

## **BAB 1**

### **PENDAHULUAN**

#### **1.1 Latar Belakang**

Saat ini penggunaan teknologi informasi sebagai media pertukaran informasi berkembang sangat luas. Berbagai jenis informasi seperti teks, gambar, suara dan video dapat dikonversikan menjadi media digital yang memungkinkan untuk diperbanyak maupun dikirimkan melalui berbagai media. Salah satunya adalah internet, melalui internet kita dapat dengan mudah untuk saling bertukar informasi dengan orang lain di berbagai tempat (Fiansyah, 2008).

Menjadi masalah adalah keamanan dalam menggunakan internet. Sangat banyak cara yang dapat dilakukan seseorang untuk mengambil informasi yang bukan miliknya di internet. Ini menimbulkan ancaman bagi pengguna internet untuk melindungi informasi yang dikirimnya dari orang-orang yang tidak bertanggungjawab (Stalling, 2005).

Salah satu teknik pengamanan informasi adalah kriptografi. Kriptografi adalah teknik untuk merahasiakan data sehingga tidak dapat diketahui oleh orang lain dengan cara memanipulasi data tersebut sehingga orang lain tidak dapat memahaminya. Kelemahan dari kriptografi adalah menghasilkan data yang sama sekali tidak dimengerti sehingga menimbulkan kecurigaan pada orang lain. Salah satu solusinya adalah dengan menggunakan steganografi. Steganografi adalah teknik untuk menyisipkan suatu media ke dalam media lainnya.

RC4 merupakan algoritma kriptografi yang tergolong kepada stream cipher dimana algoritma ini melakukan operasi penyandian karakter per karakter. LSB merupakan penyisipan informasi pada data lain dengan memanfaatkan bit data yang paling tidak signifikan. Penelitian sebelumnya telah dilakukan oleh Hermenda (2013)

melakukan pengamanan informasi menggunakan metode LSB (*least significant bit*). Pada penelitian ini penulis melakukan modifikasi proses penyisipan informasi pada metode LSB, sehingga keberadaan informasi yang telah disisipkan sulit untuk di deteksi oleh orang lain.

Berdasarkan uraian diatas, maka penulis ingin melakukan penelitian dengan rencana judul **“Implementasi Algoritma RC4 dan Modified LSB pada Pengamanan Text File”**.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang masalah, maka rumusan masalah dalam penelitian ini adalah bagaimana memberikan perlindungan informasi dengan menggunakan algoritma RC4 dan metode *modified* LSB.

## 1.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah

1. Informasi yang digunakan berupa *file* teks dengan format \*.txt.
2. Media yang digunakan untuk menyimpan pesan adalah citra digital berjenis *true color* (RGB) 24 bit dengan format citra \*.bmp.
3. Citra yang digunakan sebagai media penyisipan berukuran maksimal 1000x1000 *pixel* dan panjang informasi tidak lebih dari 2000 karakter.
4. Aplikasi dibangun dengan bahasa C# menggunakan IDE Sharp Develop.

## 1.4 Tujuan Penelitian

Adapun tujuan dari tugas akhir ini adalah memberikan pengamanan terhadap suatu informasi dengan cara sebagai berikut,

1. Melakukan penyandian suatu informasi kemudian menyisipkan informasi yang telah disandikan tersebut ke dalam suatu citra.
2. Melakukan pengungkapan kembali informasi tersandi yang telah disisipkan di dalam suatu citra kemudian mengembalikannya ke dalam bentuk semula.

## 1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah informasi hanya dapat diketahui oleh orang yang berhak sehingga komunikasi dapat dilakukan dengan aman.

## 1.6 Metodologi Penelitian

Metodologi penelitian yang digunakan adalah :

### 1. Studi literatur

Mempelajari literatur mengenai kriptografi diantaranya tujuan kriptografi, cara kerja kriptografi kunci simetri, algoritma RC4 dan juga literatur mengenai steganografi, diantaranya teknik-teknik steganografi, penyisipan metode LSB. Sumber literatur berasal dari buku cetak maupun elektronik dan penelitian-penelitian yang sudah diterbitkan.

### 2. Analisis dan perancangan sistem

Menganalisa permasalahan dalam bentuk rumusan masalah dan batasan masalah serta melakukan perancangan sistem dalam bentuk *flowchart*, diagram *use case* dan *design interface*.

### 3. Implementasi sistem

Mengimplementasikan sistem berupa aplikasi berdasarkan perancangan sistem yang telah dirancang sebelumnya.

### 4. Pengujian sistem

Menguji keberhasilan sistem dalam melakukan proses penyamaran pesan dan melakukan penyisipan pesan yang telah disamarkan ke dalam suatu citra. Adapun aspek yang harus dipenuhi dalam penyamaran pesan adalah aspek keamanan dan aspek yang harus dipenuhi dalam penyisipan adalah *recovery* dan *fidelity*.

### 5. Dokumentasi

Penyusunan laporan selama melakukan penelitian dalam bentuk skripsi.

## **1.7 Sistematika Penulisan**

Sistematika penulisan skripsi ini terdiri dari beberapa bagian utama yang dijelaskan sebagai berikut.

### **BAB 1 PENDAHULUAN**

Menjelaskan latar belakang dari penelitian yang dilakukan, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian dan sistematika penulisan skripsi.

### **BAB 2 LANDASAN TEORI**

Berisi penjelasan mengenai sistem kriptografi, tujuan kriptografi, cara kerja kriptografi kunci simetri, algoritma RC4 dan juga literatur mengenai steganografi, diantaranya teknik-teknik steganografi, penyisipan metode LSB.

### **BAB 3 ANALISIS DAN PERANCANGAN**

Membahas analisis terhadap masalah penelitian, analisis kebutuhan dalam membangun sistem dan perancangan terhadap sistem yang akan dibangun.

### **BAB 4 IMPLEMENTASI DAN PENGUJIAN**

Merupakan laporan hasil penelitian yang dilakukan. Berisi tentang penjelasan implementasi sistem berdasarkan analisis dan perancangan sistem, serta pembahasan hasil pengujian.

### **BAB 5 KESIMPULAN DAN SARAN**

Berisi kesimpulan dari keseluruhan penelitian yang dilakukan dan saran untuk pengembangan penelitian ini selanjutnya.