

BAB I

PENDAHULUAN

I.1. Latar Belakang

Pertukaran informasi menjadi hal yang sangat penting di era kemajuan saat ini. Setiap orang dengan mudah mendapatkan data ataupun berita yang diinginkan. Hal ini didukung dengan teknologi informasi dan komunikasi yang terus berkembang pesat dari tahun ke tahun. Akan tetapi kemudahan mendapatkan informasi juga memberikan ancaman. Beberapa ancaman yang diberikan adalah masalah tentang keamanan, kerahasiaan, dan keotentikan data. Masalah keamanan dan kerahasiaan data merupakan salah satu aspek penting dari suatu informasi. Dengan berkembangnya teknik pengambilan informasi secara ilegal, banyak orang yang mencoba untuk mengakses informasi yang bukan haknya. Oleh karena itu diperlukan suatu sistem pengamanan data yang bertujuan untuk meningkatkan keamanan data, melindungi suatu data atau pesan agar tidak dibaca oleh pihak yang tidak berwenang, dan mencegah pihak yang tidak berwenang untuk menyisipkan, menghapus, ataupun merubah data.

Salah satu ilmu pengamanan data yang terkenal adalah kriptografi dan steganografi. Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan, data, atau informasi dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Dalam kriptografi, terdapat 2 proses utama, enkripsi dan dekripsi. Enkripsi adalah proses penyandian pesan asli atau plainteks menjadi cipherteks (teks tersandi). Sedangkan dekripsi adalah proses penyandian

kembali cipherteks menjadi plainteks. Sedangkan steganografi merupakan teknik yang bertujuan untuk memenuhi aspek kerahasiaan sebuah pesan. Steganografi yaitu penyisipan pesan tersembunyi pada *file cover* yang berfungsi sebagai media penampung sehingga tampak seperti pesan biasa, dimana pesan yang dikirim hanya dapat dibaca oleh penerima yang memiliki hak untuk mengetahui isi pesan tersebut.

Dalam penelitian ini algoritma kriptografi dan steganografi yang digunakan oleh peneliti adalah algoritma RC4 dan LSB1. RC4 (*Rivest Cipher 4*) adalah sebuah *synchronous stream cipher*, yaitu *cipher* yang memiliki kunci simetris dan mengenkripsi plainteks secara digit per digit atau *byte per byte* dengan cara mengkombinasikan dengan operasi biner (biasanya XOR) dengan sebuah angka semiacak. Setelah pesan di enkripsi menggunakan algoritma RC4 selanjutnya pesan akan disembunyikan ke dalam gambar untuk meningkatkan keamanannya dengan algoritma LSB1, yaitu metode yang tidak terlalu kompleks serta penyimpanan pesan pada gambar juga cukup besar, sehingga memungkinkan dalam melakukan penyisipan data. Dasar dari metode ini adalah bilangan berbasis biner yaitu 0 dan 1, maka proses penerapan menjadi lebih mudah. Lebih lanjut metode ini berhubungan erat dengan ukuran 1 *bit*, *bit* yang diganti hanya *bit* yang paling akhir, maka *stego image* atau media penampung yang dihasilkan hampir sama persis dari sebelum dilakukan steganografi sehingga tidak mengubah gambar secara signifikan.

Berdasarkan latar belakang diatas pada penelitian ini akan dibangun sebuah aplikasi untuk mengamankan pesan dengan cara melakukan enkripsi terhadap pesan yang selanjutnya akan disembunyikan pada sebuah gambar, maka pada skripsi ini akan ditarik sebuah judul “**Perancangan Aplikasi Penyembunyian Pesan Ke Dalam Gambar Menggunakan Algoritma RC4 Dan LSB1**”.

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Adapun hal-hal yang menjadi identifikasi masalah aplikasi ini adalah :

1. Keamanan sebuah pesan rahasia rentan terhadap kegiatan seperti mengurangi dan menambah ataupun merubah sebuah pesan oleh pihak yang tidak berwenang.
2. Dibutuhkan aplikasi penyembunyian pesan ke dalam gambar menggunakan algoritma RC4 dan LSB1.
3. Mencoba mengimplementasikan bahasa pemrograman *Java* menggunakan perangkat lunak *Eclipse* untuk memecahkan kasus tersebut.

I.2.2. Perumusan Masalah

Berikut perumusan masalah yang akan dicari pemecahannya melalui penulisan skripsi ini, antara lain :

1. Bagaimana menjaga keamanan sebuah pesan agar dapat mencegah pihak yang tidak berwenang untuk mengurangi dan menambah ataupun merubah sebuah pesan ?
2. Bagaimana merancang sebuah aplikasi penyembunyian pesan ke dalam gambar menggunakan algoritma RC4 dan LSB1 ?
3. Bagaimana pengimplementasian perangkat lunak *Eclipse* untuk memecahkan kasus penyembunyian pesan ke dalam gambar ?

I.2.3. Batasan Masalah

Dalam penulisan skripsi ini dibatasi permasalahannya sebagai berikut :

1. Aplikasi ini dirancang menggunakan bahasa pemrograman *Java* pada perangkat lunak *Eclipse*.
2. Aplikasi ini digunakan untuk menyembunyikan pesan teks ke dalam sebuah gambar.
3. Algoritma yang digunakan pada aplikasi ini adalah algoritma RC4 dan LSB1.
4. Algoritma RC4 digunakan dalam proses enkripsi dan dekripsi pesan sedangkan algoritma LSB1 digunakan dalam proses penyembunyian dan ekstrak pesan dari gambar.
5. Aplikasi ini dirancang untuk digunakan pada perangkat lunak dengan sistem operasi *android*.

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

Tujuan yang ingin dicapai melalui penulisan skripsi ini adalah sebagai berikut :

1. Menghasilkan sebuah aplikasi untuk menyisipkan pesan ke dalam sebuah gambar.
2. Mengkombinasikan algoritma RC4 dan LSB1 untuk mengamankan dan menyembunyikan pesan ke dalam sebuah gambar.
3. Menciptakan sebuah sistem baru dalam mengamankan sebuah pesan rahasia dengan memanfaatkan metode kriptografi dan steganografi.

I.3.2. Manfaat

Adapun manfaat yang dapat diambil dalam penulisan skripsi ini adalah:

1. Sebagai bentuk realisasi teori-teori yang diterima selama masa kuliah menjadi kedalam bentuk sebuah aplikasi yang dapat digunakan banyak orang.
2. Dapat dijadikan media baru bagi pengguna untuk dapat mengamankan pesan yang bersifat rahasia tanpa disadari oleh pihak yang tidak diinginkan.
3. Dapat menjadi referensi bagi peneliti lain yang ingin membangun sebuah aplikasi penyembunyian pesan ke dalam gambar.

I.4. Metodologi Penelitian

Untuk dapat mengimplementasikan sistem di atas, maka secara garis besar digunakan beberapa metode sebagai berikut:

I.4.1. Metode Pengumpulan Data

Sistem yang dirancang tentunya memerlukan pengumpulan data, dalam proses pengumpulan data terdapat beberapa cara, berikut diantaranya :

1. Studi Literatur, dengan cara mempelajari acuan dan literatur yang berhubungan dengan materi dalam penulisan skripsi. Acuan yang digunakan umumnya adalah tentang cara penyusunan skripsi pada Universitas Potensi Utama dan juga tentang studi pustaka yang digunakan dalam penulisan skripsi.
2. Pengamatan, yaitu pengumpulan data dan informasi yang dilakukan dengan cara pengamatan langsung beberapa contoh aplikasi kriptografi dan steganografi. Pengamatan yang dilakukan adalah dengan melihat contoh-contoh *script* program bahasa pemrograman yang selanjutnya akan dituangkan kedalam bahasa pemrograman *Java*.
3. Dokumentasi, yaitu penulis mencari data-data yang mendukung penulisan skripsi melalui *internet*. Dalam penulisan skripsi ini penulis mencari jurnal-jurnal yang dijadikan acuan melalui *internet*. Jurnal yang dicari melalui *internet* dapat berupa jurnal nasional maupun internasional.

I.4.2. Metode Perancangan Sistem

Dalam merancang sistem agar mencapai hasil yang diharapkan dilakukan tahap-tahap sebagai berikut :

1. Target/Tujuan Penelitian

Target penelitian yang dilakukan untuk membuat suatu aplikasi penyembunyian pesan ke dalam gambar menggunakan algoritma RC4 dan LSB1.

2. Analisis Kebutuhan

Seluruh kebutuhan *software* harus bisa didapatkan dalam fase ini, termasuk didalamnya kegunaan *software* yang diharapkan pengguna dan batasan *software*. Informasi ini biasanya dapat diperoleh melalui wawancara, *survey* atau diskusi. Informasi tersebut dianalisis untuk mendapatkan dokumentasi kebutuhan pengguna untuk digunakan pada tahap selanjutnya. Dalam tahap ini *software* yang dibutuhkan adalah *Eclipse* untuk membangun aplikasi *android*. Dalam membuat skripsi ini, spesifikasi minimum dari perangkat keras (*Hardware*) dan perangkat lunak (*Software*) yang digunakan adalah sebagai berikut :

a. Perangkat Keras (*Hardware*)

Perangkat keras yang digunakan antara lain :

1. Laptop : *Core i3 Processor*
2. RAM 4 GB
3. *Smartphone* dengan sistem operasi *android 4.4 (Kitkat)*

b. Perangkat lunak (*Software*)

Software yang digunakan untuk membuat skripsi ini antara lain :

1. Sistem operasi *Windows 7*
2. *Eclipse*

3. Desain Sistem

Tahap ini dilakukan sebelum melakukan *coding*. Tahap ini bertujuan untuk

memberikan gambaran apa yang seharusnya dikerjakan dan bagaimana tampilannya. Tahap ini membantu dalam menspesifikasikan kebutuhan *hardware* dan sistem serta mendefinisikan arsitektur sistem secara keseluruhan. Hasilnya berupa desain dari sistem yang akan dibangun serta antar muka dari aplikasi yang akan dibuat.

4. Implementasi

Dalam tahap ini dilakukan pemrograman. Pembuatan aplikasi dipecah menjadi modul-modul kecil yang nantinya akan digabungkan dalam tahap berikutnya. Selain itu dalam tahap ini juga dilakukan pemeriksaan terhadap modul yang dibuat, apakah sudah memenuhi fungsi yang diinginkan atau belum. Fungsi-fungsi tersebut juga akan disesuaikan dengan perancangan aplikasi.

5. Pengujian

Di tahap ini dilakukan penggabungan modul-modul yang sudah dibuat dan dilakukan pengujian ini dilakukan untuk mengetahui apakah aplikasi yang dibuat telah sesuai dengan desain yang telah dirancang sebelumnya dan masih terdapat kesalahan atau tidak.

6. Pemeliharaan

Pada tahap ini aplikasi yang sudah jadi dijalankan serta dilakukan pemeliharaan. Pemeliharaan termasuk dalam memperbaiki kesalahan yang tidak ditemukan pada langkah sebelumnya. Perbaikan implementasi unit sistem dan peningkatan jasa sistem sebagai kebutuhan baru.

I.5. Kontribusi Penelitian

Pada penelitian sebelumnya proses mengamankan pesan dengan algoritma RC4 hanya sebatas melakukan enkripsi saja untuk menghasilkan *ciphertext*. Sehingga untuk memberi kontribusi dalam bidang penelitian, pada penelitian ini penulis akan membangun sebuah aplikasi untuk meningkatkan keamanan pesan dengan menyembunyikan pesan hasil enkripsi menggunakan algoritma RC4 ke dalam sebuah gambar menggunakan algoritma LSB1, sehingga tidak akan disadari oleh orang lain terdapat pesan rahasia di dalam gambar tersebut.

I.6. Sistematika Penulisan

Adapun sistematika penulisan yang diajukan dalam penulisan skripsi ini adalah sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini menerangkan tentang latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metodologi penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini menerangkan tentang teori-teori dan metode yang berhubungan dengan topik yang dibahas atau permasalahan yang sedang dihadapi.

BAB III : ANALISA DAN DESAIN SISTEM

Pada bab ini mengemukakan tentang analisa sistem yang sedang berjalan, evaluasi sistem yang berjalan dan desain sistem secara detail.

BAB IV : HASIL DAN UJI COBA

Pada bab ini menerangkan hasil dan pembahasan aplikasi yang dirancang serta kelebihan dan kekurangan aplikasi yang dirancang.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan penulisan dan saran dari penulis sebagai perbaikan di masa yang akan datang untuk pembuatan aplikasi penyembunyian pesan ke dalam gambar menggunakan algoritma RC4 dan LSB1.