

Perancangan Perangkat Lunak Steganografi Audio MP3 Menggunakan Metode *Least Significant Bit* (LSB) Dengan *Visual Basic 6.0*

¹Aminah Rizki Lubis, ²Maya Silvi Lidya, B.Sc.M.Sc, ²M. Andri Budiman, S.T.,M.Comp.Sc.M.E.M

¹Program Studi S1 Teknologi Informasi
Fakultas Ilmu Komputer dan Teknologi Informasi
Universitas Sumatera Utara

E-mail: aminahrizki@gmail.com, maya2@usu.ac.id, mandrib@gmail.com

Abstrak— Begitu banyak tindak kejahatan di dunia maya yang dilakukan oleh manusia-manusia tidak bertanggung jawab. Tindakan ini banyak merugikan pihak dari kalangan masyarakat, walaupun tidak sedikit orang yang turut menikmati keuntungan dari tindakan ini. Sebut saja, seperti maraknya pornografi, pembajakan hak cipta, tindakan kriminal di dunia maya, dan lain sebagainya. Hal ini membuat keamanan di dunia maya tidak aman. Untuk itu perlu adanya pengamanan di dunia maya. Steganografi merupakan ilmu dan seni menyembunyikan data pada suatu media. Adapun wadah yang dijadikan tempat untuk menyembunyikan data tersebut berupa *file audio mp3*. *File audio mp3* sangat populer di kalangan masyarakat. Oleh karena itu, dalam tugas akhir ini penulis merancang perangkat lunak *steganografi audio mp3* menggunakan metode LSB yaitu dengan mengubah bit yang kurang *significant* pada data yang terdapat dalam *audio mp3*. Perancangan perangkat lunak ini dapat menyisipkan pesan ke dalam *audio mp3* dan pesan tersebut dapat diamankan sedemikian mestinya.

Kata Kunci— Steganografi, *file audio MP3*, LSB

I. PENDAHULUAN

Saat ini, peradaban zaman semakin hari semakin berkembang begitu pesatnya. Setiap hari, begitu banyak berita mengenai perkembangan zaman terutama di bidang teknologi. Mulai dari munculnya berbagai inovasi perangkat teknologi terbaru *software* dan *hardware* yang begitu canggih. Hal ini membuat setiap orang berlomba-lomba untuk mengikuti perkembangan teknologi tersebut. Adapun dampak positif dan dampak negatif dari berkembangnya teknologi saat ini, yaitu dengan semakin canggihnya teknologi, maka dapat memudahkan seseorang untuk berinteraksi kepada rekan-rekannya dimanapun seseorang tersebut berada, memudahkan pekerjaan sehingga lebih efektif dan efisien, serta menambah pengetahuan seseorang menjadi semakin luas dengan berkembangnya teknologi. Bukan hanya dampak positif saja, adapun dampak negatif dengan berkembangnya teknologi, yaitu dapat dipastikan, semakin berkembangnya teknologi maka semakin berkembang pula kejahatan di dunia teknologi. Contohnya seperti, semakin maraknya situs yang tidak layak untuk dilihat oleh anak-anak, remaja bahkan orang dewasa sekalipun, transaksi perdagangan yang *illegal* seperti obat-

obatan terlarang pun juga ikut ambil bagian dalam kejahatan dunia teknologi, serta karya cipta dari pelaku hiburan yang bukan hak milik orang lain mudah sekali untuk diakses.

Berbicara soal pengamanan, banyak ilmu tentang keamanan informasi yang dapat diaplikasikan dalam kehidupan ini. Salah satunya adalah ilmu Steganografi. Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan tersebut tidak dapat diketahui. Steganografi berasal dari bahasa Yunani, yaitu “*steganos*” yang artinya tulisan tersembunyi “(*covered writing*)” [1].

Steganografi memerlukan dua properti, yaitu : wadah penampung sebagai tempat penyembunyian informasi dan data rahasia yang akan disembunyikan. Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya suara (*audio*), citra (*image*), teks (*txt*), dan *video*. Data rahasia yang disembunyikan juga dapat berupa suara (*audio*), citra (*image*), teks (*txt*), dan *video*. Jika pada kriptografi, data yang telah disandikan (*ciphertext*) tetap tersedia, maka pada steganografi, *ciphertext* dapat disembunyikan sehingga pihak ketiga tidak mengetahui keberadaannya .

Saat ini, *file audio* yang sangat populer di kalangan masyarakat adalah file berformat mp3. *File mp3* adalah salah satu *file audio* yang banyak digunakan pada berbagai alat pemutar musik sampai ke telepon selular (ponsel). *File mp3* memiliki ukuran yang kecil tetapi kualitasnya setara dengan kualitas musik CD (*compact disc*) sehingga dapat dengan mudah ditransmisikan maupun disimpan pada *media store*. Terbukti dengan mp3, masyarakat lebih mudah mengakses *file* ini di dunia teknologi yang dampaknya mengancam para pelaku hiburan, karena karyanya diambil secara gratis.

Metode yang digunakan dalam merancang perangkat lunak ini adalah metode *Least Significant Bit* (LSB). Prinsip dasar metode ini adalah dengan mengganti bit terakhir dari data *sample audio mp3* dengan *bit-bit* penyisip. Untuk melakukan penyisipan pesan ke dalam *audio*, maka *audio* dan pesan penyisip harus diubah menjadi biner.

Berdasarkan hal yang telah diuraikan di atas maka penulis ingin menganalisis dan merancang perangkat lunak steganografi *audio mp3* menggunakan metode LSB.

II. IDENTIFIKASI MASALAH

Saat ini begitu banyak kejadian-kejadian di dunia maya yang merajalela, untuk itu perlu dibuat suatu sistem pengamanan untuk mencegah hal-hal yang tidak diinginkan. Maka dibuatlah suatu perancangan perangkat lunak yang dapat memroses steganografi menggunakan LSB ke dalam *file audio* mp3. Setelah itu kita dapat melihat perbandingan melalui ukuran *file audio* sebelum disisipi pesan maupun sesudah.

Pada sistem pengamanan data, steganografi merupakan ilmu pengamanan data yang baik yang dapat memroses penyisipan pesan menggunakan *Least Significant Bit* (LSB) dan dari penyisipan pesan ke dalam *audio* inilah dapat dilihat perbandingan ukuran *file audio* sebelum dan sesudah penyisipan.

Tujuan dari penulisan penelitian ini adalah untuk memberikan pemahaman mengenai steganografi melalui media mp3.

III. PENELITIAN TERDAHULU

Pada penelitian Yusrian Roman Arubusman (2007), Teknik Informatika, Universitas Gunadarma, metode yang digunakan adalah penggunaan *audio* mp3 sebagai data masukan pembawa pesan rahasia. Dengan membagi media gambar data masukan dalam *frame*, teknik ini diharapkan dapat menyisipkan informasi rahasia ke dalam satu *frame maximum* sebanyak 1 bit sehingga perubahan yang terjadi tidak terlihat mencolok. Begitupun dengan metode yang diajukan penggunaan media audio mp3 sebagai data masukan media pembawa pesan rahasia. Dengan membagi media gambar data masukan dalam *frame*, teknik ini diharapkan dapat menyisipkan informasi rahasia ke dalam satu *frame maximum* sebanyak 1 bit sehingga perubahan yang terjadi tidak terlihat mencolok[2].

Metode proyek akhir ini membuktikan suatu teknik penyembunyian pesan rahasia dalam media *audio*. Hasil *file* keluaran yang dihasilkan oleh proyek akhir ini mengalami perubahan yang rendah, hal ini dibuktikan melalui besar rata-rata nilai *Signal-to Noise Ratio* sebesar 99.5 % yang artinya bahwa hanya terjadi kerusakan *audio* sebesar 0.5 % dalam setiap *file* hasil keluaran yang dibandingkan dengan *file* asli yang menjadi masukannya.

IV. METODE PENELITIAN

A. *Steganografi*

Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui. Steganografi berasal dari bahasa Yunani, yaitu "*steganos*" yang artinya tulisan tersembunyi ("*covered writing*"). Steganografi sangat kontras dengan kriptografi. Jika kriptografi merahasiakan makna pesan sementara eksistensi pesan tetap ada, maka steganografi menutupi keberadaan pesan. Steganografi dapat dipandang sebagai kelanjutan kriptografi dan dalam prakteknya pesan rahasia dienkripsi terlebih dahulu, kemudian cipherteks

disembunyikan di dalam media lain sehingga pihak ketiga tidak menyadari keberadaannya. Pesan rahasia yang disembunyikan dapat diekstraksi kembali persis sama seperti aslinya [1].

Steganografi bukan hal yang baru dan sudah dikenal sejak zaman Romawi dan Yunani kuno. Misalnya, pesan ditulis di kepala budak lalu menunggu sampai tumbuh cukup rambut untuk menutupi pesan tersebut sebelum ia dikirim kepada orang yang dituju dimana rambutnya akan dicukur sehingga pesan itu terlihat.

B. *Istilah-istilah dalam Steganografi*

1. *Embedding Data*

Data *embedded* yang tersembunyi dalam suatu media *audio digital* membutuhkan dua *file*. Pertama adalah media *audio digital* asli yang belum dimodifikasi yang akan menangani informasi tersembunyi, yang disebut *cover audio*. *File* kedua adalah informasi pesan yang disembunyikan. Suatu pesan dapat berupa teks, baik itu plaintexts, cipherteks, gambar, atau apapun yang dapat ditempelkan ke dalam *bit-stream*. Ketika dikombinasikan, *cover audio* dan pesan yang ditempelkan membuat *stego-audio*. Suatu *stego-key* (suatu password khusus) juga dapat digunakan secara tersembunyi, pada saat *decode* selanjutnya dari pesan [1].

2. *Coverttext* atau *cover-object*

Pesan yang digunakan untuk menyembunyikan *embedded message*.

3. *Stegotext* atau *stego-object*

Pesan yang sudah berisi *embedded message*.

4. *Encoding Data*

Encoding adalah proses menempatkan urutan karakter tertentu (huruf, angka, tanda baca, dan simbol tertentu) ke dalam format khusus untuk transmisi yang efisien atau penyimpanan. Sebuah *encoder* mengambil data yang masuk bersamaan dengan beberapa metadata (seperti *signal* yang mengindikasikan apakah data mewakili data yang sesungguhnya atau *control character*) dan menghasilkan sebuah nilai yang sudah ter-*encode*.

5. *Decoding Data*

Decoding adalah proses yang berlawanan, konversi dari format yang disandikan kembali ke urutan asli dari karakter. *Encoding* dan *decoding* digunakan dalam komunikasi data, jaringan dan penyimpanan. Istilah *encoding* dan *decoding* sering digunakan dalam referensi untuk proses analog ke *digital* konversi dan *digital* ke analog konversi. Dalam pengertian ini dapat diterapkan pada segala bentuk data, termasuk teks, gambar, *audio*, *video*, multimedia, dan lain-lain.

C. *Manfaat Steganografi*

Teori Steganografi dapat diimplementasi pada media *audio digital*. Namun saat ini, teknik penyembunyian pesan di dalam media *audio* dirasa masih kurang efektif dibandingkan dengan penyembunyian pesan dalam media teks maupun citra. Hal ini

disebabkan pendengaran manusia jauh lebih sensitif dibandingkan penglihatannya. Jika mata manusia bisa dikelabui oleh perubahan warna yang kecil, telinga manusia belum tentu dapat tertipu oleh perubahan suara walaupun sedikit. Karena alasan inilah penyisipan pesan melalui media *audio* cukup jarang dipilih. Padahal, *audio* merupakan media file yang memiliki banyak kelebihan, misalnya dapat menyimpan banyak *byte* tanpa membuat ukuran bertambah terlalu besar, serta dapat di-*generate* dengan cepat dan mudah sehingga tidak perlu menyimpan file asli di media penyimpanan. Ketika berurusan dengan transmisi sinyal *audio*, ada dua hal utama yang harus diperhatikan, yaitu bentuk representasi *audio* digital dan media transmisi yang digunakan.

D. Metode LSB (Least Significant Bit)

Untuk menjelaskan metode ini, digunakan *audio digital* sebagai *cover audio*. Pada setiap *byte* terdapat bit yang paling kurang berarti (*Least Significant Bit* atau *LSB*). Misalnya pada *byte* 00011001, maka bit *LSB*-nya adalah 1. Untuk melakukan penyisipan pesan, bit yang paling cocok untuk diganti dengan bit pesan adalah bit *LSB*, sebab pengubahan bit tersebut hanya akan mengubah nilai *byte*-nya menjadi satu lebih tinggi atau satu lebih rendah. Metode *LSB* memanfaatkan keterbatasan *visual* pada indera mata manusia yang kurang peka terhadap sedikit perubahan warna. Cara yang digunakan adalah menggantikan bit paling tidak *significant*.

E. Steganografi Pada Media Audio

Steganografi dapat diimplementasi pada media *audio digital*. Namun saat ini, teknik penyembunyian pesan di dalam media *audio* dirasa masih kurang efektif dibandingkan dengan penyembunyian pesan dalam media teks maupun citra. Hal ini disebabkan pendengaran manusia jauh lebih sensitif dibandingkan penglihatannya. Jika mata manusia bisa dikelabui oleh perubahan warna yang kecil, telinga manusia belum tentu dapat tertipu oleh perubahan suara walaupun sedikit. Karena alasan inilah penyisipan pesan melalui media *audio* cukup jarang dipilih. Padahal, *audio* merupakan media file yang memiliki banyak kelebihan, misalnya dapat menyimpan banyak *byte* tanpa membuat ukuran bertambah terlalu besar, serta dapat di-*generate* dengan cepat dan mudah sehingga tidak perlu menyimpan file asli di media penyimpanan.

Ketika berurusan dengan transmisi sinyal *audio*, ada dua hal utama yang harus diperhatikan, yaitu bentuk representasi *audio digital* dan media transmisi yang digunakan. Secara umum, file *audio* digital memiliki dua karakteristik utama, yaitu *sample quantization method* (metode kuantisasi) dan temporal *sampling rate*. Metode kuantisasi menyatakan representasi sampel *audio* berdasarkan kualitas digitalnya, misalnya format *WAV* (*Windows Audio Visual*) dan format *AIFF*. Temporal *sampling rate* yaitu kecepatan yang dapat dihitung untuk melakukan *sampling* (pengambilan sampel) *audio* secara periodik.

Media transmisi sinyal *audio* adalah lingkungan yang dilalui sinyal *audio* untuk berpindah dari satu tempat ke

tempat lain, misalnya dari *encoder to decoder*. Ada empat media transmisi yang umum digunakan, yaitu sebagai berikut :

1. *Digital end-to-end environment*
Perpindahan sinyal *audio* secara langsung dari mesin ke mesin. Sinyal hasil perpindahan akan sama antara sumber dengan tujuan.
2. *Increased/decreased resampling environment*
Perpindahan sinyal digital disertai perubahan *sampling rate*, namun tetap dalam representasi digital.
3. *Analog transmission and resampling*
Perpindahan sinyal digital dengan sebelumnya diubah ke dalam representasi analog dan dilakukan *resampling*.
4. *Over the air environment*
Perpindahan sinyal *audio* melalui udara, dengan cara memainkan sinyal *audio* tadi dan ditangkap oleh mikrofon.

Ada tiga metode yang sering digunakan untuk melakukan penyisipan data dalam media *audio*, yaitu *low bit encoding*, *spread spectrum*, serta *echo data hiding* [3].

F. Kriteria-Kriteria Penyembunyian Pesan

Beberapa kriteria yang harus diperhatikan dalam penyembunyian pesan adalah [1] :

1. *Imperceptibility*

Keberadaan pesan rahasia tidak dapat dipersepsi oleh inderawi. Misalnya, jika *coverttext* berupa citra, maka penyisipan pesan membuat citra *stegotext* sukar dibedakan oleh mata dengan citra *coverttext*-nya. Jika *coverttext* berupa *audio* (misalnya berkas *mp3*, *wav*, *midi*, dan sebagainya), maka indera telinga tidak dapat mendeteksi perubahan pada *audio stegotext*-nya.

2. *Fidelity*

Mutu media penampung tidak berubah banyak akibat penyisipan. Perubahan tersebut tidak dapat dipersepsi oleh inderawi. Misalnya jika *coverttext* berupa citra, maka penyisipan pesan membuat *stego-text* sukar dibedakan oleh mata dengan citra *coverttext*-nya. Jika *coverttext* berupa *audio* (misalnya berkas *mp3*, *wav*, *midi*, dan sebagainya), maka *audio stegotext* tidak rusak dan indera telinga tidak dapat mendeteksi perubahan tersebut.

3. *Recovery*

Pesan yang disembunyikan harus dapat diungkapkan kembali (*reveal*). Karena tujuan steganografi *data hiding*, maka sewaktu-waktu pesan rahasia di dalam *stego-text* harus dapat diambil kembali untuk digunakan lebih lanjut.

G. File MP3

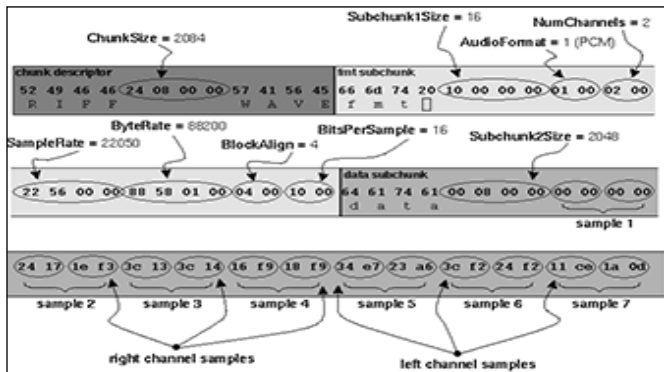
MPEG (*Moving Picture Expert Group*)-1 *audio* layer III atau yang lebih dikenal dengan *mp3*, adalah salah satu dari pengkodean dalam *digital audio* dan juga merupakan format kompresi *audio* yang memiliki sifat "menghilangkan". Istilah menghilangkan yang dimaksud adalah kompresi *audio* ke dalam format *mp3* menghilangkan aspek-aspek yang tidak signifikan pada pendengaran manusia untuk mengurangi besarnya file *audio*.

Sejarah MP3 dimulai dari tahun 1991 saat proposal dari Phillips (Belanda), CCET (Perancis), dan Institut für Rundfunktechnik (Jerman) memenangkan proyek untuk DAB (*Digital Audio Broadcast*). Produk mereka seperti Musicam (akan lebih dikenal dengan layer 2) terpilih karena kesederhanaan, ketahanan terhadap kesalahan, dan perhitungan komputasi yang sederhana untuk melakukan pengkodean yang menghasilkan keluaran yang memiliki kualitas tinggi. Pada akhirnya ide dan teknologi yang digunakan dikembangkan menjadi MPEG-1 *audio layer 3*.

Kepopuleran dari mp3 yang sampai saat ini belum tersaingi disebabkan oleh beberapa hal. Pertama mp3 dapat didistribusikan dengan mudah dan hampir tanpa biaya, walaupun sebenarnya hak paten dari mp3 telah dimiliki dan penyebaran mp3 seharusnya dikenai biaya. Pada perbandingan kualitas suara antara beberapa format kompresi *audio* hasil yang dihasilkan bervariasi pada *bitrate* yang berbeda, perbandingan berdasarkan *codec* (hasil pengkodean) yang digunakan. Pada 128 kbit/s, LAME mp3 unggul sedikit dibandingkan dengan *Ogg Vorbis*, AAC, MPC and WMA Pro. Kemudian pada 64 kbit/s, AAC-HE dan mp3 pro menjadi yang teratas diantara *codec* lainnya. Dan untuk diatas 128 kbit/s tidak terdengar perbedaan yang signifikan. Pada umumnya format mp3 sekarang menggunakan 128 kbit/s dan 192 kbit/s sehingga hasil yang dihasilkan cukup baik [4].

H. Struktur Data pada File Audio

Struktur data pada *file audio* berbeda-beda tergantung format *audio*-nya. Misalnya *file Wav* memiliki struktur seperti pada Gambar berikut.



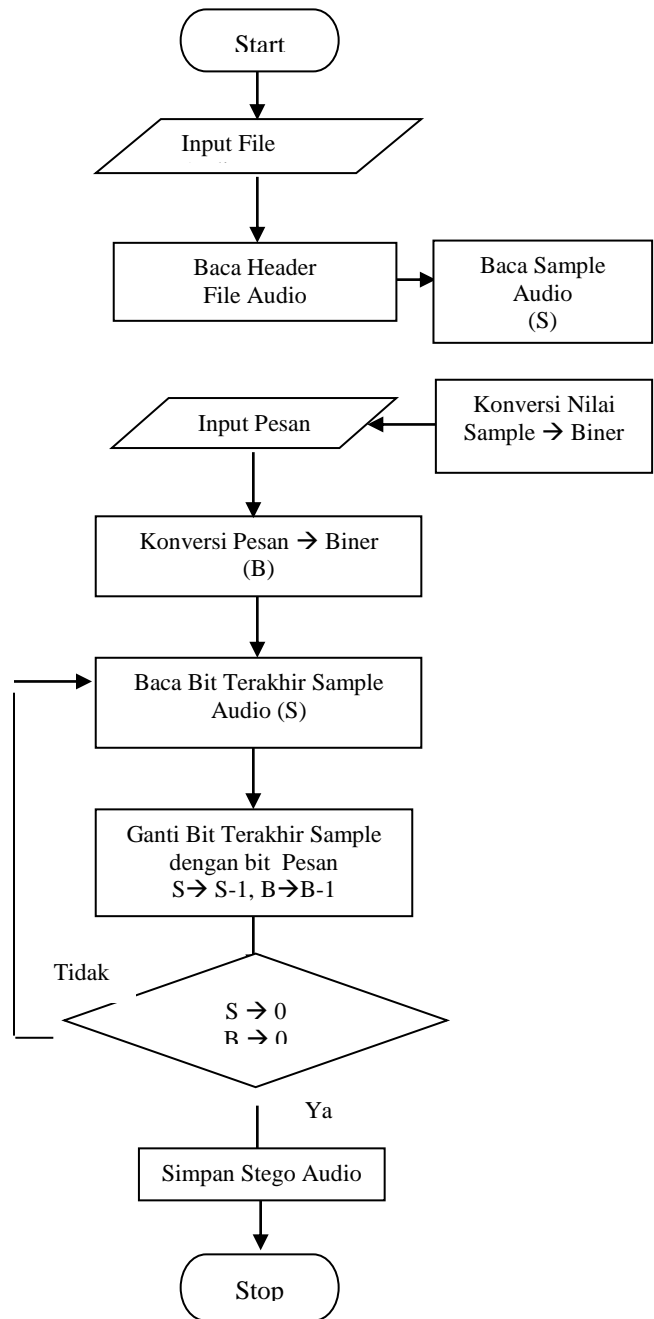
Gambar 1. Contoh Struktur file WAV dalam bentuk hexa [4]

Pada struktur *file Wav* di atas terdiri dari:

1. *Chunk Descriptor* yang terdiri dari data: 52 49 46 46 28 08 00 00 57 41 56 45.
2. *Fmt subChunk* yang terdiri data *subChunk1size*, *audioFormat*, *numChannel*, *sampleRate*, *byteRate* dan *BlockAlign* yaitu: 66 6d 74 20 10 00 00 00 01 00 02 00 22 56 00 00 ## 50 01 00 04 00 10 00
3. *Data subChunk* yang terdiri dari data *subChunk2size* serta *sample-sample* yaitu: 64 61 74 61 00 00 00 00 00 00 00 00 00 00 00 00 24 17 1e f3#3 3c 13 3c 14 #4 16 f9 18 f9 34 e7 23 a6 3c f2 24 f2 11 ce 1a 0d

I. Perancangan Flowchart Sistem

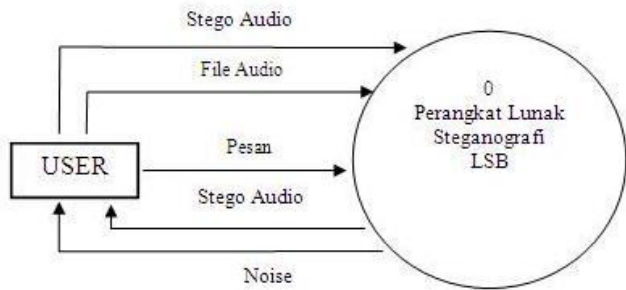
Untuk mempermudah proses perancangan sistem untuk implementasi algoritma LSB, perlu didefinisikan langkah-langkah yang dibuat kedalam *flowchart*.



Gambar 4. Flowchart Sistem

J. Diagram Konteks Sistem

Pada diagram konteks di bawah ini terlihat ada satu entiti luar (*external entity*) yang terdapat pada perangkat lunak yang dibangun yaitu *User*. *User* adalah sebagai pengguna sistem yaitu pemberi masukan berupa data *file audio* dan pesan teks. Setelah proses penyisipan, *User* memperoleh *stego audio*. Diagram Konteks dapat dilihat seperti pada gambar berikut.

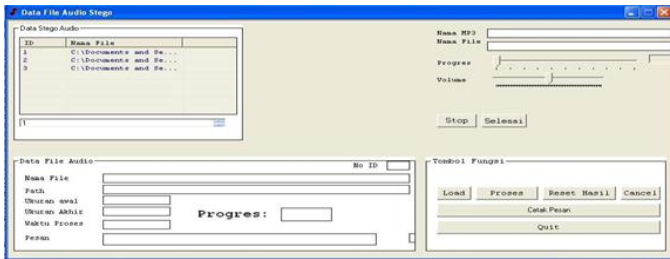


Gambar 5. Diagram Konteks

V. PEMBAHASAN

A. Tampilan Awal

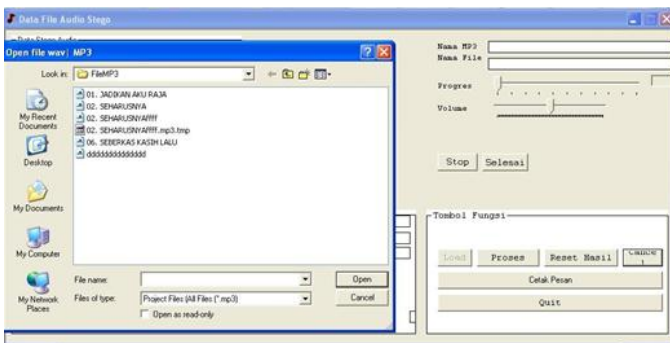
Tampilan ini berisi data stego audio, data file audio, tombol fungsi, dll. Pada tampilan ini juga terdapat tampilan mp3 yang akan didengarkan, tampilan ini akan muncul ketika proses load mp3 selesai, lalu dimainkanlah mp3 tersebut.



Gambar 6. Tampilan Awal

B. Tampilan Load

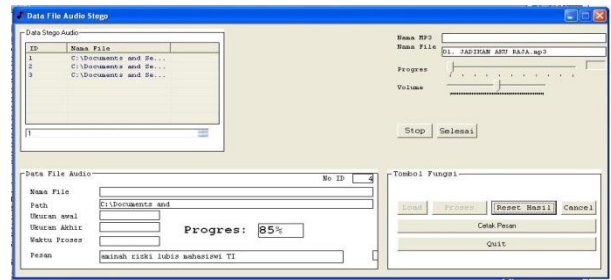
Tampilan Load merupakan tampilan berguna untuk melakukan proses pengambilan mp3 atau file audio.



Gambar 7. Tampilan Load

C. Penyisipan Pesan

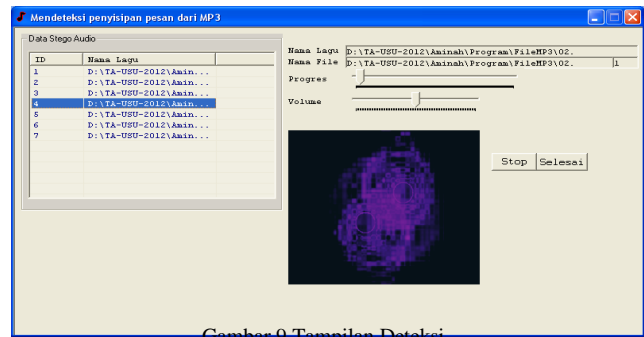
Setelah pemilihan file mp3, dilanjutkan dengan pemasukan data pesan penyisip. Selanjutnya pilih tombol Proses untuk melakukan proses perhitungan nilai sample audio untuk mendapatkan ukuran awal maupun ukuran akhir dari file mp3 sebelum disisipi dan sesudah disisipi pesan



Gambar 8. Penyisipan Pesan

D. Tampilan Deteksi

Tampilan Deteksi merupakan tampilan berguna untuk melakukan proses deteksi noise akibat penyisipan pesan ke dalam file audio MP3. Setelah pemilihan, maka nama mp3 serta nama alamat penyimpanan akan ditampilkan pada layar serta dilakukan pemutaran file mp3 oleh media player.



Gambar 9. Tampilan Deteksi

E. Tampilan Pengujian Sistem

Hasil pengujian sistem steganografi file audio dengan algoritma LSB berfungsi untuk menampilkan hasil proses penyisipan pesan.

ID	NAMA FILE	UKURAN AWAL(kb)	UKURAN	PENYISIP
1	01. JADIKAN AKU RAJA.mp3	3,849,752.00	3,860,271.00	ami
2	01. JADIKAN AKU RAJA.mp3	3,849,752.00	3,860,271.00	ami
3	02. SEHARUSNY A.mp3	4,898,005.00	4,906,422.00	lubis
4	01. JADIKAN AKU RAJA.mp3	3,849,752.00	3,860,271.00	ami

Tabel 1. Pengujian Sistem

VI. KESIMPULAN DAN SARAN

Dari simulasi yang dilakukan, dapat disimpulkan bahwa dengan menggunakan algoritma LSB, pesan dapat dibinerkan. Penelitian ini menggunakan bahasa pemrograman Visual Basic 6.0 algoritma LSB dapat diimplementasikan dengan menggunakan fungsi-fungsi khusus yang tersedia di dalamnya.

Meskipun tampilan program sederhana, tetapi program dapat bekerja cukup baik.

Penulis menyadari bahwa masih terdapat beberapa kekurangan dalam perangkat lunak ini. Untuk itu melalui bagian ini penulis hendak memberikan saran bagi pengembangan dan penyempurnaan selanjutnya. Salah satu kekurangan perangkat lunak ini adalah penyisipan pesan hanya bisa menggunakan format teks, perangkat lunak ini tidak dapat menyisipkan pesan berupa gambar maupun suara. Oleh karena itu, pada masa yang akan datang diharapkan pengembangan perangkat lunak ini dapat lebih berkembang lagi. Demikian saran yang dapat diajukan oleh penulis, semoga perangkat lunak ini dapat dikembangkan menjadi lebih baik dan lebih bermanfaat dimasa mendatang.

VII. DAFTAR PUSTAKA

- [1] Munir, R.2006. Kriptografi. Bandung: Informatika.
- [2] Arubusman, YR, 2007, "Audio Steganografi", Jakarta.
- [3] Cvejic, N. 2004. *Algorithms for Audio Watermarking and Steganography*. University of Oulu.W.K.Chen, Linear Networks and Systems (Book Style). Belmont, CA: Wadsworth, 1993, pp. 123-135.
- [4] Binanto, I. 2010. *Multimedia Digital, Dasar Teori + Pengembangan*, Yogyakarta: Andi.