IMPLEMENTASI STEGANOGRAFI DENGAN METODE LSB UNTUK MENGAMANKAN INFORMASI AKUN EMAIL PADA SUATU INSTANSI

Euis Sitinur Aisyah [1]
Rosdiana[2]
Mochammad Ridwan Qodri[3]

Email : euis@raharja.info ; rosdiana@raharja.info; ridwan.qodri@raharja.info

ABSTRAK

Steganografi dalam Image adalah bertujuan untuk menjaga kerahasiaan sebuah pesan atau informasi dengan cara menyembunyikan (*embed*) pesan teks sehingga pihak luar tidak akan menyadari pesan tersembunyi dalam gambar. Pesan yang diterima penerima pesan yang sah, akan diambil informasinya dengan meng-*extract* pesan dari gambar. Manfaat program aplikasi steganografi dalam citra menggunakan metode LSB (*Least Significant bit)* yaitu bagi para administrator jaringan dalam pengiriman pesan yang berupa kode verifikasi atau kata kunci bagi para asisten administrator, dan para pengguna jaringan internet maupun intranet dalam mengirimkan pesan-pesan yang sangat pribadi atau kode-kode kata kunci. Salah satu teknik pengamanan data dengan cara penyisipan informasi rahasia pada berkas gambar digital sebagai media penampung ialah *Steganography* berbasis *least Significant Bit (LSB)* dengan penambahan kemampuan penyisipan yang bersifat *variable-size.* Operasi teknik *Steganography* ini menggunakan tiga parameter , yaitu *capacity Evaluation* untuk menentukan kapasitas maksimum LSB dari masing-masing *pixel* media penampung, *minimum error replacement* untuk memperkecil tingkat kesalahan saat penyisipan, dan *improved grayscale compensation* untuk memisahkan kesalahan penempelan agar tidak berdekatan pada tempat *pixel* bekerja. Penelitian ini bertujuan mengimplementasikan teknik tersebut untuk menyembunyikan data rahasia pada berkas gambar digital sebagai media penampung dan menghasilkan *stego-image* dengan kesamaan tampilan dan ukuran berkas. Berkas hasil penyisipan *(stego-image)* yang diperoleh diharapkan tidak menimbulkan kecurigaan pada pihak lain, serta mampu memaksimumkan penyisipan data rahasia.

Kata kunci: *steganografi, penyisipan informasi, simple LSB substitution*

[2] Dosen Sistem Informasi STMIK Raharja Informatika
Jl. Jend.Sudirman No. 40 Modern Cikokol-Tangerang 15117

[2] Dosen Sistem Komputer STMIK Raharja Informatika
Jl. Jend.Sudirman No. 40 Modern Cikokol-Tangerang 15117

[2] Mahasiswa AMIK Bina Sarana Informatika
Cabang Bumi Serpong Damai

PENDAHULUAN

Latar Belakang

Saat ini internet sudah berkembang menjadi salah satu media yang paling populer di dunia. Karena fasilitas dan kemudahan yang dimiliki oleh internet maka internet untuk saat ini sudah menjadi barang yang tidak asing lagi. Dengan berkembangnya internet dan aplikasi menggunakan internet semakin berkembang pula kejahatan sistem informasi. Dengan berbagai teknik banyak yang mencoba untuk mengakses informasi yang bukan haknya. Maka dari itu sejalan dengan berkembangnya media internet ini harus juga dibarengi dengan perkembangan pengamanan sistem informasi.

Keamanan pada suatu informasi atau data pada saat ini dapat dibagi menjadi dua, yakni: Kriptografi dan Steganografi. Dari dua metode tersebut, metode yang satu dapat menjadi tambahan bagi metode yang lain. Kriptografi adalah suatu seni untuk mengacak suatu informasi atau data yang memiliki arti, menjadi sesuatu yang tidak dapat di mengerti atau seakan-akan tidak berarti. Berbeda dengan kriptografi, Steganografi adalah suatu seni untuk menyembunyikan suatu data, dimana data tersebut disembunyikan ke dalam suatu media yang tampak biasa saja. (Renaldi Munir, 2004: 209)

Digital steganografi memerlukan suatu media sebagai tempat penyembunyian informasi. Secara teori penyisipan informasi pada data digital dengan menggunakan teknik steganografi dapat dilakukan pada semua format data digital yang ada dalam komputer sebagai media covernya seperti format teks, format gambar, bahkan untuk format audio dan sebagainya asalkan file-file tersebut mempunyai bit-bit data redundan yang dapat dimodifikasi.

Rumusan Masalah

a. Bagaimana melakukan penyisipan pesan teks ke dalam gambar dengan menggunakan teknik steganografi
b. Bagaimana penerapan teknik steganografi terhadap pengiriman informasi akun email pada suatu instansi

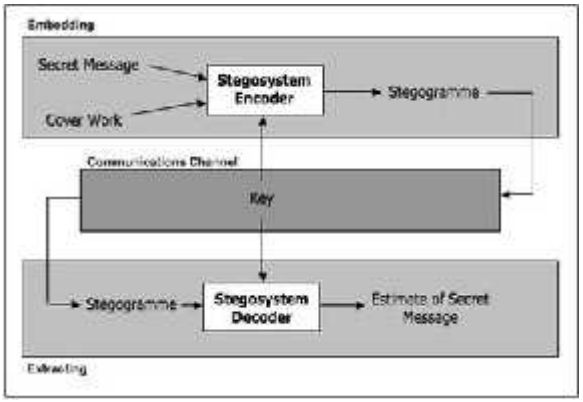
LANDASAN TEORI

Konsep Steganografi

Steganografi adalah ilmu pengetahuan dan seni dalam menyembunyikan komunikasi. Suatu sistem *steganografi* sedemikian rupa menyembunyikan isi suatu data di dalam suatu sampul media yang tidak dapat di duga oleh orang biasa sehingga tidak membangunkan suatu kecurigaan kepada orang yang melihatnya, Gambar 1 adalah ilustrasi dasar dari konsep steganografi.

Di masa lalu, orang-orang menggunakan tato tersembunyi atau tinta tak terlihat untuk menyampaikan isi *steganografi*. Sekarang, teknologi jaringan dan komputer menyediakan cara *easy-to-use*

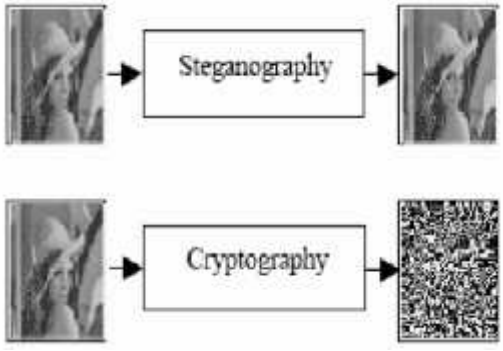
jaringan komunikasi untuk *steganografi*. Proses penyembunyian informasi di dalam suatu sistem *steganografi* dimulai dengan mengidentifikasi suatu sampul media yang mempunyai bit berlebihan (yang dapat dimodifikasi tanpa menghancurkan integritas media). Proses menyembunyikan (*embedding*) menciptakan suatu proses stego medium dengan cara menggantikan bit yang berlebihan ini dengan data dari pesan yang tersembunyi.



Gambar 1. Diagram Steganografi

Perbedaan Steganografi dengan Kriptografi

Steganography berbeda dengan *cryptography*, letak perbedaannya adalah pada hasil keluarannya. Hasil dari *cryptography* biasanya berupa data yang berbeda dari bentuk aslinya dan biasanya data seolah-olah berantakan sehingga tidak dapat diketahui informasi apa yang terkandung didalamnya (namun sesungguhnya dapat dikembalikan ke bentuk semula lewat proses dekripsi), sedangkan hasil keluaran dari *steganography* memiliki bentuk persepsi yang sama dengan bentuk aslinya. Kesamaan persepsi tersebut adalah oleh indera manusia (khususnya visual), namun bila digunakan komputer atau perangkat pengolah digital lainnya dapat dengan jelas dibedakan antara sebelum proses dan setelah proses (Suhono, 2000). Gambar 2 menunjukkan ilustrasi perbedaan antara steganografi dan kriptografi.



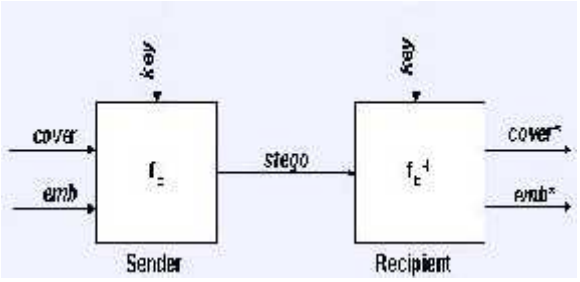
Gambar 2. Perbedaan steganografi dan kriptografi

Dasar Penyembunyian (Embedding)

Tiga aspek berbeda di dalam sistem penyembunyian informasi bertentangan dengan satu sama lain yaitu: kapasitas, keamanan, dan ketahanan (*robustness*). Kapasitas adalah mengacu pada jumlah informasi yang dapat tersembunyi di dalam sampul media, keamanan adalah pencegahan bagi orang biasa yang tidak mampu untuk mendeteksi informasi tersembunyi, dan ketahanan adalah untuk modifikasi media stego sehingga dapat bertahan terhadap suatu *attack* yang dapat menghancurkan informasi tersembunyi.

Penyembunyian informasi biasanya berhubungan dengan *watermarking* dan *steganografi*. Tujuan utama sistem *watermarking* adalah untuk mencapai tingkat ketahanan yang lebih tinggi, sangatlah mustahil untuk menghilangkan suatu proses *watermarking* tanpa menurunkan tingkat kualitas objek data. steganografi, pada sisi lain, mengejar kapasitas dan keamanan tinggi, yang dimana sering diketahui bahwa informasi yang tersembunyi mudah diketahui. Bahkan modifikasi kecil kepada media stego dapat menghancurkannya (Provos, 2003).

Model dasar untuk *embedding* adalah sebagaimana pada Gambar 3 (Zolnerr et al., 2004). Sementara Gambar 4 menunjukkan hubungan antara steganografi dengan watermarking (Suhono et al., 2000).



Gambar 3. Model dasar embedding

f_E: steganographic function "embedding"
f_E^{-1}: steganographic function "extracting"
cover: cover data in which *emb* will be hidden
emb: message to be hidden
key: parameter of f_E
stego: cover data with the hidden message

Teknik LSB (Least Significant Bit)

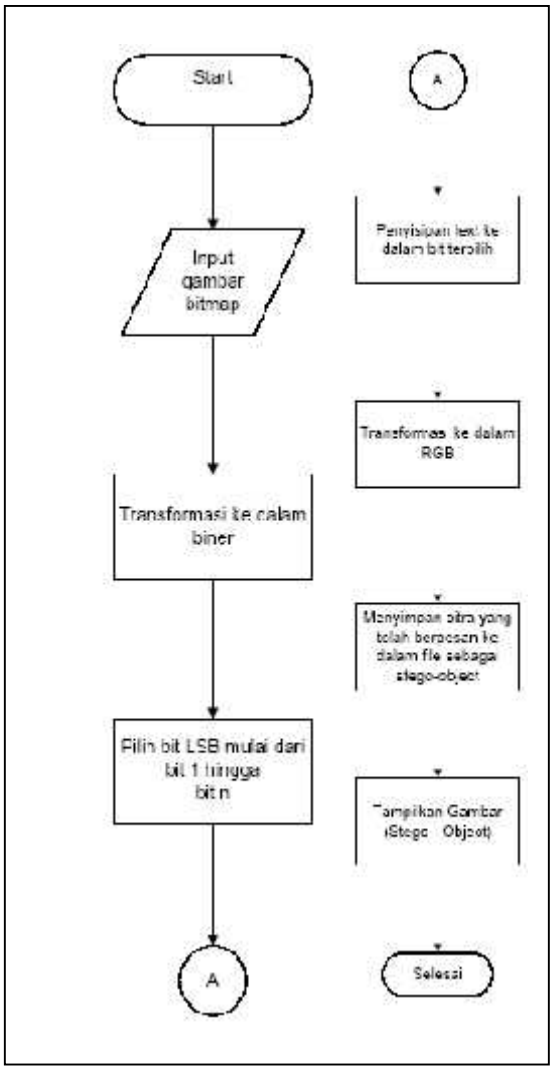
Teknik steganografi yang paling paling sederhana sekaligus paling populer adalah teknik substitusi LSB. Teknik ini mengganti bit terakhir dari media steganografi dengan bit dari pesan [4]. Secara umum, cara kerja teknik subtitusi ini adalah sebagai berikut. Misalkan kita memiliki informasi pada media seperti:
10110101
10010111
10000100
00110001
01100001
10110101
01100110
10110101

Kemudian, kita akan menyisipkan pesan “00100101” pada deretan informasi awal yang ada. Maka, setiap bit pesan akan disubstitusi satu per satu pada informasi awal. Setelah dilakukan proses substitusi, informasi media akan berubah menjadi sebagai berikut.
10110100
10010110
10000101
00110000
01100000
10110101
01100110
10110101

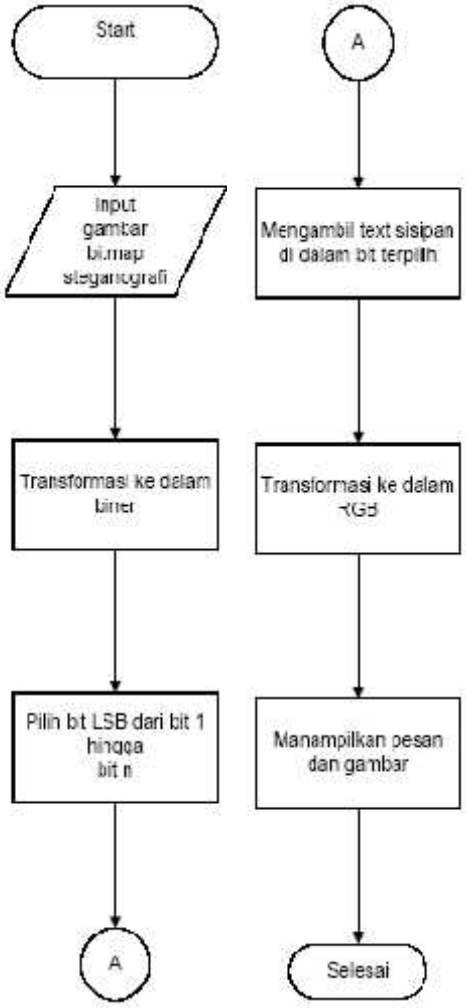
Supaya tidak menyebabkan perubahan besar, penggantian bit ini hanya boleh dilakukan pada informasi yang sifatnya redundan dan memiliki toleransi terhadap perubahan kecil. Informasi yang memiliki toleransi ini misalnya informasi warna pada bitmap gambar atau frekuensi pada data audio. Perubahan kecil pada warna gambar tidak dapat dideteksi oleh mata manusia. Frekuensi audio yang bergeser kecil juga tidak dapat terdeteksi oleh pendengaran biasa.

Sejak ditemukan, teknik LSB telah mengalami berbagai perkembangan. Beberapa modifikasi yang dapat dilakukan terhadap teknik LSB antara lain:
1. Substitusi bit tidak dilakukan secara sekuensial.
2. Substitusi tidak hanya dilakukan terhadap 1 bit, namun beberapa bit sekaligus.
3. Bit yang diubah tidak hanya bit terakhir, melainkan bit pada posisi tertentu.

ALGORITMA



Gambar 6. Diagram alir proses penyisipan pesan



Gambar 7. Diagram alir proses ekstraksi pesan

IMPLEMENTASI

Implementasi dari steganografi ini menggunakan software QuickStego yang dirancang oleh Cybernescence. Media yang digunakan untuk menyebunyikan pesan adalah media gambar berekstensi bmp, jpg, jpeg, gif. Sedangkan gambar yang telah disipkan pesan disimpan dalam format bmp.

Gambar 8. Tampilan program steganografi

Gambar yang akan digunakan sebagai wadah penyimpanan pesan adalah sebagai berikut:

No	Nama file	Type	Size
1	iraharja.jpg	Digital image	9 kb

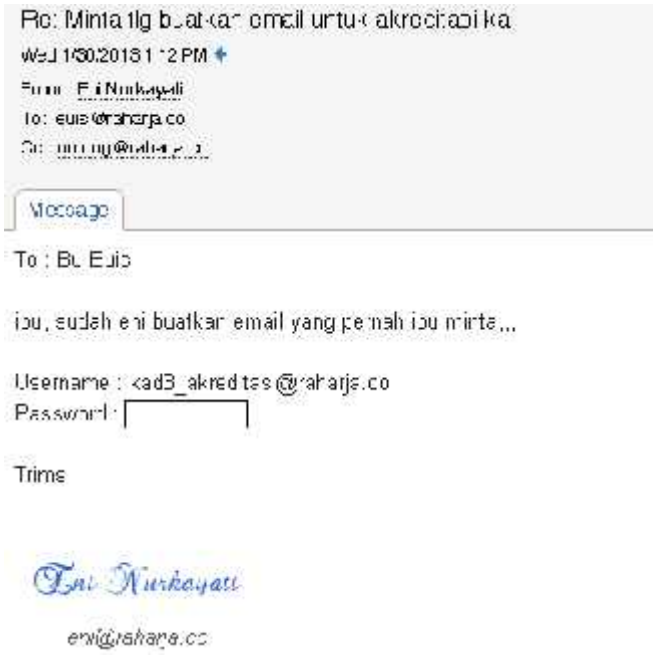
Sedangkan pesan yang disisipkan disimpan dalam file txt sebagai berikut:

No	Nama file	Type	Size	Isi pesan
1	user_euis.txt	File txt	1 kb	username: kad3@rahaarja.co Password: Rhj0987

Hasil gambar yang belum dan telah disisipkan pesan dapat dilihat pada gambar 9 dan gambar 10. Hasil penyisipan pesan melalui steganografi tidak tampak perubahan gambar.

Gb 9. Gambar sebelum disisipkan pesan	Gb 10. Gambar setelah disisipkan pesan
	

Sedangkan proses pengiriman email juga mengalami perubahan, pengiriman informasi akun email sebelumnya melalui message, namun setelah menerapkan metode steganografi pengiriman informasi melalui attachment gambar.



Gambar 11. Informasi akun email sebelum menggunakan steganografi

Gambar 12. Informasi akun email setelah menggunakan steganografi

KESIMPULAN

Dari penjelasan pada bab-bab sebelumnya dapat diambil kesimpulan sebagai berikut:

a. Penerapan steganografi pada file gambar yang berisi pesan user dan password email baru pada suatu instansi, disimpulkan lebih terjamin keamanan datanya.
b. File tidak mengalami banyak perubahan dengan kata lain gambar yang dihasilkan masih sama dengan file aslinya, hanya berbeda pada size atau ukurannya.
c. Teknik *Steganography* berbasis LSB pada gambar dengan metode penyisipan *variable-size* mampu memyenbunyikan informasi rahasia dengan baik. Selain itu penggunaannya dapat disesuaikan dengan ukuran media gambar yang digunakan dan informasi yang akan disisipkan.

DAFTAR PUSTAKA

1) Brittnee Morgan, uri.com-index. Retrieved February 10, 2009
2) Available:http://www.uri.edu/personal2/love0945/stegdetection3.htm
3) Implementasi dan Analisa Teknik Steganografi Multi-Carrier Pada File Multimedia, Canggih Satriatama, Poltek Negeri Surabaya
4) Krenn, J.R., 2004, *Steganography and Steganalysis*, www.krenn.nl/univ/cry/steg/article.pdf
5) V. K. Sharma and V. Shrivastava, "A Steganography Algorithm for Hiding Image in Image by Improved LSB Substitution by Minimize Detection," Journal of Theoritical and Applied Information Technology, 2012.
6) Provos, N., Honeyman, P. (2003). Hide and Seek: An Introduction to Steganography. *IEEE Computer Society.*
7) http://id.wikipedia.org/wiki/Steganografi , diakses tanggal 21 April 2013
8) http://www.mathworks.com/matlabcentral/fileexchange/11813-lsb-steganography, diakses tanggal 18 April 2013