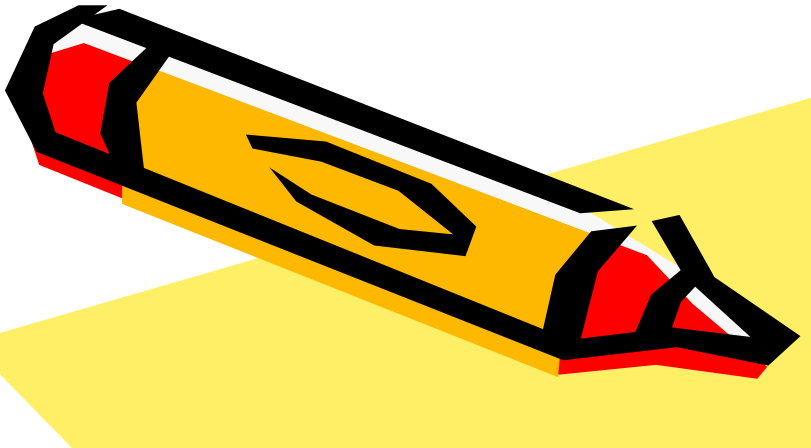
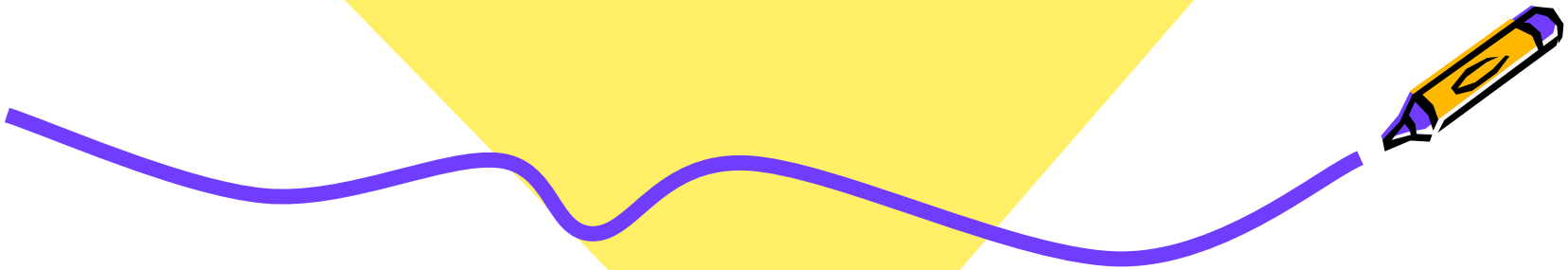
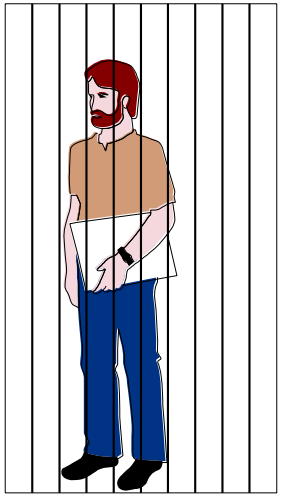


Steganografi

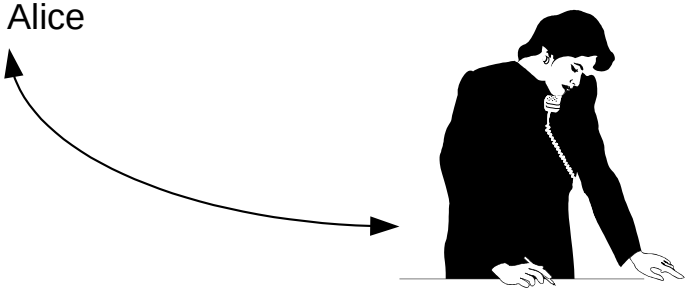


Pengantar: *Prisoner's Problem*



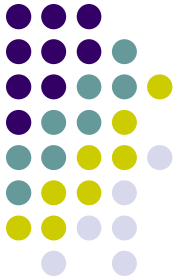
Alice

Bob



Fred

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 aku 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 di dalam pesan lain [1].

Steganografi digital: steganografi pada data digital dengan menggunakan komputer digital

Pesan (*message*)

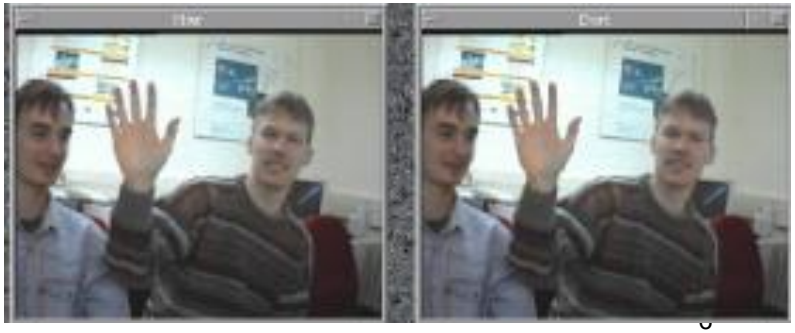
1. Teks

   “Torang semua bersodara”

2. Audio

3. Gambar (*image*)

4. Video



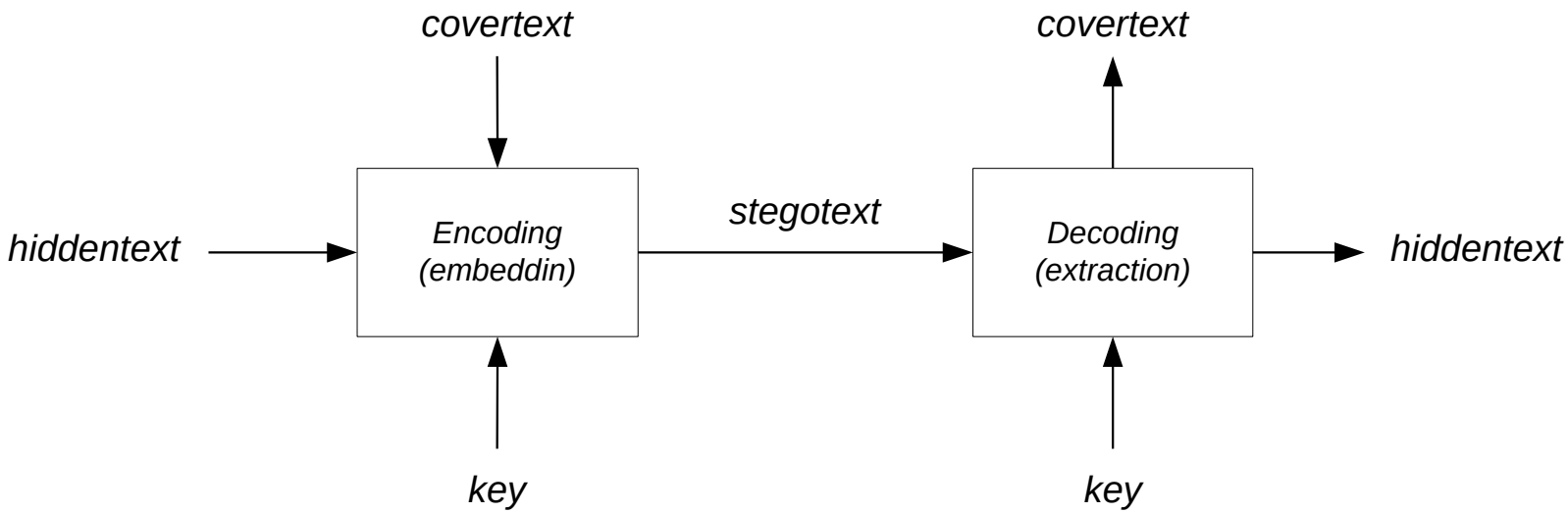
Properti Steganografi

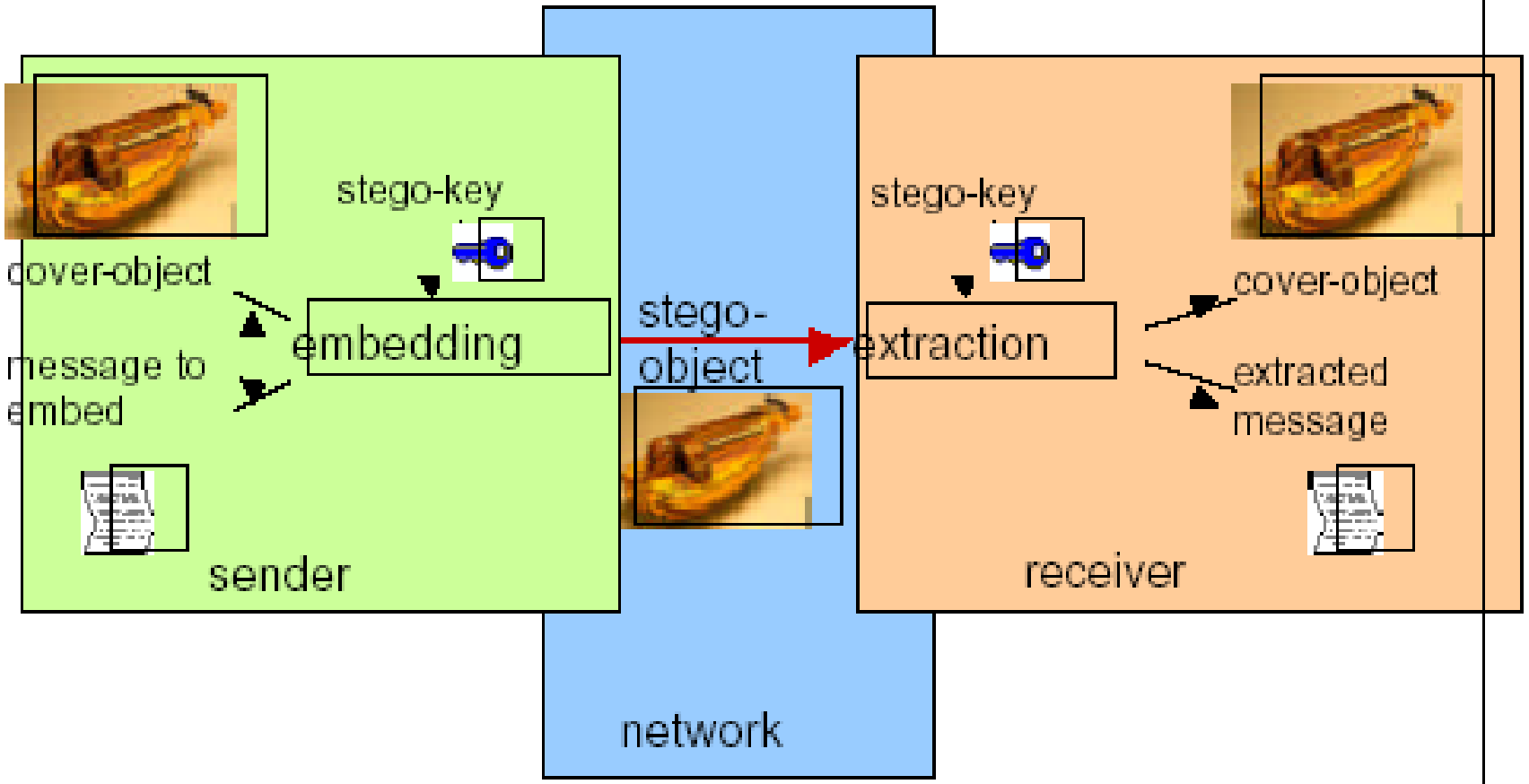
1. *Embedded message* (*hiddentext)*: pesan yang disembunyikan.

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

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

4. *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
sender
stego-object
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)

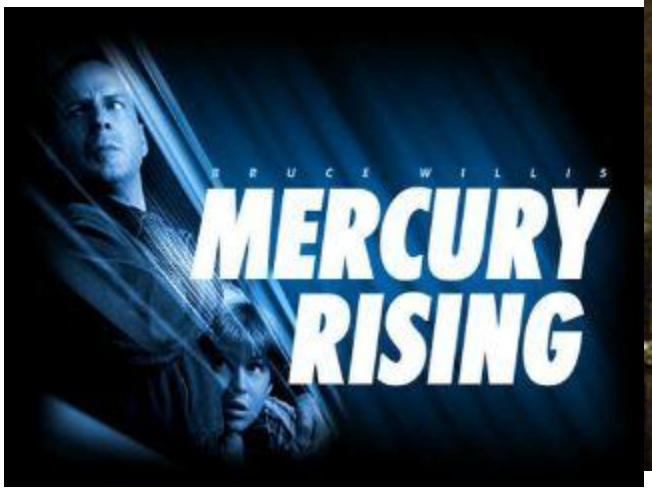
Langdon and Neveu find themselves matching wits with a faceless powerbroker who appears to anticipate their every move. Unless they can decipher the labyrinthine puzzle, the Priory's secret—and an explosive ancient truth—will be lost forever.

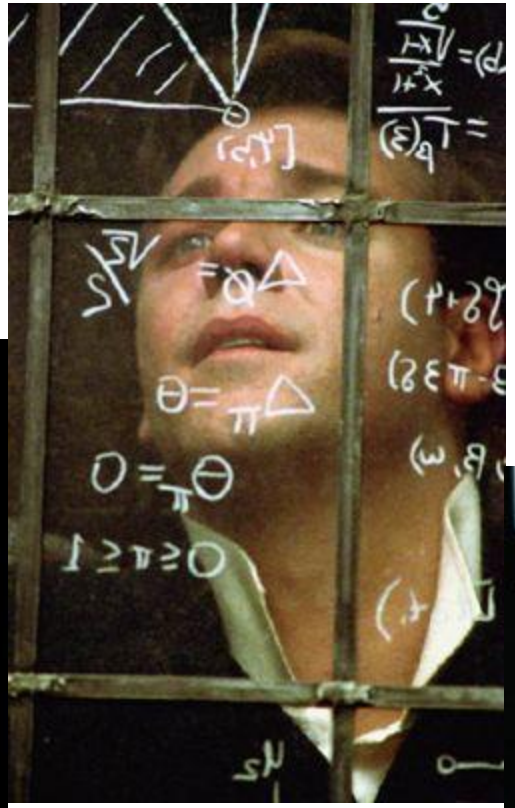
Breaking the mold of traditional suspense novels, *The Da Vinci Code* is simultaneously lightning-paced, intelligent, and intricately layered with remarkable research and detail. From the opening pages to the unpredictable and stunning conclusion, bestselling author Dan Brown proves himself a master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

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





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

Sejarah Steganografi

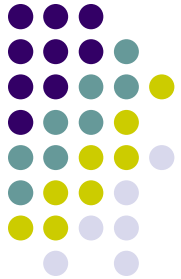
- Steganografi dengan media kepala budak (Herodatus, penguasa Yunani).

  Kepala budak dibotaki, ditulisi pesan, rambut budak dibiarkan tumbuh, budak dikirim.

- 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

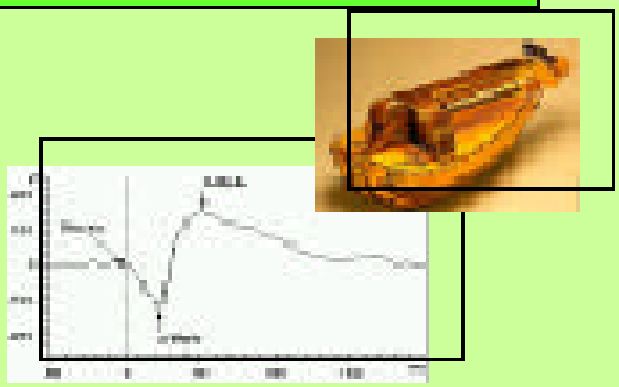
  Tujuan: untuk menghindari kecurigaan (*conspicuous*)

- 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/9KBX2jS17O5SRQsL2PF
caBqUXIQdyt1Fri/Wsg+eXoYsxnJI1Cn2JD7vjl
F2GH8GEr/vGQk8SQVCMyXzfPkgW0tr6RJX
AEIFF9rjnDB3kOmmVc1adrTQnLrqiC/I5r/kUs
ezowgZI82T/QVk59YsuChd+Ce8vql/klCeqmv
w9J2amre3uxpWIOqCEQNzZyHx8HeYPf29k
Xu+uk1gekZZVdELmLD/Wa/xBKFTNUBrI+16
ewoQBxQ8+3cTXSIGPTqdzDSasgQG17Z1sr
/Lhu9qzam64GYY0OukeiCPvhHJQuXZn2UW

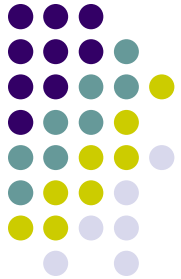
- Latihan: Buat pesan *stegotext* untuk menyembunyikan pesan rahasia:

  “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).

Teknik yang Digunakan

- *Spatial (time) domain*

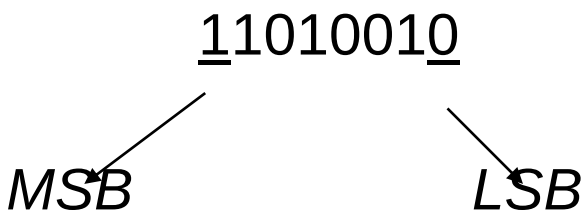
  Memodifikasi langsung nilai *byte* dari *cover-object* (nilai *byte* dapat merepresentasikan intensitas/warna *pixel* atau amplitudo)

- *Tranform domain*

  Memodifikasi hasil transformasi sinyal dalam ranah frekuensi.

Metode LSB (spatial domain)

Mengganti bit *LSB* dengan bit data.

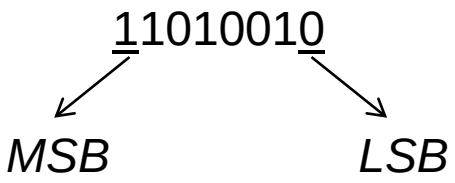


LSB = Least Significant Bit

MSB = Most Siginificant Bit

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

- Mengganti bit *LSB* dengan bit data.



LSB = Least Significant Bit
MSB = Most Siginificant Bit

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

- Contoh

  Nilai Asal :

  11010010 = 210 (desimal)
- LSB : 1101001**1** = 211
- MSB : **0**1010010 = 82

- Pesan asal: “aku#” akan disembunyikan di dalam image 6x6

196	10	97	182	101	40
67	200	100	50	90	50
25	150	45	200	75	28
176	56	77	100	25	200
101	34	250	40	100	60
44	66	99	125	190	200

- Pesan: aku dalam kode ascii adalah : 97 107 117 35, dan dalam kode biner:

a 97 1100001

k 107 1101011

u 117 1110101

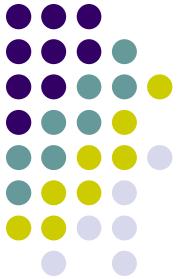
35 0100011

- Covertex

196	10	97	182	101	40
67	200	100	50	90	50
25	150	45	200	75	28
176	56	77	100	25	200
101	34	250	40	100	60
44	66	99	125	190	200

- Dalam kode biner

11000100	00001010	01100001	10110110	01100101	00101000
01000011	11001000	01100100	00110010	01011010	00110010
00011001	10010110	00101101	11001000	01001011	00011100
10110000	00111000	01001101	01100100	00011001	11001000
01100101	00100010	11111010	00101000	01100100	00111100
00101100	01000010	01100011	01111101	10111110	11001000



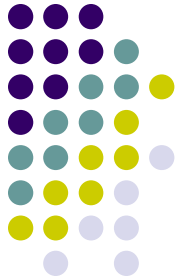
- Embed pesan di dalam cover (LSB diganti dengan text pesan)

11000101	00001011	01100001	10110111	01100100	00101000
01000011	11001001	01100101	00110010	01011010	00110010
00011000	10010111	00101101	11001001	01001011	00011100
10110000	00111000	01001101	01100100	00011001	11001000
01100100	00100011	11111011	00101001	01100100	00111100
00101100	01000010	01100010	01111100	10111110	11001000

11000101	00001011	01100001	10110111	01100100	00101000
01000011	11001001	01100101	00110010	01011010	00110010
00011000	10010111	00101101	11001001	01001011	00011100
10110000	00111000	01001101	01100100	00011001	11001000
01100100	00100011	11111011	00101001	01100100	00111100
00101100	01000010	01100010	01111100	10111110	11001000

- Diubah ke kode desimal menjadi

197	11	97	183	100	40
67	201	101	50	90	50
24	151	45	201	75	28
176	56	77	100	25	200
100	35	251	41	100	60
44	66	98	124	190	200



- Before

196	10	97	182	101	40
67	200	100	50	90	50
25	150	45	200	75	28
176	56	77	100	25	200
101	34	250	40	100	60
44	66	99	125	190	200

- After

197	11	97	183	100	40
67	201	101	50	90	50
24	151	45	201	75	28
176	56	77	100	25	200
100	35	251	41	100	60
44	66	98	124	190	200

Metode LSB

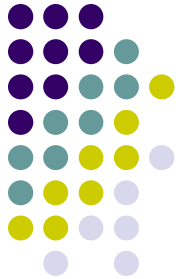
- Misalkan penyisipan pada citra 24-bit.
- Setiap *pixel* panjangnya 24 bit (3 x 3 *byte*, masing-masing komponen *R* (1 *byte*), *G* (1 *byte*), dan *B* (1 *byte*))

  00110011 10100010 11100010
  (misal *pixel* berwarna merah)

- Misalkan *embedded message*: 010

- *Encoding*:

  00110010 10100011 11100010
  (*pixel* berwarna “merah berubah sedikit”, tidak dapat dibedakan secara visual dengan citra aslinya)



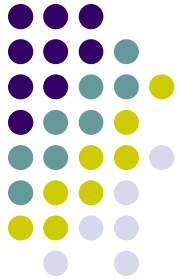
- Jika pesan = 10 bit, maka jumlah *byte* yang digunakan = 10 *byte*

- 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

Metode LSB



- Ukuran data yang akan disembunyikan bergantung pada ukuran *cover-object*.
- Citra 24-bit 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*

LSB

- 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.

LSB

- Keuntungan

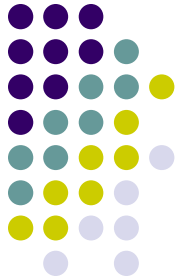
  Mudah diimplementasikan dan proses *encoding* cepat

- Kelemahan

  Tidak tahan terhadap pengubahan (modifikasi) terhadap *cover object.*

  Mudah dihapus karena lokasi penyisipan diketahui (bit LSB)

Tranform Domain



- Sinyal dalam ranah spasial/waktu diubah ke ranah frekuensi dengan menggunakan transformasi seperti
  - *DCT* (*Discrete Cosine Transform*),
  - *DFT* (*Discrete Fourier Transform*), dan
  - *DWT* (*Discrete Wavelet Trabform*)

- Penyisipan pesan dilakukan pada koefisien tranformasi.

- Keuntungan: kokoh (*robust*) terhadap manipulasi pada *stego-object*.

- *DCT*: $C(p,q) = \alpha_p \alpha_q \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} I(m,n) \cos \frac{\pi(2m+1)p}{2N} \cos \frac{\pi(2n+1)q}{2N}$
- *IDCT*: $I(m,n) = \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} \alpha_p \alpha_q C(p,q) \cos \frac{\pi(2m+1)p}{2N} \cos \frac{\pi(2n+1)q}{2N}$
- Keterangan: Citra berukuran *M* x *N*

$$0 \le p \le M-1 \qquad 0 \le q \le N-1$$

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}} & , p = 0 \\ \sqrt{\frac{2}{M}} & , 1 \le p \le M-1 \end{cases} \qquad \alpha_q = \begin{cases} \frac{1}{\sqrt{N}} & , q = 0 \\ \sqrt{\frac{2}{N}} & , 1 \le q \le N-1 \end{cases}$$

- Penyisipan dilakukan pada koefisien *DCT*, yaitu *C(p, q)*

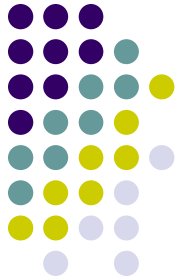
- Misalkan semua koefisien *DCT* disimpan di dalam vektor/larik *v*[1..*n*]

- Pesan yang akan disembunyikan (dalam biner) adalah

  $X = x_1 x_2 \ldots x_m$

  dikodekan sebagai barisan {–1, +1} dengan pemetaan:

$$b_i = \begin{cases} 1 & , x_i = 1 \\ -1 & , x_i = 0 \end{cases}$$

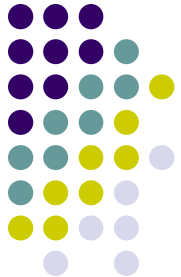


- Posisi penyisipan pesan dapat ditentukan secara acak atau pada posisi berurutan
- Penyisipan pesan dengan formula: $\hat{v}_i = v_i + \alpha b_i$
- α dipilih sedemikian sehingga tidak merusak *content* sinyal semula. Nilai α antara 0 dan 1.

- Selanjutnya dilakukan *IDCT* untuk mengembalikan sinyal dalam ranah frekuensi ke ranah spasial/waktu.

- Metode lain yang berbasis *tranform domain*: *spread spectrum steganography*.

Steganalisis



- Steganalisis: Ilmu dan seni untuk mendeteksi ada-tidaknya pesan tersembunyi dalam suatu objek.
- Steganalisis adalah ilmu yang mempelajari karakteristik penyembunyian suatu data pada media (steganografi) dan bagaimana cara untuk mendeteksi bahkan sampai membongkar data tersembunyi tersebut.
- 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*