

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi komputer saat ini mengalami perkembangan yang sangat pesat dan menjadi salah satu aspek penting dalam kehidupan manusia yang dapat menyelesaikan hampir semua pekerjaan. Perkembangan teknologi tersebut tidak terlepas dari perkembangan ilmu matematika karena setiap pembuatan sebuah teknologi baru selalu dihitung secara matematis menggunakan matematika. Namun dengan kecanggihan teknologi sekarang segala sesuatu yang menjadi rahasia dapat ditemukan dengan mudah hanya melalui kerja komputer. Hal ini juga merupakan salah satu dampak negatif dari perkembangan teknologi.

Dalam menemukan suatu data atau informasi yang dirahasiakan membuat orang yang ingin mengetahuinya menempuh segala cara untuk menemukannya, baik dengan cara membobol, mencuri, atau bahkan menyadap. Tidak jarang orang melakukan kejahatan-kejahatan seperti itu demi mendapatkan informasi tersebut. Hal ini termasuk pelanggaran terhadap hak cipta yang terdapat dalam UU No.28 tahun 2014. Karena informasi yang didapatkan tidak menggunakan izin dari pemilik atau pembuatnya. Selain itu, Indonesia juga mengatur tentang hukum pencurian data dalam UU ITE tahun 2008 pasal 3^[1].

Berbagai macam teknik digunakan untuk melindungi informasi yang dirahasiakan dari orang-orang yang tidak berhak. *File* citra digital atau gambar terkadang merupakan suatu aset yang berharga. Misalkan saja seorang pegawai pada divisi *engineering* yang bekerja disebuah perusahaan yang bergerak di bidang produksi mobil akan mengirim *design* gambar kendaraan khusus berupa *softcopy* kepada divisi kendaraan khusus melalui internet. *Design* gambar kendaraan tersebut perlu diamankan agar tidak diketahui atau ditiru oleh pesaing (*competitor*) perusahaan tersebut. Untuk mengamankan gambar yang dikirimkan melalui media internet, maka diperlukan suatu teknik keamanan yaitu *steganography*^[2].

Steganografi adalah teknik yang digunakan untuk menyembunyikan informasi ke dalam sebuah media, bisa berupa media gambar, suara ataupun video. Pada *steganography* media gambar dikenal sebuah teknik yang dinamakan *Least Significant Bit* (LSB). Metode penyisipan LSB (*Least Significant Bit*) ini adalah menyisipi pesan dengan cara mengganti bit ke 8, 16, dan 24 pada representasi biner *file* gambar dengan representasi biner pesan rahasia yang akan disembunyikan^[2].

Selain menggunakan teknik steganografi dengan menggunakan metode LSB (*Least Significant Bit*), peneliti juga menambahkan teknik kriptografi dengan menggunakan algoritma AES (*Advanced Encryption Standard*) dengan ukuran kunci 128 bit agar *file* citra digital dapat terlindungi secara maksimal.

Kriptografi merupakan studi matematika komputasi yang mempunyai hubungan dengan keamanan informasi seperti integritas data, keaslian entitas dan keaslian data. Kriptografi menggunakan berbagai macam teknik dalam upaya untuk mengamankan data. Dalam algoritma kriptografi terdapat dua jenis, yaitu algoritma kriptografi simetris dan algoritma kriptografi asimetris. Algoritma simetris disebut juga algoritma konvensional, algoritma ini menggunakan kunci yang sama untuk enkripsi dan dekripsi. Sedangkan algoritma asimetris menggunakan kunci yang berbeda dalam proses enkripsi dan dekripsi^[1].

Algoritma AES merupakan salah satu algoritma kriptografi simetris yang beroperasi pada sekumpulan *byte* data atau per blok. Algoritma kriptografi Rijndael yang didesain oleh Vincent Rijmen dan John Daemen ini adalah pengembangan dari algoritma DES (*Data Encryption Standard*), karena algoritma DES dianggap sudah tidak aman lagi karena dengan perangkat keras khusus kuncinya dapat ditemukan dalam beberapa hari saja. Algoritma AES berorientasi pada penyandi blok (*block cipher*) yang memproses blok data dengan panjang kunci 128-bit, 192-bit, atau 256-bit. Pada tahun 2006, AES merupakan salah satu algoritma terpopuler yang digunakan dalam kriptografi kunci simetrik^[1].

Adapun beberapa referensi dari penelitian terdahulu sebagai acuan, Penelitian Nur Afifah pada tahun 2018 mengenai Perancangan Aplikasi Kriptografi *Image* Menggunakan Metode *Advanced Encryption Standard*

(AES)^[1], Penelitian Hertika Yuni Asti Sinaga, dan Lamhot Sitorus pada tahun 2017 mengenai Pengamanan File Citra Digital Dengan Menggunakan Metode Least Significant Bit Dan End Of File^[2], Penelitian Pratiksha Sethi, dan V. Kapoor pada tahun 2016 mengenai A Proposed Novel Architecture for Information Hiding in Image Steganography by using Genetic Algorithm and Cryptography^[3], Penelitian Darmayanti, dan Awang Harsa.K pada tahun 2016 mengenai Sistem Steganografi Pada Citra Digital Menggunakan Least Significant Bit^[4], Penelitian Rahmat Tullah, Muhammad Iqbal Dzulhaq, Yudi Setiawan pada tahun 2016 mengenai Perancangan Aplikasi Kriptografi File Dengan Metode Algoritma *Advanced Encryption Standard* (AES)^[5], Penelitian Siti Nur'aini pada tahun 2019 mengenai Steganografi Pada Digital Image Menggunakan Metode Least Significant Bit Insertion^[6], Penelitian Nunung Nurmaesah, Tutik Lestari, Ami Retno Mariana pada tahun 2017 mengenai Aplikasi Steganografi Untuk Menyisipkan Pesan Dalam Media Image^[7], Penelitian Finna Monica, dan Ahmadi Surahman pada tahun 2016 mengenai Aplikasi Steganografi Citra Digital Menggunakan Metode LSB (*Least Significant Bit*) Visual Basic 6^[8], Penelitian Ade Trian Aulia, dan Achmad Ridwan pada tahun 2020 mengenai Steganografi Menyembunyikan Teks Pada Gambar Menggunakan Metode Dynamic Cell Spreading Dan Algoritma Huffman^[9], Penelitian Eza Budi Perkasa pada tahun 2020 mengenai Implementasi Algoritma Username, Resolution, Color, and Hash Dalam Otentikasi Login Sistem^[10].

Penelitian ini dilakukan dengan model *waterfall*. Model ini dipilih karena memiliki tahapan pengerjaan dengan metode yang teratur dan berurutan sehingga dapat memperkecil tingkat kesalahan yang mungkin terjadi dalam setiap tahapan pengerjaannya. Sistem berbasis desktop ini diharapkan dapat mempermudah karyawan instansi dalam melakukan pengamanan data *file* citra digital. Berdasarkan latar belakang, masalah dan model yang digunakan maka penelitian ini diberikan judul **“ANALISA DAN PERANCANGAN APLIKASI STEGANOGRAFI DAN KRIPTOGRAFI FILE CITRA DIGITAL BERBASIS DESKTOP DI PT. BANGKA MEDIA GRAFIKA (BANGKA POS GROUP)”**.

1.2 Rumusan Masalah

Untuk menemukan solusi yang tepat dalam suatu permasalahan, maka terlebih dahulu permasalahan tersebut dianalisis dan disusun kedalam bentuk formula yang sistematis. Dari latar belakang yang telah diuraikan maka peneliti dapat merumuskan masalah sebagai berikut:

1. Apakah metode LSB (*Least Significant Bit*) dapat digunakan untuk menyembunyikan pesan pada citra digital?
2. Apakah metode AES (*Advanced Encryption Standard*) dapat digunakan untuk melakukan enkripsi dan dekripsi *file* citra digital?
3. Bagaimana membuat sebuah aplikasi desktop steganografi dengan metode LSB dan kriptografi dengan algoritma AES untuk citra digital?

1.3 Tujuan dan Manfaat Penelitian

1.3.1. Tujuan Penelitian

Berdasarkan rumusan masalah dapat disimpulkan bahwa tujuan dari penelitian ini adalah:

1. Untuk mengetahui penyembunyian pesan pada sebuah data citra digital menggunakan metode LSB (*Least Significant Bit*).
2. Untuk mengetahui enkripsi dan dekripsi pada sebuah data citra digital menggunakan AES (*Advanced Encryption Standard*).
3. Untuk merancang dan membuat aplikasi desktop steganografi dengan metode LSB dan kriptografi dengan algoritma AES untuk citra digital.

1.3.2. Manfaat Penelitian

Manfaat dari penelitian ini antara lain:

1. Bagi penulis, dapat menerapkan dan mengembangkan ilmu keamanan data citra digital dan juga dapat menambah pengetahuan terapan dan mengaplikasikan ilmu steganografi dan kriptografi yang dapat dikembangkan lebih lanjut dengan menggunakan metode ataupun algoritma lain.

2. Bagi pembaca, dapat menambah pengetahuan, wawasan, dan pemahaman tentang metode LSB (*Least Significant Bit*) dalam steganografi dan metode AES (*Advanced Encryption Standard*) dalam kriptografi.
3. Bagi pengguna, aplikasi steganografi dan kriptografi ini dapat dijadikan sebagai salah satu media alternatif untuk mengamankan sebuah *file* data citra digital.

1.4 Batasan Masalah

Adapun beberapa batasan masalah yang penulis lakukan pada penelitian ini, sehingga dapat menghindari persepsi yang berbeda dan meluasnya pembahasan topik permasalahan sebagai berikut:

1. Membuat program steganografi dan kriptografi sederhana yang berfungsi untuk menyisipkan informasi berupa teks kedalam media gambar yang kemudian data *file* gambar tersebut dilakukan penyandian data..
2. Format gambar yang digunakan dan diuji adalah JPG, JPEG, dan PNG.
3. Metode yang digunakan dalam steganografi adalah LSB (*Least Significant Bit*).
4. Metode yang digunakan dalam kriptografi adalah AES (*Advanced Encryption Standard*) dengan ukuran blok dan kunci 128 bit atau 16 *byte*.
5. Rancangan aplikasi dibuat dengan menggunakan NetBeans IDE 8.1.
6. Bahasa pemrograman yang digunakan adalah Java.

1.5 Metodologi Penelitian

Metode penelitian yang dilakukan adalah:

1. Wawancara
Dalam tahap ini, penulis melakukan pengumpulan data-data yang diperlukan sebagai dasar dari perancangan aplikasi. Kebutuhan tersebut didapat dengan cara mewawancarai pembimbing lapangan tempat riset di PT. Bangka Media Grafika (Bangka Pos Group).
2. Studi Pustaka

Penulis melakukan pengumpulan data sekunder dari berbagai sumber, agar representatif dan variatif. Penulis mengumpulkan data dengan mengadakan studi penelaan terhadap buku-buku, literatur-literatur, catatan dan laporan yang ada hubungannya dengan masalah yang ingin penulis pecahkan. Kajian pustaka untuk membantu dalam perancangan aplikasi dengan cara mempelajari penelitian-penelitian sebelumnya dengan topik yang serupa sehingga dapat dijadikan acuan yang tepat.

3. Perancangan Aplikasi

Dalam tahap ini, penulis mulai merancang aplikasi dengan bahasa pemrograman Java dan MySQL sebagai aplikasi *database*-nya. Pertama-tama, penulis membuat *database* yang dibutuhkan dengan menggunakan MySQL. Selanjutnya, penulis mulai merancang antarmuka aplikasi menggunakan bahasa pemrograman Java.

4. Implementasi dan Evaluasi

Setelah aplikasi selesai dirancang, penulis mencoba untuk mengimplementasikan dan melakukan evaluasi aplikasi dengan cara menguji coba dengan data contoh serta meminta evaluasi dari para pihak yang terkait.

Metodologi yang digunakan adalah SDLC (*System Development Life Cycle*) yaitu perencanaan (*planning*), analisis (*analysis*), perancangan (*design*), implementasi (*implementation*).

Model yang digunakan adalah *Waterfall* dan UML (*Unified Modeling Language*) sebagai *tools* bantuan. *Diagram* yang digunakan peneliti yaitu *Use Case Diagram*, *Activity Diagram*, *Sequence Diagram*, dan *Class Diagram*.

1.6 Sistematika Penulisan

Sistematika penulisan menggambarkan uraian bab per bab dari keseluruhan bab, agar penulisan laporan kerja praktek lebih terarah dan tersusun dengan baik. Adapun maksud dari uraian singkat tersebut yaitu:

BAB I PENDAHULUAN

Berisi tentang beberapa hal umum tentang maksud dan tujuan penulisan Kerja Praktek serta pelaksanaan penelitian pada perusahaan PT. Bangka Media Grafika (Bangka Pos Group) sebagai acuan dalam pembuatan rancangan aplikasi steganografi dan kriptografi, yang terdiri dari latar belakang dilaksanakannya penelitian, tujuan dari dilaksanakannya penelitian, perancangan, dan pembuatan aplikasi dengan model *waterfall* dalam menunjang penulisan kerja praktek, manfaat penulisan, metode pelaksanaan dan penulisan kerja praktek, serta sistematika dalam penyusunan Kerja Praktek ini.

BAB II LANDASAN TEORI

Membahas tentang landasan teori yang diambil dan digunakan dalam melakukan penulisan. Sumber-sumber teori ini dijadikan acuan dan panduan dalam melakukan penulisan teori.

BAB III ORGANISASI

Bab ini berisikan gambaran dan sejarah singkat organisasi, visi dan misi organisasi, struktur organisasi yang bertugas dan wewenang organisasi di PT. Bangka Media Grafika (Bangka Pos Group).

BAB IV PEMBAHASAN

Bab ini berisi tentang definisi masalah atau analisa yang terkait dengan topik yang diambil, rancangan tampilan dan algoritma penyelesaian masalah dan pembahasannya, serta pembahasan lainnya.

BAB V PENUTUP

Bab ini merupakan bagian yang terakhir dari bab yang menguraikan kesimpulan dari keseluruhan bab dan saran-saran yang diharapkan rancangan sistem dapat bermanfaat untuk diterapkan oleh PT. Bangka Media Grafika (Bangka Pos Group).