

BAB I

PENDAHULUAN

I.1 Latar Belakang

Kemajuan cara berpikir manusia membuat masyarakat menyadari bahwa teknologi informasi merupakan salah satu alat bantu penting dalam peradaban manusia untuk mengatasi sebagian masalah dasarnya arus informasi. Teknologi informasi dan komunikasi saat ini adalah bagian penting dalam manajemen informasi. Selain memiliki potensi dalam memilah data dan mengolah menjadi informasi, teknologi informasi mampu menyimpannya dengan jumlah kapasitas jauh lebih banyak dari cara-cara *manual*. Salah satu pekerjaan manusia yang akan sangat terbantu dengan hadirnya teknologi informasi, dengan keuntungan yang ditawarkan, yaitu pekerjaan manusia dalam menyembunyikan pesan.

Saat ini teknologi kriptografi sudah dapat dipecahkan dalam sistem pengamanan pesan. Untuk itu diperlukan teknologi steganografi dalam teknik pengamanan pesan. Steganografi merupakan ilmu yang mempelajari, meneliti, dan mengembangkan seni menyembunyikan sesuatu informasi. Steganografi berasal dari bahasa Yunani yang berarti “tulisan tersembunyi”. Zaman dahulu kegiatan ini sudah sering dilakukan untuk menyampaikan pesan-pesan rahasia. Misalnya dengan cara *mentatoo* pesan rahasia di kulit kepala para pembawa pesan. Sebelumnya kepala si pembawa pesan digunduli dahulu, kemudian di *tatoo*. Setelah rambutnya tumbuh maka pesan tadi tertutup oleh rambut, kemudian si pembawa pesan dilengkapi dengan pesan palsu di tangannya sebagai umpan.

Selain itu, banyak teknik lainnya seperti penulisan dengan tinta yang tidak tampak (*invisible ink*), titik-titik mikro (*microdot*), penyusunan karakter, dan banyak lagi kejadian-kejadian besar masa lalu seperti peperangan juga terukir salah satunya dengan peran serta steganografi di dalamnya. Seiring dengan perkembangan jaman, metode steganografi semakin lama semakin berkembang.

Teknologi komputer memberikan kontribusi baru dalam revolusi menyembunyikan pesan. Steganografi pada era informasi digital merupakan teknik dan seni menyembunyikan informasi dan data digital dibalik informasi digital lain. *File* media merupakan komponen penting pada proses penyembunyian informasi ini. Dengan *file* yang terlihat sama sekali tidak mencurigakan, data anda yang sebenarnya akan tetap tidak terdeteksi dengan mata telanjang. Secara teori, semua *file* umum yang ada di dalam komputer dapat digunakan sebagai media, seperti *file* gambar berformat PNG (*Portable Network Graphics*), JPEG (*Joint Photographic Experts Group*), GIF (*Graphics Interchange Format*), BMP (*Bitmap*), atau di dalam musik MP3 (*Media Player*), atau bahkan di dalam sebuah film dengan format WMV (*Windows Media Video*) atau AVI (*Audio Video Interleave*) semua bisa dijadikan tempat bersembunyi, selama *file* media tersebut jika dimodifikasi, maka kualitas dan tampilan *file* yang sesungguhnya tidak akan terganggu banyak. Kemudian pada data digital, teknik-teknik yang sering digunakan dalam steganografi modern antara lain : Modifikasi *Least Significant Bit* (LSB), *Mask and Filtering*, Algoritma kompresi dan transformasi, dan Teknik *Pixel Mapping* yang dikenal dengan Metode Modifikasi *RedGreenBlue* (RGB) *Level*.

Atas dasar uraian diatas, maka pada penulisan skripsi ini akan membahas mengenai bagaimana mengamankan suatu pesan dengan menyisipkan (menyembunyikan) kedalam pesan lainnya yaitu *file* gambar dengan menggunakan algoritma LSB (*Least Significant Bit*) pada suatu aplikasi steganografi.

I.2 Ruang Lingkup Permasalahan

I.2.1 Identifikasi Masalah

Berdasarkan analisis judul yang telah diambil, maka identifikasi masalahnya adalah :

1. Keamanan teks sangat penting dalam bisnis besar maupun menengah saat ini.
2. Masih kurangnya sistem keamanan yang digunakan pada teks didalam gambar.
3. Sistem keamanan yang digunakan saat ini masih rentan terhadap pembobolan (*hacking*).

I.2.2 Perumusan Masalah

Adapun rumusan masalah yang penulis lakukan dalam menyusun skripsi yang dibahas diatas, sebagai berikut :

1. Bagaimana cara enkripsi pesan teks yang akan disisipkan kedalam *file* gambar ?

2. Bagaimana cara memanfaatkan *file* gambar agar dapat mengirim dan menerima pesan yang bersifat rahasia ?

I.2.3 Batasan Masalah

Mengingat luasnya permasalahan yang ada, maka penulis membuat batasan masalah sebagai berikut :

1. Karakter yang akan dienkripsi hanya yang terdapat pada *keyboard*.
2. Format pesan yang akan disisipkan berupa *.txt* atau *notepad*.
3. Format gambar yang akan disisipkan teks hanya JPG/JPEG (*Join Photographic Experts Group*).
4. Pengiriman pesan tidak menggunakan media *internet* melainkan media *hard drive*.
5. Hasil gambar yang telah disisipkan teks hanya berupa format PNG (*Portable Network Graphics*).
6. Bahasa pemrograman yang dipakai adalah *Java* dengan *Netbeans* IDE.

I.3 Tujuan dan Manfaat

I.3.1 Tujuan

Adapun tujuan dari penulisan skripsi ini adalah :

1. Menghasilkan suatu aplikasi yang dapat digunakan untuk mengamankan informasi pesan teks.
2. Memudahkan pengguna untuk bertukaran pesan rahasia.

3. Menghasilkan tampilan aplikasi yang mudah dimengerti penggunaannya.

I.3.2 Manfaat

Manfaat dari penulisan skripsi dan pembuatan aplikasi tersebut adalah :

1. Pada aplikasi ini seseorang dapat mengirimkan suatu informasi rahasia dengan aman.
2. Bisa lebih mamahami bahasa pemrograman yang digunakan.
3. Lebih memahami metode *Vigenere Cipher* dan *Least Significant Bit* (LSB).

I.4 Metode Penelitian

Penulis melakukan penelitian terhadap Implementasi Kriptografi dan Steganografi pada *File Gambar Menggunakan Metode Vigenere Chiper dan LSB (Least Significant Bit)*. Implementasi pengamanan ini secara umum memiliki 4 (empat) fungsi utama sekaligus yaitu mengenkripsikan pesan, menyisipkan pesan, mendekripsikannya kembali dan pesan pun diekstraksi. Adapun tahapan metodologi peneLitian sebagai berikut :

1. Metode pengumpulan data, metode yang digunakan dalam pengumpulan data adalah studi pustaka dan *Research and Site Visitis* (Penelitian dan Mengunjungi Situs).

2. Alur penelitian :

- a. Perencanaan Sistem / Planning, kegiatan yang dilakukan pada tahapan ini yaitu dengan mengenali dan mendefenisikan masalah pengamanan pesan dan mencari alternatif pemecahannya.
- b. Analisa Sistem, analisa terhadap kebutuhan perangkat keras dan perangkat lunak merupakan proses pengumpulan sistem yang diinginkan. Dengan adanya analisis ini, diharapkan kebutuhan akan perangkat keras dan perangkat lunak dalam mengembangkan sistem akan terpenuhi. Sehingga akan menghasilkan sebuah sistem yang sesuai dengan tujuan penelitian.
- c. Implementasi Sistem dan *Coding*, pada tahap ini dilakukan proses transformasi pesan teks kebentuk kode yang dapat diimplentasikan oleh mesin. Tahap implementasi ini akan menggunakan beberapa *tool* pengembangan sistem yang meliputi mengkonversi pesan teks menjadi rangkaian bit, mengenkripsi *plaintext* dan mendekripsi *Chipertext* dengan menggunakan algoritma *Vigenere Cipher*.

I.5 Keaslian Penelitian

Pada pembuatan skripsi ini penulis akan menerangkan keaslian penelitian yang terdapat dalam jurnal yang dikutip :

Tabel I.1 Perbandingan Penelitian yang dibuat

No	Judul	Hasil Penelitian	Penelitian yang dibuat
1	ALPHA-QWERTY CIPHER: AN EXTENDED VIGENÈRE CIPHER	<i>Alpha-qwertycipher</i> bermaksud untuk memperpanjang karakter asli 26 <i>Vigenère cipher</i> ke 92 karakter huruf <i>cipher</i> sensitif termasuk angka dan beberapa simbol lain yang umum digunakan dalam Bahasa Inggris dan dapat ditulis dari <i>keyboard</i> komputer	Pada penelitian yang penulis buat karakter yang digunakan diperpanjang sebanyak 94 karakter huruf <i>cipher</i> sensitif dan dilanjutkan dengan penyisipan kedalam gambar dengan metode <i>least significant bit</i> .
2	IMAGE STEGANOGRAPHY DENGAN METODE LEAST SIGNIFICANT BIT (LSB)	Penelitian ini menghasilkan sebuah perangkat lunak untuk menyisipkan pesan teks sebagai sebuah pesan tersembunyi ke dalam sebuah citra digital. Perangkat lunak ini dibangun menggunakan bahasa pemrograman visual basic 6.0	Berbeda dengan penelitian sebelumnya, penelitian yang penulis buat saat ini tidak hanya sekedar menyisipkan pesan teks tapi juga menggunakan fungsi kriptografi didalamnya. Dan dibuat menggunakan bahasa pemrograman java yang bisa dijalankan dibeberapa sistem operasi saat ini.
3	STEGANOGRAFI GAMBAR DENGAN METODE LEAST SIGNIFICANT BIT UNTUK PROTEKSI KOMUNIKASI PADA MEDIA ONLINE	Proses embedding pesan ini terdapat 2 proses yang membangun proses embedding yaitu proses Cek data dan proses Embedding teks. Pada proses cek data, file gambar di cek apakah terdapat fleck, dimana fleck adalah tanda bahwa file gambar telah disisipkan pesan rahasia sebelumnya. Bila di dalam file gambar tidak terdapat fleck maka proses embedding teks dapat dilakukan.	Proses embedding yang penulis buat dalam penelitian ini terdapat 4 proses yaitu pertama proses cek pesan teks apakah yang dimasukan benar-benar teks atau bukan, kedua proses enkripsi, ketiga proses cek gambar apakah gambar cukup untuk menampung teks yang akan disisipkan. Terakhir proses penyisipan pesan teks kedalam gambar.

I.6 Sistematika Penulisan

Sistematika penulisan tugas akhir ini dibagi menjadi lima bab yang merangkum tiap tahapan yang penulis lakukan, antara lain:

BAB I PENDAHULUAN

Pada bab ini berisikan konsep dasar penyusunan laporan skripsi diantaranya latar belakang, identifikasi masalah, perumusan masalah, batasan masalah, tujuan dan manfaat, metodologi penelitian, keaslian penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini dibahas mengenai teori-teori yang mendukung pembahasan tentang Steganografi, Kriptografi, *Least Signifacant Bit*, *Algoritma Vigenere Cipher* dan materi – materi yang berhubungan dengan perancangan aplikasi tersebut.

BAB III ANALISA DAN DESAIN SISTEM

Pada bab ini berisikan analisa permasalahan dan kebutuhan rancangan aplikasi, serta pemodelan sistem secara fungsional.

BAB IV HASIL DAN UJI COBA

Pada bab ini berisikan gambaran rancangan aplikasi pengamanan pesan teks secara keseluruhan dan kode program, serta implementasinya yaitu menguji untuk menemukan kesalahan.

BAB V KESIMPULAN DAN SARAN

Merupakan rangkuman dari laporan skripsi berupa kesimpulan atas pembahasan laporan penulisan dan saran untuk kesempurnaan sistem yang ingin dikembangkan.