

STEGANOGRAFI AUDIO (WAV) MENGGUNAKAN METODE LSB (*LEAST SIGNIFICANT BIT*)

Sugeng Santoso¹

Arisman²

Windy Sentanu³

Alumni Universitas Budi Luhur¹, Alumni STMIK Raharja², Alumni STMIK³

e-mail : sugeng.santoso@raharja.info, arisman@raharja.info, windy.sentanu@raharja.info.

Diterima: 10 Agustus 2014/ Disetujui : 3 September 2014

ABSTRACT

Security of distributed information is essential for maintaining the confidentiality of the information. The process of securing is done by hiding the information on other digital media that are not visible existence. This technique is called steganography, the art of hiding data into digital media with a particular method so that other people do not realize there is something in the digital media. In this paper conducted a study to hide information into digital audio file is not compressed (.Wav) as a carrier file using the Least Significant Bit Modification. Least Significant Bit Modification is a method of hiding information by modifying the last bits of carrier files with the bits of information and only cause changes in the value of a bit higher or a lower one. The system was designed with two main processes, namely phase Embedding and Extracting stage.

KEYWORD : *Steganografi, Least Significant Bit Modification, Wideband Angular Vibration Experiment (WAVE) Format.*

ABSTRAK

Pengamanan terhadap informasi yang didistribusikan sangat penting untuk menjaga kerahasiaan suatu informasi. Proses pengamanan dilakukan dengan menyembunyikan informasi tersebut pada media digital lain agar tidak terlihat keberadaannya. Teknik ini disebut Steganography, yaitu seni menyembunyikan data ke dalam media digital dengan metode tertentu sehingga orang lain tidak menyadari ada sesuatu di dalam media digital tersebut. Dalam tulisan ini akan dilakukan penelitian untuk menyembunyikan sebuah informasi ke dalam file audio digital tidak terkompresi (.wav) sebagai file carrier dengan menggunakan metode Least Significant Bit Modification. Least Significant Bit Modification merupakan metode menyembunyikan informasi dengan memodifikasi bit terakhir dari file carrier dengan bit-bit informasi dan hanya menyebabkan perubahan nilai bit satu lebih tinggi atau satu lebih rendah. Sistem dirancang dengan dua buah proses utama yaitu tahap Embedding dan tahap Extracting.

Kata kunci : *Steganografi, Least Significant Bit Modification, Wideband Angular Vibration Experiment (WAVE) Format.*

PENDAHULUAN

Diseluruh dunia Internet (*Interconnection Network*) sudah berkembang menjadi salah satu media komunikasi data yang sangat populer. Kemudahan dalam penggunaan dan fasilitas yang lengkap merupakan keunggulan yang dimiliki oleh internet, dan bukan menjadi salah satu rahasia umum di kalangan masyarakat pengguna internet pada saat ini. Akan tetapi seiring dengan berkembangannya media internet dan aplikasi yang menggunakan internet semakin bertambah pula kejahatan dalam sistem informasi.

Berbagai macam teknik yang digunakan untuk melindungi informasi yang dirahasiakan dari orang yang tidak berhak telah banyak dilakukan dengan upaya mengamankan suatu data penting, salah satunya usaha untuk menangani masalah untuk keamanan data dalam media informasi adalah teknik kriptografi (*cryptography*). Dengan teknik kriptografi pesan asli (*plaintext*) yang ada diubah atau di enkripsi dengan suatu kunci (*key*) menjadi suatu informasi acak (*chiperteks*) yang tidak memiliki. Kunci hanya diketahui oleh yang memiliki informasi dari data tersebut dan yang menerima data tersebut, kemudian dapat digunakan untuk mengembalikan chiperteks dan plaintext oleh si penerima. Sehingga orang lain tidak dapat mengetahui pesan tersembunyi dalam media informasi tersebut melainkan hanya mengetahui pesan yang sudah diacak saja.

Namun dengan sifatnya yang acak dapat menimbulkan kecurigaan terhadap pesan yang sudah di acak oleh teknik kriptografi untuk mengatasi kecurigaan itu dapat dilakukan dengan metode lain yaitu adalah Steganografi yang dapat menyembunyikan data rahasia yang digunakan untuk menghindari keinginan orang untuk mengetahui isi pesan rahasia tersebut.

Steganografi (*steganography*) berasal dari kata Yunani yaitu *steganos* yang artinya adalah

tersembunyi atau terselubung dan *graphein* yang artinya menulis, sehingga arti lengkapnya adalah “ menulis suatu tulisan yang terselubung atau tersembunyi ”. Teknik ini meliputi metode komunikasi menyembunyikan pesan rahasia.

1. Perumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, permasalahan yang dihadapi dirumuskan sebagai berikut :

- a. Bagaimana mengimplementasikan algoritma Least Significant Bit untuk steganografi pada media audio ?
- b. Bagaimana perubahan dalam file output dari segi kualitas file audio sebelum dan sesudah disisipkan pesan ?

2. Tujuan

Tujuan pada proyek ini adalah :

- a. Menerapkan konsep steganografi untuk menyembunyikan keberadaan data dalam media informasi.
- b. Menganalisis sistem keamanan data yang digunakan saat ini sehingga dapat membantu pengguna media informasi agar lebih aman.

PEMBAHASAN

A. 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. (Alatas Putri, 2009:4)

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

1. Teks
 Dalam algoritma Steganografi yang menggunakan teks sebagai media penyisipannya biasanya digunakan teknik NLP (Natural Language Processing) sehingga teks yang telah disisipkan ke dalam pesan rahasia tidak akan mencurigakan untuk orang yang melihatnya.
 2. Audio
 Format ini pun sering dipilih karena biasanya berukuran relatif besar. Sehingga dapat menampung pesan rahasia dalam jumlah yang besar pula.
 3. Citra
 Format ini pun paling 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 mengurangkan kepraktisannya dan juga ukurannya yang mendukung format ini.
- 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, 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. (Alatas Putri, 2009:5)

B. Kriteria Steganografi

Kriteria steganografi yang baik yakni sebagai berikut : (Ariyus, 2009:12)

1. Imperceptibility

Keberadaan pesan tidak dapat dipersepsi oleh indera manusia. Jika pesan disisipkan ke dalam sebuah citra, citra yang telah disisipi pesan harus tidak dapat penurunan kualitas warna pada file citra yang telah disisipi pesan rahasia dengan citra asli oleh mata. Begitu pula dengan suara, seharusnya tidak terdapat perbedaan antara suara asli dengan suara yang telah disisipi pesan.

2. Fidelity

Mutu media penampung (cover object) tidak berubah banyak akibat penyisipan (embedded). Citra hasil steganografi masih terlihat dengan baik. Pengamat tidak mengetahui kalau di dalam citra tersebut terdapat data rahasia.

3. Robustness

Pesan atau data yang disembunyikan harus tahan terhadap manipulasi yang dilakukan ke pada citra penampung, seperti pengubahan kontras, penajaman, pemampatan, rotasi, perbesaran gambar, pemotongan (cropping), enkripsi, dan sebagainya. Bila pada citra dilakukan hal tersebut

but, maka data yang disembunyikan tidak rusak.

4. Recovery

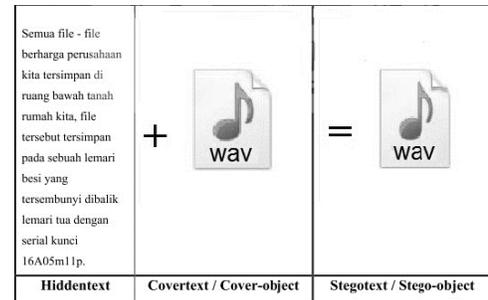
Pesan yang disembunyikan harus dapat diungkap kembali. Tujuan steganografi adalah menyembunyikan informasi, maka sewaktu-waktu informasi yang disembunyikan ini harus dapat diambil kembali untuk dapat digunakan lebih lanjut sesuai keperluan.

C. Konsep Steganografi

Konsep dari steganografi adalah menyembunyikan pesan dalam media lain, sehingga pesan tidak dapat diterjemahkan secara langsung, dalam steganografi dikenal beberapa istilah yaitu: (Alatas Putri, 2009:8)

1. *Hidden Text*, merupakan pesan yang disembunyikan.
2. *Cover text*, merupakan media yang digunakan untuk menampung pesan.
3. *Stego text*, merupakan media yang sudah disisipkan pesan.
4. *Stego key*, merupakan kunci yang digunakan untuk menyisipkan pesan maupun membaca pesan.

Didalam Steganografi citra digital ini, hidden text atau embedded message yang dimaksudkan adalah teks yang akan disisipkan ke dalam cover text atau cover – object yaitu file citra digital yang digunakan sebagai media penampung pesan yang disipkan. Dari hasil encoding atau embedding pesan kedalam file citra akan dihasilkan stegotext atau stego – object yang merupakan file citra yang berisikan pesan *embedding*. Pada gambar dibawah ini merupakan contoh hiddentext, coverttext dan stegotext.



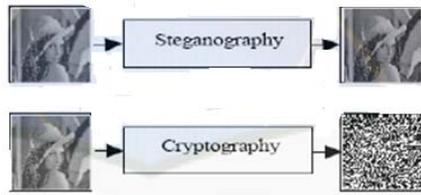
Gambar 2.1 Contoh Hiddentext, Coverttext dan Stegotext.

Penyisipan pesan ke dalam media coverttext dinamakan encoding, sedangkan ekstraksi pesan dari pesan dari stegotext dinamakan decoding. Kedua proses ini memerlukan kunci rahasia (stegokey) agar hanya pihak yang berhak saja yang dapat melakukan penyisipan dan ekstraksi pesan.

D. Perbedaan Steganografi dengan Kriptografi

Steganografi merupakan pelengkap dari kriptografi bukan pengganti. Sebab dari kedua disiplin ilmu tersebut dapat digunakan konsep secara bersamaan ataupun secara terpisah. Seperti halnya pesan yang telah terenkripsi disembunyikan ke dalam suatu media audio. Proses enkripsi merupakan teknik dalam ilmu kriptografi sedangkan menyembunyikan pesan yang telah terenkripsi merupakan teknik ilmu steganografi.

Dari segi tujuan kriptografi bertujuan untuk menyembunyikan isi (content) pesan agar pesan tidak dapat dibaca. Sedangkan steganografi bertujuan untuk menyembunyikan keberadaan (existence) pesan untuk menghindari kecurigaan (conspicuous). Gambar berikut ini merupakan visualisasi steganografi dan kriptografi. (Fahri,2010:13)

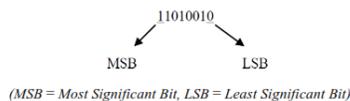


Gambar 2.2 Steganography versus Cryptography

E. Metode LSB (Least Significant bit)

Least Significant Bit (LSB) adalah cara yang paling umum untuk menyembunyikan pesan. LSB dilakukan dengan memodifikasi bit-bit yang termasuk bit LSB pada setiap byte warna pada sebuah piksel. Bit-bit LSB ini akan dimodifikasi dengan menggantikan setiap LSB yang ada dengan bit-bit pesan rahasia yang ingin disembunyikan. Setelah semua bit pesan rahasia menggantikan bit LSB file tersebut, maka pesan rahasia telah berhasil disembunyikan.

Metode ini membutuhkan syarat, yaitu jika dilakukan kompresi pada file stego, harus digunakan format lossless compression. Hal ini dikarenakan metode ini menggunakan bit-bit pada setiap piksel pada image. Jika digunakan format lossy compression, pesan rahasia yang disembunyikan dapat hilang. Contoh penggunaan LSB, sebuah susunan bit pada sebuah byte :



Bit yang sesuai untuk ditukar adalah bit LSB

karena perubahan pada daerah tersebut hanya akan menyebabkan nilai byte menjadi lebih tinggi 1 angka atau lebih rendah jika dalam nilai sebelumnya.

Pada gambar 1, menandakan bahwa bit 1 dari depan menyatakan bit MSB dan bit 0 dari bilangan biner terakhir adalah bit LSB. Dapat dilihat contoh dibawah ini :

Jika pesan = 10 bit, maka jumlah byte yang digunakan = 10 byte

```

00110011
10100010 10100011
00100110
01011001
01101110 10110101
00010101
11100110
11011010
    
```

Misalkan binary dari embedded message: 1110101011 Hasil penyisipan pada bit LSB:

```

00110011
10100011 10100011
00100110
01011001
01101110 10110101
00010100
11100111
11011011
    
```

Pada contoh diatas, hanya sebagian yang berubah dari Least Significant Bit. Berdasarkan teori maka didapatkan bahwa ukuran file asli tidak mengalami perubahan yang begitu besar sehingga sulit terdeteksi oleh indra manusia.

F. File WAV

Format file audio tanpa proses kompresi yang paling

sering ditemui adalah PCM (Pulse Code Modulation), yang biasanya tersimpan dalam file .wav di dalam Windows dan sebagai .aiff di dalam Mac OS.

WAV adalah bentuk format file yang fleksibel untuk menyimpan semua kombinasi audio baik rates maupun bitrates. Hal ini menyebabkan format file dalam bentuk .wav sangat layak untuk menyimpan dan mengarsipkan rekaman asli. Untuk format audio lossless, akan dibutuhkan lebih banyak proses pada saat direkam, tetapi akan sangat efisien dalam hal penggunaan memori. WAV, seperti halnya seluruh format file yang tidak dikompres, akan meng-enkodng-kan semua suara, baik suara yang kompleks maupun tanpa suara, dengan jumlah bit yang sama setiap satuan waktunya. Contohnya: sebuah file menyimpan rekaman dari orkestra selama satu menit akan sama besar dengan file yang menyimpan satu menit keadaan diam tanpa suara apabila keduanya disimpan dalam bentuk format WAV. Apabila file di encoding dengan format file lossless, maka dengan contoh yang sama, file pertama akan menempati lebih sedikit memori sedangkan file kedua sangat sedikit menggunakan memori. Namun bagaimanapun juga, untuk meng-encoding file ke dalam format file lossless akan membutuhkan waktu yang jauh lebih lama dibandingkan dengan format file yang tidak dikompres sama sekali, yakni dalam format WAV. Dewasa ini, format audio lossless telah mengalami perkembangan, contoh: TAK, di mana dapat menyimpan file dengan cepat dengan kompresi yang juga baik.

G. Struktur WAV

File WAV menggunakan struktur standar RIFF dengan mengelompokkan isi file ke dalam bagian-bagian seperti format WAV dan data digital audio. Setiap bagian memiliki headernya sendiri-sendiri beserta dengan ukurannya.

Struktur RIFF (Resource Interchange File Format) ini merupakan struktur yang biasa digunakan untuk data multimedia dalam Windows. Struktur ini mengatur data dalam file ke dalam bagian-bagian yang masing-masing memiliki header dan ukurannya sendiri dan disebut sebagai chunk. Struktur ini memungkinkan bagi program bila tidak mengenali bagian tertentu untuk melompati bagian tersebut dan terus memproses bagian yang dikenal. Data dari suatu bagian bisa memiliki sub-bagian dan seluruh data dalam file berstruktur RIFF selalu merupakan subbagian dari suatu bagian yang memiliki header "RIFF". Contoh file yang menggunakan struktur RIFF adalah file WAV dan AVI.

Sesuai dengan struktur file RIFF, file WAV diawali dengan 4 byte yang berisi 'RIFF' lalu diikuti oleh 4 byte yang menyatakan ukuran dari file tersebut dan 4 byte lagi yang berisi 'WAVE' yang menyatakan bahwa file tersebut adalah file WAV. Berikutnya adalah informasi dari format sample yang menjadi sub-bagian dari bagian RIFF lalu diikuti sub-bagian data audionya.

H. Spesifikasi Sistem

Spesifikasi sistem aplikasi Steganografimeliputi input file, output dan proses yang direncanakan.

1. Input
Input yang dibutuhkan adalah file teks data r yang merupakan pesan atau informasi yang dirahasia yang akan disisipkan pada audio WAV. Format file teks mempunyai karakter yang harus mendukung ASCII, yang dapat dibaca pada sistem operasi Unix, Mac, Ms. Windows dan DOS dan sistem operasi lainnya. Dengan sedikit bentuk format (tidak dicetak tebal atau miring), karakter yang mendukung ISO 8859-1 dan juga ANSI. Encoding yang digunakan juga harus mendukung UTF-8, karena serupa dengan ASCII. Input selanjutnya adalah file audio dengan format WAV yang mendukung jenis Gelombang, Amplitudo, Struktur RIFF (Resource Interchange File Format) dalam format WAV.
2. Output
File audio WAV dengan file teks yang telah disisipkan dengan proses encode, yang disebut stego audio. Kemudian pesan teks yang telah disisipkan, dapat dibaca kembali dengan menggunakan proses decode.
3. Proses Yang Direncanakan
Di dalam sistem aplikasi Steganografi, masukan file awal adalah file teks data dengan ukuran yang cukup kecil, file teks data yang mendukung karakter ASCII dan akan dikonservasi menjadi

bilangan biner, kemudian file binary tersebut satu persatu akan disisipkan pada file binary audio WAV, yang nantinya menjadi stego audio. Langkah-langkah proses yang direncanakan:

Proses encode yang meliputi tahapan sebagai berikut :

- a. Menginputkan file teks.
- b. Menginputkan file audio.
- c. Melakukan penyisipan.
- d. Penyimpanan file audio stego.

Proses decode yang meliputi tahapan sebagai berikut :

- Memanggil file stego audio.
- Menampilkan pesan Teks.
- Menyimpan file teks.
- Memutar file audio.

I. Parameter kesuksesan

Sistem aplikasi Steganografi dapat dikatakan berhasil jika sistem memiliki parameter dibawah ini :

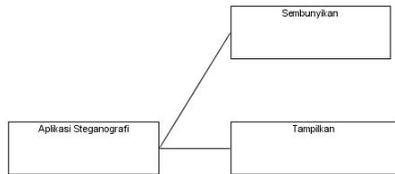
1. File teks dengan karakter ASCII.
2. File audio WAV yang mendukung format Gelombang, Amplitudo, Struktur RIFF.
3. Melakukan proses encode.
4. Melakukan proses decode.
5. Pesan pada stego audio dapat ditampilkan kembali.
6. File audio dapat diputar.

J. Interface pembuatan sistem

Perancang tampilan menu dan fitur pada sistem aplikasi Steganografi meliputi perancang tampilan menu utama, tampilan untuk proses encode dan tampilan untuk proses decode. Perancang sistem interface menggunakan tool pengembang dari MathWorks, yaitu Matlab R2010b.

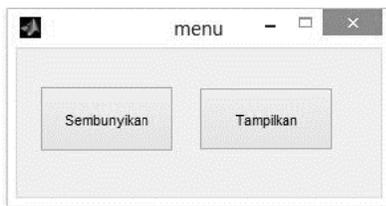
1. Struktur Menu

Struktur menu yang adapada program aplikasidirancangsebagaiberikut.



Gambar 2.3 Struktur menu

2. Rancangan layar

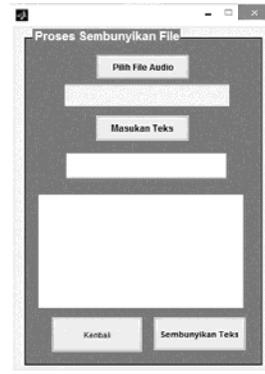


a. RancanganLayarUtama

Gambar2.4

RancanganLayarUtamaPadagambar 3.8menggambarkanperancangantampilan ayarutamasystemSteganografi yang terdiridariduabagian : bagian tampilan menu proses Sembunyikan yang terdiridari form teks yang berfungsiinput file teks , menginputkan kata sandiantombolbuka audio yang berfungsiuntukmengambil file audio dengan format WAVpada media penyimpanan, dankemudian proses encode. Untukbagiantampilan proses Tampilkanmeliputifungsiuntukmemanggil file stego audiodari media penyimpanan, validasi kata sandi, danmenampilkanpesanstegopada menu tampilanpesan.

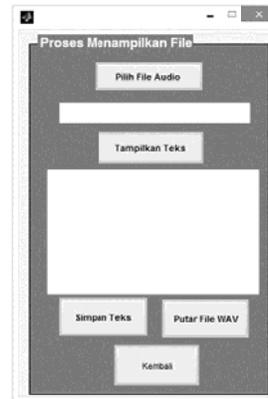
b. RancanganLayarSembunyikan



Gambar2.5 RancanganLayarSembunyikan

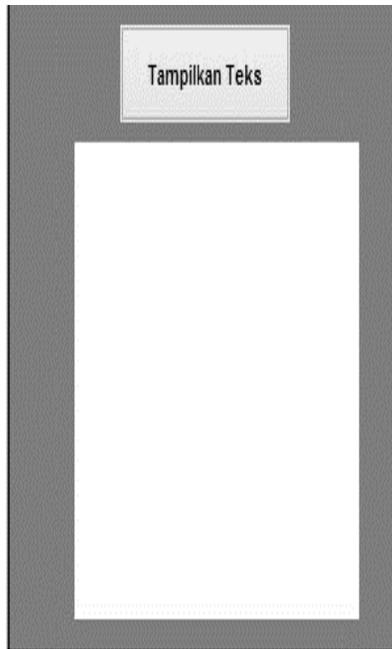
Padagambar 2.5 menampilkanperancangan proses penginputanteks, fileAudio, proses encode, danSembunyikanTeks.

c.RancanganLayarTampilkan



Gambar 2.6 RancanganLayarTampilkan

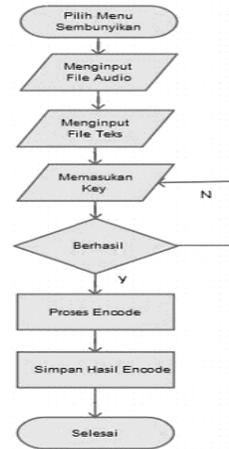
Perancangan tampilanuntuk melihat pesan teks rahasia yang disembunyikan pada file stego audio dapat dilihat pada gambar 2.6.



Gambar 2.7 Rancangan Layar Pesan

3. Flowchart
Flowchart merupakan gambar atau bagan yang memperlihatkan urutan dan hubungan antar proses beserta instruksinya. Gambar ini dinyatakan dengan simbol. Dengan demikian setiap simbol menggambarkan proses tertentu. Sedangkan hubungan antar proses digambarkan dengan garis penghubung. Perancangan proses pada system Enkripsi meliputi pembuatan flowchart dari proses encode dan proses decode. Dalam perancangan proses encode dan proses decode akan digambarkan pada gambar dibawah ini:

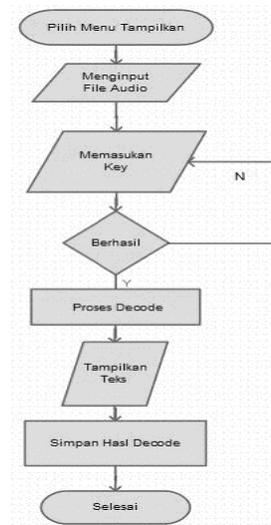
a. Flowchart Enkripsi pada steganografi



Gambar2.8 Proses encode

Pada gambar 2.8 menggambarkan proses encode pada system Enkripsi yang akan dirancang.

b. Flowchart deskripsi pada steganografi



Gambar2.8 Proses decode

Padagambar 3.4 menggambarkan proses decode pada system Enkripsi dan melihat hasil akhir dari proses tersebut yaitu menampilkan pesan yang disembunyikan pada File audio.

K. Pengujian steganografi

Pengujian system steganografi meliputi pengujian, pengujian system pada Cover Audio, pengujian system pada Audio yang dijadikan cover.

1. Pengujian Dengan Cover Audio

Adapun data awal sebelum dilakukan proses penyembunyian file Audio WAV dan proses enkripsi, yaitu :

- Bit Rate : 1411 kbps
- Ukuran Audio : 21,151 KB (21.657.644 bytes)
- Ukuran File Teks : 142 bytes (18 karakter)

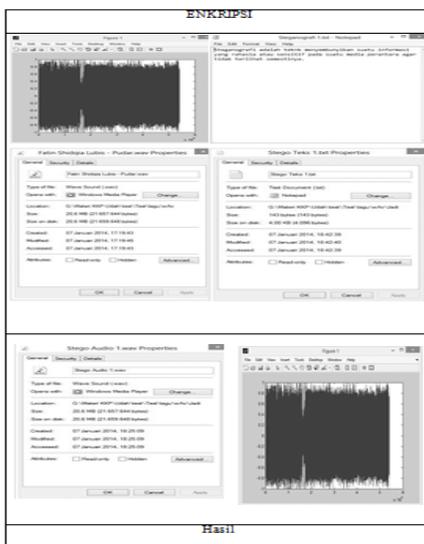


Table 2.1 Proses Penyembunyian Menggunakan Plot Gelombang

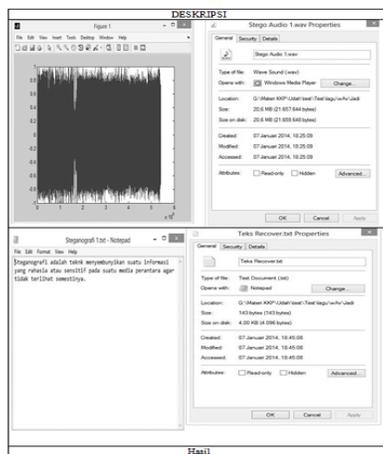


Table 2.2 Proses Pengembalian Teks

L. Spesifikasi hardware

Sistem aplikasi steganografi dibuat dengan perangkat keras dengan spesifikasi sebagai berikut :

Processor : Intel (R) Pentium (R) CPU P6100 @2.00GHz (2 CPUs), ~2.0Ghz.

Memory : 3072 MB RAM.

Adapter Video : Intel (R) HD Graphics 1275 MB

Chipset Type : Intel (R) HD Graphics (Pentium).

Display Mode : 1366 x 768 (32 Bit) (60 Hz).

Monitor : 14 Inch.

KESIMPULAN

Berdasarkan analisa yang telah diuraikan dan juga berdasarkan hasil pengamatan penulis, maka dapat diambil kesimpulan sebagai berikut:

- Sistem Algoritma Least Significant Bit pada file audio adalah dengan menyisipkan pesan tersembunyi yang disisipkan dalam file audio sehingga pesan tersebut dapat di isi dengan file rahasia sehingga keamanan data menjadi lebih baik karena file audio yang telah disisipkan tidak diketahui dengan kasat mata.
- Sistem Algoritma Least Significant Bit pada file audio Mempunyai kendala yaitu User B harus mempunyai aplikasi yang dibutuhkan untuk melihat pesan tersembunyi yang di inginkan dan file yang disisipkan hanya ber – format Txt (Teks) dan Microsoft Exxel Saja dalam file audio.
- File yang telah mengalami kompresi dengan dengan disisipi pesan menggunakan Stego Audiofile Wav sebagai cover audio tidak mengalami perubahan dan juga untuk file teks

yang di tampilkan dan disimpan kembali tidak mengalami perubahan saat mengembalikan pesan rahasia yang telah disisipkan di dalam file cover. Tetapi saat file Teks yang digunakan melebihi file cover maka program tidak dapat dijalankan dan dapat menyebabkan munculnya pesan kesalahan.

Saran

Dalam penerapan sistem penulis ingin mengemukakan saran-saran agar sistem bisa berjalan dengan baik, diantaranya:

1. Untuk memaksimalkan sistem, perlu adanya pengembangan dalam sistem menjadi lebih mudah di gunakan tidak hanya dalam bentuk format WAV saja melainkan dalam format yang lain dan sistem yang terproteksi agar kesalahan bisa diminimalisasi.
2. Dengan sistem yang lebih dikembangkan lagi dapat mempermudah pengguna dalam penyisipan informasi rahasia dan dapat membuat kenyamanan bagi pengguna.
3. Penulis menyarankan untuk pengembangan sistem, tidak hanya satu buah file saja yang dapat disembunyikan melainkan beberapa file sekaligus.

DAFTAR PUSTAKA

- [1] Maselano, K. 2009. *Pengenalan Steganografi Dengan Metode LSB (Least Significant Bit)* . Dina Ardinanti. Bandung.
- [2] Mustakini. 2009. *Definisi Sistem*.Yogjakarta.
- [3] Sutarman. 2012. *Konsep Dasar Sistem*.Bandung.
- [4] Ariyus, D. 2009. *Kemanan Multimedia*. Andi. Yogyakarta.
- [5] Alatas Putri. 2009, *Implementasi Teknik Steganografi Denganmetode LSB Pada. Citra Digital*, Tugas Akhir, Universitas Gunadarma.San Maria.2007. *Transparent Digisec-9 VPN*.Indianapolis: Rehearsal Studio. Jakarta.
- [6] Prasetyo Fahri. 2010, *Steganografi Menggunakan Metode LSB dengan Software Matlab*, Tugas Akhir, Universitas Islam Negeri Syarif Hidayatullah, Fakultas Saint Dan Teknologi.Jakarta.
- [7] Jogyanto H.M,2009. *Pengenal komputer: dasar ilmu komputer, pemrograman, sistem informasi dan intelegensi buatan.*, Andi Offset .Yogyakarta.
- [8] Donald Weiman2009 *,ASCII Conversion Chart*, Copyright © 2009.
- [9] Kriti Saroha,2010. *A Variant of LSB Steganography for Hiding Images in Audio*, International Journal of Computer ApplicationsSOITCDAC. U.P., INDIA.
- [10]Wijaya, Ermadi Satriya. 2009. *Konsep Hidden MessageMenggunakan Teknik Steganografi Dynamic Cell Spreading*, Jurnal, Universitas Islam Indonesia. Yogyakarta.
- [11]Widyanti, Hendri, 2010. *Uji Coba Paket Pembelajaran Matematika Pokok Bahasan Grafik Fungsi Trigonometri Dengan Menggunakan Matlab Di Smuk Yos Soedarso Pati*, Universitas Sanata Dharma. Yogyakarta.