

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kriptografi adalah ilmu yang berfokus pada metode enkripsi di mana data diubah menjadi bentuk yang sulit dimengerti tanpa mengetahui kunci dekripsi yang sesuai (Kromodimoeljo, 2009). Salah satu algoritma kriptografi yang populer adalah *Advanced Encryption Standard* yang merupakan pengganti algoritma *Data Encryption Standard* atau disingkat DES.

Sedangkan steganografi adalah teknik yang digunakan untuk menyembunyikan keberadaan pesan atau data di dalam suatu media seperti gambar atau audio tanpa menarik perhatian. Dalam steganografi, pesan tetap ada, tapi tidak terlihat oleh mata (Stallings, 2017). Salah satu metode steganografi yang digunakan adalah *end of file* di mana pesan disisipkan di bagian akhir media yang digunakan.

Dengan kombinasi antara algoritma kriptografi AES dan steganografi end of file tentu dapat meningkatkan keamanan pesan dan informasi yang ingin dirahasiakan dengan tujuan agar pesan dan informasi tersebut tidak disalahgunakan oleh pihak yang tidak bertanggungjawab. Algoritma kriptografi AES dapat mengacak pesan dan informasi sehingga menghasilkan sesuatu yang tidak bermakna sedangkan steganografi end of file menyisipkan pesan ke suatu media penampung agar pesan dan informasi yang sudah teracak dapat disembunyikan.

Walaupun cara tersebut dapat meningkatkan keamanan pesan dan informasi, tapi ketika pesan yang disisipkan semakin panjang maka media penampung pesan juga akan semakin besar ukurannya. Tentunya ini akan menimbulkan kecurigaan yang baru bahwa ada sesuatu yang tersimpan pada media penampung tersebut.

Pada penelitian terdahulu oleh Putri, dkk. (2020) dengan judul “Implementasi Kriptografi Dengan Algoritma *Advanced Encryption Standard (AES) 128 Bit* Dan Steganografi Menggunakan Metode *End Of File (EOF)* Berbasis Java Desktop Pada Dinas Pendidikan Kabupaten Tangerang” penelitian tersebut membahas tentang mengamankan file seperti .docx, .doc, .xlsx, .xls, dan

.jpg. Menghasilkan kesimpulan bahwa algoritma AES 128 bit dan steganografi *end of file* dapat meningkatkan keamanan file.

Pada penelitian yang dilakukan oleh Handayani, dkk. (2021) berjudul “Implementasi Steganografi Dengan Metode End Of File (EOF) Untuk Menyisipkan Pesan Teks Pada Gambar” membahas tentang bagaimana cara menggunakan metode EOF untuk menyembunyikan pesan teks pada gambar dengan kesimpulan bahwa menyisipkan pesan diakhir file menghasilkan gambar dengan kualitas yang baik karena nilai pixel tidak berubah.

Dan pada penelitian yang dilakukan oleh Pramusinto, dkk (2019) dengan judul “Apilkasi Pengamanan File Dengan Metode Kriptografi AES 192, RC4 Dan Metode Kompresi Huffman” membahas tentang pembuatan sebuah aplikasi berbasis web yang dapat mengamankan dokumen digital dengan menggunakan algoritma kompresi Huffman, kriptografi AES 192, dan RC4. menghasilkan kesimpulan bahwa algoritma huffman berhasil mengecilkan ukuran hasil enkripsi dari algoritma AES dan RC4.

Dari penjelasan serta pemaparan diatas peneliti akan mencoba mengkombinasikan algoritma AES 128 bit untuk mengenkripsi pesan dan steganografi EOF untuk menyembunyikan pesan dengan algoritma *huffman* sebagai algoritma kompresi dengan tujuan agar ukuran media penampung pesan tidak terlalu besar. Pada penelitian ini menggunakan pesan dengan panjang 100 – 1000 kata dan menggunakan citra *grayscale* sebagai media penampung pesan. Judul penelitian yang akan peneliti angkat yaitu “Implementasi Kriptografi AES, Steganografi EOF, dan Kompresi Huffman untuk Mengamankan Pesan ke dalam Citra Grayscale”.

1.2 Rumusan Masalah

Adapun rumusan masalah dari latar belakang adalah sebagai berikut:

1. Bagaimana hasil dari algoritma kompresi huffman terhadap ukuran media penampung pesan?
2. Bagaimana hasil dari pesan yang telah melewati proses dekompresi, ekstrasi, dan dekripsi?

1.3 Batasan masalah

Agar pembahasan tidak melebar maka penulis membatasi permasalahan sebagai berikut:

1. Media yang digunakan untuk menyisipkan pesan merupakan media gambar berformat *bmp*.
2. Media gambar yang digunakan merupakan citra grayscale dengan ukuran 100 x 100 pixel, 200 x 200 pixel, 300 x 300 pixel, 400 x 400 pixel, dan 500 x 500 pixel.
3. Pesan yang diamankan merupakan pesan tulisan dengan panjang 100 sampai 1000 kata.
4. Pada penelitian ini tidak membahas media pengiriman pesan.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah membuat sistem berbasis web yang digunakan untuk meningkatkan keamanan pesan dengan mengimplementasikan algoritma kriptografi *AES 128 bit* dan steganografi *end of file* serta menerapkan algoritma huffman untuk proses kompresi agar ukuran gambar yang telah disisipkan pesan tidak terlalu besar.

1.5 Manfaat Penelitian

Adapun manfaat yang dapat diambil dari penelitian ini adalah :

1. Dengan adanya penelitian ini proses pertukaran pesan rahasia yang disisipkan pada media gambar dapat dilakukan dengan cepat karena ukuran gambar telah dikompres menggunakan algoritma huffman dan dapat menghilangkan kecurigaan apabila ada pihak yang tidak berwenang mendapatkan gambar tersebut.
2. Dengan adanya penelitian ini diharapkan dapat menambah pengetahuan serta dapat dijadikan referensi bagi pembaca dan individu yang tertarik dibidang kriptografi, steganografi, dan kompresi data.

1.6 Sistematika Penulisan

Penulisan skripsi ini terdiri dari beberapa bab atau bagian sebagai berikut :

BAB I PENDAHULUAN

Bab ini terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi tentang penelitian terdahulu dan landasan teori yang berkaitan dengan penelitian yang dilakukan.

BAB III METODE PENELITIAN

Pada bab ini membahas tentang implementasi serta analisis dari metode yang digunakan untuk mengamankan pesan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi hasil dari metode yang digunakan yaitu *Advanced Encryption Standard*, Steganografi EOF, dan kompresi huffman. Serta antar muka sistem yang telah dibuat.

BAB V PENUTUP

Pada bab ini berisi tentang kesimpulan dari hasil penelitian yang telah dilakukan serta saran dari peneliti untuk penelitian yang akan datang.