BAB I

PENDAHULUAN

A. Latar Belakang

Keamanan dan kerahasiaan merupakan aspek penting yang dibutuhkan dalam proses pengiriman pesan. Semakin berkembangnya teknologi, pengiriman suatu pesan juga menjadi semakin kurang aman. Tidak menutup kemungkinan saat proses pengiriman pesan ada pihak ketiga yang ingin mengambil ataupun merubah isi dari pesan tersebut. Salah satu cara untuk mempertahankan kerahasiaan dari pesan tersebut adalah pesan yang akan dikirim disandikan terlebih dahulu menjadi kode – kode yang tidak dipahami maksudnya, sehingga bila ada pihak ketiga yang ingin mengambil ataupun merubahnya akan kesulitan dalam menterjemahkan isi pesan yang sebenarnya. Teknik tersebut dikenal dengan *kriptografi*. *Vigenere cipher* merupakan salah satu algoritma *kriptografi* klasik yang menggunakan substitusi abjad majemuk,dimana dengan menggunakan bujursangkar *vigenere* tiap huruf pada *plainteks* akan disubstitusi menjadi huruf lain berdasarkan kunci yang digunakan. Namun *vigenere cipher* telah berhasil dipecahkan oleh Friedrich Kasiski pada tahun 1863 dengan menggunakan metode *kasiski*. Oleh karena itu, dalam penelitian ini penulis melakukan sebuah modifikasi, yaitu dengan menyisipkan huruf – huruf yang ada pada kunci ke dalam *plainteks*. Dengan metode ini, diharapkan algoritma ini menjadi lebih kuat dan akan lebih sulit untuk dipecahkan. Tindakan pengamanan menggunakan teknik

kriptografi ini ternyata dianggap belum cukup dalam mengamankan suatu pesan, karena *cipherteks* mengandung karakter – karakter yang tidak wajar sehingga menimbulkan kecurigaan. Untuk mengatasi hal tersebut dapat digunakan teknik lain yaitu *steganografi*. *Steganografi* adalah ilmu dan seni untuk menyembunyikan pesan rahasia di dalam media digital sedemikian rupa sehingga orang lain tidak menyadari ada suatu pesan rahasia di dalam media tersebut. Implementasi steganografi saat ini telah menggunakan media digital sebagai media untuk menyembunyikan pesan, salah satunya adalah media gambar (citra digital).

Steganografi menyisipkan atau menyembunyikan pesan di dalam sebuah citra, agar pihak lain tidak menyadari keberadaan pesan yang ada di dalam citra tersebut. Salah satu metode *steganografi citra digital* adalah *Least Significant Bit* (*LSB*), yaitu teknik penyembunyian pesan pada lokasi *bit* terendah dalam citra digital. Pesan dikonversi ke dalam bentuk biner dan disembunyikan pada citra digital dengan metode *LSB*. Dalam penelitian ini, penulis menggunakan citra digital sebagai media penyembunyian pesan karena hasil keluaran dari *steganografi LSB* ini memiliki perubahan yang tidak dapat dibedakan oleh mata manusia. Kombinasi modifikasi vigenere cipher dan *steganografi LSB* dapat lebih meningkatkan keamanan pada pesan rahasia. Pesan rahasia terlebih dahulu dienkripsi dengan menyisipkan huruf – huruf pada kunci ke dalam *plainteks*, kemudian cipherteks hasil *kriptografi* tersebut disembunyikan didalam citra digital dengan metode *steganografi LSB*.

B. Rumusan Masalah

Berdasarkan latar belakang masalah diatas, maka dapat diidentifikasikan masalah pokok yang akan dipilih sebagai topik dari penelitian ini adalah sebagai berikut:

1. Apa fungsi steganografi tersebut?
2. Bagaimana menerapkan suatu sistem keamanan data agar data selain dapat disembunyikan, dapat pula terjaga kerahasiaannya dari pihak yang tidak berwenang?

C. Batasan masalah

Dengan mempertimbangkan keterbatasan waktu, ruang tulis,dan pustaka tugas akhir ini dibatasi hanya membahas hal-hal sebagai berikut:

1. Data yang dienkripsi merupakan *file text (txt*).*
2. Media *Steganografi* adalah file gambar yang memiliki format *JPEG.*
3. Algoritma *Steganografi* yang digunakan adalah algoritma *LSB dan Viginer Chiper.*
4. Program dibuat dengan menggunakan *Java*.
5. File output di simpan dengan format *JPEG.*

D. Tujuan Masalah

1. Agar pesan tidak di ketahui oleh pihak ketiga
2. untuk menerapkan suatu sistem keamanan data dengan algoritma-algoritma *Steganografi*.

E. Manfaat Penelitian

1. Menambah wawasan tentang *Steganografi* beserta algoritma-algoritmanya.
2. Penelitian ini diharapkan dapat memberikan keamanan untuk menyembunyikan, menjaga kerahasiaan data, serta mengintegrasikan data sehingga orang-orang yang berwenang saja yang dapat mengakses data tersebut.