TEKNIK STEGANOGRAFI PADA MEDIA DIGITAL FILE GAMBAR BMP MENGGUNAKAN BORLAND DELPHI 7.0

TUGAS AKHIR

Diajukan sebagai salah satu syarat
Untuk memperolch gelar Ahli Madya Dari
Politeknik Universitas Andalas

Olch :

OKTA HADI SAPUTRA
05 075 034

PROGRAM STUDI TELEKOMUNIKASI MULTIMEDIA
JURUSAN TEKNIK ELEKTRO

POLITEKNIK UNIVERSITAS ANDALAS
PADANG
2008

ABSTRAK

TEKNIK STEGANOGRAFI PADA MEDIA DIGITAL FILE GAMBAR BMP MENGGUNAKAN BORLAND DELPHI 7.0

Oleh :

OKTA HADI SAPUTRA

BP : 05075034

Steganografi merupakan satu metode yang popular, dimana sesuatu pesan (teks atau image) boleh dirahasiakan di dalam file-file lain yang mengandung teks, image, bahkan suara tanpa menunjukkan ciri-ciri perubahan yang nyata atau terlihat dalam kualitas dan struktur dari file semula. Tugas akhir ini memaparkan kriteria-kriteria perancangan algoritma untuk media digital khususnya file gambar dengan jenis BMP menggunakan metode LSB. LSB (*Least Significatin Bit*) merupakan metoda yang mengubah nilai luminansi atau warna menjadi bit yang bersesuai dengan bit label yang akan disembunyikan (menyisipkan citra biner ke dalam citra *grayscale*). Metoda LSB ini bekerja pada domain spasial. *Steganografi* pada media digital tidak tahan terhadap proses yang dapat mengubah data citra seperti pada file gambar jenis BMP.

Kata kunci (*key words*) : *Steganografi, kriptografi, Least Significatin Bits grayscale,.*

BAB I
PENDAHULUAN

1.1 Latar Belakang

Jaringan komputer dan Internet telah mengalami perkembangan yang sangat pesat. Teknologi ini mampu menyambungkan hampir semua komputer yang ada di dunia sehingga bisa saling berkomunikasi dan bertukar informasi. Bentuk informasi yang dapat ditukar berupa data teks, gambar, gambar bergerak dan suara. Seiring dengan perkembangan tersebut, secara langsung ikut mempengaruhi cara kita berkomunikasi. Kalau dahulu untuk berkomunikasi pesan atau surat dengan menggunakan pos, sekarang telah banyak layanan *e-mail* di Internet yang dapat mengirimkan pesan secara langsung ke penerimanya. Akan tetapi sebagai suatu jaringan publik, Internet rawan terhadap pencurian data.

Steganografi sebagai suatu seni penyembunyian pesan ke dalam pesan lainnya yang telah ada sejak sebelum masehi dan kini seiring dengan kemajuan teknologi jaringan serta perkembangan dari teknologi digital, steganografi banyak dimanfaatkan untuk mengirim pesan melalui jaringan Internet tanpa diketahui orang lain dengan menggunakan media digital berupa file gambar.

Penggunaan steganografi menjadi daya tarik banyak orang pada peristiwa penyerangan gedung WTC, 11 September 2001. Pada peristiwa tersebut disebutkan oleh "pejabat pemerintah dan para ahli dari pemerintahan AS" yang tidak disebut namanya bahwa "para teroris menyembunyikan peta-peta dan foto-foto target dan juga perintah untuk aktivitas teroris di ruang *chat sport*, *bulletin boards* porno dan *web site* lainnya". Isu lainnya menyebutkan bahwa teroris menyembunyikan pesan-pesannya dalam gambar-gambar porno di *web site* tertentu.

Steganografi (*covered writing*) didefinisikan sebagai ilmu dan seni untuk menyembunyikan pesan rahasia (*hiding message*) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia. Steganografi telah dikenal semenjak tahun 500 SM, dimana Herodotus (sejarawan Yunani) menuliskan pesan pada kepala budak dan menunggu sampai rambut kepalanya

tumbuh kembali sehingga pesan tidak terlihat dan selanjutnya dia diutus untuk menyampaikan pesan tersebut tanpa menimbulkan kecurigaan oleh bangsa Persia.

Saat ini dalam dunia digital, teknik steganografi banyak digunakan untuk menyembunyikan informasi rahasia dengan berbagai maksud. Salah satu tujuan dari steganografi adalah mengirimkan informasi rahasia melalui jaringan tanpa menimbulkan kecurigaan.

Steganografi berbeda dengan kriptografi. Jika dalam kriptografi pesan yang dirahasiakan tidak disembunyikan, seorang kriptanalis dapat membaca pesan dalam format yang terenkripsi dan juga melakukan dekripsi data, maka dalam steganografi yang pertama kali harus dilakukan oleh seorang steganalis adalah menemukan stego objek terlebih dahulu, hal ini karena pesan yang dirahasiakan /disembunyikan (tidak nampak) dalam medium lain (*cover*).

Steganografi pada media digital file gambar digunakan untuk mengeksploitasi keterbatasan kekuatan sistem penglihatan manusia dengan cara menurunkan kualitas warna pada file gambar yang belum disisipi pesan rahasia. Sehingga dengan keterbatasan tersebut manusia sulit menemukan gradasi penurunan kualitas warna pada file gambar yang telah disisipi pesan rahasia.

Aplikasi steganografi yang dibuat akan meyisipkan pesan pada format file BMP 24 bit. Format file BMP merupakan format file standar sistem operasi MS Windows 3.11/9x/NT dan IBM OS/2. Format file BMP 24 bit menggunakan model warna RGB. Pada model warna RGB, warna yang ditampilkan di layar monitor disusun oleh tiga buah warna primer, yaitu Red (merah), Green (hijau), Blue (Biru). Pada model warna RGB setiap titik pada layar monitor berisi angka yang menunjukkan intensitas yang dipilih pada suatu tabel warna RGB. Jadi pada setiap titik dapat dipilih salah satu warna dari RGB.

1.2 Perumusan Masalah

Perumusan Masalah pada tugas akhir ini adalah bagaimana mengimplentasikan teknik steganografi pada file gambar dengan format Bitmap 24 bit menggunakan software Borland Delphi 7.0 dan proses pengujian atau unjuk kerja pada file gambar tersebut dengan tujuan untuk perlindungan hak cipta.

BAB V
PENUTUP

5.1 Kesimpulan

1. Metode penyisipan LSB menyisipi pesan dengan cara mengganti bit ke 8, 16 dan 24 pada representasi biner file gambar dengan representasi biner pesan rahasia yang akan disembunyikan
2. Semakin besar ukurun file gambar yang digunakan media penampung maka semakin besar pula pesan yang dapat disembunyikan.
3. Pada citra 24-bit yang berukuran 256 x 256 pixel , satu pixel berukuran 3 byte (R,G, dan B) bisa menyisipkan pesan sebayak 65536 x 3 bit = 196608 bit .
4. Proses penulisan pesan rahasia pada aplikasi steganografi ini melalui 3 proses yaknik : cek fleck, sisip fleck, sisip pesan dan sisip lokasi.
5. Proses pembacaan pesan rahasia melalui 3 proses yakni: cek fleck, ambil lokasi dan ambil pesan.
6. Proses kerja aplikasi steganografi dengan metode LSB memiliki nilai perceptual transparency yang tinggi sehingga data gambar yang disisipi pesan tidak mengalami perubahan yang merusak gambar secara visual.
7. Proses penulisan pesan rahasia menggunakan Metode LSB memiliki kelemahan sangat sensitif terhadap proses manipulasi dari gambar stego-image.

DAFTAR PUSTAKA

Budi sukmawan, http://bdg.centrin.net.id/~budskman/stegano.htm / articles/ *"Steganografi"*.

Johnson, Neil F.; Duric, Zoran; Jajodia, Shushil: *"Information Hiding Steganography and Watermaking-Attacks and Countermeasures"*, Advanced in Information Security, Kluwer Academic Publisher, United State, 2001.

Neil F. Johnson, Sushil Jajodia, *"Steganography: Seeing the Unseen"*.

TuTran,http://www.cs.sfu.ca/CourseCentral/365/li/material/notes/Chap4/Chap4.2/Chap4.2.html, *"Steganography : The Art of Hiding Data"*, Mills College Spring 2002

Al-Mualla, Dr. Muhammed, Al – Ahmad, Prof. Husein, *Information Hiding: Steganography and Watermarking*, Etisalat College of Engineering, UAE, 2003

Deutsch, Peter, RFC 1952 *GZIP herkas format specification Bitmap version 4.3*, http://rfceditor. org/

Kharrazi, Mehdi, Sencar, Husrev T. Memon, Nasir, *Image Steganography: Concept and Practice*, Polytechnic University, New York, 2004

Noname,*How to: Use Interpolation Mode to Control Image Quality During Scaling*, MSDN Library for Visual Studio 2005, Microsoft Corporation, 2005.

http://72.14.203.104/search?q=cache:CXn3xfQhu9cJ:www.dinkes-sumsel.or.id/%3Fpilih%3Dlihat%26id%3D8+steganography&hl=id&ct=clnk&cd=4&gl=id