BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi pada dua dasawarsa terakhir ini demikian pesat, terutama bidang teknologi informasi. Pertukaran informasi pada saat ini sangat berbeda dengan era puluhan tahun yang lalu. Dahulu, informasi disampaikan dalam bentuk fisik seperti surat, namun kini dunia telah berubah berkat hadirnya internet. Dengan internet, informasi dapat dikirimkan dengan cepat tanpa mengenal batas-batas geografis. Namun demikian, informasi yang dikirimkan dapat disadap ditengah jalan oleh pihak yang tidak diinginkan. Ada banyak teknik untuk mencegat informasi yang dikirimkan melalui jaringan publik seperti internet. Hal ini lazim disebut sebagai serangan "*man in the middle*", dimana ada pihak lain diantara pengirim dan penerima yang mengambil informasi yang dikirimkan. Perangkat lunak untuk membaca aliran data dalam jaringan biasa disebut "*packet sniffer*". Packet sniffer dapat digunakan untuk mengamati data yang dikirimkan antara pengirim dan penerima.

Proses penyadapan tersebut tidak rumit, sehingga dapat dilakukan bahkan oleh orang dengan pengetahuan yang minim, atau biasa disebut "*script kiddies*". Hal ini menjadi sangat berbahaya, bila informasi yang dikirimkan tersebut dinilai sensitif, seperti rahasia negara atau perusahaan.

Untuk mencegah jatuhnya informasi penting ke tangan yang salah, maka digunakanlah teknik kriptografi, yaitu proses mengubah (*encrypt*) suatu informasi (*plaintext*) dengan suatu algoritma khusus (*cipher*) dengan tujuan agar informasi tersebut tidak dapat dibaca (*decrypt*) tanpa bantuan kunci (*key*) khusus. Kriptografi telah lama digunakan untuk mengamankan komunikasi di berbagai negara, terutama militer, organisasi-organisasi tertentu, serta individu yang memiliki kepentingan yang sangat mendesak akan kerahasiaan..

Teknik enkripsi memiliki beberapa kelemahan, salah satunya yaitu mengundang perhatian. Menggunakan logika, mudah ditebak bahwa file yang dilindungi enkripsi pasti mengandung informasi yang penting. Pesan yang dienkripsi juga menyolok dan mengundang perhatian. Enkripsi juga dapat dipecahkan menggunakan teknik *brute force,* maupun *dictionary attack.*

Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Berbeda dengan enkripsi, steganografi kurang mengundang kecurigaan karena pesan rahasia disembunyikan dalam file yang "normal", seperti file MP3 atau bitmap. Karena keunggulan proses steganografi tersebut, maka pada penelitian ini akan dikembangkan sebuah perangkat lunak untuk menyembunyikan informasi berupa file gambar atau teks, didalam file lain. Dengan teknik ini, diharapkan informasi yang penting dapat dipertukarkan didalam file gambar biasa tanpa mengundang kecurigaan, sehingga mencegah informasi tersebut jatuh ke pihak yang tidak berwenang.

1.2 Rumusan Masalah

Dari uraian latar belakang diatas, dapat dirumuskan masalah pada penelitian ini adalah sebagai berikut :

1. Bagaimana membangun aplikasi untuk menyembunyikan pesan rahasia ke dalam file gambar (BMP) dan audio terkompresi (MP3)
2. Bagaimana membangun aplikasi untuk mengambil kembali pesan rahasia dari dalam file
3. Seberapa besar perubahan ukuran media file yang telah disiapkan data dibandingkan dengan file aslinya.
4. Bagaimana perbedaan kualitas file gambar dan suara sebelum dan setelah dilakukan penyisipan
5. Bagaimana aplikasi akan bereaksi saat menerima input yang tidak diharapkan seperti teks bahasa China (unicode), kode program, dan sebagainya

1.3 Batasan Masalah

Untuk membatasi ruang lingkup pembahasan agar tidak keluar dari topik permasalahan, maka masalah pada penelitian ini dibatasi sebagai berikut :

1. Pesan rahasia yang akan disisipkan berupa teks ANSI, bukan unicode
2. File perantara yang digunakan menggunakan format bitmap (BMP) atau MP3

3. Aplikasi menggunakan algoritma Least Significant Byte untuk menyembunyikan pesan
4. Aplikasi terdiri dari form penyisipan, form ekstraksi, analisis data sebelum dan sesudah penyisipan, serta petunjuk penggunaan

1.5 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Menerapakan pengetahuan yang telah dipelajari selama kuliah.
2. Membangun sebuah aplikasi untuk mengamankan pertukaran pesan, dengan cara menyembunyikan pesan tersebut kedalam file perantara
3. Memenuhi persyaratan dalam menyelesaikan gelar sarjana komputer

1.6 Metode Penelitian

Metode yang digunakan sebagai acuan untuk pengumpulan data adalah

Studi Pustaka

Studi pustaka dilakukan dengan cara mempelajari sumber-sumber mengenai steganografi, baik buku teks maupun internet

1.7 Jadwal Penelitian

No	KEGIATAN	OKTOBER				NOVEMBER				DESEMBER			
		I	II	III	IV	I	II	III	IV	I	II	III	IV
1	Identifikasi masalah												
2	Pengumpulan data												
3	Analisis kebutuhan sistem												
4	Membuat rancangan sistem												
5	Pembuatan Program												
6	Uji coba program (testing)												
7	Revisi konsep, disain rancangan, code program												
8	Implementasi Program												
9	Pembimbingan penulisan naskah skripsi												
10	Penulisan akhir laporan												

Tabel 1.1 Jadwal Penelitian

1.8 Sistematika Penulisan

Penulisan naskah penelitian ini disusun dalam 5 (lima) bab. Pada setiap bab akan diuraikan sebagai berikut :

BAB I : PENDAHULUAN

Dalam bab ini berisi tentang deskripsi umum isi tugas akhir skripsi yang meliputi latar belakang, batasan

masalah, tujuan penyusunan tugas akhir, metodologi penyusunan tugas akhir dan sistematika penulisa tugas akhir

BAB II : LANDASAN TEORI

Dalam bab ini berisi tentang teori konsep dasar kriptografi, steganografi, LSB, format-format gambar, serta bahasa pemrograman Delphi

BAB III : ANALISIS PERANCANGAN SISTEM

Dalam bab ini berisi tetang analisis sistem yang dilakukan dan perancangan aplikasi yang akan dibuat.

BAB IV : IMPLEMENTASI PEMBAHASAN

Dalam bab ini berisi tentang proses implementasi dan penggunaan program

BAB V : PENUTUP

Dalam bab ini berisi tentang kesimpulan dan saran.