BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era digital saat ini, internet telah menjadi media utama dalam pertukaran informasi, khususnya dalam bentuk citra digital. Setiap hari, diperkirakan lebih dari 350 juta gambar diunggah secara global, menjadikannya bagian dari fenomena Big Data [1]. Banyak dari gambar tersebut memuat informasi bersifat pribadi atau sensitif, seperti dalam bidang medis, militer, atau komunikasi pribadi, sehingga membutuhkan sistem pengamanan yang andal untuk mencegah penyalahgunaan dan pelanggaran privasi.

Citra digital memiliki karakteristik khusus, seperti ukuran file yang besar, tingkat redundansi tinggi, serta korelasi piksel yang kuat. Hal ini menyebabkan metode enkripsi konvensional seperti RSA dan DES yang dirancang untuk teks kurang mampu menyamarkan struktur visual gambar bila langsung diterapkan pada gambar [2]. Tantangan lainnya adalah menjaga keseimbangan antara keamanan dan efisiensi, sebagai contoh gambar setelah dienkripsi tidak menjadi dua kali lebih besar, proses enkripsi tidak butuh waktu terlalu lama, dan format gambar tetap bisa dikirim/diterima tanpa rusak. Hal ini tentu agar proses enkripsi tidak menyebabkan pembengkakan ukuran file atau perubahan format yang mengganggu fungsionalitas.

Salah satu solusi yang berkembang adalah penggunaan enkripsi gambar, yang mengubah gambar asli menjadi bentuk terenkripsi yang tidak dapat dikenali tanpa kunci yang sesuai. Teknik ini memungkinkan pengamanan secara selektif serta pemulihan gambar secara utuh dan berkualitas oleh penerima yang sah [3]. Algoritma Advanced Encryption Standard (AES) dengan mode Cipher Block Chaining (CBC) menjadi salah satu metode yang potensial, karena mampu menggabungkan kecepatan dan keamanan data citra dalam proses enkripsi [4].

Mode CBC bekerja dengan mengaitkan setiap blok data dengan blok sebelumnya dan menggunakan initialization vector sebagai elemen acak awal. Hal

ini menghasilkan sensitivitas tinggi terhadap perubahan kecil dalam data [5]. Untuk mengevaluasi performanya, digunakan metrik kualitas seperti MSE, PSNR, dan SSIM, serta metrik ketahanan seperti NPCR, UACI, dan Correlation Coefficient (CC) [6] - [8] . Pendekatan ini memberikan analisis menyeluruh terhadap kualitas dan keamanan data citra pada hasil enkripsi, serta mendukung pengembangan sistem perlindungan data citra yang lebih efektif.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas maka dapat rumusan masalah yaitu bagaimana mengimplementasikan algoritma AES-CBC (Cipher Block Chaining) untuk enkripsi dan dekripsi file gambar serta mengevaluasi efektivitasnya menggunakan metrik *Encryption Quality* dan *Differential Analysis*?.

1.3 Batasan Masalah

Untuk menghindari pelebaran masalah yang diuraikan, maka lingkup penelitian dibatasi oleh permasalahan sebagai berikut:

1. Algoritma enkripsi yang akan digunakan dalam penelitian ini adalah AES-CBC (Cipher Block Chaining).
2. Fokus utama adalah pada pengujian algoritma AES mode CBC untuk meningkatkan keamanan dan keandalan pengamanan data citra.
3. Penelitian ini tidak akan membahas aspek-aspek terkait dengan steganografi, namun akan berfokus pada enkripsi dan dekripsi foto dalam aspek keamanan data citra dan.
4. Tipe data yang akan digunakan untuk evaluasi berupa gambar color dan grayscale dengan resolusi 512 x 512.

1.4 Tujuan Penelitian

Penelitian ini dilakukan dengan tujuan sebagai berikut:

1. Mengimplementasikan atau menerapkan algoritma AES-CBC (Cipher Block Chaining) untuk mengenkripsi dan dekripsi data file gambar.
2. Mengevaluasi hasil enkripsi dan dekripsi menggunakan metode *Encryption Quality* dan *Differential Analysis* kemudian mengevaluasi keandalan AES-

CBC (Cipher Block Chaining) dalam melindungi data gambar.

1.5 Manfaat Penelitian

Penelitian menggunakan Algoritma Kriptografi AES-CBC (Cipher Block Chaining) dilakukan dengan harapan menghasilkan manfaat sebagai berikut:

1. Meningkatkan keamanan dan keandalan pengamanan data citra file gambar.
2. Memberikan kontribusi terhadap pemahaman tentang penerapan kriptografi dalam melindungi data citra gambar.

1.6 Sistematika Penulisan

Pada penelitian ini terdiri dari 5 BAB, berdasarkan sistematika penulisan sebagai berikut ;

BAB I : Pendahuluan

Pada bab ini berisikan uraian singkat mengenai latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II : Landasan Teori

Pada bab ini akan menjelaskan teori – teori penunjang yang mendukung terhadap Analisis Evaluasi Kinerja Quality & Differential Analysis pada Algoritma AES-CBC

BAB III Metodelogi Penelitian berisi penjelasan tentang alur penelitian yang di gunakan untuk mempermudah dalam proses penelitian, alat dan bahan penelitian.

BAB IV Pembahasan berisi pengumpulan dataset, implementasi algoritma AES-CBC, evaluasi kinerja metrik, dan Kelebihan dan Keterbatasan Penelitian.

BAB V Berisi kesimpulan dari hasil akhir pengujian algoritma dan saran.