Bahan kuliah IF4020 Kriptografi

Steganografi
(Bagian 3)

Oleh: Dr. Rinaldi Munir

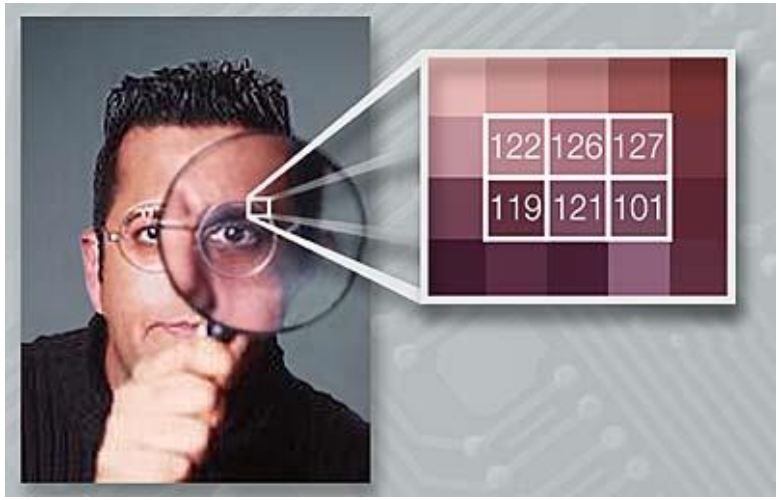
Prodi Informatika

Sekolah Teknik Elektro dan Informatika

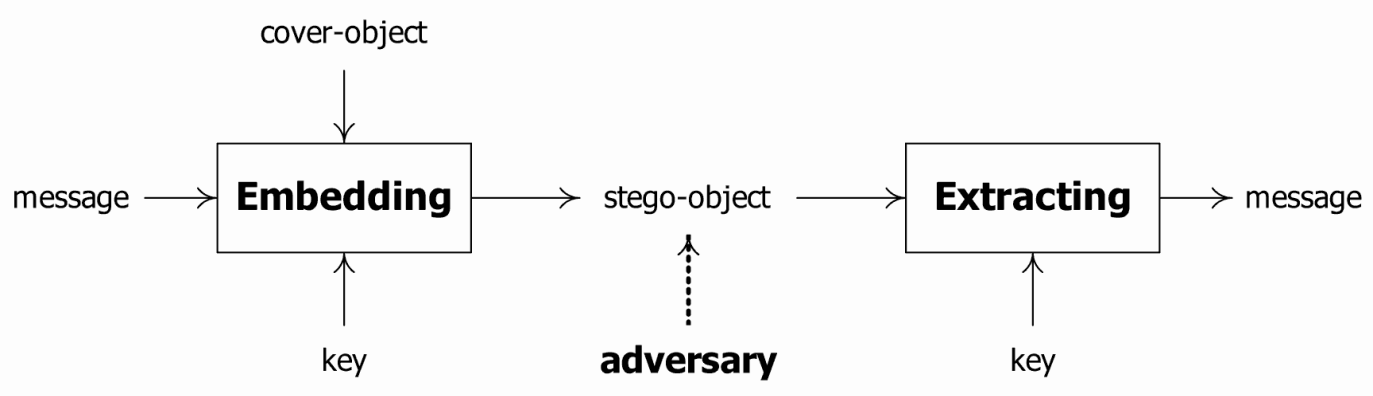
Pengantar Steganalisis

Steganalysis

- Tujuan: menentukan apakah sebuah media *suspect* mengandung pesan tersembunyi



- Steganografi



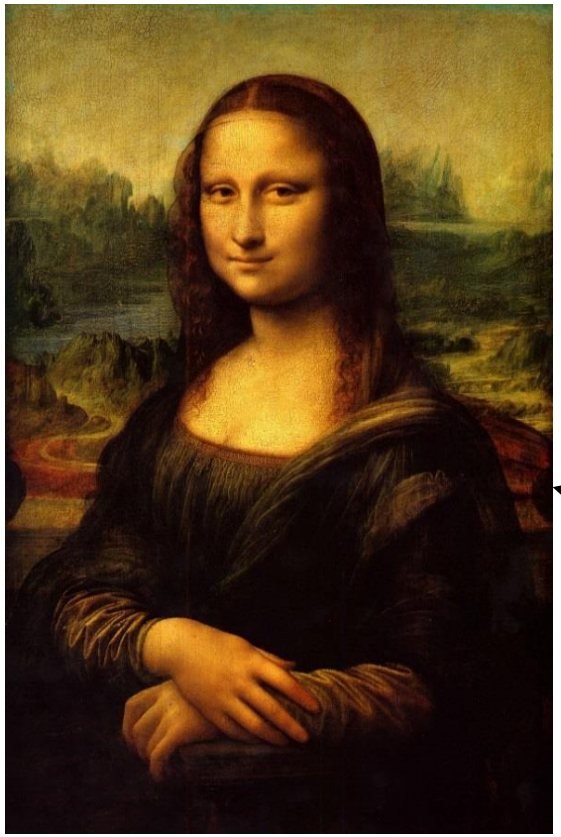
- Steganalisis

*) Keterangan: 1 jika ada pesan tersembunyi, 0 jika tidak

Fakta: Gambar-gambar bertebaran di internet

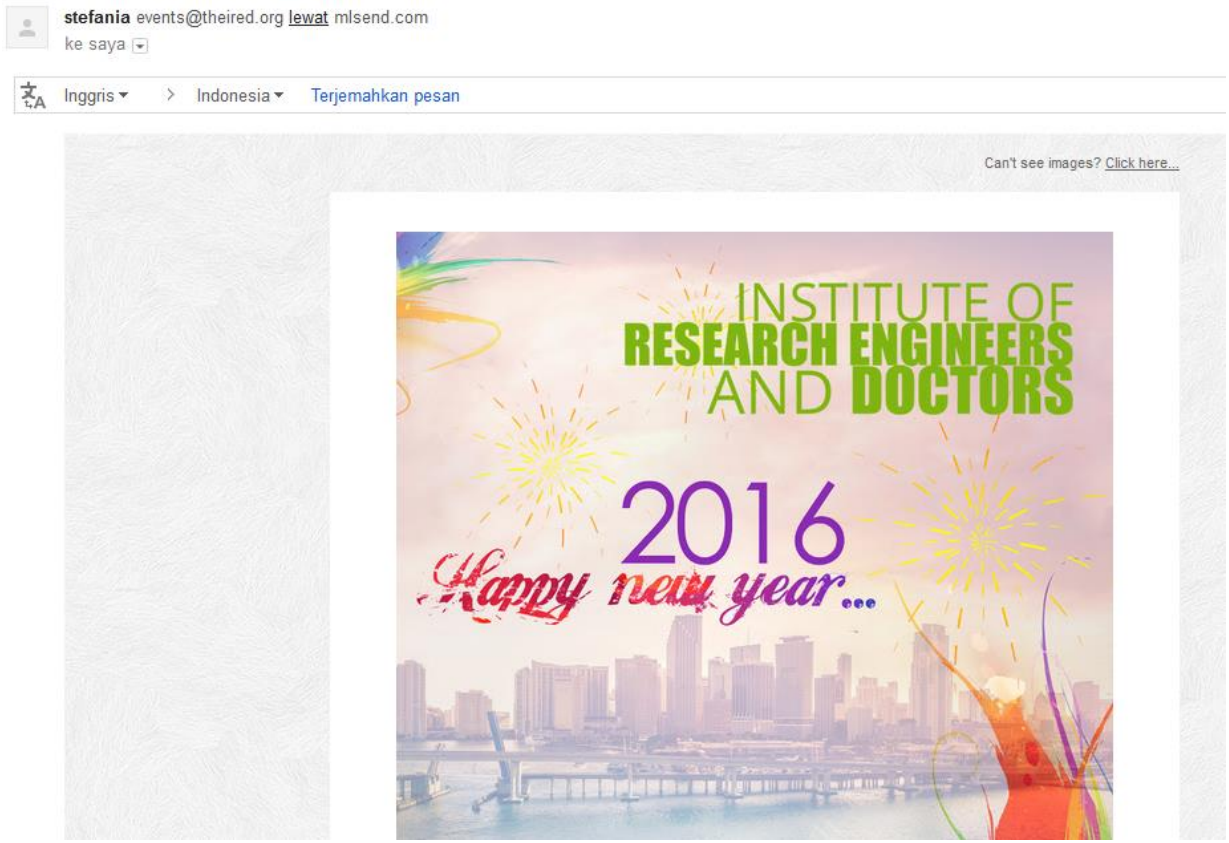
(*website*, *social media*, *social networking*)

Namun, dibalik sebuah gambar dapat tersembunyi informasi rahasia

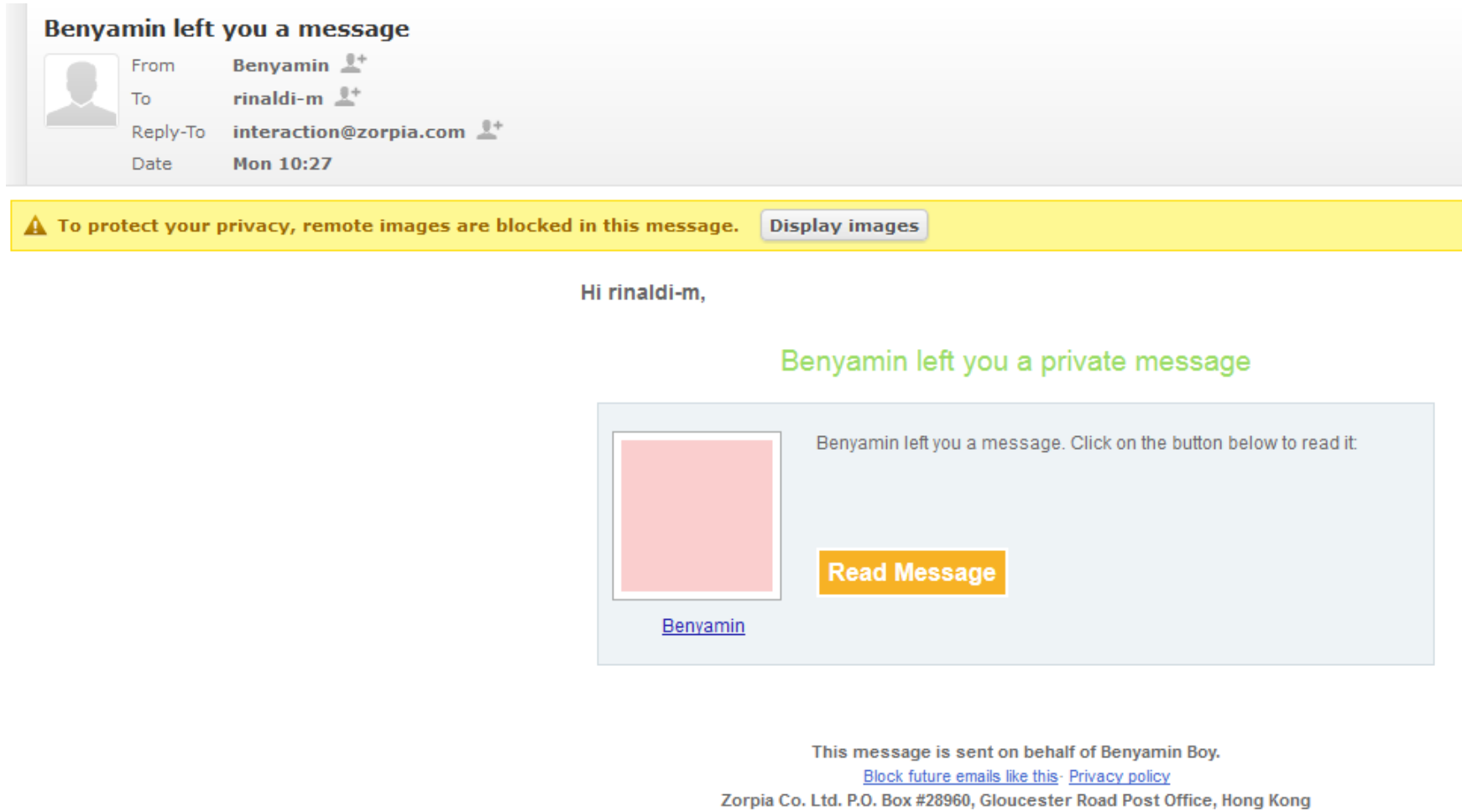


Informasi rahasia tersebut dapat berupa pesan biasa, pesan kejahatan, program jahat, bahkan virus komputer!

Pernah terima surel (*e-mail*) dari orang tak dikenal dan mengandung *file attachmet* berupa gambar seperti di bawah ini?



HATI-HATI!!!!!!!!!



HATI-HATI! Jangan langsung klik jika anda tidak yakin!

Ingat kembali stegosploit!!!

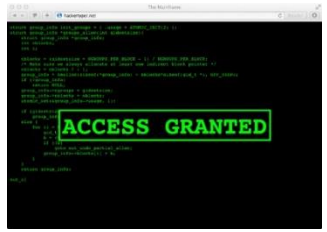
How to Hack a Computer Using Just An Image

Monday, June 01, 2015 Swati Khandelwal

Next time when someone sends you a photo of a cute cat or a hot chick than be careful before you CLICK on the image to view — it might hack your machine.

Yes, the normal looking images could hack your computers — thanks to a technique discovered by security researcher *Saumil Shah* from India.

Dubbed "***Stegosploit***," the technique lets hackers hide malicious code inside the pixels of an image, hiding a malware exploit in plain sight to infect target victims.



Just look at the image and you are HACKED!

http://thehackernews.com/2015/06/Stegosploit-malware.html

- Steganalisis diperlukan di dalam *forensic image analysis*

- ***Forensic Image Analysis*** *is the application of image science and domain expertise to interpret the content of an image and/or the image itself in legal matters.*

- Subdisiplin dari *Forensic Image Analysis:*

  (1) Photogrammetry

  (2) Photographic Comparison

  (3) Content Analysis

  (4) Image Authentication

- Salah satu pekerjaan di dalam *content analysis* adalah mendeteksi apakah ada pesan tersembunyi di dalam sebuah gambar.

- Contoh sebuah skenario: Mr. Abdul, seorang investigator forensik, diminta Lab Forensik Polri untuk menginvestigasi sebuah *cybercrime* berupa foto. Sebagai investigator forensik yang ahli, dia menganalisis foto untuk menemukan pesan tersembunyi di dalamnya dengan kakas steganalisis.

- Tujuan utama steganalisis adalah untuk membedakan apakah sebuah media mengandung pesan rahasia atau tidak.

- Steganalisis dianggap berhasil jika ia dapat menentukan apakah sebuah media mengandung pesan tersembunyi dengan peluang lebih tinggi daripada menerka secara acak.

- Selain tujuan utama di atas, terdapat beberapa tujuan minor steganalisis:

  - menentukan panjang pesan

  - menentukan tipe algoritma penyisipan

  - kunci yang digunakan

Jenis-jenis steganalisis

1. Targeted steganalysis

- Teknik steganalisis yang bekerja pada algoritma steganografi spesifik, dan kadang-kadang dibatasi hanya pada format media tertentu saja.

- Teknik ini mempelajari dan menganalisis algoritma penyisipan, lalu menemukan statistik yang berubah setelah penyisipan.

- Hasil steganalisis sangat akurat, tetapi tidak fleksibel karena tidak dapat diperluas untuk algoritma steganografi yang lain atau format media yang berbeda.

2. *Blind steganalysis*

- Teknik steganalisis yang bekerja pada sembarang algoritma steganografi dan sembarang format media.

- Teknik ini mempelajari perbedaan antara statistik *cover-object* dan *stego-object* dan membedakannya. Proses pembelajaran (*learning*) dilakukan dengan melatih (*training*) mesin pada sekumpulan database media. Model *machine learning* yang digunakan misalnya jaringan syaraf tiruan.

- Hasil steganalisis kurang akurat dibandingkan dengan teknik *targeted steganalysis*, tetapi kelebihannya adalah dapat diperluas untuk algoritma yang lain.

Metode Steganalisis

1 . **Serangan berbasis visual (*visual attacks*)**

- Khusus untuk *stego-object* berupa citra
- Bersifat subjektif, karena melakukan pengamatan secara kasat mata dengan melihat artefak yang mencurigakan di dalam *stego-image*, lalu membandingkannya dengan citra asli (cover *image*)
- Digunakan pada masa-masa awal riset steganalisis
- Contoh serangan visual:

  a. *LSB plane attack*

  b. *Filtered visual attack* (E*nhanced LSB*)

2. Serangan berbasis statistik (*statistical attack*)

- Menggunakan analisis matematik pada citra untuk menemukan perbedaan antara *cover image* dengan *stego image*.
- Didasarkan pada fakta bahwa penyembunyian pesan ke dalam media menimbulkan artefak yang dapat dideteksi secara statistik sehingga dapat mengungkap penyembunyian pesan atau pesan yang disembunyikan itu sendiri.
- Contoh serangan statistik:
  a. *histogram analysis*
  b. *Regular-singular* (RS) *analysis*
  c. *Chi-square analysis*
  d. *Sample pair* (SP) *analysis*

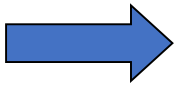
Visual Attack

- Memanfaatkan indera penglihatan → inspeksi kerusakan pada gambar akibat penyisipan

- Ide dasar :

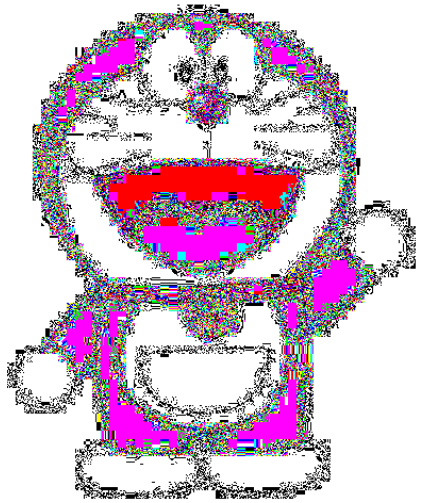
Metode Enhanced LSB

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



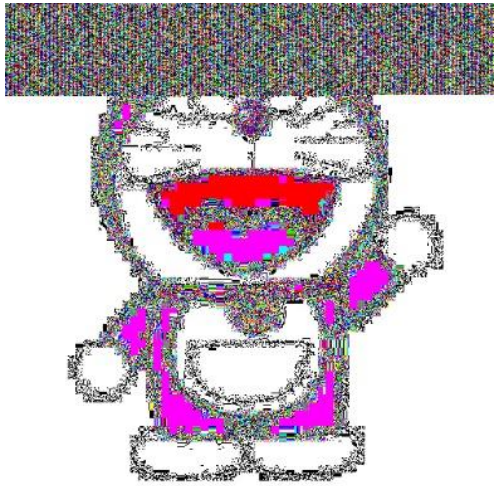
BLUE	GREEN	RED
11111111	**00000000**	**11111111**

(a) Citra orisinal



(b) Citra hasil *enhanced LSB*

(c) Citra stego



(b) Citra hasil *enhanced LSB*

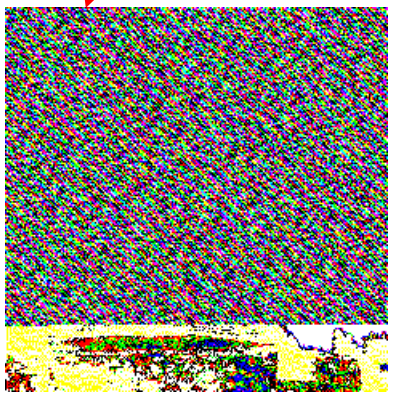
Teknik Steganalisis: *Visual Attack*

Artefak mencurigakan

Gambar asli

Hasil penapisan (asli)

Terdeteksi ada pesan



Terdeteksi ada pesan

Terdeteksi ada pesan

Terdeteksi ada pesan

Metode *enhanced-LSB* bagus untuk citra dengan kontras tinggi, yaitu citra yang memiliki warna latar yang jelas atau memiliki perbedaan warna yang kontras antara latar dengan gambar utama

Gambar III-1 Gambar yang mengandung pesan rahasia dan hasil *enhanced LSB*-nya [PAU07]

Untuk citra dengan kontras rendah (seperti citra hasil fotografi), metode *enhanced LSB* seringkali menyulitkan steganalis. Karena steganalis akan kesulitan membedakan antara gambar yang seharusnya muncul dengan pesan rahasia.

Gambar III-3 Gambar dengan kontras rendah dan hasil *enhaced LSB*-nya

- Sekali citra diketahui mengandung pesan rahasia, maka pesan tsb bisa dihancurkan dengan mengganti seluruh bit-bit LSB

Contoh penghancuran pesan pada citra adalah sebagai berikut :

1. Terdapat citra yang bit *LSB*-nya telah disisipi pesan rahasia, sbb:

   (00100111 11101000 11001000)

   (00100110 11001000 11101000)

   (11001000 00100110 11101001)

2. Maka bit pesan rahasia tersebut adalah : **100000001**
3. Dilakukan penggantian bit *LSB* citra, menjadi : **000000000**

4. Bit tersebut kembali disisipkan pada citra, menjadi :

(00100110 11101000 11001000)

(00100110 11001000 11101000)

(11001000 00100110 11101000)

Penggantian seluruh bit *LSB* menjadi 0, tidak akan merusak tampilan citra, karena mata manusia tidak dapat membedakan perubahan yang terjadi pada bit *LSB*. Contoh citra yang memiliki pesan dan citra setelah pesan dihancurkan dapat dilihat pada Gambar III-5

Gambar III-5 Citra dengan pesan rahasia (kanan) dan citra setelah pesan dihancurkan (kiri)

Ada pertanyaan?

Referensi

- Li, F., *The art and science of writing hidden messages: Steganography*
- Khan, M. M. , *Steganography*
- Wohlgemuth, S. (2002), IT-Security: Theory and Practice : *Steganography and Watermarking,* University of Freiburg, Denmakr, 2002.
- Wong, P.W. (1997). *A Watermark for Image Integrity and Ownership Verification*. Prosiding *IS&T PIC Conference*.
- *Tawalbeh, L.* (2006), *Watermarking,* Information System Security AABFS-Jordan.
- Bae, S.H. (2006), *Copyright Protection of Digital Image*, Tongmyong University of information technology
- Yuli Anneria Sinaga, *Steganalisis dengan Metode Chi-square dan RS-analysis*, Tugas Akhir Informatika, IT