

IMPLEMENTASI PENYEMBUNYIAN DATA MENGGUNAKAN METODE AUDIO STEGANOGRAFI

Muhammad Agus Sunandar¹, Wiro Sugeng Jatniko²

¹²Teknik Informatika, STT Wastukencana

Abstrak

Privasi data pada dokumen setiap orang perlu dilindungi kerahasiaannya. Hal ini perlu dilakukan untuk menjaga data tersebut agar tidak di akses oleh pihak lain yang tidak berkepentingan. Audio Steganografi merupakan metode keamanan untuk melindungi informasi, dengan pengkodean data agar dapat disebarkan ke setiap spectrum frekuensi audio. Audio Steganografi dapat melindungi data dari penyadapan, kerusakan, dan pemalsuan data.

Kata Kunci: Audio Steganografi, Data, Privasi.

PENDAHULUAN

Penggunaan komunikasi data sudah menjadi hal yang penting untuk kita sebagai makhluk sosial. Banyaknya kebutuhan dalam pengiriman data menuntut jaminan keamanan data yang dikirimkan. Karena sejatinya data itu merupakan kumpulan dari pada fakta-fakta yang dapat diolah menjadi informasi (Moh.Nazir,2005) maka informasi yang disajikan harus tepat waktu, akurat, lengkap dan konsisten.

Penelitian ini mengacu pada penelitian terdahulu mengenai studi penyisipan pesan pada arsip suara ini, menggunakan metode steganografi sederhana yaitu LSB. Cara kerja metode ini dengan mengganti *least significant bit* dari setiap sampling point dengan rentetan bit binary dari data yang disembunyikan. Akan tetapi masih banyaknya noise yang dihasilkan dari metode LSB tersebut. Sehingga diusulkan penggunaan metode Audio Steganografi dengan cara mengkodekan data sehingga dapat disebarkan ke setiap spectrum frekuensi audio. Metode audio steganografi yang diusulkan ini bertujuan untuk mempersembahkan karya ilmiah berupa perangkat lunak keamanan bagi pengguna komputer untuk digunakan sebagai langkah pengamanan data maupun informasi.

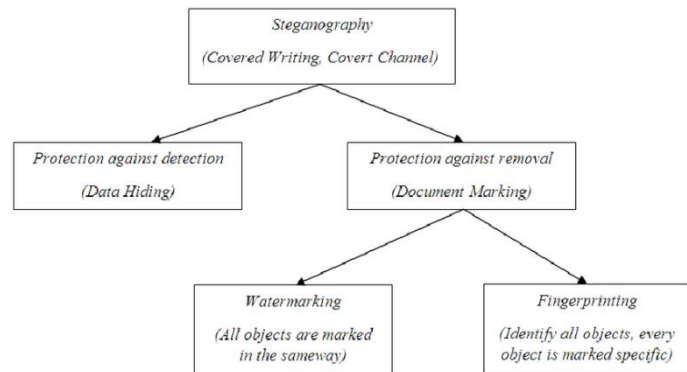
METODE

Metode Audio Steganografi merupakan fokus penelitian pada teknik penyembunyian data untuk keamanan data pribadi.

Metode Steganografi

Menurut Rinaldi Munir, steganografi merupakan teknik penyembunyian data rahasia ke dalam sebuah wadah (media) sehingga data yang disembunyikan sulit dikenali oleh indera manusia.

Pembagian Steganografi



Gambar 1 Cabang Steganografi

Berdasarkan pada *tree diagram* diatas *teganografi* terbagi menjadi dua model, yaitu :

1. Proteksi terhadap deteksi untuk teknik penyembunyian data
Model ini digunakan untuk piranti keamanan dalam suatu pengiriman dokumen melalui media internet atau yang lainnya.
2. Proteksi terhadap kehilangan untuk teknik pemberian tanda terhadap data

Model ini digunakan dalam media *secure digital* atau steganografi yang berfungsi sebagai penanda hak cipta (*copyright*) agar tidak dapat dimusnahkan maupun digandakan oleh pihak lain yang tidak bertanggung jawab.

Metode Audio Steganografi

Audio steganografi merupakan perkembangan ilmu dari steganografi. Ada dua buah proses dalam steganografi, yakni proses penyisipan pesan dan proses ekstrasi pesan. Proses penyisipan pesan membutuhkan masukan media penyisipan, pesan yang akan disisipkan dan kunci. Keluaran dari proses penyisipan ini adalah media yang telah berisi pesan. Sedangkan ekstrasi membutuhkan masukan media yang telah berisi pesan. Keluarannya adalah pesan yang telah disisipkan.

Ada beberapa cara untuk mengaplikasikan steganografi pada *file* audio yaitu :

1. Low Bit coding

Teknik ini bekerja dengan cara mengganti (*Least Significant Bit*) LSB input setiap samplingnya dengan data yang dikodekan.

2. Phase coding

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

3. Spread Spectrum

Spread spectrum atau penyebaran *spectrum* merupakan metode yang bekerja dengan cara mengkodekan pesan dan disebarkan ke setiap *spectrum* frekuensi yang memungkinkan.

4. Echo Hiding

Metode ini digunakan dengan cara menyembunyikan pesan melalui teknik *echo*. Pesan disembunyikan dengan memvariasikan tuga parameter dalam *echo*, yaitu besar *amplitude* awal, tingkat penurunan *atenuasi* dan *offset*.

HASIL DAN PEMBAHASAN

Perencanaan

Tahapan perencanaan meliputi kebutuhan sistem yang disesuaikan dengan aturan-aturan yang ada pada audio steganografi. Berikut ini merupakan *project definition* dari kebutuhan system :

1. Carrier File : file yg berisi pesan rahasia
2. Stego-medium : media yang digunakan untuk membawa pesan rahasia
3. Payload : informasi yang akan disembunyikan

Kebutuhan sistem

Kebutuhan meliputi batasan minimal dalam kelengkapan komputer yang akan digunakan pada aplikasi penyembunyian informasi ini, sebagai berikut:

- a. Sistem Operasi : Microsoft Windows XP
- b. Aplikasi Pendukung : Sound Forge
- c. Pemograman : Visual Basic 6.0
- d. Format Citra Digital : WAV
- e. Sumber Informasi Disembunyikan : TXT

Cara Menggunakan Aplikasi

Ada beberapa tahapan yang perlu dilakukan oleh *user* untuk menggunakan Aplikasi ini. Berikut ini merupakan tahapan-tahapan yang perlu dilakukan , yaitu:

1. Merubah *file* berektensi DOC ke *file* TXT .
2. Melakukan *encode Audio Steganograf*, yaitu menyisipkan atau menyembunyikan *file* TXT ke *file* WAV, *user* yang sudah menyimpan informasi dalam *file* TXT akan disembunyikan pada *file* WAV lalu diberi *code* atau *password* dan kemudian *file* WAV yang sudah tersisipi oleh *file* TXT akan disimpan kembali untuk di *shared* atau hanya untuk keamanan pribadi.
3. Melakukan *Decode Audio Steganografi*, yaitu pengembalian *file* WAV atau Mp3 yang sudah tersisipi oleh *file* TXT , dimana *user* yang menyimpan informasi pada *file* TXT yang disisipkan pada *file* WAV/Mp3 akan dikeluarkan dari *file* WAV.Mp3 tersebut.

- Melakukan proses merubah *file* berektensi TXT ke *file* DOC, yaitu mengembalikan *file* berektensi TXT ke *file* berektensi DOC, *user* yang sudah mengubah *file* DOC menjadi *file* TXT akan dikembalikan menjadi *file* DOC.

- Hasil dari aplikasi audio steganografi ini akan sulit dikenali ataupun diidentifikasi oleh orang lain, karena mempunyai format Mp3.

Pengujian Perangkat Lunak

Tabel 1 Pengujian Peerangkat Lunak

NO	Fungsi	Output	Hasil
1	Memberikan kemudahan dalam proses <i>encrypt</i> informasi.	Sistem memberikan hasil proses <i>encrypt</i> yaitu <i>chiphertext</i> .	Berhasil
2	Memberikan Kemudahan dalam proses <i>decrypt</i> informasi.	Sistem memberikan hasil proses <i>decrypt</i> yaitu <i>plaintext</i> .	Berhasil

SIMPULAN

Berdasarkan hasil studi penelitian yang dilakukan, maka di dapatkan hasil mengenai keamanan data atau informasi yang menggunakan metode audio steganografi:

- Kunci atau *password* dan *code* adalah akses awal untuk menembus sebuah informasi yang terdapat didalamnya, maka audio steganografi adalah metode yang relevan digunakan untuk melindungi sekumpulan *password* dan *code*.
- Penyembunyian informasi pada aplikasi audio steganografi sangat mudah dan aman untuk para *user* yang kegiatan atau aktivitas kesehariannya berhubungan dengan dunia internet.
- Keamanan pada audio steganografi ini sangat aman karena mempunyai dua fase proses penyembunyian.
- Aplikasi audio steganografi ini memiliki *size* cukup kecil dapat digunakan pada komputer dengan spesifikasi standar dan penggunaannya yang tidak menghabiskan banyak waktu.

DAFTAR PUSTAKA

- Aji (2010) *Prinsip dan Siklus Hidup Keamanan Informasi*. Yogyakarta: GAVA MEDIA.
- Beranda (2011) *Pengamanan Total Data dan Informasi Penting*. Bandung: Informatika.
- Darsono (2010) *Filsafat Ilmu*. Jakarta: MIZAN.
- Nazir, M. (2005) *Metode Penelitian*. Jakarta: GHALIA INDONESIA.
- Niel F Johnson, Zoran Duric, S. J. (2000) *Information Hiding Steganography and Watermarking Attack and Countermeasures*. London: KLUWER ACADEMIC PUBLISINER.
- Riko (2006) *Metode Parati Coding Versus Metode Spread Spectrum pada Audio Steganografi*. Bandung: Paper.
- Rizky, S. (2011) *Konsep Dasar Rekayasa Perangkat Lunak*. Jakarta: Prestasi Pustaka Publisher.
- Soetam (2011) *Konsep Dasar Rekayasa Perangkat Lunak*. Jakarta: Prestasi Pustaka Publisher.

