

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Informasi merupakan suatu hal yang sangat penting dalam kehidupan kita. Seperti dengan adanya teknologi internet semua orang memanfaatkannya sebagai media pertukaran informasi karena melalui teknologi tersebut segala jenis informasi begitu bebas dapat kita diperoleh. Akan tetapi perkembangan teknologi ini tidak selalu memberi dampak yang positif dan menguntungkan. Pencurian informasi melalui penyadapan merupakan salah satu contoh dampak negatif dari perkembangan teknologi tersebut. sehingga masalah keamanan dan kerahasiaan informasi menjadi hal yang sangat penting untuk diperhatikan.

Untuk mengamankan suatu pesan atau informasi, saat ini sudah banyak ilmu kriptografi dan steganografi yang mulai diterapkan dalam bentuk modern untuk menjamin kerahasiaan dan keamanan pesan. Ilmu kriptografi biasanya banyak digunakan untuk membuat sebuah pesan rahasia menjadi acak atau menjadi sesuatu yang tidak dimengerti. Sudah banyak algoritma kriptografi yang diterapkan namun dapat dengan mudah dipecahkan, sehingga dengan alasan tersebut maka

harus menggunakan algoritma yang benar – benar sulit untuk dipecahkan salah satunya algoritma *one time pad*. Algoritma ini merupakan salah satu algoritma yang belum terpecahkan karena kunci yang digunakan harus sama panjang dengan panjang pesan dan setiap kuncinya hanya digunakan sekali pakai dengan pemilihan kunci secara acak agar tidak bisa diproduksi ulang, sehingga lawan tidak mudah untuk menerka.

Namun dengan hanya menerapkan ilmu kriptografi itu saja belum cukup untuk menjamin keamanan dan kerahasiaan suatu pesan. Karena masih menimbulkan kecurigaan dengan adanya pesan yang tidak dimengerti. Maka untuk menghindari kecurigaan tersebut diterapkanlah sebuah ilmu steganografi yang merupakan seni untuk menyembunyikan pesan kedalam pesan lainnya. Maka pesan yang telah dienkripsi menggunakan algoritma *One Time Pad* akan disembunyikan kedalam sebuah citra dengan metode *Least Significant Bit (LSB)*. Metode LSB merupakan salah satu metode dari ilmu steganografi yang digunakan untuk menyembunyikan data dengan memanfaatkan bit akhir dari saluran warna. Metode LSB sangat cocok diterapkan pada citra, karena dengan teknik pemanfaatan bit akhir disetiap saluran warna sebagai media penyimpanan tidak akan menyebabkan kerusakan pada citra. Sehingga citra yang

telah berisi pesan tersembunyi tidak akan terlihat berbeda dengan citra pada saat sebelum disisipi pesan.

Sehingga dari uraian permasalahan yang telah dijelaskan diatas, untuk meningkatkan keamanan dan menjamin kerahasiaan suatu pesan maka akan diterapkanlah sebuah ilmu steganografi dan kriptografi dengan mengkombinasikan metode LSB dan algoritma *One time pad* untuk menyisipkan dan mengenkripsi pesan rahasia pada citra. Sehingga dengan memanfaatkan kelebihan – kelebihan kedua algoritma dan citra digital yang digunakan maka orang tidak akan menjadi curiga pada pesan rahasia yang akan kita kirimkan, sehingga tingkat keamanan pesan tersebut lebih terjamin kerahasiannya dan sulit untuk dipecahkan.

1.2 Rumusan Masalah

Rumusan masalah dari penelitian ini yaitu bagaimana membangun sebuah aplikasi steganografi untuk mengamankan pesan dengan menggunakan kombinasi metode *Least Significant Bit* dan algoritma *One time pad* pada citra digital.

1.3 Ruang Lingkup

Pada penelitian ini, peneliti mempunyai ruang lingkup sebagai berikut:

- a. Aplikasi ini berbasis desktop dengan bahasa pemrograman java.
- b. Media tempat menyisipkan pesan rahasia yang digunakan yaitu citra digital dengan format jpg dengan citra keluaran berekstensi png.
- c. Algoritma *One time pad* digunakan untuk proses enkripsi dan dekripsi pesan sebelum pesan disisipkan.
- d. Kunci yang digunakan untuk enkripsi dan dekripsi pesan yaitu kunci yang dibangkitkan secara acak berupa huruf alfabet dengan menggunakan *generate key*.
- e. Metode *Least Significant Bit* digunakan untuk proses penyisipan dan pengekstrakan pesan pada citra.
- f. Pengujian yang dilakukan yaitu Pengujian terhadap jumlah karakter dan aspek *robustness*.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah

1. Membangun sebuah aplikasi yang digunakan untuk menyisipkan pesan terenkripsi ke dalam format Jpg dengan menggunakan kombinasi metode LSB dan algoritma *One time pad*. sehingga pesan yang disisipkan pada citra digital akan sulit untuk dicurigai dan keamanannya lebih terjamin.
2. Untuk mengetahui seberapa jauh tingkat ketahanan citra yang disisipi pesan terenkripsi jika terkena gangguan.