

PERANCANGAN APLIKASI STEGANOGRAFI TEKNIK LSB(LEAST SIGNIFICANT BIT) DALAM KEAMANAN KOMPUTER

Irvando¹, Benny Purnama, SE,M.Kom², Ibnu Sani Wijaya,S.Kom,M.S.I³
Teknik Informatika¹³,Sistem Informasi², STIKOM Dinamika Bangsa¹²³, Jambi
Sekolah Tinggi Ilmu Komputer (STIKOM) Dinamika Bangsa, Jambi
E-mail: irvando.218@gmail.com¹, bennip2007@yahoo.com², xxxxxxxxx@xxxx.com³

ABSTRAK

Keamanan file merupakan suatu tindakan yang bertujuan untuk mengamankan data yang penting dalam suatu file dari gangguan pihak lain yang tidak bertanggung jawab terhadap kerahasiaan data. Terkadang ada informasi yang hanya ditujukan untuk orang-orang tertentu atau badan-badan tertentu saja karena sangat dirahasiakannya informasi tersebut.

Keamanan file menjadi suatu kewajiban yang harus dilakukan demi terjaminnya kerahasiaan data dalam suatu file. Teknik LSB atau Least Significant Bit merupakan salah satu teknik yang digunakan dalam steganografi. Teknik ini digunakan dengan cara mengganti bit terakhir citra dengan pesan rahasia. Teknik ini mengurangi kekurangan dari kriptografi yang dapat dengan mudah menimbulkan kecurigaan. Steganografi menyembunyikan informasi rahasia di dalam informasi lain sehingga informasi tersebut tidak dapat diketahui oleh orang lain yang tidak bersangkutan.

Kata kunci: Steganografi, Least Sinificant Bit, Keamanan Komputer

ABSTRACT

Security File is an act that aims to secure critical data in a file of the interference of others who are not responsible for data confidentiality . Sometimes there is information that is intended only for certain people or entities - certain agencies because the information is very secretive.

Security file into an obligation that must be done for the sake of ensuring the confidentiality of data in a file. LSB tehnic or least significant bit is a one of the technic used in steganography. This technique used by replacing the last bit image with a secret message . This technique reduces the shortage of cryptography that can easily arouse suspicion . Steganography hides secret information in other information so that the information can not be known by others who are not concerned

Keywords: Steganography, Least Signicant Bit, Computer Security

1. PENDAHULUAN

1.1 LATAR BELAKANG

Cepatnya perkembangan teknologi informasi saat ini didukung dengan pentingnya kebutuhan akan mendapatkan informasi. Hal ini dapat dilihat dari berkembangnya jaringan internet saat ini yang semakin pesat. Informasi yang dikirimkan tidak hanya informasi untuk semua orang. Terkadang ada juga informasi yang hanya ditujukan untuk orang-orang tertentu atau badan-badan tertentu saja karena sangat dirahasiakannya informasi tersebut.

Seiring dengan perkembangan teknologi tersebut, ancaman terhadap keamanan informasi yang dibutuhkan semakin besar, terutama untuk informasi yang dirahasiakan tersebut. Berbagai ancaman di dunia maya seperti hacker, cracker, carder membuat orang khawatir akan keamanan informasi yang dikirimnya. Kekhawatiran inilah yang membuat pengiriman informasi sedikit terhambat, sedangkan informasi tersebut sangat penting orang-orang tertentu.

Teknik penyembunyian informasi yang cukup terkenal adalah steganografi. Dimana teknik ini mengurangi kekurangan dari kriptografi yang dapat dengan mudah menimbulkan kecurigaan.

Steganografi menyembunyikan informasi rahasia di dalam informasi lain sehingga informasi tersebut tidak dapat diketahui oleh orang lain yang tidak bersangkutan.

Steganografi metode LSB merupakan metoda yang digunakan untuk menyembunyikan pesan pada media digital tersebut berbeda-beda. Contohnya, pada berkas image pesan dapat disembunyikan dengan

menggunakan cara menyisipkannya pada bit rendah atau bit yang paling kanan (LSB) pada data pixel yang menyusun file tersebut.

Untuk menjaga keamanan file yang berupa pesan tentunya perlu suatu cara agar enkripsi file tidak mudah untuk dipecahkan oleh orang lain serta hasil dari stego image tidak menimbulkan kecurigaan. Dengan studi pustaka ini penulis akan membuat sebuah aplikasi Steganografi metode LSB, yang penulis tuangkan dalam sebuah penelitian yang berjudul “PERANCANGAN APLIKASI STEGANOGRAFI TEKNIK LSB (LEAST SIGNIFICANT BIT) DALAM KEAMANAN KOMPUTER”

1.2 RUMUSAN MASALAH

Dari penjelasan di atas maka dapat dirumuskan permasalahan pokok yaitu “Bagaimana merancang suatu sistem keamanan data agar data selain dapat disembunyikan, dapat pula terjaga kerahasiaannya dari pihak yang tidak berwenang”.

1.3 BATASAN MASALAH

Adapun batasan masalah yang terdapat dalam penelitian ini antara lain:

1. Metode yang digunakan adalah LSB (Least Significant Bit).
2. Format file yang dijadikan media untuk menyembunyikan pesan hanya sebatas file gambar berekstensi BMP.
3. Bahasa pemrograman yang dipakai adalah Delphi 7

1.4 TUJUAN DAN MANFAAT PENELITIAN

1.4.1 Tujuan Penelitian

Adapun tujuan dari penelitian ini antara lain:

1. Merancang suatu sistem keamanan data dengan menggunakan metode LSB (Least Significant Bit).
2. Memberikan keamanan kepada user dalam mengirimkan pesan singkat pada jaringan global atau internet.

1.4.2 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan keamanan untuk menyembunyikan, menjaga kerahasiaan data, serta mengintegrasikan data sehingga hanya orang-orang yang berwenang saja yang dapat mengakses data tersebut.

2. LANDASAN TEORI

2.1 PERANCANGAN APLIKASI

2.1.1 Pengertian Perancangan

Perancangan merupakan “rekayasa representasi yang berarti terhadap sesuatu yang hendak dibangun”^[1].

Perancangan adalah “sebuah proses untuk mendefinisikan sesuatu yang akan dikerjakan dengan menggunakan teknik yang bervariasi serta di dalamnya melibatkan deskripsi mengenai arsitektur serta detail komponen dan juga keterbatasan yang akan dialami dalam proses pengejaannya”^[14].

Perancangan adalah “satu proses untuk membuat keputusan tentang apa yang perlu dilakukan oleh organisasi”^[11].

Dari pengertian diatas, maka dapat disimpulkan bahwa perancangan adalah penggambaran, perencanaan dan pembuatan sketsa atau pengaturan terhadap sesuatu yang akan dibangun.

2.1.2 Pengertian Aplikasi

Program aplikasi adalah “program yang direka untuk melaksanakan suatu fungsi bagi pengguna atau aplikasi lain”^[9].

Perangkat lunak aplikasi merupakan “program-program yang dibuat oleh suatu perusahaan komputer untuk para pemakai yang beroperasi dalam bidang umum, seperti pertokoan, penerbitan, komunikasi, penerbangan, perdagangan dan sebagainya”^[15].

Aplikasi adalah “kumpulan perintah program yang dibuat untuk melakukan pekerjaan-pekerjaan tertentu (khusus)”^[8].

Dari pengertian diatas, maka dapat disimpulkan bahwa aplikasi adalah perangkat lunak komputer yang memanfaatkan kemampuan komputer langsung untuk melakukan suatu tugas yang diinginkan pengguna.

2.2 KEAMANAN KOMPUTER

Sistem informasi akademik adalah: Keamanan komputer adalah suatu perlindungan yang diusahakan oleh suatu system informasi dalam rangka mencapai sasaran hasil yang bisa diterapkan atau cara untuk memelihara integritas, kerahasiaan dan tersedianya informasi. Tetapi pada saat ini sistem komputer yang terpasang makin mudah diakses. Sistem time sharing dan akses jarak jauh menyebabkan kelemahan komunikasi data menjadi pokok masalah keamanan. Kelemahan ini menjadi amat serius dengan meningkatnya perkembangan jaringan komputer. Saat ini, implementasi pengamanan sangat penting untuk menjamin sistem tidak diinterupsi dan diganggu. Proteksi dan pengamanan terhadap perangkat keras dan sistem operasi sama pentingnya^[3].

2.3 STEGANOGRAFI PADA FILE GAMBAR

Steganografi adalah “seni atau ilmu menyamarkan sebuah pesan/data rahasia di dalam data atau media yang dampaknya biasa saja”^[4].

Steganografi adalah “ilmu menyembunyikan teks pada media lain yang telah ada demikian sehingga teks yang tersembunyi menyatu dengan media lain. Media tempat menyembunyikan pesan tersembunyi dapat berupa media teks, gambar, audio, atau video. Steganografi yang kuat memiliki sifat media yang telah ditanam teks tersembunyi sulit dibedakan dengan media asli namun teks tersembunyi tetap dapat diekstraksi”^[12].

Steganografi adalah “paduan antara seni dan ilmu pengetahuan yang mempelajari cara menuliskan pesan tersembunyi. Isi maupun arti pesan tersebut hanya bisa diterjemahkan oleh pembuat dan orang yang berhak menerima pesan”^[5].

2.4 LEAST SIGNIFICANT BIT (LSB)

2.4.1 Pengertian Least Significant Bit

Leas Significant Bit (bit paling signifikan, singkatnya LSB) adalah “bit yang terletak paling kanan dan sebuah angka 1 pada posisi itu 2^0 . Sebuah angka 1 berikutnya mempresentasikan 2^1 , pada posisi setelahnya 2^2 dan pada keempat dari kanan 2^3 ”^[2].

Metode Least significant bit (LSB) adalah metode yang paling sering digunakan dalam teknik steganografi, misalnya penyisipan teks kedalam gambar. Dasar dari metode ini adalah bilangan berbasis biner atau dengan kata lain angka 0 dan angka 1. Karena data digital merupakan susunan antara angka 0 dan 1 maka proses penerapannya menjadi mudah. Lebih lanjut lagi, metode ini berhubungan erat dengan ukuran 1 bit dan ukuran 1 byte. 1 byte data dapat dikatakan terdiri dari 8 bit data. Dimana bit pada posisi paling kanan lah yang disebut dengan bit pada posisi LSB (Least Significant Bit).

Teknik steganography dengan menggunakan metode LSB adalah teknik dimana kita mengganti bit pada posisi LSB pada data dengan bit yang dimiliki oleh data yang akan disembunyikan. Karena bit yang diganti hanyalah bit yang paling akhir, maka meskipun data telah berubah, kita tetap tidak akan bisa mengenalinya, karena media stego yang dihasilkan hampir sama persis dengan media sebelum disisipi oleh data yang ingin disembunyikan^[7].

2.4.2 LSB pada gambar 24-bit

Untuk menyembunyikan gambar dengan LSB pada tiap byte gambar 24-bit dibutuhkan 3 bit pada tiap pixel (minimal). Sebuah gambar berukuran 1024 x 768 pixel memiliki potensi untuk menyembunyikan 2.359.296 bit (294,912 bytes) informasi. Apabila pesan yang hendak disembunyikan dikompresi sebelum dimasukkan kedalam gambar lain, informasi berukuran besar pun dapat disembuyikan.

Bagi mata manusia, hasil dari stego-image akan terlihat identik dengan cover image. Ketika menggunakan gambar 24 bit, tiap bit terdiri dari komponen warna merah, hijau, dan biru yang dapat digunakan, karena tiap komponen merepresentasikan satu byte. Dengan kata lain, satu komponen dapat menyimpan 3 bit sekaligus dalam satu pixel.

Contoh LSB pada gambar 24 bit, misalnya kita hendak memasukkan pesan berisi huruf A ke dalam gambar dengan data bit sebagai berikut :

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

Huruf A, pesan yang hendak kita masukkan, memiliki representasi biner 1000011. Bila pesan tersebut dimasukkan ke gambar, bitnya akan menjadi :

(00100111 1110100011001000)
(0010011011001000 11101000)
(1100100000100111 11101001)

Bit yang digarisbawahi merupakan bit-bit yang diubah dari 8 bit yang digunakan. Berdasarkan keseluruhan, rata-rata teknik LSB hanya membutuhkan setengah bit dari gambar aslinya untuk diubah. Setidaknya, kita dapat menyembunyikan data pada bit terakhir atau dua bit terakhir dan mata manusia tetap tidak menyadari adanya perubahan atas hal tersebut^[7].

2.4.3 LSB pada gambar 8-bit

Gambar dengan 8 bit tidak semudah yang dibayangkan untuk diberi teknik LSB karena batasan warna yang digunakan. Oleh karena itu, ada beberapa trik tertentu yang dapat kita gunakan untuk tetap menggunakan LSB pada gambar 8 bit. Salah satunya adalah, cover image harus dipilih secara hati-hati sehingga stego-image tidak akan memberi kesempatan terlihatnya ada keberadaan pesan rahasia di dalamnya.

Bagian yang menyulitkan pada gambar 8-bit berwarna adalah ketika informasi dimasukkan ke dalam gambar tersebut. Untuk tiap palette, warna putih, merah, biru, dan hijau direpresentasikan dengan 00, 01, 10, dan 11 secara berurutan. Misalkan kita hendak memasukkan nilai 1010 kedalam urutan warna putih, putih, biru, dan biru. Maka bit semulanya adalah :
00 00 10 10 setelah menerapkan LSB, hasil yang didapat adalah: 0100 1110

Itu berarti gambar yang semulanya putih-putih-birubiru menjadi merah-putih-hijau-biru. Hal ini tentunya kentara sekali apabila dilakukan. Ini jugalah yang menjadi titik lemah pada LSB 8-bit berwarna. Namun, dengan ini pula dapat ditemukan trik lain yaitu dengan merubah gambar ke format grayscale^[7].

2.4.4 Kelebihan dan Kekurangan teknik *Least Significant Bit* (LSB)

Teknik LSB pada Steganografi ini mempunyai beberapa kelebihan dan kekurangan, diantaranya:

- 1 Kelebihan teknik LSB
 - a Pesan-pesan yang disisipkan tidak menarik perhatian orang lain
 - b Tidak mengubah ukuran file
 - c Mempunyai algoritma yang mudah
- 2 Kekurangan teknik LSB
 - a apesan/data yang disisipkan terbatas, sesuai dengan ukuran citra
 - b perubahan format gambar akan mengakibatkan hilangnya pesan didalamnya
 - c memerlukan banyak ruang untuk dapat menyembunyikan beberapa bit pesan.

2.6 ALAT BANTU PERANCANGAN SISTEM

2.6.1 *Use Case Diagram*

use case adalah “potongan fungsionalitas tingkat tinggi yang disediakan oleh sistem”^[13].

Diagram *use-case* (*use-case diagram*) merupakan “salah satu diagram untuk memodelkan aspek perilaku sistem. Masing-masing diagram *use-case* menunjukkan sekumpulan *use-case*, aktor dan hubungannya. Diagram *use-case* adalah penting untuk memvisualisasikan, menspesifikasikan, dan mendokumentasikan kebutuhan perilaku sistem”^[11].

Use case atau diagram *use case* “merupakan permodelan untuk kelakuan (behavior) sistem informasi yang akan dibuat”^[16].

2.6.2 *Class Diagram*

Diagram kelas untuk menunjukkan peran dan tanggung jawab yang terdapat di entitas-entitas pada sistem yang memberikan perilaku-perilaku sistem^[1].

Diagram kelas digunakan untuk menampilkan kelas-kelas atau paket-paket dalam sistem dan relasi antar mereka^[13].

Diagram kelas atau class diagram menggambarkan struktur sistem dari segi pendefinisian kelas-kelas yang akan dibuat untuk membangun sistem^[16].

2.6.3 Activity Diagram

Diagram aktivitas adalah diagram Flowchart yang diperluas yang menunjukkan aliran kendali satu aktivitas ke aktivitas lain^[1].

Diagram aktivitas atau *activity diagram* menggambarkan workflow (aliran kerja) atau aktivitas dari sebuah sistem atau proses bisnis^[16].

Activity diagram adalah “teknik untuk menggambarkan logika, prosedural, proses bisnis, dan jalur kerja”^[6].

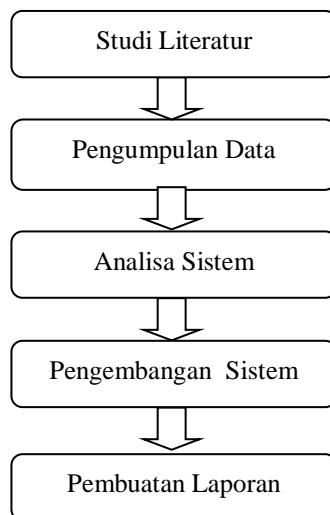
2.6.4 Flowchart Diagram

Flowchart (bagan aliran) adalah “gambar yang menggunakan lambing-lambang baku untuk menggambarkan sistem atau proses”^[17].

Bagan alir program (program *Flowchart*) merupakan “bagan yang menjelaskan secara rinci langkah-langkah proses program, dibuat dari derivikasi bagan alir sistem”^[10].

3. KERANGKA KERJA PENELITIAN

Kerangka kerja penelitian digunakan sebagai acuan atau pedoman dalam agenda penelitian yang akan dilakukan agar penulis dapat melakukan penelitian secara terstruktur dan dapat menyelesaikan penelitian tepat pada waktunya, juga agar penelitian dapat berjalan sesuai dengan yang diharapkan. Tahapan – tahapan kerangka kerja penelitian adalah berikut :



Gambar : Kerangka Kerja Penelitian

4. ANALISIS DAN PERANCANGAN SISTEM

4.1 GAMBARAN UMUM STEGANOGRAFI TEKNIK LSB

Steganografi adalah paduan antara seni dan ilmu pengetahuan yang mempelajari cara menuliskan pesan tersembunyi. Isi maupun arti pesan tersebut hanya bisa diterjemahkan oleh pembuat dan orang yang berhak menerima pesan. Steganografi ini mempunyai beberapa teknik salah satunya adalah steganografi teknik Least Significant Bit atau yang sering disingkat dengan LSB.

Steganografi teknik LSB adalah suatu teknik dimana kita mengganti bit pada posisi LSB pada data dengan bit yang dimiliki oleh data yang akan disembunyikan. Karena bit yang diganti hanyalah bit yang paling akhir, maka meskipun data telah berubah, kita tetap tidak akan bisa ngenalnya, karena media stego yang dihasilkan hampir sama persis dengan media sebelum disisipi oleh data yang ingin disembunyikan.

Dalam sistem ini nantinya akan memiliki beberapa tahapan. Tahapan ini akan menuntun pengguna sampai pengguna dapat menyisipkan teks/pesan ataupun membaca teks/pesan yang telah disisipkan dalam media lain.

Cara kerja dari aplikasi ini adalah mengambil media yang akan dibuat sebagai media penyisipan yaitu file gambar berformat bmp yang kemudian disisipin teks/pesan yang akan dirahasiakan. Bila penyisipan telah selesai maka pengguna dapat menyimpan file tersebut yang merupakan file gambar yang juga berformat bmp juga.

4.2 ANALISIS PERANCANGAN APLIKASI STEGANOGRAFI

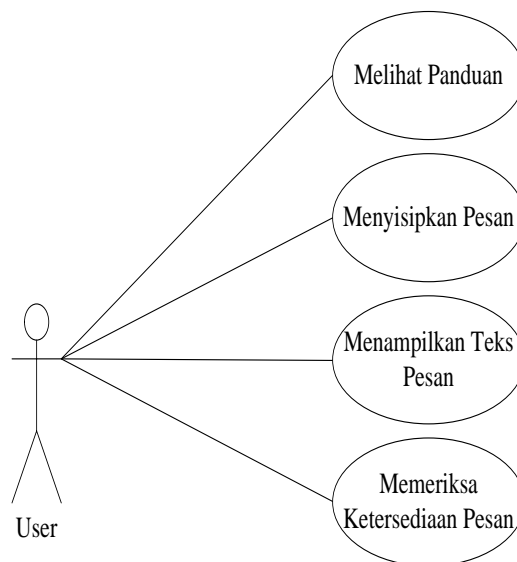
Aplikasi steganografi ini dirancang dan dibuat untuk diimplementasikan pada PC (Personal Computer) dengan sistem operasi Windows XP / Windows 7.

Berikut rincian aplikasi yang akan dibuat:

- 1 Aplikasi dibuat menggunakan Borland Delphi7.
- 2 Aplikasi bersifat portable.
- 3 Input gambar berformat BMP.
- 4 Output gambar yang dihasilkan berformat BMP.
- 5 Aplikasi ini dapat disisipkan karakter berupa abjad (a-z), numerik (0-9), dan juga karakter khusus (!@#\$\$%^&).
- 6 Aplikasi dapat menyisipkan karakter sesuai dengan panjang dan lebar gambar.
- 7 Aplikasi ini berguna untuk menyisipkan dan membaca pesan rahasia

4.2.1 Use Case Diagram

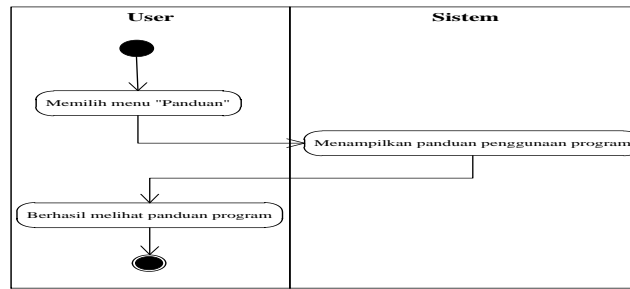
Use Case Diagram untuk *user*



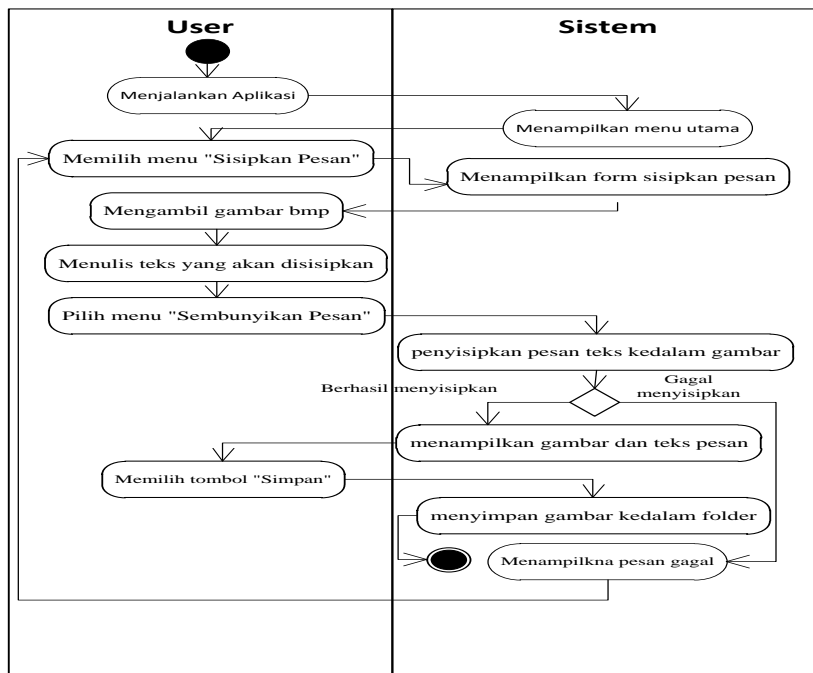
Gambar: *Use Case Diagram User*

Use Case Diagram untuk *user* menggambarkan bagaimana berinteraksi dengan sistem, dimana didalamnya terdapat *use case* menyisipkan pesan, menampilkan pesan, memeriksa ketersediaan pesan, melihat panduan.

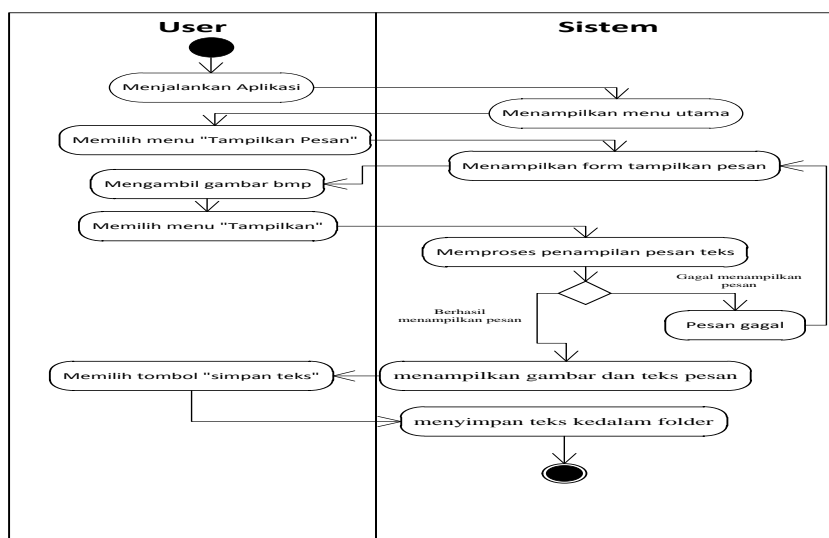
4.2.2 Activity Digram



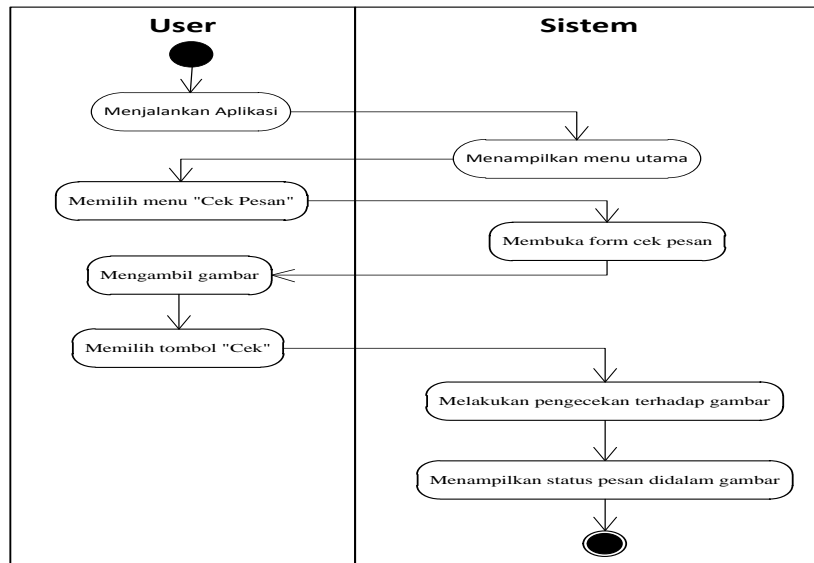
Gambar: Activity Diagram Melihat Panduan



Gambar: Activity Diagram Menyisipkan Pesan

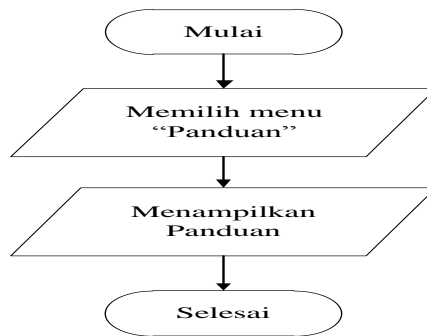


Gambar: Activity Diagram Menampilkan Pesan

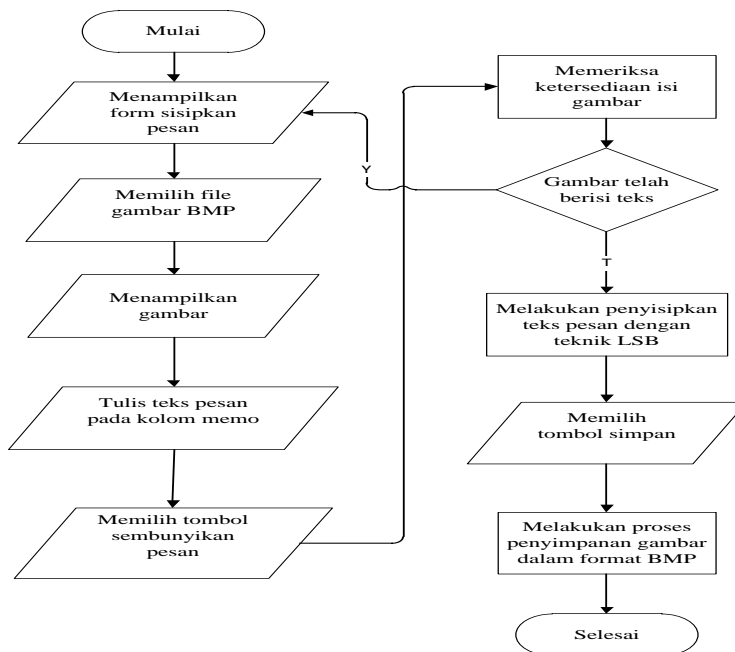


Gambar: Activity Diagram Memeriksa ketersediaan pesan

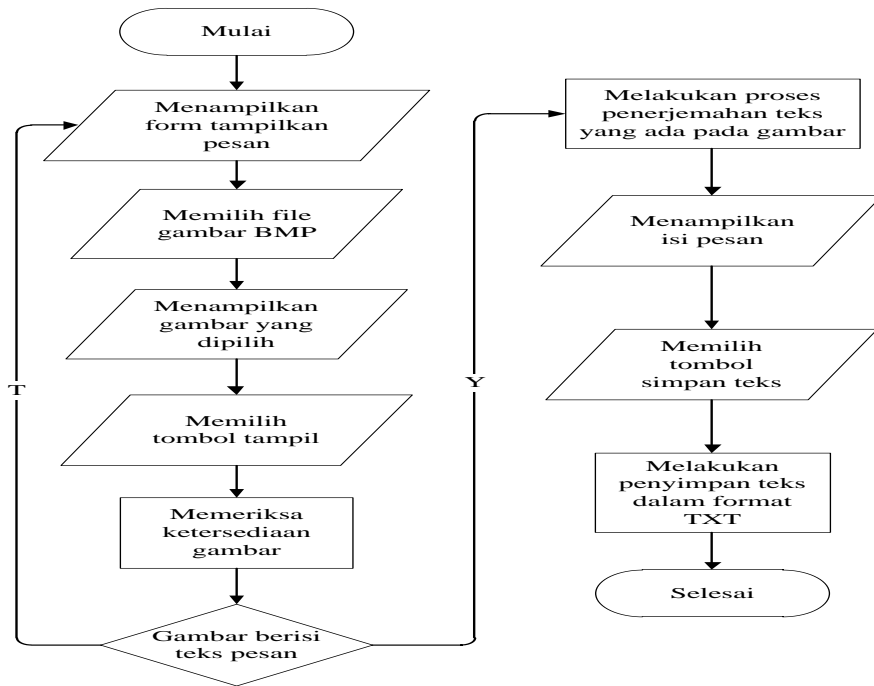
4.2.3 Flowchart



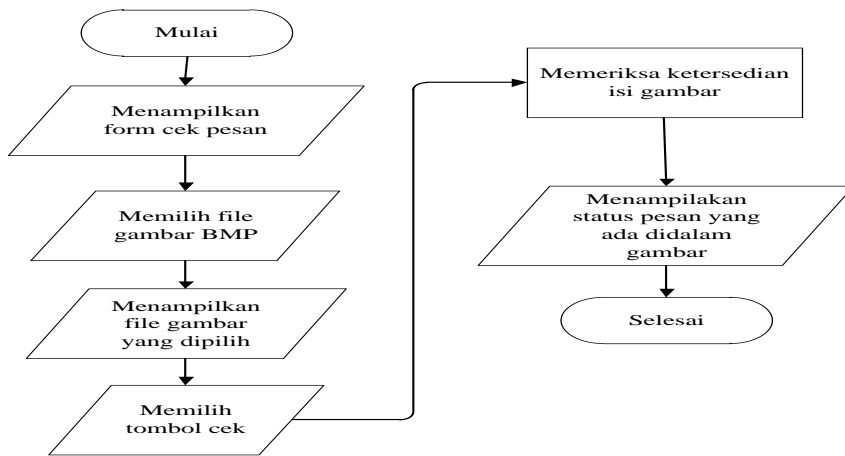
Gambar: Flowchart Diagram Panduan



Gambar: *Flowchart Diagram Sisipkan Pesan*



Gambar: *Flowchart Diagram Tampilkan Pesan*

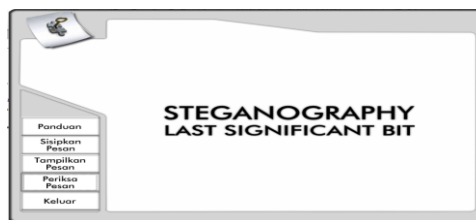


Gambar: *Flowchart Diagram Periksa Ketersediaan Pesan*

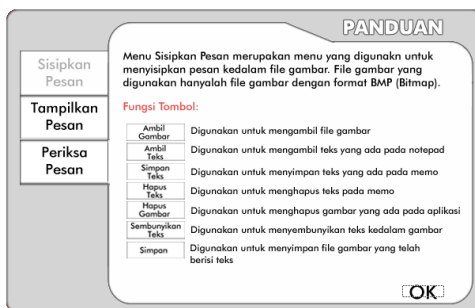
5. IMPLEMENTASI DAN PENGUJIAN SISTEM

Pada tahap ini penulis mengimplementasikan hasil dari rancangan yang telah dibuat pada tahap sebelumnya. Implementasi yang dimaksud adalah proses menterjemahkan rancangan menjadi sebuah program aplikasi.

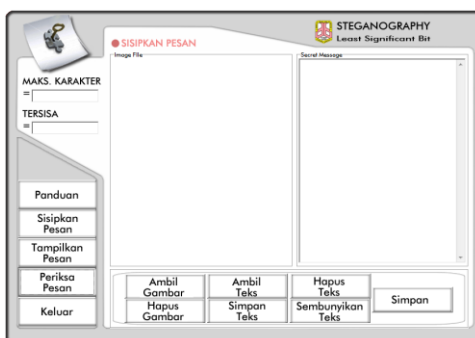
Adapun hasil implementasi adalah sebagai berikut:



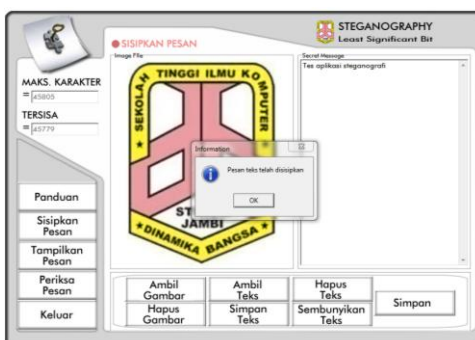
Gambar: Tampilan Menu Utama



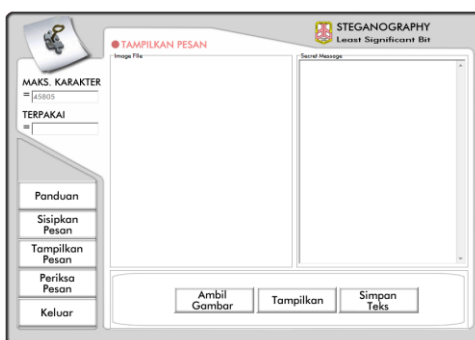
Gambar: Tampilan Menu Panduan



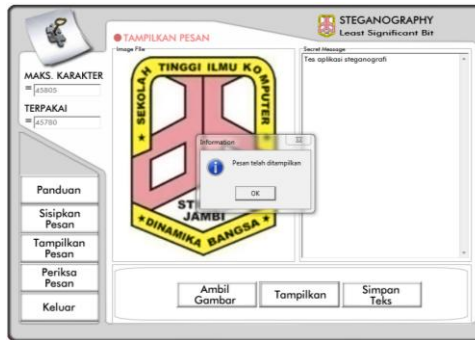
Gambar: Tampilan Menu Utama Sisipkan Pesan



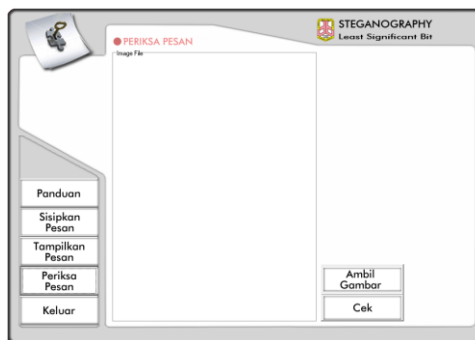
Gambar: Tampilan Menu Sisipkan Pesan



Gambar: Tampilan Menu Utama Tampilkan Pesan



Gambar: Tampilan Menu Tampilkan Pesan



Gambar: Tampilan Menu Periksa Ketersediaan Pesan

6. PENUTUP

6.1 KESIMPULAN

Berdasarkan hasil penelitian yang penulis lakukan, maka dapat diambil kesimpulan sebagai berikut :

- 1 Program ini berhasil dalam menyisipkan dan mengekstraksi pesan rahasia dengan baik karena pesan yang didapatkan isinya sama tanpa perubahan dengan pesan yang disisipkan.
- 2 Kualitas yang di hasilkan mempunyai kualitas yang tidak jauh berbeda dengan citra digital file gambar aslinya.
- 3 Waktu proses penyisipan dan penampilan pesan akan semakin cepat bila jumlah teks yang disembunyikan jauh lebih kecil dibandingkan jumlah maksimum penampungan pesan teks oleh citra digital.
- 4 Perubahan pada gambar akan mengakibatkan kerusakan pada pesan didalamnya.

7. DAFTAR PUSTAKA

- [1] Bambang Haryanto, 2004, *Rekayasa Sistem Berorientasi Objek*. Bandung: Informasi Bandung.
- [2] Bolton, William., 2003, *Progmmmer Logic Controller (PLC)*. Jakarta: Erlangga.
- [3] Desmirazli. (2013). *Computer Security*. [Online]. Tersedia: <http://www.studensite.stemikubidiyah.ac.id/desmirazli/2013/11/27/computer-security>. Html [29 November 2013].
- [4] Eko Arryawan, dan Smidev Community, 2010, *Mengatasi Investigasi Komputer Forensik*. Jakarta: Elex Media Komputindo.
- [5] Enterprise, Jublee., 2010, *13 Ancaman PC dan Cara Mengatasinya*. Jakarta: Elex Media Komputindo.
- [6] Fowler, Martin., 2004, *UML Destilled Edisi 3*. Yogyakarta: Andi.
- [7] Hapsari Muthi Amira., 2009, *Studi Steganografi pada Image File*. Bandung. Volume 7.
- [8] Hendrayudi, 2009, *VB 2008 Untuk Keperluan Programming*. Jakarta: Elex Media Komputindo
- [9] Jack Febrian, 2007, *Kamus Komputer dan Teknologi Informasi*. Bandung: Informasi Bandung.
- [10] Kusriani, dan Andri Koniyo, 2007, *Tuntunan Praktis membangun Sistem Informasi Akutansi dengan Visual Basic dan Microsoft SQLServer*. Yogyakarta: Andi Offset.

- [11]Nain, Ahmad Shukri, dan Rasli, Amran MD., 2005, *Pengurusan Teknologi*. Malaysia: Universiti Teknologi Malaysia.
- [12]Rifki Sadikin, 2012, *Kriptografi Untuk Keamanan dan Implementasi Dalam Bahasa Java*. Yogyakarta: Andi Offset.
- [13]Sholiq, dan Imam Robandi, 2010, *Analisis & Perancangan Obyek*. Bandung: Muara Indah.
- [14]Soetam Rizki, 2011, *Konsep Dasar Rekayasa Perangkat Lunak*. Jakarta: Prestasi Pustakaraya.
- [15]Sutarman, 2009, *Pengantar Teknologi Informasi*. Jakarta: Bumi Aksara.
- [16]Rosa, dan Salahuddin, 2011, *Modul Pembelajaran Rekayasa Perangkat Lunak*. Bandung: Modula.
- [17]Wing Wahyu Winarno, 2006, *Sistem Informasi Manajemen*. Yogyakarta: UPP STIM YKPN