STUDI PUSTAKA UNTUK STEGANOGRAFI DENGAN BEBERAPA METODE

Yogie Aditya, Andhika Pratama, Alfian Nurlifa
Laboratorium Komputasi dan Sistem Cerdas
Jurusan Teknik Informatika, Fakultas Teknologi Industri,Universitas Islam Indonesia
Jl. Kaliurang Km. 14 Yogyakarta 55501
E-mail: hinoka.franzy@yahoo.com , dhika_hunt@gmail.com, lifa.nurlifa13@gmail.com

ABSTRAKS

Penyembunyian pesan dalam sebuah gambar atau lebih sering dikenal dengan istilah steganografi adalah pengembangan dari kriptografi. Steganografi ini bisa dikatakan lebih aman karena sifatnya yang tidak mengacak sehingga file yang disisipi tidak mencurigakan. Metode yang digunakan dalam steganografi tidak hanya satu. Beberapa metode telah digunakan dalam pengembangannya untuk mendapatkan gambar stego atau stego image yang lebih aman, tidak jah beda dengan aslinya dan tidak mudah untuk di pecahkan oleh orang lain yang tidak diberi hak.

Dari metode yang telah ada, tentunya memiliki kekurangan dan kelebihannya masing-masing. Metode yang dibandingkan antara lain metode Least Significant Bit (LSB) dan End Of File (EOF). Kedua metode ini merupakan metode yang sering digunakan untuk pengembangan. LSB adalah metode lama yang terus menjadi dasar untuk menciptakan metode-metode baru lainnya, seperti halnya EOF yang merupakan pengembangan dari metode LSB.

Melalui studi pustaka ini penulis menganalisis metode mana yang lebih efektif untuk penyembunyian pesan. Selain itu, dari studi pustaka ini penulis ingin mengembangkan aplikasi steganografi. Dengan melihat dan mempelajari dari kedua metode tersebut diharapkan pengembangan yang dilakukan akan lebih baik dan dapat menutupi kekurangan sebelumnya.

Kata Kunci: End Of File (EOF), Least Significant Bit (LSB), Steganografi

1. PENDAHULUAN

1.1 Latar Belakang

Cepatnya perkemabangan teknologi informasi saat ini didukung dengan pentingnya kebutuhan akan mendapatkan informasi. Hal ini dapat dilihat dari berkembangnya jaringan internet saat ini yang semakin pesat. Informasi yang dikirimkan tidak hanya informasi untuk semua orang. Terkadang ada juga informasi yang hanya ditujukan untuk orang – orang tertentu atau badan – badan tertentu saja karena sangat dirahasiakannya informasi tersebut.

Seiring dengan perkembanagn teknologi tersebut, ancaman terhadap keamanan informasi yang dibutuhkan semakin besar, terutama untuk informasi yang dirahasiakan tersebut. Berbagai ancaman di dunia maya seperti *hacker, cracker, carder* membuat orang khawatir akan keamanan informasi yang dikirimnya. Kekhawatiran inilah yang membuat pengiriman informasi sedikit terhambat, sedangkan informasi tersebut sangat penting orang-orang tertentu.

Teknik penyembunyian informasi yang cukup terkenal adalah steganografi. Teknik mengurangi kekurangan dari kriptografi yang dapat dengan mudah menimbulkan kecurigaan. Steganografi menyembunyikan informasi rahasia di dalam informasi lain sehingga informasi tersebut tidak dapat diketahui oleh orang lain yang tidak bersangkutan.

Teknik ini mempunyai beberapa metode yang digunakan untuk mengenkripsinya. Salah satunya adalah *LSB(Least Significant Bit)* dan *EOF(End Of File)*. Kedua metode tersebut mempunyai kelemahan dan kelebihan masing-masing dalam proses enkripsi.

Untuk menjaga keamanan file yang berupa pesan tentunya perlu suatu cara agar enkripsi file tidak mudah untuk dipecahkan oleh orang lain serta hasil dari *stego image* tidak menimbulkan kecurigaan. Dengan studi pustaka ini penulis ingin mempelajari bagaimana metode yang telah ada tersebut dalam implementasinya sehingga penulis dapat membuat aplikasi untuk mengembangkannya.

1.2 Tujuan

Pada makalah ini dilakukan studi pustaka yang membandingkan dua metode yang ada untuk mengtahui kelemahan dan kekurangan dari metode tersebut.

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini adalah sebagai berikut :

a. Merupakan studi pustaka.
b. Metode yang digunakan yaitu dua metode pada Steganografi.

2. DASAR TEORI

2.1 Steganografi

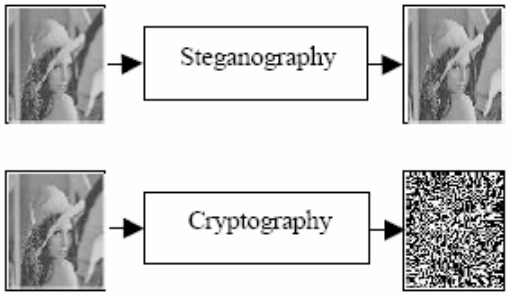
Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu

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 berasal dari bahasa Yunani *steganos*, yang artinya tersembunyi atau terselubung, dan *graphein* artinya menulis.

Kini, istilah steganografi termasuk penyembunyian data digital dalam file-file komputer. Contohnya, si pengirim mulai dengan file gambar biasa, lalu mengatur warna setiap *pixel* ke-100 untuk menyesuaikan suatu huruf dalam alphabet (perubahannya begitu halus sehingga tidak ada seorangpun yang menyadarinya jika ia tidak benar-benar memperhatikannya).

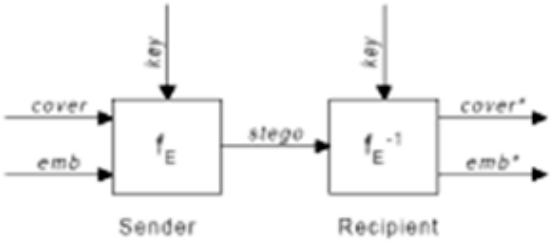
Pada umumnya, pesan steganografi muncul dengan rupa lain seperti gambar, artikel, daftar belanjaan, atau pesan-pesan lainnya. Pesan yang tertulis ini merupakan tulisan yang menyelubungi atau menutupi. Contohnya, suatu pesan bisa disembunyikan dengan menggunakan tinta yang tidak terlihat diantara garis-garis yang kelihatan.

Teknik steganografi meliputi banyak sekali metode komunikasi untuk menyembunyikan pesan rahasia (*teks* atau gambar) di dalam file-file lain yang mengandung *teks, image,* bahkan *audio* tanpa menunjukkan ciri-ciri perubahan yang nyata atau terlihat dalam kualitas dan struktur dari file semula. Metode ini termasuk tinta yang tidak tampak, *microdots*, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya kebanyakan diselesaikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya.



Gambar 1. Perbedaan Steganografi dengan Kriptografi

Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.



Gambar 2. Proses Steganografi

f_E = fungsi steganografi *"embedding"*
f_E^{-1} = fungsi steganografi "*extracting*"
cover = *coverdata* pada *emb* akan di sembunyikan
emb= pesan yang akan disisipakan
key = parameter f_E
stego = *coverdata* dengan pesan yang telah disisipkan

2.2 *Least Significant Bit* (LSB)

Least Significant Bit (LSB) merupakan salah satu teknik dalam Steganografi. LSB menambahkan bit data yang akan disembunyikan (pesan) di bit terakhir yang paling cocok atau kurang berarti. Misalkan bit pada *image* dengan ukuran 3 *pixel* sebagai berikut :

(0011111 11101001 11001000)
(0011111 11001000 11101001)
(1100000 00100111 11101001)

Pesan yang akan disisipkan adalah karakter 'A' yang memiliki biner 10000001, *stego image* yang akan dihasilkan adalah :

(0011111**1** 1110100**0** 1100100**0**)
(0011110 1100100**0** 1110100**0**)
(1100000 0010011**1** 11101001)

Ada dua teknik yang dapat digunakan pada LSB, yaitu penyisipan secara sekuensial dan secara acak. Penyisipan sekuensial dilakukan berurutan sedangkan acak dialakukan dengan acak pada *image* dengan memasukan kata kunci (*stego key*)

2.3 *End Of File (EOF)*

Selain teknik diatas, salah satu teknik lain dari Steganografi adalah *End Of File* (EOF). Teknik ini tidak jauh beda dengan teknik LSB. Jika LSB menambahakan data file pada akhir bit-nya, maka EOF langsung menambahkan data diakhir file image.

Untuk teknik ini dapat menambahkan data atau file yang akan disembunyikan lebih dari ukuran file image. Data yang disembunyikan tersebut akan disisipkan pada akhir file sehingga file image akan terlihat sedikit berbeda dengan aslinya. Ada penanda khusus yang terlihat dari file image di paling bawah seperti garis-garis.

3. HASIL DAN PEMBAHASAN

3.1 Analisis Kebutuhan Sistem

Pada analisis kebutuhan Sistem akan dibahas beberapa kebutuhan dan persyaratan terkait dengan input, proses, dan output sistem. Kebutuhan (persyaratan) ini diperoleh berdasarkan dari teori yang sudah dijelaskan sebelumnya juga dari sumber referensi. Berdasarkan hasil analisa tersebut kebutuhan Sistem antara lain seberikut :

3.1.1 Kebutuhan Input

Sistem yang akan dibandingkan membutuhkan beberapa data input, antara lain :

a. Input data pertama : image
b. Input data kedua : file yang berupa teks

3.1.2 Kebutuhan Proses

Proses yang dibutuhkan untuk mengolah data input menjadi output berupa stego image. Proses yang terjadi adalah proses enkripsi dari file yang berupa teks ke dalam image tanpa mengubah kualitas dari image.

3.1.3 Kebutuhan Output

Output yang dihasilkan dari sistem adalah stego image.

3.2 Hasil Perbandingan

Dari metode yang telah penulis uji, metode *End Of File* (EOF) dengan *Least Significant Bit* (LSB) tidak begitu banyak perbedaan dalam alur algoritmanya, namun terdapat perbedaan yaitu pada pesan yang di sisipi dan *output*.

Pada metode LSB, pesan yang di sisipi ukurannya harus lebih kecil dari citra yang akan di sisipi, tetapi lain halnya pada metode EOF ukuran pesan yang akan di sisipi bisa lebih besar dari ukuran citranya. Pada metode LSB citra yang telah di sisipi pesan *(hidden text)* tidak terlalu mempengaruhi ukuran citranya, tetapi akan mempengaruhi kualitas citranya. Sedangkan pada metode EOF, kualitas citra setelah di sisipi pesan tidak berubah, tetapi akan mengubah ukuran citranya.

Misalkan kita memiliki citra asal yang berukuran 150x200 piksel. Pesan yang disisipkan ada 422 karakter. Ukuran citra setelah disisipkan menjadi 153x200, dengan kata lain 422 karakter yang ada memakan tempat sebanyak 3 baris.

Oleh karena itu, jika kita perhatikan pada citra setelah disisipi pesan, akan nampak seperti garis-garis tambahan dibagian paling bawah citra.

- Metode LSB

Gambar 3. Citra sebelum disisipi pesan

Gambar 4. Citra setelah disisipi pesan

- Metode EOF

Gambar 3. Citra Sebelum disisipi pesan

Gambar 4. Citra setelah disisipi pesan

3.2.1 Perbandingan Ukuran Stego Image

No	Metode	Size Image	Size Pesan	Stego Image
1	LSB	150x200	422 karakter	150x200
2	EOF	150x200	422 karakter	153x200

Tabel 1. Tabel Hasil Perbandingan Ukuran *Stego image*

4. KESIMPULAN

Berdasarkan hasil studi pustaka yang dilakukan oleh penulis dapat disimpulkan bahwa :

a. Jika dilihat berdasarkan ukuran *stego image* LSB lebih baik karena tidak mengubah ukuran file yang disisipi, namun untuk kualitas *image*, LSB banyak mengurangi kualitas *image* yang semula.
b. Untuk kualitas *image,* EOF lebih baik karena kualitas *image* tetap terjaga, namun ukuran file lebih besar dari sebelum disisipi oleh pesan.

Studi pustaka ini dilakukan untuk mempelajari metode – metode yang ada untuk membantu penulis mengembangkan aplikasi steganografi.

PUSTAKA

Sejati, A., (2010). *Studi dan Perbandingan Steganografi Metode EOF(End of File) dengan DCS(Dynamic Cell Spreading)*. ITB, Bandung.

Sinaga, Y.A., (2008). *Program Steganalisis Metode LSB pada Citra dengan Enhanced LSB, Uji Chi-Square, dan RS-Analysis*

Sukrisno dan Utami, E., (2007). *Implementasi Steganografi Teknik EOF dengan Gabungan Enkripsi Rijndael, Shift Cipher dan Fungsi Hash Md5*, Prosiding Seminar Nasional Tekhnologi, Yogyakarta.

Wijaya, E.S., Prayudi, Y., (2004). *Konsep Hidden Message Menggunakan Teknik Steganografi Dynamic Cell Spreading.* Media Informatika , Yogyakarta.