STMIK GI MDP

Program Studi Teknik Informatika
Skripsi Sarjana Komputer
Semester Genap Tahun 2009/2010

PENGEMBANGAN APLIKASI STEGANOGRAFI UNTUK PENYISIPAN BERKAS TEKS KE DALAM BERKAS SUARA

Andrie Gunawan 2002250087
Muhamad Efi Fahlawi 2006250505

Abstrak

Keamanan data dan informasi berkembang sangat luas dan pesat pada saat ini. Untuk menangani permasalahan-permasalahan seputar keamanan data dan informasi, sebuah metode yang disebut Steganografi telah dikembangkan. Steganografi dapat menyembunyikan data atau informasi rahasia kedalam suatu media lain tanpa merusak kualitas media pembawa tersebut, sehingga kerahasiaan data dan informasi tersebut sangat sulit diketahui oleh orang yang tidak berhak.
Pada penelitian ini, penulis membuat suatu aplikasi steganografi dengan memanfaatkan berkas suara untuk menyisipkan data teks yang bersifat rahasia. Metode yang digunakan pada penelitian ini adalah metode *Least Significant Bit* (LSB). Sampel yang akan digunakan untuk uji coba penelitian ini berupa data teks dengan kapasitas yang berbeda dan berkas suara dengan format wav.
Hasil akhir yang dicapai pada penelitian ini adalah membuat suatu aplikasi yang dapat menyisipkan data teks kedalam berkas suara tanpa merusak kualitas dari berkas suara tersebut karena tidak ada perubahan yang sangat signifikan pada berkas suara tersebut. Data teks yang telah disisipkan tersebut juga dapat diekstraksi kembali.

Kata kunci :
Berkas suara wav, Steganografi, LSB (*Least Significant Bit*), DELPHI 7

Pernyataan Keaslian Skripsi

Pernyataan Penyusunan Skripsi

Kami, Andrie Gunawan,
Muhamad Efi Fahlawi,

Dengan ini menyatakan bahwa Skripsi yang berjudul :

PENGEMBANGAN APLIKASI STEGANOGRAFI UNTUK PENYISIPAN BERKAS TEKS KE DALAM BERKAS SUARA

adalah benar hasil karya kami dan belum pernah diajukan sebagai karya ilmiah, sebagian atau seluruhnya, atas nama kami atau pihak lain.

Penulis,

Andrie Gunawan
2002250087

Muhamad Efi Fahlawi
2006250505

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Dewasa ini, pertukaran informasi di internet telah menjadi bagian yang penting dalam perkembangan teknologi informasi di seluruh dunia. Perkembangan dibidang Teknologi Informasi (TI) saat ini memberikan kemudahan manusia untuk melakukan aktifitasnya. Termasuk juga bertukar informasi dalam bentuk *file* melalui jaringan komputer menjadi hal yang biasa di era komputerisasi saat ini. Banyak diantara *file* tersebut bersifat rahasia dan sangat penting, dan tidak boleh diketahui oleh pihak lain. Seiring dengan perkembangan teknologi informasi tersebut, semakin berkembang pula teknik kejahatan berupa perusakan maupun pencurian data oleh pihak yang tidak memiliki wewenang atas data tersebut. Ada beberapa bentuk penyerangan terhadap data dan informasi, seperti *hacker*, *cracker, trojan force attack*, dan lain-lain. Hal tersebut tentu saja membuat media internet bukanlah media yang aman untuk pertukaran informasi. Seseorang bisa saja menyadap aliran data pengiriman *e-mail* penting atau bahkan mengganggu transaksi *online*.

Hingga saat ini ada berbagai macam upaya yang telah dilakukan untuk menjaga keamanan data dan mengatasi serangan-serangan tersebut. Salah satu

diantaranya adalah dengan menggunakan teknik kriptografi. Sesuai perkembangan zaman, teknik kriptografi klasik berubah menjadi teknik kriptografi modern yang beroperasi pada satuan bit atau byte. Namun dengan kriptografi, walaupun makna suatu pesan menjadi hilang atau kacau, keberadaan akan pesan rahasia tersebut masih diketahui. Hal tersebut membuat penyadap informasi menyadari adanya pesan rahasia yang disembunyikan, dan mengundang kriptanalis untuk melakukan kriptanalisis. Selain kriptografi, ada lagi satu teknik penyembunyian pesan yaitu steganografi. Steganografi bisa dikatakan sangat kontras dengan kriptografi. 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.

Steganografi modern menggunakan berkas digital untuk menampung pesannya. Berkas digital yang digunakan untuk penampung bisa bervariasi, mulai dari berkas teks, citra, suara (*audio*), atau bahkan *video klip* (*audio-video*). Steganografi juga sering disebut sebagai langkah setelah kriptografi karena pada kenyataannya, pesan yang disembunyikan sering dienkripsi terlebih dahulu. Tiap teknik steganografi biasanya berbeda tergantung jenis berkas pembawa yang digunakan. Beberapa teknik yang sering digunakan diantaranya *Spatial Domain* dan *Transform Domain*. Dari beberapa teknik tersebut, yang paling sering digunakan adalah teknik *Least Significant Bit (LSB)* yang termasuk dalam *Teknik Spatial Time*, karena kemudahan dalam

implementasinya. Dalam implementasinya ada banyak bahasa pemrograman yang dapat digunakan, namun pada penelitian ini, Penulis menggunakan bahasa pemrograman Delphi 7.

1.2 Perumusan Masalah

Dari latar belakang yang telah dikemukakan pada Pendahuluan dan dengan memanfaatkan bahasa pemrograman *Borland* Delphi *7* dan teknik steganografi, maka dapat diambil suatu perumusan masalah yaitu bagaimana membuat aplikasi yang dapat melindungi keamanan data teks yang bersifat rahasia yang disisipkan pada berkas *audio* format wav dengan metode *Least Significant Bit (LSB)*, sehingga kerahasiaan data lebih terjamin dan tidak menimbulkan kecurigaan bagi pihak lain.

1.3 Ruang Lingkup

Dalam pembuatan skripsi ini, untuk mengatasi permasalahan yang ada maka penyusun membatasi permasalahan sebagai berikut:

1. Aplikasi steganografi ini hanya menangani berkas suara yang belum dikompresi (*format* .wav).
2. Data yang akan disisipkan berupa berkas teks dan maksimal bit karakter yang bisa disisipkan tidak melebihi batas maksimum.

1.4 Tujuan dan Manfaat Penelitian

1.4.1. Tujuan Penelitian

Tujuan penyusunan skripsi ini adalah:

1. Membangun sebuah aplikasi yang dapat melakukan penyembunyian data teks rahasia ke dalam berkas suara.
2. Menerapkan Teknik Steganografi pada berkas suara digital format WAV.

1.4.2. Manfaat Penelitian

Manfaat yang ingin dicapai dari penelitian ini adalah agar aplikasi yang dibuat mampu menyimpan berkas teks yang bersifat penting dan rahasia agar tidak dapat dibaca oleh orang yang tidak diinginkan.

1.5 Metodologi Penelitian

Metodologi penelitian yang digunakan dalam penelitian ini adalah bersifat deskripsi studi kasus, yaitu suatu metode untuk mengemukakan masalah dengan mengumpulkan data-data dan penyajian data yang tujuannya menggambarkan karakteristik suatu keadaan atau objek penelitian dan mengambil suatu kesimpulan yang telah dilakukan.

Dalam pengumpulan data untuk penelitian digunakan beberapa cara yaitu :

1. Studi Pustaka, dengan mempelajari hal-hal yang berhubungan dengan penelitian yang dilakukan. Sumber kepustakaan diambil

dari buku-buku yang berkaitan dengan keamanan komputer dan informasi yang juga dapat diperoleh dari internet.

2. Wawancara, dengan mengajukan pertanyaan kepada narasumber yang berkompeten dibidang pembuatan perangkat lunak.

1.6 Metodologi Penyelesaian Masalah

Dalam penulisan skripsi ini, ada beberapa tahapan yang dilakukan yaitu

a Analisis

Menganalisa kebutuhan program yang akan dibuat. Pada tahap analisis dilakukan pengumpulan data yang di dapat dengan cara mempelajari prosedur dalam teknik steganografi.

b Desain

Memperoleh spesifikasi rancangan program steganografi dengan berkas suara digital yang diperlukan untuk tahapan selanjutnya.

c Pemrograman

Memperoleh spesifikasi program steganografi dengan berkas suara digital yaitu tentang bagaimana program akan bekerja.

d Pengujian

Mengevaluasi kemampuan program steganografi dengan berkas suara digital yang telah dibuat.

e Implementasi

Mengimplementasikan aplikasi steganografi yang telah dibuat.

BAB 5

PENUTUP

5.1 Kesimpulan

Dari hasil pengujian yang dilakukan pada Bab 4, maka dapat Penulis simpulkan sebagai berikut :

1. Perubahan spectrum berkas suara sebelum dan setelah penyisipan pesan tidak terlihat.
2. Tidak terjadi kerusakan pada berkas suara yang telah disisipkan pesan.
3. Berkas suara yang telah disisipkan pesan sama *properties*-nya dengan berkas suara sebelum disisipkan pesan, sehingga kecurigaan akan adanya pesan dapat dihindari (*Imperceptability*).
4. Kualitas suara yang dihasilkan setelah dilakukan penyisipan pesan hampir sama dengan kualitas suara dari berkas suara sebelum penyisipan pesan. Sesuai dengan kriteria steganografi (*Fidelity*).
5. Pesan yang telah disisipkan dapat diungkapkan kembali dengan hasil yang sama dengan pesan pada saat disisipkan. Sesuai dengan kriteria *Recovery* pada steganografi yang baik.
6. Waktu yang dibutuhkan untuk menyisipkan pesan berbanding lurus dengan besarnya kapasitas pesan. Semakin besar kapasitas pesan, semakin lama waktu proses penyisipan.

5.2 Saran

Dalam melakukan perancangan aplikasi Steganowave ini, penulis memiliki keterbatasan waktu, biaya, dan sumber pustaka sehingga aplikasi Steganowave ini memiliki beberapa kekurangan. Untuk itu Penulis menyarankan beberapa point penting untuk lebih meningkatkan kualitas aplikasi steganowave diantaranya sebagai berikut :

1. Untuk lebih meningkatkan keamanan pesan, maka dianjurkan untuk melakukan enkripsi pesan sebelum disisipkan
2. Aplikasi diharapkan agar dapat ditingkatkan sehingga tidak hanya dapat menyisipkan pesan teks namun juga pesan lain seperti gambar.
3. Agar dapat meningkatkan kapasitas pesan yang disisipkan, maka terlebih dahulu dilakukan pengkompresian pesan.