BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam perkembangan teknologi komputer saat ini telah mengalami kemajuan yang sangat pesat dan menjadi salah satu aspek penting dalam kehidupan manusia yang dapat menyelesaikan banyak jenis pekerjaan. Perkembangan teknologi komputer 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.

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*.

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.

Selain menggunakan teknik steganografi dengan menggunakan metode LSB (*Least Significant Bit*), peneliti juga menambahkan teknik kriptografi dengan menggunkan algoritma AES (*Advanced Encryption Standard*) dengan ukuran kunci 256 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 deskripsi. Sedangkan algoritma asimetris menggunakan kunci yang berbeda dalam proses enkripsi dan deskripsi.

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.

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 Architechture 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 Rivian Nuari, dan Niki Ratama pada tahun 2020 mengenai Implementasi Algoritma Kriptografi AES (*Advanced Encryption Standard*) 128 Bit Untuk Pengamanan Dokumen *Shipping*[9], Penelitian Eza Budi Perkasa pada tahun 2020 mengenai Implementasi Algoritma Username, Resolution, Color, and Hash Dalam Otentikasi *Login* Sistem[10].

Berdasarkan latar belakang, masalah dan model yang digunakan maka penelitian ini diberikan judul "**IMPLEMENTASI PENYISIPAN PESAN TEKS PADA CITRA DIGITAL DENGAN LSB DAN AES 256**".

1.2 Rumusan Masalah

Untuk menemukan solusi yang tepat dalam suatu permasalahan, maka terlebih dahulu permasalahan tersebut dianalisis dan disusun ke dalam bentuk formula yang sistematis. Dari latar belakang yang telah diuraikan maka masalah dapat dirumuskan "Apakah AES 256 dapat digunakan untuk mengenkripsi pesan teks yang selanjutnya disisipkan ke citra digital menggunakan LSB?".

1.3 Tujuan dan Manfaat Penelitian

Berdasarkan rumusan masalah dapat disimpulkan bahwa tujuan dari penelitian ini adalah mengetahui enkripsi pesan teks dengan menggunakan AES 256 dan penyisipan pesan teks hasil enkripsi ke citra digital menggunakan LSB (*Least Significant Bit*). Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Bagi pengguna (pengirim pesan maupun penerima pesan), dapat menjaga kerahasiaan suatu pesan teks dengan pengamanan ganda, yaitu enkripsi menggunakan AES 256 dan steganografi menggunakan LSB. Hal ini juga untuk meminimalisir kemungkinan penyadapan pesan dikarenakan media citra digital yang digunakan sebagai media "tidak mencurigakan" saat didistribusikan ke penerima pesan. Walaupun penyadap berhasil memperoleh citra digital yang digunakan sebagai media untuk penyisipan pesan, penyadap tersebut membutuhkan waktu yang sangat lama untuk mendekripsi pesan yang ada pada citra digital, bahkan oleh super komputer sekalipun.
2. Bagi pembaca, dapat menambah pengetahuan terkait cara mengenkripsi dan mendekripsi suatu *string* (pesan teks/*plain text*) menggunakan AES 256. Selain itu, pembaca dapat mengetahui cara menyisipkan pesan teks hasil enkripsi (*chipertext)* ke citra digital menggunakan LSB.
3. Bagi penulis, dapat menerapkan dan mengembangkan ilmu pengetahuan terkait keamanan data, khususnya steganografi dan kriptografi untuk pesan teks pada citra digital.

1.4 Batasan Masalah

Adapun batasan masalah untuk 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 yang telah dienkripsi ke dalam file citra dengan bahasa pemrograman Java.

2. Agar penerima pesan dapat mengungkap pesan yang disisipkan pada file citra digital, file citra tersebut harus menggunakan media yang tidak mengubah atau mengkompresi file citra.
3. Format citra digital yang digunakan dan diuji pada penelitian ini adalah JPG, JPEG, dan PNG.
4. Algoritma yang digunakan untuk penyisipan pesan (steganografi) adalah LSB (*Least Significant Bit*) sedangkan algoritma yang digunakan untuk melakukan kriptografi adalah AES (*Advanced Encryption Standard*) dengan ukuran blok dan kunci 256 bit atau 32 *byte*.
5. Resolusi citra yang dapat digunakan sebagai media steganografi minimal 256 piksel (*width x height*) dengan jumlah bit per piksel (*bit depth*) 8.

1.5 Sistematika Penulisan

Penulisan laporan Skripsi ini dibagi ke dalam bab per bab untuk mempermudah pembahasan. Perincian pembahasan tiap bab pada laporan ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisikan tentang latar belakang, perumusan masalah, tujuan dan manfaat penelitian, batasan masalah, dan sistematika penulisan laporan.

BAB II LANDASAN TEORI

Bab ini berisi tentang landasan teori yang menjadi pendukung penelitian, antara lain model pengembangan perangkat lunak dengan Waterfall, metode pemrograman berorientasi obyek, pemodelan sistem dengan UML, steganografi dengan algoritma LSB, kriptografi dengan algoritma AES 256, citra digital, bahasa pemrograman Java, dan tinjauan penelitian terdahulu.

BAB III METODOLOGI PENELITIAN

Bab ini menyampaikan penggunaan model Waterfall dalam penelitian, pemrograman berorientasi obyek, alat bantu pemodelan sistem berupa UML, sampai dengan algoritma AES 256 dan algoritma LSB.

BAB IV HASIL DAN PEMBAHASAN

Bab ini membahas tentang simulasi algoritma AES 256 dan algoritma LSB, jadwal penelitian, analisa kebutuhan, analisa sistem berjalan, perancangan sistem, implementasi, dan pengujian.

BAB V PENUTUP

Bab ini berisikan kesimpulan dari hasil penelitian dan saran yang dapat digunakan untuk pengembangan hasil penelitian ini.