BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi sekarang ini yang semakin pesat dan juga memberikan banyak sekali manfaat bagi kehidupan manusia. Salah satunya adalah penggunaan jaringan internet yang memungkinkan orang dengan mudah untuk saling bertukar informasi. Pengiriman informasi dengan menggunakan internet ini banyak dilakukan karena disamping kecepatannya juga biayanya pun murah. Namun disisi lain penggunaan internet sebagai sarana bertukar informasi juga tidak lepas dari sebuah ancaman. Ancaman keamanan yang terjadi terhadap informasi dapat berupa interupsi, penyadapan, modifikasi, dan fabrikasi. Hal ini menjadi sangat berbahaya jika informasi yang dikirimkan merupakan informasi yang memiliki aspek kerahasiaannya cukup berharga. Mengatasi permasalahan tersebut berbagai cara untuk meningkatkan keamanan sebuah informasi terus dikembangkan, diantaranya steganografi dan kriptografi.

Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan, data, atau informasi dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna[1]. Dalam kriptografi, terdapat 2 proses utama, enkripsi dan dekripsi. Enkripsi adalah proses penyandian pesan asli atau plainteks menjadi *chiperteks* (teks tersandi). Sedangkan dekripsi adalah proses penyandian kembali *chiperteks* menjadi *plaintext*[1]. Untuk membangun sebuah sistem penyandian pesan yang baik dan kuat, pada penelitian ini penulis melakukan penggabungan

delapan algoritma kriptografi modern. Algoritma yang dimaksud meliputi algoritma AES, Camellia, Cast6, Mars, RC6, Safer+, Serpent dan Twofish. Fungsi *hash* SHA-3 juga akan digunakan untuk proses pembuatan kunci.

Steganografi merupakan cabang ilmu yang mempelajari tentang bagaimana menyembunyikan suatu informasi "rahasia" didalam suatu informasi lainnya[2]. Sistem steganografi akan menanamkan informasi tersembunyi ke media lainnya sebagai cover sehingga tidak menimbulkan kecurigaan[3]. Berbeda dengan teknik kriptografi, jika pada kriptografi ini akan timbul kecurigaan terhadap pesan yang telah disamarkan karena pesan yang disamarkan ini secara fisik telah dilakukan proses pengacakan data aslinya agar tidak terbaca. Steganografi tidak menimbulkan kecurigaan, steganografi menyembunyikan dalam data lain yang akan ditumpanginya tanpa mengubah data yang ditumpanginya tersebut sehingga data yang ditumpanginya sebelum dan setelah proses penyembunyian hampir sama[2]. Salah satu algoritma steganografi yang paling populer dan sering digunakan untuk menyembunyikan informasi pada citra digital adalah metode penyisipan algoritma *least significant bit* (LSB). Algoritma LSB merupakan sebuah algoritma sederhana dengan menukar nilai bit-bit terendah dari beberapa byte media cover dengan byte yang mengandung data rahasia yang akan disembunyikan secara berurutan[4].

Kriptografi dan steganografi sama-sama memiliki kelemahan. Namun tidak menutup kemungkinan jika kedua teknik ini digunakan secara bersama-sama. Dengan melakukan enkripsi pesan terlebih dahulu, kemudian menanamkan

chiperteks kedalam media *cover* dengan bantuan kunci stego maka kombinasi dari kedua teknik ini akan meningkatkan keamanan informasi yang telah tertanam[5].

Berdasarkan hal tersebut maka dilakukan penelitian sebagai objek dalam penyusunan skripsi ini dengan judul "Steganografi Pada Citra Digital Dengan Metode Least Significant Bit, Algoritma Kriptografi Modern, dan SHA-3".

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah pada penelitian ini adalah membangun aplikasi steganografi dengan menggunakan metode Least Significant Bit (LSB), algoritma kriptografi modern dan fungsi hash SHA-3 untuk mengamankan sebuah informasi ke dalam citra digital.

1.3 Batasan Masalah

Adapun batasan masalah yang akan dibahas dalam penulisan skripsi ini adalah sebagai berikut :

1. Aplikasi yang dibangun berbasis *desktop*.
2. Teknik enkripsi dan dekripsi pesan yang digunakan adalah algoritma kriptografi modern (AES, Camellia, Cast6, Mars, RC6, Safer+, Serpent dan Twofish) dan fungsi *hash* (SHA-3).
3. Metode steganografi yang digunakan untuk proses penyisipan pesan atau informasi ke dalam citra digital yaitu metode *Least Significant Bit* (LSB).
4. Media yang digunakan sebagai penampung pesan adalah citra digital berformat *.png, *.jpg dan *.jpeg. Ukuran maksimal pesan tergantung dari ukuran citra penampung.
5. File citra yang dihasilkan dari proses penyandian steganografi berformat *.png.
6. Pesan yang dapat disisipkan kedalam citra berupa teks dan file.

7. *Software* yang digunakan peneliti dalam membuat aplikasi ini yaitu Netbeans 8.2 dan Java sebagai bahasa pemrogramannya.
8. Tidak membahas dalam proses pengiriman citra pada jalur komunikasi.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut :

1. Menghasilkan sebuah aplikasi yang menerapkan metode steganografi LSB (*Least Significant Bit*), algoritma kriptografi modern dan fungsi hash SHA-3 yang digunakan untuk mengamankan sebuah informasi.
2. Melihat tingkat perubahan yang dialami oleh citra digital yang telah disisipkan sebuah informasi rahasia didalamnya.
3. Memperdalam ilmu mengenai keamanan dalam sebuah informasi.

1.5 Manfaat Penelitian

Manfaat dari penetilian ini adalah sebagai berikut :

1. Bagi Penulis

   Menerapkan dan mengembangkan ilmu serta teori-teori yang telah didapatkan selama studi sebagai persiapan pengaplikasian pada dunia kerja.

2. Bagi Perkembangan Ilmu Pengetahuan

   Penulis berharap aplikasi yang dirancang ini dapat ikut andil dan menjadi pelopor diciptakaannya aplikasi-aplikasi baru tentang pengamanan sebuah informasi yang dianggap penting.

3. Bagi Masyarakat

   Penulis berharap aplikasi ini dapat digunakan oleh masyarakat sebagai media keamanan informasi.

1.6 Metode Penelitian

Berikut metode yang digunakan untuk perancangan aplikasi steganografi pada citra digital dengan metode *Least Significant Bit*, algoritma kriptografi modern dan SHA-3 .

1.6.1 Metode Kepustakaan

Metode kepustakaan merupakan metode pengumpulan data yang dilakukan dengan cara membaca dan mempelajari buku, artikel, jurnal ilmiah yang berkaitan dengan steganografi, kriptografi, algoritma penyisipan dan ekstrasi pesan/data steganografi, fungsi hash dan juga hal yang berkaitan dengan topik yang akan dibahas.

1.6.2 Metode Analisis Data

Melakukan analisis data yang telah dikumpulkan untuk penyusunan laporan kemudian merancang dan membuat aplikasi. Analisis data dalam penelitian meliputi:

1. Analisis kebutuhan fungsional

   Merupakan pendefinisian fungsi sistem yang harus disediakan, bagaimana reaksi sistem terhadap input dan apa yang harus dilakukan sistem jika dalam situasi khusus.

2. Analisis kebutuhan non fungsional

   Melakukan analisis kebutuhan pendukun bagi sistem.

1.6.3 Metode Perancangan Aplikasi

Perancangan aplikasi meliputi perancangan antarmuka dan perancangan algoritma yang akan digunakan dalam pembuatan aplikasi.

1.6.4 Implementasi Aplikasi

Pada tahap ini dilakukan pembuatan sistem sesuai dengan analisis dan perancangan yang sudah didefinisikan sebelumya.

1.6.5 Evaluasi Aplikasi

Melakukan evaluasi terhadap aplikasi yang telah diimplementasikan.

1.7 Sistematika Penulisan

Dalam penulisan skripsi ini, dilakukan pembahasan yang dibagi kedalam lima 5, yaitu :

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini merupakan tinjauan pustaka, berisi dasar-dasar teori yang digunakan dalam penyusunan skripsi. Pada bab ini juga berisi tentang *software / tools* yang digunakan dalam pembuatan aplikasi.

BAB III ANALISI DAN PERANCANGAN

Bab ini menjelaskan tentang analisis terhadap kasus yang diteliti dan perancangan aplikasi yang akan dibuat.

BAB IV HASIL DAN PEMBAHASAN

Bab ini dibahas implementasi dari algoritma steganografi dan kriptografi yang digunakan pada skrisi ini dan beberapa hasil uji coba terhadap citra yang telah disisipkan pesan atau informasi.

BAB V PENUTUP

Bab ini berisi beberapa kesimpulan berdasarkan uraian-uraian yang diperoleh sebelumnya pada skripsi ini dan berupa saran untuk pengembangan lebih lanjut.