BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Jaringan komputer dan internet telah mengalami perkembangan yang sangat pesat. Teknologi ini mampu menyambungkan hampir semua komputer yang ada di dunia sehingga bisa saling berkomunikasi dan bertukar informasi. Bentuk informasi yang dapat ditukar berupa data teks, gambar, gambar bergerak, atau suara. Seiring dengan perkembangan tersebut, secara langsung ikut mempengaruhi cara kita berkomunikasi. Kalau dahulu untuk berkomunikasi pesan atau surat dengan menggunakan pos, sekarang telah banyak layanan *e-mail* di internet yang dapat mengirimkan pesan secara langsung ke penerimanya. Akan tetapi sebagai suatu jaringan publik, internet rawan terhadap pencurian data.

Steganografi sebagai suatu seni penyembunyian pesan ke dalam pesan lainnya yang telah ada sejak sebelum masehi dan kini seiring dengan kemajuan teknologi jaringan serta perkembangan dari teknologi digital, steganografi banyak dimanfaatkan untuk mengirim pesan melalui jaringan internet tanpa diketahui orang lain dengan menggunakan media digital berupa *file image*.

Penggunaan steganografi menjadi daya tarik banyak orang pada peristiwa penyerangan gedung WTC, 11 September 2001. Pada peristiwa tersebut disebutkan oleh “pejabat pemerintah dan para ahli dari pemerintahan AS” yang tidak disebut namanya bahwa “para teroris menyembunyikan peta-peta dan foto-foto target dan juga perintah untuk aktivitas teroris di ruang *chat sport*, *bulletin*

boards porno dan *web site* lainnya". Isu lainnya menyebutkan bahwa teroris menyembunyikan pesan-pesannya dalam gambar-gambar porno di *web site* tertentu. Walaupun demikian, sebenarnya belum ada bukti nyata dari pernyataan-pernyataan tersebut di atas (Andino Masaleno, 2003; Rodiah, 2004).

Kata steganografi (*steganography*) berasal dari bahasa Yunani yaitu *steganos* yang artinya tersembunyi atau terselubung dan *graphein* yang artinya menulis. Sehingga kurang lebih artinya adalah "menulis tulisan yang tersembunyi atau terselubung". Teknik ini meliputi banyak sekali metode komunikasi untuk menyembunyikan pesan rahasia.

Catatan pertama tentang steganografi ditulis oleh seorang sejarawan Yunani, Herodotus, yaitu ketika Histaeus seorang raja kejam Yunani dipenjarakan oleh Raja Darius di Susa pada abad ke-5 sebelum Masehi. Histaeus harus mengirim pesan rahasia kepada anak laki-lakinya, Aristagoras, di Militus. Histaeus menulis pesan dengan cara menato pesan pada kulit kepala seorang budak. Ketika rambut budak itu mulai tumbuh, Histaeus mengutus budak itu ke Militus untuk mengirim pesan di kulit kepalanya tersebut kepada Aristagoras.

Cerita lain tentang steganografi datang juga dari sejarawan Yunani, Herodotus, yaitu dengan cara menulis pesan pada papan kayu yang ditutup dengan lilin. Demeratus, seorang Yunani yang akan mengabarkan berita kepada Sparta bahwa Xerxes bermaksud menyerbu Yunani. Agar tidak diketahui pihak Xerxes, Demeratus menulis pesan dengan cara mengisi tabung kayu dengan lilin dan menulis pesan dengan cara mengukirnya pada bagian bawah kayu, kemudian tabung kayu ditutupi kembali dengan lilin.

Teknik steganografi yang lain adalah tinta yang tak terlihat. Teknik ini pertama digunakan pada zaman Romawi kuno yaitu dengan menggunakan air sari buah jeruk, urine, atau susu sebagai tinta untuk menulis pesan. Cara membacanya adalah dengan dipanaskan di atas nyala lilin. Tinta yang sebelumnya tidak terlihat, ketika terkena panas akan berangsur-angsur menjadi gelap, sehingga pesan dapat dibaca. Teknik ini pernah juga digunakan pada Perang Dunia II.

Pada abad ke-20, steganografi benar-banar mangalami perkembangan. Selama berlangsung perang Boer, Lord Boden Powell (pendiri gerakan kepanduan) yang bertugas untuk membuat tanda posisi sasaran dari basis artileri tentara Boer, untuk alasan keamanan, Boden Powell menggambar peta-peta posisi musuh pada sayap kupu-kupu agar gambar-gambar peta sasaran tersebut terkamuflase.

Perang Dunia II adalah periode pengembangan teknik-teknik baru steganografi. Pada awal Perang Dunia II walaupun masih digunakan teknik tinta yang tak terlihat, namun teknik-teknik baru mulai dikembangkan seperti menulis pesan rahasia ke dalam kalimat lain yang tidak berhubungan langsung dengan isi pesan rahasia tersebut. Kemudian teknik menulis pesan rahasia ke dalam pita koreksi karbon mesin ketik, dan juga teknik menggunakan pin berlubang untuk menandai kalimat terpilih yang digunakan dalam pesan. Teknik terakhir adalah *microdots* yang dikembangkan oleh tentara Jerman pada akhir Perang Dunia II.

Dari contoh-contoh steganografi konvensional tersebut dapat dilihat bahwa semua teknik steganografi konvensional berusaha merahasiakan komunikasi dengan cara menyembunyikan pesan ataupun mengamuflase pesan.

Maka sesungguhnya prinsip dasar dalam steganografi lebih dikonsentrasikan kepada kerahasiaan komunikasinya bukan pada datanya.

Seiring dengan perkembangan teknologi terutama teknologi komputasi, steganografi merambah juga ke media digital. Walaupun steganografi dapat dikatakan mempunyai hubungan erat dengan kriptografi, tetapi kedua metode ini sangat berbeda. Kriptografi mengacak pesan sehingga tidak dimengerti, sedangkan steganografi menyembunyikan pesan sehingga tidak terlihat (Andino Masaleno, 2003: 3).

Tugas akhir ini membahas pengenalan steganografi dengan menggunakan metode *Least Significant Bit* (*LSB*) serta pembuatan aplikasinya dengan *Borland Delphi 7*. *Borland Delphi 7* dipilih dengan alasan karena menggunakan bahasa *Object Pascal* yang telah memasyarakat bagi masyarakat awam, pelajar, dan mahasiswa, terlebih mahasiswa informatika dan ilmu komputer di Indonesia.

1.2 Perumusan masalah

Berdasarkan uraian pada latar belakang, maka permasalahannya dirumuskan sebagai berikut:

1. Bagaimanakah konsep steganografi sebagai media penyembunyian atau penyisipan pesan rahasia?
2. Bagaimana penjelasan dan penerapan metode *Least Significant Bit* (*LSB*)?
3. Bagaimana menganalisis perbedaan antara *file image* yang belum disisipi pesan rahasia dengan *file image* yang sudah disisipi pesan rahasia?

1.3 Tujuan Penulisan

Tujuan dari penulisan ini adalah:

1. Memperkenalkan steganografi sebagai media penyembunyian atau penyisipan pesan rahasia.
2. Menjelaskan metode *Least Significant Bit* (*LSB*) dan mengimplementasikannya ke dalam sebuah program aplikasi dengan menggunakan bantuan *software Borland Delphi 7*.
3. Menganalisis *file image* rahasia, sedemikian sehingga kita dapat mengetahui proses atau cara kerja dari metode yang digunakan.

1.4 Pembatasan Masalah

Batasan masalah yang perlu diberikan berdasarkan permasalahan yang telah dikemukakan di atas adalah sebagai berikut:

1. Metode yang digunakan dalam kajian steganografi ini adalah metode *Least Significant Bit* (*LSB*).
2. Pesan rahasia yang disisipkan atau disembunyikan berupa pesan dalam bentuk teks.
3. Media yang digunakan untuk menyisipkan pesan yaitu media *file image*.
4. *File image* yang digunakan adalah *file image* dalam bentuk format *file bitmap 24 bit* (*bmp 24 bit*).
5. *Software* sebagai alat bantu dalam membuat aplikasi steganografi ini yaitu dengan menggunakan *Borland Delphi 7.*

1.5 Metodologi Penulisan

Metodologi penulisan yang digunakan dalam penyusunan tugas akhir ini adalah sebagai berikut:

1. Studi Pustaka dan Literatur.

   Mempelajari jurnal dan artikel-artikel yang terkait dengan steganografi yang menggunakan metode *Least Significant Bit* (*LSB*).

2. Perancangan Sistem.

   Melakukan pembuatan alur proses yang tergambar dalam bentuk diagram alir (*flowchart*) dan pembuatan rancangan antarmuka (*User Interface*).

3. Implementasi.

   Mengimplementasikan suatu simulasi sistem yang telah terdisain ke dalam program komputer dengan bantuan *software Borland Delphi 7*.

4. Verifikasi.

   Menganalisis simulasi sistem yang telah dibuat berdasarkan metode yang digunakan dan mencocokkan hasilnya.

1.6 Sistematika Penulisan

Sistematika penulisan dijelaskan sebagai berikut:

1. Bab I (Pendahuluan) membahas Latar Belakang Masalah, Perumusan Masalah, Tujuan Penulisan, Pembatasan Masalah, Metodologi Penulisan, dan Sitematika Penulisan.
2. Bab II (Landasan Teori) membahas Konsep Steganografi, Representasi Bilangan, *Borland Delphi*, dan Diagram Alir (*Flowchart*).

3. Bab III (Perancangan Sistem) membahas Rancangan Diagram Alir dan Rancangan Antarmuka (*User Interface*).
4. Bab IV (Implementasi dan Analisis) membahas tentang Menulis dan Membaca Pesan Rahasia serta Analisis *File Image* Rahasia.
5. Bab V (Penutup) berisi Kesimpulan dan Saran untuk pengembangan lebih lanjut.