IMPLEMENTASI STEGANOGRAFI DALAM MENYEMBUNYIKAN FILE PADA FILE MP3 MENGGUNAKAN SPREAD SPECTRUM IMPLEMENTATION OF STEGANOGRAPHY TO HIDE FILE WITHIN MP3 FILE USING SPREAD SPECTRUM METHOD

Hanafi Adib Nugraha[1], -[2]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Dalam dunia digital saat ini, terdapat banyak sekali informasi atau data yang dapat diakses dalam berbagai bentuk : teks, gambar, audio, dan video. Beberapa file mungkin bagi kita sangat penting sehingga harus dijaga keamanannya agar tidak dicuri, diubah atau dihapus orang lain. Salah satu metode dalam keamanan data adalah steganografi dimana file yang dianggap penting tersebut disembunyikan dalam file lain. Secara umum, file yang ada di komputer, seperti MP3, WAV, BMP, JPEG, GIF, AVI, dan file lainnya dapat disembunyikan atau dijadikan sebagai cover carrier. File audio(wav) dan image adalah file yang umum digunakan sebagai cover carrier. File audio yang masih jarang digunakan sebagai media cover salah satunya adalah MP3.

Dalam tugas akhir ini diimplementasikan teknik steganografi pada file MP3 menggunakan metode spread spectrum. Data berupa sembarang file akan disisipkan secara tersebar dalam dua domain, yakni domain waktu dan domain frekuensi. Untuk mengetahui metode mana yang lebih baik, maka terhadap file StegoMP3 dilakukan pengujian secara objektif dengan perhitungan Signal to Noise Ratio (SNR) dan secara subjektif oleh 20 responden, sedangkan terhadap data yang disembunyikan dilakukan pengujian tingkat validitas data hasil ekstraksi steganografi.

Dari pengujian yang telah dilakukan diperoleh hasil bahwa penyembunyian dalam domain waktu lebih baik daripada penyembunyian dalam domain frekuensi. Besar ukuran data yang disembunyikan mempengaruhi kualitas StegoMP3 yang dihasilkan dengan hubungan berbanding terbalik, namun tidak mempengaruhi validitas data yang disembunyikan. Kualitas StegoMP3 akan menyerupai aslinya jika menghasilkan nilai SNR lebih besar atau sama dengan 28,58 dB. Besar ukuran data maksimal yang dapat disembunyikan pada file MP3 berdurasi 60 detik untuk menghasilkan nilai SNR lebih besar atau sama dengan 28,58 dB adalah 6500 byte.

Kata Kunci : Steganografi, MP3, Spread Spectrum

Abstract

In today's digital world, there is a great wealth of information, which can be accessed in various forms : text, images, audio and video. Some of them maybe very important to us, so we must keep the security of the data for not be stolen, changed or demolished by another person. One of any methode in data security is steganography, which the important ones of file hide within other file. Generally, files in the computer, like MP3, WAV, BMP, JPEG, GIF, AVI and the other files can be hide or make them as cover carrier. Audio file(wav) and image are commonly used as cover carrier. Audio file which still seldom be used as media cover one of them is MP3.

This Final project implementing technique of steganography at MP3 file use spread spectrum method. Data in the form of any file will be inserted spread over in two domain, namely time domain and frequency domain. To know which method is better, hence to StegoMP3 file done by examination objectively with calculation of Signal to Noise Ratio (SNR) and subjectively by 20 respondent, while to data which be hidden done by examination to compute level validity of data resulted from extraction of steganography.

From conducted examination, conclude that concealment in time domain better than concealment in frequency domain. Size of hidden data influence the quality of yielded StegoMP3 with inversely proportional relation, but not influences the validity of hidden data. Quality of StegoMP3 will similar with the original if resulting SNR value grather than or equal to 28,28 dB. Maximum size of data that can be hide in MP3 file which have 60 second long to produce SNR value grather than or equal to 28,58 dB is 6500 bytes.

Keywords : Steganography, MP3, Spread Spectrum

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi telekomunikasi tidak hanya mendorong kecenderungan orang untuk saling berkomunikasi semata. Tuntutan menjadi semakin kompleks sehingga masalah keamanan data menjadi hal yang sangat penting, apalagi data yang dikirimkan adalah data yang amat rahasia.

Berbagai usaha dilakukan untuk menjamin agar data rahasia yang dikirimkan tersebut tidak bisa diakses oleh pihak lain. Oleh karena itu kemudian dalam dunia keamanan data muncul istilah kriptografi dan steganografi.

Walaupun steganografi dapat dikatakan mempunyai hubungan yang erat dengan kriptografi, tapi metode ini sangat berbeda dengan kriptografi. Kriptografi mengacak pesan sehingga tidak dimengerti, sedangkan steganografi menyembunyikan pesan sehingga tidak terlihat. Pesan dalam *ciphertext* mungkin akan menimbulkan kecurigaan sedangkan pesan yang dibuat dengan steganografi tidak akan. Agar lebih baik lagi, kedua teknik ini dapat digabungkan untuk mendapatkan hasil yang semakin sulit dilacak.

Selain steganografi, ada istilah lain dalam *data hiding,* yakni *watermarking.* Keduanya hampir sama, hanya dibedakan dari tujuan penggunaannya. *Watermark* dapat dikatakan sebagai atribut dari *carrier,* yang dapat berupa *copyright, license, owner,* dan informasi lain. Sedangkan steganografi, menyembunyikan data yang tidak ada hubungannya dengan *carrier*. Oleh karena itu, yang menjadi fokus perhatian dalam steganografi adalah data rahasia yang dibawanya, bukan pada kehandalan *carrier,* walaupun tetap harus dipertimbangkan kualitas audionya agar tidak menimbulkan kecurigaan. Penurunan kualitas audio harus masih dalam taraf yang bisa ditolelir oleh sistem pendengaran manusia.

MP3 memiliki ukuran yang relatif lebih besar daripada file image, sehingga memungkinkan lebih banyak data bisa disembunyikan dalam file ini. Dan lagi, MP3 saat ini sudah sangat populer, ditunjukkan dengan meluasnya penggunaan MP3 oleh banyak orang, bahkan mungkin hampir semua harddisk memuat file MP3. Semakin familiar

seseorang dengan suatu hal, maka semakin sedikit kecurigaannya terhadap hal tersebut. Dengan begitu, dalam beberapa waktu kedepan MP3 tidak hanya berfungsi sebagai media audio saja tetapi dapat berfungsi lebih banyak, salah satunya sebagai media penyimpanan data.

Dengan sistem ini, keamanan data dapat lebih terjamin, karena yang dapat mengambil file yang tersembunyi hanya orang yang memiliki kode kunci untuk mengaksesnya.

1.2 Rumusan Masalah

Dalam tugas akhir ini, akan dirancang dan diimplementasikan steganografi pada audio digital. Data yang disembunyikan berupa file. Adapun data tersebut akan disembunyikan di dalam file audio menggunakan metode *spread spectrum*. Pada metode *spread spectrum*, data yang telah dikodekan disebar pada domain waktu dan spektrum frekuensi. Metode ini dapat membuat data-data yang dikirimkan sulit ditemukan oleh yang tidak berhak. Metode ini menggunakan *pseudo-random* untuk menyebar data pada jangkauan frekuensi. Sistem ini menggunakan kode kunci untuk autentikasi user yang berhak mengakses.

Untuk mengimplementasikan hal tersebut, ada beberapa point yang menjadi perhatian, yaitu :

A. File audio dibangun dari bagian bagian yang disebut frame, oleh karena itu harus diketahui bagaimana mendapatkan data audio dari setiap frame tersebut.
B. Data audio yang terdapat pada file MP3 merupakan sinyal pada domain waktu. Untuk melakukan penyisipan pada domain frekuensi, maka harus diketahui bagaimana mentransformasikan data audio tersebut menjadi domain frekuensi. Dan begitu juga sebaliknya, hasil transformasi harus dapat dikembalikan menjadi formatnya semula.
C. Bagaimana mengkodekan data yang akan disembunyikan sehingga dapat disisipkan dengan baik pada domain waktu maupun domain frekuensi.

D. Karena data ini akan disebar secara acak, maka harus dicari bagaimana teknik *pseudo-random* yang baik, agar data yang disembunyikan tadi dapat direkonstruksi kembali.

1.3 Tujuan Tugas Akhir

Tugas Akhir ini bertujuan untuk :

A. Merancang dan mengimplementasikan perangkat lunak steganografi pada audio digital yang berfungsi untuk :
   i. Menyembunyikan file dalam audio digital menggunakan metode *spread spectrum*.
   ii. Mengambil *(extract)* kembali file yang disembunyikan.

B. Menganalisis metode yang terbaik untuk melakukan steganografi pada file MP3 dengan melakukan perbandingan antara penyisipan pada domain waktu dengan penyisipan pada domain frekuensi yang diimplementasikan pada beberapa karakter atau warna audio. Analisis difokuskan dalam hal :
   i. Validitas data hasil ekstraksi steganografi.
   ii. Kualitas audio hasil implementasi steganografi dengan pengujian objektif menggunakan perhitungan *Signal to Noise Ratio (SNR)* untuk membandingkan audio asli dengan audio yang sudah menjadi *cover carrier*.
   iii. Kualitas audio hasil implementasi steganografi untuk menilai tingkat perbedaan antara audio asli dengan audio yang sudah menjadi *cover carrier* secara subjektif oleh 20 orang responden.

C. Menganalisis pengaruh besar ukuran file yang disembunyikan terhadap validitas data hasil ekstraksi steganografi dan kualitas audio hasil implementasi steganografi.

1.4 Batasan Masalah

Dalam penyelesaian tugas akhir ini, bahasan akan dibatasi hanya mencakup pada :

A. File audio yang digunakan sebagai *cover carrier* adalah file yang memiliki format MP3 yakni MPEG layer 3.
B. File MP3 yang digunakan hanya file MP3 yang memiliki *bitrate* yang tetap *(constant bitrate).*
C. Data yang disembunyikan memiliki ukuran yang lebih kecil dibandingkan ukuran file MP3 yang menjadi *cover*.
D. Untuk mentransformasikan audio menjadi domain frekuensi digunakan metode *Fast Fourier Transform (FFT)*.

1.5 Metodologi

Untuk menyelesaikan pembuatan tugas akhir ini, akan dilakukan beberapa langkah kerja sebagai berikut :

A. Identifikasi masalah, yaitu dengan mencari kemungkinan masalah yang akan dihadapi. Dalam hal ini termasuk pengidentifikasian dan batasan masalah.
B. Studi literatur tentang steganografi pada audio digital, format file MP3, metode *Fast Fourier Transform (FFT),* metode *spread spectrum*, metode *pseudo random* yang digunakan, *Auditory Masking,* serta *Digital Signal Processing* sebagai pendukung.
C. Analisis dan perancangan perangkat lunak, yaitu menganalisa kebutuhan yang digunakan untuk perangkat lunak dan merancang perangkat lunak dengan mempertimbangkan sistem pendengaran manusia, namun tetap berfungsi dengan baik sebagai media penyimpanan data.
D. Implementasi, yaitu merealisasikan hasil rancangan menjadi suatu perangkat lunak.
E. Analisis hasil, yaitu dengan mengadakan pengujian terhadap performansi sistem secara obyektif dan subyektif.

1.6 Sistematika Penulisan

Tugas akhir ini disusun dengan sistematika pembahasan sebagai berikut :

BAB I PENDAHULUAN

Bab ini memaparkan latar belakang dilakukannya penelitian, perumusan masalah yang akan dibahas, pembatasan masalah, tujuan yang ingin dicapai melalui penelitian ini, metode penyelesaian masalah dan sistematika penulisan.

BAB II DASAR TEORI

Bab ini membahas teori yang mendukung penyusunan tugas akhir ini yaitu mengenai steganografi, format file MP3, *Fast Fourier Transform (FFT)*, *Spread Spectrum* dan *Auditory Masking*.

BAB III ANALISIS DAN PERANCANGAN

Menguraikan mengenai analisis awal sistem serta proses perancangan sistem secara keseluruhan.

BAB IV IMPLEMENTASI DAN PENGUJIAN DAN ANALISIS

Bab ini berisi tentang implementasi dari hasil analisa dan perancangan. Juga berisi pengujian beserta analisis hasil pengujian yang dilakukan..

BAB V KESIMPULAN DAN SARAN

Berisi kesimpulan dari hasil penelitian tugas akhir ini serta saran-saran untuk pengembangan lebih lanjut.

Telkom University

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan pemahaman teori dan hasil penelitian yang dilakukan selama menyusun tugas akhir ini, maka dapat disimpulkan :

1. Steganografi dapat dilakukan pada file MP3.
2. Dikarenakan kondisi data audio MP3 berupa bilangan bulat, proses penyembunyian lebih baik dilakukan pada domain waktu (tanpa melalui FFT).
3. Kualitas hasil penyembunyian berbanding terbalik dengan banyak data yang disembunyikan.
4. Besar ukuran data yang disembunyikan pada domain waktu tidak mempengaruhi validitas data hasil ekstraksi steganografi.
5. Dari analisis hasil pengujian kualitas secara objektif dan subjektif, kualitas audio StegoMP3 mempunyai kualitas baik bila nilai SNR yang dihasilkan lebih besar dari atau sama dengan 28,58 dB.
6. Ukuran file data yang bisa disisipkan pada file MP3 berdurasi $\pm$ 60 detik dengan kualitas audio StegoMP3 yang tetap *excellent* dan menghasilkan nilai SNR lebih besar atau sama dengan 28,58 dB adalah file dengan ukuran maksimal 6500 byte.

5.2 Saran

Beberapa saran yang bisa diberikan antara lain :

1. Pengembangan aplikasi sehingga MP3 yang memiliki *variable bitrate* juga bisa digunakan sebagai *host*, tidak hanya MP3 yang memiliki *constant bitrate* saja.
2. Dari segi metode penyisipan, dapat dikembangkan dengan melakukan *spread spectrum* pada domain yang lain, seperti *wavelet, cepstral,* dan sebagainya.

DAFTAR PUSTAKA

[1] Aisyah, Siti. *"Implementasi Audio Watermarking Menggunakan Fast Fourier Transform (FFT)"*, Bandung: Tugas Akhir. Jurusan Teknik Informatika. STT Telkom. 2004.

[2] Fraunhofer. *"Audio & Multimedia, MPEG Audio Layer-3"*. Web Sites. 1998

[3] Hoffman, Forrest M. *"An Introduction to Fourier Transform"*.

[4] John G. Proakis, Dimitris G. Manokalis. *"Pemrosesan Sinyal Digital"*. PT. Prenhallindo, Jakarta. 1995.

[5] Jonathan Cummins, Patrick Diskin, Samuel Lau, Robert Parlett. *"Steganography and Digital Watermarking"*. School of Computer Science, The University of Birmingham. 2004.

[6] Moving Pictures Expert Group (MPEG). *"Coding of Moving Pictures and Associated Audio for Digital Storage Media at Up to About 1.5 Mbit/s Part 3"*. Standart CD 11172-3. 1991.

[7] Noll, Peter. *"Digital Audio for Multimedia"*. Technische Universidt Berlin, Jerman. 1999.

[8] Ross J. Anderson, Fabien A.P. Petitcolas. *"On The Limit of Steganography"*. IEEE Journal. 1998.

[9] W. Bender, D. Gruhl, N. Morimoto, A. Lu. *"Techniques for Data Hiding"*. IBM system journal, vol 35 NOS 3&4. 1996.