STEGANORAFI PADA CITRA JPEG MENGGUNAKAN METODE SPREAD SPECTRUM

Rico Ardiles.S[1], Prihambodo H.S[2], Marlindawati [3]
Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Bina Darma

Jalan Jenderal Ahmad Yani No.12 Palembang

E-mail : ricoardiless@yahoo.co.id[1], p.h.saksono@mail.binadarma.ac.id[2], marlindawati@mail.binadarma.ac.id[3]

Abstract : *Development of information technology (IT) is currently providing convenience to human activities. Includes send send information in the form of a common file in the current era of computerization. steganography which in Greek means "hidden message" (covered writing) in an effort to maintain the confidentiality of data, Steganography is a technique of inserting a message into the media, where the secret message that is sent is not changed in shape, but is inserted in the other media (cover-object) . There are two processes in steganography, the message insertion and extraction process of messages. Basically the insertion of a secret message can be carried into the JPEG image format. Spread spectrum method is the insertion process using the message consisting of three processes, namely spreading, modulation, and the insertion of messages into JPEG images. Application of spread spectrum method with menyisipan messages in JPEG with values used are 0 and 1.*

Keyword*: steganography, JPEG, method of spread spectrum*

Abstrak *: Perkembangan teknologi informasi (TI) saat ini memberikan kemudahan manusia untuk melakukan aktivitasnya. Termasuk kirim mengirim informasi dalam bentuk file menjadi hal yang biasa di era komputerisasi saat ini. steganografi yang dalam bahasa Yunani berarti "pesan tersembunyi" (covered writing) dalam usaha menjaga kerahasiaan data, Steganografi adalah teknik menyisipkan pesan kedalam suatu media, dimana pesan rahasia yang akan dikirimkan tidak diubah bentuknya, melainkan disisipkan pada sebuah media lain (cover-object). Ada dua buah proses dalam steganografi, yaitu proses penyisipan pesan dan ekstraksi pesan. Secara mendasar penyisipan pesan rahasia dapat dilakukan ke dalam format gambar JPEG. Metode spread spectrum adalah proses penyisipan pesan menggunakan yang terdiri tiga proses, yaitu spreading, modulasi, dan penyisipan pesan ke citra JPEG. Penerapan metode spread spectrum dengan menyisipan pesan dalam JPEG dengan nilai yang digunakan adalah 0 dan 1.*

Kata kunci*: Steganografi, JPEG,Metode Spread Spectrum*

1. PENDAHULUAN

Perkembangan teknologi informasi (TI) saat ini memberikan kemudahan manusia untuk melakukan aktivitasnya. Termasuk kirim mengirim informasi dalam bentuk file menjadi hal yang biasa di era komputerisasi saat ini. Banyak diantara file tersebut bersifat rahasia dan sangat penting, dan tidak boleh diketahui oleh pihak lain. Dan 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.

Untuk itu diterapkan *steganografi* yang dalam bahasa Yunani berarti "pesan tersembunyi" *(covered writing)* dalam usaha menjaga kerahasiaan data, *Steganografi* adalah teknik menyisipkan pesan kedalam suatu media, dimana pesan rahasia yang akan dikirimkan tidak diubah bentuknya, melainkan disisipkan pada sebuah media lain (*cover-object*).

Ada dua buah proses dalam *steganografi,* yaitu proses penyisipan pesan dan ekstraksi pesan. Secara mendasar penyisipan pesan rahasia dapat dilakukan ke dalam format gambar *JPEG.* Salah satunya dengan menggunakan metode *spread spectrum,* dengan adanya metode Spread Spectrum ini pesan dikodekan dan disebar kesetiap spektrum frekuensi yang memungkinkan, penyebaran ini berguna untuk menambah tingkat redundansi yang ditentukan oleh faktor pengali cr yang bernilai 4 (empat) dan panjang bit-bit hasil penyebaran ini menjadi cr kali panjang bit-bit awal.

Pada dasarnya terdapat 7 (tujuh) metode yang digunakan dalam *steganografi* seperti *injection*, *subsitusi*, *transform domain*, *spread spectrum*, *statistical method*, *distortion* dan *cover generation*. Pada penelitian steganografi citra JPEG metode yang digunakan adalah metode *spread spectrum*. Metode *spread spectrum* adalah proses penyisipan pesan menggunakan yang terdiri tiga proses, yaitu *spreading*, modulasi, dan penyisipan pesan ke citra JPEG. Penerapan metode *spread spectrum* dengan menyisipan pesan dalam JPEG dengan nilai yang digunakan adalah 0 dan 1. Oleh karena itu, penulis mencoba mengambil topik dalam penulisan skripsi dengan judul : **"** *Steganografi pada Citra JPEG Menggunakan* Metode *Spread Spectrum''*.

Berdasarkan latar belakang di atas, maka masalah yang dirumuskan adalah "Bagaimana membangun suatu aplikasi *steganografi* untuk menyembunyikan pesan rahasia dan dapat melindungi keamanan data yang disisipkan pada citra *JPEG* dengan menggunakan metode *spread spectrum* tanpa terjadi perubahan yang berarti pada citra JPEG".

Tujuan penelitian ini adalah untuk mengembangkan teknik *Steganografi* pada citra *image* yang sudah ada dikembangkan lagi menjadi teknik *steganografi* yang dapat menyembunyikan dan melindungi keamanan data yang disisipkan pada citra *JPEG* dengan menggunakan metode *spread spectrum.*

2. METODOLOGI PENELITIAN

2.1 Metode Pengumpulan Data

Dalam pengumpulan data yang digunakan pada penelitian ini adalah sebagai berikut :

Studi kepustakaan dilakukan untuk mencari informasi tentang *steganografi* pada Citra *JPEG* dan prosesnya. Sumber

kepustakaan diambil dari buku-buku yang berkaitan dengan *steganografi* pada Citra *JPEG* dan informasi dari jurnal-jurnal yang terkait yang diperoleh dari *internet*.

2.1.1 Metode Pengembangan Sistem

Menurut Pressman (2002:36), metode pengembangan sistem dalam perangkat lunak ini adalah metode *Linier Sekuensial model* atau disebut juga *"Classic Life cycle"* atau "Waterfall Model" adalah metode pembangunan perangkat lunak dengan pendekatan sekuensial yang sistematik dan sekuensial yang mulai pada tingkat dan kemajuan sistem pada setiap tahapan. Pada model ini terdapat aktifitas-aktifitas sebagai berikut :

1. Rekayasa Sistem dan Analisis (*Sistem Engineeering and Analysis*)

   Karena perangkat lunak adalah bagian dari sistem yang lebih besar, pekerjaan dimulai dari pembentukan kebutuhan-kebutuhan untuk seluruh elemen sistem dan kemudian memilih mana yang untuk pengembangan perangkat lunak.

2. Analisis Kebutuhan Perangkat Lunak (*Software Requirements Analysis*)

   Pengumpulan kebutuhan dengan fokus pada perangkat lunak, yang meliputi domain informasi, performasi dan antarmuka. Hasilnya harus didokumentasi dan *direview*.

3. Perancangan (*Design*)

   Ada 4 (empat) atribut untuk program yaitu : struktur data, arsitektur perangkat lunak, prosedur detil dan karakteristik antarmuka. Proses desain mengubah kebutuhan-kebutuhan menjadi bentuk karakteristik yang dimengerti perangkat lunak sebelum dimulai penulisan program. Desain ini harus terdokumentasi dengan baik dan menjadi konfigurasi perangkat lunak.

4. Pembuatan Kode (*coding*)

   Menerjemah perancangan ke bentuk yang dapat dimengerti oleh mesin, dengan menggunakan bahasa pemograman.

5. Pengujian (*Testing*)

   Setelah kode program selesai, testing dapat dilakukan. Testing memfokuskan pada logika internal dari perangkat, fungsi eksternal dan mencari segala kemungkinan kesalahan dan memeriksa apakah sesuai dengan hasil yang diinginkan.

2.3 Rekayasa Sistem dan Analisis

Pada dasarnya terdapat 7 (tujuh) metode yang dapat digunakan dalam *steganografi* yaitu : *injection*, *subsitution*, *transform domain*, *spread spectrum*, *statistical method*, *distortion* dan *cover generation*. Dalam tugas akhir ini dipilih metode *spread spectrum* untuk *steganografi* citra JPEG.

Dalam metode *spread spectrum* proses penyisipan pesan dilakukan melalui tiga proses, yaitu spreading, modulasi, dan penyisipan pesan ke citra JPEG. Pesan yang disisipkan bernilai biner. Untuk itu dibangun perangkat lunak yang berfungsi untuk menyisipkan pesan dan membaca isi pesan rahasia. Perangkat lunak ini dibangun menggunakan *microsoft visual basic.6.0*.

2.4 Analisis Kebutuhan Perangkat Lunak

Kebutuhan sistem yang digunakan dalam *steganografi pada citra JPEG menggunakan* metode *spread spectrum* meliputi alat serta bahan–bahan penunjang lainnya seperti sebagai berikut :

1. Perangkat Keras (*Hardware*)

   Satu buah laptop dengan *hardware* minimal yang digunakan berikut:

   1. *Processor Intel Pentium MMX*
   2. *RAM 64 GB*
   3. *Hardisk 20 GB*
   4. *Monitor Standar*
   5. *CDRW Room*

2. Perangkat Lunak (*Software*)

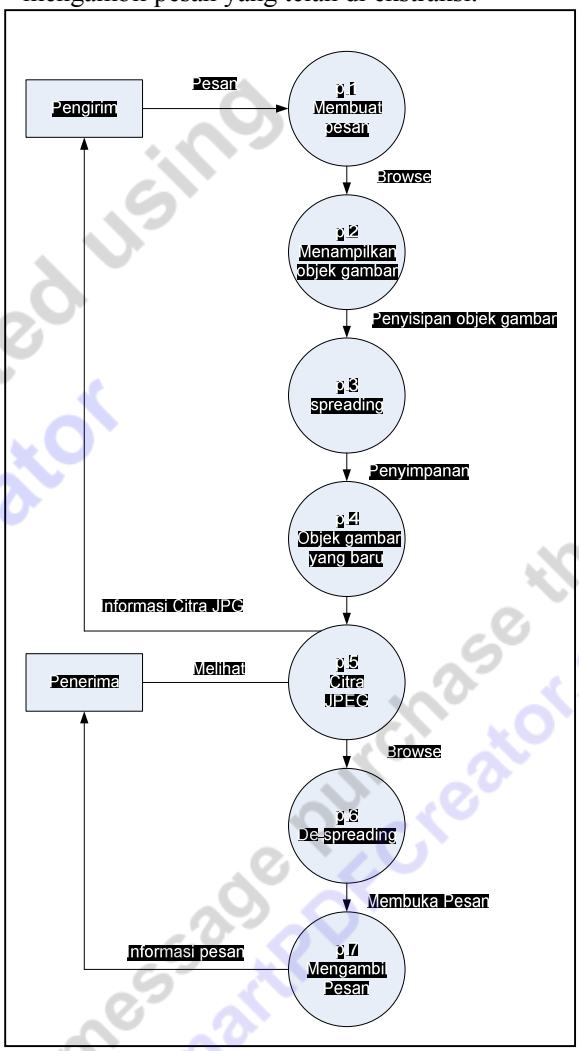
   Microsoft Visual Basic 6.0

2.5 Perancangan

Perancangan *steganografi pada citra JPEG menggunakan* metode *spread spectrum* menggunakan data *flow* diagram dan *flowchart*. Sedangkan untuk tampilan program terdiri dari *form* menu utama, *form* penyisipan pesan dan *form* ekstrasi pesan.

2.5.1 Data Flow Diagram

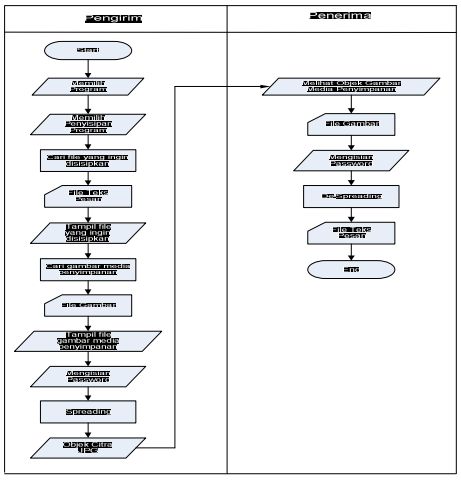
Data *flow* diagram (DFD) menjelaskan tentang aktor pengirim melakukan penyisipan pesan yang terdiri dari membaca pesan, penyimpanan pesan, spreading dan membaca citra jpeg. Aktor penerima melakukan pengekstraksi pesan yang terdiri dari membaca citra jpeg, penyimpanan pesan, de-spreading dan mengambil pesan yang telah di ekstraksi.



Gambar 2.5.1 Data *Flow* Diagram

2.5.2 *Flowchart*

Flowchart merupakan penggambaran secara grafik dari langkah-langkah dan urut-urutan prosedur dari suatu program.



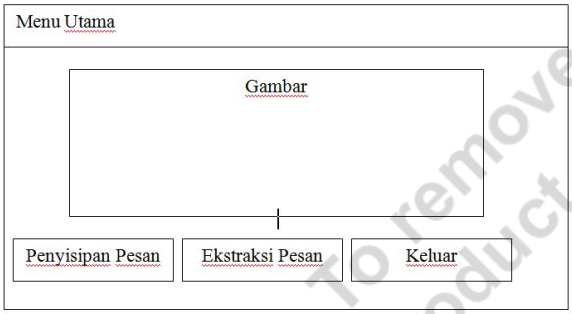
Gambar 2.5.2 *Flowchart*

2.6 Tampilan Program

Tampilan program terdiri dari *form* menu utama, *form* penyisipan pesan dan *form* ekstrasi pesan.

1. *Form* Menu Utama

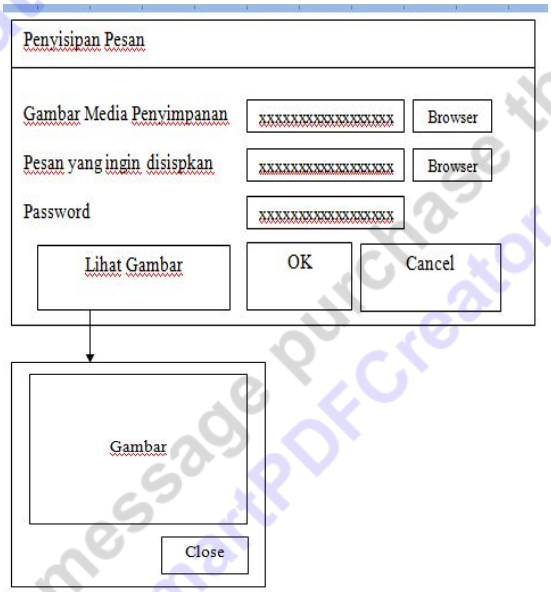
Form menu utama merupakan tampilan pertama ketika program dijalankan, pada *form* menu utama ini terdapat gambar, tombol-tombol seperti tombol penyisipan pesan, tombol ekstraksi pesan dan tombol keluar.



Gambar 2.6.1 Rancangan *Form* Menu Utama

2. *Form* Penyisipan Pesan

Form penyisipan pesan merupakan *form* yang tampil jika pengguna klik tombol penyisisipan pesan. Pada *form* penyisipan pesan ini terdapat fasilitas untuk masukan pesan yang ingin disisipkan dengan klik tombol *browser* untuk mencari *file* pesan yang ingin di sisipkan. Terdapat gambar media penyimpanan untuk objek yang disisipkan pesan dengan klik tombol *browser* untuk mencari gambar sebagai objek yang disisipkan.



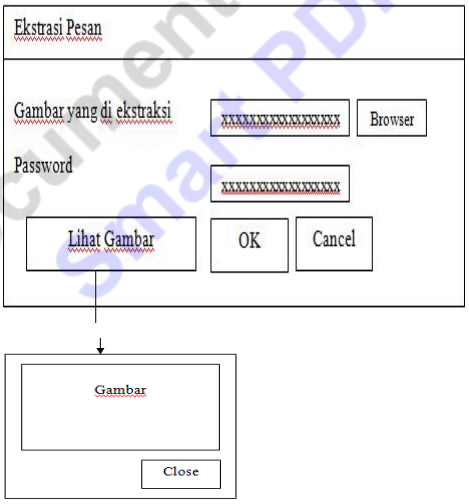
Gambar 2.6.2 Rancangan *Form* Penyisipan Pesan

Sistem kerja pada *form* penyisipan pesan yaitu memasukan nama *file* teks seperti yang extensinya txt (*.txt) pada *textbox* secara langsung atau dengan cara mencari *file* dengan klik *browser* pada pesan yang ingin disisipkan. Memasukan gambar pada *textbox* dengan klik *browser* pada gambar media penyimpanan. Setelah melakukan dua kegiatan diatas langkah selanjutnya memasukan *password* pada *textbox* yang sudah disediakan. *Password*

ditentukan oleh pengirim untuk penerima gambar yang telah disisipakan pesan rahasia. Media untuk pengiriman gambar dan *password* dengan komputer melalui *email*.

3. Form Ekstraksi Pesan

Form ekstraksi pesan merupakan *form* yang tampil jika pengguna klik tombol ekstraksi pesan. Pada *form* ekstraksi pesan ini terdapat fasilitas gambar yang di ekstrasi sebagai media penyimpanan untuk objek yang disisipkan pesan dengan klik tombol browser untuk mencari gambar sebagai objek yang disisipkan tersebut dan terdapat memasukan password untuk kata sandinya.



Gambar 2.6.3 Rancangan Form Ekstraksi Pesan

Sistem kerja pada *form* ekstrasi pesan yaitu. Memasukan gambar pada *textbox* dengan klik *browser* pada gambar media penyimpanan. Setelah melakukan kegiatan tersebut langkah selanjutnya memasukan *password* pada *textbox* yang sudah disediakan. *Password* dan gambar yang telah disisipkan pesan rahasia diperoleh oleh penerima dari pengirim melalui melalui *email*.

3. HASIL

Hasil dari rancangan program pada pembahasan bab III adalah tampilan dari masing-masing *form* dan bagaimana cara penggunaanya. Dari rancangan ini dibuat sebuah aplikasi *steganografi* dengan menggunakan *microsoft visual basic versi 6.0* sebagai bahasa pemrograman. Sebagai contoh penggunaan aplikasi disisipkan pesan berupa kalimat dari format txt (*.txt) yang disisipkan pada citra *JPEG*. Dalam program *steganografi pada citra JPEG menggunakan metode spread spectrum* sudah dibuat *file.exe* jadi untuk menjalankan aplikasi *steganografi* ini cukup mengklik *file* yang sudah dibuat, apabila *file* sudah diklik maka *steganografi pada citra JPEG menggunakan* metode *spread spectrum* langsung masuk ke menu utama. Adapun cara menjalankannya adalah sebagai berikut, hidupkan komputer dengan sistem operasi minimal *windows XP,* pada *desktop* komputer terdapat *shortcut* steganografi.exe klik dua kali, maka secara otomatis akan tampil *steganografi pada citra JPEG menggunakan* metode *spread spectrum* dan menampilkan menu utama.

Adapun *form-form* pada sebuah *steganografi pada citra JPEG menggunakan* metode *spread spectrum* dengan *microsoft visual basic versi 6.0* ini memiliki sub-sub *form* sebagai berikut :

1. *Form* penyisipan pesan merupakan *link* ke *form* penyisipan pesan yang berfungsi

untuk menampilkan proses penyisipan pesan pada *steganografi pada citra JPEG menggunakan* metode *spread spectrum*.

2. *Form* ekstrasi pesan merupakan *link* ke *form* ekstraksi pesan yang berfungsi untuk menampilkan proses ekstraksi pesan pada *steganografi pada citra JPEG menggunakan* metode *spread spectrum*.

Tampilan program terdiri dari *form* menu utama, *form* penyisipan pesan dan *form* ekstrasi pesan.

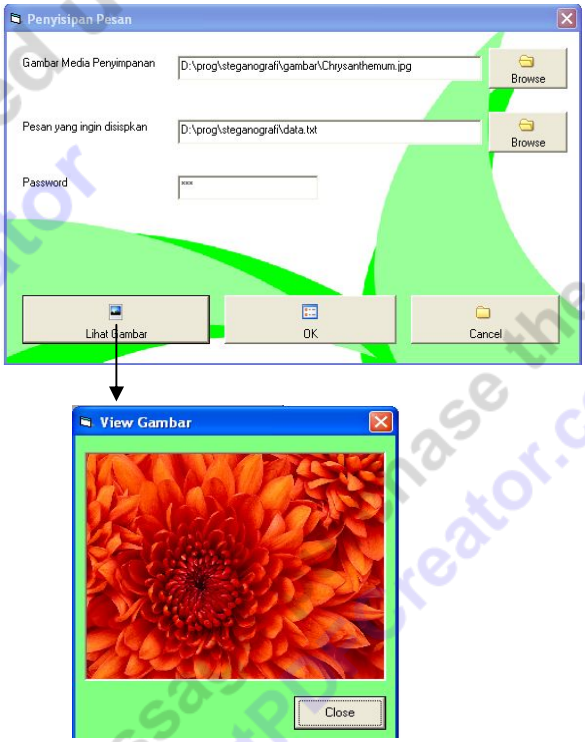
1. *Form* Menu Utama

Form menu utama merupakan tampilan pertama ketika program dijalankan, pada *form* menu utama ini terdapat gambar, tombol-tombol seperti tombol penyisipan pesan, tombol ekstraksi pesan dan tombol keluar.

Gambar 3.1 *Form* Menu Utama

2. *Form* Penyisipan Pesan

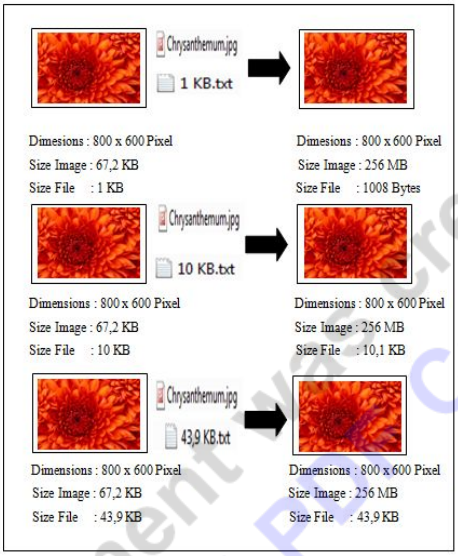
Form penyisipan pesan merupakan *form* yang tampil jika pengguna klik tombol penyisisipan pesan. Pada *form* penyisipan pesan ini terdapat fasilitas untuk memasukkan pesan yang ingin disisipkan dengan klik tombol *browser* untuk mencari *file* pesan yang ingin disisipkan. Terdapat gambar media penyimpanan untuk objek yang disisipkan pesan dengan klik tombol *browser* untuk mencari gambar sebagai objek yang disisipkan.



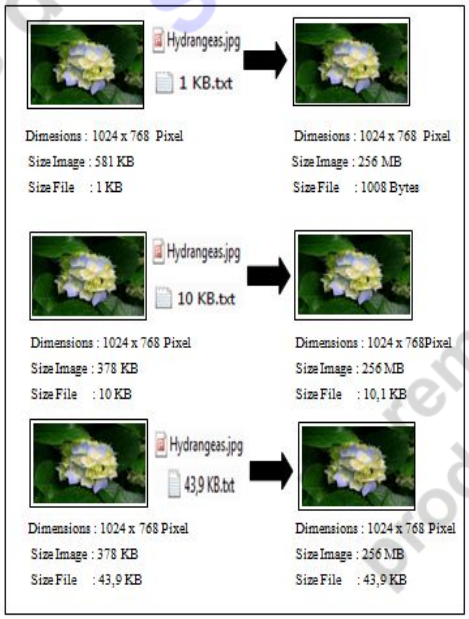
Gambar 3.2 *Form* Penyisipan Pesan

Sistem kerja pada *form* penyisipan pesan yaitu memasukan nama *file* teks seperti yang extensinya txt (*.txt) pada *textbox* secara langsung atau dengan cara mencari *file* dengan klik *browser* pada pesan yang ingin disisipkan. Memasukan gambar pada *textbox* dengan klik *browser* pada gambar media penyimpanan. Setelah melakukan dua kegiatan diatas langkah selanjutnya memasukan *password* pada *textbox* yang sudah disediakan. *Password* ditentukan oleh pengirim untuk penerima gambar yang telah disisipkan pesan rahasia. Media untuk pengiriman gambar dan

password dengan komputer melalui *email* dan ini merupakan hasil penyisipan pesan rahasia pada sebuah citra JPEG sebelum disisipkan pesan rahasia dan sesudah disisipkan oleh pesan rahasia.



Gambar 3.3 Penyisipan Pesan Rahasia Pada Gambar Dimensions 800 x 600 Pixel

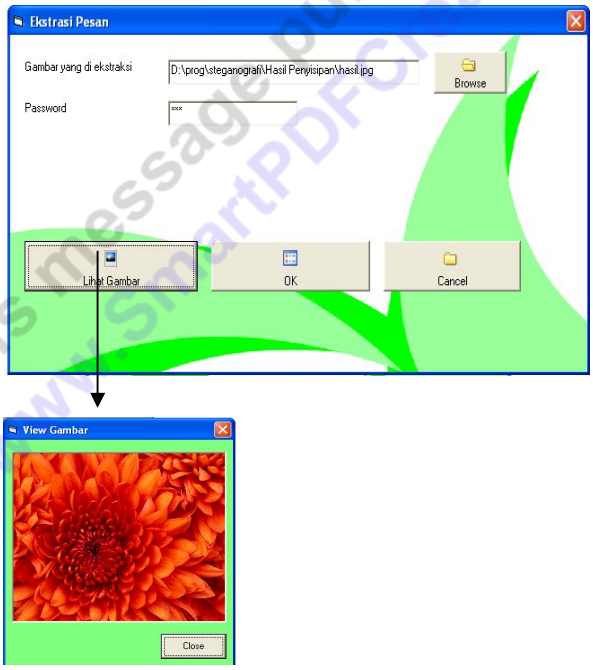


Gambar 3.4 Penyisipan Pesan Rahasia Pada Gambar Dimensions 1024 x 768 Pixel

Setelah dilakukan proses penyisipan jumlah size yang menjadi objek penyisipan sama dan hanya terjadi perubahan size data setelah proses ekstraksi.

3. *Form* Ekstraksi Pesan

Form ekstraksi pesan merupakan *form* yang tampil jika pengguna klik tombol ekstraksi pesan. Pada *form* ekstraksi pesan ini terdapat fasilitas untuk mengekstraksikan gambar yang telah disisipkan pesan dengan cara klik tombol browser untuk mencari gambar yang menjadi objek penyisipan dan terdapat memasukkan *password* untuk kata sandinya.



Gambar 3.5 *Form* Ekstraksi Pesan

Sistem kerja pada *form* ekstrasi pesan yaitu Memasukan gambar pada *textbox* dengan klik *browser* pada gambar media

penyimpanan. Setelah melakukan kegiatan tersebut langkah selanjutnya memasukan *password* yang sesuai dengan pengirim, lalu memasukan *password* tersebut pada *textbox* yang sudah disediakan. *Password* dan gambar yang telah disisipkan pesan rahasia diperoleh oleh penerima dari pengirim melalui *email*. Hasil dari ektraksi isi pesan rahasia tersebut tidak berubah, hanya size isi pesan rahasia saja yang bertambah apabila nama file hasil penyisipan pesan rahasia berbeda dengan hasil ektraksi pesan rahasia tersebut.

3. SIMPULAN

Berdasarkan dari penelitian yang telah dilaksanakan dan sudah diuraikan dalam steganografi pada citra jpeg menggunakan metode spread spectrum, maka penulis dapat menarik kesimpulan sebagai berikut :

1. Perangkat lunak ini dapat menyembunyikan dan melindungi keamanan data yang disisipkan pada citra *JPEG* dengan menggunakan metode *spread spectrum.*
2. Perangkat lunak steganografi pada citra jpeg menggunakan metode spread *spectrum* dibuat dengan *microsoft visual basic 6.0*.
3. Perangkat lunak ini hanya dapat menyisipkan data yang berformat txt (*.txt) dan data yang disisipkan tidak lebih dari 100 KB.
4. Perangkat lunak ini hanya dapat menyisipkan objek penyisipan berformat jpg (*.jpg).
5. Perangkat lunak ini menghasilkan size objek penyisipan yang sama setelah dilakukan proses penyisipan dan menghasilkan size data yang berbeda setelah dilakukan proses ekstraksi.

DAFTAR RUJUKAN

Dony, Ariyus. (2009), *Keamanan Multimedia*, Andi, Yogyakarta.

Pradito, Pandu. (2007), *JPEG (Joint Photographic Expert Group).* http://www.google.co.id/url?sa=t&rct=j&q=menurut%20pandu%20jpeg&source=web&cd=5&ved=0CDYQFjAE&url=http%3A%2F%2Fblog.ub.ac.id%2Fyafemo%2Ffiles%2F2011%2F07%2FJPEG.doc&ei=iRxBT5GtNYm0rAf9us3GBw&usg=AFQjCNEUrmXraHu3urdopU6Grvp8tjBZow&cad=rja (Didownload pada tanggal 04 November 2011)

Pressman, Roger.s. (2002), *Rekayasa Perangkat lunak*. ANDI, Yogyakarta.

Sutoyo T., dkk. (2009), *Teori Pengolahan Citra Digital*, Andi, Yogyakarta.

Winanti, Winda. (2009), *Penyembunyian Pesan pada Citra Terkompresi JPEG Menggunakan Metode Spread Spectrum*, Institut Teknologi Bandung, Bandung.