**BAB I**

**PENDAHULUAN**

1. **Latar Belakang**

Dewasa ini dimana informasi telah menjadi kebutuhan yang sangat penting, komunikasi menjadi kegiatan yang semakin intens dilakukan manusia. Berkat dukungan perkembangan teknologi informasi yang semakin maju, khususnya teknologi internet, hampir tidak ada batasan lagi bagi seseorang untuk melakukan komunikasi dengan orang lain. Kini seseorang dapat dengan mudahnya melakukan percakapan dengan orang lain yang berjauhan jaraknya melalui berbagai macam media, misalnya teks (SMS atau *chatting*), suara (telepon), atau video (*video chat*).

Seiring dengan perkembangan teknologi, kebutuhan akan keamanan komunikasi juga menjadi semakin tinggi. Komunikasi-komunikasi yang dilakukan tersebut memiliki kepentingan-kepentingan yang berbeda, dari sekedar percakapan yang sifatnya kasual, hingga pesan-pesan penting yang bersifat rahasia. Selain itu, semakin maraknya *cybercrime* seperti *tapping* (penyadapan), *hacking*, dan lain-lain juga menjadi alasan akan kebutuhan keamanan komunikasi. Salah satu metode yang umum digunakan untuk melindungi informasi yang berbentuk teks adalah kriptografi. Metode yang dapat diterapkan untuk meningkatkan keamanan informasi yaitu dengan menggabungkan kriptografi dan steganografi.

Steganografi merupakan sebuah metode untuk melindungi informasi dengan cara menyembunyikan keberadaan sebuah informasi di balik sebuah penutup. Pada steganografi modern, hal tersebut biasanya dilakukan dengan cara menyisipkan informasi ke dalam media lain, misalnya citra digital, suara, atau video. Citra digital sebagai media untuk melakukan steganografi memiliki kelebihan antara lain akses dan pengolahannya yang relatif mudah serta waktu transmisi yang relatif lebih cepat sehingga media citra dirasa cocok sebagai media untuk melakukan steganografi.

Metode *Pixel Value Differencing* (PVD) merupakan salah satu metode yang dapat digunakan untuk melakukan steganografi pada citra digital. Metode ini memanfaatkan selisih nilai yang dimiliki antara dua buah *pixel* yang bertetangga untuk menentukan berapa banyak informasi yang dapat disisipkan sehingga metode ini memiliki kapasitas penyimpanan yang lebih besar dan kualitas citra yang lebih baik. Untuk meningkatkan keamanan, steganografi akan dikombinasikan dengan kriptografi sehingga informasi yang disisipkan tidak mudah dibaca oleh pihak-pihak yang tidak berhak. Metode kriptografi yang digunakan yaitu Vigenere *cipher* yang pada masa kejayaannya mendapatkan julukan *le chiffre indechiffrable* (sandi yang tak terpecahkan).

Berdasarkan uraian di atas, penulis mengambil judul Tugas Akhir **“Implementasi Kriptografi dan Steganografi Teks pada Citra Digital Menggunakan Algoritma Vigenere *Cipher* dan *Pixel Value Differencing*”**.

1. **Rumusan Masalah**

Berdasarkan uraian di atas, rumusan masalah yang dibahas dalam penelitian ini adalah bagaimana membuat aplikasi kriptografi dan steganografi teks pada *file* citra digital untuk melindungi informasi yang bersifat rahasia dengan mengimplementasikan algoritma kriptografi Vigenere *cipher* dan algoritma steganografi *Pixel Value Differencing* (PVD).

1. **Batasan Masalah**

Agar pembuatan aplikasi ini lebih terfokus, masalah dibatasi pada hal-hal berikut ini.

1. Karakter yang boleh digunakan dalam pesan hanya A-Z, a-z, dan spasi.
2. Jumlah karakter yang dapat diamankan maksimal 40 karakter.
3. Aplikasi hanya melakukan steganografi pada *file* citra digital.
4. Format *file* citra digital yang didukung oleh aplikasi ini adalah BMP dan JPG.
5. *Output* aplikasi berupa *file* citra dengan format BMP.
6. **Tujuan Penelitian**

Tujuan penelitian ini adalah merancang dan membuat aplikasi yang dapat melakukan kriptografi pada teks menggunakan metode Vigenere *cipher* dan steganografi pada *file* citra digital menggunakan algoritma *Pixel Value Differencing* (PVD) yang berguna untuk melindungi informasi yang bersifat rahasia.

1. **Manfaat Penelitian**

Adapun manfaat penelitian ini adalah sebagai berikut.

1. Meningkatkan keamanan informasi dengan cara menyembunyikan makna (melalui kriptografi) dan keberadaannya (melalui steganografi).
2. Mengimplementasikan algoritma kriptografi Vigenere *cipher* dan algoritma steganografi *Pixel Value Differencing* (PVD) untuk melakukan kriptografi pada teks dan steganografi pada *file* citra digital.
3. **Sistematika Penulisan**

Sistematika penulisan Tugas Akhir ini adalah sebagai berikut.

**BAB I PENDAHULUAN**

Bab ini memuat latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

**BAB II LANDASAN TEORI**

Bab ini memuat berbagai teori yang digunakan penulis sebagai acuan dalam melakukan analisa dan memecahkan masalah.

**BAB III METODOLOGI PENELITIAN**

Bab ini berisi metode penelitian yang digunakan. Metode pengembangan aplikasi yang digunakan penulis adalah RUP (*Rational Unified Process*).

**BAB IV ANALISIS DAN PERANCANGAN**

Bab ini memuat gambaran umum sistem, perancangan proses, pemodelan sistem menggunakan UML (*Unified Modelling Languange*), desain *database*, dan desain *interface*.

**BAB V IMPLEMENTASI**

Bab ini memuat pembahasan mengenai implementasi analisis dan desain ke dalam bahasa pemrograman serta pengujian aplikasi.

**BAB VI PENUTUP**

Bab ini berisi kesimpulan dan saran untuk Tugas Akhir.

**DAFTAR PUSTAKA**

**LAMPIRAN**

1. **Tinjauan Pustaka**

Penelitian ini didasarkan pada penelitian-penelitian sebelumnya mengenai kriptografi menggunakan metode Vigenere *cipher* dan steganografi menggunakan metode *Pixel Value Differencing*. Salah satu penelitian yang menjadi dasar penelitian ini yaitu penelitian yang dilakukan oleh Fahmi Aulia Tsani (2012) yang berjudul “*Implementasi Steganografi dan Algoritma Enkripsi Vigenere Cipher pada Media Plain Text*”. Penelitian ini bertujuan untuk menghindari penyadapan informasi yang dilakukan oleh *cracker* dengan cara mengenkripsi pesan dengan menggunakan metode Vigenere *cipher*, kemudian merubah pola pesan tersebut sedemikian rupa sehingga pesan tersebut menjadi mirip dengan pola pesan *spam* dengan tujuan menghindari pantauan *cracker*. Hasil penelitian ini adalah sebuah sistem yang dapat melakukan enkripsi menggunakan algoritma Vigenere *cipher* serta mampu menyembunyikannya ke dalam pesan berpola *spam*. Hasil enkripsi dan steganografi pesan ini juga bisa didekripsi melalui sistem dengan terlebih dahulu mengetahui kombinasi kunci dan *tabula recta* yang digunakan.

Berikutnya adalah penelitian yang dilakukan oleh Bayu Kristian Nugroho (2010) yang berjudul “*Aplikasi Enkripsi pada Telepon Selular Berbasis J2ME dengan Metode Vigenere Cipher*”. Penelitian ini bertujuan untuk mengamankan suatu informasi rahasia yang terdapat pada SMS dengan cara melakukan enkripsi pada SMS tersebut dengan menggunakan metode Vigenere *cipher*. Hasil penelitian ini adalah sebuah aplikasi pada telepon selular untuk memodifikasi pesan SMS menjadi *ciphertext* agar isi informasi dari SMS tersebut tidak diketahui orang lain. Untuk pengiriman SMS, sistem mengenkripsi pesan menjadi *ciphertext* menggunakan *key* yang dimasukkan oleh pengirim kemudian mengirimkan ke nomor tujuan. Untuk penerimaan SMS, sistem mendekripsi *ciphertext* menjadi *plaintext* menggunakan *key* yang dimasukkan oleh penerima kemudian menampilkan pesan asli kepada penerima.

Penelitian lain dilakukan oleh Muhammad Azhari (2014) yang berjudul “*Pengembangan Aplikasi Steganografi Pixel Value Differencing (PVD)*”. Penelitian ini bertujuan untuk mengamankan sebuah pesan dengan cara menyisipkan pesan tersebut ke dalam sebuah citra digital dengan menggunakan metode *Pixel Value Differencing* (PVD). Uji coba yang dilakukan dengan menggunakan citra *cover* dan pesan berupa citra 24 *bit* membuktikan bahwa aplikasi yang dikembangkan dapat digunakan dalam proses penyisipan dan ekstraksi pesan. Selain itu, *Peak Signal to Noise Ratio* (PSNR) dapat diukur dengan aplikasi tersebut sehingga besaran distorsi yang dihasilkan pada proses penyisipan pesan dapat diketahui.