BAB 1
PENDAHULUAN

1.1 Latar Belakang

Saat ini *internet* sudah berkembang menjadi salah satu media yang sangat populer di berbagai belahan dunia (Bunyamin dan Andrian, 2009). Namun dengan semakin berkembangnya *internet*, semakin berkembang pula kejahatan dalam penyalahgunaan informasi. Dengan menggunakan berbagai teknik, banyak orang yang mencoba untuk mengakses informasi yang bukan haknya. Oleh karena itu, keamanan suatu sistem informasi juga harus diutamakan seiring dengan berkembangnya aplikasi menggunakan *internet*.

Keamanan suatu informasi pada zaman global ini menjadi sebuah kebutuhan vital dalam berbagai aspek kehidupan (Anna *et. al.*, 2009). Suatu informasi akan memiliki nilai lebih tinggi apabila menyangkut tentang aspek-aspek keputusan bisnis, keamanan, ataupun kepentingan umum. Informasi-informasi tersebut tentunya akan banyak diminati oleh berbagai pihak yang juga memiliki kepentingan di dalamnya.

Dengan berkembangnya ilmu pengetahuan, terutama di bidang informatika, penerapan teknik-teknik pengamanan informasi dan data yang sudah pernah dipakai pada zaman dulu dapat menjadi alternatif dalam pengamanan komunikasi data melalui jaringan *internet* (Sukrisno, 2007). Sebagai contoh adalah kriptografi, yaitu suatu ilmu dan seni untuk menjaga keamanan pesan yang dikirim dari suatu tempat ke tempat yang lain. Kriptografi tetap saja dapat dipecahkan meskipun prosesnya membutuhkan waktu, biaya dan tenaga. Teknik pengamanan data lain yang juga cukup populer adalah teknik steganografi.

Perkembangan steganografi menjadi salah satu alternatif pengamanan dalam komunikasi informasi dan data di jaringan *internet*. Berbeda dengan teknik kriptografi yang dapat menimbulkan kecurigaan karena pesan disamarkan dengan cara mengubah pesan yang asli menjadi seolah-olah tidak terbaca, steganografi justru lebih bisa mengurangi kecurigaan karena pesan yang disamarkan

disembunyikan dalam *file* lain. Dalam penerapannya, steganografi membutuhkan dua properti, yaitu media penampung dan data rahasia yang akan disembunyikan (Anggraini dan Utami, 2007).

Melalui penelitian ini, kedua teknik pengamanan data tersebut akan digabungkan. Kasus yang dibahas dalam penelitian ini adalah pengamanan pesan rahasia dengan menggunakan algoritma RC4 (*Ron's Code* 4) dan metoda LSB (*Least Significant Bit*). Media penampung pesan rahasia yang digunakan adalah citra digital. Hal ini karena adanya batasan kepekaan manusia dalam hal sistem visualisasi (Anggraini dan Utami, 2007). Sedangkan algoritma kriptografi RC4 dan metoda steganografi LSB dipilih karena keduanya paling sederhana dan paling mudah diimplementasikan (Munir, 2006).

1.2 Perumusan Masalah

Berdasarkan latar belakang di atas, maka permasalahan yang muncul adalah bagaimana membuat perangkat lunak pengamanan pesan rahasia menggunakan algoritma RC4 (*Ron's Code* 4) dan metoda LSB (*Least Significant Bit*)?

1.3 Batasan Masalah

Batasan masalah yang akan dikaji dalam penelitian ini sebagai berikut:

1. format *file* citra digital yang digunakan sebagai media penampung maupun yang akan dihasilkan dari perangkat lunak adalah bitmap berekstensi BMP,
2. pesan rahasia yang dapat disisipkan hanya pesan yang berupa teks,
3. algoritma kriptografi yang digunakan untuk mengamankan pesan rahasia adalah RC4,
4. metoda penyisipan pesan rahasia ke dalam citra digital yang digunakan adalah metoda LSB dengan hanya menggunakan 1 bit LSB,
5. media penampung hasil penyisipan tidak mengalami perubahan data saat proses pengungkapan, dan
6. waktu untuk proses penyisipan dan proses pengungkapan tidak menjadi pembahasan.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk membuat perangkat lunak pengamanan pesan rahasia menggunakan algoritma RC4 (*Ron's Code* 4) dan metoda LSB (*Least Significant Bit*).

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari hasil penelitian ini sebagai berikut:

1. dapat melindungi pesan yang ingin dikirimkan dari sasaran kejahatan,
2. mencegah orang-orang yang tidak berhak mengakses pesan yang ingin dikirimkan tersebut, dan
3. agar keamanan data dalam berkirim pesan rahasia dapat lebih terjamin.

1.6 Metodologi Penelitian

Dalam penelitian ini metoda pengembangan perangkat lunak yang digunakan adalah *waterfall model* (Pressman, 2002). Tahapan-tahapan penelitian ini sebagai berikut.

1. Rekayasa dan permodelan sistem

   Dalam tahap ini ditentukan layanan, batasan, dan tujuan dari perangkat lunak yang akan dibuat. Pada tahap inilah ditentukan hal-hal apa saja yang dapat dilakukan oleh perangkat lunak yang akan dibuat.
2. Analisis kebutuhan perangkat lunak

   Tahap ini merupakan suatu tahap di mana proses pencarian kebutuhan diintensifkan dan difokuskan pada perangkat lunak. Kebutuhan-kebutuhan apa saja yang perlu disediakan untuk membuat perangkat lunak dicari pada tahap ini. Studi literatur dan *site visit* digunakan untuk memperoleh informasi yang dibutuhkan.
3. Desain

   Proses ini digunakan untuk mengubah kebutuhan-kebutuhan hasil analisis sebelumnya menjadi bentuk "blueprint" perangkat lunak sebelum proses impelementasi dimulai. Pada tahap inilah *user interface* dan *flowchart* sistem yang bekerja dari perangkat lunak yang dibuat mulai dirancang.

4. Implementasi

   Implementasi adalah melakukan penerjemahan spesifikasi desain ke dalam kode komputer. Pada tahapan ini, sistem dibangun dengan menggunakan *tools* yang telah ditentukan sebelumnya yaitu Microsoft Visual Basic 6.0.

5. Pengujian

   Semua fungsi-fungsi perangkat lunak harus diujicobakan, agar perangkat lunak bebas dari *error*, dan hasilnya harus benar-benar sesuai dengan kebutuhan yang sudah didefinisikan sebelumnya.

1.7 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam penelitian ini adalah sebagai berikut.

BAB 1 PENDAHULUAN

Bab awal penelitian ini menjelaskan tentang latar belakang, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, serta sistematika penulisan.

BAB 2 LANDASAN TEORI

Bab ini berisi tentang teori-teori dasar dan tinjauan pustaka yang digunakan sebagai landasan dan acuan dalam penelitian.

BAB 3 ANALISIS DAN PERANCANGAN

Analisis sistem yang dibuat serta desain *input* dan *output* yang akan digunakan diuraikan dalam bab ini.

BAB 4 IMPLEMENTASI DAN PENGUJIAN

Bab ini membahas proses pembuatan program secara garis besar dan tampilan program yang berhasil dibuat serta hasil pengujian program.

BAB 5 PENUTUP

Bab terakhir membahas kesimpulan dan memberikan saran yang diperoleh sebagai penutup keseluruhan penelitian ini.