Analisis Dan Implementasi Teknik Steganografi Sebagai Fasilitas Pengamanan Proses Pengiriman File Secara Online

Achmad Sidik[1], Zainul Hakim[2], Eko Andi Permana[3]
[1,2,3]Dosen STMIK Bina Sarana global
Email : [1]sidik@stmikglobal.ac.id,[3]ekoandi@gmail.com

***Abstrak*— Steganografi adalah salah satu mengamankan pengiriman pesan. *Spread spectrum* dan *Least significant bit* (LSB) adalah metode steganografi umum yang sering digunakan. Masukan dari proses embedding tersebut akan menjadi file gambar jenis BMP dan JPEG dan file text, sedangkan keluaran akan menjadi sebuah file text. Hasil gambar pembanding antara masukan dan keluaran tidak menunjukkan perubahan yang signifikan, seperti untuk file text. Metode LSB ,memiliki proses *embedding* dan proses ekstrasi lebih cepat dibandingkan dengan *spread spectrum*, keamanan lebih baik dibandingkan dengan LSB, hasil dari proses *embedding* gambar dengan jenis BPM tidak akan jauh berbeda dari gambar aslinya jika dibandingkan dengan JPEG karena jenis BPM telah dipadatkan.**

***Kata kunci*— Steganografi, *Least Significant Bit, Spread Spectrum*.**

I. PENDAHULUAN

Keamanan suatu sistem informasi pada era digital ini makin penting peranannya dalam berbagai aspek kehidupan, terutama untuk informasi yang memiiki nilai lebih dibanding dengan informasi yang lain, misalnya informasi yang berkaitan dengan aspek aspek keputusan bisnis, kemanan Negara, ataupun kepentingan umum, tentunya informasi informasi tersebut diminati oleh berbabagi pihak.

Oleh karena itu pengamanan informasi dalam hal ini adalah steganografi, semakin dibutuhkan guna memberikan rasa aman dalam proses penyampaian informasi. Steganografi sendiri merupakan cara untuk menyembunyikan rahasia didalam suatu informasi lain yang tampak tidak bermakna, kecuali bagi orang yang mengerti kuncinya. Teknik steganografi menggunakan dua media yang berbeda secara bersamaan, diaman salah satu berfungsi sebagai media yang berisikan informasi informasi rahasia Pertukaran informasi melalui media internet merupakan salah satu keuntungan yang diperoleh dari berkembangnya teknologi saat ini. Bagaimana menjaga kemanan data yang dikirim serta menjamin keabsahan data yang diterima merupakan salah satu yang menjadi tujuan utama. Dalam dunia komputer, ada 2 istilah teknik keamanan data yang sangat dikenal yaitu steganografi dan kriptografi.

Steganografi adalah teknik menyembunyikan atau menyamarkan keberadaan pesan rahasia dalam media penampungnya. Sedangkan Kriptografi menyamarkan arti dari suatu pesan, tetapi tidak menyembunyikan bahwa ada suatu pesan. Secara teori, semua file yang ada didalam computer dapat digunakan sebagai media penampung pesan, seperti file citra berformat JPG, GIF, BMP. Dengan adanya teknik steganografi yang melakukan penyamaran pada media yang di bawah dan kriptografi yang mempunyai tugas sebagai kunci acak maka informasi yang akan disampaikan dapat terjaga sifat kerahasiannya.

A. Perumusan Masalah

Dalam Pembuatan makalah ini terdapat beberapa permasalahan yang menjadi titik utama pembahasan, Adapun permasalahan permaslaahan tersebut adalah sebagai berikut:

a. Bagaimana Menyisipkan suatu informasi ke dalam File gambar.
b. Bagaimana Melindungi suatu informasi menggunakan teknik stego.
c. Bagaimana mengambil Kembali suatu Informasi dari stego.

B. Batasan Masalah

Adapun Batasan masalah pada makalah ini agar tidak terjadi kesalahan persepsi dan tidak meluasnya pokok bahasan adalah sebagai berikut:

a. Implementasi teknik steganografi untuk mengamankan dokumen digital dalam bentuk gambar.
b. Format file citra yang akan di gunakan adalah bmp, png
c. Ukuran secret file dan carrier file disesuaikan dengan metode dan scenario yang tercantum pada bagian pengujian.

C. Tujuan

Tujuan yang ingin dicapai dalam tugas makalah ini adalah:

a. Memberikan informasi dan mengimplementasikan teknik steganografi kedalam file gambar.
b. Mengembangkan aplikasi berbasis macromedia dreamwever cs 4 yang mampu menyembunyikan, melindungi, dan membagi informasi kedalam file gambar menggunakan teknik steganografi.

II. TEORI DASAR

David Khan menyatakan bahwa “pengamanan informasi dapat dibedakan ke dalam 2 kelompok, *security* dan *intelligence*. *Security* dikaitkan dengan pengamanan data (penting bagi perusahaan) Intelligence dikaitkan dengan pencarian (penyadapan, pencurian) data (penting bagi militer/ intel). Security dapat dilakukan dengan 3 cara: *Cryptography*,

Steganography, *Watermarking* [1].

Pada prinsipnya, ketiganya memiliki fungsi yang sama,yaitu sama-sama berperan dalam keamanan suatu data, tapi ketiganya memiliki maksud yang berbeda.

- *Cryptography*, pesan dikodekan sedemikian rupa sehingga orang lain tidak mengerti atau mengenali pesan tersebut[2].
- *Steganography*, pesan disembunyikan pada media tertentu, sehingga orang lain tidak mengetahui keberadaan pesan tersebut.
- *Watermarking*, bertujuan untuk mengamankan otoritas sebuah file/media digital yang dapat berupa *copyright*, kepemilikan, atau lisensi. Steganografi (dalam bahasa Yunani disebut *Steganos*, "tersembunyi/disembunyikan", dan *grapphein*, "menulis"). Adalah sebuah seni dan ilmu (science) tentang berkomunikasi dengan cara menyembunyikan, menanamkan / melekatkan *(embedding)* eksistensi informasi dari suatu komunikasi ke dalam sebuah media yang disebut carrier file.

A. *Prinsip Dasar*

Bagaimana cara merahasiakan komunikasiantara orang pertama dengan orang kedua yang pasti mengandung suatu informasi rahasia yang ada dalam komunikasi tersebut, sehingga orang ketiga tidak tahu eksistensi suatu informasi yang ada dan tidak memiliki kecurigaan terhadap komunikasi yang dirahasiakan tersebut.

B. *Metode Steganografi*

1. Least Significant Bit (LSB)

Merupakan sebuah metode yang lazim digunakan oleh para peneliti pada sebuah steganografi. Karena merupakan metode steganografi yang paling sederhana, cepat, dan mempunyai kapasitas penyisipan suatu informasi digital yang menyisipkan sebuah informasi rahasia pada bit rendah atau bit yang paling kanan dari sebuah data pixel yang menyusun sebuah informasi digital yang menjadi media penampung suatu informasi rahasia.[4]

2. *Masking* and *Filtering*

Metode ini biasanya dibatasi pada image 24 bit warna dan *image grayscale*. Beberapa literatur menyatakan bahwa metode ini mirip dengan watermark, dimana suatu image diberi tanda *(marking)* untuk menyembunyikan pesan rahasia.Hal ini dapat dilakukan dengan memodifikasi *luminance image* dibeberapa bagiannya. Metode ini memiliki ketahanan *(robustness)* terhadap kompresi, dan *cropping*. Namun, memiliki batasan kapasitas tertentu pada informasi yang akan disembunyikan.

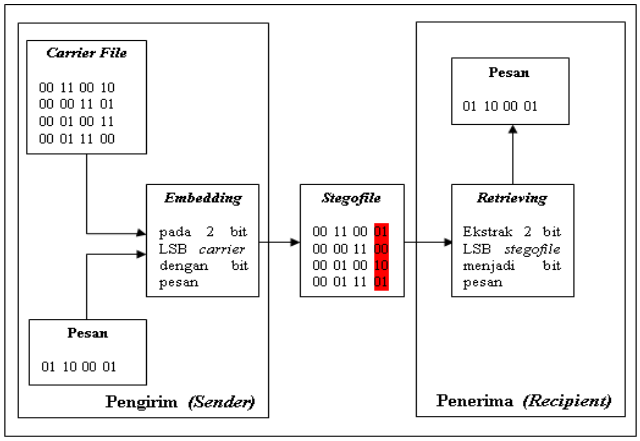
3. *Algorithm* and *Transformation*

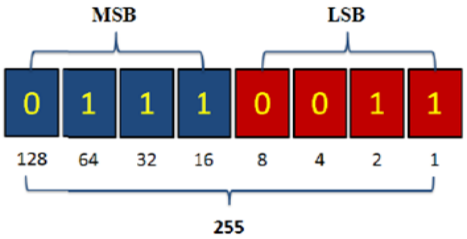
Metode ini merupakan metode steganografi yang jauh lebih kompleks dari metode-metode sebelumnya, artinya tingkat kesulitan dalam penerapan metode ini lebih tinggi Untuk menyembunyikan sebuah informasi digital pada media penampungnya dilakukan dengan memanfaatkan *Discerete Cosine Transformation* (DCT) dan Wavelet Compression. DCT digunakan pada file-file terkompresi, seperti JPEG. Metode ini terjadi di domain frekuensi dari sebuah file digital, bukan pada domain spasial.

4. *Spread Spectrum Methode*

Teknik metode ini dalam menyembuyikan suatu informai digital adalah dengan mengkodekan informasi rahasia dan disebarkan ke setiap spektrum frekuensi yang memungkinkan Namun, metode ini masih mudah diserang, yaitu dengan cara penghancuran atau pengrusakan dari kompresi dan proses image (gambar).

C. *Konsep LSB*





Gambar 1 Representasi Biner

D. *Perbedaan Steganografy Dan Kriptografy*

Steganografi dan kriptografi mempunyai prinsip kerja yang berbeda, meskipun keduanya mempunyai hubungan yang dekat dalam dunia keamanan data. Hasil dari kriptografi 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)[3], sedangkan hasil keluaran dari steganografi 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.

III. METODOLOGI PENELITIAN

a. Fase Analisis

- Studi Literatur

Studi ini dilakukan dengan cara mencari sekaligus mempelajaribeberapa literatur dan artikel mengenai steganografi dan kriptografi sebagai acuan dalam

perencanaan dan pembuatan sistem atau aplikasi.Pendefinisian dan analisis masalah untuk mencari solusi yang tepat.

- Studi Pustaka

b. Fase Pembuatan Program

Perancangan dan implementasi sistem yang dilakukan secara eksperimental yaitu bereksperimen membuat program berdasarkan materi dan algoritma yang telah dipelajari.

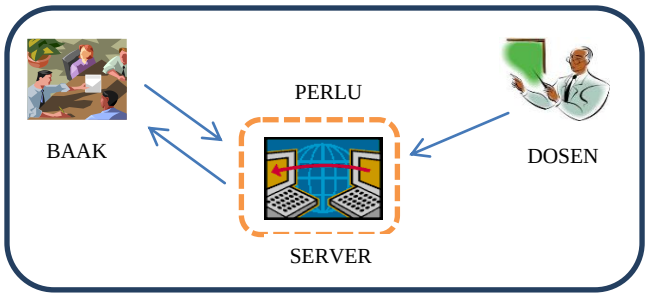
c. Pengujian Program

Pengujian dilakuakan terhadap program yang telah dibuat.

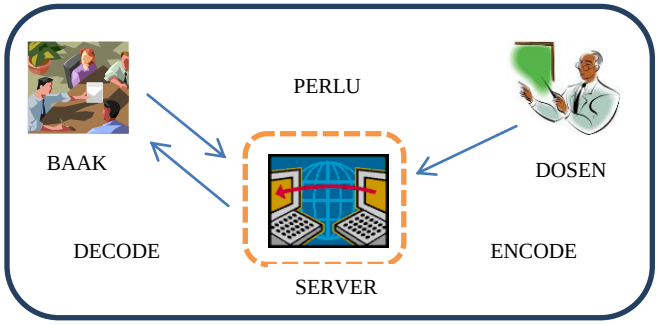
IV. HASIL DAN PEMBAHASAN

Teknik Steganografi Modifikasi LSB dilakukan dengan memodifikasi bit-bit yang termasuk bit LSB pada setiap byte warna pada sebuah pixel. Bit-bit LSB ini akan dimodifikasi dengan menggantikan setiap LSB yang ada dengan bit bit informasi lain yang ingin disembunyikan. Setelah semua bit informasi lain menggantikan bit LSB di dalam file tersebut, maka informasi telah berhasil disembunyikan. Ketika informasi rahasia tersebut ingin kembali dibuka, maka bit-bit LSB yang sekarang ada, diambil satu per satu kemudian disatukan kembali menjadi sebuah informasi yang utuh seperti semula. Penentuan bit-bit LSB dilakukan secara berurutan, mulai dari byte awal sampai byte terakhir sesuai panjang dari data rahasia yang akan disembunyikan. Mengubah bit LSB hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya tidak berpengaruh terhadap persepsi visual/auditori[5].

Pada pembahasan kali ini bisa diilustrasikan proses data data yang dikirim oleh dosen ke server dalam bentuk file/dokumen dokumen penting bisa digunakan teknik steganografi untuk melindungi keabsahan dari suatu data.



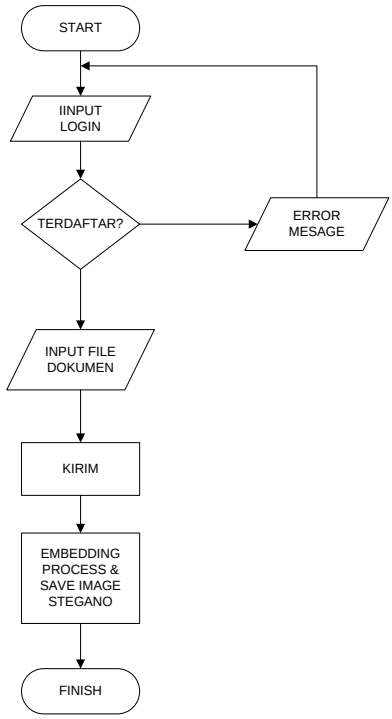
Gambar 2 Illustrasi



Gambar 3 Setelah Ada Proses Decode & Encode

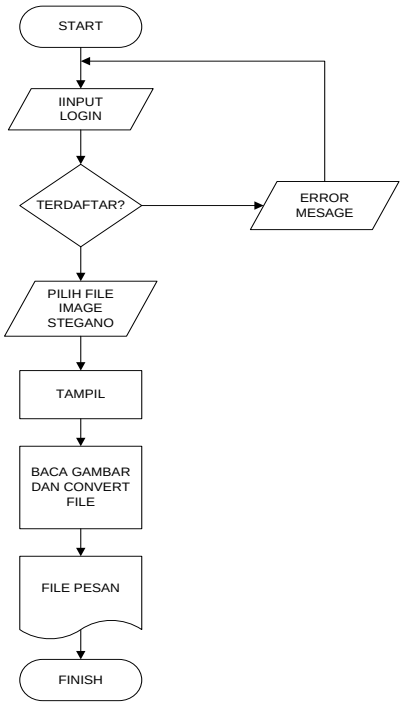
A. *Tahapan Flowchart*

Setelah tahapan pola piker dan alur dari konsep sudah didapatkan maka disini akan diperlihatkan tahapan flowchartnya. Berikut adalah tahapan dalam flowchart pada saat penyisipan pesan.



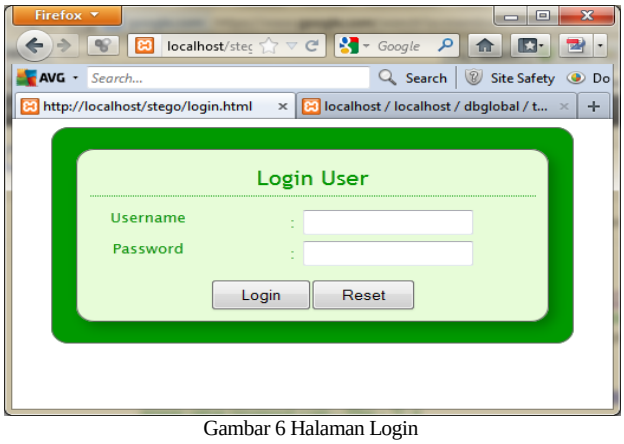
Gambar 4 Flowchart Embedding

Berikut adalah gambar flowchart untuk mengembalikan pesan text yang disisipkan, sehingga menghasilkan pesan text dari gambar.

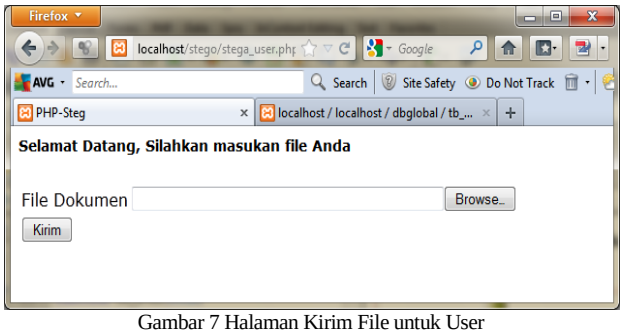


Gambar 5 Flowchart Ekstraksi

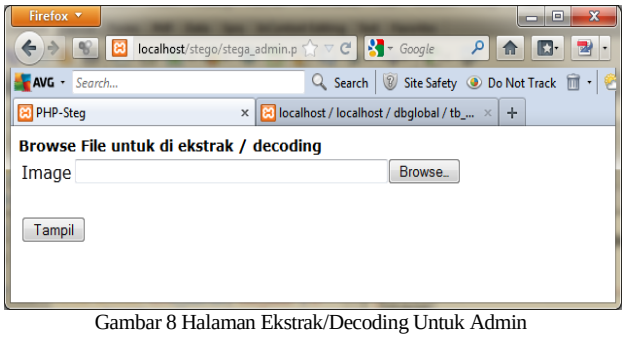
B. Hasil Percobaan



Gambar 6 Halaman Login



Gambar 7 Halaman Kirim File untuk User



Gambar 8 Halaman Ekstrak/Decoding Untuk Admin

C. Analisa

Dari hasil analisa flowchart gambar 4, dapat dijelaskan alur program yaitu program akan meminta memasukan login terlebih dahulu, apabila login berhasil, maka user dapat menginput file atau dokumen yang akan diproses, tombol kirim akan mengaktifkan bahwa file siap disimpan. Sedangkan untuk analisa flowchart pada gambar 5, dapat dijelaskan bahwa alur program setelah input halaman login maka program akan membuka pesan atau text yang disisipkan pada gambar yang sudah kita lakukan proses stegano, pilih image dan tampilkan file pesan.

V. KESIMPULAN

Penelitian ini dapat ditarik beberapa kesimpulan, yaitu :

1. Steganografi merupakan metode untuk menyembunyikan pesan di dalam sebuah pesan baik yang berupa image, suara, dan file-file yang mengandung teks tanpa menunjukan ciri-ciri perubahan yang nyata atau terlihat dalam kualitas dan struktur dari file semula sehingga orang lain tidak menyadari bahwa ada sesuatu didalam pesan tersebut.
2. Keunggulan teknik steganografi dibandingkan dengan teknik kriptografi yaitu dengan steganografi keberadaan pesan yang disembunyikan tidak dapat dideteksi dengan mudah karena pesan disembunyikan sedemikian rupa sehingga tidak akan menimbulkan kecurigaan. Sedangkan untuk kriptografi keberadaan dari informasi yang disembunyikan dengan jelas diketahui.
3. Dengan menggunakan teknik steganografi memungkinkan untuk memvalidasi kebenaran suatu data yang diterbitkan secara online.

DAFTAR PUSTAKA

[1] David, Murtado A. dan Kasma Utin.“Steganografi Gambar Dengan MetodeLeast Significant Bit Untuk Proteksi Komunikasi Pada Media Online”. Program Studi Teknik Informatika, Sekolah Tinggi Manajemen Informatika dan Komputer Pontianak, 2012.

[2] Sasongko, Jati. “Pengamanan Data Informasi menggunakan Kriptografi Klasik,” Fakultas Teknologi Informasi, Universitas Stikubank Semarang, 2005.

[3] Westfeld Andreas. “Steganalysis in the Presence of Weak Cryptography and Encoding,” Technische Universit¨at Dresden Institute for System Architecture, Germany, 2006.

[4] Aditya Yogie, Pratama Andhika dan Nurlifa Alfian. “Studi Pustaka Untuk Steganografi Dengan Beberapa Metode,” Fakultas Teknologi Industri, Universitas Islam Indonesia, 2010.

[5] Maulana, Ahmad Mansur, “Data Hiding Steganograph Pada File Image Menggunakan Metode Least Significant Bit,” PENS-ITS, Surabaya, 2009.