APLIKASI AUDIO STEGANOGRAFI UNTUK MELINDUNGI DATA MENGGUNAKAN BAHASA PEMROGRAMAN JAVA

Ibnu Rachman Chalid

Jurusan Teknik Informatika

Fakultas Teknologi Industri

Universitas Gunadarma

8 Agustus 2009

ABSTRAKSI

Dalam hal perlindungan data dan proteksi, banyak orang mengirim file satu terhadap yang lainnya, dan ada beberapa kasus agar pesan tersebut tidak dapat diketahui atau dibaca bahkan dipecahkan oleh orang yang tidak berhak. Maka dari itu perlu dibangun suatu aplikasi Audio steganografi yang memanfaatkan media file audio untuk menyisipkan pesan / file rahasia agar terselubung dan tidak diketahui oleh orang lain.

Aplikasi ini menggunakan metode LSB dengan memodifikasi bit-bit yang tergolong bit LSB pada setiap byte pada sebuah berkas. Tahapan pembuatan aplikasi yang dilakukan adalah perancangan aplikasi, pembuatan rancangan diagram, pembuatan aplikasi dan uji coba dan analisa program. Perkakas (tools) yang digunakan adalah bahasa pemrograman Java yaitu Java 2 System Development Kit (J2SDK) versi 1.5.0 dan perangkat lunak Eclipse SDK 3.0 untuk mengimplementasikan koding program.

Tahap pengujian yang dilakukan pada penulisan ini ada 2 yaitu tahap embedding dan tahap retrieving. Tahap embedding merupakan pengujian yang dilakukan dalam lingkup proses penyisipan data berupa teks atau file sedangkan tahap retrieving pengujian yang dilakukan dalam lingkup proses pengembalian data. Program aplikasi steganografi ini mampu membaca file audio dengan tipe format mp3 dan au serta dapat menyembunyikan pesan rahasia ke dalam media audio dengan berupa gambar, teks, video, dokumen. Aplikasi ini dibuat agar dapat dikembangkan lagi. Dikarenakan aplikasi ini masih belum sempurna dan masih terdapat kekurangan-kekurangan yaitu salah satunya adalah semakin besar file atau pesan yang disisipkan berbanding lurus dengan hasil output pada file dalam tahap *embedding*.

Kata Kunci : Audio Steganografi , *Least Significant Bit (*LSB), *Embedding, Retrieving*

1. Pendahuluan

1.1 Latar Belakang

Seringkali seseorang yang hendak mengirim pesan kepada orang lain, tidak ingin isi pesan tersebut diketahui oleh orang lain. Biasanya isi pesan tersebut bersifat sangat rahasia atau pribadi, yang hanya boleh diketahui antara pihak pengirim dan pihak penerima pesan, atau kalangan

terbatas saja. Oleh karena itu, biasanya pengirim tersebut mengirim pesan secara sembunyi-sembunyi agar tidak ada pihak lain yang mengetahui. Walaupun seringkali dilakukan dengan sembunyi-sembunyi tetapi tetap saja pesan tersebut dapat diketahui oleh orang lain ataupun karena mungkin adanya suatu hambatan atau masalah seperti misalnya media pesannya berupa kertas dan kertas tersebut jatuh di jalan atau rusak terkena air.

Hal-hal seperti itu membuat orang yang mengirim pesan rahasia tersebut semakin lama semakin malas atau lelah untuk melakukannya dan menginginkan sesuatu yang lebih aman dan mudah untuk mengirim pesan tersebut. Salah satu hal yang dapat dilakukan untuk mengatasi situasi di atas adalah mengembangkan suatu aplikasi yang mampu menyamarkan pesan tersebut pada suatu media yang dapat diakses oleh setiap orang. Teknik ini disebut steganografi, setiap orang bisa menampilkan atau membuka media tersebut, namun tidak menyadari bahwa media tersebut telah dibubuhkan pesan rahasia oleh pengirim.

Dengan berkembangnya dunia multimedia, maka steganografi modern menggunakan *file-file* multimedia ini sebagai kedok untuk menyembunyikan pesan, teknik ini dikenal dengan sebutan *digital watermarking*. Lalu lintas *file-file* multimedia di internet sudah lumrah sehingga akan mengurangi kecurigaan akan adanya pesan rahasia.

Salah satu jenis *file* multimedia yang populer adalah *file* dengan format mp3. Semenjak 6-7 tahun terakhir, *file* audio dengan format ini menjadi yang terpopuler hingga sekarang. Walaupun jenis kompresi yang lainnya beberapa memiliki kualitas yang lebih baik, namun sifat kosmopolit dari mp3 belum dapat tersaingi hingga saat ini.

Maka dari itu penggunaan mp3 sebagai salah satu media steganografi merupakan langkah yang baik. Lalu lintas pertukaran mp3 di internet merupakan hal biasa sehingga steganografi menggunakan mp3 adalah teknik yang baik untuk mengamankan pesan rahasia melalui media internet.

1.2 Batasan Masalah

Dalam penulisan ini, penulis akan mengembangkan program steganografi yang mampu menyembunyikan informasi rahasia di dalam media audio. Media audio yang digunakan berformat terutama format *.mp3, *.au dengan menggunakan metode LSB (*Least Significant Bit*).

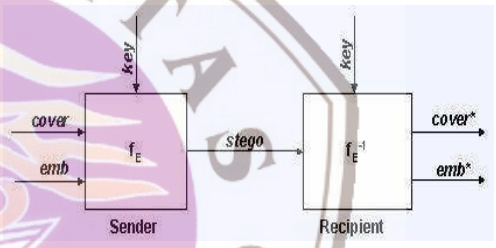
2. Landasan Teori

2.1 Pengertian Steganografi

Kata steganografi berasal dari bahasa Yunani yaitu steganos yang berarti penyamaran atau penyembunyian dan graphein atau graptos yang berarti tulisan sehingga secara keseluruhan artinya adalah tulisan yang disembunyikan. Secara umum steganografi merupakan seni atau ilmu yang digunakan untuk menyembunyikan pesan rahasia (informasi) tertulis kedalam pesan lain dengan segala cara sehingga selain orang yang dituju, orang lain tidak akan menyadari keberadaan dari pesan rahasia tersebut. Meskipun memiliki tujuan yang sama dengan kriptografi,

keduanya merupakan hal berbeda. Pada kriptografi informasi diamankan sedemikian rupa sehingga orang lain tidak mengenali informasi tersebut, sedangkan steganografi menyembunyikan informasi sedemikian rupa sehingga tidak disadari keberadaannya oleh orang lain. Satu hal yang menjadi kelebihan dari steganografi adalahkemampuannya untuk menipu persepsi manusia, manusia tidak memiliki insting untuk mencurigai adanya arsip-arsip yang memiliki informasi yang tersembunyi didalamnya, terutama bila arsip tersebut tampak seperti arsip normal lainnya.

Steganografi merupakan salah satu cara untuk menyembunyikan suatu pesan atau data rahasia di dalam data atau pesan lain yang tampak tidak mengandung apa-apa, kecuali bagi orang yang mengerti kuncinya. Dalam bidang keamanan komputer, steganografi digunakan untuk menyembunyikan data rahasia saat enkripsi tidak dapat dilakukan atau bersamaan dengan enkripsi. Jadi, walaupun enkripsi berhasil dipecahkan pesan atau data rahasia tetap tidak terlihat. Selain itu, pada kriptografi pesan disembunyikan dengan diacak sehingga pada kasus-kasus tertentu dapat dengan mudah mengundang kecurigaan, sedangkan pada steganografi pesan disamarkan dalam bentuk yang relatif aman sehingga tidak terjadi kecurigaan itu. Steganografi dapat digunakan pada berbagai macam bentuk data, yaitu citra, audio dan video.



Gambar 2.1 Gambaran Umum Steganografi

2.2 Metode Steganografi pada Suara

Cara untuk mengaplikasikan steganografi pada file audio terdiri dari beberapa cara yang lazim digunakan dan prinsip kerja atau algoritma yang digunakan sama eperti pada metode steganografi pada gambar. Berikut adalah beberapa teknik yang digunakan:

1. *Low Bit coding / Least Significant Bit*

Cara ini lazim digunakan dalam teknik digital steganografi yaitu mengganti LSB input setiap samplingnya dengan data yang dikodekan. Metode ini sama dengan LSB pada media gambar. Dengan menyisipkan bit-bit dari pesan yang akan dimasukkan kedalam bit yang sudah tersedia dari file induk atau file aslinya. Karena metode ini mudah diterapkan dalam implementasi steganografi untuk suara atau audio Dengan metode ini keuntungan yang didapatkan adalah ukuran pesan yang disispkan relative besar,namun berdampak pada hasil audio yang berkualitas kurang dengan banyaknya noise.

2. *Phase coding*

Metode kedua yang digunakan ini adalah merekayasa fasa dari sinyal masukan. Teori yang digunakan adalah dengan mensubstitusi awal fasa dari tiap awal segment dengan fasa yang telah dibuat sedemikian rupa dan merepresentasikan pesan yang disembunyikan. Fasa dari tiap awal segment ini dibuat sedemikian rupa

sehingga setiap segmen masih memiliki hubungan yang berujung pada kualitas suara yang tetap terjaga. Teknik ini menghasilkan keluaran yang jauh lebih aik daripada metode pertama namun dikompensasikan dengan kerumitan dalam realisasinya.

3. *Spread Spectrum*

Metode yang ketiga adalah penyebaran spektrum. Dengan metode ini pesan dikodekan dan disebar ke setiap spectrum frekuensi yang memungkinkan. Makadari itu akan sangat sulit bagi yang akan mencoba memecahkannya kecuali ia memiliki akses terhadap data tersebut atau dapat merekonstruksi sinyal random yang digunakan untuk menyebarkan pesan pada range frekuensi.

4. *Echo Hiding*

Metode terakhir yang sering digunakan adalah menyembunyikan pesan melalui teknik echo. Teknik menyamarkan pesan ke dalam sinyal yang membentukecho. Kemudian pesan disembunyikan dengan menvariasikan tiga parameter dalam echo yaitu besar amplitude awal, tingkat penurunan atenuasi, dan offset.Dengan adanya offset dari echo dan sinyal asli maka echo akan tercampur dengan sinyal aslinya, karena sistem pendengaran manusia yang tidak memisahkanantara echo dan sinyal asli.

Keempat metode di atas memiliki kesamaan yaitu menggunakan kelemahan dari sistem pendengaran manusia. Maka dari itu teknik steganografi dalam MP3 juga akan menggunakan kelemahan ini untuk menyembunyikan pesan.

2.3 Bahasa Java

Versi pertama bahasa pemrograman Java dirilis pada akhir 1995, dan dalam beberapa bulan Java menjadi bahasa pemrograman pada World Wide Web. Beberapa tahun kemudian merupakan salah satu bahasa pemrograman serbaguna yang pernah dikembangkan dan banyak digunakan. Java memiliki beberapa keunggulan bila dibandingkan dengan bahasa pemrograman lainnya. Diantaranya :

1. Java bersifat lebih sederhana dan relatif mudah Java dimodelkan sebagian dari bahasa C++, namun dengan memperbaik beberapa karakteristik C++, seperti mengurangi kompleksitas beberapa fitur, penambahan fungsionalitas, serta penghilangan beberapa aspek pemicu ketidakstabilan sistem pada C++.
2. Java berorientasi objek Java adalah bahasa pemrograman berorientasi objek (OOP), yang dimaksud dengan pemrograman berorientasi objek adalah suatu konsep pemrograman yang memecahkan masalah dengan cara memilah program menjadi objek – objek yang saling berinteraksi satu sama lain.
3. Java bersifat multiplatform
Dapat diterjemahkan oleh Java interpreter pada berbagai sistem operasi.
4. Java bersifat multithread
Thread adalah proses yang dapat dikerjakan oleh program dalam suatu waktu. Ini berarti Java dapat mengerjakan beberapa proses dalam waktu yang hampir bersamaan.

Program Java dapat dibedakan menjadi dua jenis, yaitu applet dan aplikasi.

1. Applet, adalah program yang dibuat dengan Java, dapat diletakkan pada Web server dan diakses melalui web browser. Dalam hal ini browser yang digunakan adalah yang memiliki kemampuan Java (misalnya Netscape Navigator, Internet Explorer, dan Hot Java).
2. Aplikasi, adalah program yang

dibuat dengan Java yang bersifat umum. Aplikasi dapat dijalankan secara langsung, tidak perlu perangkat lunak browser untuk menjalankannya. Aplikasi dapat dibayangkan seperti program yang ditulis dengan bahasa C atau Pascal. Setelah dikompilasi, dapat dieksekusi secara langsung. Java dipaketkan dalam tiga edisi, yaitu Java 2 Standard Edition (J2SE), Java 2 Enterprise Edition (J2EE), dan Java 2 Micro Edition (J2ME).

3. Analisis dan Pembahasan

3.1 Gambaran Umum Program

Secara umum program Steganografi ini (yang diberi versi 1.0) digunakan untuk menyembunyikan suatu data atau informasi ke dalam sebuah media sehingga sulit dideteksi keberadaan data atau informasi tersebut karena hasil dari penyembunyian tersebut tidak berbeda dengan sumbernya. Media yang digunakan dalam penulisan ini adalah objek digital berupa file audio atau suara. Setelah media tersebut ditentukan, data atau informasi tersebut baru dapat disisipkan atau disembunyikan ke dalam media tersebut

Untuk menyisipkan informasi atau data rahasia ke dalam objek digital diperlukan suatu algoritma yang disebut dengan algoritma embedding. Algoritma tersebut dapat memodifikasi objek digital sehingga menghasilkan objek digital baru yang berisi informasi tersembunyi. Dalam proses modifikasi perubahan yang terjadiantara objek digital (media asli) dengan objek digital baru hasil modifikasi media tidak boleh terlalu terlihat perbedaannya.

Dalam steganografi agar kerahasiaan data atau informasi yang terkandung dalam objek digital tetap aman dan tidak sembarang orang dapat menggunakan aplikasi serta mengambil data yang terdapat didalamnya, maka dibutuhkan suatu kunci untuk mengambil data rahasia yang terkandung dalam objek digital tersebut. Kunci tersebut adalah yang biasa disebut dengan istilah kata sandi. Kata sandi ini akan diminta pada awal penggunaan dari program ini. Orang awam atau orang yang bermaksud menyalahgunakan data atau informasi tersebut tidak dapat menggunakan aplikasi ini jika mereka tidak mengetahui kata sandi dalam aplikasi ini

Teknik Steganografi Modifikasi LSB dilakukan dengan memodifikasi bit-bit yang termasuk bit LSB pada setiap byte sample pada sebuah file audio. Bit-bit LSB ini akan dimodifikasi dengan menggantikan setiap LSB yang ada dengan bit-bit informasi lain yang ingin disembunyikan. Setelah semua bit informasi lain menggantikan bit LSB didalam file tersebut, maka informasi telah berhasil disembunyikan. Ketika informasi rahasia tersebut ingin kembali dibuka, maka bit- bit LSB yang sekarang ada, diambil satu per satu kemudian disatukan kembali menjadi sebuah informasi yang utuh seperti semula.

3.2 FlowChart

Untuk Menggambarkan keterhubungan antara masing proses pada alur tahap embeding dan Alur tahap retrieving agar masing-masing proses tergambarkan dengan jelas

3.3 UML (*Unified Modelling language)*.

Uml digunakan untuk menggambarkan gambaran program / sistem secara umum (*Use Case Diagram*), lalu menggambarkan prosedur atau jalannya program secara rinci pada *Activity Diagram*, Serta Keterhubungan antar masing – masing *class* yang digunakan dalam pembuatan program

.

3.4 Uji Coba Program

Pelaksanan uji coba dilakukan guna mencari hasil dan menjawab berbagai macam teori an analisa yang hendak dibuktikan oleh penyusun. Secara garis besar, pelaksanaan ujicoba dibedakan dalam dua tahap yaitu tahap embedding dan tahap retrieving. Dalam program ini, dilakukan uji coba berbagai format audio. Format audio yang digunakan dalam uji coba adalah mp3 dan au.

3.5 Analisis dengan Metode SNR (*Signal to Noise Ratio)*

Analisa dengan menggunakan signal-to noise ratio (SNR) terhadap sebuah file hasil keluaran dengan menggunakan perangkat lunak tambahan yang bernama Oscillometer 7.0, yang di dalam file keluraran terdapat file atau pesan rahasia. Ini dilakukan untuk mengetahui seberapa besar terjadinya *noise* yang dikeluarkan setelah penyisipan dari tahap embedding.

Dari analisa signal-to noise ratio (SNR) ini didapatkan besarnya *noise* yang dihasilkan pada file hasil keluaran dengan satuan *desible* (db).

Dalam pengujian analisa terhadap SNR 30 detik pertama, digunakan sebuah file pembawa/master dan beberapa file data Hero.mp3 dan face down.mp3 dalam jenis steganografi embed file . Pengujian pertama akan dilakukan dengan sebuah file pembawa dan sebuah file data dengan perubahan ukuran pada file.

3.6 Analisis Hasil dengan Metode *Wave Analysis*

Wave Analysis atau biasa disebut dengan analisa gelombang suara yang ditimbulkan oleh setiap file audio (dalam hal ini mp3) yaitu dengan mengamati perubahan , ampluitudo bahkan sampai celah terkecil yang dihasilkan dari file hasil pada tahap embedding. Dalam tahap ini digunakan perangkat lunak tambahan yang bernama Wavepad Sound Editor 3.05 yang menganalisa gelombang keluaran dari file tahap embedding.

3.7 Spesifikasi Perangkat Keras dan Perangkat Lunak

Dalam penulisan ini, spesifikasi perangkat lunak dan perangkat keras yang digunakan dalam pembuatan aplikasi ini adalah sebagai berikut:

- Processor : Intel Pentium 4 2,4 GHz
- Memory : DDRAM 512 MB
- HardDisk : 40 GB
- Sistem Operasi: Windows XP SP2
- Software : J2SDK1.5.0, Eclipse SDK 3.0, Oscillometer 7.01, WavePad Sound Editor 3.05

4. Penutup

4.1 Kesimpulan

Aplikasi audio steganografi ini berhasil dibuat dan dapat digunakan sebagai mana mestinya baik penyisipan maupun pengambilan kembali pesan atau file.

4.2 Saran

Diharapkan aplikasi ini dapat ditambah dalam ekstensi audio yang digunakan, agar dapat memproses lebih banyak tipe file audio

.

Referensi

1. Kadir, Abdul, "Dasar Pemrograman Java 2", Andi, Yogyakarta, 2003.
2. Hakim S, Rachmad, "Mastering Java", Elex Media Komputindo, Jakarta, 2009.
3. Fowler, Martin, " UML Distilled :Panduan Lengkap Bahasa Pemodelan Objek Standar", Andi , Yogyakarta, 2005.
4. Munawar, "Pemodelan Visual Dengan UML", Graha Ilmu, Yogyakarta, 2005.
5. Sri Dharwayanti, Pengantar Unified Modeling Language (UML), http://www.ilmukomputer.com/, Juni 2007.
6. Stefanus Soehono, Audio Steganografi, Informatika Bandung, Bandung, 2006
7. Budi Sukmawan, Steganografi, http://students.ukdw.ac.id/~22033120/steganografi.html, 2008.
8. Dwidy Putut W, Audio Steganografi, http://images.doank29.multiply.com/attachment/0/Rkb9qgoKCp4AAEwAjaU1/Steganografi.doc?nmid=42039797, 2008.
9. Muhammad Hakim A, Studi dan Implementasi Steganografi Metode LSB dengan Preprocessing Kompresi data dan Ekspansi Wadah, http://www.informatika.org/~rinaldi/Kriptografi/2007-/Makalah1/MakalahIF5054-2007-A-077.pdf, 2008.
10. Andino Masaleno, "Pengantar Steganografi", http://ikc.muganet.com/umum/andino-steganografi.php, Juni 2008.
12. Herianto, " Pembangunan Perangkat Lunak Steganografi Audio MP3 dengan Teknik *Parity Coding* pada Perangkat *Mobile Phone*", Tulisan Ilmiah, ITB. (Diakses Mei 2009).
11. Dian Dwi Hapsari, "Aplikasi Video Steganografi dengan Metode Least Significant Bit", Skripsi, Gunadarma, September 2008.
12. Indah Kusuma Wardani, " Penyisipan Pesan Berbasis Least Bit Significant pada Citra Digital Menggunakan Matlab", Tulisan Ilmiah, Gunadarma, Oktober 2008.
13. Hasan, Rusydi. 2003. Mengenal Algoritma DES, (online), http://www.ilmukomputer.com, (diakses Juni 2009).
14. Sukrisno dan Ema Utami, " Implementasi Steganografi Teknik EOF dengan Gabungan Enkripsi Rijndael, Shift Chipper dan Fungsi Hash MD5", Yogyakarta, Seminar Nasional Teknologi 2007. (Diakses Juli 2009).