PERANCANGAN APLIKASI STEGANOGRAPHY PADA FILE IMAGE MENGGUNAKAN BAHASA C#

DESIGN OF STEGANOGRAPHY APPLICATION ON IMAGE FILE USING C#

Devy Septiani[1], Siti Madinah Ladjamuddin[2]
Program Studi Teknik Informatika, Fakultas Sains dan Teknologi Informasi
Institut Sains dan Teknologi Nasional
Jl. Moh. Kahfi II, Bhumi Srengseng Indah, Jagakarsa, Jakarta Selatan 12640
Telp. (021) 7874647, Fax. (021) 7866955
[1]septianidevy@gmail.com, [2]citymadinah07@istn.ac.id

ABSTRAKSI
Perkembangan media digital yang pesat dan penggunaannya yang meliputi berbagai bidang menimbulkan tuntutan yang semakin besar untuk menciptakan suatu sistem penyampaian informasi yang terjamin keamanannya. Salah satunya adalah dengan steganografi. Steganografi merupakan suatu metode untuk menyisipkan potongan informasi rahasia dalam suatu objek atau media lain. Dengan steganografi, informasi disembunyikan sedemikian rupa sehingga tidak diketahui keberadaannya, yang dikenal dengan istilah informasi hiding. Metode ini berbeda dengan metode kriptografi, yang menyandikan informasi yang ada sehingga tidak dapat dibaca tanpa mengetahui kunci atau sandi yang digunakan, namun keberadaannya tetap diketahui dan tidak disembunyikan. Penelitian akhir ini dikembangkan dengan menggunakan Microsoft Visual C# mengimplementasikan metode steganografi Simple Least Significant Bit Substitution (Simple LSB Subtitution) untuk menyembunyikan suatu informasi ke dalam file multimedia. File multimedia yang digunakan adalah file citra sebagai media pembawa informasi rahasia.
Kata kunci: steganografi, multimedia, penyisipan informasi, simple LSB substitution,

ABSTRACT
The rapid development of digital media and its use covers various fields which are becoming a bigger challenge to create an information delivery system that ensures its security. One of them is with steganography. Steganography is a method for inserting pieces of confidential information in an object or other media. With steganography, information is hidden in such a way that its whereabouts are unknown, which is known as hidden information. This method is different from cryptographic methods, which encode existing information so that it cannot be read without knowing the key or password used, but remains known and not hidden. In this study, it was developed using Microsoft Visual C# to implement the Simple Least Significant Bit Substitution (Simple LSB Substitution) steganography method to hide information into a multimedia file. The multimedia file used is an image file as a medium for carrying confidential information.
Keywords: steganography, multimedia, information insertion, simple LSB substitution

1. PENDAHULUAN

Teknologi yang begitu pesat membuat penggunaan komputer menjadi sangat penting hal ini juga diikuti oleh berkembangnya telekomunikasi, salah satunya internet. Melalui internet kita dapat mengenal dunia luar dengan cepat, namun internet memiliki beberapa kekurangan salah satunya adalah keamanan data sehingga menimbulkan tantangan dan tuntutan akan tersedianya suatu sistem pengamanan data yang sama canggihnya dengan kemajuan teknologi komputer itu sendiri.

Keamanan informasi menjadi bagian yang tidak dapat dipisahkan dalam dunia digital seperti sekarang ini. Seiring dengan berkembangnya teknologi, resiko ancaman terhadap informasi akan semakin besar, terutama pada informasi-informasi yang bersifat rahasia. Berbagai ancaman dari dunia maya seperti hacker dan cracker memperbesar resiko bocornya informasi tersebut ke pihak-pihak yang tidak dikehendaki. Kekhawatiran inilah yang menyebabkan terhambatnya penyampaian informasi, sementara informasi tersebut sangat dibutuhkan oleh pihak-pihak tertentu. Misalnya informasi yang berkaitan dengan aspek-aspek keputusan bisnis, keamanan negara, ataupun kepentingan umum. Tentunya informasi-informasi tersebut diminati oleh berbagai pihak.

Oleh karena itu, pengamanan informasi dalam hal ini adalah steganografi, semakin dibutuhkan guna memberikan rasa aman dalam proses penyampaian informasi. Steganografi sendiri merupakan cara untuk menyembunyikan suatu informasi rahasia di dalam suatu informasi atau informasi lain yang tampak tidak bermakna, kecuali bagi orang yang mengerti kuncinya. Teknik steganografi menggunakan dua media yang

berbeda secara bersamaan, dimana salah satunya berfungsi sebagai media yang berisikan informasi-informasi rahasia (dapat juga disebut *secret file*) dan yang lain berfungsi sebagai media pembawa informasi tersebut (*carrier file*). Pada penelitian akhir ini akan dibangun suatu aplikasi berbasis Microsoft Visual C# yang mengimplementasikan steganografi dengan menggunakan metode *simple least lignificant bit substitution* sebagai cara untuk menyembunyikan suatu informasi ke dalam *file* multimedia. Penggunaan teknologi steganografi ini diharapkan bukan hanya dapat membantu upaya meningkatkan keamanan penyampaian informasi, namun juga dapat membantu dalam proses perlindungan atas hak cipta hasil karya media elektronik.

Dalam pelaksanaan tugas penelitian ini terdapat beberapa permasalahan yang menjadi titik utama pembahasan, adapun permasalahan-permasalahan tersebut adalah sebagai berikut :

a. Bagaimana menyisipkan suatu informasi ke dalam file multimedia.
b. Bagaimana melindungi suatu informasi ke dalam file multimedia.
c. Bagaimana mengambil kembali suatu informasi dari berkas stego.

Batasan masalah pada penelitian ini agar tidak terjadi kesalahan persepsi dan tidak meluasnya pokok bahasan adalah sebagai berikut:

a. Format file citra digital yang akan digunakan adalah .bmp
b. Aplikasi yang dibuat mencakup aplikasi steganografi sederhana yang berfungsi untuk menyisipkan dan mengekstrak informasi dari media gambar.

2. METODOLOGI PENELITIAN

Perancangan Umum

Dalam perkembangan dunia informasi, keamanan suatu informasi merupakan suatu hal yang sangat vital. Hal ini dikarenakan tidak semua pihak, berhak untuk mengakses informasi yang bersangkutan. Oleh karena itu, diperlukan suatu aplikasi yang dapat digunakan untuk menyembunyikan atau menyamarkan suatu informasi ke dalam media lain.

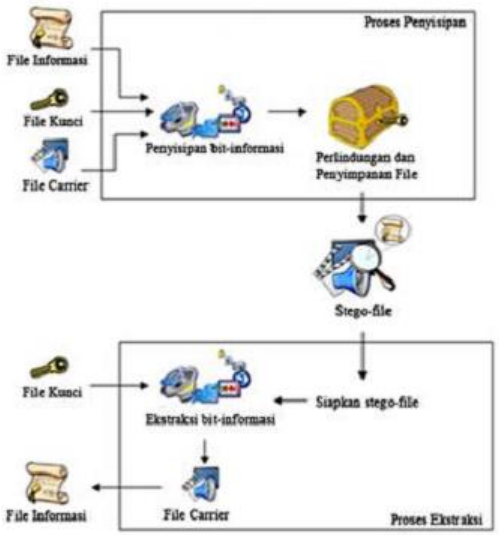
Steganografi merupakan suatu teknik berkomunikasi dimana informasi disembunyikan pada media pembawa seperti citra, suara atau video tanpa memberikan perubahan yang berarti pada media tersebut. Berbeda dengan kriptografi hanya menyembunyikan arti atau isi dari sebuah informasi, steganografi mampu menyembunyikan keberadaan informasi.

Pada bagian ini akan dijelaskan mengenai gambaran umum dari proses kerja aplikasi steganografi yang akan dibuat sebelum memulai fase perancangan sistem. Sebelum masuk ke dalam proses penyisipan (hiding), ada beberapa hal yang harus dilakukan terlebih dahulu oleh aplikasi ini nantinya. Pertama dilakukan penghitungan ukuran file informasi yang akan disisipkan. Dan yang kedua adalah penghitungan LSB dari calon carrier apakah mampu menampung keseluruhan file informasi tersebut. Jika tidak, maka harus ditambahkan file lainnya hingga mampu menampung keseluruhan file informasi yang akan disisipkan dan kemudian mempersiapkan pembagian file informasi untuk disisipkan ke dalam satu carrier file.

Penjelasan Skema Proses Kerja

Proses Penyisipan

Proses penyisipan dimulai dengan menyiapkan *key file*, *file* informasi, dan *carrier file*. Langkah berikutnya adalah menentukan LSB dari *file carrier*, dan kemudian menyisipkan informasi *key file* dan *file* informasi di dalamnya. Untuk penyisipan *file* citra digital, maka pada bagian ini akan menggunakan algoritma *simple LSB substitution* mekanisme penyisipan informasinya dan menggunakan dukungan stego.dll.



Gambar 1 Skema Proses Penyisipan dan Ekstraksi

Proses Ekstraksi

Proses ekstraksi informasi dimulai dengan menyiapkan *stego-file* dan *key file*. Aplikasi steganografi akan mencocokkan informasi *key file* yang ada dalam *stego-file* dengan *key file* yang disertakan saat proses ekstraksi. Dan jika terjadi kecocokan maka *file* informasi dapat diekstrak kembali. Proses ekstraksi informasi secara umum akan dilakukan dengan cara membalik algoritma proses penyisipan dan juga menggunakan *library* yang digunakan proses penyisipan tersebut.

Perancangan Sistem

Prosedur perancangan sistem secara umum untuk pembangunan aplikasi steganografi pada *file* multimedia ini terdiri atas beberapa tahap, antara lain meliputi perancangan :

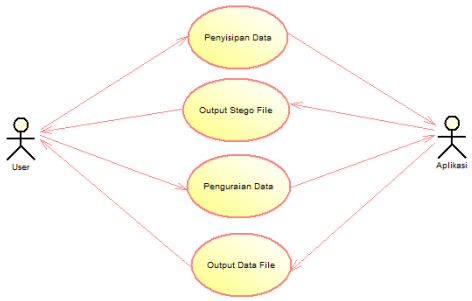
ISSN 2337-6805

Proses

Perancangan proses yang dimaksudkan adalah bagaimana sistem akan bekerja, proses-proses yang digunakan, mulai dari user melakukan input kemudian hingga aplikasi mengeluarkan *output* berupa *stego file* pada proses penyisipan (*hiding*). Dan juga saat user melakukan input *stego file* dan *key file* hingga aplikasi memberikan output berupa *secret file* dan *carrier file* pada proses penguraian (*extracting*).

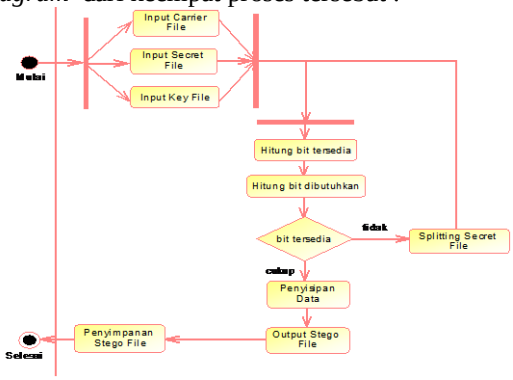
Antarmuka

Perancangan antarmuka mengandung penjelasan tentang desain dan implementasi sistem yang digunakan dalam sistem yang dibuat dan diwujudkan dalam tampilan antarmuka yang menghubungkan *user* dengan aplikasi. Gambar 2 menunjukkan *use case* diagram dari sistem yang akan dibangun.



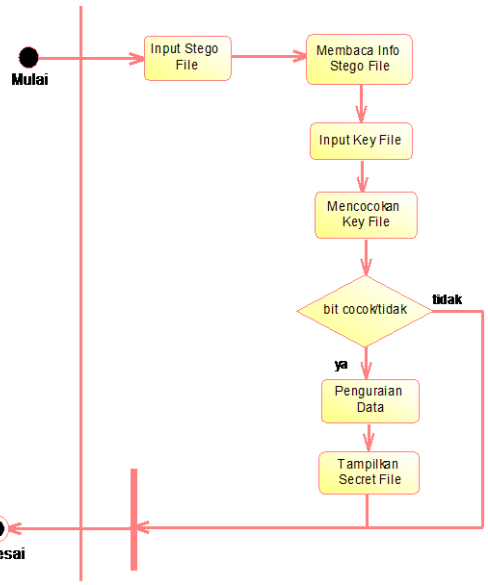
Gambar 2 *Use Case* Diagram Aplikasi

Proses utama yang dilakukan ada empat yaitu proses penyisipan informasi, proses *output stego image*, proses penguraian informasi dan proses *output* informasi *file*. Berikut *activity diagram* dari keempat proses tersebut :



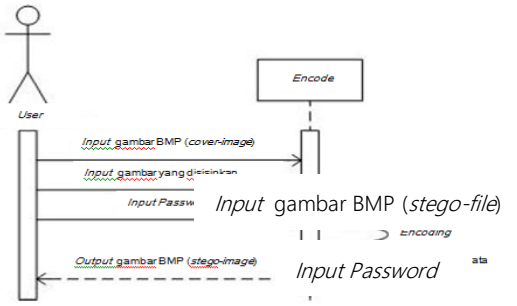
Gambar 3 *Activity Diagram* Penyisipan Informasi

Proses yang dijelaskan oleh gambar 3 berlangsung saat *user* ingin melakukan penyisipan informasi ke dalam *file* multimedia. Dari proses penyisipan informasi maka diperoleh hasil output *file* berupa stego-file.

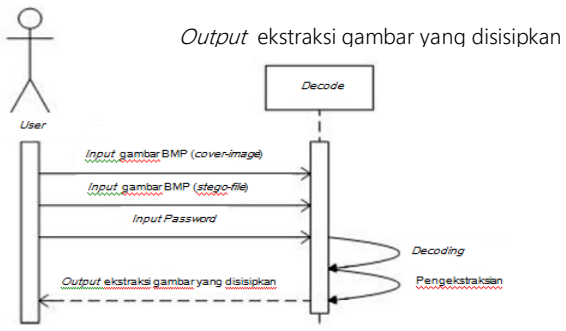


Gambar 4 *Activity Diagram* Penguraian Informasi

Proses yang ditunjukkan oleh gambar 4 berlangsung saat *user* ingin melakukan ekstraksi informasi dari *stego-file*. Dari hasil proses penguraian informasi, diperoleh hasil keluaran berupa *secret file* yang telah disisipkan pada proses sebelumnya.



Gambar 5 *Sequnce* Diagram *Encode*



Gambar 6 *Sequnce* Diagram *Decode*

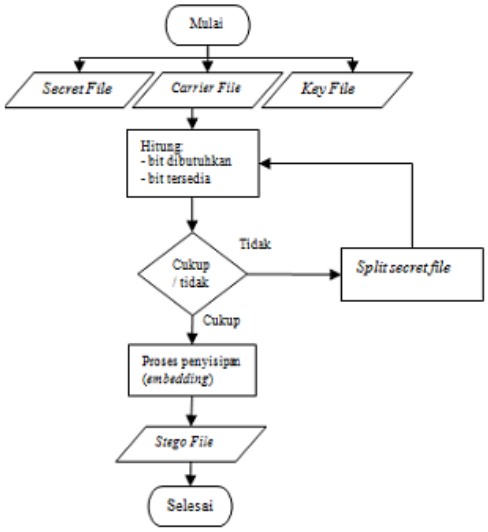
Uraian Perancangan Sistem

Perancangan sistem ini terdiri atas dua tahap, yaitu tahap penyisipan informasi dan tahap ekstraksi informasi yang akan diuraikan pada sub bab di bawah ini :

Tahap Penyisipan Informasi

Tahap penyisipan informasi merupakan tahap penyisipan atau penyamaran suatu informasi ke dalam *file* multimedia yang bertujuan untuk menyembunyikan informasi tersebut agar tidak terlihat oleh pihak yang tidak berhak. Pada tugas akhir ini, dilakukan beberapa teknik penyisipan informasi ke dalam *file* multimedia bergantung dari jenis *file* multimedia yang digunakan. Adapun metode yang digunakan adalah *Least Significant Bit Modification* untuk proses penyisipan informasi.

Flowchart Penyisipan Informasi



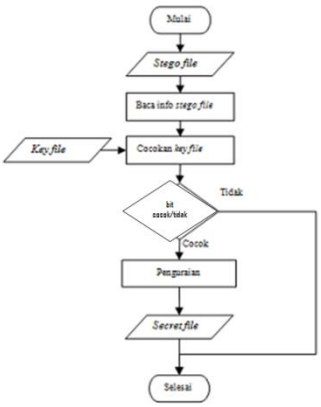
Gambar 7 *Flowchart* Penyisipan Informasi

Dari gambar 7 dapat dijelaskan langkah-langkah proses sebagai berikut: setelah memulai sistem (*start*), selanjutnya *user* melakukan input untuk *secret file*, *carrier file*, *key file*. Kemudian lakukan penghitungan bit yang dibutuhkan oleh *key file* dan *secret file*, serta berapakah bit yang mampu disediakan oleh *carrier file*, apakah bit yang tersedia mencukupi atau tidak. Jika tidak mencukupi maka akan diambil langkah-langkah untuk mencukupkan, jika yang dipilih adalah membagi *secret file* ke dalam lebih dari satu *carrier* maka akan dilakukan penambahan *carrier file*. Selanjutnya akan dimulai proses penyisipan informasi. Dari proses ini, akan dihasilkan *stego file*.

Tahap Ekstraksi Informasi

Pada tahap ini akan dilakukan proses ekstraksi informasi yang telah disisipkan dalam stego-file.

Flowchart Ekstraksi Informasi



Gambar 8 *Flowchart* Ekstraksi Informasi

3. HASIL DAN PEMBAHASAN

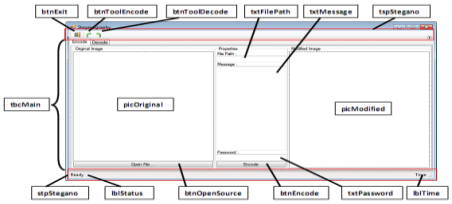
Implementasi

Implementasi merupakan tahap dimana program aplikasi siap dioperasikan pada keadaan yang sebenarnya sehingga dari sini akan diketahui apakah program aplikasi benar-benar dapat menghasilkan keluaran yang sesuai dengan tujuan yang diinginkan.

Tampilan Antar-muka Form Utama

Form Utama ini merupakan main-form dalam program *Steganography*. Pada form ini terdapat 2 tab untuk mengakses ke form berikutnya, yaitu *tab encode* dan *tab decode*. *Tab Encode* berfungsi untuk menyisipkan pesan berupa objek gambar dengan menambahkan sebuah *message* dan *password* untuk disisipkan pada objek tersebut.

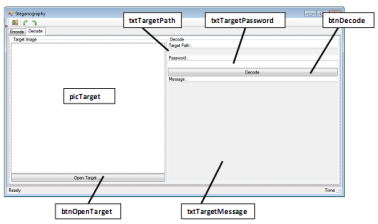
Tab Encode :



Gambar 9 Tampilan Form pada *Tab Encode*

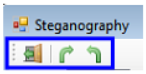
Pada *tab decode* berfungsi untuk mengekstrak pesan gambar agar *message* yang telah disisipkan tadi dapat terlihat. Form ini terdapat open target untuk mengambil gambar yang telah disimpan pada saat penyisipan file.

Tab Decode :



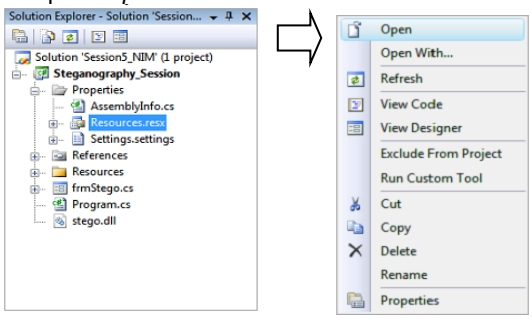
Gambar 10 Tampilan Form pada *Tab Decode*

Diatas tampilan *form steganography* terdapat 3 icon yaitu, *exit*, *encode* dan *decode* yang nantinya akan digunakan pada program tersebut. Pada *icon exit* berfungsi keluar dari program sedangkan icon *encode* dan *decode* fungsinya sama seperti pada *tab encode* dan *decode*.



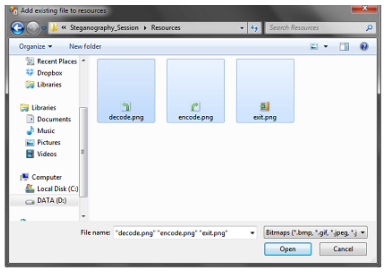
Gambar 11 *Icon* pada Program

Langkah untuk menampilkan *icon* tersebut yaitu dengan klik kanan pada Resource.resx di project dan pilih *Open*.



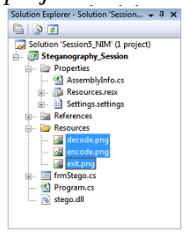
Gambar 12 Resource.resx

Setelah itu, klik *Add Resource – Add Existing File* kemudian pilih gambar-gambar yang ingin dimasukkan dan tekan OK.



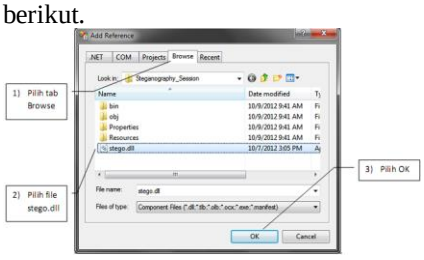
Gambar 13 *Add Existing File to Resource*

Gambar yang tadi ditambahkan akan terlihat pada *project*.



Gambar 14 *Solution Explorer*

Untuk mendukung aplikasi *steganography* dibutuhkan *library*. Klik kanan pada *project* dan pilih *Add Reference* kemudian akan muncul dialog berikut.



Gambar 15 *Add Reference*

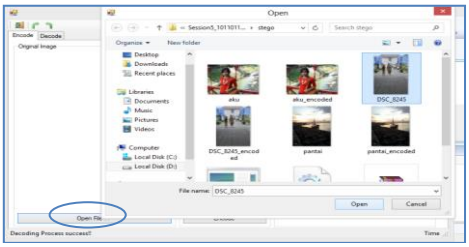
Ketika tombol OK ditekan, *library* sudah berhasil ditambahkan. *Library* yang baru ditambahkan bisa dilihat pada *project*.

Tampilan Program

Pada tahapan pertama proses encode terdapat form open file yang berfungsi untuk membuka *file image* dengan format .bmp kemudian saat program dijalankan, pilih open file pada image yg akan disisipkan.

ALGORITMA : Proses open file

```
Var : Image
      Image source = null
   If Bitmap image ==  Write (image) then
      Write (file path)
      Contain bitmap object
Write (image source)
   End if
```



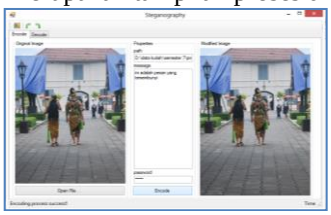
Gambar 16 Proses *Open File*

Setelah proses open file selesai, sisipkan pula *message* yang akan disampaikan. Dan gunakan password untuk menjaga keamanan data. Password tersebut merupakan *key file* yang dalam program ini adalah kunci dari aman atau tidaknya data yang kita miliki. Password yang digunakan jangan sampai salah pada saat akan mengestraksi data, karena jika sampai salah atau lupa, *message* yang disampaikan tidak akan terbaca pada proses *decode*.

ALGORITMA: Proses *encode* (penyisipan gambar)

```
Var : ICoverFile
          Image
          Cover picture = null
          Stego picture = null
      Try
Input cover picture
      String ⟶ temp
      String ⟶ new file
Write (new file, message, password)
Contain bitmap object
Write ("Encoding Process Success!!")
      Catch
Write ("Encoding Process failed!!")
      Finally
      If  stegoPicture != null then
          Write (stego picture)
      End if
```

Berikut ini merupakan tampilan proses *encode*.



Gambar 17 Proses *Encode*

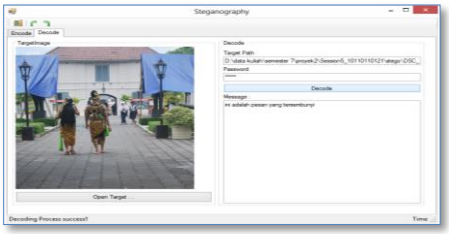
Proses *decode* yaitu proses mengekstrasi data yang telah disisipkan. Tahapan pada proses ini yaitu pilih open target pada *file image* yang telah disimpan pada saat proses *encode*, setelah selesai masukkan *password* yang sama dengan sebelumnya, kemudian *message* yang disampaikan akan terlihat.

ALGORITMA : Proses *decode* (mengekstrak gambar)

```
Var : String ⟶ TargetFile
      String ⟶ Password
Try
      Read (targetFile, password)
Read (message)
Write ("Decoding Process Success!!")
Catch
Write ("Decoding Process Failed!!")
Write (message)
```

ALGORITMA : Proses open target

```
Var :  Image
       Image source = null
   If  Bitmap image ==  Write (image) then
       Write (target path)
       Contain bitmap object
Write (image source)
   End if
```



Gambar 18 Proses *Decode*

4. SIMPULAN

Dari uraian hasil dan pembahasan diatas, dapat disimpulkan bahwa:

1. Untuk menyisipkan suatu informasi ke dalam file multimedia dibutukan suatu metode yaitu metode Least Significant Bit Modification, karena dengan menggunakan metode ini pesan dapat disembunyikan secara efektif.
2. Untuk melindungi suatu informasi ke dalam file multimedia dibutuhkan key file atau password. Dengan password ini pesan dapat terjaga keamanannya dengan baik.
3. Untuk mengambil kembali suatu informasi dari berkas stego diperlukan stego-file (image yang telah disimpan pada proses encode) dan key file (password). Dengan file tersebut aplikasi steganografi akan mencocokkan informasi key file yang ada dalam stego-file dengan key file.

Saran

Dari beberapa kesimpulan yang diambil, dapat diambil saran-saran yang dapat digunakan dalam membuat suatu aplikasi :

1. Untuk selanjutnya diharapkan mampu melakukan operasi steganography pada berbagai variasi ekstensi file multimedia.
2. Tampilan user interface untuk lebih disempurnakan agar lebih memudahkan use untuk mengoperasikan aplikasi ini.

5. DAFTAR PUSTAKA

[1] Tamim, Azwar. 2013, *Penyembunyian Pesan Text ke Dalam File .rtf dengan Perubahan Property Visual Minimum*, Kampus ITB Bandung.

[2] Putra, DOrisman. 2010, *Teknik Steganografi pada Rich Text Format File*, Institut Pertanian Bogor.

[3] Arryawan,Eko. *Anti Forensik, Mengatasi Investigasi Ahli Ahli Forensik*: Penerbit Elex Media Komputindo.

[4] Sadikin, Rifki. 2007. *Kriptografi, Untuk Keamanan jaringan*: Yokyakarta : Penerbit ANDI.

[5] Paulus, Erick & Nataliani, Yessica. 2007. *Cepat Mahir GUI MATLAB*, Yokyakarta : Penerbit ANDI.

[6] Ramza, Harry & Dewanto, Yohannes . 2007. *Teknik Pemrograman Menggunakan Matlab*, Jakarta : Grasindo.

[7] Yourdan, Edward. 1988. Modern Structured Analysis, New York : Yourdon Press Computing Series.

[8] Caesarendra, Wahyu. 2007. *Panduan Belajar Mandiri Matlab*: Penerbit Elex Media komputindo.

[9] *Aplikasi Pengamanan Dokumen dengan Menggunakan Algoritma El Gamal*. Penulis : Eko Aribowo, Teknik Informatika Ahmad Dahlan Jogjakarta.

[10] http://id.wikipedia.org/wiki/Steganografi, (Online), (diakses 02 Januari 2015 jam 21:05 WIB) .