BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan data merupakan salah satu aspek yang sangat penting dalam era digital saat ini. Semakin banyak data yang dikirimkan dan disimpan secara elektronik, baik untuk keperluan pribadi maupun bisnis, menuntut adanya metode pengamanan data yang efektif. Masalah utama yang dihadapi adalah bagaimana melindungi data dari akses yang tidak sah dan menjaga kerahasiaan informasi. *Advanced Encryption Standard* (AES) merupakan salah satu algoritma enkripsi yang terkenal karena kekuatannya dalam melindungi data. AES menyediakan enkripsi yang kuat dan telah digunakan secara luas dalam berbagai aplikasi keamanan data.

Selain enkripsi, steganografi merupakan teknik penting lainnya yang digunakan untuk meningkatkan keamanan data. Steganografi adalah seni menyembunyikan informasi dalam media lain, seperti gambar atau audio, sehingga informasi tersebut tidak terdeteksi oleh pihak yang tidak berwenang. Salah satu teknik steganografi yang efektif adalah *Bit-Plane Complexity Segmentation* (BPCS). BPCS mampu menyembunyikan data dalam gambar digital dengan mengubah *bit-plane* yang memiliki kompleksitas tinggi, sehingga perubahan pada gambar tidak terlihat signifikan oleh mata manusia.

Dengan menggabungkan enkripsi AES dan steganografi BPCS, kita dapat mencapai tingkat keamanan yang lebih tinggi. Enkripsi AES akan mengenkripsi data teks sehingga tidak dapat dibaca oleh pihak yang tidak berwenang, sementara steganografi BPCS akan menyembunyikan data terenkripsi dalam gambar digital, membuatnya lebih sulit untuk dideteksi. Pendekatan ini tidak hanya melindungi data melalui enkripsi tetapi juga menyembunyikan keberadaan data tersebut.

Manfaat dan kontribusi penelitian ini adalah untuk mengembangkan metode keamanan data yang lebih efektif dan dapat diterapkan dalam berbagai aplikasi, baik untuk keperluan pribadi maupun bisnis. Penelitian ini juga akan memberikan panduan teknis bagi pengembang sistem keamanan data serta menambah wawasan di bidang keamanan data.

1.2 Rumusan Masalah

1. Bagaimana mengimplementasikan algoritma AES untuk enkripsi file teks?
2. Bagaimana mengimplementasikan teknik steganografi BPCS untuk menyembunyikan file teks?

1.3 Batasan Masalah

Penelitian ini hanya berfokus pada penerapan algoritma *Advanced Encryption Standard* (AES) untuk enkripsi file teks, dan juga teknik steganografi *Bit-Plane Complexity Segmentation* (BPCS) untuk menyembunyikan file teks.

1.4 Tujuan Penelitian

1. Mengimplementasikan algoritma AES untuk enkripsi file teks.
2. Mengimplementasikan teknik steganografi BPCS untuk menyembunyikan file teks.
3. Menganalisis efektivitas kombinasi antara AES dan steganografi BPCS dalam meningkatkan keamanan file teks.

1.5 Manfaat Penelitian

1. Menghasilkan metode yang lebih efektif dalam melindungi data dengan menggabungkan enkripsi AES dan steganografi BPCS.
2. Memberikan panduan teknis bagi pengembang sistem keamanan data dalam mengimplementasikan kombinasi metode ini.
3. Menambah pengetahuan dan literatur di bidang keamanan data, khususnya mengenai kombinasi metode enkripsi dan steganografi.

1.6 Kajian Terdahulu

1. Pada Jurnal Implementasi Kriptografi Pada Keamanan Data Menggunakan Algoritma *Advanced Encriyption Standard* (AES) Brikitha Olivia Putri Irine Irawan (2023). Membahas mengenai penggunaan algoritma *Advanced Encryption Standard* (AES) dapat digunakan untuk meningkatkan keamanan data dalam sistem informasi yang semakin kompleks. Penelitian ini menunjukkan bahwa AES mampu mengubah data menjadi bentuk yang tidak bisa dibaca, sehingga aman dari akses tidak sah. Dengan proses dekripsi, data dapat kembali ke bentuk aslinya

menggunakan kunci yang benar, menjadikan AES pilihan yang efektif untuk menjaga kerahasiaan dan informasi sensitif.

2. Pada Jurnal Implementasi Steganografi dengan Metode *Bit-Plane Complexity Segmentation* (BPCS) untuk Dokumen Citra Terkompresi yang ditulis oleh Arya Widyanarko (2023). Membahas mengenai penggunaan metode Bit-Plane Complexity Segmentation (BPCS) untuk menyembunyikan informasi rahasia dalam dokumen citra terkompresi. Steganografi diterapkan untuk menyisipkan data tanpa menarik perhatian, dan BPCS menawarkan kapasitas penyisipan yang lebih besar dibandingkan teknik lain. Penelitian ini mengembangkan perangkat lunak bernama *Secret-Postcard* dan menganalisis tiga format citra—JPEG, GIF, dan PNG—untuk menemukan yang paling sesuai untuk digunakan.
3. Pada Jurnal Implementasi Aplikasi Steganografi Berbasis *Web* Menggunakan Algoritma LSB Dan BPCS yang ditulis oleh Laily Farkhah Adhimah dkk. (2023). Membahas mengenai aplikasi steganografi berbasis *web* yang menggabungkan algoritma *Least Significant Bit* (LSB) dan *Bit-Plane Complexity Segmentation* (BPCS). Aplikasi ini dirancang agar pengguna dapat dengan mudah menyisipkan data ke dalam gambar dan dibangun menggunakan HTML, CSS, dan JavaScript untuk akses yang mudah melalui browser. Hasil penelitian menunjukkan bahwa aplikasi ini berhasil menyisipkan informasi rahasia dengan efektif.