

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan internet telah memberikan kemudahan yang sangat besar dalam komunikasi dan transportasi data, mempermudah dan mempercepat akses informasi, meningkatkan portabilitas, efisiensi dan keakuratan informasi. Namun disisi lain hal ini juga membuka kemungkinan yang lebih besar terhadap pembajakan data yang dikirim, memodifikasi isi data, dan penyebarluasan salinan yang tidak sah.

Dewasa ini perkembangan komunikasi dan komputer telah memungkinkan seseorang melakukan berbagai transaksi komunikasi baik untuk kepentingan bisnis, pendidikan sampai hiburan. Selain itu mereka juga dapat dengan bebas saling mengirimkan informasi dengan rekannya secara *on-line*. Kegiatan saling bertukar informasi tersebut tentu saja akan menimbulkan resiko bilamana informasi yang bersifat rahasia dan berharga dapat diakses bebas oleh orang yang tidak berhak (*unauthorized persons*).

Untuk mengatasi permasalahan tersebut maka diperlukan sistem keamanan secara khusus pada saat penyimpanan dan transmisi data, salah satu caranya adalah steganografi. Steganografi sendiri berasal dari bahasa Yunani yang berarti tulisan yang tertutup/tersamar (*covered letter*).

Steganografi diartikan sebagai ilmu yang mempelajari, meneliti, dan mengembangkan seni untuk menyembunyikan suatu informasi. Ada berbagai teknik dalam sistem steganografi salah satunya adalah dengan teknik penyisipan pesan.

Digital steganografi memerlukan suatu media sebagai tempat menyembunyikan informasi. File teks merupakan salah satu media yang paling diminati karena ukuran filenya yang relatif kecil apabila dibandingkan dengan file audio, citra, dan video. Tetapi jika data yang akan disisipkan dalam ukuran yang besar maka membutuhkan memori penyimpanan yang besar pula. Jadi salah satu cara untuk mewujudkan hal tersebut file teks sebelum disisipkan, dikompres terlebih dahulu. Semakin kecil ukuran file, semakin cepat proses waktu yang dibutuhkan untuk pengiriman data.

Dokumen dapat menyembunyikan informasi melalui penyisipan pesan rahasia ke dalam teks yang tidak teracak (null cipher) dalam dokumen tersebut. Bentuk-bentuk komunikasi yang mencurigakan akan terdeteksi dan hanya pesan tidak terenkripsi saja yang akan dibiarkan lewat. Untuk mengatasi hal itu maka pesan yang terenkripsi dan terkompres disisipkan kedalam media yang tidak terenkripsi sehingga tidak menimbulkan kecurigaan.

Dalam penyusunan skripsi sebelumnya yang telah disusun oleh Sukrisno berjudul **"Implementasi Steganografi Teknik EOF dengan Gabungan Enkripsi Rijndael, Shift Cipher dan Fungsi Hash MD5"**.

Skripsi tersebut membandingkan media file teks dan biner yang cocok sebagai media file steganografi.

Namun dari hasil penelitian sebelumnya menunjukkan kelemahan pada jenis media file teks, dimana data teks yang disisipkan terlihat dalam karakter tak terbaca dan jika disisipkan dalam *source code*, file tersebut tidak bisa di-*compile* untuk dijalankan.

Dari hasil penelitian tersebut melatarbelakangi penulis untuk menyempurnakan penelitian sebelumnya. Penulis memilih teknik penyisipan *end of line* dengan metode *whitespace* serta melakukan kompresi *Huffman* sebelum data dienkripsi menggunakan *ice mode* yang akan disisipkan ke dalam media file teks. Jadi diharapkan skripsi yang penulis susun ini bisa menyempurnakan pada penelitian sebelumnya.

1.2 Rumusan Masalah

Berdasarkan pendahuluan di atas rumusan masalah penelitian ini adalah :

1. Bagaimanakah cara membuat aplikasi steganografi berbasis metode *whitespace* dengan teknik *end of line* guna menyembunyikan file terenkrip dan terkompres pada *plaintext*?
2. Apakah media file berupa teks dan *source code* sebelum dan sesudah disisipkan data akan mengalami perubahan jika dilihat secara kasat mata?
3. Seberapa besar perubahan selisih ukuran media file terhadap jenis penyisipan data sebelum dikompres dan sesudah dikompres?

1.3 Batasan Masalah

Mengingatnya luasnya cakupan pemmasalahan maka penelitian ini dibatasi pada media *plaintext* dengan metode *whitespace* dan data dikompres menggunakan kompresi *Huffman* sebelum data dienkripsi, teknik enkripsi menggunakan *ICE mode*. Teknik penyembunyian disisipkan pada akhir setiap baris dalam media (*end of line*). Skripsi ini akan menunjukkan bagaimana algoritma dan implementasi metode *whitespace* ke dalam kode program dengan menggunakan Visual C++ sebagai operasi inti dan Visual C# sebagai form interface. Pembahasan pembuatan aplikasi steganografi terbatas pada penyembunyian data atau informasi yang bersifat rahasia untuk data terenkripsi dan terkompres kedalam suatu media file teks yang berupa *plaintext* antara lain *.html, *.c, *.rtf, *.txt.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah membuat aplikasi steganografi menggunakan metode *whitespace* dengan teknik EOL untuk pesan yang terenkripsi dan terkompres dalam *plain text*.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian yang dilakukan antara lain :

1. Menghasilkan aplikasi steganografi untuk pesan terenkripsi dan terkompres dalam *plaintext* yang dapat dipelajari dan dikembangkan lebih lanjut.

2. Dapat mengirim data rahasia pada *plain text* tanpa menimbulkan kecurigaan.

1.6 Metodologi Penelitian

Penulis menggunakan beberapa metode pengumpulan data, yaitu:

1. Metode Kepustakaan

Penulis melakukan studi literatur dari berbagai artikel, online help perangkat lunak dan situs-situs internet

2. Metode eksperimental

Melakukan perancangan program, menerapkan rancangan program kedalam kode program, melakukan pengujian dan analisis serta hasil kerja dengan program yang telah dibuat pada *plain text*.

3. Metode Wawancara

Penulis menanyakan langsung ataupun lewat *chat* kepada peneliti sebelumnya untuk membandingkan dan menyempurnakan skripsi yang penulis buat dengan skripsi terdahulu.

1.7 Sistematika Penulisan

Sistematika penulisan laporan di bawah ini dibagi menjadi lima bab meliputi :

BAB I PENDAHULUAN

Bab ini berisi latar belakang masalah, batasan masalah, tujuan, manfaat, metodologi penelitian, sistematika penulisan dan jadwal kegiatan dari penulisan laporan ini.

BAB II TINJAUAN PUSTAKA DAN LANDASAN TEORI

Bab ini berisi tinjauan pustaka berupa perbandingan antara skripsi sebelumnya dengan skripsi yang penulis buat sekarang, dan dasar teori yang dipakai adalah membangun aplikasi steganografi pada media *plain text* untuk pesan terenkripsi dan terkompres. Bab ini juga membahas tentang komponen-komponen steganografi di dalam media *plain text*.

BAB III HASIL PENELITIAN DAN PEMBAHASAN

Bab ini menjelaskan hasil penelitian berupa analisis dan proses rancangan steganografi serta implementasi dengan menggunakan metode *whitespace* pada *plaintext* untuk penyisipan data terenkripsi dan terkompres kedalamnya. Dan pembahasan terhadap hasil pengujian unjuk kerja program steganografi

BAB IV PENUTUP

Bab ini berisi kesimpulan dari hasil penelitian yang telah dilakukan dan saran-saran pengembangan penelitian ini untuk penelitian selanjutnya.

