Aplikasi Steganografi Menggunakan LSB *(Least Significant Bit)* dan Enkripsi Triple Des Menggunakan Bahasa Pemrograman C#

Teguh Budi Harjo[1], Marly Kapriati[2], Dwi Andrian Susanto[3]
[1,2,3]Program Studi Pascasarjana, Magister Ilmu Komputer, Universitas Budi Luhur
Email : tepanzz@gmail.com[1], mkapriati@gmail.com[2], dwiandriansusanto@gmail.com[3]

Abstrak - Steganografi adalah sebuah teknik yang digunakan dalam penyembunyain pesan dalam sebuah gambar. Steganografi merupakan sebuah ilmu yang sudah ada sejak jaman terdahulu yang digunakan untuk menghindari berbagai ancaman dari berbagai penyerang. Dengan teknik ini diharapkan dapat menyembunyikan pesan maupun data digital.

Dalam tulisan ini akan dibahas tentang cara menyembunyikan pesan melalui gambar dengan metode LSB *(Least Significant Bit)* dan enkripsi Triple DES *(Data Encryption Standard)*. Metode LSB *(Least Significant Bit)* merupakan teknik penyembunyian pesan dalam steganografi dimana penyembunyian pesan rahasia dilakukan dengan mengganti bit-bit dalam segmen gambar dengan bit-bit pesan rahasia. Sedangkan enkripsi Triple DES *(Triple Data Encryption Standard)* merupakan salah satu algoritma simetris pada kriptografi yang digunakan untuk mengamankan data dengan cara menyandikan data. Dengan penulisan ini kita akan lebih mengerti bagaimana cara menyembunyikan pesan dengan menggunakan steganografi dan kriptografi.

Kata Kunci — Steganografi, *Least Significant Bit* (LSB), Kriptografi, TripleDES, C#.

I. PENDAHULUAN

A. Latar Belakang

Teknik menjaga kerahasiaan pesan tidak hanya menggunakan kriptografi. Teknik lain yang dapat digunakan yaitu steganografi. Steganografi adalah seni dan ilmu untuk menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui. Berbeda dengan kriptografi yang merahasiakan makna pesan namun keberadaan pesan tetap ada, steganografi merahasiakan dengan menutupi atau menyembunyikan pesan.

Salah satu metode steganografi citra digital adalah *Least Significant Bit* (LSB), dengan teknik penyembunyian pesan pada lokasi bit terendah dalam citra digital. Pesan dikonversi ke dalam bentuk bit biner dan disembunyikan pada citra digital dengan metode LSB. Implementasi metode LSB tanpa dilengkapi dengan sistem keamanan berpeluang untuk dapat dibongkar dengan mudah melalui teknik pemecahan analisis frekuensi dengan membaca bit terendah.

Pada jurnal ini penulis akan membahas tentang steganografi menggunakan LSB (*Least Significant Bit*) dan kriptografi Triple DES.

Tujuan penulisan ini adalah penulis ingin mengimplementasikan metode penyisipan document pada media gambar dengan merancang program aplikasi steganografi dengan metode LSB (*Least Significant Bit*) dan kriptografi Triple DES.

Karena bahasan mengenai steganografi dan kriptografi terlalu luas maka penulis memberikan batasan, masalah yang akan dibahas, yaitu:

1. Penelitian dan implementasi steganografi hanya menggunakan metode LSB (*Least Significant Bit*)
2. Output sistem steganografi berupa file (.bmp)
3. Document yang dicoba untuk disisipkan dengan steganografi memiliki format (.docx, .pdf, .ppt, .xls, .zip)

Penulis hanya melakukan implementasi menggunakan bahasa pemrograman C#.

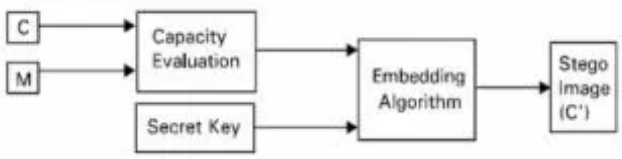
II. STUDI LITERATUR

A. Steganografi

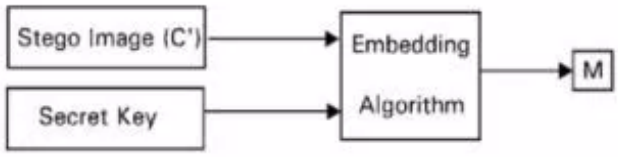
Steganografi berasal dari bahasa yunani "*steganos*" yang artinya "tersembunyi" atau "terselubung" dan "*graphein*" yang artinya "menulis". *Steganografi* dapat diartikan "tulisan tersembunyi" (*cover writing*). *Steganografi* adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui (Rakhmat, 2010).

Steganografi membutuhkan dua properti: wadah penampung dan data rahasia yang akan disembunyikan. *Steganografi* digital menggunakan media digital sebagai wadah penampung, misalnya: voice, video, image dan teks. Data rahasia yang disembunyikan jugadapatberupa voice, video, image dan teks (Saputra, 2012).

Proses steganografi bisa dilihat pada gambar 1 dan gambar 2.



Gambar 1. Cara Penyembunyian Pesan Steganografi



Gambar 2. Cara Pengambilan Pesan Steganografi

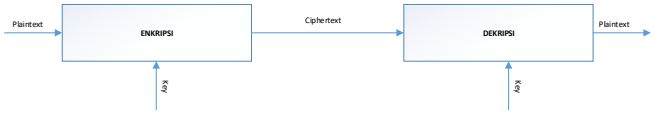
B. Metode LSB (Least Significat Bit)

LSB (*Least Significant Bit*) merupakan metode stegnografi yang paling sederhana dan mudah untuk diimplementasikan ke sebuah aplikasi. Metode ini menggunakan citra digital sebagai convertext. Pada susunan bit di dalam sebuah byte (1 byte = 8 bit), ada bit yang paling berarti (*most significant bit atau MSB*) dan bit yang paling kurang berarti *(least significant bit atau LSB).* (Rakhmat, 2010).

C. Kriptografi

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim kepenerima tanpa mengalami gangguan dari pihak ketiga. Menurut Bruce Scheiner dalam bukunya "Applied Cryptography", kriptografi adalah ilmu pengetahuan dan seni menjaga pesan tetap aman (Fairuz abadi, 2010).

Dalam kriptografi diperlukan parameter yang digunakan untuk proses konversi data yaitu suatu set kunci. Enkripsi dan dekripsi data dikontrol oleh sebuah kunci atau beberapa kunci (dafid, 2006). Proses enkripsi dan dekripsi dalam kriptografi.



Gambar 3.Proses Enkripsi/Dekripsi

D. Triple DES Kriptografi

Triple DES merupakan kriptografi simetris dengan kunci *encrypt* dan *decrypt message* adalah sama. Triple DES merupakan penyempurnaan dari kriptografi DES sebelumnya. Pada Triple DES pengenkripsian pesan dilakukan sebanyak tiga kali.

Enkripsi ini dapat dicapai dengan beberapa cara. Sebagai contoh, pesan dapat dienkripsi dengan kunci 1, dekripsi dengan kunci 2 (pada dasarnya enkripsi yang lain), dan dienkripsi lagi dengan kunci 1:

[E{E[E(M,K1)],K2},K1]

Sama dengan diatas:

[E{E[E(M,K1)],K2},K3]

Persamaan terakhir menggambarkan enkripsi Tripel DES-EEE3 dengan tiga kunci yang berbeda dan merupakan bentuk yang paling aman dari Triple DES.

III. ANALISA DAN PERANCANGAN

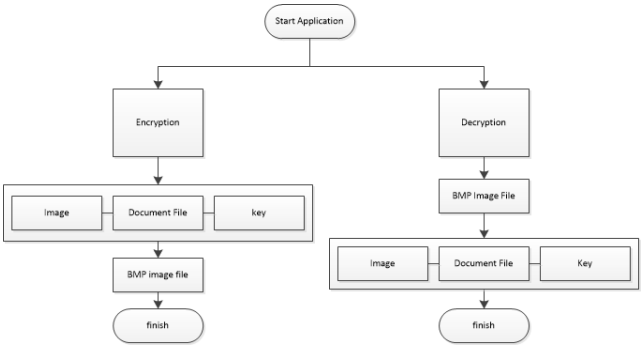
A. Analisis

Perancangan aplikasi menggunakan bahasa pemrograman C# untuk implementasi steganografi dan kriptografi. Adapun dua proses yang terjadi dalam implementasi steganografi yaitu proses enkripsi dan dekripsi. Enkripsi adalah proses penyisipan document kedalam gambar dan Dekripsi adalah proses ekstraksi untuk mengeluarkan document atau pesan asli.

B. Perancangan Aplikasi

Aplikasi steganografi yang akan diusulkan yakni membuat sebuah aplikasi yang dapat digunakan untuk menyembunyikan dokumen/pesan rahasia dengan stegannografi metode LSB (*Least Significant Bit*) dan kriptografi Triple DES.

Gambar alur perancangan aplikasi bisa dilihat pada gambar 4.

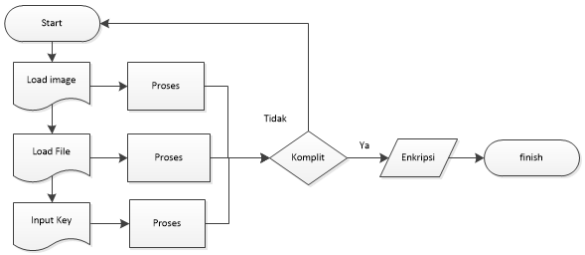


Gambar 4. Alur Perancangan aplikasi

C. Perancangan Aplikasi

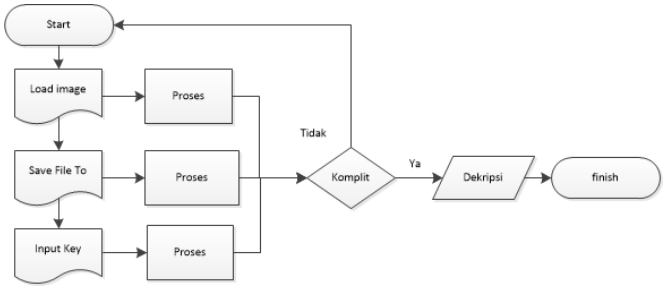
Dalam membuat suatu aplikasi rancangan layar merupakan suatu hal yang sangat penting. Rancangan layar harus mudah dimengerti, agar dalam menggunakan aplikasi ini pemakai atau pengguna merasa nyaman dalam menggunakan aplikasi.

Flowchart untuk enkripsi image dapat dilihat pada gambar 5.



Gambar 5.*Flowchart Encypt Image*

Flowchart untuk dekripsi image dapat dilihat pada gambar 6.

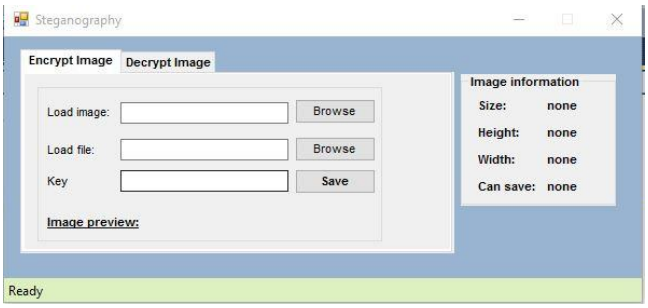


Gambar 6.*Flowchart Decrypt Image*

IV. PERANCANGAN SISTEM

A. Form Encypt Image

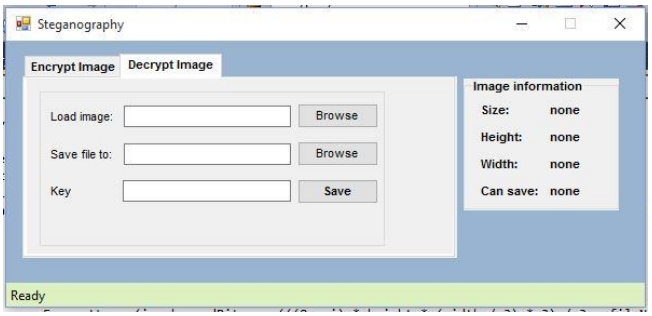
Pada gambar 7 merupakan tampilan layar form *Encypt Image* yang berfungsi untuk melalukan enkripsi dan menyisipkan dokumen/pesan rahasia terhadap gambar.



Gambar 7.Tampilanlayar encrypt image

B. Form Decrypt Image

Pada gambar 8 merupakan tampilan layar *Decrypt Image* yang berfungsi untuk melalukan dekripsi dan menyisipkan dokumen/pesan rahasia terhadap gambar.



Gambar 8.Tampilanlayar decrypt image

V. HASIL PENGUJIAN APLIKASI

1. Pengujian Menggunakan Format PDF

Setelah dilakukan proses enkripsi ukuran gambar yang dihasilkan dengan file pesan yang diuji mengalami banyak perubahan dari segi warna. Semakin besar file yang diujikan maka semakin besar pula kualitas citra warna yang berubah. Adapun hasil perubahan pada file gambar tersebut bisa dilihat pada gambar 9 dan dijelaskan pada tabel 1.

Gambar 9. Hasil Enkripsi Dengan Format Pdf

Tabel 1. Hasil Enkripsi Pesan Pdf

Nama File	pdf.bmp
Size	0.9 MB (1.028.332 bytes)
Width	586 pixels
Height	584 pixels

a. Pengujian Menggunkaan Format PPT

Setelah dilakukan proses enkripsi ukuran gambar yang dihasilkan dengan file pesan yang diuji tidak terlalu mengalami banyak perubahan dari segi warna hanya saja ukuran gambar yang berubah. Adapun hasil perubahan pada file gambar tersebut bisa dilihat pada gambar 10 dan dijelaskan pada tabel 2.

Gambar 10. Hasil Enkripsi Dengan Format Ppt

Tabel 2. Hasil Enkripsi Pesan Ppt

Nama File	ppt.bmp
Size	560 KB (573,928 bytes)
Width	586 pixels
Height	584 pixels

b. Pengujian Menggunkaan Format XLS

Setelah dilakukan proses enkripsi ukuran gambar yang dihasilkan dengan file pesan yang diuji tidak terlalu mengalami banyak perubahan dari segi warna hanya saja ukuran gambar yang berubah. Adapun hasil perubahan pada file gambar tersebut bisa dilihat pada gambar 11 dan dijelaskan pada tabel 3.

Gambar 11. Hasil Enkripsi Dengan Format Xls

Tabel 3. Hasil Enkripsi Pesan Xls

Nama File	xls.bmp
Size	354 KB (363,466 bytes)
Width	586 pixels
Height	584 pixels

c. Pengujian Menggunkaan Format Doc

Setelah dilakukan proses enkripsi ukuran gambar yang dihasilkan dengan file pesan yang diuji tidak terlalu mengalami banyak perubahan dari segi warna hanya saja ukuran gambar yang berubah. Adapun hasil perubahan pada file gambar tersebut bisa dilihat pada gambar 12 dan dijelaskan pada tabel 4.

Gambar 12. Hasil Enkripsi Dengan Format Doc

Tabel4. Hasil Enkripsi Pesan Doc

Nama File	docx.bmp
Size	460 KB (471,660 bytes)
Width	586 pixels
Height	584 pixels

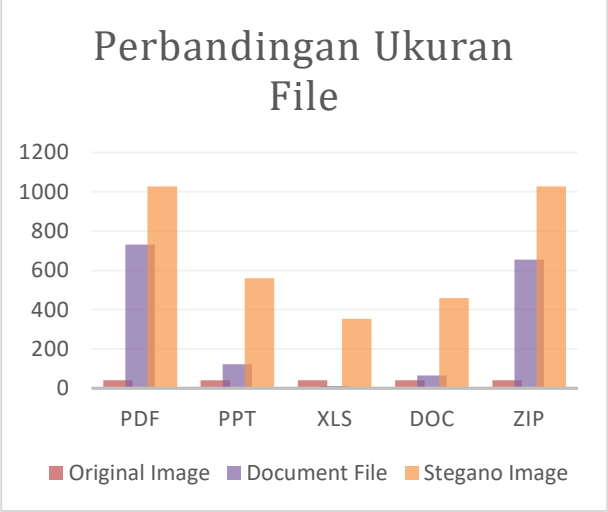
d. Pengujian Menggunakan Format Zip

Gambar 13. Hasil Enkripsi Dengan Format Zip

Tabel5. Hasil Enkripsi Pesan Zip

Nama File	zip.bmp
Size	0.98 MB (1,028,949 bytes)
Width	586 pixels
Height	584 pixels

Dengan adanya grafik perbandingan ukuran file diatas terlihat bahwa file bertipe pdf dan zip mengubah ukuran hasil stegano image menjadi lebih besar dibandingkan file dengan ukuran laindapatdilihatpadagambar 14.



Gambar 14. Chart Hasil Perbandingan Steganografi

VI. KEKURANGAN DAN KELEBIHAN

Pengujian aplikasi *steganografi* untuk pengamanan dokumen dilakukan dengan tujuan untuk mengetahui keseluruhan program aplikasi *steganografi* ini sudah dapat berjalan dengan baik dan benar.

Program aplikasi ini harus dikembangkan seiring dengan kebutuhan dan kemajuan teknologi yang semakin berkembang dan meningkatnya kebutuhan yang semakin beragam sehingga dapat memenuhi kebutuhan tersebut, berikut kekurangan dan kelebihan aplikasi *steganografi*:

a. Kekurangan program
1. Aplikasi baru bisa mengeluarkan output dengan format .bmp.
2. Gambar yang disisipkan dengan dokument format pdf mengalami kehancuran yang cukup serius.
3. Gambar yang di cropping mengalami kehancuran pesan sehingga pesan yang disisipkan tidak bisa ditampilkan.

b. Kelebihan program
1. Untuk melakukan enkripsi pesan tidak memerlukan waktu yang lama.
2. Gambar asli yang telah disisipkan dokumen tidak mengalami perubahan dengan format dokumen (doc, xls, ppt).
3. Gambar hasil steganografi yang sudah diubah bentuk (misalkan: coret gambar) akan tetap menampilkan pesan
4. Gambar hasil steganografi yang sudah disisipkan pesan mengalami perubahan ukuran.

VII. PENUTUP

Berdasarkan analisa yang telah dilakukan, Penulis menemukan beberapa kesimpulan dan saran yang mungkin diperlukan untuk pengembangan aplikasi ke tahap berikutnya.

a. Kesimpulan

Adapun kesimpulan yang diperoleh penulis dari hasil perancangan, pembuatan serta uji coba dan analisa program aplikasi steganografi ini, maka penulis dapat membuat kesimpulan antara lain:

1. Hasil dari penerapan untuk penyisipan pesan rahasia pada gambar berjalan dengan baik. Pesan atau dokumen yang disisipkan pada file gambar dapat diperoleh kembali secara utuh atau dengan kata lain pesan yang disisipkan sebelum proses enkripsi dan setelah proses dekripsi mempunyai hasil yang sama tanpa ada perubahan pesan atau gangguan.
2. Aplikasi steganografi yang telah dihasilkan dari implementasi menggunakan metode LSB *(Least Significant Bit)* memberikan suatu hal yang menarik untuk diterapkan bagi institusi-institusi yang berkepentingan untuk menjaga kerahasiaan.
3. Dengan metode LSB *(Least Significant Bit)*, image yang disisipkan pesan atau dokumen tidak terlalu banyak terlihat perbedaan dari citra warna terkecuali disisipkan pesan atau dokumen dengan ukuran besar.
4. Output gambar hasil enkripsi mengalami perubahan ukuran file gambar.

b. Saran

Selain menarik beberapa kesimpulan, penulis juga mengajukan beberapa saran yang mungkin bisa dijadikan pertimbangan dalam pengembangan aplikasi steganografi sebagai berikut:

1. Tampilan layar bisa lebih disempurnakan lagi agar tampak lebih menarik dan memudahkan pengguna dalam pemakaiannya.
2. Menambahkan metode kompresi agar ukuran image atau size tidak terlalu besar setelah disisipkan pesan ataupun dokumen.
3. Mengeluarkan output gambar yang lebih beragam karena aplikasi saat ini hanya mengeluarkan output bertipe (.bmp).
4. Bukan hanya pesan atau document saja yang bisa disisipkan ke image (misal voice, video, mp3).

DAFTAR PUSTAKA

[1] Rakmat, Basuki.,dan Fairuzabadi, Muhammad. 2010. Steganografi menggunakan Metode Least Significant Bit dengan Kombinasi Algoritma Kriptografi Vignere dan RC4

[2] Abdul Jalid, Alfian. 2013. Aplikasi Pengamanan data dan informasi dengan Metode Steganografi LSB dan Algoritma Kriptografi Triple DES menggunakan Bahasa Pemrograman C#

[3] Saputra, Hasbian. 2012. Implementasi Algoritma steganografi Embedding dengan Metode Least Significant Bit (LSB) Insertion dan Huffman coding pada pengiriman pesan menggunakan media MMS berbasis J2ME

[4] Prihanto, Agus.,dan Sri Wahyuningsih, Suluh. 2009. Penyembuyian dan Pengacakan Data Text Menggunakan Steganografi dan Kriptografi Triple DES pada Image.