BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi saat ini telah mengalami kemajuan yang sangat pesat, menjadikannya sebagai komponen vital dalam kehidupan manusia. Teknologi ini memiliki kemampuan untuk menyelesaikan berbagai jenis pekerjaan yang beraneka ragam. Pertumbuhan teknologi informasi tak terpisahkan dari perkembangan matematika, karena setiap inovasi teknologi selalu melibatkan perhitungan matematis.

Dalam era teknologi canggih saat ini, kemudahan dalam mengakses informasi rahasia menjadi semakin meningkat, terutama melalui peran komputer. Individu yang ingin mengakses data atau informasi rahasia akan melakukan berbagai upaya, termasuk meretas, mencuri, atau mengintai. Oleh karena itu, penting untuk menyimpan data dengan tingkat keamanan yang tinggi, terutama saat mengirimnya melalui Internet. Media yang digunakan untuk menyimpan informasi ini dapat berupa berbagai jenis file, seperti gambar, audio, atau dokumen. Dengan demikian, orang yang tidak memiliki izin akses tidak akan dapat mengidentifikasi informasi tersebut dengan mudah.

Salah satu cara untuk menyembunyikan informasi adalah melalui teknik steganografi, yang dapat disempurnakan dengan menggunakan teknik kriptografi. Teknik ini melibatkan pengacakan informasi dengan menggunakan kunci tertentu untuk menjaga kerahasiaannya. Terdapat berbagai metode steganografi yang dapat digunakan, seperti LSB, EOF, DCT, dan lain sebagainya. Sementara itu, algoritma enkripsi terdiri dari dua jenis, yaitu enkripsi asimetri dan enkripsi simetris, dengan perbedaan terutama pada jenis kunci yang digunakan.

Enkripsi asimetris, juga dikenal sebagai enkripsi kunci publik, melibatkan penggunaan kunci publik dan kunci pribadi dalam proses enkripsi dan dekripsi. Contoh algoritma yang termasuk dalam kategori ini adalah DSA, RSA, dan lain sebagainya. Penelitian ini menggunakan metode steganografi Least Significant Bit (LSB) dan algoritma kriptografi simetris Advanced Encryption Standard (AES).

Hasil dari proses penyandian pesan rahasia adalah pesan acak yang sulit dipahami maknanya. Untuk menghindari kecurigaan, digunakan teknik penyembunyian pesan rahasia yang dikenal sebagai steganografi.

Adapun beberapa referensi dari penelitian terdahulu sebagai dasaran, Penelitian Dian Novanto, Yohanes Setiawan pada tahun 2018 mengenai Aplikasi Pengamanan Informasi Menggunakan Metode Least Significant Bit (LSB) dan Algoritma Kriptografi Advanced Encryption Standard (AES) [1], Penelitian Andre Chandra pada tahun 2021 mengenai Implementasi Penyisipan Teks Pada Citra Digital Dengan LSB Dan AES 256 [2], Penelitian Yulia Fatma, Afdhil Hafid, Heru Oktavian Dani pada tahun 2020 mengenai Peningkatan Keamanan Pengiriman Pesan Teks: Kombinasi Advanced Encryption Standard (AES) 128 dan Least Significant Bit (LSB) [3], Penelitian Mohammad Imron, Aditiya Pratama pada tahun 2022 mengenai Pengamanan E-Dokumen Berbasis Steganografi Dengan Kombinasi Advanced Encryption Standard (AES) 128 Bit [4], Penelitian Feri Rama Andika pada tahun 2020 mengenai Pengamanan File Menggunakan Advanced Encryption Standard Dan Least Significant Bit [5].

Berdasarkan latar belakang tersebut, permasalahan dan model yang dipakai maka penelitian ini akan diberikan judul "**IMPLEMENTASI PESAN TERSEMBUNYI PADA CITRA DIGITAL DENGAN ALGORITMA LEAST SIGNIFICANT BIT (LSB) DAN ADVANCED ENCRYPTION STANDARD (AES)**".

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dijelaskan sebelumnya, maka yang menjadi rumusan masalah dalam penelitian ini adalah "Bagaimana cara menyisipkan pesan tersembunyi pada file citra digital dengan mengkombinasikan algoritma Advanced Encryption Standard (AES) dan algoritma Least Significant Bit (LSB)?".

1.3 Tujuan dan Manfaat Penelitian

Tujuan dan manfaat pada penelitian ini adalah sebagai berikut :

1.3.1 Tujuan Penelitian

Dalam penyusunan penelitian ini mempunyai tujuan yang dilakukan berhubungan dengan steganografi menggunakan metode algoritma Least Significant Bit (LSB) dan algoritma kriptografi Advanced Encryption Standard (AES) yaitu untuk mengimplementasikan pesan tersembunyi pada file citra digital dengan menggunakan metode LSB serta algoritma AES untuk mengamankan data.

1.3.2 Manfaat Penelitian

Adapun manfaat penelitian dalam penelitian ini adalah :

1. Mampu membangun sebuah aplikasi untuk keamanan data dengan cara menyisipkan pesan teks tersembunyi kedalam Image dengan metode LSB dan kriptografi AES
2. Dapat memahami proses encoding dan decoding dalam penggunaan kombinasi teknik steganografi dengan LSB dan kriptografi AES, yang digunakan untuk mengamankan serta mengembalikan pesan, sekaligus menyisipkan pesan tersebut ke dalam sebuah berkas citra digital dalam bentuk gambar.

1.4 Batasan Masalah

Adapun batasan masalah memahami pembahasan topik permasalahan sebagai berikut:

1. Membangun aplikasi steganografi dan kriptografi untuk membuat pesan tersembunyi berupa teks yang telah dienskripsi ke dalam file citra digital berbentuk Image.
2. Untuk mengungkapkan pesan yang telah disisipkan pada citra digital, file citra digital tersebut tidak boleh melalui proses dikompres, diedit, diubah format, dan dirotasikan.
3. Format file citra digital yang dipakai dan diuji pada penelitian ini adalah format PNG, JPEG, dan JPEG.

4. Bahasa Pemrograman yang dipakai adalah bahasa pemrograman Java dengan software NetBeans versi 8.2.
5. Algoritma yang dipakai untuk menyisipkan pesan (steganografi) adalah LSB sedangkan algoritma yang dipakai untuk melakukan kriptografi adalah AES.

1.5 Sistematika Penulisan

Penulisan laporan Skripsi dibagi tiap bab untuk mempermudah pembahasan. Rincian pembahasan tiap bab pada penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini menjelaskan latar belakang, rumusan masalah, tujuan dan manfaat penelitian, batasan masalah, dan sistematika penulisan laporan

BAB II LANDASAN TEORI

Bab ini menjelaskan landasan teori yang menjadi dasaran penelitian, antara lain berupa model pengembangan perangkat lunak dengan prototype, metode pemrograman berorientasi obyek, pembuatan model dengan UML, steganografi dan kriptografi dengan algoritma LSB dan AES, file citra digital, bahasa pemrograman Java, dan tinjauan dari penelitian terdahulu.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan penggunaan model prototype dalam penelitian, pemrograman berorientasi obyek, alat bantu pemodelan sistem berupa UML, dan algoritma AES & algoritma LSB

BAB IV PEMBAHASAN

Bab ini menjelaskan tentang cara kerja algoritma AES dan LSB, analisa kebutuhan, analisa sistem berjalan, perancangan sistem, implementasi, dan pengujian.

BAB V PENUTUP

Bab ini menjelaskan kesimpulan hasil penelitian dan saran untuk evaluasi dari hasil penelitian ini.