BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi pada saat ini mempengaruhi banyaknya masyarakat yang bisa mengakses berbagai bentuk informasi dalam bentuk, data, dan dokumen, serta kemudahan bertukar informasi dan pengiriman pesan melalui *e-mail* (*publik dan privat*). Dalam hal ini dapat menimbulkan masalah baru, pada pengamanan file, dimana beberapa informasi, data dan dokumen (*file*) merupakan data rahasia milik pengguna. Banyak pihak akan mencari cara untuk mendapatkan dan mengakses data atau informasi yang dapat disalahgunakan oleh pihak yang tidak bertanggung jawab melalui *e-mail*. *E-mail* merupakan salah satu teknologi komunikasi yang paling banyak digunakan pada saat ini (Abdurrahman et al., 2018).

Dengan menggunakan *e-mail* dapat memberikan kemudahan yang cukup untuk mengirimkan informasi penting, berupa data dan dokumen melalui internet, tanpa perlu bertemu dengan penerima. Melalui *e-mail*, kita juga dapat bertukar informasi, data dan dokumen dengan sangat cepat, dan biaya yang dikeluarkan juga sangat rendah (Abdurrahman et al., 2018). Tetapi belakangan ini, sering terjadi masalah, antara lain pemalsuan *e-mail (spoofing),* penyalahgunaan *e-mail* (spam), peretas menggunakannya sebagai media penyebaran malware, kebocoran *e-mail* (*man-in-the-middle attack*), dan beberapa lainnya. Pada saat mengirim *e-mail*, perlu memperhatikan kerahasiaan, integritas, otentikasi, dan non-penyangkalan. Ketika informasi yang dikirimkan melalui *e-mail* perantara disimpan di media penyimpanan publik dan swasta, keamanannya harus terjamin (Zulfikar et al., 2019). Keamanan

diperlukan untuk mencegah pihak-pihak yang tidak bertanggung jawab mengakses isi dari dokumen yang dikirim melalui *e-mail*. Aplikasi *e-mail* dapat melindungi dokumen dengan aman, tetapi jika pihak yang tidak bertanggung jawab berhasil mencuri sandi pengguna, iya dapat masuk kedalam akun *e-mail* tersebut. Untuk itu, kita membutuhkan aplikasi keamanan file atau dokumen dan isi pesan di *e-mail (Abdurrahman et al., 2018).*

Untuk meningkatkan keamanan pada penelitian ini akan dibangun sebuah aplikasi keamanan data *e-mail* untuk pengiriman *e-mail* dengan mengkombinasikan kriptografi dan steganografi yang dapat digunakan untuk mengatasi masalah keamanan pada saat pengiriman informasi rahasia. Kriptografi merupakan studi yang dirancang untuk melindungi dan menjaga kerahasiaan data untuk dilindungi dengan enkripsi dan dekripsi (Zulfikar et al., 2019). Dengan menggunakan teknologi kriptografi, data rahasia memiliki keamanan kontrol akses, tetapi teks sandi yang terenkripsi akan mudah dideteksi oleh pihak ketiga dan dapat mengetahui kerahasiaan data tersebut. Selain itu, penerapan steganografi adalah untuk menjaga kerahasiaan data berupa bit data sebagai wadah bit dalam bentuk gambar digital. Steganografi juga dapat digunakan untuk menyampaikan pesan rahasia dalam wadah citra digital, karena sifat steganografi yang sulit dideteksi karena tersembunyi (Hafiz, 2019). Kelebihan dari steganografi terdapat pada pesan yang dikirim tidak menarik perhatian sehingga tidak menimbulkan kecurigaan oleh orang lain (Munir, 2019). Tujuan dari steganografi adalah memanipulasi sebuah objek yang digunakan untuk menyembunyikan pesan kedalamnya (Handoyo et al., 2018)

Penelitian ini menggunakan kombinasi steganografi LSB dan kriptografi AES. Pemilihan teknik ini berdasarkan bahwa teknik LSB merupakan teknik penyembunyian data yang bekerja pada domain spatial atau waktu (Indriyono, 2016). Dengan menggunakan metode bit terkecil, steganografi dapat dilakukan dengan memasukkan data ke dalam citra/gambar yang diinginkan (Hafiz, 2019). Selanjutnya peneliti menggunakan metode AES (*Advanced Encryption Standard*). Metode AES merupakan algoritma block cipher yang menggunakan teknik substitusi, mutasi dan bilangan bulat pada setiap blok untuk dienkripsi dan dideskripsikan. Algoritma AES (*Advanced Encryption Standard*) dipilih karena dirancang khusus untuk keamanan tingkat lanjut dan ketahanan terhadap berbagai jenis serangan, kesederhanaan desain, kekompakan kode dan kecepatan enkripsi, serta deskripsi setiap file atau data (Nuari et al., 2020).

Least Significant Bit (LSB), merupakan metode yang tidak terlalu kompleks dan penyimpanan pesan pada *cover object* juga cukup besar, sehingga data dapat disisipkan. Dasar metode ini adalah berdasarkan bilangan biner yaitu 0 dan 1, sehingga proses aplikasinya menjadi lebih mudah. Selain itu, metode ini sangat erat kaitannya dengan ukuran 1 bit yang hanya diganti dengan bit terakhir, maka *stego image* atau media penampung yang dihasilkan hampir sama persis dari sebelum dilakukan steganografi sehingga tidak mengubah *cover image* secara signifikan (Darwis, 2016). Kelebihan dari metode LSB adalah ukuran dimensi yang mengandung pesan tidak berubah secara signifikan, namun kekurangannya adalah kapasitas pesan yang akan disisipkan dibatasi sesuai dengan jumlah frame. (Riadi et

al., 2020). Algoritma yang digunakan dalam kriptografi adalah *Advanced Encryption Standard* (AES) menggunakan kunci yang sama dalam proses enkripsi dan deskripsi, sehingga data yang kita miliki akan sulit dimengerti maknanya. Teknologi algoritma digunakan untuk mentransformasi data dalam bentuk kode-kode tertentu, dengan tujuan agar informasi yang disimpan tidak dapat dibaca oleh pihak yang tidak berhak. Teknologi enkripsi metode AES akan digunakan untuk mengubah data atau informasi berupa teks biasa menjadi teks sandi. Selain itu, metode steganografi LSB akan digunakan untuk menyembunyikan ciphertext ke dalam format citra RGB. Secara garis besar, proses enkripsi AES mencakup 4 jenis konversi, yaitu *SubBytes, ShiftRows, MixColumns dan AddRoundKey*, sedangkan pada ronde terahir tidak dilakukan *transformasi Mixcolumns*. Proses dekripsi AES menggunakan *transformasi invers, yaitu InvSubBytes, InvShiftiRows, InvsMixColumns. AddRoundKey* merupakan transformasi yang bersifat self invers dengan syarat menggunakan kunci yang sama (Darwis et al., 2018). Dalam penelitian yang dilakukan (Sodikin et al., 2020) menggunakan metode AES untuk melakukan penelitian keamanan *e-commerce*, dalam proses enkripsi dan deskripsi algoritma, ada bidang tunggal terbatas unik yang digunakan untuk mengubah bilangan prima dan pemilihan polynomial biner berderajat delapan. Algoritma AES juga dapat menahan berbagai serangan. Fungsi algoritma AES jauh melebihi DES, jika sebuah mesin yang digunakan untuk memecahkan DES digunakan untuk memecahkan AES, maka akan membutuhkan jutaan tahun untuk menyelesaikan AES (Rahman et al., 2017).

Untuk menjamin kerahasiaan informasi yang dikirim melalui *e-mail*, informasi tersebut harus ditempatkan dalam wadah pengiriman yang dapat meningkatkan keamanan informasi tersebut. Wadah informasi ini merupakan media yang dapat berupa berbagai jenis file, seperti file gambar, file suara, dan file dokumen. Sehingga informasi tidak akan dikenali secara langsung oleh pihak yang berniat untuk mendapatkan informasi tersebut tanpa hak akses (Novianto & Setiawan, 2019). Dalam penelitian ini steganografi yang digunakan berupa gambar. Karena gambar adalah matriks titik (*piksel*), setiap titik menunjukkan rona atau tingkat warna pada posisi spasialnya. Oleh karena itu, citra secara matematis dapat direpresentasikan sebagai matriks, dimana angka menunjukkan nilai piksel (Antono et al., 2020). Alasan lainnya adalah banyaknya algoritma steganografi yang dapat digunakan untuk wadah media berupa gambar (Putra et al., 2018)

1.2 Rumusan Masalah

Berdasarkan latar belakang, maka dapat dirumuskan suatu permasalahan sebagai berikut :

1. Bagaimana cara membuat aplikasi pengiriman surat elektronik *(e-mail)* untuk menjaga keamanan data menggunakan algoritma *Advanced Encryption Standard* (AES) dan steganografi *Least Significant Bit* (LSB)?
2. Bagaimana implementasi kombinasi teknik kriptografi *Advanced Encryption Standard* (AES) dan steganografi *Least Significant Bit* (LSB) dalam mengamankan penyampaian informasi melalui media gambar?

1.3 Batasan Masalah

Dalam pembuatan aplikasi ini agar pembahasan dalam penelitian ini bisa terarah dan tidak melebar dari konsep yang dikerjakan, maka diberikan beberapa batasan sebagai berikut:

1. Cover yang digunakan sebagai media untuk menampung informasi pesan adalah gambar RGB.
2. Format gambar yang digunakan adalah jpg.
3. Informasi yang akan disisipkan adalah dalam bentuk teks.
4. Bahasa pemrograman yang digunakan adalah PHP.
5. Metode kriptografi yang digunakan adalah AES 128 bit.
6. Dimensi gambar 512x512 pixel.

1.4 Tujuan Penelitian

Beberapa tujuan yang ingin dicapai dalam penelitian ini antara lain sebagai berikut:

1. Membuat sebuah aplikasi yang dapat mengenkripsi dan mendekripsi pesan teks menggunakan algoritma kriptografi AES dan juga sebuah aplikasi yang dapat menyisipkan dan mengekstrak cipherteks berupa blok-blok integer dalam media berupa citra digital menggunakan algoritma LSB.
2. Dapat menerapkan teknik kriptografi AES dan steganografi LSB ke dalam sebuah aplikasi yang dapat digunakan untuk mengirimkan surat elektronik (*e-mail*) melalui media gambar.

1.5 Manfaat Penelitian

Manfaat yang di peroleh dari penelitian ini adalah

1. Dengan melakukan enkripsi dan dekripsi pada isi pesan *e-mail* dan file *e-mail*, sehingga apabila akun *e-mail* seseorang menjadi korban kejahatan hacker, maka hacker tidak dapat membaca isi dari pesan *e-mail* dan file *e-mail* yang ada.
2. Dengan menggunakan aplikasi ini, diharapkan pengguna akan dapat melakukan pertukaran data atau informasi yang sifatnya rahasia dan penting tanpa takut akan ada pihak lain yang dapat membaca atau mengetahui isi pesan dan *file* tersebut.