TEKNIK STEGANOGRAFY PADA FILE AUDIO DIGITAL TIDAK TERKOMPRESI

Harlian Renato[1], Agus Virgono Ir .mt ; Joko Haryatno Mt.[2], [3]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Kata Kunci :

Abstract

Keywords :

Telkom University

Bab I
Pendahuluan

1.1 Latar Belakang

Teknologi digital serta jaringan internet saat ini telah memberi kemudahan bagi kita untuk melakukan akses serta mendistribusikan berbagai informasi dalam format digital. Saat ini jaringan jaringan internet telah digunakan untuk berbagai kebutuhan, baik itu untuk kepentingan komersial, maupun penggunaan secara individual. Seiring dengan semakin meluasnya penggunaan jaringan internet, pengiriman informasi semakin rentan terhadap penyadapan, pelanggaran terhadap hak cipta, dan bentuk serangan lain yang dapat mengubah autentifikasi dan integritas data.

Untuk mengurangi atau mencegah terjadinya pemalsuan ataupun penggunaan secara tidak legal pada suatu informasi yang didistribusikan menggunakan jaringan internet maka kita bisa menyembunyikan informasi rahasia yang tidak terlihat atau tidak disadari oleh orang lain di dalam sebuah informasi lainnya. Teknik ini disebut steganografi, yaitu seni untuk menyembunyikan pesan di dalam pesan lainnya sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu di dalam pesan tersebut.

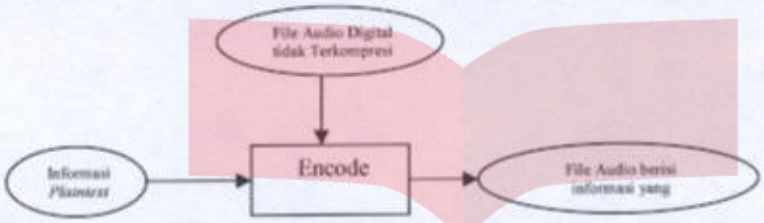
Dalam tugas akhir ini akan dilakukan penelitian untuk menyembunyikan sebuah informasi di dalam file audio digital, karena saya melihat hingga saat ini file audio digital sebagai pembawa atau *host* bagi informasi yang dirahasiakan kurang digunakan. Yang banyak digunakan sebagai host bagi informasi yang dirahasiakan adalah file image. Padahal lalu lintas peredaran dan distribusi file audio digital di jaringan internet sangat tinggi, berangkat dari hal tersebut tidak ada salahnya bila di dalam file audio digital disembunyikan informasi yang berupa kode-kode rahasia dan informasi mengenai suatu hak cipta sehingga tingkat pemalsuan dan penggunaan informasi secara ilegal yang sangat merugikan dapat ditekan / dicegah.

1.2 Perumusan Masalah

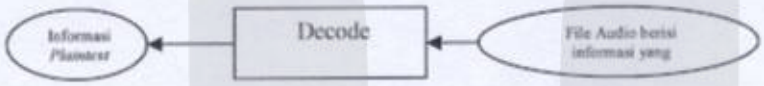
Adapun permasalahan yang ingin diangkat dalam penelitian tugas akhir ini adalah :

- Bagaimana penggunaan *steganografy* untuk file audio digital tidak terkompresi (*.wav).

- Bagaimana performansi file audio (*.wav) yang telah diisi informasi (*.All Files) dengan melihat kualitas suara dan kehandalannya terhadap kemungkinan terdeteksi dan terjadinya *cracking*.
- Berapa persen dari ukuran file audio (*.wav), ukuran informasi (*.All Files) maksimal yang dapat disembunyikan tanpa menurunkan performansi.



Gambar 1.1 Proses *Encoding*



Gambar 1.2 Proses *Decoding*

Proses *encoding* dilakukan untuk menyembunyikan informasi (*.All Files) ke dalam file audio, dimana informasi akan disembunyikan, dan pada proses *decoding* file audio yang sudah diberi informasi akan diproses untuk mendapatkan kembali informasi yang tadinya disembunyikan. Untuk meningkatkan keamanan, maka informasi yang disembunyikan akan di-*enkripsi* dengan password, dan pada saat *decoding* password yang sama akan diperlukan untuk men-*dekrip* informasi tersebut.

Pada saat informasi (*.All Files) telah disembunyikan diharapkan ukuran file audio digital (*.wav) sebagai *carrier* tidak akan mengalami perubahan yang signifikan, sehingga kemungkinan informasi yang disembunyikan untuk terdeteksi sangat kecil.

Dalam penelitian ini saya memiliki asumsi bahwa ukuran informasi (*.All Files) yang disembunyikan di dalam file audio tidak terkompresi (*.wav) akan sangat berpengaruh terhadap performansi yang dihasilkan yaitu kualitas suara, kemungkinan terdeteksi dan *packet loss*.

1.3 Batasan Masalah

Pembahasan masalah pada tugas akhir ini akan dibatasi pada ruang lingkup :

- Membahas teknik substitusi pada LSB untuk menyembunyikan informasi (*.All Files) ke dalam file audio digital tidak terkompresi (*.wav).
- Pembuatan perangkat lunak untuk menyembunyikan informasi (*.All Files) ke dalam file audio digital tidak terkompresi (*.wav).
- Proses *steganografy* yang dilakukan tidak merubah ukuran file audio digital (*.wav).
- Analisis pengaruh besar-kecilnya informasi (*.All Files) yang disembunyikan terhadap kualitas suara yang dihasilkan oleh file audio digital (*.wav).
- Melakukan uji kehandalan (kemampuan tidak terdeteksi dan mempertahankan infomasi yang disembunyikan) output perangkat lunak yang dirancang terhadap proses deteksi dan *cracking* (pengambilan informasi yang disembunyikan dengan tidak menggunakan password) menggunakan software-software *steganalysis*, untuk mengetahui tingkat keamanan yang dihasilkan oleh perangkat lunak yang dirancang.

1.4 Tujuan Penelitian

Tujuan penelitian dari tugas akhir ini adalah :

- Mengaplikasikan teknologi *steganografy* dengan menggunakan teknik substitusi pada LSB file pembawa untuk menyembunyikan informasi (*.All Files) ke dalam file audio digital yang tidak terkompresi (*.wav).
- Menganalisa pengaruh besar-kecilnya informasi (*.All Files) yang disembunyikan terhadap kualitas suara yang dihasilkan oleh file audio digital (*.wav).

1.5 Metodologi Penelitian

Metode penelitian yang digunakan dalam penulisan tugas akhir ini adalah :

- Studi literatur, yaitu dengan mengumpulkan referensi mengenai teknik substitusi pada LSB untuk melakukan proses *steganografy* dan file audio digital yang tidak terkompresi (*.wav).

- Diskusi dan konsultasi dengan dosen pembimbing dan pihak lain untuk penyempurnaan pengerjaan tugas akhir ini.
- Melakukan ujicoba lapangan untuk melakukan penelitian / survey subyektif dengan metode MOS.

1.6 Sistematika Penulisan

Penulisan tugas akhir ini dibagi dalam 5 bab, yaitu :

BAB I. Pendahuluan

Dalam bab ini akan dikemukakan latar belakang, perumusan masalah, batasan masalah, tujuan penelitian, metodologi penelitian dan sistematika penulisan.

BAB II. Dasar Teori

Penjelasan dasar dari teknik substitusi pada LSB file pembawa untuk melakukan proses *steganografy* dan audio digital khususnya audio digital yang tidak terkompresi (*.wav).

BAB III. Perancangan Perangkat Lunak

Dalam bab ini akan menjelaskan proses perancangan aplikasi teknologi *steganografy* yang akan dilakukan terhadap file audio digital (*.wav).

BAB IV. Implementasi dan Analisis

Dalam bab ini akan menjelaskan analisis hasil percobaan penyisipan informasi (*.All Files) ke dalam file audio digital (*.wav), mengenai berubah tidaknya ukuran file pembawa, perubahan bit yang terjadi serta analisis performansi dari hasil MOS *(Mean Opinion Score)*.

BAB V. Kesimpulan dan Saran

Pada bab ini berisi kesimpulan hasil analisis dan saran perbaikan mengenai tugas akhir ini.

Bab V
Kesimpulan dan Saran

5.1 Kesimpulan

Adapun kesimpulan yang bisa diambil dari penelitian tugas akhir ini adalah sebagai berikut :

1. *Steganography* dapat diaplikasikan pada file wav sebagai media pembawa informasi.
2. Teknik substitusi LSB memungkinkan perubahan yang terjadi adalah mendekati 50% dari ukuran file yang disembunyikan, hal ini akan mengurangi kemungkinan degradasi kualitas suara yang dihasilkan.
3. Ukuran informasi maximal yang bisa disembunyikan menggunakan teknik substitusi LSB tanpa menimbulkan noise yang mencurigakan adalah sekitar 1/16 atau 6.25 % dari besarnya ukuran file pembawa.
4. Dengan menggunakan teknik substitusi LSB untuk file audio digital tidak terkompresi, terbukti software *steganalysis* tidak mendeteksi adanya keanehan pada file pembawa.

5.2 Saran

1. Agar tidak menimbulkan noise yang mencurigakan, maka besarnya informasi yang bisa disembunyikan di dalam file wav adalah = 1/16 atau 6.25 % dari besarnya ukuran file pembawa.
2. Penggunaan kata kunci sebaiknya cukup panjang dan mudah diingat.
3. Kerahasiaan file pembawa (file wav) yang asli perlu dijaga, agar pihak lain tidak dapat memperbandingkannya dengan file terlabel.
4. Perlunya pengembangan kunci rahasia yang digunakan, misalnya penggunaan kunci asimetris untuk lebih meningkatkan keamanan informasi yang dirahasiakan.

UNIT PELAKSANA TEKNIS PERPUSTAKAAN STTTELKOM

Daftar Pustaka

[1] Eric Metois, *Audio Watermarking and Applications*, September 1999.

[2] I.W.P. Agung, *Digital Watermarking for Multimedia*, M.Phil-Ph.D. Transfer Report, University of Surrey UK, September 2000.

[3] K Matsui dan K. Tanaka, *Video – Steganography : How to Secretly Embed a Signature in a Picture,* Journal Of The Interactive Multimedia Association Intellectual Property Project, Vol.1, No.1, pp. 187 205, January 1994.

[4] L. Boney A.H. Tewfik, dan K.N. Hamdy, *Digital Watermarks for Audio Signals*, Department Of Electrical Engineering University Of Minnesota, Minneapolis, March 27, 1996.

[5] M. Csele, *COMP 630 Wav File Format Description,* <http://www.technology.niagarac.on.ca/courses/comp630/WavFileFormat.htm> , Communications and Information Technology Division Niagara College Of Applied Arts and Technology, Ontario Canada.

[6] Martin, Christoper G., *Digital Image Watermarking Techniques,* Master Of Science in Computer Sciences Thesis, Rochester Institute Of Technology, 23 May 2000.

[7] W. Bender, D. Gruhl, N. Morimoto, dan A. Lu, *Techniques For Data Hiding,* IBM Systems Journal, Vol.35, NOS 3&4, 1996.

[8] Johnson, Neil F., *Steganography : Introduction, Purpose, and Structure,* <http://www.jjtc.com/stegdoc/stegdoc.html>, Center Of Secure Information Systems George Mason University.

[9] A. Menezes, P. Van Oorschot dan S Vanstone, *Handbook Of Applied Cryptography,* CRC Press Inc., Florida : 1996.

[10] Anderson, Ross J. dan Petitcolas, Fabien A.P., *On The Limit Of Steganography,* IEEE Journal Of Selected Areas in Communications – Special Issue on Copyright & Privacy Protection, 16(4) : 474-481, May 1998.

STT Telkom 2005

[11] G. Voyatzis dan I. Pitas, *Problems and Challenges in Multimedia Networking and Content Protection,* Trends and Important Challenges in Signal Processing, 1998.

[12] Schneier, Bruce., *Applied Cryptography,* 2nd Editions, John Willey and Sons Inc., Illionis : 1996.

[13] Tinder, Richard F., *Digital Engineering Design : A Modern Approach,* Prentice-Hall Inc., New Jersey, 1991.

[14] http://www.watermarkingworld.org

Telkom University

STT Telkom 2005