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

Sugeng Santoso[1]
Arisman[2]
Windy Sentanu[3]
Alumni Universitas Budi Luhur[1], Alumni STMIK Raharja[2] ,Alumni STMIK[3]
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 penyembunyian 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 penyembunyian 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 BitModification, Wideband Angular Vibration Experiment (WAVE)Format.

PENDAHULUAN

Diseluruh dunia Internet (*Interconnection Network*) sudah berkembang menjadi salah satu media komunikasi data yang sangat popular. 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 kemamanan 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
   DalamalgoritmaSteganografi yang menggunakantekssebagai media penyisipannyabiasanyadigunakanteknik NLP (Natural Language Processing) sehinggateks yang telahdisisipipesanrahasiatidakakanmencurigakanuntuk orang yang melihatnya.
2. Audio
   Formatini pun seringdipilihkarenabiasanyaberkasdengan formatiniberukuranrelativebesar.
   Sehinggadapatmenampungpesanrahasiadalamjumlah yang besar pula.
3. Citra
   Format ini pun paling seringdigunakan, karena format inimerupakansalahsatu format file yang seringdipertukarkandalamduniainternet.
   Alasanlainnyaadalahbanyaknyatersediaalgoritmasteganografi untuk media penampung yang berupacitra.
4. Video
   Format inimemangmerupakan format denganukuranfile yang relativesangatbesarnamunjarangdigunakankarenaukurannya yang terlalubesarsehinggamengurangikepraktisannyadanjugakurangnyaalgoritma 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. Impercepbility

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

2.*Fidelity*

Mutu media penampung (coverobject) 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

Pesanatau data yang disembunyikanharustahanterhadap manipulasi yang dilakukankepadacitrapenampung, seperti pengubahankontras, penajaman, pemampatan, rotasi, perbesaran gambar, pemotongan (cropping), enkripsi, dansebagainya. Bila padacitradilakukanhalterse

but, maka data yang disembunyikan tidakrusak.

4. *Recovery*

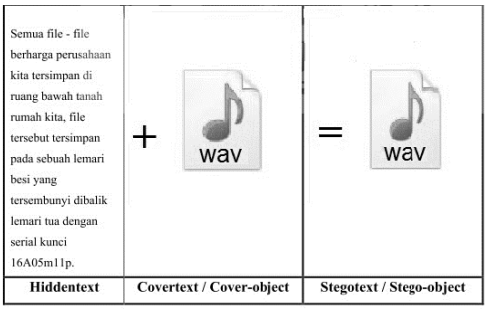
Pesan yang disembunyikan harus dapat diungkap kembali.Tuju ansteganografi adalah menyembunyikan informasi, maka sewaktu- waktu informasi yang disebunyikan ini harus dapat diambil kembali untuk dapat digunakan lebih lanjut sesuai keperluan.

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*, merupakanpesan 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, covertext dan stegotext.



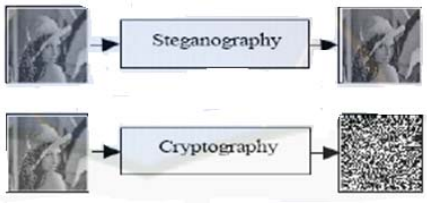
Gambar 2.1 Contoh Hiddentext, Covertext dan Stegotext.

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

D. Perbedaan Steganografi dengan Kritptografi

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)

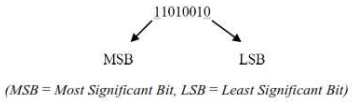


Gambar 2.2 Steganography versus Cr yptography

E. Metode LSB (*Least Significant bit*)

Least Significant Bit (LSB) adalahcara yang paling umumuntukmenyembunyikanpesan. LSB dilakukandenganmemodifikasibit-bit yang yangtermasuk bit LSB padasetiapbytewarnapadas sebuahpiksel. Bit-bit LSB iniakandimodifikasidenganmenggantikansetiap LSB yang adadengan bit-bit pesanrahasia yang ingindisembunyikan. Setelahsemua bit pesanrahasiamenggantikan bit LSB file tersebut, makapesanrahasiatelahberhasildisembunyikan.

Metodeinimembutuhkansyarat, yaitujikadilakukankompresipadafile stego, harusdigunakan format lossless compresion.Hal inidikarenakanmetodeinimenggunakan bit-bit padasetiappikselpadaimage.Jikadigunakan format lossycompresion, pesanrahasia yang disembunyikandapathilang. Contohpenggunaan LSB, sebuahsusunan bit padasebuahbyte :



(MSB = Most Significant Bit, LSB = Least Significant Bit)

Bit yang sesuaiuntukditukaradalah bit LSB karenaperubahanpadadaerahtersebuthanyaakanmenyebabkannilaibyte menjadilebihtinggi 1 angkaataulebihrendahangkadarinilaisebelumnya.

Padagambar 1, menandakanbahwa bit 1 daridepanmenyatakan bit MSB dan bit 0 daribilanganbinerterakhiradalah 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-enkoding-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 mengelompokan 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 yangberisi 'RIFF' lalu diikuti oleh 4 byte yang menyatakan ukuran dari file tersebutdan 4 byte lagi yang berisi 'WAVE' yang menyatakan bahwa file tersebut adalahfile WAV. Berikutnya adalah informasi dari format sample yang menjadi sub-bagian dari bagian RIFF lalu diikuti sub-bagian data audionya.

H. Spesifikasi Sistem

SpesifikasisystemaplikasiSteganografimeliputi input file, outputdan proses yang direncanakan.

1. Input
   Input yang dibutuhkanadalahfileteksdatar yang merupakanpesanatauinformasirahasia yang akandisisipkanpadaaudio WAV. Format fileteksmempunyaikarakter yang harusmendukung ASCII, yang dapatdibacapadasystemoperasiUnix, Mac, Ms. Windowsdan DOS dansystemoperasilainnya. Dengansedikitbentukformatan (tidakdicetaktebalatau miring), karakter yang mendukung ISO 8859-1 danjuga ANSI. Encoding yangdigunakanjugaharusmendukung UTF-8, karenaserupadengan ASCII. Input selanjutnyaadalah file audiodengan format WAV yang mendukungjenisGelombang, Amplitudo, Struktur RIFF (Resource Interchange File Format) dalam format WAV.
2. Output
   Fileaudio WAV denganfileteks yang telahdisisipkandengan proses encode, yang disebutstegoaudio. Kemudianpesanteks yang telahdisisipkan, dapatdibacakembalidenganlengkapsesuaifileteksawaldengan proses decode.
3. Proses Yang Direncanakan
   DidalamsystemaplikasiSteganografi, masukanfileawaladalahfileteksdatardenganukuran yang cukupkecil, fileteksdatar yang mendukungkarakter ASCII danakandikonversikanmenjadibilanganbiner, kemudianfilebinarytersebutsatu per satuakandisisipkanpadafilebinaryaudio WAV , yang nantinyamenjadistegoaudio. Langkah-langkah proses yang direncanakan:

   Proses encode yang meliputitahapansebagaiberikut :
   a. Menginputkanfileteks.
   b. Menginputkanfileaudio.
   c. Melakukanpenyisipan.
   d. Penyimpanan file audiostego.

   Proses decode yang meliputitahapansebagaiberikut :

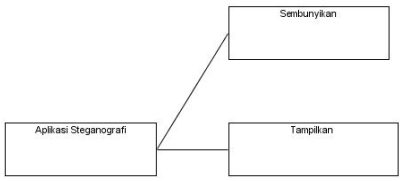
   - Memanggil file stegoaudio.
   - MenampilkanpesanTeks.
   - Menyimpanfileteks.
   - Memutarfile audio.

I. Parameter kesuksesan
SistemaplikasiSteganografidapatdikatakanberhasiljikasystemmemiliki parameter dibawahini :
1. Fileteksdengankarakter ASCII.
2. Fileaudio WAV yang mendukung format Gelombang, Amplitudo, Struktur RIFF.
3. Melakukan proses encode.
4. Melakukan proses decode.
5. Pesanpadastegoaudiodapatditampilkankembali.
6. Fileaudiodapatdiputar.

J. Interface pembuatan sistem
Perancangantampilan menu danfiturpadasystemaplikasiSteganografimeliputiperancangantampilan menu utama , tampilanuntuk proses encodedantampilanuntuk proses decode. Perancangansistem interface menggunakan tool pengembangdariMathWorks, yaituMatlab R2010b.

1. Struktur Menu

Struktur menu yang adapada program aplikasidirancangsebagaiberikut.



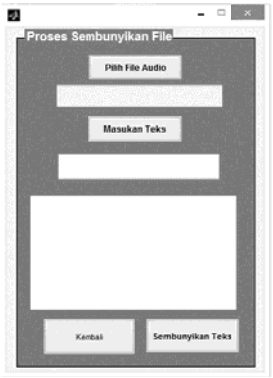
Gambar 2.3Struktur menu

2. Rancangan layar

a. RancanganLayarUtama

*Gambar2.4 RancanganLayarUtamaPadagambar 3.8menggambarkanperancangantampilanl ayarutama*systemSteganografi yang terdiridariduabagian : bagiantampilan menu proses Sembunyikan yang terdiridari form teks yang berfungsimenginput file teks , menginputkan kata sandidantombolbuka 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.

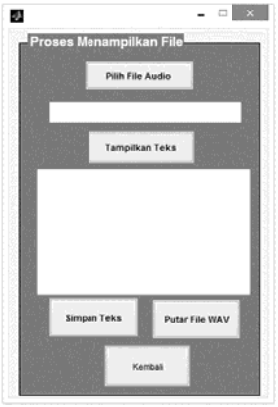
b. RancanganLayarSembunyikan



Gambar2.5 RancanganLayarSembunyikan

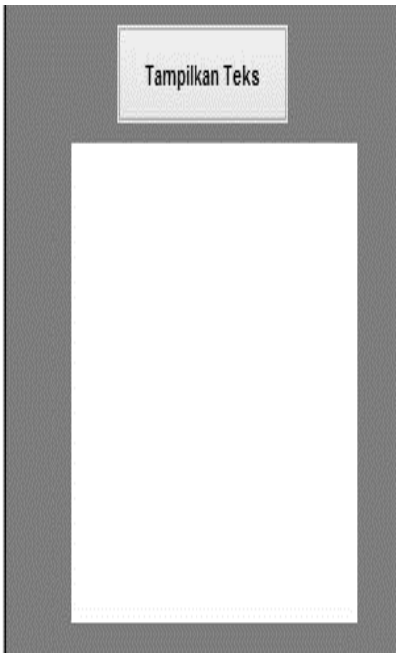
Padagambar 2.5 menampilkanperancangan proses penginputanteks, fileAudio, proses encode, danSembunyikanTeks.

c.RancanganLayarTampilkan



Gambar 2.6 RancanganLayarTampilkan

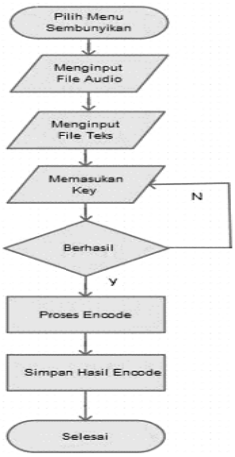
Perancangan tampilanuntuk melihat pesan teks rahasia yang disembunyikan pada file stego audio dapat dilihat pada gambar 2.6.



Gambar 2.7 Rancangan Layar Pesan

3. Flowchart
   Flowchart merupakangambarataubagan yang memperlihatkanurutandanhubunganantar proses besertainstruksinya. Gambaraninidinyatakandengan simbol. Dengandemikiansetiapsymbol menggambarkan proses tertentu. Sedangkanhubunganantar proses digambarkandengangarispenghubung.
   Perancangan proses pada system Enkripsi meliputi pembuatan flowchart dari proses encode dan proses decode.Didalam perancangan proses encode dan proses decode akan digambarkan pada gambar dibawah ini:

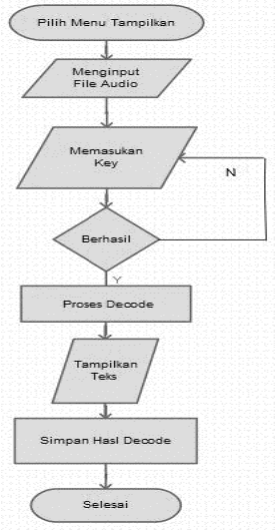
a. Flowchart Enkripsi pada steganografi



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 decodepadasystem Enkripsi danmelihathasilakhirdari proses tersebutyaitumenampilkanpesan yang disembunyikanpada File audio.

K. Pengujian steganografi

Pengujiansystemsteganografimeliputi pengujian, pengujiansystempadaCover Audio , pengujiansystempadaAudio yang dijadikancover.

1. PengujianDenganCover Audio

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

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

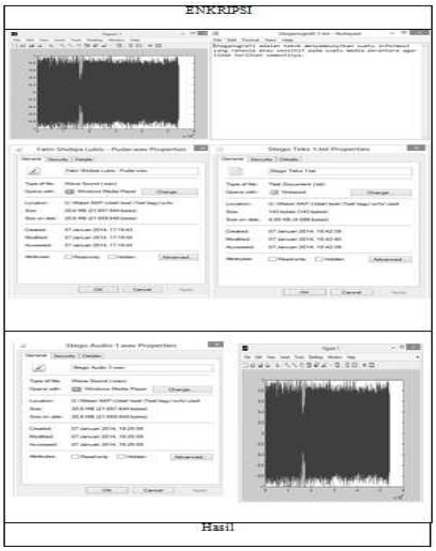


Table 2.1 Proses Penyembunyian Menggunakan Plot Gelombang

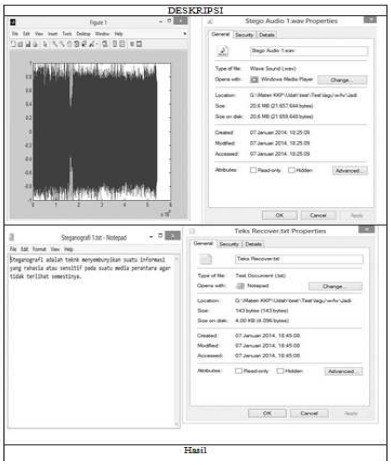


Table 2.2 Proses Pengembalian Teks

L. Spesifikasi hardware

Sistemaplikasisteganografidibuat denganperangkatkerasdenganspesifikasisebagaiberikut :

Processesor : 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:

1. 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.
2. 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.
3. 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 Negri Syarif Hidayatullah, Fakultas Saint Dan Teknologi.Jakarta.

[7] Jogiyanto H.M,2009. Pengenal komputer: dasar ilmu komputer, pemrogaman, 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.