BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi perangkat lunak semakin pesat dan mahal karena perubahan persyaratan yang cepat dan pengenalan teknologi baru [1]. Untuk pengembangan atau pemeliharaan perangkat lunak, tidak cukup hanya melindunginya, tetapi perlu menemukan cara yang lebih canggih untuk perlindungan [2]. Teknologi informasi saat ini lebih maju dibandingkan masa lalu yang masih memiliki banyak kekurangan [3]. Kemajuan teknologi ini memungkinkan manusia meningkatkan kualitas hidup dengan memanfaatkan teknologi untuk memenuhi kebutuhan, menciptakan nilai baru dalam kehidupan sosial, dan mendorong perkembangan manusia [4].

Teknologi modern memungkinkan manusia menggunakan jaringan yang sangat cepat untuk mencari informasi secara daring. Jaringan internet yang sebelumnya menggunakan 4G kini telah ditingkatkan menjadi 5G, yang kecepatannya hingga 20 kali lipat lebih cepat dari 4G. Bahkan, jaringan 6G sedang dipersiapkan untuk masa depan [5]. Seiring dengan kemajuan teknologi, keamanan juga harus ditingkatkan untuk melindungi dari serangan kejahatan di internet. Peningkatan penggunaan teknologi dan internet juga berdampak pada meningkatnya kejahatan daring oleh individu yang tidak bertanggung jawab untuk keuntungan pribadi. Salah satu bentuk kejahatan dunia maya adalah phishing [6].

Phishing adalah tindakan kriminal di internet yang bertujuan mencuri informasi pribadi korban. Kegiatan phishing dilakukan dengan tujuan mendapatkan informasi rahasia pengguna melalui email dan situs web palsu yang menyerupai situs web resmi[7]. Informasi yang dicari pelaku phishing mencakup kata sandi akun atau nomor kartu kredit. Email sering menjadi media utama untuk kegiatan phishing. Sebagai alat penting pertukaran informasi, email diperlukan oleh individu maupun lembaga. Dalam pertukaran informasi, sering terjadi pertukaran data

sensitif yang memerlukan perlindungan. Untuk menjaga keamanan pesan yang dikirim, enkripsi digunakan untuk mengamankan data digital sehingga tidak dapat dipahami oleh pihak yang tidak berwenang [8]. Dalam konteks keamanan lampiran email, teknologi yang dapat digunakan mencakup lapisan transport yang menggunakan algoritma seperti *Advanced Encryption Standard* (AES) dan *Spread Spectrum* [9].

Advanced Encryption Standard (AES) adalah algoritma enkripsi simetris yang diperkenalkan oleh *National Institute of Standards and Technology* (NIST) pada tahun 2001. AES menggantikan algoritma enkripsi sebelumnya, *Data Encryption Standard* (DES). Algoritma ini memiliki tiga variasi, yaitu AES-128, AES-192, dan AES-256, yang masing-masing memiliki panjang kunci yang berbeda. Semakin panjang kunci, semakin tinggi tingkat keamanannya [10]. Proses enkripsi AES melibatkan beberapa tahap, termasuk *SubBytes* (penggantian byte), *ShiftRows* (pergeseran baris), *MixColumns* (penggabungan kolom), dan *AddRoundKey* (penambahan kunci putaran). Setiap langkah diulang dalam beberapa putaran, tergantung pada panjang kunci yang digunakan [11].

Sementara itu, *Spread Spectrum* adalah metode transmisi yang menggunakan kode pseudo noise untuk menyebar energi sinyal dalam jalur komunikasi. Penerima akan mengumpulkan kembali sinyal menggunakan replikasi kode pseudo noise yang disinkronkan [12]. Dalam konteks steganografi, teknik *Spread Spectrum* menambahkan derau semu (pseudo noise) ke objek penutup. Karena karakteristiknya mirip dengan noise, spread spectrum sulit dideteksi, diinterferensi, atau dimanipulasi [13]. Masalah yang dihadapi dalam penelitian ini adalah bagaimana menjaga keamanan dan kerahasiaan data teks saat dikirim melalui jaringan yang rentan terhadap serangan. Data yang dienkripsi menggunakan metode kriptografi saja masih dapat menarik perhatian pihak yang tidak berwenang, sehingga diperlukan teknik tambahan untuk menyembunyikan keberadaan data tersebut agar tidak mudah dideteksi [14]. Oleh karena itu, penelitian ini bertujuan untuk mengimplementasikan kombinasi kriptografi AES dan steganografi Spread Spectrum dalam pengamanan data teks pada media

gambar. Selain itu, penelitian ini juga bertujuan untuk menganalisis efektivitas metode yang digunakan dalam menjaga kualitas gambar setelah penyisipan pesan, dengan mengukur Mean Square Error (MSE) dan Peak Signal-to-Noise Ratio (PSNR). Dengan metode ini, diharapkan data yang dikirim tidak hanya terenkripsi dengan aman tetapi juga tersembunyi dengan baik dalam media gambar, sehingga sulit dideteksi oleh pihak yang tidak berwenang.

1.2 Rumusan Masalah

Berdasarkan permasalahan yang telah diuraikan pada latar belakang penelitian, berikut adalah rumusan masalah yang ditemukan untuk penelitian, Seberapa efektif metode steganografi gambar dengan teknik *spread spectrum* dalam menyembunyikan data teks yang telah dienkripsi menggunakan algoritma AES.

1.3 Pertanyaan Penelitian

Berdasarkan rumusan masalah diatas, maka pertanyaan peneliti dalam melakukan penelitian ini yaitu:

1. Bagaimana mengamankan data teks dengan menggunakan kriptografi AES dan steganografi pada media gambar dengan metode *Spread Spectrum*?
2. Bagaimana melakukan analisis kinerja atau performa dari sistem kriptografi AES dan steganografi pada media gambar dengan metode *Spread Spectrum*?

1.4 Batasan Masalah

Berdasarkan rumusan masalah dan tujuan penelitian, maka untuk mewujudkan penelitian yang sesuai dengan masalah yang ada diperoleh batasan-batasan masalah penelitian sebagai berikut:

1. Pesan rahasia yang akan di proses berupa teks.
2. Proses enkripsi menggunakan AES 128-bit.
3. Media gambar yang digunakan untuk penyisipan pesan adalah gambar berformat png.
4. Proses penyisipan pesan menggunakan teknik *Spread Spectrum*

1.5 Tujuan Penelitian

Tujuan yang ingin dicapai dari penyusunan penelitian ini sebagai berikut :

1. Mengimplementasikan Kriptografi AES dan Steganografi pada media gambar dengan metode *Spread Spectrum* untuk pengamanan data teks.
2. Untuk mengetahui analisis kinerja atau performa dari sistem Kriptografi AES dan Steganografi pada media gambar dengan metode *Spread Spectrum* untuk pengamanan data teks.

1.6 Manfaat Penelitian

1. Dapat mengimplementasikan Kriptografi AES dan Steganografi pada media gambar dengan metode *Spread Spectrum* untuk pengamanan data teks
2. Dapat mengetahui dan melakukan analisis kinerja atau performa dari sistem Kriptografi AES dan Steganografi pada media gambar dengan metode *Spread Spectrum* untuk pengamanan data teks.