Kajian mengenai Stegosistem dan Steganalisis pada File Gambar

Hendy Sutanto - 13507011

Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Jalan Ganeca no.10 Bandung, 40132
e-mail: hendy_lau8@yahoo.com

ABSTRAK

Semakin berkembangnya kemajuan teknologi dalam bidang data digital juga memacu kebutuhan akan keamanan data digital tersebut. Salah satu metode yang terkenal dalam bidang kriptografi adalah steganografi.

Steganografi merupakan seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Kata steganografi (steganografi) berasal dari bahasa Yunani steganos, yang artinya "tersembunyi atau terselubung", dan graphein, "menulis".

Stegosistem disini berisi tentang penyerangan-penyerangan yang dilakukan terhadap suatu sistem steganografi, sebuah perbedaan penting harus dibuat di antara penyerangan-penyerangan pasif dimana penyerang hanya dapat memotong data dan penyerangan-penyerangan aktif dimana penyerang juga dapat memanipulasi data.

Steganalisis didefinisikan sebagai suatu seni dan ilmu dalam mendeteksi informasi tersembunyi. Sebagai tujuan dari steganografi adalah untuk merahasiakan keberadaan dari sebuah pesan rahasia, satu keberhasilan penyerangan pada sebuah sistem steganografi terdiri dari pendeteksian bahwa sebuah file yang diyakini berisikan data terselubung.

Makalah ini membahas steganografi dengan covertext berupa file gambar. File gambar sering digunakan sebagai covertext karena stegotext-nya hampir tidak berbeda dengan covertextnya, dan sangat tidak mencurigakan. Selain itu dibahas juga mengenai pendeteksian informasi tersembunyi dalam stegotext dan penyerangan terhadap suatu sistem steganografi dengan beberapa macam metode.

Kata Kunci: Steganografi, Stegosistem, Steganalisis

1. PENDAHULUAN

Keamanan dan kerahasiaan data sekarang telah menjadi isu penting dalam dunia sehari-hari. Privasi menjadi hal yang tak dapat diabaikan, oleh karena itu muncul bermacam cara untuk menjaga privasi tersebut, salah satunya dengan kriptografi.

Kriptografi merupakan seni mengubah suatu pesan (plaintext) menjadi bentuk yang tidak dapat dibaca secara harafiah (ciphertext). Hal ini bertujuan untuk mencegah adanya pihak lain yang tidak berhak tahu isi pesan tersebut dapat membacanya.

Namun dengan kriptografi, ciphertext yang ada akan berupa pesan tanpa makna, hal ini dapat membuat orang lain curiga bahwa ada suatu pesan tersembunyi di baliknya. Dengan Steganografi, kita dapat meminimalisasi kecurigaan orang lain karena stegotext yang dihasilkan masih memiliki makna, namun tersimpan pesan rahasia di dalamnya.

Seperti kriptanalisis pada kriptografi, pada steganografi juga terdapat seni untuk mendeteksi adanya pesan rahasia pada stegotext, yang disebut steganalisis. Selain sekedar pendeteksian pesan tersembunyi, terdapat pula serangan terhadap sistem steganografi yang disebut stegosistem.

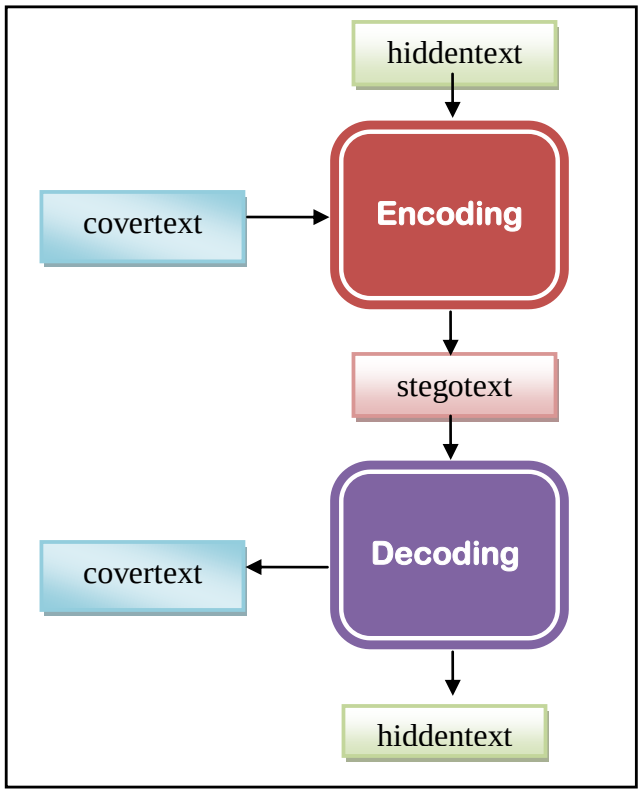
2. TEORI SINGKAT

2.1 Steganografi

Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Kata steganografi (steganografi) berasal dari bahasa Yunani steganos, yang artinya "tersembunyi atau terselubung", dan graphein, "menulis".

Steganografi memiliki empat properti :

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
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, namun kunci ini bersifat opsional.



Gambar 1 Diagram Steganografi

Kriteria steganografi yang bagus:

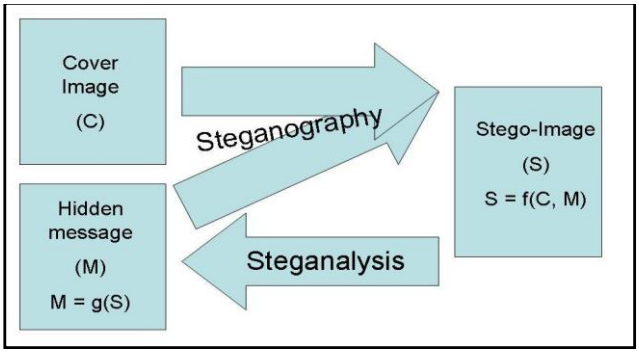
a. **Imperceptible**
   Keberadaan pesan rahasia tidak dapat dipersepsi.
b. **Fidelity.**
   Mutu cover-object tidak jauh berubah akibat embedded.
c. **Recovery.**
   Data yang disembunyikan harus dapat diungkapkan kembali.

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

2.2 Steganalisis

Steganalisis didefinisikan sebagai suatu seni dan ilmu dalam mendeteksi informasi tersembunyi. Sebagai tujuan dari steganografi adalah untuk merahasiakan keberadaan dari sebuah pesan rahasia, satu keberhasilan penyerangan pada sebuah sistem steganografi terdiri dari pendeteksian bahwa sebuah file yang diyakini berisikan data terselubung.

Tujuan steganalisis adalah untuk mengidentifikasi pesan yang dicurigai, menentukan apakah ada atau tidak pesan yang disembunyikan di dalamnya, dan jika mungkin, me-recover nya.



Gambar 2 Diagram Steganalisis

2.2.1 Teknik Dasar Steganalisis

Pada umumnya, steganalisis dalam dilakukan dengan analisis statistik. Suatu himpunan file yang belum diubah dengan tipe yang sama, dan idealnya berasal dari sumber yang sama (misalnya sekumpulan foto dari kamera yang sama) diperiksa dan dianalisis untuk dicatat dan dibuat statistiknya. Sebagian dari data tersebut dapat dianalisis dengan mudah seperti analisis spektrum, namun karena kebanyakan file gambar dan suara jaman sekarang ini telah memiliki kompresi yang cukup kuat seperti JPEG dan MP3, terdapat inkonsistensi dari data sebelum dikompres. Maka dari itu, dengan algoritma encoding steganografi yang sederhanapun, perbedaan atau distorisi dapat dideteksi dengan cukup mudah.

Kasus termudah dalam pendeteksian suatu file yang dicurigai mengandung pesan rahasia adalah jika kita memiliki file original yang memang diyakini belum disisipi pesan apapun. Membandingkan stegotext dengan covertext yang masih original akan menimbulkan berbedaan yang disebabkan encoding hiddentext.

2.3 Stegosistem

Stegosistem disini berisi tentang penyerangan-penyerangan yang dilakukan terhadap suatu sistem steganografi, sebuah perbedaan penting harus dibuat di antara penyerangan-penyerangan pasif dimana penyerang

hanya dapat memotong data dan penyerangan-penyerangan aktif dimana penyerang juga dapat memanipulasi data.

Penyerangan-penyerangan berikut memungkinkan dalam model dari stegosistem ini :

1. **Stego-Only-Attack**
   Penyerang telah menghalangi stego data dan dapat menganalisisnya.
2. **Stego-Attack**
   Pengirim telah menggunakan cover yang sama berulangkali untuk data terselubung. Penyerang memiliki file stego yang berasal dari cover file yang sama. Dalam setiap file-file stego tersebut, sebuah pesan berbeda disembunyikan.
3. **Cover-Stego-Attack**
   Penyerang telah menghalangi file stego dan mengetahui cover file mana yang digunakan untuk menghasilkan file stego ini. Ini menyediakan sebuah keuntungan melalui penyerangan stego-only untuk si penyerang.
4. **Manipulating the stego data**
   Penyerang memiliki kemampuan untuk memanipulasi data stego. Jika penyerang hanya ingin menentukan sebuah pesan disembunyikan dalam file-stego ini, biasanya ini tidak memberikan sebuah keuntungan tapi memiliki kemampuan dalam memanipulasi data stego yang berarti bahwa si penyerang mampu memindahkan pesan rahasia dalam data stego (jika ada).
5. **Manipulating the cover data**
   Penyerang dapat memanipulasi data terselubung dan menghalangi hasil data stego. Ini dapat membuat tugas dalam menentukan apakah data stego berisikan sebuah pesan rahasia lebih mudah bagi si penyerang.

3. CONTOH PENYERANGAN PADA STEGANOGRAFI

3.1 Visual Attacks

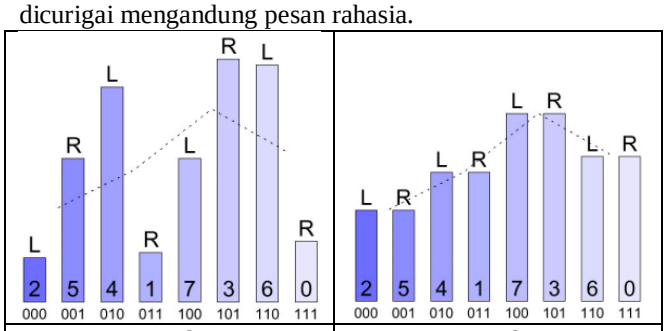
Sebagian besar orang beranggapan bahwa LSB (least significant bit) dari nilai yang penting itu benar-benar acak dan digantikan dengan bit lainnya. Namun dengan Visual Attack, asumsi itu terbukti tidak tepat.

Cover-object	Stego-object

Tabel 1 Perbandingan cover-object dan stego-object dalam visual attack

3.2 Statistical Attacks

Dengan menggunakan statitical attack, kita mencatat semua histogram warna dari suatu file gambar original dan membandingkannya dengan statistik file gambar yang dicurigai mengandung pesan rahasia.



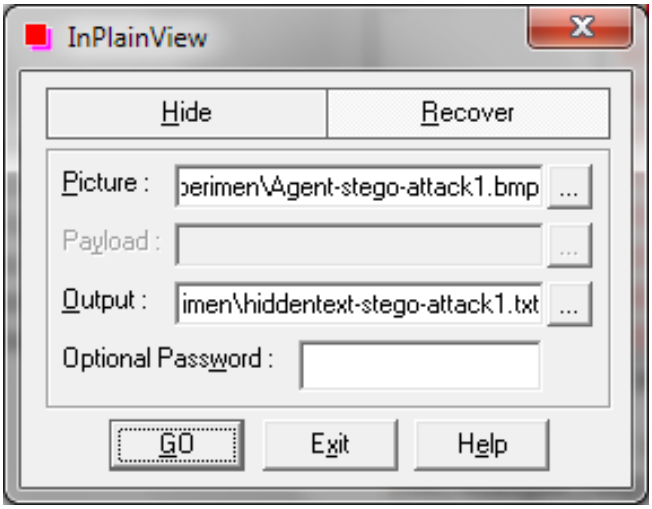
Cover-object	Stego-object

Tabel 2 Perbandingan cover-object dan stego-object dalam statistical attack

4. EKSPERIMEN

Eksperimen dilakukan dengan bantual tool InPlainView (http://www.softpile.com/Utilities/Encryption/Download_05300_1.html), sebuah program sederhana dan gratis yang berfungsi untuk menyisipkan suatu file ke dalam file gambar bertipe bitmap (bmp). File bmp yang menjadi cover-object harus bertipe 24 bit true color bmp.

Perangkat lunak ini juga dapat menerima password untuk meningkatkan keamanan. Namun besarnya file yang dapat disisipkan sangat tergantung oleh besarnya file bitmap yang digunakan sebagai cover-object, yaitu 37 bytes per 100 pixels.



Gambar 3 Tampilan perangkat lunak InPlainView

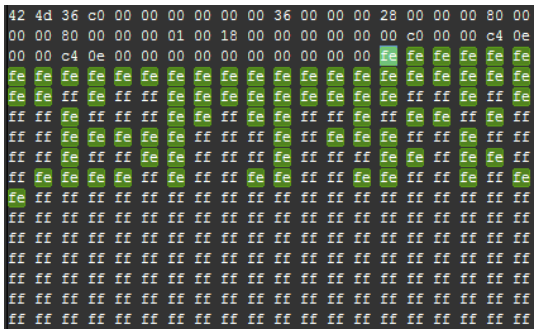
4.1 Eksperimen Steganalisis

Eksperimen ini menggunakan cover-object Agent.bmp dan menyisipkan file hiddentext.txt yang berisi pesan rahasia "kriptografi"

Cover-object	
Hidden-text	kriptografi
Stego-object	

Tabel 3 cover-object, hiddentext, dan stego-object dalam eksperimen yang dilakukan

Kedua gambar di atas tampak identik dan memiliki ukuran file yang sama. Namun ketika diperiksa isinya dalam bentuk heksadesimal dan dibandingkan, ternyata terdapat perbedaan.

Cover-Object	
Stego-object	

Tabel 4 perbandingan isi file cover-object dan stego-object dalam bentuk heksadesimal

Teknik steganalisis ini termasuk dalam kasus yang mudah karena kita telah memiliki file gambar originalnya sehingga dengan mudah kita bisa melakukan perbandingan dan melihat isinya.

4.1 Eksperimen Stegosistem

Penyerangan yang akan dilakukan adalah dengan mengubah satu digit heksadesimal pada stego-object. Hal ini tidak akan merusak cover-object (masih bisa ditampilkan dengan normal) namun ketika dilakukan proses decoding kepadanya, hiddentext yang di-recover akan rusak, dan dapat dikatakan bahwa penyerangan stegosistem ini telah berhasil.

Sebelum dilakukan penyerangan	42 4d 36 c0 00 00 00 00 00 00 36 00 00 00 28 00 00 00 80 00 00 00 80 00 00 00 01 00 18 00 00 00 00 00 00 c0 00 00 c4 0e 00 00 c4 0e 00 00 00 00 00 00 00 00 00 00 fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe ff fe ff ff fe fe fe fe fe fe fe fe fe ff ff fe ff fe ff ff fe ff ff ff fe fe ff fe fe ff ff fe ff fe fe ff fe ff ff ff fe fe fe fe fe ff ff ff fe ff fe fe fe ff ff fe ff ff ff ff fe ff ff fe fe ff ff ff fe ff ff ff fe fe ff fe fe ff ff fe fe fe fe ff fe ff ff fe fe ff ff fe fe ff ff fe ff fe fe ff ff ff ff ff ff ff ff ff ff ff
Setelah dilakukan penyerangan	42 4d 36 c0 00 00 00 00 00 00 36 00 00 00 28 00 00 00 80 00 00 00 80 00 00 00 01 00 18 00 00 00 00 00 00 c0 00 00 c4 0e 00 00 c4 0e 00 00 00 00 00 00 00 00 00 00 fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe ff fe ff ff fe fe fe fe fe fe fe fe fe ff 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61

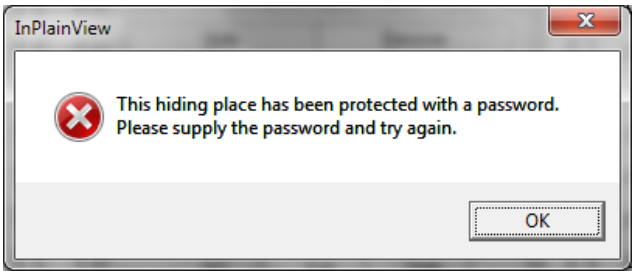
Tabel 5 penyerangan pada stego-object

Heksadesimal 61 menyatakan huruf ‘a’ dalam desimal. Penyerangan yang dilakukan adalah mengganti setiap data yang berbeda antara cover-object dengan stego-object dengan huruf ‘a’ karena data yang berbeda itu dicurigai merupakan akibat dari adanya pesan rahasia yang disisipkan.

Sebelum penyerangan	kriptografi
Sesudah penyerangan	□ÿÿÿÿÿÿÿÿÿ

Tabel 6 perbandingan hiddentext sebelum dan sesudah penyerangan

Namun jika penyerangan dilakukan pada bagian awal data yang berbeda, akan muncul pesan untuk mengisi password seperti ini.



Gambar 4 Pesan kesalahan pada perangkat lunak InPlainView

5. ANALISA

Pada perangkat lunak InPlainView, bagian data yang berbeda antara cover-object dan stego-object diawali dengan header file yang menyimpan data untuk dicocokan dengan password yang ada. Oleh karena itu, pada saat penulis mengganti bagian awal data yang berbeda, pada saat akan dilakukan decoding, perangkat lunak InPlainView meminta masukan password, padahal ketika dilakukan encoding, tidak digunakan password sama sekali.

Setiap baris setelah data heder tersebut mewakili setiap karakter pada pesan rahasia tersebut, terbukti ketika penulis mencoba menyerang satu baris saja, ketika dilakukan decoding, pesan yang rusak hanya satu karakter saja.

6. KESIMPULAN

a. Seperti kriptografi dan kriptanalisis, steganografi juga dapat diserang dengan steganalisis dan stegosistem.
b. Pada umumnya, steganografi pada gambar akan mengubah kualitas gambar cover-object meskipun kadang sulit dibedakan.
c. Stego-object pasti memiliki data yang berbeda dengan cover-object diakibatkan adanya pesan rahasia yang disisipkan ke dalamnya.
d. Stegosistem bertujuan untuk merusak pesan rahasia yang terdapat dalam suatu sistem steganografi. Namun sangat sulit untuk bisa mengekstrak pesan rahasia tersebut dari sistem steganografi yang ada.

Daftar Pustaka

1. http://www.defendingthenet.com/Newsletters/Steganography.htm
   tanggal akses : 23 Maret 2010
2. http://www.jjtc.com/Security/stegtools.htm
   tanggal akses : 23 Maret 2010
3. http://www.dia.unisa.it/~ads/corso-security/www/CORSO-0203/steganografia/LINKS%20LOCALI/Attacks.pdf
   tanggal akses : 24 Maret 2010
4. http://rodiah.staff.gunadarma.ac.id/Downloads/files/10352/Steganografi.pdf
   tanggal akses : 24 Maret 2010
5. http://cdn.simtel.net/pub/simtel/00/01/27/96/inplainv.zip
   tanggal akses : 23 Maret 2010
6. http://www.outguess.org/detection.php
   tanggal akses : 23 Maret 2010
7. Munir, Rinaldi, "Kriptografi", Institut Teknologi Bandung, 2009.