PEMBUATAN APLIKASI *STEGANOGRAFI* PADA CITRA DIGITAL

Dian Gustina dan Achmad Sumbaryadi
Universitas Persada Indonesia YAI, AMIK BSI Jakarta
dgustina@yahoo.com, asumbaryadi@yahoo.com

Abstrak

Steganografi mempunyai fungsi untuk menyembunyikan informasi berupa data teks digital. Media yang digunakan adalah citra digital. Pesan Rahasia yang di sisipkan dalam gambar disini dilakukan dengan menggunakan teknik *Steganografi* yang hanya dibatasi untuk gambar *Jpeg*. *Steganografi* sebagai suatu seni dan *sains* untuk penyembunyian informasi atau pesan ke dalam pesan lainnya pada media cover yang lain misalnya gambar, *Audio MP3*, sedemikian rupa sehingga tidak menimbulkan kecurigaan. Teknik *steganografi* dapat digunakan untuk menyembunyikan data dalam digital dengan sedikit atau tanpa terasa adanya perubahan yang tampak pada gambar tersebut dan dapat dieksploitasi untuk mengeksport pesan rahasia. Berkaitan dengan bahasan tersebut penulis tertarik untuk membuat aplikasi *steganografi*, yang bertujuan untuk dapat menyembunyikan pesan sehingga terjaga kerahasiaannya. Untuk menampung pesan rahasia kedalam objek digital yakni berupa citra digital tentunya membutuhkan suatu algoritma yang dapat memodifikasi objek digital sehingga menghasilkan objek digital baru yang berisi pesan tersembunyi, yang disebut dengan istilah *embedding algorithm*.

Abstract

Steganografi has the function to hide information in the form of digital text data. Medium used is a digital image. The secret message in paste in the picture here is done by using a technique that Steganografi only limited to JPEG images. Steganografi as an art and science for the concealment of information or messages in other messages to cover other media such as images, audio MP3, so as not to arouse suspicion. Steganografi techniques can be used to hide data in digital with little or no change was visible in the image and can be exploited to export the secret message. Discussion related to the authors are interested in creating applications steganografi, which aims to hide the message so discreet. To accommodate a secret message into a digital object that is in the form of a digital image certainly requires an algorithm that can modify the digital object to produce a new digital object that contains a hidden message, which is called the embedding algorithm

Keywords : Steganografi, Digital image, embedding algorithm

PENDAHULUAN

Perkembangan teknologi informasi saat ini memberikan kemudahan manusia untuk melakukan aktivitasnya. Termasuk kirim mengirim informasi dalam bentuk *file* menjadi hal biasa di era komputerisasi saat ini. Banyak diantara *file* tersebut bersifat rahasia dan sangat penting, dan tidak boleh diketahui oleh pihak lain. Seiring dengan perkembangan teknologi informasi tersebut, semakin berkembang pula teknik kejahatan yang berupa perusakan maupun pencurian data oleh pihak yang tidak memiliki wewenang atas data tersebut. Ada beberapa bentuk penyerangan terhadap data dan informasi, seperti *hacker*, *cracker*, *trojan force attack*, dan lain-lain. Oleh karena itu, pada saat ini telah dilakukan berbagai upaya untuk menjaga keamanan data dan mengatasi serangan-serangan tersebut.

Sebelumnya ada cara untuk menjaga keamanan data yang dikenal dengan nama *kriptografi*. Dengan *kriptografi* data rahasia terjaga keamanannya, namun bentuk *chipertex* yang diacak akan mudah terdeteksi dan menyadarkan pihak ketiga akan kerahasiaan *file* tersebut. Untuk itu diterapkan *steganografi* yang dalam bahasa yunani berarti “pesan tersem-

bunyi“ (*covered writing*) dalam usaha menjaga kerahasiaan data. *Steganografi* merupakan salah satu cara untuk menyembunyikan suatu pesan rahasia di dalam data atau pesan lain yang tampak tidak mengandung apa-apa, kecuali bagi orang yang mengerti kuncinya. Dalam bidang keamanan komputer, *steganografi* digunakan untuk menyembunyikan data rahasia pada saat proses enkripsi tidak dapat dilakukan atau bersamaan dengan proses enkripsi. Jadi, walaupun enkripsi dipecahkan (*dechiper*) pesan/data rahasia tetap tidak terlihat. Pada steganografi pesan disamarkan dalam bentuk yang relatif aman sehingga tidak terjadi kecurigaan tersebut. *Steganografi* dapat digunakan pada berbagai macam bentuk data, yaitu *image*, *audio*, dan *video*.

PEMBUATAN APLIKASI *STEGANOGRAFI* PADA CITRA DIGITAL

Batasan Masalah

Dalam pembuatan tugas akhir ini, untuk mengatasi permasalahan yang ada maka penyusun membatasi permasalahan sebagai berikut:

a. Format *file* citra digital yag dapat digunakan untuk menyimpan pesan rahasia adalah berformat *Joint Photographic Expert Group (JPEG)*.
b. Metode *steganografi* yang di gunakan adalah *Least Significant Bit* (*LSB*).

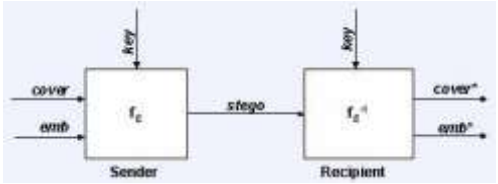
Tujuan Pembuatan Aplikasi

Ada beberapa tujuan dalam pembuatan aplikasi *steganografi,* antara lain adalah :

a. Membuat aplikasi penyembunyian informasi ke dalam citra digital dengan *Least Significant Bit* (*LSB*).
b. Memanipulasi citra digital yang didalamnya terdapat informasi rahasia sehingga pesan rahasia tersebut tidak dapat diketahui keberadaannya dan secara kasat mata tidak terjadi perubahan pada citra digital hasil manipulasi.

Steganografi adalah suatu teknik untuk menyembunyikan informasi yang bersifat pribadi dengan sesuatu yang hasilnya akan tampak seperti informasi normal lainnya. Media yang digunakan umumnya merupakan suatu media yang berbeda dengan media pembawa informasi rahasia, dimana fungsi dari *steganografi* yaitu sebagai teknik penyamaran menggunakan media lain yang berbeda sehinnga infomasi rahasia dalam media awal tidak terlihat secara jelas (Waheed, 2000)

Steganografi merupakan salah satu cara untuk menyembunyikan suatu pesan / data rahasia di dalam data atau pesan lain yang tampak tidak mengandung apa-apa, kecuali bagi orang yang mengerti kuncinya. Dalam bidang keamanan komputer, *steganografi* digunakan untuk menyembunyikan data rahasia saat enkripsi tidak dapat dilakukan atau bersamaan dengan enkripsi. Jadi, walaupun enkripsi dipecahkan (*decipher*) pesan/data rahasia tetap tidak terlihat. Selain itu pada *cryptografi* pesan di sembunyikan dengan “diacak” sehingga pada kasus-kasus tertentu dapat dengan mudah mengundang kecurigaan, sedangkan pada *steganografi* pesan “disamarkan” dalam bentuk yang relatif “aman” sehiggga tidak terjadi kecurigaan itu. *Steganografi* dapat digunakan pada berbagai macam bentuk data, yaitu *image*, *audio*, dan *video*.



Gambar 2.1. *steganografi* sistem

Gambar ini menunjukkan sebuah sistem *steganografi* umum, dimana di bagian pengirim pesan (*sender*), dilakukan proses *embedding* (f_E) pesan yang hendak dikirim secara rahasia (*emd*) ke dalam data *cover* sebagai tempat menyimpannya (*cover*), dengan menggunakan kunci tertentu (*key*), sehingga dihasilkan data dengan pesan tersembunyi di dalamnya (*stego*). Di bagian penerima pesan (*recipient*), dilakukan proses *extracting* (f_E^{-1}) pada *stego* untuk memisahkan pesan rahasia (*emb*) dan data penyimpanan (*cover*) dengan menggunakan kunci yang sama seperti pada proses *embedding*. Jadi hanya orang yang tahu kunci ini saja yang dapat mengekstrak pesan rahasia .

Kata *steganografi* berasal dari bahasa Yunani yaitu *steganos* yang berarti penyamaran atau penyembunyian dan *grafien* atau *graftos* yang berarti tulisan sehingga secara keseluruhan artinya adalah tulisan yang disembunyikan. Secara umum *steganografi* merupakan suatu seni atau ilmu yang digunakan untuk menyembunyikan pesan rahasia (informasi) tertulis kedalam pesan lain dengan segala cara sehingga selain orang yang dituju, orang lain tidak akan menyadari keberadaan dari pesan rahasia tersebut (Soehono, 2006)

Steganografi bukan merupakan hal yang baru, *steganografi* sudah dikenal sejak zaman Romawi dan Yunani kuno. Misalnya, pesan ditulis di kepala budak lalu menunggu sampai tumbuh cukup rambut untuk menutupi pesan rahasia tersebut sebelum ia dikirim kepada orang yang dituju dimana rambutnya akan dicukur sehingga pesan itu terlihat.

Manfaat *Steganografi*

Steganografi adalah sebuah pisau bermata dua, ia bisa digunakan untuk alasan-alasan yang baik, tetapi bisa juga digunakan sebagai sarana kejahatan. *Steganografi* juga dapat digunakan sebagai sala satu metode *watermaking* pada *image* untuk proteksi hak cipta, seperti juga digital watermaking (*fingerprinting*). Dan yang paling terutama, seperti yang disebutkan sebelumnya, *steganografi* dapat digunakan untuk menyembunyikan informasi rahasia, untuk melindunginya dari pencurian dan dari orang yang tidak berhak untuk mengetahuinya. Sayangnya, *steganografi* juga dapat digunakan untuk mencuri data yang disembunyikan pada data lain sehingga dapat dikirim ke pihak lain, yang tidak berhak, tanpa ada yang curiga. *Steganografi* juga dapat digunakan oleh para teroris untuk saling berkomunikasi satu dengan yang lain.

Sehubungan dengan keamanan sistem inforamasi, *steganografi* hanya merupakan salah satu dari banyak cara yang dapat dilakukan untuk menyembunyikan pesan rahasia. *Steganografi* lebih cocok digunakan bersamaan dengan metode lain tersebut untuk menciptakan keamanan yang berlapis. Sebagai contoh *steganografi* dapat digunakan bersama dengan enkripsi. *Windows* dan *unix* juga menggunakan steganografi dalam mengimplementasikan *hidden directory*.

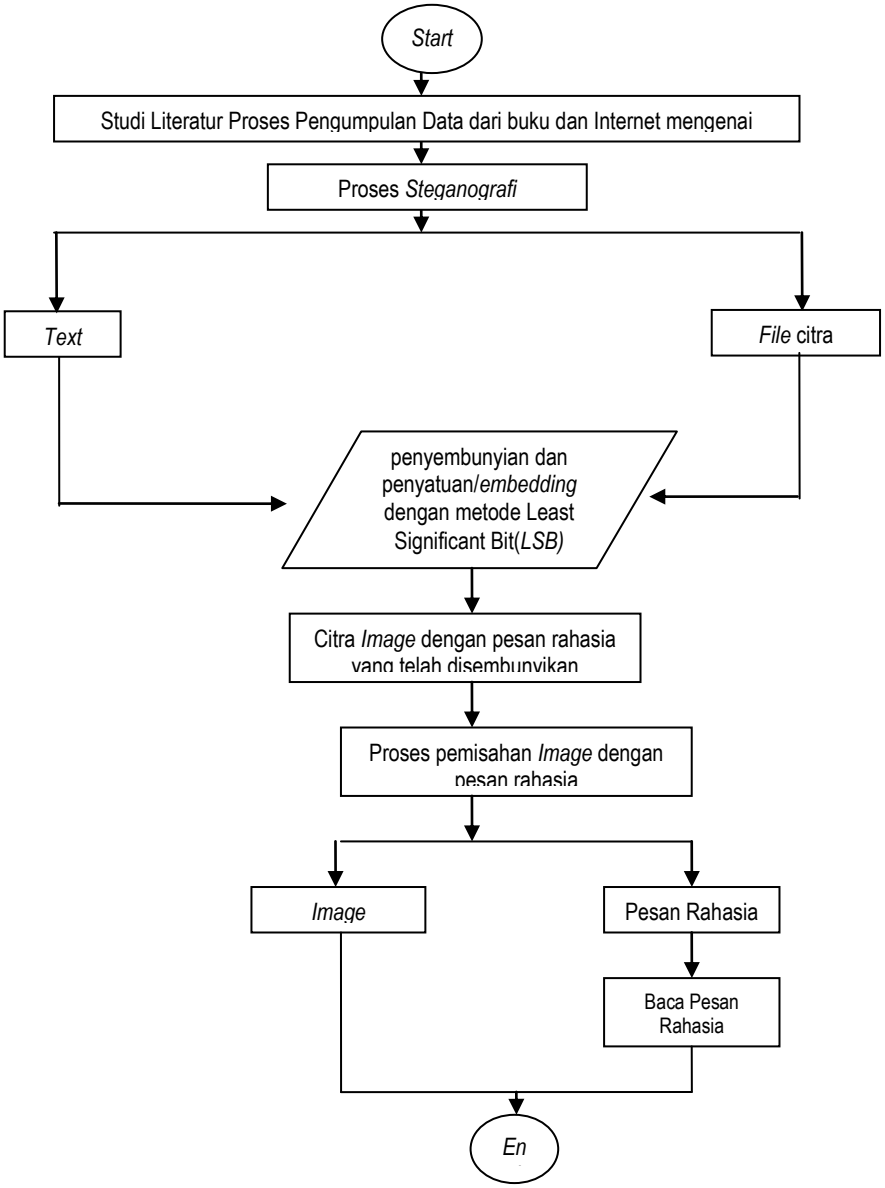
Metode Penelitian

Secara umum program *steganogrfi* ini mempunyai fungsi untuk menyembunyikan informasi berupa data teks digital dibalik data digital lainnya dalam hal ini media yang digunakan adalah citra digital berupa *Joint Photographic expert Group* (*JPEG*).

Penelitian dalam pembuatan aplikasi *Steganografi*. Metode penelitian yang digunakan oleh penulis dalam penelitian ini adalah dengan melakukan studi literatur serta pengum-

pulan data-data dari buku maupun dari internet mengenai *Steganografi*.

Untuk menampung pesan rahasia ke dalam objek digital yakni berupa citra digital tentunya membutuhkan suatu algoritma yag dapat memodifikasi objek digital sehingga menghasilkan objek digital yang baru yang berisi pesan tersembunyi, yang disebut dengan istilah *Embedding Algorihtm*, dan harus menjadi perhatian bahwa dalam proses modifikasi modifikasi media penampung tidak boleh terlalu mencolok atau dengan kata lain secara kasat mata, perubahan pada citra penampung yang telah termodifikasi tidak terlalu terlihat. Proses penyembunyian pesan dalam citra digital bermula dari adanya pesan atau informasi yang ingin disampaikan dengan cara mengetik pesan (*input* pesan dari *keyboard*). Ketikan (*input*) pesan rahasia kemudian disatukan dengan *Image file JPEG*, sehingga terjadi proses *Embedding* pesan dengan gambar. Setelah proses penyatuan (*Embedding*) terlaksana, proses berlanjut pada pemisahan pesan rahasia dengan gambar, sehingga pesan rahasia dapat dibaca. Berikut ini *Flowchart* Metode Penelitian *Steganografi.*



Gambar 3.1 *Flowchart* Metode Penelitian *Steganografi.*

Perangkat Yang Digunakan

Dalam pembuatan aplikasi ini ada beberapa perangkat yang dibutuhkan, dari perangkat lunak (*software*) dan perangkat keras (*hardware*). Penggunaan *software* berkaitan dengan penggunaan *hardware* yang memiliki spesifikasi tertentu.

Persiapan Perangkat Lunak (*Software*)

Dalam pembuatan aplikasi ini *software* pendukung adalah *Borland Delphi 7,* sebelum pembuatan aplikasi *Steganografi* harus dipastikan bahwa *software* ini telah terinstal dikomputer. Spesifikasi perangkat lunak yang digunakan secara umum adalah Sistem Operasi *Windows 98/2000/NT/XP* dan Pemrograman *Borland Delphi 7*.

Persiapan Perangkat Keras (*Hardware*)

Hardware merupakan pendukung untuk menjalani sebuah program, pada aplikasi ini memiliki spesifikasi *hardware* untuk menjalankan *Borland Delphi 7* seperti berikut :

1. Minimum Prosesor yang digunakan adalah *Intel Pentium* II atau kelas diatasnya.
2. *Hardisk* minimal 5 GB.
3. *Memory* (RAM) dengan kapasitas 128 MB lebih tinggi kapasitas akan lebih baik dalam proses eksekusi program.

***Least Significant Bit* (*LSB*)**

Penyisipan *Least Significant Bit* (LSB) adalah umum, pendekatan yang sederhana untuk menempelkan informasi di dalam *file* suatu *cover. Metode* yang digunakan untuk penyembunyian pesan rahasia pada aplikasi ini adalah dengan cara menyisipkan pesan ke dalam bit rendah *LSB* (*least significant bit*) pada data *pixel* yang menyusun *file* gambar *JPEG* 24bit tersebut. Penggunaan *Least Significant Bit* (*LSB)* karena *bit pixel LSB* mempunyai kontribusi sangat kecil terhadap penampakan *pixel* tersebut, maka penggantian bit-bit ini sering tidak memiliki efek yang tampak jelas pada gambar, selain itu bit yang cocok untuk diganti adalah bit *LSB*, sebab perubahan tersebut hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. (Budi Sukmawan, 2002)

Langkah-langkah penyembunyian pesan dengan metode *Least Significant Bit* (*LSB)* sebagai berikut :

1. Cara paling umum untuk menyisipkan pesan adalah dengan memanfaatkan *Least Significant Bit* (*LSB*). Pada *file* gambar *JPEG* 24 bit setiap *pixel* pada gambar terdiri dari susunan tiga warna yaitu merah, hijau, biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (1 byte) dari 0 sampai 255 atau dengan *format biner* 00000000 sampai 11111111. sebagai contoh *file* gambar *BMP* 24 bit dengan warna merah murni, hijau murni, dan biru murni dalam *format biner* akan terlihat pada tabel sebagai berikut :

Tabel. *Format biner* warna *RGB*

warna	Biner		
	BIRU (BLUE)	**HIJAU (GREEN)**	**MERAH (RED)**
MERAH (RED)	00000000	00000000	**11111111**
HIJAU (GREEN)	00000000	**11111111**	00000000
BIRU (BLUE)	**11111111**	00000000	00000000

2. Dari uraian di atas dapat dilihat bahwa informasi dari warna biru berada pada bit pertama sampai bit delapan, dan informasi warna hijau berada pada bit sembilan sampai dengan bit 16, sedangkan informasi

warna merah berada pada bit 17 sampai dengan bit 24.

3. Metode penyisipan *Least Significant Bit* (*LSB)* ini adalah menyisipkan pesan dengan cara mengganti bit ke 8, 16 dan 24 pada representasi *biner file* gambar dengan representasi *biner* pesan rahasia yang akan disembunyikan. Dengan demikian pada setiap *pixel file* gambar *BMP* 24 bit dapat disisipkan 3 bit pesan

Pembuatan Program

Dalam pembuatan aplikasi *Steganografi* Penulis menggunakan *Delphi 7*, dimana nantinya penulis akan melampirkan *sourcecode* program *Steganografi* pada lampiran diakhir laporan penulisan.

Aplikasi *Steganografi* yang dibuat akan menyisipkan pesan pada *format file JPEG* 24 bit. *Format file JPEG* merupakan *format file* standar *system* operasi *MS Windows 3.11/9x/NT* dan *IBM OS/2. format file* ini mendukung resolusi warna dari *monocrom* hingga *true color* (16,7 juta warna). *Format file BMP* 24 bit mengunakan model warna *RGB*. Pada model warna *RGB*, warna yang ditampilkan di layar monitor disusun oleh tiga warna primer, yaitu *Red* (Merah), *Green* (Hijau), *Blue* (Biru). Pada model warna *RGB* setiap titik pada *layer* monitor berisi angka yang salah satu warna dari *RGB*.

Warna dari *table RGB* memiliki 3 buah warna kombinasi warna yaitu *R, G, B,* yang menentukan proporsi warna merah, hijau, biru dari warna tersebut. Warna di *table* yang dapat dipilih untuk mengisi warna pada sebuah *pixel* adalah 256 x 256 x 256 = 16,7 juta warna.

Embedding* dengan Metode *Least Significant Bit (LSB)

Sistem *Steganografi* pertama yang tersedia untuk gambar adalah *Jsteg*nya Derek *UphAm*. Dimana Algoritma *embedding*nya secara berurutan (Sekuensial) mengganti *LSB* dari koefisien-koefisien *DCT (Discrete Cosine Transform)* dengan data pesan rahasia*.* Pada algoritma *Steganografi* (penyembunyian pesan dalam gambar *BMP*) *raster original* dari *Image* diganti dengan representasi biner dari pesan dengan metode *least significant bit*, kemudian sisipkan biner pesan kedalam *Image,* sehingga menghasilkan *Stego image.*

Sebagai contoh, berikut merupakan algoritma sederhana untuk menyembunyikan pesan di dalam image *JPEG* :

Input : pesan, cover image
Output: stego
While (data untuk di *emmbed*) ***do***
    LSB dari *cover image*
If ambil bit selanjutnya dari pesan
End if
Masukan biner pesan
End while

Pada proses *Steganografi Embedding* pesan rahasia dalam gambar menggunakan Algoritma dengan metoda *LSB (Least significant bit)* pada *Steganografi* ini adalah menyisipkan pesan dengan cara mengganti bit ke 8, 16, dan 24 pada representasi biner *file* gambar dengan representasi biner pesan rahasia yang akan disembunyikan. Dengan demikian pada setiap *pixel* file gambar *JPEG* 24 bit dapat disisipkan 3 bit pesan. *Pixel* disusun di layar monitor dalam susunan baris dan kolom. Susunan *Pixel* dalam baris dan kolom ini dinamakan resolusi monitor.

Pembuatan Tampilan Program *Steganografi*

Tampilan program *Steganografi* dibagi menjadi 4 bagian antara lain tampilan Menu Utama, *Form* Tulis Pesan, *Form* Baca Pesan, *Form* About. Keempat bagian tersebut saling berkaitan satu sama lainnya.

Antar muka Menu Utama ini merupakan antar muka yang pertama kali muncul pada aplikasi. Pada antar muka Menu Utama ini terdapat tiga buah tombol yang menghubungkan ke proses selanjutnya yaitu tombol Tulis Pesan yang jika diklik akan masuk ke antar muka Tulis Pesan yang terdiri dari :

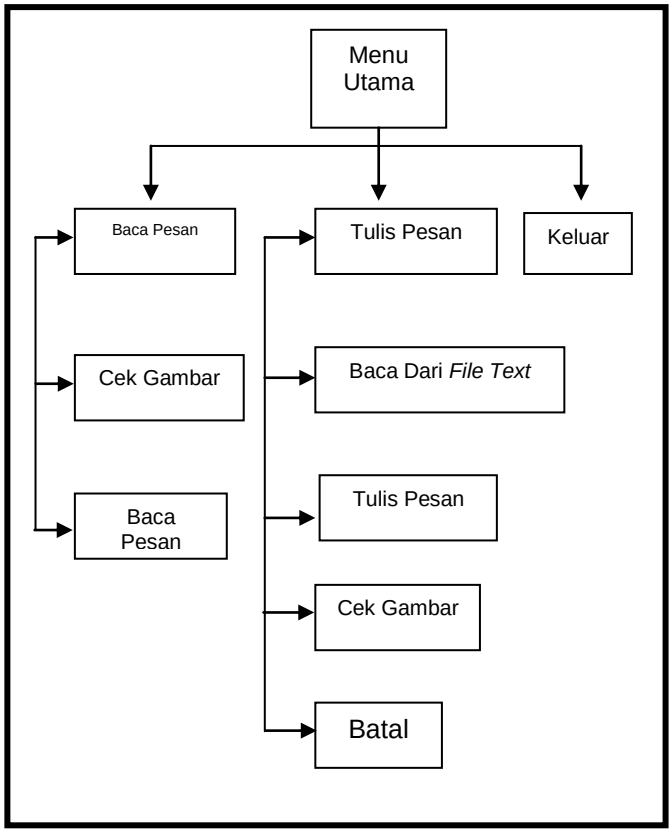
1. Tombol baca *file text*, Text, berfungsi meng*upload file text.*
2. Tombol Tulis Pesan, berfungsi untuk proses menyatukan pesan rahasia dengan gambar.
3. Tombol Cek Gambar, berfungsi untuk memeriksa gambar asli atau gambar yang telah tersimpan rahasia. Pada proses ini tidak secara otomatis melakukan ke proses selanjutnya jika gambar yang di*upload* merupakan gambar asli, sehingga proses pemilihan gambar berulang dari awal.
4. Tombol Batal, berfungsi untuk membatalkan proses penulisan pesan.

Tombol Baca Pesan yang jika diklik akan masuk ke antar muka Baca Pesan yang terdiri dari :

1. Tombol Cek Gambar, berfungsi untuk memeriksa gambar asli atau gambar yang telah tersimpan rahasia (*Carrier File*). Pada proses ini tidak secara otomatis melakukan ke proses selanjutnya jika gambar yang di*upload* merupakan gambar asli, sehingga proses pemilihan gambar berulang dari awal
2. Tombol Baca Pesan, berfungsi untuk membaca pesan, ketika *Carrier File* telah tampil di*Image* gambar maka langsung klik *Button* Baca Pesan.

Dan tombol Keluar yang jika diklik akan keluar dari aplikasi.

Berikut ini tampilan rancangan menu aplikasi program *Steganografi* :



Gambar 4.1 Rancangan Menu Aplikasi Program *Steganografi*

Kesimpulan

Pada penulisan jurnal yang berjudul: Pembuatan Aplikasi *Steganografi* pada citra digital dapat disimpulkan sebagai berikut :

1. Penggunaan *steganografi* bertujuan untuk menyamarkan eksistensi pesan rahasia sehingga tidak dapat dideteksi. *Steganografi* ini menggunakan metode *Least Significan Bit (LSB)*
2. *Steganografi* membutuhkan dua property, yaitu media penampung berupa citra digital dan bisa juga dengan media *video, audio* dan

pesan rahasia yang akan di-sembunyikan.

DAFTAR PUSTAKA

Maseleno, Andino, 2005, "*Modul Pelatihan Delphi*", IT Community, Yogyakarta.*(www.google.com)*

M.Agus J. Alam, 2000, Belajar Sendiri BORLAND DELPHI 5.0, PT Elex Media Komputindo, Jakarta.

Munir, Rinaldi, 2004, *Bahan Kuliah ke 7 IF5054 Kriptografi*, ITB, Bandung.

Pramono, Djoko, 2000, *Mudah menguasai Delphi 3.0 Jilid dua*, PT Elex Media Komputindo, Jakarta.

Rahardjo, Budi, 2005, *Handbook Keamanan Sistem Informasi Berbasis Internet,* PT Insan Infonesia – Bandung & PT INDOCISC – Jakarta.

Riyanto, Slamet, *"Memilih Format File Yang Tepat Untuk Image". (www.google.com)*

Santosa, Djaka, "*Seminar Tentang Digital Image"*. *(www.google.com)*

Seri Panduan Pemrograman Pemrograman Borland Delphi 7 (jilid 1). 2002 Madiun : MADCOMS dan Yogyakarta : Andi, Edisi I

Sukmawan,Budi,Steganografi(http://Student.ukdw.ac.id/~22033120/Steganografi.html).http://www.tiac.net/uses/korejwa/jsteg.html

Susany soplanit, Sendy Christian Sunarsa, Dali Santun Naga. *Pengamanan data dengan Chaotic Least Significant Bit encoding (Clsbe) dan New Chaotict Substitution Image Encryption (NCSIE).* Prosiding Seminar Nasional SIIT 2005, Universitas Kristen Petra, Surabaya, 28 Juli 2005

www.google.com
www.ilmukomputer.com
wikiipedia.com