Penyembunyian Pesan Dengan Menggunakan Steganografi LSB Dan Algoritma Enkripsi Serpent Pada Citra Digital

Pradhipta Ramadhinara H
Mahasiswa Pasca Sarjana, Universitas Budi Luhur
Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, Indonesia, 12260
dithorh@gmail.com

M. Khoirul Anam
Mahasiswa Pasca Sarjana, Universitas Budi Luhur
Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, Indonesia, 12260
andez.shared@gmail.com

Danna Saputra
Mahasiswa Pasca Sarjana, Universitas Budi Luhur
Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, Indonesia, 12260
danna.saputra22@gmail.com

Abstract*— Perkembangan teknologi informasi dalam aspek komunikasi mendorong kemajuan teknologi internet. Internet yang memiliki jangkauan luas dan transfer data yang cepat membuat manusia beralih ke teknologi ini. Hal ini membuat internet menjadi salah satu kebuthan manusia dalam menjalankan aktivitas sehari – harinya. Karena dengan internet informasi yang dapat dikirim maupun diakses menjadi sangat mudah dan cepat. Namun teknologi internet mempunyai kelemahan dimana pesan yang kita kirim dapat diambil ataupun dimodifikasi oleh orang yang tidak bertanggung jawab. Oleh karena itu dibutuhkan suatu teknik untuk melindungi pesan tersebtu dari pihak yang tidak berkepentingan. Metode itu ialah steganografi dan kriptografi. Dalam penulisan ini penulis mengusulkan menggunakan metode Least Significant Bit (LSB) dan algoritma enkripsi Serpetn. Dimana sebelumnya belum ada yang menggunakan algoritma Serpent ini dengan mengkombinasikan LSB yang akan dibuat dalam sebuah aplikasi dengab berbasiskan bahasa programming Java. Dengan aplikasi ini, maka pesan yang ingin dikrimkan dapat disisipkan dalam sebuah citra digital yang kemudian akan dienkripsi dengan algoritma Serpent untuk meningkatkan keamanan dari pesan tersebut. Sehingga menghindari pencurian data dan modifkasi data dari pesan yang dikirimkan.

Keywords*— steganography, Least Significant Bit (LSB), Serpent algoritma, enkripsi

I. PENDAHULUAN

Dengan pesatnya perkembangan teknologi informasi, hampir sebagian orang lebih memilih menggunakan internet sebagai media transfer data dalam kehidupan sehari – hari yang memiliki jangkauan yang luas dan dengan waktu yang sesingkat mungkin. Karena hal ini maka privasi di dalam komunikasi digital menjadi suatu kewajiban dasar ketika seseorang ingin saling bertukar informasi.

Oleh karena itu dibutuhkan suatu teknik dimana ketika ada pihak yang ingin saling bertukar informasi dapat melakukanya dengan aman. Artinya informasi yang terjadi pada aktivitas pertukaran tersebut benar – benar sampai kepada pihak yang dituju dan informasi tersebut valid sesuai dengan aslinya. Teknik yang dimaksud ialah steganografi dan kriptografi.

Steganografi meruapakan seni dan ilmu untuk menyembunyikan pesan dalan suatu media penampung, yaiu audio, visual ataupun gabungan keduanya. Pesan yang disembunyikan dalam suatu media tersebut tidak terlihat secara kasat mata apabila itu sebuah gambar dan tidak terdengar perbedaanya apabila sebuah suara. Hal ini bertujuan agar pesan yang disembunyikan tersebut hanya bisa dibaca oleh pihak yang dituju dan pesan tersebut tetap terjaga keaslianya. Metode yang digunakan dalam menyembunyikan pesan dalam steganografi.

Metode LSB atau *Least Significant Bit* merupakan metode yang paling sering digunakan dalan steganografi. Karena dengan metode ini gambar ataupun suara yang telah di-encode tidak akan terlihat atau terdengar perbedaannya dibandingkan dengan sumber aslinya. Caranya dengan memodifikasi bit terakhir atau bit paling rendah dari file media dengan bit – bit data atau informasi yang akan disembunyikan, dan hanya menyebabkan perubahan nilai bit lebih tinggi atau lebih rendah. Sedangkan metode MSB atau *Most Significat Bit* caranya hampir mirip dengan LSB, perbedaanya ialah MSB memodifikasi bit – bit awal dari suatu file media, sehingga akan menyebabkan perubahan yang signifikan terhadap media aslinya. Dan oleh sebab itu dapat dengan mudah ditangkap dengan indra manusia. Maka dari itu metode ini jarang digunakan dan biasanya apabila digunakan selalu digabungkan dengan metode lainya agar dapat menutup kekurangan yang telah disebut tadi.

Untuk meningkatkan keamanan informasi yang disembunyikan tidak hanya digunakan steganografi saja, tetapi juga menerapkan kriptografi. Kriptograpi merupakan ilmu untuk mengenkripsi suatu data agar data tersebut tidak bisa dimodifkasi dan juga tidak bisa digunakan oleh orang yang tidak mempunyai akses.

II. LANDASAN TEORI

A. Steganografi

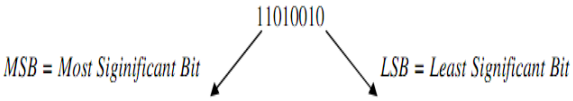
Steganografi (steganography) merupakan kata yang berasal dari bahasa Yunani yaitu steganos yang artinya tersembunyi atau terselubung dan graphein atau graptos, yang artinya menulis sehingga artinya adalah menulis tulisan yang tersembunyi atau terselubung.

Steganografi didefinisikan sebagai ilmu dan seni untuk menyembunyikan pesan rahasia (hiding message) sedemikian rupa sehingga keberadaan pesan tidak terdeteksi oleh indera manusia. Steganografi merupakan suatu cabang ilmu yang mempelajari tentang bagaimana menyembunyikan suatu informasi – rahasia di dalam suatu informasi lainnya [1].

B. Least Significant Bit (LSB)

Metode LSB telah terbukti memiliki sifat imperceptibility (sesuatu yang tidak diketahui) yang baik, kapasitas datanya cukup kecil, karena hanya bisa menyimpan pada LSB setiap pixel pada warna. Sehingga pihak ketiga tidak menyadari adanya pesan rahasia yang tersimpan di dalam stego image tersebut. Informasi yang disembunyikan berupa data ASCII, dikonversikan dan diambil nilai binernya, kemudian baru disisipkan [2].

Pada susunan bit di dalam sebuah byte (1 byte = 8 bit), ada bit yang paling berarti (Most Significant Bit atauMSB) dan bit yang paling kurang berarti (Least Significant Bit atau LSB). Berikut contoh sebuah susunan bit pada sebuah byte:



Untuk memperkuat teknik penyembunyian data, bit-bit data rahasia tidak digunakan mengganti byte-byte yang berurutan, namun dipilih susunan byte secara acak. Misalnya jika terdapat 50 byte dan 6 bit data yang akan disembunyikan, maka byte yang diganti bit LSB-nya dipilih secara acak, contoh byte nomor 36, 5, 21, 10, 18, 49. Penerapannya dapat dilihat pada gambar 2 berikut ini:

41	42	43	44	45	46	47	48	49	50
31	32	33	34	35	36	37	38	39	40
21	22	23	24	25	26	27	28	29	30
11	12	13	14	15	16	17	18	19	20
1	2	3	4	5	6	7	8	9	10

Gambar 2 Proses Penempatan Bit Pesan

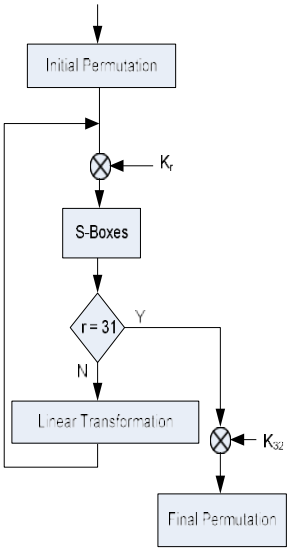
C. Kriptografi

Kriptografi (*cryptographic*) merupakan teknik yang digunakan untuk menjamin keamanan dari aktivitas pertukaran data, seperti kerahasiaan data, integritas data, serta autenktikasi data [3]. Untuk menjamin keamanan pertukaran data, dapat dilakukan dengan berbagai cara, salah satunya dengan proses penyandian dengan menggunakan algoritma sandi. Proses penyandian dilakukan agar data yang dikirim tidak dapat dimengerti oleh pihak selain yang memiliki akses terhadap data tersebut Dalam proses penyandian terdapat dua konsep utama yaitu enkripsi dan dekripsi.

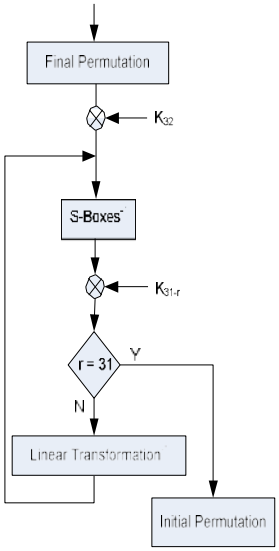
Enkripsi merupakan proses yang mengubah data atau informasi yang akan dikirim menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya. Enkripsi biasanya dilakukan sebelum data atau informasi tersebut dikirimkan. Dalam kriptografi data atau informasi yang dapat dimengerti maknanya dikenal dengan *plaintext* atau *clear text*, sedangkan informasi yang telah disamarkan dikenal dengan *ciphertext* [3].

D. Algoritma Serpent

Serpent merupakan algoritma cipher blok yang memiliki ukuran blok sebesar 128 bit dan mendukung ukuran kunci sebesar 128, 192, atau 256 bit. Cipher ini berbentuk Substitution-Permutation Network (SP-network) yang merupakan rangkaian operasi-operasi matematis yang saling berhubungan. SP-network memiliki S-boxes dan P-boxes yang mengubah blok bit masukan menjadi suatu bit keluaran.



Gambar 3 Proses Enkripsi



Gambar 4 Proses Dekripsi

Serpent mendukung masukan kunci sepanjang 128 bit, 192 bit, dan 256 bit. Kenyataannya, dalam mekanisme penjadwalan kunci dibutuhkan kunci sepanjang 256 bit. Oleh karena itu, untuk masukan kunci sepanjang 128 bit dan 192 bit memerlukan mekanisme tambahan, yaitu padding. Padding menambahkan bit "1" pada bit terpenting (most significant bit) dan beberapa bit "0" sampai ukuran kunci mencapai 256 bit.

Untuk proses enkripsi, Serpent membutuhkan 32 upakunci 128 bit yang dinotasikan dengan K0, … , K32. Tahapan untuk mendapatkan ke-33 upakunci yaitu [4]:

1. Membagi kunci masukan K menjadi delapan bagian, masing-masing 32 bit yang dinotasikan dengan w-8, … , w-1
2. Membentuk 132 kunci antara (*prekey*) yang dinotasikan dengan w0, … , w131 melalui persamaan:

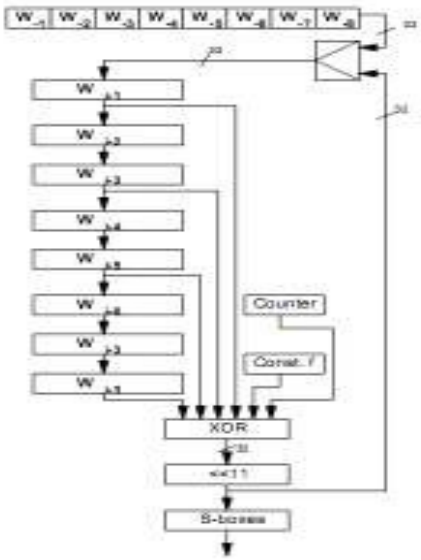
$$wi = \oplus\, wi\text{-}5 \oplus wi\text{-}3 \oplus wi\text{-}1 \oplus Ø \oplus i) <<< 11$$

Notasi Ø merupakan bagian kecil dari *golden ratio* ($\sqrt{5}$ + 1) / 2 atau 0x9e3779b9 dalam heksadesimal

3. Membentuk 132 kunci putaran (*round key*) k_0 sampai k_{131} yang dibentuk dari kunci antara yang dihasilkan dari proses sebelumnya dengan menggunakan *S-boxes*. *S-boxes* digunakan untuk mengubah kunci antara w_i menjadi k_i dengan ketentuan berikut ini :

$$\{k_0, k_1, k_2, k_3\} = S_3 (w_0, w_1, w_2, w_3)$$
$$\{k_4, k_5, k_6, k_7\} = S_2 (w_4, w_5, w_6, w_7)$$
$$\{k_8, k_9, k_{10}, k_{11}\} = S_1 (w_8, w_8, w_{10}, w_{11})$$
$$\{k_{12}, k_{13}, k_{14}, k_{15}\} = S_0 (w_{12}, w_{13}, w_{14}, w_{15})$$
$$\ldots$$
$$\{k_{124}, k_{125}, k_{126}, k_{127}\} = S_4 (w_{124}, w_{125}, w_{126}, w_{127})$$
$$\{k_{128}, k_{129}, k_{130}, k_{131}\} = S_3 (w_{128}, w_{129}, w_{130}, w_{131})$$

Pembentukan kunci putaran untuk tahap (1) sampai tahap (3) dapat digambarkan dalam gambar 3.



Gambar 5 Pembentukan kunci

4. Membentuk upakunci 128 bit K_i (untuk I € {0, …, 32}) dari 32 bit nilai k_j dengan cara:
$$K_i = \{k_{4i}, k_{4i+1}, k_{4i+2}, k_{4i+3}\}$$
5. Menerapkan IP pada upakunci yang dihasilkan untuk menempatkan bit-bitnya ke dalam urutan yang sesuai.
$$i = IP (K_i)$$

Algoritma Serpent digunakan untuk enkripsi bit pada citra digital dengan mengubah mode operasi yang digunakan hingga karakteristiknya menyerupai aliran *cipher*, yaitu dengan metode operasi Counter.

Cara untuk membangkitkan blok *counter* yaitu [DWO01]:

1. Dari satu blok counter awal (T_1), akan diterapkan fungsi penambah untuk membangkitkan blok counter selanjutnya
2. Blok counter akan terbagi menjadi dua bagian, yaitu *message nonce* dan bit yang akan bertambah (*increment*). *Message nonce* akan diambil dari angka acak.
3. Fungsi penambah yang digunakan, didasarkan pada definisi yang diberikan oleh *National Institute of Standards and Technology* (NIST), yaitu:
$$[X]_m = [X + 1 \bmod 2^m]_m$$
m = jumlah bit dalam fungsi penambah

Proses dekripsi dengan mode operasi counter membutuhkan masukan blok *counter* yang digunakan pada proses enkripsi. Oleh karena itu, blok *counter* yang digunakan dalam proses enkripsi akan ikut dikirimkan bersama dengan cipherteks hasil enkripsi.

D. Tinjauan Studi

Tinjauan studi yang dijadikan sebagai acuan dalam melakukan penelitian tesis ini ialah berdasar pada penelitian terkait mengenai penggunaan teknik steganografi pada media citra digital menggunakan metode LSB (Least Significant Bit) dan algoritma enkripsi *Serpent*. Berikut ini merupakan beberapa ringkasan dari penelitian terdahulu dengan cara yang berbeda-beda:

1) Nazori Agani, Ahmad Farisi dan Agnes Aryasanti pada tahun 2013 dalam papernya yang berjudul ImplementationAnd Analysis Steganography Technique of Least Significant Bit (LSB) on Image File menguraikan mengenai sebuah skema implementasi metode LSB untuk menyisisipkan pesan berupa text dan gambar ke dalam sebuah gambar. Stego image yang dihasilkan memiliki kualitas yang baik sehingga secara kasat mata tidak terlihat perbedaan antara cover image dengan stego image [4].
2) M.Anggrie Andriawan, Solikin & Setia Juli Irzal Ismail, melakukan penelitian mengenai implementasi Steganografi pada citra digital file gambar bitmap (BMP) menggunakan java dengan penyisipan pesan ke dalam bit terendah (LSB) bitmap 24 bit. Menyembunyikan pesan rahasia dengan metode LSB untuk mengeksploitasi keterbatasan sistem penglihatan manusia [5].
3) Penelitian yang dilakukan Antonio harianto membandingkan steganografi menggunakan metode Least Significant Bit dan End Of File. Kesimpulan yang didapat dari hasil perbandingan itu adalah file gambar hasil steganografi yang menggunakan metode Least Significant Bit memiliki ukuran yang sama dengan file aslinya, sedangkan file gambar hasil steganografi yang menggunakan metode End Of File memiliki ukuran yang lebih besar dibandingkan file aslinya[6].
4) Penelitian yang dilalkukan Lindayanti mentatakan bahwa pengimplementasian steganografi berbasis Least Significant Bit (LSB) pada gambar dengan penyisipanberukuran variable sudah dapat menghasilkan stego- image yang bila dilhat secara visual memiliki tampilan yang hamper sama dengan covernya [7].
5) Penelitian yang dilakukan oleh Tri cahyadi meneliti steganografi menggunakan metode Least Significant Bit dan mendapat kesimpulan bahwa semakin besar wadah (cover-image) yang digunakan untuk penyembunyian pesan maka semakin besar atau banyak pula jumlah karakter yang dapat disembunyikan dan semakin besar teks yang disembunyikan di dalam citra, semakin besar pula kemungkinan teks tersebut rusak akibat manipulasi pada citra penampung [8].
6) Anggi Alisia Putri dalam tulisanya meneliti engkripsi algoritma Serpent pada media audio. Dari hasil pengujian disebutkan

bahwa dengan mengenkripsi audio menggunakan algoritma Serpent didapat hasil audio yang cukup baik dari file aslinya [9].

E. Hipotesis

Hipotesis dari penelitian ini yaitu memberikan alternatif dalam algoritma enkripsi sekaligus meningkatkan keamanan data dengan menggunakan steganografi untuk menyisipkannya data tersebut kedalam citra digital menggunakan metode LSB dan menggunakan algoritma enkripsi Serpent, sehingga data yang dimaksud tetap aman dari orang yang tidak berkepentingan maupaun yang akan memodifkasinya.

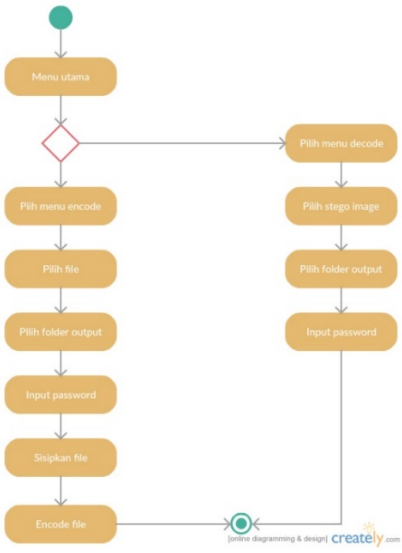
III. METODE PENELITIAN

A. Metode Pengumpulan Data

Untu metode pengumpulan data penulis dalam penelitian ini menggunakan metode pengamatan atau observasi. Observasi adalah kegiatan pengamatan yang direncanakan, sistematis dan hasilnya dicatat serta diinterpretasikan dalam rangka memperoleh pemahaman tentang objek yang diamati [4]. Pada penelitian ini observasi dilakukan dengan cara mempelajari landasan teori yang dibutuhkan mengenai steganografi dan LSB pada beberapa literature dan refersi lainnya. Selain itu penulis juga mempelajari literature mengenai algoritma Serpetn sebgai metode enkripsinya. Observasi selanjutnya adalah dengan melakukan ujicoba.

B. Metode Pengembangan Sistem

Untuk metode pengembangan sistem penulis dalam penelitian ini menggunakan metode *Prototype*. [5] Model ini dimulai dengan pengumpulan kebutuhan. Pendekatan prototyping model digunakan jika pengguna hanya mendefenisikan objektif umum dari perangkat lunak tanpa merinci kebutuhan input, pemrosesan dan outputnya, sementara pengembang tidak begitu yakin akan efisiensi algoritma, adaptasi sistem operasi, atau bentuk antarmuka manusia-mesin yang harus diambil.

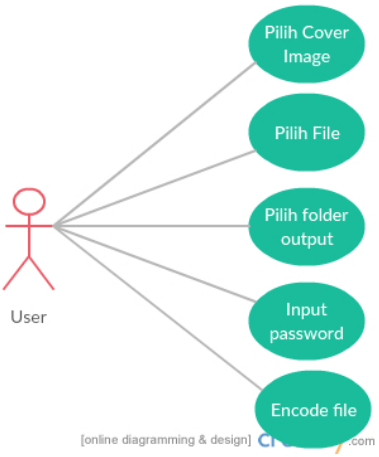


Gambar 4 Activity Diagram aplikasi steganografi

Pada gambar 4 diatas menjelaskan proses alur berjalannya sistem aplikasi steganografi yang akan dikembangkan. Proses yang pertama dimulai adalah user masuk ke menu utama aplikasi. Dari situ user bisa memilih dua menu, yaitu encode dan decode. Apabila memilih menu encode, maka user memilih cover image yang akan digunakan dan file yang akan disisipkan kedalam cover image, kemudian memasukkan password sebagai kunci ekripsi.

Lalu pada menu decode user memilih stego image yang telah di-encode, kemudian memilih folder output dan memasukkan password sesuai dengan password pada saat proses encode.

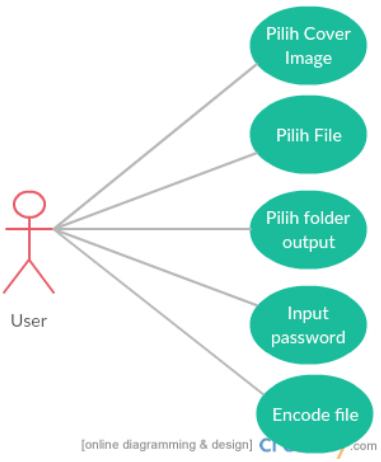
Peneliti membagi menjadi dua *use case* dari *activity diagram* diatas, karena terdapat dua proses, yaitu encode pada gambar 6 dan decode pada gambar 7.



Gambar 6 Use Case Encode

Tabel I
menjelaskan *use case encode*

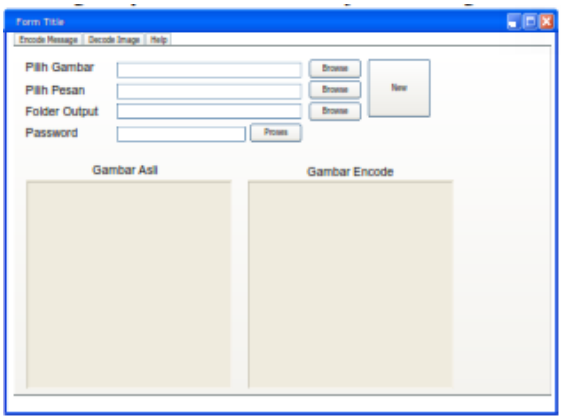
Use case	Penjelasan
Brief description	*Use case* ini memungkinkan actor untuk memilih cover image, file pesan, folder output, memasukkan atau menginput password dan menyisipkan pesan kedalam *cover image*
Actor	User
Pre-Condition	User menyiapkan pesan yang akan disisipka dan menyiapkan tempat penyimpanannya
Main flow	• Use case ini diawali dengan memilih cover image • Pada use case selanjutnya staf memilih file • Selanjutnya user memilih folder output • Kemudian input password • Selanjutnya menyisipkan file kedalam sebuah cover image dengan proses encode
Post-condition	• post-condition setelah file disisipkan kedalam cover image kemudian disimpan



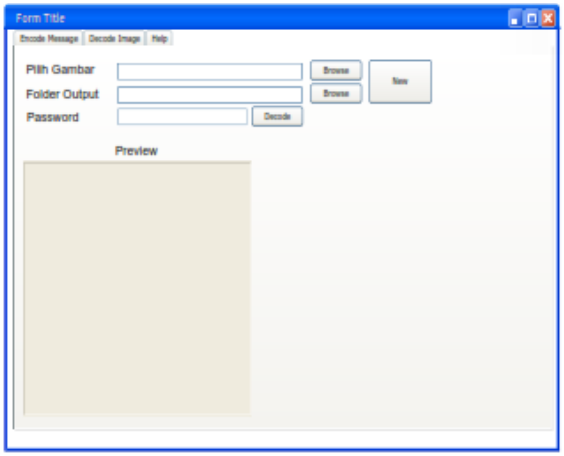
Gambar 7 Use Case Decode

Tabel II
Menjelaskan *use case* decode

Use case	Penjelasan
Brief description	*Use case* ini memungkinkan actor untuk membaca file yang telah disisipkan ke dalam cover image.
Actor	User
Pre-Condition	Kondisi sebelum men-*decode* file user sudah mendapatkan *stego-image* yang disimpan.
Main flow	• Use case ini diawali dengan memilih stego image • Pada use case selanjutnya stego image di *decode* dengan memilih folder output terlebih dahulu dan memasukkan password. • Selanjutnya file asli yang telah disisipkan akan ditampilkan.
Post-condition	• post-condition file yang telah disisipkan kedalam cover image berhasil dibaca.



Gambar 8 Rancangan layar menu encode



Gambar 9 Rancangan layar menu encode

C. Metode Pengujian Sistem

Pada langkah ini menentukan tingkat keberhasilan rancangan yang dibuat apakah dapat menjawab masalah yang dirumuskan. Pada tahap ini dilakukan proses pengujian dan analisis. Proses pengujian dan analisis dilakukkan untuk mengidentifikasi apakah aplikasi yang dikembangkan sesuai dengan analisis system yang telah dibuat. Ujicoba terhadapa alat penguji dilakukan dengan metode kualitatif dan black box.

Metode kualitatif dengan cara melakukan ujicoba terhadap alat penguji dengan berbagai jenis gambar sebagai cover image dan berbagai jenis file sebagai pesan yang akan disisipkan. Gambar digital yang akan diuji akan menggunakan file dengan ektensi PNG. File yang akan dijadikan pesan yang disisipkan akan menggunakan ektensi DOCX. Dari pengujian ini akan diketahui keberhasilan aplikasi penguji mengolah data.

Pengujian pada fungsionalitas dari sebuah sistem perangkat lunak dapat dilakukan menurut dua cara, yaitu pengujian secara white box dan pengujian secara black box. Perbedaan yang mencolok diantara keduanya adalah pengujinya. Black-Box dilakukan oleh pengguna perangkat lunak yang mana hanya memperhatikan input dan outputnya saja. Apabila hasil output telah sesuai dengan input yang diuji, maka perangkat lunak telah lulus uji. Sedangkan White-Box testing biasanya dilakukan oleh tim penguji dari pembuat perangkat lunak. Sehingga yang diperhatikan bukan hanya input dan output, melainkan proses yang terjadi yang mengakibatkan perubahan input menjadi output.

D. Penarikan Kesimpulan

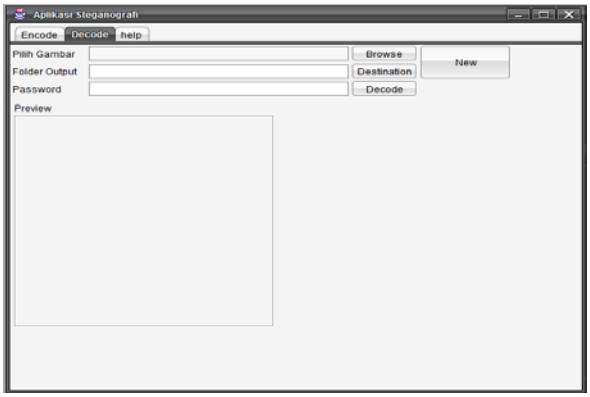
Dari penelitian yang telah dilakukkan, kemudian dilakukan penarikan kesimpulan yang akan menjadi jawaban dari permasalahan, bagaimana mengamankan suatu dokumen penting dengan menerapkan teknik steganografi dengan metode Least Significant Bit (LSB) agar tidak dapak dilihat sembarang orang.

IV. HASIL DAN PEMBAHASAN

A. Implementasi Program

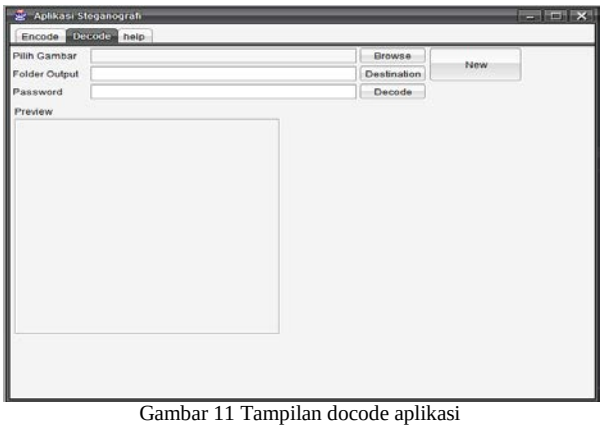
Pada tahap ini peneliti melakukan implementasi sistem yang telah melalui beberapa tahap perancangan. Pada tahap ini peneliti akan membagi penelitian menjadi bagian-bagian yang menjelaskan komponen yang harus diperhatikan dalam implementasi sistem. Tahap ini meliputi spesifikasi perangkat keras, perangkat lunak dan implemetasi program.

Pada saat aplikasi dijalankan langsung tertuju pada tab *encode* seperti gambar 10 dibawah ini. Dalam melakukan penyisipan file, user terlebih dahulu memilih gambar terlebih dahulu sebagai file panampung pesan. Gambar yang dipilih harus berformat jpeg atau png. Setelah itu *user* memilih pesan yang akan disisipkan bisa berupa *.doc, *.pdf atau *.docx.



Gambar 10 Tampilan encode aplikasi

Jika user ingin melakukan pengambilan pesan yang ada pada gambar hasil encode, dapat di lakukan pada tab decode seperti pada gambar 11. pertama yang dilakukan untuk melakukan pengambilan pesan user harus memilih gambar yang telah disisipi pesan dan memilih tempat penyimpanan pesan yang telah di ambil.



Gambar 11 Tampilan docode aplikasi

B. Hasil Pengujian

Pada pengujian sistem atau ujicoba terhadap alat penguji dilakukan dengan metode uji kualitatif, dan black box. Metode uji kualitatif dilakukan dengan cara melakukan ujicoba terhadap alat penguji dengan berbagai gambar sebagai cover image dan berbagai jenis file pesan yang akan disisipkan. Pengujian black box dilakukan untuk mengetahui apakah semua fungsi perangkat lunak telah berjalan semestinya.

Hasil Pengujian Uji Kualitatif

Pengujian kualitatif dilakukan pada alat penguji dengan sample citra digital dan file pesan yang sudah disebutkan diatas. Citra digital tersebut akan disisipi file pesan, kemudian akan dibandingkan ukuran file sebelum disisipi pesan dan setelah disisipi pesan dan dicari selisihnya.

Berikut adalah sample citra digital yang telah disisipi file pesan yang telah dilakukan.

Table III
Hasil Pengujian berdasarkan ukuran file

No	File Citra Digital (PNG)	Ukuran sebelum	File pesan	Ukuran sesudah	Selisih ukuran
1	canvas005-inca-100dpi-00_1. png	18 KB	data 1.docx	18 KB	100 KB
2	canvas005-inca-100dpi-00_2. png	18 KB	data 2.docx	18 KB	98 KB
3	beer_PNG2352 canvas005-inca-100dpi-00_3. png	18 KB	data 3.docx	18 KB	125 KB
4	canvas005-inca-100dpi-00_4. png	18 KB	data 4.docx	18 KB	110 KB
5	canvas005-inca-100dpi-00_5.png	18 KB	data 5.docx	18 KB	137 KB

Pada modul encode disini akan berfungsi sebagai proses penyisipan file pesan ke dalam file citra.

Table IV
Pengujian pada modul encode

Skenario Pengujian	Hasil yang diharapkan	Hasil Pengujian
Memilih citra cover dengan mengklik tombol browse disamping textbox pilih gambar	Menampilkan pop up windows browse	Sesuai yang diharapkan
Memilih tombol open	Menampilkan citra yang dipilih	Sesuai yang diharapkan
Memilih tombol cancel	Kembali ke tab encode	Sesuai yang diharapkan
Memilih file pesan dengan mengklik tombol browse yang ada disamping textbox pilih pesan	Menampilkan pop up windows browse	Sesuai yang diharapkan
Memilih tombol open	Menampilkan file pesan yang dipilih	Sesuai yang diharapkan
Memilih tombol cancel	Kembali ke tab encode	Sesuai yang diharapkan
Memilih folder output dengan mengklik tombol browse yang ada	Menampilkan pop up windows browse	Sesuai yang diharapkan

disamping textbox folder output		
Memilih tombol open	Menampilkan folder output yang dipilih	Sesuai yang diharapkan
Memilih tombol cancel	Kembali ke tab encode	Sesuai yang diharapkan
Menginput password	Menapilkan password	Sesuai yang diharapkan
Tidak menginput password	Menampilkan pop up belum menginput password	Sesuai yang diharapkan
Melakukan proses encode dengan mengklik tombol proses yang ada disamping textbox password	Menampilkan file dialog input nama file	Sesuai yang diharapkan

C. Implikasi Penelitian

Berdasarkan pada penilitian yang telah dilakukan, maka ada beberapa dampak yang dapat dikembangkan :

1) Aspek Sistem
   Aplikasi ini tidak memerlukan spesifikasi computer yang tinggi sehingga dapat berjalan pada computer lama sekalipun.
2) Aspek Penelitian Lanjutan
   Penelitian yang telah dilakukan ini masih memiliki banyak sekali kekurangan dan memerlukan penelitian lanjutan guna melakukan penyempurnaan dalam perancangan dan implementasi aplikasi ini. Oleh karena itu, penulis memberikan saran yang dapat dijadikan acuan untuk penelitian lebih lanjut.
   a) pada penelitian lebih lanjut disarankan untuk menambahkan proses kompresi pada file citra yang telah disisipi file pesan. Sehingga ukuran file yang sudah disisipi file pesan tidak terlalu besar.
   b) Penelitian lebih lanjut disarankan bahwa media yang disisipi file pesan bisa berupa audio dan video.

V. KESIMPULAN DAN SARAN

Kesimpulan yang didapat dari pembuatan aplikasi steganografi ini adalah sebagai berikut:

- Penggunaan metode Least Significant Bit (LSB) tidak mengubah gambar yang disisipkan pesan berubah secara drastis, sehingga tidak mudah tertangkap oleh indera manusia.
- Dengan adanya algoritma Serpent, pesan yang disisipkan menjadi lebih aman. Sebab pesan tersebut diacak dan dan dienkripsi sehingga keaman pesan terjaga dari pihak yang tidak berkepentingan.

Saran untuk penelitian ini lebih lanjut ialah sebagai berikut :

- Media yang digunakan penlitian ini masih terbatas pada citra digital saja. Kedepanya bisa dibuat untuk media audio dan video.
- Ukuran file yang diencode pada aplikasi masih lebih besar disbanding ukuran aslinya. Sehingga perlu adanya kompresi data saat proses encode terjadi.

VI. DAFTAR PUSTAKA

[1] Pebrianti, Wira, 2012.―Pemanfaatan Steganografi Untuk Keamanan Pada Pengiriman Email‖.
[2] Ariyus, Dony, .2009. Pengantar Ilmu Kriptografi, Algoritma Kriptografi Modern,.Jakarta *: Andi Publisher*.
[3] Halik, Idham dan Prayudi,Yudi. Studi dan Analisis Algoritma Rivest Code 6 (Rc6) Dalam Enkripsi/Dekripsi Data. *Program Studi Teknik Informatika, Universitas Islam Indonesia.Yogyakarta*. 2005.
[4] Sugiyono, Metode Penelitian Kuantitatif, Kualitatif dan R&D, Bandung: *Alfabeta*, 2012.
[5] Pahri, Adam. ―Metode pengembangan perangkat lunak. http://www.academia.edu/4844015/Metode_pengembangan_perangkat_lunak. (diakses pada 30 juli 2014).
[6] Nazori Agani, Ahmad Farisi dan Agnes Aryasanti, Universitas Budi Luhur, ―Implementation and Analysis Steganography Technique of Least Significant Bit (LSB) on Image and Audio File‖, *ICIBA2013, the Second International Conference on Information Technology and Business Application Palembang*, Indonesia, 22-23 February 2013.
[7] M.Anggrie Andriawan, Solikin & Setia Juli Irzal Ismail, ―implementasi Steganografi pada citra digital file gambar bitmap (BMP) menggunakan java dengan penyisipan pesan ke dalam bit terendah (LSB),2012.
[8] Antonio, Harianto, ―Studi Perbandingan Enkripsi Steganografi LSB Dengan EOF‖, *Program Studi Teknik Informatika, Universitas Tanjungpura*, Pontianak. 2013.
[9] Lindayanti, ―steganografi berbasis Least Significant Bit(LSB) pada gambar dengan penyisipan berukuran variable‖, *Departemen Ilmu Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam, Institut Pertanian Bogor*, Bogor.2007.
[10] Alisia, Anggi ―Studi dan Implementasi Enkripsi Pengiriman Pesan Suara dengan Algoritma Serpent. Program Studi Teknik *Informatika, Sekolah Teknik Elektro dan Informatika*, Instintut Teknologi Bandung.