APLIKASI PENGAMANAN DATA EMAIL DENGAN TEKNIK STEGANOGRAFI

Zaenal Rifai[1], Solichul Huda[2]
[1,2]Program Studi Teknik Informatika, Fakultas Ilmu Komputer
Universitas Dian Nuswantoro Semarang
Jl. Nakula I No 5-11 Semarang 50131
Telp : (024) 3517361, Fax : (024) 3520165
Email : huda@dosen.dinus.ac.id[2]

Abstrak

Pengamanan pesan yang dikirim lewat email merupakan aplikasi penting. Aplikasi pengamanan email sudah tersedia di internet, namun aplikasi yang dapat mengamankan pesan dalam berbagai format file dan mudah dibawa, sejauh yang peneliti ketahui belum ada. Paper ini menawarkan aplikasi pengamanan pesan lewat e-mail menggunakan teknik steganografi yang mudah dibawa kemana-mana dan pesan dalam berbagai format. Modifikasi yang digunakan adalah Least Significant Bit (LSB) dan Method Red Green Blue Level (RGB). Ujicoba yang dilakukan menunjukkan bahwa pesan yang dapat disembunyikan di file format BMP terdiri dari 4 format file yaitu Doc, TXT, RTF dan PDF.

Kata Kunci : *Pengamanan, email, steganografi, LSB, RGB*

Abstract

Email message security is an important application. Email monitoring application has already provided in internet, but application that is able to secure message in various file format and portable, as far as the researcher know, does not exist. This paper discusses about email message security application using steganography method that is easy to be carried anywhere and supports various format message. Modification method uses Least Significant Bit (LSB) and Red Green Blue Level (RGB) Method. Testing that is done showed that hidden message in BMP format file consists of 4 format files, those are Doc, Txt, RTF and PDF.

Keywords : *Security, email, steganography, LSB, RGB*

1. LATAR BELAKANG

Teknologi informasi dan komunikasi saat ini merupakan bagian penting dalam manajemen informasi. Selain memiliki potensi dalam menyaring data dan mengolah menjadi informasi, teknologi informasi mampu menyimpannya dengan jumlah kapasitas jauh lebih banyak dari cara-cara manual. Salah satu pekerjaan yang akan sangat membantu teknologi informasi, yaitu pekerjaan dalam menyembunyikan pesan. Steganografi merupakan ilmu yang mempelajari, meneliti, dan mengembangkan seni menyembunyikan sesuatu informasi. Pada saat itu teknik ini sudah sering dilakukan untuk menyampaikan pesan-pesan rahasia. Berbagai teknik dalam steganografi dipergunakan menyembunyikan pesan dalam sebuah file gambar. Teknik ini semakin maju sehingga dapat dipergunakan untuk menyembunyikan file dalam berbagai format file misalnya TXT dan RTF.

File media merupakan komponen penting pada proses penyembunyian informasi ini. Dengan file yang terlihat sama sekali tidak mencurigakan, data anda yang sebenarnya akan tetap tidak

terdeteksi dengan mata telanjang. Pada umumnya file yang ada di dalam komputer dapat digunakan sebagai media penyembunyian, seperti file gambar berformat PNG (*Portable Network Graphics*), JPEG (*Joint Photographic Experts Group*), GIF (*Graphics Interchange Format*), BMP (*Bitmap*), atau di dalam music MP3 (*Media Player*), atau bahkan di dalam sebuah film dengan format WAV (*Waveform Audio Format*) atau AVI (*Audio Video Interleave*).

Kemudian pada data digital, teknik-teknik yang sering digunakan dalam steganografi modern antara lain : Modifikasi *Least Significant Bit* (LSB), *Mask and Filtering*, Algoritma kompresi dan transformasi, dan Teknik *Pixel Mapping* yang dikenal dengan Metode Modifikasi *RedGreenBlue* (RGB) Level.

Pengamanan email sangat penting untuk menjamin kenyamanan user berkomunikasi [1]. E-mail merupakan salah satu bentuk komunikasi lewat jaringan komputer. Bentuk komunikasi ini membuat user berkomunikasi dengan biaya yang murah dan akses yang cepat. Komunikasi lewat email membuat user nyaman karena komunikasi tetap berjalan ketika salah satu pelaku komunikasi off line.

Penyadapan, pemalsuan, penyusupan, spamming adalah bentuk gangguan komunikasi lewat email [2]. Penyusupan biasanya menjadi masalah yang sering muncul dalam e-mail ini.

Ada beberapa aplikasi pengamanan komunikasi lewat email, salah satunya Pretty Good Privacy (PGP)[3]. User dapat menggunakan PGP untuk mengirimkan pesat lewat e-mail. Pesan yang akan dikirim akan dienkripsi sebelum di kirim lewat e-mail dan akan didekripsi oleh email penerima. Walaupun begitu, aplikasi ini mempunyai rumus enkripsi yang sama untuk semua user dan dipakai oleh semua user.

Oleh karena itu dalam paper ini ditawarkan pengaman data yang dikirim lewat email dimana pengamannya menggunakan teknik steganografi. Steganografi ini akan menyembunyikan pesan lewat file digital sehingga tidak membuat hacker tertarik untuk membukanya

2. TINJAUAN PUSTAKA

2.1. Pengertian Steganografi

Steganografi adalah suatu ilmu dan seni menyembunyikan pesan. Steganografi membutuhkan dua properti yaitu tempat menyembunyikan dan pesan yang akan disembunyikan. Steganografi juga menggunakan media digital sebagai tempat menyembunyikan pesan diantaranya tesk, audio, citra dan video. Pesan yang akan disembunyikan dapat berupa tesk, audio, citra dan video[4].

Berikut ini media yang dapat dipergunakan untuk menyembunyikan pesan dalam teknik Steganography yaitu :

A. Teks

Algoritma Steganografi yang menggunakan teks sebagai media penyipanan biasanya digunakan teknik NLP sehingga teks yang tersebut tidak mencurigakan

B. Audio

File audio juga dapat dipergunakan untuk menyembunyikan pesan, karena biasanya file dengan format ini berukuran relatif besar. File yang berukuran besar dapat menampung pesan dalam jumlah yang besar juga.

C. Citra
File citra juga sering digunakan. Format ini sering dikirim lewat internet. Selain itu tersedia algoritma Steganography untuk tempat penyembunyian yang berupa file citra.
D. Video
File ini sebagian besar berukuran relatif sangat besar. Walaupun begitu, file ini diangap kurang praktis karena ukurannya besar. Selain itu masih sedikit algoritma yang mendukung format ini.

Steganografi dapat dipandang sebagai kelanjutan kriptografi. Pada kriptografi pesan disandikan (*ciphertext*), sehingga data tetap terlihat oleh user. sedangan steganografi *ciphertext* tersebut dapat disembunyikan dalam media digital, sehingga pesan tidak terlihat. Secara umum, steganografi adalah cara menyisipkan informasi/pesan pada file digital. Informasi/pesan tersebut tidak terlihat karena tampilan didominan oleh media yang tempat menyembunyikan.

2.2 Teknik Steganografi
Ada 2 jenis teknik yang sering digunakan dalam steganografi modern yaitu :
1. *Least Significant Bit Insertion* (LSB)
2. Teknik *Pixel Mapping* (Metode RGB Level)
Pada paper ini teknik yang digunakan adalah Teknik Modifikasi LSB, dan Metode RGB Level yang merupakan pengembangan dari teknik *Grey Level Modification* (GLM).

2.3 Kriteria Steganografi
Proses penyembunyian pesan ke dalam citra digital (*image*) akan mengubah kualitas citra tersebut. Kriteria yang harus diperhatikan dalam penyembunyian data agar dapat menghasilkan steganografi itu baik adalah :

A. Ketepatan (*Fidelity)* adalah mutu citra asli dengan citra setelah disisipi hampir sama. Setelah penambahan data rahasia, citra hasil steganografi masih terlihat dengan baik, user tidak mengetahui adanya pesan dalam citra tersebut
B. Ketahanan (*Robustness)* adalah pesan yang disembunyikan harus tahan (*robust*) terhadap berbagai operasi manipulasi yang dilakukan pada citra penampung, seperti pengubahan kontras, penajaman, pemampatan, rotasi, pembesaran gambar, pemotongan (*cropping*), enkripsi dan sebagainya. Bila tempat menyembunyikan dilakukan operasi-operasi pengolahan citra tersebut, maka data yang disembunyikan seharusnya tidak rusak (tetap valid jika diekstraksi kembali). Proses *robustness* ini tidak dilakukan pada aplikasi steganografi ini.
C. Pemulihan (*Recovery)* adalah Data yang disembunyikan harus dapat diungkapkan kembali (*reveal*). Karena tujuan steganografi adalah menyembunyikan data, maka sewaktu-waktu data rahasia di dalam citra penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

2.4 Cara Kerja Steganografi

2.4.1. LSB *(Least Significant Bit)*
Bentuk yang paling umum digambarkan untuk serangkaian bit ini adalah 8 bit yang sering disebut dengan istilah 1 byte.

Jika pada susunan bit di dalam sebuah byte, ada bit yang paling berarti MSB (*Most Significant Bit*) dan bit yang

paling kurang berarti LSB (*Least Significant Bit*). Misalnya pada byte 11010010, bit 1 yang paling pertama (digarisbawahi) adalah bit MSB dan bit 0 yang terakhir (digarisbawahi) adalah bit LSB.

Penyembunyian data pada teknik steganografi Modifikasi LSB dilakukan dengan mengganti bit-bit di dalam segmen citra (*image*) dengan bit-bit pesan. Bit yang akan diganti adalah bit LSB, karena penggantian hanya mengubah nilai byte tersebut satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte tersebut di dalam gambar menyatakan warna tertentu, maka perubahan satu bit LSB tidak mengubah warna tersebut secara signifikan. Keuntungan teknik ini perubahan yang ada tidak terlihat oleh mata manusia.

Sebagai sebuah contoh, segmen pixel-pixel citra sebelum penambahan bit-bit informasi adalah :

00110011	10100010
11100010	01101111

Informasi yang telah dikonversi ke sistem biner adalah 01100001 (huruf = a). Bilangan biner dari informasi tersebut kemudian dibagi dua bit menjadi 01, 10, 00, 01. Setiap dua bit dari informasi tersebut menggantikan posisi LSB dari segmen data citra menjadi :

00110001	10100010
11100000	01101101

Teknik penyembunyian data untuk citra 8-bit berbeda dengan citra 24-bit. Pada citra 8-bit, setiap elemen data bitmap menyatakan indeks dari peta warnanya di palet RGB. Pada citra 24-bit menggunakan 8 bit untuk setiap channel warna merah, hijau dan biru. Pixel tersebut mampu merepresentasikan 224 atau 16.777.216 nilai warna.

Perubahan maksimum dalam setiap pixel akan menjadi 26 atau 64 nilai warna, dimana hal ini merupakan bagian yang kecil dari seluruh ruang warna. Perubahan yang kecil ini tidak tampak oleh mata manusia. Contoh lainnya, misalkan suatu gambar 735 pixel x 485 pixel dapat menghandel 735*485*6 bit/pixel*1byte/8bit = 267.356 byte data.

Pesan yang disembunyikan di dalam citra dapat dibaca kembali dengan cara *reveal/extraction*. Bit-bit LSB diambil satu per satu dan disatukan kembali menjadi sebuah informasi.

2.4.2 Metode RGB (Red, Green, Blue) Level

Teknik ini merupakan teknik pengembangan dari teknik GLM (*Grey Level Modification*), jika pada metode GLM gambar yang digunakan adalah gambar hitam putih (*Grayscale*) maka dengan metode RGB Level ini kita dapat menggunakan gambar RGB yang terdiri dari tiga tingkatan warna, yaitu : R (*red*), G (*green*), dan B (*blue*). Warna = RGB(30, 75, 255). Putih = RGB (255,255,255), sedangkan untuk Hitam= RGB(0,0,0). Algoritma RGB ini sama seperti algoritma GLM. Algoritma ini dirancang dengan tujuan untuk menyembunyikan informasi di dalam sebuah gambar. Teknik penyembunyian gambar dengan metode RGB level ini menggunakan citra 16-bit. Sebagai sebuah contoh, pixel-pixel citra sebelum penambahan bit-bit informasi adalah :

101 98 67 77 99 103 68 98 90 65
102 99 77 97 109 153 68 98 90 65

101 98 67 77 99 103 68 98 90 65
103 98 67 77 99 103 68 98 90 65

Maka pertama-tama kita merubah pixel diatas yang bernilai ganjil menjadi genap, sehingga pixel-pixelnya menjadi:

100 98 66 76 98 102 68 98 90 64
102 98 76 96 108 152 68 98 90 64
100 98 66 76 98 102 68 98 90 64
102 98 66 76 98 102 68 98 90 64

Misal informasi yang akan disisipkan dalam citra tersebut adalah huruf a (bilangan ASCII = 97), maka jika dikonversi ke sistem biner menjadi 0000 0000 0110 0001. Dan pixel yang dihasilkan setelah penambahan bit-bit informasi adalah :

100 98 66 76 98 102 68 98 90 65
103 98 76 96 108 153 68 98 90 64
100 98 66 76 98 102 68 98 90 64
102 98 66 76 98 102 68 98 90 64

Untuk contoh yang lain misalnya terdapat Gambar berukuran 100 *pixel* x 100 *pixel* dengan *color encoding* 24 bits dengan R = 8 bits, G = 8 bits, B = 8 bits, maka *color encoding* akan mampu mewakili 0 ... 16.777.215 (mewakili 16 juta warna), dan ruang *disk* yang dibutuhkan = 100 x 100 x 3 byte (karena RGB) = 30.000 bytes = 30 KB atau 100 x 100 x 24 bits = 240.000 bits.

3. METODE

3.1 Tahap Sistem Steganografi

Pembangunan aplikasi sistem steganografi dilakukan tahapan analisis kebutuhan yaitu :

A. Menentukan masalah yang dibangun aplikasi steganografi. Sistem yang akan dibangun merupakan implementasi steganografi didalam file *gambar.*
B. Mengumpulkan data – data yang diperlukan untuk membangun sebuah sistem, yaitu berupa teknik – teknik yang digunakan dalam steganografi.
C. Menentukan metode inferensi yang digunakan.
D. Menentukan target user yang akan menggunakan sistem steganografi ini.
E. Usulan aplikasi sistem yang dibangun.

3.2 Identifikasi Input

Dalam identifikasi input hal pertama yang harus dilakukan adalah mengumpulkan fakta – fakta atau informasi yang nantinya akan diperlukan dalam pembuatan aplikasi, untuk memecahkan masalah dan selanjutnya akan diolah oleh aplikasi sistem steganografi. Semua ini dilakukan dalam upaya mengamankan informasi yang di anggap sangat penting kerahasiaannya.

Daftar file input sistem implementasi steganografi yang dibangun ini ditunjukkan dalam Tabel 1.

Tabel 1: Tabel Enkripsi

No	File
1.	Pesan Rahasia (**.Txt*)
2.	Image Penampung (**.Bmp*)

3.3 Identifikasi Output

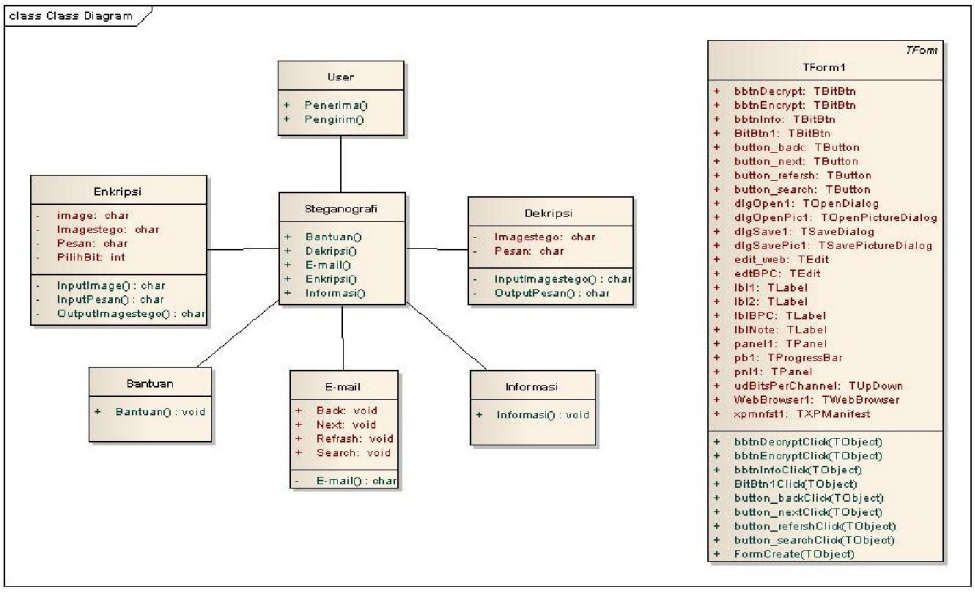
Jika sistem steganografi enkripsi telah menerima input, maka akan dihasilkan suatu output berupa *gambar* yang sudah berisi sebuah pesan rahasia. Dan pesan rahasia tersebut tidak akan bisa terlihat dengan panca indara manusia, karena antara file gambar yang sudah disisipi dengan gambar aslinya sangatlah mirip dan hampir tidak ada perbedaan yang signifikan.

Daftar output dari sistem aplikasi steganografi ditunjukkan dalam Tabel 2.

Tabel 2: Tabel Dekripsi

No	File
1.	Image stego (*.*Bmp*)
2.	File Pesan rahasia (*.*Txt*)

3.4 Analisis Kebutuhan Pengguna



Gambar 1. Class Diagram Steganografi

A. Pengirim
Dalam hal ini, pengirim merupakan pengguna yang akan memanfaatkan aplikasi steganografi. Dalam proses ini kami menyebutnya dengan proses enkripsi data.

B. Penerima
Dalam hal ini, penerima akan menerima sebuah file Imagestego (*gambar*) yang didalam *gambar* tersebut telah tersimpan sebuah pesan rahasia yang hanya bisa diketahui dengan melakukan proses deskripsi. Tanpa melakukan proses deskripsi ini pesan rahasia yang dikirimkan tidak akan bisa diketahui.

3.5 Membangun Desain Aplikasi

3.5.1 Use Case Model

Use case diagram digunakan untuk memodelkan system. Proses berdasarkan perspektif pengguna system, yang terdiri atas diagram untuk use case dan *actor*.

Actor merepresentasikan *orang* yang akan mengoperasikan atau orang yang berinteraksi dengan sistem aplikasi[5].

Use case merepresentasikan operasi-operasi yang dilakukan oleh *actor*. Use case digambarkan berbentuk *elips* dengan *nama operasi* dituliskan di dalamnya. *Actor* yang melakukan operasi dihubungkan dengan garis lurus ke use case.

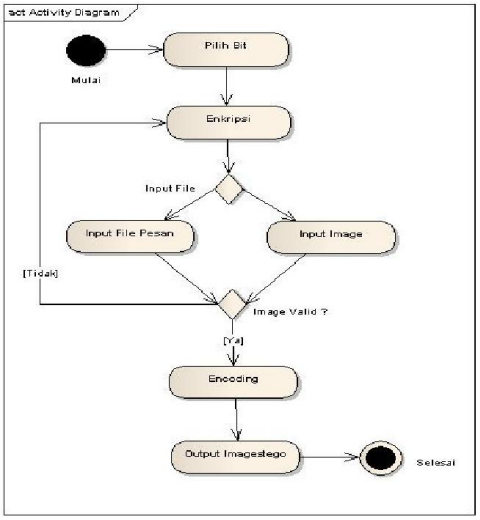
3.5.2 Class Diagram

Gambar 1 di atas menunjukkan class diagram yang merupakan diagram yang selalu ada di permodelan sistem berorientasi objek. Class diagram menunjukkan hubungan antar *class* dalam sistem yang sedang dibangun dan

bagaimana mereka saling berkolaborasi untuk mencapai suatu tujuan.

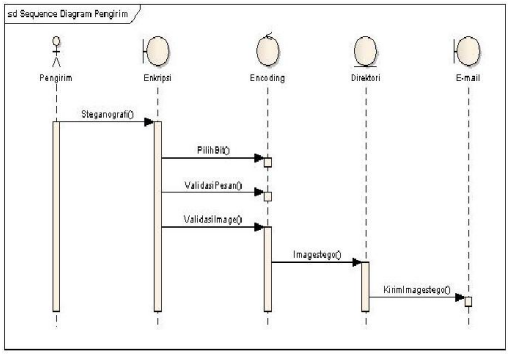
3.5.3 Proses Enkripsi Data Dan Image

Case diagram enkripsi data ke dalam image ditunjukkan dalam Gambar 2.



Gambar 2. Activity Diagram

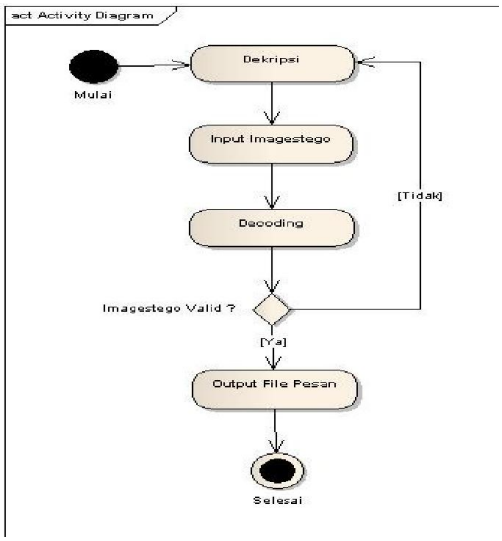
Sedangkan sequence diagram enkripsi ditunjukkan dalam gambar 3.



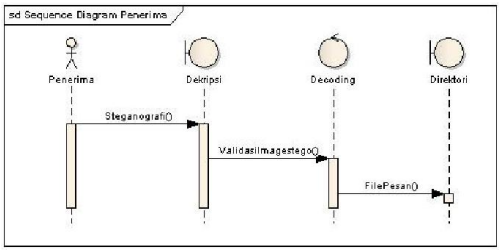
Gambar 3. Sequence Diagram Enkripsi

3.5.4 Proses Dekripsi Data Dan Image

Untuk case diagram proses dekripsi data dan image ditunjukkan dalam Gambar 4. Sedangkan untuk sequence diagram dekripsi ditnjukan dalam Gambar 5.



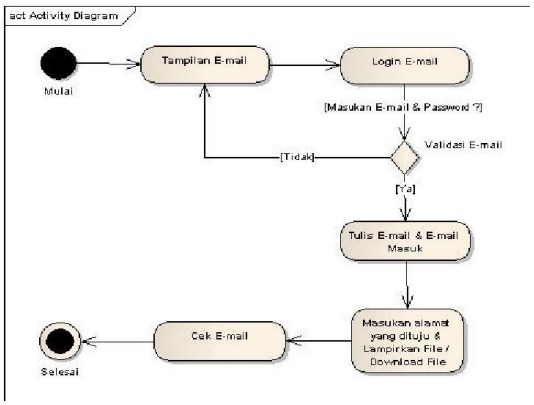
Gambar 4. Activity Diagram Dekripsi



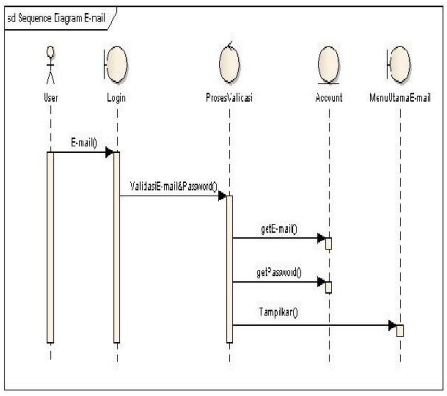
Gambar 5. Sequence Diagram Dekripsi

3.5.5 Proses E-mail

Case diagram proses email ditunjukkan dalam Gambar 6. Sedangkan sequence diagram email ditunjukkan dalam Gambar 7.



Gambar 6. Activity Diagram E-mail.



Gambar 7. Sequence Diagram E-mail.

4. PEMBAHASAN

4.1. Pengujian Sistem

Untuk menguji aplikasi pengamanan steganografi ini, pengujian dilakukan dengan mengirimkan pesan 6 kali. Pesan yang dikirim dalam 6 format yang berbeda yaitu txt, ppt, rtf, doc, 3GP dan PDF. Sedangkan file yang dipergunakan untuk menyembunyikan dalam format BMP. Pengujian dilakukan terhadap proses enkripsi dan dekripsi. Hasil pengujian enkripsi ditunjukkan dalam tabel 3.

Tabel 3: Hasil pengujian enkripsi

No	Pesan Rahasia	Image Penampung	Image Stego	Hasil
1	File.Txt 286 Bytes	Image.Bmp 1.04 MB	Image. Bmp 1.04 MB	Sukses
2	File.Rtf 1.18 KB	Image.Bmp 900 KB	Image. Bmp 900 KB	Sukses
3	File.Ppt 187 KB	Image.Bmp 1.37 MB	Image Tidak Cukup Menampung File	Gagal
4	File.Doc 123 KB	Image.Bmp 1.37 MB	Image. Bmp 1.37 MB	Sukses
5	File.3Gp	Image.Bmp	Image	Gagal
	2.16 MB	1.37 MB	Tidak Cukup Menampung File	
6	File.Pdf 41.6 KB	Image.Bmp 1.37 MB	Image. Bmp 1.37 MB	Sukses

Tabel 4: Proses Pengujian Enkripsi

No	ImageStego	Pesan Rahasia	Hasil
1	Image.Bmp 1.04 MB	File.Txt 286 Bytes	Sukses
2	Image.Bmp 900 KB	File.Rtf 1.18 KB	Sukses
3	Image.Bmp 1.37 MB	File.Doc 10.2 KB	Sukses
4	Image.Bmp 1.37 MB	File.Pdf 41.6 KB	Sukses

Pengujian dengan 6 kali pengiriman pesan menunjukkan bahwa 5 pesan berhasil di enkripsi dan 1 pesan gagal dienkripsi. Kegagalan ini diakibatkan oleh file penampung pesan tidak dapat memuat pesan yang dikirim dalam bentuk PPT. Sedangkan dari 5 pesan yang dapat dienkripsi, pesan dalam format 3GP tidak dapat didekripsi kembali.

Aplikasi penyembunyian pesan dengan steganografi ini dibuat dalam file excutable, sehingga file tersebut mudah dibawah. Untuk menggunakan aplikasi tersebut diperlukan komputer yang terkoneksi ke internet.

4. KESIMPULAN

Dari uraian diatas, dapat disimpulkan bahwa teknik steganografi dapat diterapkan untuk pengamana pesan yang akan dikirim lewat e-mail.

Penggunaan metode *Least Significant Bit* (LSB) dan Metode RGB sangat baik untuk teknik menyembunyikan pesan didalam *image Bitmap. Image bitmap* mampu menyimpan file atau pesan yang ukurannya besar, seperti file *.Txt, *.Rtf, *.Pdf, dan *.Doc. Aplikasi steganografi dapat diimplementasikan dalam pengamanan pesan yang dikirim lewat e-mail. Implementasi keamanan pesan dalam aplikasi ini yaitu pesan tidak dapat terlihat ketika pesan e-mail dibuka. Aplikasi ini dapat dibawa dengan mudah dikarenakan tidak memerlukan media penyimpanan yang besar dapat dapat dijalankan di sistem operasi windows.

DAFTAR PUSTAKA

[1] Arif, R., M., 2007, e-Mail Security**,** *Seminar Nasional Teknologi 2007 (SNT 2007),* ISSN : 1978 – 9777

[2] Indocisco, Email security, Materi pelatihan

[3] Husni, 2010, Keamanan komputer, *Teknik Informatika, Universitas Trunojoyo*, Materi kuliah

[4] Ermadi Satria Wijaya,2004, *Konsep Hidden Message Menggunakan Teknik Steganografi*, Media Informatika, Vol. 2,.

[5] Nurokhim, Rohmah, Nur, R., 2002, *Case Tool Pengembangan Perangkat Lunak Berorientasi-objek menggunakan Unified Modeling Language (UML)*. EMITOR, Jurnal Teknik Elektro dan Komputer.