BAB I
PENDAHULUAN

1.1. Latar Belakang

Seiring berkembangnya zaman, teknologi pun ikut berkembang terutama teknologi di bidang informasi. Dalam berbagai bidang, banyak keuntungan yang diperoleh dari berkembangnya teknologi tersebut, baik dalam bidang ekonomi, pendidikan, maupun bidang lainnya. Saat ini, informasi dapat dengan mudah tersebar di mana pun dan kapan pun melalui media internet. Internet adalah sekumpulan jaringan komputer yang terhubung dengan berbagai situs pemerintah, grup, maupun perorangan dengan tujuan memberikan informasi kepada pengguna (Handoyo dkk, 2018). Di samping banyaknya keuntungan yang diperoleh dari perkembangan teknologi tersebut, ada banyak juga resikonya, seperti pencurian informasi, penyadapan data penting seseorang, sehingga diperlukan pengamanan data dan informasi.

Keamanan data sangat diperlukan oleh perseorangan, grup, maupun perusahaan. Keamanan digunakan untuk mencegah bocornya informasi atau dicurinya informasi oleh orang lain. Sejak zaman dahulu, ada banyak metode yang digunakan untuk mengamankan pesan, contohnya seperti mengamankan pesan dengan menyandikan atau mengubah pesan tersebut tidak bisa terbaca menggunakan berbagai perhitungan. Ilmu itu disebut *cryptography*.

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi (Jaya, 2017). Kriptografi pertama kali ditemukan oleh bangsa Mesir pada tahun 3000 SM. Kriptografi berasal dari kata *kriptos* dan *graphia* dari Bahasa Yunani yang artinya “tulisan yang tersembunyi”. Dalam kriptografi ada banyak metode yang digunakan untuk persandiannya. Semakin rumit metode yang digunakan maka pesan akan lebih susah dipecahkan.

Salah satu metode dalam pengamanan pesan adalah *Elliptic Curve Cryptography* (ECC). ECC termasuk dalam kriptografi asimetris, di mana kunci enkripsi dan kunci dekripsi berbeda. Kriptografi ini dikembangkan oleh Victor Miller dan Neal Koblitz (Zahra, 2021). ECC memanfaatkan permasalahan matematis kurva eliptik sebagai dasar keamanan pada algoritmanya. Keunggulan dari algoritma ECC adalah ukuran kunci enkripsi yang lebih kecil daripada algoritma asimetris lainnya tetapi memiliki tingkat keamanan yang sama.

Selain dengan menyandikan pesan, ada juga metode pengamanan pesan dengan cara menyembunyikan pesan ke dalam media lain seperti gambar, video, audio, maupun media lainnya agar orang lain hanya dapat melihat medianya saja, tidak dengan pesan yang disembunyikan. Ilmu ini disebut steganografi. Steganografi merupakan teknik menyembunyikan pesan pada media lain, contohnya seperti menyembunyikan pesan ke dalam media gambar agar tidak ada yang curiga bahwa gambar tersebut menyimpan pesan rahasia. Gambar yang telah disisipkan pesan disebut *stego-image.* Salah satu metode steganografi dalam pengamanan pesan adalah *Spread Spectrum*.

Spread Spectrum adalah metode komunikasi di mana sinyal informasi disebar diseluruh frekuensi yang tersedia dengan memilih tempat penyisipan data pada frekuensi yang rendah serta menambahkan *pseudo-noise* (PN) (Yusuf, 2020). Metode *Spread Spectrum* bekerja dengan menyisipkan dan menyebarkan data kedalam objek dengan melakukan perhitungan modulasi terlebih dahulu. Metode *Spread Spectrum* dipilih karena gambar hasil steganografi (*stego-image*) pada warna, ukuran, dan kualitas gambar asli tidak rusak ataupun berubah. Metode *Spread Spectrum* harus melalui operasi hitung dahulu sebelum menyisipkan pesan ke dalam gambar hal ini dinilai lebih aman dibanding metode steganografi lainnya, misal metode *Least Significant Bit* (LSB) yang langsung menyisipkan pesan tanpa melalui operasi apapun (Pakereng 2010).

Penelitian mengenai penggabungan ECC dengan steganografi antara lain telah dilakukan oleh Luthfan, dkk (2018). Mereka menyimpulkan bahwa penggabungan metode kriptografi dan steganografi terbukti dapat meningkatkan tingkat keamanan

suatu data. Dikarenakan penyisipan *noise* mengakibatkan penerima tidak berhak diharuskan mendekripsi semua data termasuk *noise*. Sedangkan penerima yang berhak tidak perlu mendekripsikan *noise*, tapi cukup mendekripsikan data yang berisi pesannya saja. Tetapi, semakin banyak *noise* semakin lama pula waktu untuk mendekripsikan data. Penelitian mengenai pengamanan pesan juga telah dilakukan oleh Zahra (2020) dan Athalla (2022). Mereka meneliti tentang bagaimana mengkonstruksi aplikasi program komputer untuk pengamanan pesan dengan metode kriptografi visual menggunakan algoritma ECC.

Pada penelitian ini, penulis menggabungkan ECC dengan steganografi metode *Spread Spectrum* untuk mengamankan pesan dengan cara mengenkripsi pesan memakai metode ECC lalu menyembunyikan hasil enkripsi (cipherteks) kedalam objek dengan metode *Spread Spectrum*. Jenis objek yang diterapkan pada penelitian ini adalah objek gambar. Pemilihan objek gambar bertujuan untuk mengurangi rasa curiga pihak yang tidak memiliki otoritas dalam mengambil informasi data teks. Metode dalam penelitian ini diharapkan dapat menjaga kerahasiaan isi pesan dari orang yang tidak berkepentingan dengan cara mengkombinasikan teknik kriptografi dan steganografi.

1.2. Rumusan Masalah

Berdasarkan latar belakang, maka dapat dirumuskan masalah yang berkaitan dengan penjelasan tersebut yaitu:

1. Bagaimana proses implementasi pengamanan pesan dengan kriptografi ECC dan steganografi *Spread Spectrum* ke dalam gambar?
2. Bagaimana konstruksi program aplikasi pengamanan pesan dengan kriptografi ECC dan steganografi *Spread Spectrum* dalam bentuk program komputer?

1.3. Tujuan Penelitian

Tujuan yang ditetapkan berdasarkan rumusan masalah tersebut adalah:

1. Untuk mengetahui proses implementasi pengamanan pesan dengan kriptografi ECC dan steganografi *Spread Spectrum* ke dalam gambar.

2. Memberikan gambaran dari implementasi kriptografi ECC dan steganografi *Spread Spectrum* dalam bentuk program komputer.

1.4. Manfaat Penelitian

Penelitian ini diharapkan bermanfaat dalam beberapa hal, sebagai berikut:

1. Pesan yang telah terenkripsi akan terjaga kerahasiaannya dan keasliannya.
2. Keberadaan pesan akan tersamarkan oleh bentuk *stego-image*, sehingga akan terjaga kerahasiaannya.

1.5. Batasan Masalah

Batasan masalah pada penelitian ini yaitu:

1. Pesan yang digunakan berupa data teks yang terdiri dari karakter-karakter yang termasuk dalam rentang ASCII 0 hingga 127.
2. Ukuran data teks harus lebih kecil dari ukuran data gambar supaya pesan dapat tersampaikan secara utuh.