Aplikasi Steganografi Citra Digital Menggunakan Metode LSB (Least Significant Bit) Visual Basic 6

Working Paper · May 2016

CITATIONS
0

READS
1,171

3 authors, including:

Finna Monica
UIN Sunan Gunung Djati Bandung
3 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Aplikasi Steganografi Citra Digital Menggunakan Metode LSB (*Least Significant Bit*) Visual Basic 6

Finna Monica[1], Entik Insanudin, MT.[2]
Jurusan Teknik Informatika
Fakultas Sains dan Teknologi UIN Sunan Gunung Djati Bandung
Jalan. A.H. Nasution 105 Cibiru-Bandung 40614
finnaica@student.uinsgd.ac.id

Abstrak

Saat ini teknologi informasi sudah sangat berkembang menjadi salah satu media yang paling populer didunia. Sayangnya dengan berkembangnnya teknologi informasi semakin berkembang pula tindak penyalahgunaan informasi yang bukan haknya. Dengan berbagai teknik banyak yang mencoba untuk mengakses informasi yang bukan haknya. Maka dari itu sejalan dengan berkembangnya media internet ini harus juga dibarengi dengan perkembangan pengamanan informasi. Berbagai macam teknik digunakan untuk melindungi informasi yang dirahasiakan dari orang yang tidak berhak, salah satunya adalah teknik steganografi.

Pada tugas akhir ini, dibuat aplikasi steganografi yang bertujuan untuk mengamankan informasi berupa pesan teks dengan menyisipkan (menyembunyikan) kedalam pesan lainnya yaitu pada citra digital dengan menggunakan metode algoritma LSB (Least Significant Bit).

Hasil dari aplikasi ini adalah dapat menyisipkan pesan tersembunyi berupa teks ke dalam berkas citra digital berformat JPEG dan dapat mengekstraksi kembali pesan tersembunyi tersebut dari dalam citra (stego-image).

***Kata Kunci* - Steganografi, LSB, VB 6**

Abstract

Current information technology has been highly developed into one of the most popular media in the world. Unfortunately with the growing information technology followed by misuse information that is not right. With various techniques ofmany who try to access information which is not right. Therefore, in line with the development of internet media must also be coupled with the development of information security. Various techniques are used to protect confidential information from a person who is not entitled to, one of which is the technique of steganography.

In this final task, steganography applications were made aimed at securing information in the form of a text message with the Insert (hide) into another message that is on a digital image using the algorithm LSB (Least Significant Bit).

The results of this application is able to insert hidden messages in the form of text into a digital image file formats such as JPEG and can extract the hidden message from back in the image (stego-image).

Keywords – Steganography, LSB, VB 6

I. PENDAHULUAN

Steganografi adalah seni dan ilmu untuk menyembunyikan pesan dalam sebuah pesan. Seni dan ilmu ini telah diterapkan sejak dahulu oleh orang Yunani kuno yang menyembunyikan pesan dengan cara membuat tato di kepala pembawa berita yang dibotaki dan menunggu sampai rambutnya tumbuh. Ketika perang dunia pertama, orang Jerman menyembunyikan pesan dalam bentuk "microdot", yaitu titik-titik yang kecil. Agen dapat membuat foto kemudian mengecilkannya sampai sekecil titik di tulisan dalam buku. Buku ini kemudian bisa dibawa-bawa tanpa ada yang curiga bahwa tanda titik di dalam tulisan di buku itu berisi pesan ataupun gambar.

Kerahasiaan pesan yang ingin disampaikan merupakan faktor utama sehingga digunakan metode steganografi. Dengan metode steganografi, pesan yang ingin disampaikan disembunyikan dalam suatu media umum sehingga diharapkan tidak akan menimbulkan kecurigaan dari pihak lain yang tidak diinginkan untuk mengetahui pesan rahasia tersebut. Oleh sebab itu metode steganografi terus digunakan dan dikembangkan sampai saat ini.

Saat ini internet sudah berkembang menjadi salah satu media yang paling populer di dunia. Karena fasilitas dan kemudahan yang dimiliki oleh internet maka internet untuk saat ini sudah menjadi barang yang tidak asing lagi. Sayangnya dengan berkembangnya internet dan aplikasi menggunakan internet semakin berkembang pula kejahatan sistem informasi. Dengan berbagai teknik banyak yang mencoba untuk mengakses informasi yang bukan haknya. Maka dari itu sejalan dengan berkembangnya

media internet ini harus juga dibarengi dengan perkembangan pengamanan sistem informasi.

Atas dasar uraian diatas, maka pada penulisan tugas akhiri ini akan membahas mengenai bagaimana mengamankan suatu pesan dengan menyisipkan (menyembunyikan) kedalam pesan lainnya yaitu file citra dengan menggunakan algoritma LSB (*Least Significant Bit*) pada suatu aplikasi steganografi.

II. LANDASAN TEORI

II.1 Steganografi

Steganografi berasal dari bahasa Yunani yaitu *Steganós* yang berarti menyembunyikan dan *Graptos* yang artinya tulisan, sehingga secara keseluruhan artinya adalah "tulisan yang disebunyikan". Secara umum steganografi merupakan ilmu yang mempelajari, meneliti, dan mengembangkan seni menyembunyikan sesuatu informasi. Secara teori, semua file umum yang ada di dalam komputer dapat digunakan sebagai media, seperti file gambar berformat JPEG, GIF, BMP, atau di dalam musik MP3, atau bahkan di dalam sebuah film dengan format WAV atau AVI. Semua dapat dijadikan tempat bersembunyi, asalkan file tersebut memiliki bit-bit data redundan yang dapat dimodifikasi. Setelah dimodifikasi file media tersebut tidak akan banyak terganggu fungsinya dan kualitasnya tidak akan jauh berbeda dengan aslinya.

II.2 Pengertian Steganografi

Steganografi merupakan suatu ilmu atau seni dalam menyembunyikan informasi dengan memasukkan informasi tersebut ke dalam pesan lain. Dengan demikian keberadaan informasi tersebut tidak diketahui oleh orang lain. Tujuan dari steganografi adalah menyembunyikan keberadaan pesan dan dapat dianggap sebagai pelengkap dari kriptografi yang bertujuan untuk menyembunyikan isi pesan. Oleh karena itu, berbeda dengan kriptografi, dalam steganografi pesan disembunyikan sedemikian rupa sehingga pihak lain tidak dapat mengetahui adanya pesan rahasia. Pesan rahasia tidak diubah menjadi karakter aneh seperti halnya kriptografi. Pesan tersebut hanya disembunyikan ke dalam suatu media berupa gambar, teks, musik, atau media digital lainnya dan terlihat seperti pesan biasa.

Teknik Steganografi yang digunakan dalam dunia moderrn sekarang ini sudah sangat beragam. Beragam mulai dari algoritma yang digunakannya sampai pada media yang digunakannya.

Beberapa contoh media penyisipan pesan rahasia yang digunakan dalam teknik Steganography antara lain adalah

1. **Teks.**
   Dalam algoritma Steganografi yang menggunakan teks sebagai media penyisipannya biasanya digunakan teknik NLP sehingga teks yang telah disisipi pesan rahasia tidak akan mencurigakan untuk orang yang melihatnya.
2. **Audio.**
   Format ini pun sering dipilih karena biasanya berkas dengan format ini berukuran relatif besar. Sehingga dapat menampung pesan rahasia dalam jumlah yang besar pula.
3. **Citra.**
   Format ini juga sering digunakan, karena format ini merupakan salah satu format file yang sering dipertukarkan dalam dunia internet. Alasan lainnya adalah banyaknya tersedia algoritma Steganografi untuk media penampung yang berupa citra.
4. **Video.**
   Format ini memang merupakan format dengan ukuran file yang relatif sangat besar namun jarang digunakan karena ukurannya yang terlalu besar sehingga mengurangi kepraktisannya dan juga kurangnya algoritma yang mendukung format ini.

II.3 Teknik Penyembunyian Data

Teknik penyembunyian data ke dalam citra digital dapat dilakukan dalam dua macam domain:

1. **Domain Spasial/waktu (*spatial/time domain*).**
   Teknik ini memodifikasi langsung nilai byte dari covertext (nilai byte dapat merepresentasikan intesitas/warna pixel atau amplitude). Metode yang tergolong ke dalam teknik ranah spasial adalah metode LSB.
2. **Domain Transform (*frequency transform domain*).**
   Teknik ini memodofikasi langsung hasil transformasi frekuensi sinyal. Metode yang tergolong ke dalam teknik ini ranah frekuensi adalah *spread spectrum*.

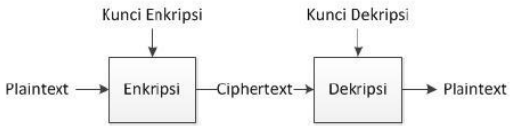
Pada tugas akhir ini, akan digunakan metode LSB (*Least Significant Bit*) yang merupakan teknik penyembunyian data yang bekerja pada domain spasial. Tiga aspek yang berbeda yang mempengaruhi sifat sistem penyembunyian atau penyisipan pesan rahasia pada gambar adalah : kapasitas, keamanan, dan ketahanan. Kapasitas merujuk pada jumlah informasi yang dapat disembunyikan dalam medium cover. Keamanan adalah ketidakmampuan pengamat untuk mendeteksi pesan yang tersembunyi, dan ketahanan yaitu jumlah modifikasi *stego medium*

yang dapat bertahan sebelum musuh dapat merusak pesan rahasia yang tersembunyi tersebut.

Steganografi modern hanya dapat dideteksi jika pesan rahasia diketahui kunci rahasianya. Hal ini mirip dengan prinsip Kerckhoff dalam kriptografi, yaitu memegang suatu keamanan sistem *kriptografi* harus mempercayakan semata-mata pada materi kuncinya. Dalam hal steganografi untuk tetap tidak terdeteksi, maka *medium cover* yang tidak dimodifikasi harus dijaga tetap rahasia, karena jika diperlihatkan, maka perbandingan antara medium cover dan medium stego akan mudah terungkap perbedaannya. Christian Cachin mengusulkan suatu model informasi teoritis untuk steganografi dengan mempertimbangkan masalah keamanan dari sistem *steganografi* terhadap pengintai yang pasif. Dalam model ini, dianggap bahwa musuh telah mengetahui sistem *encoding* tetapi tidak mengetahui kunci rahasianya.

Pada dasarnya komunikasi steganografi yaitu, pengirim dan penerima setuju pada suatu sistem steganografi dan membagi pakai (sharing) kunci rahasia untuk menentukan bagaimana suatu pesan dikodekan dalam citra digital. Untuk mengirim suatu pesan rahasia yang tersembunyi.

Proses utama dalam kriptografi ada dua, yaitu enkripsi dan dekripsi. Enkripsi adalah proses penyembunyian pesan dengan menggunakan key tertentu. Sedangkan dekripsi adalah proses pembacaan atau ekstrasi pesan dari *ciphertext*. Berikut ini gambaran umum dari proses tersebut.



Gambar 2.1 Enkripsi-Dekripsi

Berikut ini penjelesan mengenai istilah dan component utama yang sering dipakai dalam kriptografi:

1. ***Plaintext.***
   Plaintext adalah pesan yang akan kita kirim atau simpan dalam bentuk aslinya. Plaintext dapat dibaca secara langsung dan bermakna.
2. ***Ciphertext .***
   Ciphertext adalah pesan yang sudah kita enkripsi. Ciphertext tidak dapat dibaca secara langsubg dan tidak bermakna.
3. ***Enkripsi.***
   Enkripsi adalah proses penyembunyian pesan. Proses enkripsi merubah pesan plaintext menjadi ciphertext yang tidak bermakna. Pada algoritma saat ini, untuk melakukan enkripsi diperlukan suatu kunci.
4. ***Dekripsi.***
   Dekripsi adalah proses mengekstraksi pesan yang ada dalam ciphertext. Proses dekripsi akan menghasilkan plaintext yang sama seperti sebelum dienkripsi. Dalam dekripsi diperlukan juga kunci.
5. ***Key / kunci.***
   Key adalah suatu parameter yang digunakan untuk melakukan enkripsi maupun dekripsi. Kunci yang digunkan dapat berbentuk apapun seperti abjad, bilangan, atau bahkan dalam kriptografi modern dapat berupa bit.

Lewat notasi, proses tersebut dapat ditulis sebagai berikut:

Enkripsi

Ek(P) = C

E = fungsi enkripsi C = ciphertext
P = plaintext K = key

Dekripsi

Dk(C) = P

D = fungsi dekripsi C = ciphertext
P = plaintext K = key

II.4 Ukuran Teks yang Disembunyikan

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. Rumus untuk menghitung jumlah maksimal karakter yang dapat disisipkan ke gambar :

$$Max\ char = \frac{lebar\ gambar\ x\ panjang\ gambar}{8\ bit\ karakter} = \frac{200x200}{8} = 5000\ \text{char}$$

Ukuran teks yang akan disembunyikan bergantung pada ukuran gambar yang dijadikan sebagai wadah penyimpanan. Misalnya Suatu gambar yang digunakan sebagai wadah untuk penyimpanan berukuran 200 x 200 x 8b, berarti gambar mempunyai panjang 200 piksel, lebar 200 piksel dan 8b menunjukan format pikselnya 8 bit. Gambar tersebut mempunyai 40000 piksel, karena 1 karakter terdiri dari 8 bit (ASCII) maka pesan disisipkan pada setiap 8 piksel sehingga teks maksimal yang dapat disembunyikan pada gambar adalah sebanyak 40000/8=5000 karakter.

II.5 Teknik Steganografi Least Significant Bit (LSB)

Teknik Steganografi dengan menggunakan metode modifikasi Least Significant Bit (*LSB*) adalah teknik yang paling sederhana, pendekatan yang sederhana untuk menyisipkan informasi di dalam suatu citra digital (*medium*

cover). Mengkonversi suatu gambar dari format GIF atau BMP, yang merekonstruksi pesan yang sama dengan aslinya (*lossless compression*) ke JPEG yang *lossy compression*, dan ketika dilakukan kembali akan menghancurkan informasi yang tersembunyi dalam LSB.

Untuk menyembunyikan suatu gambar dalam LSB pada setiap byte dari gambar 24-bit, dapat disimpan 3 byte dalam setiap pixel. Gambar 1,024 x 768 mempunyai potensi untuk disembunyikan seluruhnya dari 2,359,296 bit (294,912 byte) pada informasi. Jika pesan tersebut dikompres untuk disembunyikan sebelum ditempelkan, dapat menyembunyikan sejumlah besar dari informasi. Pada pandangan mata manusia, hasil *stego-image* akan terlihat sama dengan gambar cover.

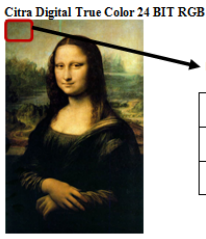
II.6 Visual Basic 6

Microsoft Visual Basic 6.0 (disingkat sebagai VB6.0) merupakan sebuah bahasa pemrograman yang menawarkan Integrated Development Environment (IDE) visual untuk membuat program perangkat lunak/ aplikasi berbasis sistem operasi Microsoft Windows yang berbasis GUI (Grapical User Interface).

Microsoft Visual Basic merupakan event-driven programming (pemrograman terkendali kejadian) artinya program menunggu sampai adanya respon dari pemakai berupa event atau kejadian tertentu (tombol diklik, menu dipilih, disentuh, dan lain-lain).

III. PEMBAHASAN

III.1 Algoritma LSB Proses Penyisipan (Embedding) pesan ke Citra Digital



Nilai Pixel Citra (RGB)

(100,120,80)	(90,75,190)	(100,80,80)
(80,180,35)	(80,122,200)	(85,120,100)
(100,120,80)	(80,122,200)	(80,122,200)

CONVERT KE BINER

Nilai Pixel Citra (Biner 8 bit)

(01100100,01111000,01010000)	(01011010,01001011,10111110)	(01100100,01010000,01010000)
(01010000,10110100,00100011)	(01010000,01111010,11001000)	(01010101,01111000,01100100)
(01100100,01111000,01010000)	(01010000,01111010,11001000)	(01100100,01111010,11001000)

PESAN YANG AKAN DISISIPKAN ADALAH “AB”
NILAI ASCII “A” ADALAH 65, BINERNYA 01000001
NILAI ASCII “B” ADALAH 66, BINERNYA 01000010

EMBEDDING PESAN KE CITRA DIGITAL DENGAN MENGGANTI BIT TERAKHIR

Nilai Pixel Setelah Embedding

(01100100,01111001,01010000)	(01011010,01001010,10111110)	(01100100,01010001,01010000)
(01010001,10110100,00100010)	(01010000,01111010,11001001)	(01010100,01111000,01100100)
(01100100,01111000,01010000)	(01010000,01111010,11001000)	(01100100,01111010,11001000)

CONVERT NILAI BINER KE DESIMAL

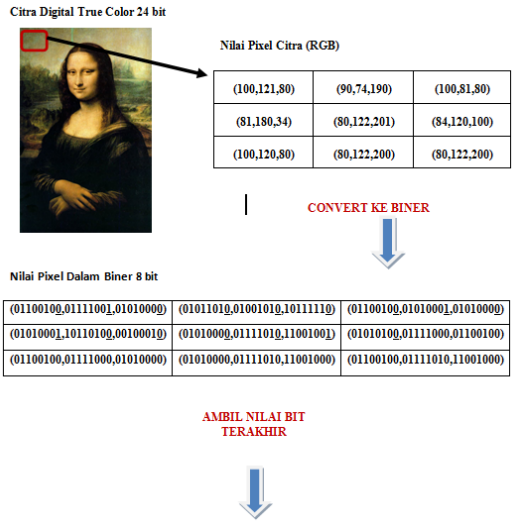
Nilai Pixel Citra (RGB)

(100,121,80)	(90,74,190)	(100,81,80)
(81,180,34)	(80,122,201)	(84,120,100)
(100,120,80)	(80,122,200)	(80,122,200)

CONVERT NILAI DESIMAL KE PIXEL

Convert Nilai Desimal ke Pixel. maka Citra digital yang sudah disisipi pesan tidak tampak / perbedaanya jika di lihat dengan kasat mata.

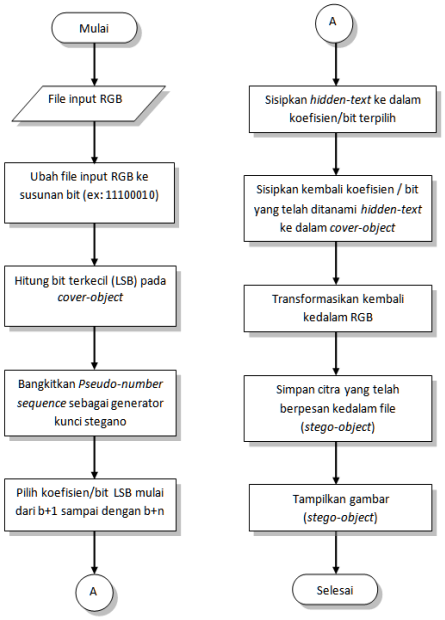
III.2 Algoritma proses Dekripsi (Ekstraksi) Pesan dari Citra Digital



Ambil Nilai Bit Terakhir:
01000001 = 65 = A
01000010 = 66 = B
PESAN HASIL EKSTRAKSI ADALAH "AB"

III.3 Flowchart LSB Proses Penyisipan (Embedding) pesan ke Citra Digital

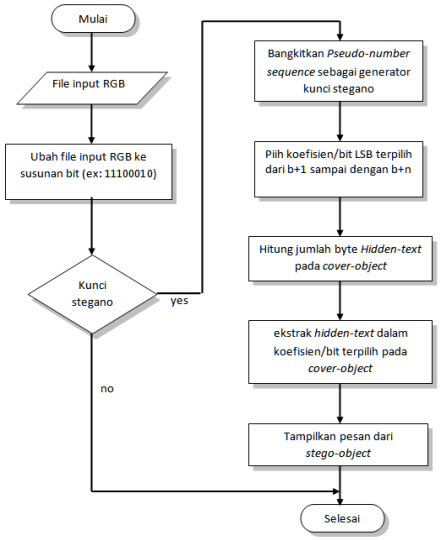
Diagram alir penyisipan teks ke dalam gambar dengan menggunakan Teknik *Least Significant Bit* pada perangkat lunak steganografi dapat dijabarkan dalam diagram alir berikut :



Gambar 1. Flowchart LSB Proses Penyisipan (Embedding) pesan ke Citra Digital

III.4 Flowchart proses Dekripsi (Ekstraksi) Pesan dari Citra Digital

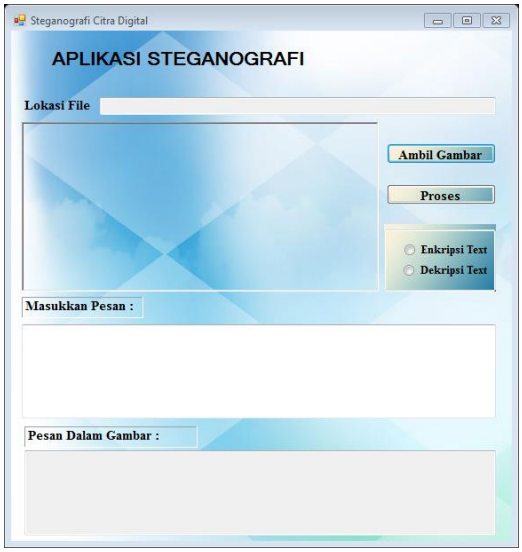
Diagram alir pengekstrakan teks yang ada pada gambar dapat dijelaskan pada gambar berikut :



Gambar 2. Flowchart proses Dekripsi (Ekstraksi) Pesan dari Citra Digital

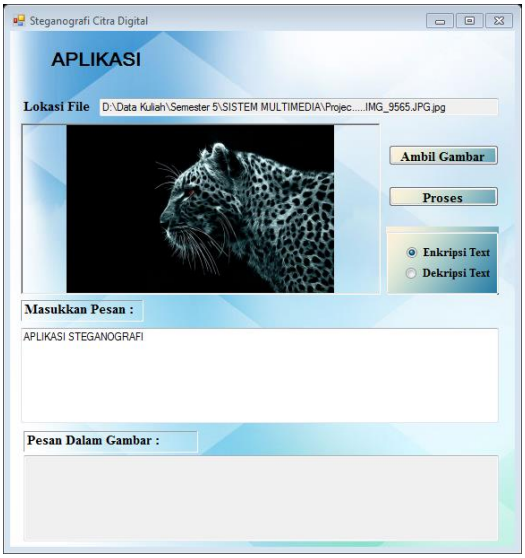
III.5 Design Interface Aplikasi

Berikut adalah design interface dari aplikasi steganografi yang dibangun dengan menggunakan Visual Basic 6.



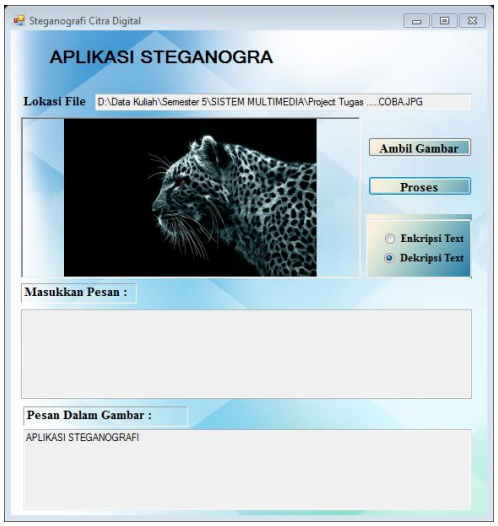
Gambar 3. Tampilan Utama

Dari tampilan utama, lakukan pengambilan gambar yang akan dijadikan sebagai wadah untuk menyisipkan teks. Kemudian dapat dilakukan pemilihan apakan akan mengenkripsi teks atau mendekripsi teks.



Gambar 4. Tampilan Citra yang Digunakan untuk Menyisipkan Text

Pada proses pemilihan citra pada enkripsi dan dekripsi tidak berbeda jauh. Perbedaannya hanyalah terletak pada hasil. Untuk proses dari enkripsi yaitu menghasilkan gambar yang didalamnya telah mengandung teks. Sedangkan pada proses dekripsi, hasilnya adalah teks yang sebelumnya telah disisipkan pada gambar dan hasilnya dapat dilihat pada gambar berikut :



Gambar 5. Tampilan Hasil Dekripsi Test pada Citra

IV. PENUTUP

IV.1 Simpulan

Hasil perancangan aplikasi steganografi dengan metode LSB dapat disimpulkan bahwa dapat dilakukan penyisipan pesan tersembunyi berupa teks ke dalam berkas citra digital berformat JPEG dan dapat mengekstraksi kembali pesan tersembunyi tersebut dari dalam citra. Memang terjadi perubahan pada ukuran citra namun secara kasat mata, perbedaan antara gambar sebelum dan sesudah disisipkan pesan tidak terlihat. Selain itu waktu yang dibutuhkan untuk proses enkripsi dan dekripsi dipengaruhi oleh kecepatan komputer yang digunakan dan ukuran citra

IV.2 Saran

Meskipun perancangan program enkripsi, dekripsi dan tahapan implementasi telah memenuhi kebutuhan proses pengamanan data namum aplikasi perlu dilakukan pengembangan agar lebih sempurna lagi

DAFTAR PUSTAKA

Alatas, Putri. (2009).*Implementasi Teknik Steganografi dengan Metode LSB pada Citra Digital*. Universitas Gunadarma : Jakarta

Cahyadi, Tri.(2012).*Steganografi LSB dengan Enkripsi Vigenere Chiper pada Citra JPEG*.Universitas Dipenogoro.

Setiawan, Wawan.(2012)*Aplikasi Keamanan Pesan Menggunakan Algoritma Steganografi dan Kriptografi*.Teknik Informatika UPN: Yogyakarta.

Suranta, Ricardo Pramana. (2012). *Perbandingan Ketahanan Algoritma LSB dan F5 dalam Steganografi Citra*.ITB: Bandung.