BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Peneliti mengamati peningkatan insiden keamanan siber yang mengkhawatirkan akibat pesatnya perkembangan teknologi komunikasi, seperti pencurian data [1]. Perlindungan informasi menjadi sangat mendesak karena metode komunikasi konvensional rentan terhadap intersepsi, sehingga steganografi diperlukan untuk menyembunyikan pesan tanpa memicu kecurigaan [2]. Berbeda dengan kriptografi yang hasil acakannya terlihat mencurigakan, steganografi bertujuan membuat komunikasi rahasia sama sekali tidak kasat mata oleh pengamat [4]. Oleh karena itu, pengembangan metode steganografi yang tangguh menjadi solusi krusial untuk memastikan keamanan pertukaran data di jaringan publik [5].

Dalam upaya menyembunyikan data tersebut, Peneliti memilih format citra JPEG sebagai media penampung karena efisiensinya dalam menangani gradien warna kompleks dibandingkan format lain [6]. Meskipun sangat dominan digunakan, karakteristik kompresi *lossy* pada JPEG menimbulkan tantangan tersendiri bagi metode steganografi tradisional [6]. Peneliti menemukan bahwa metode domain spasial seperti *Least Significant Bit* (LSB) tidak efektif karena data mudah hilang akibat pembuangan frekuensi tinggi saat proses kompresi komputasi [7]. Kondisi inilah yang mengharuskan adaptasi teknik steganografi beralih ke domain frekuensi menggunakan *Discrete Cosine Transform* (DCT) [8].

Walaupun pendekatan domain frekuensi memberikan perlindungan yang lebih baik dari kompresi, teknik ini tidak sepenuhnya bebas dari celah keamanan karena penyisipan data pada koefisien DCT berisiko meninggalkan jejak statistik yang dapat dideteksi [9]. Modifikasi koefisien secara kaku sering kali mengubah bentuk histogram secara tidak wajar, sehingga rentan terhadap serangan steganalisis statistik seperti analisis *Regular-Singular* (RS) [10]. Kurangnya perhatian pada kesamaan konten antar blok dalam proses tersebut menyebabkan distorsi yang semakin memudahkan deteksi oleh pihak ketiga [11]. Selain rentan secara statistik, modifikasi ini juga berpotensi menurunkan kualitas visual yang secara langsung memengaruhi nilai *Peak Signal-to-Noise Ratio* (PSNR) [12]. Oleh karena itu,

menjaga keseimbangan yang optimal antara kapasitas penyisipan dan imperseptibilitas visual menjadi tantangan utama dalam steganografi transformasi saat ini [13].

Untuk mengatasi celah keamanan statistik dan degradasi visual tersebut, Peneliti mengusulkan pendekatan adaptif yang lebih dinamis dalam memodifikasi koefisien DCT [14]. Fokus utama dari teknik ini adalah meminimalkan perubahan statistik agar pesan yang disisipkan tahan terhadap serangan analisis modern [1]. Sistem ini dirancang untuk menjaga tingkat distorsi tetap berada di bawah batas persepsi penglihatan manusia dengan target capaian nilai PSNR yang tinggi [15]. Guna mewujudkannya, Peneliti menargetkan penyisipan pesan pada koefisien frekuensi menengah untuk menghindari artefak kompresi [7]. Tujuan akhirnya adalah mempertahankan integritas citra asli sekaligus mengamankan data yang tersembunyi di dalamnya [3].

Berdasarkan pemaparan masalah dan urgensi solusi di atas, penelitian ini bertujuan untuk meningkatkan teknik steganografi DCT pada JPEG guna mengurangi risiko deteksi histogram serta mempertahankan nilai PSNR yang optimal. Signifikansinya terletak pada penyediaan metode komunikasi yang aman dengan memanfaatkan popularitas format JPEG tanpa mengorbankan kualitas visual [6]. Peneliti berharap eksperimen ini dapat memberikan kontribusi nyata dalam melawan ancaman steganalisis statistik yang semakin canggih. Untuk membuktikan bahwa sistem yang dibangun benar-benar tangguh dari deteksi pihak ketiga, maka diperlukan sebuah evaluasi yang komprehensif. Kebutuhan untuk memvalidasi seberapa baik kualitas visual (*imperceptibility*) dan seberapa efektif penurunan selisih entropi yang dihasilkan oleh algoritma adaptif inilah yang kemudian ditarik menjadi rumusan masalah dalam penelitian ini.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan sebelumnya, Peneliti merumuskan masalah-masalah yang akan diselesaikan dalam penelitian ini sebagai berikut:

1. Bagaimana kinerja metode *Adaptive* LSB *Matching* pada citra JPEG

dalam mempertahankan kualitas visual (*imperceptibility*) jika dibandingkan dengan metode DCT Standar?

2. Seberapa efektif penerapan teknik modifikasi nilai koefisien ($X \pm 1$) pada frekuensi rendah-menengah dalam meminimalkan deteksi statistik berbasis analisis entropi?

1.3 Batasan Masalah

Agar pembahasan penelitian ini lebih terarah dan tidak meluas, Peneliti menetapkan batasan masalah sebagai berikut:

1. Objek Penelitian: Media penampung (*cover image*) yang digunakan adalah citra digital berformat JPEG yang dikonversi ke *grayscale* dengan dimensi ternormalisasi 512×512 piksel.
2. Metode: Metode yang dikembangkan adalah steganografi berbasis *Discrete Cosine Transform* (DCT) menggunakan teknik *Adaptive* LSB *Matching* dengan mekanisme penyesuaian nilai ($X \pm 1$) pada koefisien frekuensi rendah hingga menengah.
3. Data Pesan: Pesan rahasia yang disisipkan berupa teks biner dengan panjang maksimum 144 bit (sebagai *Proof of Concept* untuk validasi stabilitas entropi).
4. Parameter Pengujian: Variabel yang diukur untuk menentukan keberhasilan sistem adalah kualitas visual menggunakan *Peak Signal-to-Noise Ratio* (PSNR), keamanan statistik menggunakan analisis Selisih Entropi (ΔH), dan integritas pesan menggunakan *Bit Error Rate* (BER).
5. Lingkungan Pengembangan: Implementasi algoritma dilakukan menggunakan bahasa pemrograman Python dengan pustaka OpenCV, NumPy, dan SciPy.

1.4 Tujuan Penelitian

Tujuan yang akan dicapai oleh Peneliti dalam penelitian ini adalah:

1. Mengimplementasikan teknik steganografi *Adaptive* LSB *Matching*

pada domain DCT citra JPEG untuk menyembunyikan pesan rahasia.

2. Menganalisis perbandingan kualitas visual citra hasil steganografi (*stego-image*) antara metode usulan dengan metode DCT Standar berdasarkan nilai PSNR.
3. Membuktikan efektivitas metode usulan dalam mengurangi risiko deteksi statistik dengan menekan nilai selisih entropi (ΔH) seminimal mungkin.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat baik secara teoritis maupun praktis sebagai berikut:

1. Manfaat Teoritis
- Memberikan kontribusi keilmuan mengenai efektivitas penggunaan teknik LSB *Matching* ($X \pm 1$) pada koefisien frekuensi rendah-menengah dalam domain DCT.
- Menjadi referensi akademik bagi peneliti selanjutnya yang ingin mengembangkan teknik steganografi resisten terhadap serangan steganalisis statistik modern.

2. Manfaat Praktis
- Bagi Praktisi Keamanan Siber: Menyediakan alternatif metode pengamanan transmisi data rahasia (seperti kunci kriptografi atau tanda tangan digital) melalui media gambar JPEG yang aman dari deteksi visual maupun statistik di jaringan publik.
- Bagi Pengguna Umum: Memberikan solusi keamanan privasi untuk menyembunyikan informasi sensitif ke dalam media digital yang umum digunakan tanpa menimbulkan kecurigaan pihak ketiga.

1.6 Sistematika Penulisan

Untuk memberikan gambaran yang menyeluruh dan sistematis mengenai penyusunan skripsi ini, materi pembahasan dibagi menjadi lima bab dengan rincian

sebagai berikut:

BAB I PENDAHULUAN Bab ini menguraikan latar belakang masalah mengenai kerentanan steganografi DCT konvensional terhadap deteksi entropi, rumusan masalah yang berfokus pada keseimbangan kualitas visual dan keamanan statistik, batasan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA Bab ini berisi kajian teori yang mendasari penelitian, meliputi konsep dasar steganografi, format kompresi citra JPEG, transformasi *Discrete Cosine Transform* (DCT), teori entropi informasi, serta algoritma *Least Significant Bit* (LSB) *Matching*. Bab ini juga memuat tinjauan penelitian terdahulu (*state of the art*) untuk memposisikan kontribusi penelitian ini terhadap literatur yang ada.

BAB III METODE PENELITIAN Bab ini menjelaskan tahapan dan metode yang digunakan dalam penyelesaian masalah, mulai dari analisis kebutuhan sistem, perancangan algoritma *Adaptive* LSB *Matching* $(X \pm 1)$ pada domain frekuensi, alur eksperimen perbandingan dengan metode standar, hingga teknik analisis data menggunakan parameter PSNR dan selisih entropi (ΔH).

BAB IV HASIL DAN PEMBAHASAN Bab ini memaparkan hasil implementasi dan pengujian sistem terhadap citra sampel. Pembahasan difokuskan pada analisis komparatif antara metode usulan dan metode standar berdasarkan data kuantitatif kualitas visual, keamanan statistik (entropi), dan akurasi ekstraksi pesan, serta interpretasi terhadap temuan tersebut.

BAB V PENUTUP Bab ini merupakan bagian akhir yang memuat kesimpulan dari seluruh hasil penelitian yang menjawab rumusan masalah, serta saran-saran konstruktif bagi pengembangan penelitian steganografi di masa mendatang.