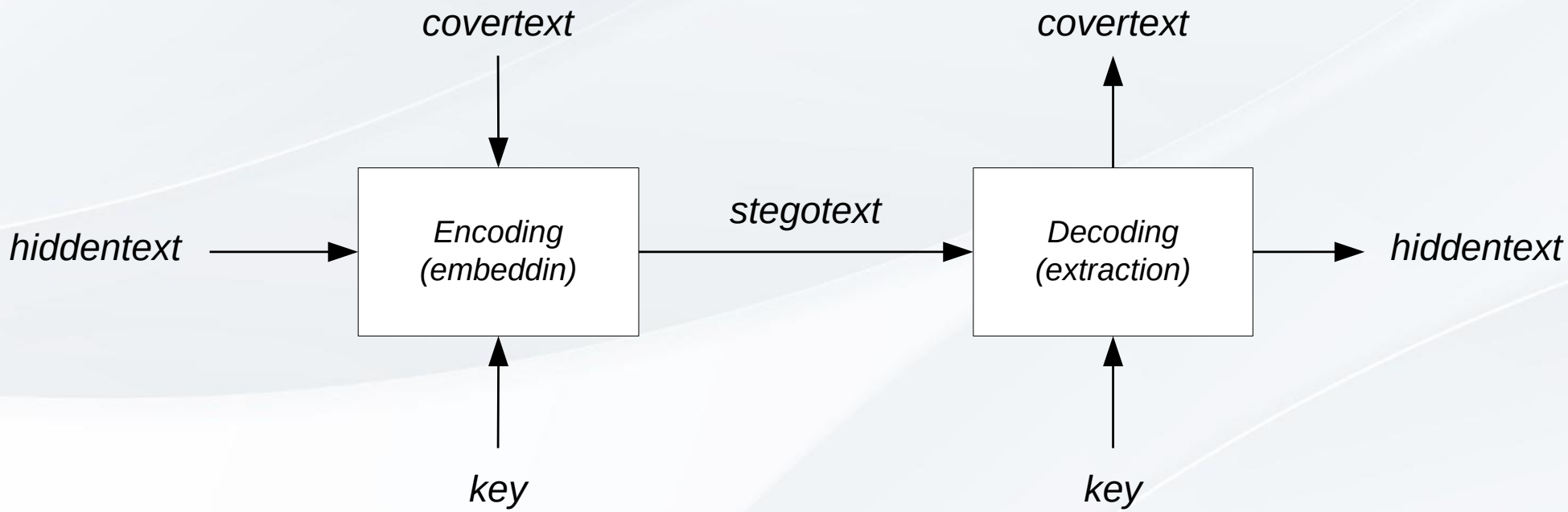
   Bisa berupa teks, gambar, audio, video, dll

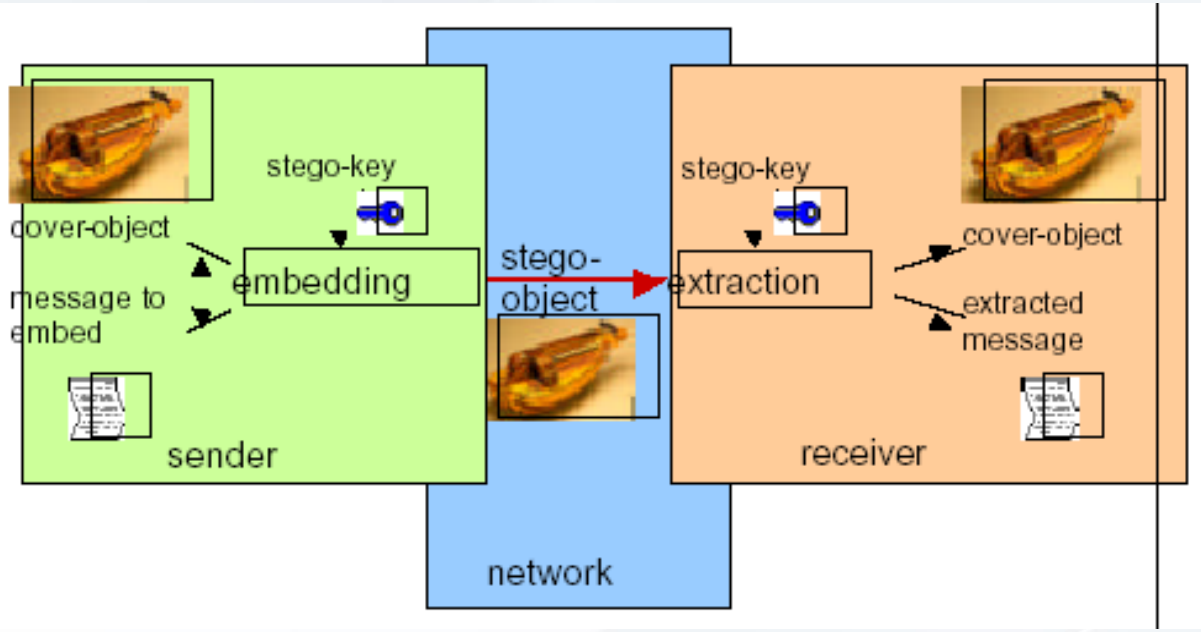
2. *Cover-object* (*covertext):* pesan yang digunakan untuk menyembunyikan *embedded message*.

   Bisa berupa teks, gambar, audio, video, dll

2. *Stego-object* (*stegotext):* pesan yang sudah berisi pesan *embedded message*.

3. *Stego-key*: kunci yang digunakan untuk menyisipan pesan dan mengekstraksi pesan dari stegotext.


covertext
covertext
hiddentext
Encoding
(embeddin)
stegotext
Decoding
(extraction)
hiddentext
key
key


stego-key
cover-object
embedding
message to embed
stego-object
sender
network
stego-key
extraction
cover-object
extracted message
receiver

Contoh-contoh:

Lupakan asal rumor itu, jaga aga matamu sehat atau turunkan ubanmu

Covertext:

upakan sal umor tu aga aga atamu ehat tau turunkan banmu

Hiddentext:

Lari jam satu

Stegotext:

Lupakan asal rumor itu, jaga aga matamu sehat atau turunkan ubanmu

Gerakan **o**rang-**o**rang **d**ari **y**ogya **e**nggan **a**mbil **r**esiko

Covertext:

erakan rang-rang ari ogya nggan mbil esiko

Hiddentext:

Good year

Stegotext:

Gerakan **o**rang-**o**rang **d**ari **y**ogya **e**nggan **a**mbil **r**esiko

http://www.randomhouse.com/doubleday/davinci/

While in Paris on business, Harvard symbologist Robert Langdon receives an urgent late-night phone call. The elderly curator of the Louvre has been murdered inside the museum, a baffling cipher found near the body. As Langdon and a gifted French cryptologist, Sophie Neveu, sort through the bizarre riddles, they are stunned to discover a trail of clues hidden in the works of Da Vinci—clues visible for all to see and yet ingeniously disguised by the painter.

The stakes are raised when Langdon uncovers a startling link: The late curator was involved in the Priory of Sion—an actual secret society whose members included Sir Isaac Newton, Botticelli, Victor Hugo, and Da Vinci, among others. Langdon suspects they are on the hunt for a breathtaking historical secret, one that has proven through the centuries to be as enlightening as it is dangerous. In a frantic race through Paris, and beyond,

(continued on back flap)

(continued from front flap)

Langdon and Neveu find themselves matching wits with a faceless powerbroker who appears to anticipate their every move. Unless they can decipher the labyrinthine puzzle, the Priory's secret—and an explosive ancient truth—will be lost forever.

Breaking the mold of traditional suspense novels, *The Da Vinci Code* is simultaneously lightning-paced, intelligent, and intricately layered with remarkable research and detail. From the opening pages to the unpredictable and stunning conclusion, bestselling author Dan Brown proves himself a master storyteller.

Sumber: http://budi.paume.itb.ac.id

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

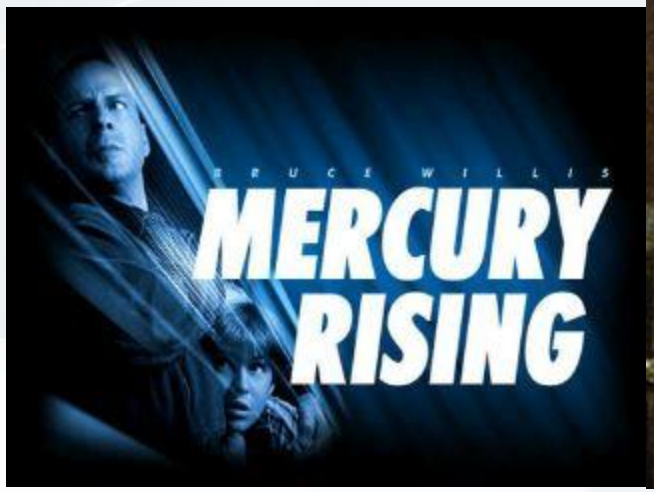
Cover image

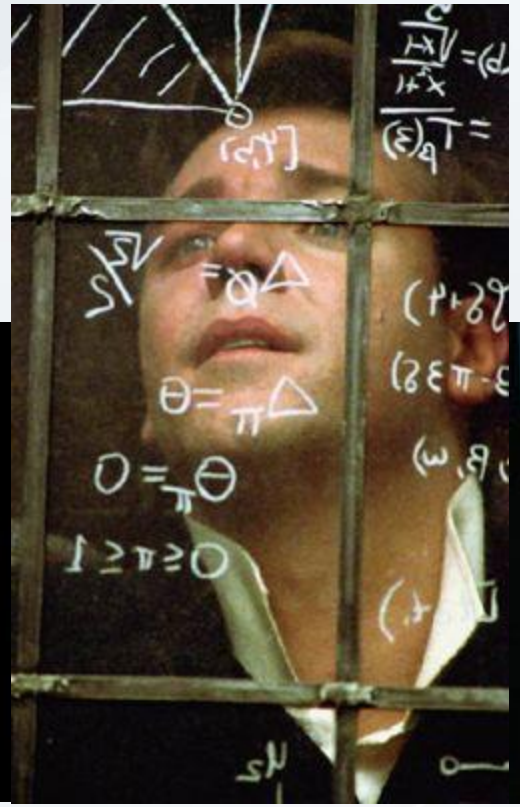
Embedded image

Stego-image

Extracted image

- Steganografi di dalam film *Mercury Rising* dan *Beautiful Mind*





Sumber: http://budi.paume.itb.ac.id

Sejarah Steganografi

- Steganografi dengan media kepala budak (dikisahkan oleh Herodatus, penguasa Yunani pada tahun 440 BC di dalam buku: *Histories of Herodatus*).

  Kepala budak dibotaki, ditulisi pesan, rambut budak dibiarkan tumbuh, budak dikirim. Di tempat penerima kepala budak digunduli agar pesan bsia dibaca.

- Penggunaan tinta tak-tampak (*invisible ink*).

  Tinta dibuat dari campuran sari buah, susu, dan cuka. Tulisan di atas kertas dapat dibaca dengan cara memanaskan kertas tersebut.

Steganografi vs Kriptografi

- Steganografi dapat dianggap pelengkap kriptografi (bukan pengganti).

- Steganografi: menyembunyikan *keberadaan* (*existence*) pesan

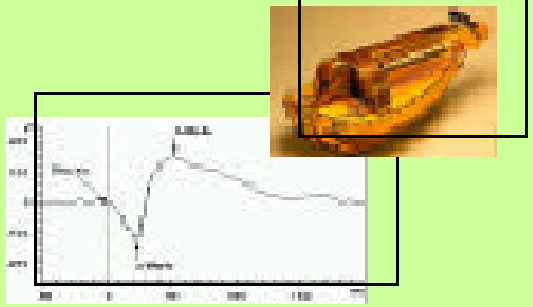
  Tujuan: untuk menghindari kecurigaan (*conspicuous*)

- Kriptografi: menyembunyikan *isi* (*content*) pesan

  Tujuan: agar pesan tidak dapat dibaca

Stego-data are inconspicuous. Steganography will **not be detected**.

George obtains oranges yet eights' are rubbish!



Encrypted messages are conspicuous. They will be detected as ciphertext or silly data.

hIwDIwFpbAtjdf0BA/9KBX2jS17O5SRQsu2PF
caBqUXIQdyt1Fri/Wsg+eXoYsxnJI1Cn2JD7vjl
F2GH8GEr/vGQk8SQVCMyXzfPkgW0tr6RJX
AEIFF9rjnDB3kOmmVc1adrTQnLrqiC/I5r/kUs
ezowgZl82T/QVk59YsuChd+Ce8vql/klCeqmv
w9J2amre3uxpWIOqCEQNzZyHx8HeYPf29k
Xu+uk1gekZZVdELmLD/Wa/xBKFTNUBrl+16
ewoQBxQ8+3cTXSIGPTqdzDSasgQG17Z1sr
/Lhu0qzemi84GYY0OukeiCPvhHJQuXZn2UW

Steganografi vs Kriminal

- Steganografi sering digunakan dalam melakukan komunikasi rahasia antar teroris atau pelaku kriminal.
- Rumor tentang teroris menggunakan steganografi pertama kali ditulis di dalam Harian *USA Today* pada 5 February 2001 dalam dua artikel: "*Terrorist instructions hidden online*" dan "*Terror groups hide behind Web encryption*"

- Latihan: Buat pesan *stegotext* untuk menyembunyikan pesan rahasia:

  “serbu nanti malam”

  dengan ketentuan:

  1. Disembunyikan sebagai huruf awal setiap kata
  2. Disembunyikan sebagai huruf akhir setiap kata

Kriteria Steganografi yang Bagus

1. *Imperceptible*

   Keberadaan pesan rahasia tidak dapat dipersepsi.

2. *Fidelity*.

   Mutu *cover-object* tidak jauh berubah akibat *embedded.*

3. *Recovery*.

   Data yang disembunyikan harus dapat diungkapkan kembali.

   Kriteria *robustness* tidak terlalu penting karena yang utama steganografi bertujuan untuk menghindari kecurigaan (lawan tidak menyadari keberadaan pesan tersembunyi).

Steganografi pada Citra Digital

Teknik yang digunakan:

- *Spatial (time) domain*

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

  Contoh: Metode modifikasi LSB

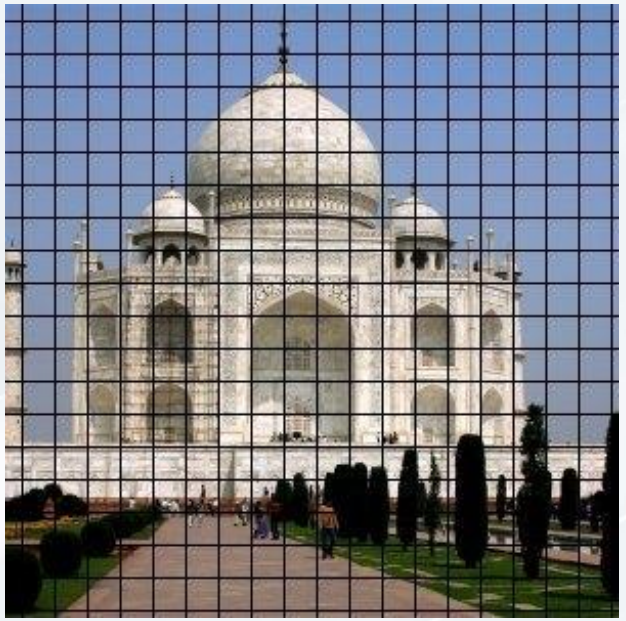
- *Tranform domain*

  Memodifikasi hasil transformasi sinyal dalam ranah frekuensi.

  Contoh: Metode *Spread Spectrum*

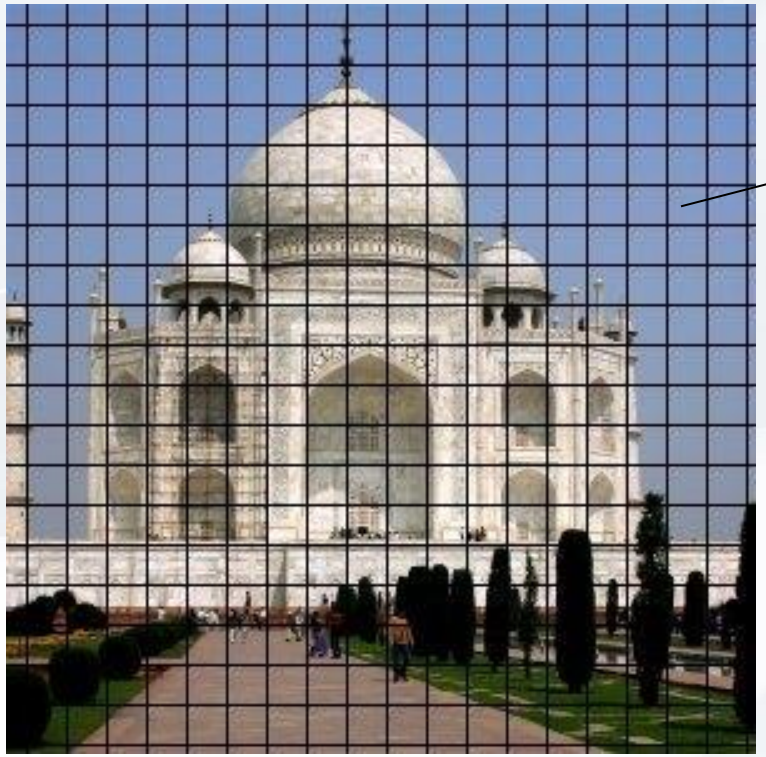
Citra Digital

- Citra terditri atas sejumlah *pixel.* Citra 200 x 150 berarti memiliki 200 x 150 pixel = 30000 pixel



- Setiap *pixel* panjangnya *n*-bit. Contoh: citra 8- bit, citra 24-bit, dsb. Nilai pada setiap pixel menyatakan derajat keabuan.

Pada citra 24-bit (*real image*), 1 pixel = 24 bit, terdiri dari komponen RGB (Red-Green-Blue)



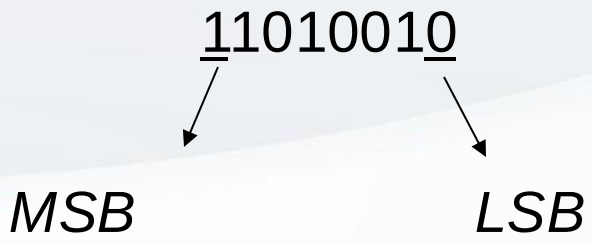
100100111001010010001010

R G B

Metode LSB (spatial domain)

- Memanfaatkan kelemahan indra visual manusia dalam mengamati perubahan sedikit pada gambar

- Caranya: Mengganti bit *LSB* pixel dengan bit data.



LSB = Least Significant Bit
MSB = Most Significant Bit

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

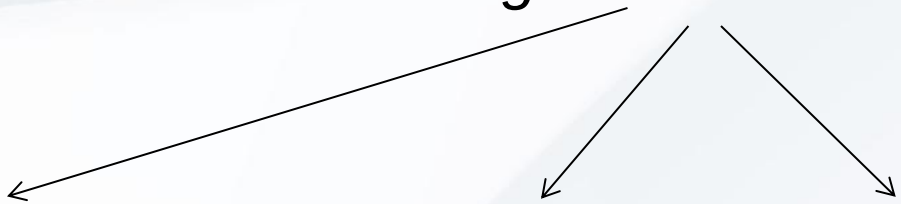
Metode LSB

- Misalkan penyisipan pada citra 24-bit. Setiap *pixel* panjangnya 24 bit (3 x 3 *byte*, masing-masing komponen *R* (1 *byte*), *G* (1 *byte*), dan *B* (1 *byte*))

  00110011 10100010 11100010

  (misalkan *pixel* dipersepsi sebagai warna ungu)

- Misalkan bit-bit *embedded message*: 010



- *Encoding*: 00110010 10100011 11100010

  (*pixel* berwarna “ungu berubah sedikit”, manusia tidak dapat membedakan secara visual dengan citra aslinya)

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

0111

PESAN RAHASIA :
LEDAKAN BOM PUKUL 13.00!

00110011 00110010

10100010 10100011

11100010 11100011

01101111 01101111

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

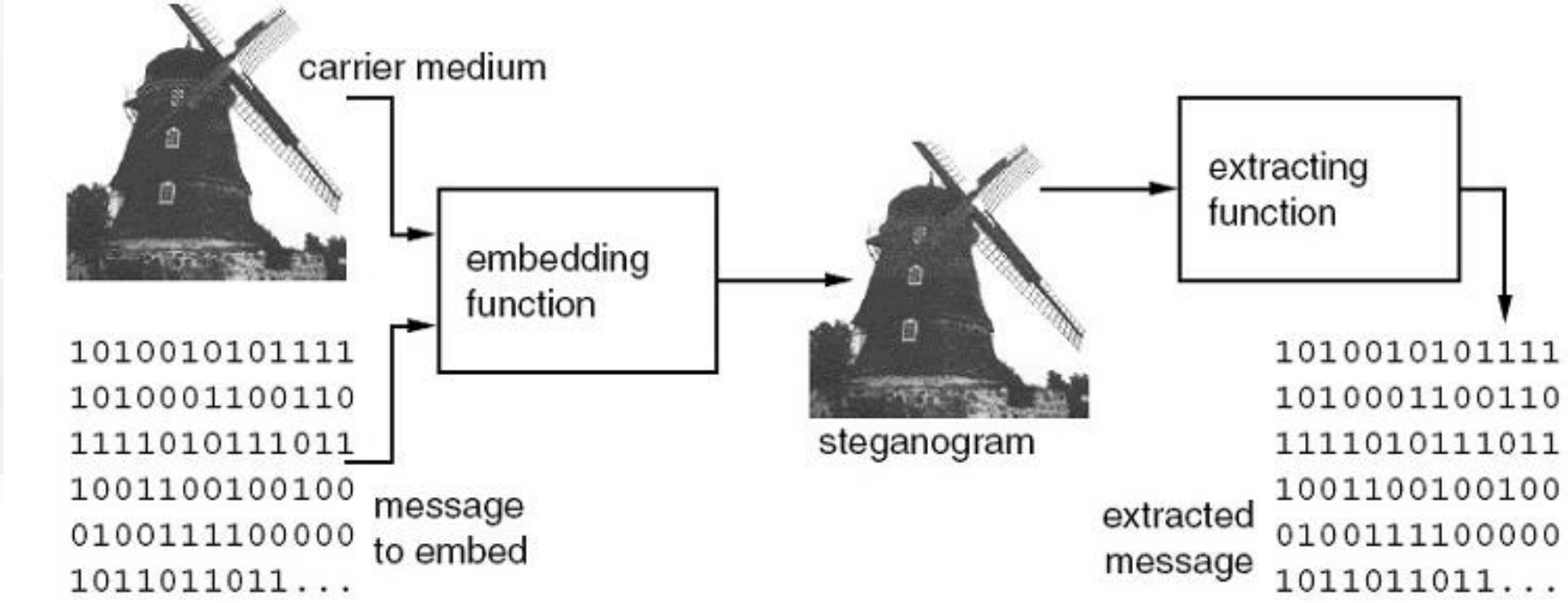
- Contoh susunan *byte* yang lebih panjang:

  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


carrier medium
embedding function
1010010101111
1010001100110
1111010111011
1001100100100
0100111100000
1011011011...
message to embed
steganogram
extracting function
extracted message
1010010101111
1010001100110
1111010111011
1001100100100
0100111100000
1011011011...

- Ukuran data yang akan disembunyikan bergantung pada ukuran *cover-object*.

- Mialkan citra 24-bit ber ukuran 256 $\times$ 256 *pixel* = 65536 *pixel.*

- Setiap *pixel* berukuran 3 *byte* (komponen *RGB*), berarti ada 65536 $\times$ 3 = 196608 *byte*.

- Setiap 1 *byte* menyembunyikan satu bit di *LSB*-nya, maka ukuran data yang dapat disembunyikan:

  196608/8 = 24576 *byte*

- Untuk memperkuat teknik penyembunyian data, bit-bit data rahasia tidak digunakan mengganti *byte-byte* yang berurutan, namun dipilih susunan *byte* secara acak.

- Pembangkit bilangan acak-semu (*PRNG*: *pseudo-random number generator*) digunakan untuk membangkitkan bilangan acak.

- Umpan (*seed*) untuk bilangan acak berlaku sebagai kunci (*stego-key*).

- Misalnya jika terdapat 50 *byte* dan 6 bit data yang akan disembunyikan, maka maka *byte* yang diganti bit *LSB*-nya dipilih secara acak, misalkan *byte* nomor 36, 5, 21, 10, 18, 49.

Ekstraksi pesan dari *Stego-object*

- Pesan yang disembunyikan di dalam citra dapat diungkap kembali dengan mengekstraksinya.

- Posisi *byte* 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 data rahasia yang bertaburan di dalam citra dapat dikumpulkan kembali.

Program Stegano *shareware*

1. InPlainView:
   http://www.simtel.net/product.php%5Bid%5D12796%5BSiteID%5Dsimtel.net

   Keterangan: hanya untuk citra .bmp

1. S-tools

   http://digitalforensics.champlain.edu/download/s-tools4.zip

   Keterangan: untuk citra GIF dan BMP. Pesan dienkripsi terlebih dahulu.

Steganalisis

- Steganalisis: Ilmu dan seni untuk mendeteksi ada-tidaknya pesan tersembunyi dalam suatu objek.

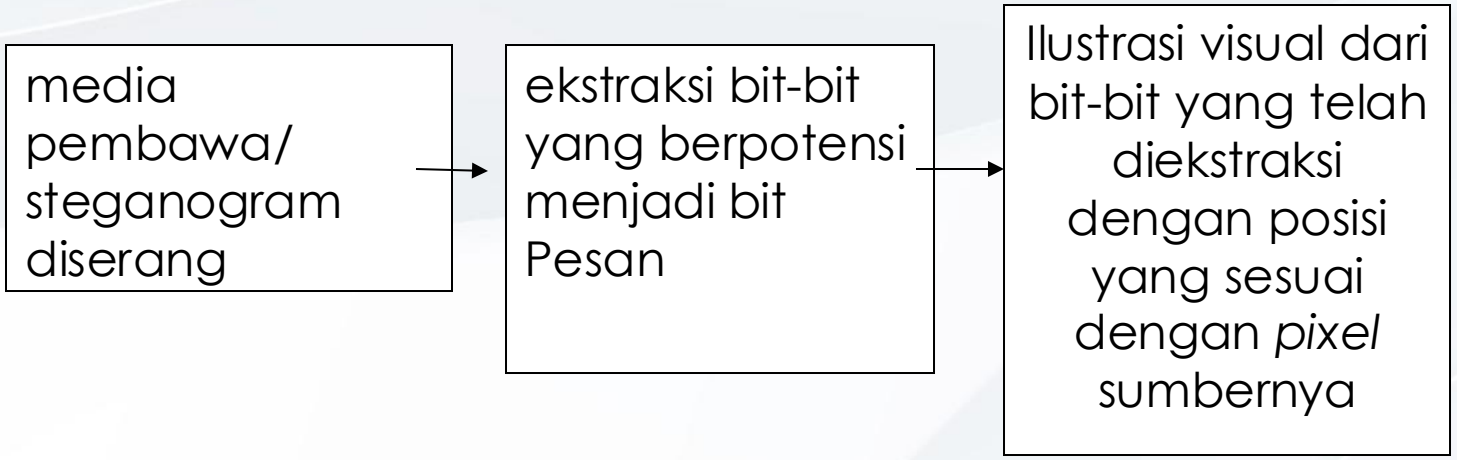
- Steganalisis untuk metode *LSB:*
  - Metode subjektif melibatkan indera penglihatan manusia.
    contoh: *enhanced LSB*

  - Metode statistik melibatkan analisis matematis.
    contoh : uji *chi-square* dan *RS-analysis*

Enhanced LSB

- Memanfaatkan indera penglihatan → inspeksi kerusakan pada gambar akibat penyisipan [WES99]

- Ide dasar :



Enhanced LSB (2)

BLUE	GREEN	RED
1010010**1**	1001110**0**	1110011**1**

BLUE	GREEN	RED
11111111	**00000000**	**11111111**

Setelah melalui proses penyaringan, maka citra pada bagian gambar yang tidak disisipi pesan akan mendekati bagian gambar semula. Sedangkan bagian gambar yang mengandung pesan rahasia akan menjadi ”rusak” setelah disaring. Dengan demikian, dari gambar yang dihasilkan setelah penyaringan, mata manusia dapat dengan mudah membedakan apakah pada gambar tersebut terdapat pesan rahasia atau tidak.

INSTITUT TEKNOLOGI DAN BISNIS STIKOM BALI

INSTITUT TEKNOLOGI DAN PENDIDIKAN MARKANDEYA BALI

Kampus Merdeka INDONESIA JAYA

Single Degree Program

S2 - Sistem Informasi (M.Kom.)
S1 - Sistem Komputer (S.Kom.)
S1 - Sistem Informasi (S.Kom.)
S1 - Teknologi Informasi (S.Kom.)
S1 - Bisnis Digital (S.Bns.)
D3 - Manajemen Informatika (A.Md.Kom.)

Dual Degree International Program

S1 - Sistem Informasi (S.Kom., B.IT.)
(collaboration with HELP University)
S1 - Bisnis Digital (S.Bns., B.M.)
(collaboration with DNUI University)

Dual Degree National Program

S1 - Sistem Informasi (S.Kom., S.Ds.)
(collaboration with Universitas Teknologi Bandung)

www.stikom-bali.ac.id info@stikom-bali.ac.id (0361) 244445

STIKOMERS TV STIKOM Bali @stikombali

Always The First