BAB I PENDAHULUAN

1.1 Latar Belakang

Di era modern saat ini, kemajuan teknologi internet telah merevolusi dan mengubah cara kita berkomunikasi. Komunikasi digital menjadi semakin mudah dan terjangkau berkat internet. Namun, kemudahan ini juga disertai dengan risiko keamanan yang tinggi. Tanpa adanya sistem keamanan yang memadai, data penting dan bersifat rahasia berisiko dicuri saat proses pengiriman [1]. Ancaman terhadap keamanan informasi muncul ketika data yang dikirimkan bersifat rahasia dan hanya diperuntukkan bagi pihak tertentu. Dalam kondisi seperti ini, jika tidak dilindungi dengan baik, informasi tersebut rentan disusupi oleh pihak yang tidak berwenang. Terlebih lagi, maraknya kejahatan siber saat ini memungkinkan peretas *(hacker)* untuk mencuri informasi sensitif tanpa terdeteksi [2].

Untuk melindungi data digital, berbagai pendekatan keamanan telah dikembangkan, seperti enkripsi dan teknik penyembunyian data [1]. Salah satu teknik penyembunyian data yang terus berkembang adalah steganografi, yaitu menyembunyikan pesan rahasia dalam medium komunikasi seperti gambar, teks, atau audio tanpa menarik perhatian pihak ketiga [3]. Dalam konteks digital, steganografi umumnya mencakup dua tahap utama, yaitu tahap penyisipan data (*embedding* atau *encoding*) dan tahap pengambilan kembali data tersembunyi (*extracting* atau *decoding*). Setelah tahap penyisipan selesai, media yang telah berisi pesan rahasia disebut sebagai *stego object*. Jika media yang digunakan berupa gambar, maka hasil akhirnya dikenal dengan istilah *stego image* [4].

Metode steganografi berbasis citra yang umum diterapkan adalah *Least Significant Bit* (LSB), yaitu metode konvensional yang menyisipkan pesan ke dalam bit paling tidak signifikan dari piksel gambar. Dalam pengambilan bit paling tidak signifikan, perubahan nilai-nilai tersebut biasanya sulit dikenali secara visual oleh manusia, menjadikannya cara yang populer untuk menyembunyikan informasi secara rahasia di dalam gambar tanpa mengganggu penampilan visualnya [3].

Namun, metode steganografi konvensional sering menghadapi kesulitan dalam menjaga keseimbangan antara *imperceptibility* (ketidaknampakan), *robustness* (ketahanan), dan *security* (keamanan). Teknik berbasis domain spasial, seperti *Least Significant Bit* (LSB), memiliki keunggulan dalam hal kesederhanaan dan efisiensi komputasi, namun mudah terdeteksi dan rentan terhadap perubahan akibat manipulasi citra [5]. Untuk mengatasi masalah ini, Salah satu pendekatan yang dikembangkan adalah metode *Adaptive* LSB, yang menyesuaikan lokasi dan jumlah bit yang disisipkan berdasarkan tekstur citra [6]. Salah satu pendekatan adaptif yang menjanjikan adalah dengan memanfaatkan deteksi tepi, karena area tepi pada citra memiliki toleransi yang lebih tinggi

terhadap perubahan nilai piksel dibandingkan dengan area non-tepi [7]. Dengan demikian, penyisipan pesan pada area tepi dapat meminimalkan penurunan kualitas imperseptibilitas citra stego [1]. Dalam penelitian ini, digunakan kombinasi algoritma deteksi tepi *Canny* dan *Kirsch*. Deteksi *Canny* unggul dalam memberikan ketajaman pada tepi, sementara *Kirsch* mampu memberikan ketebalan tepi dalam berbagai arah dengan ketahanan terhadap noise yang lebih baik. Dengan menggabungkan keduanya melalui operasi logika OR, dihasilkan peta tepi yang lebih menyeluruh, memungkinkan strategi penyisipan adaptif berdasarkan area *edge* dan *non-edge* [1].

Meskipun pendekatan adaptif LSB dapat meningkatkan kualitas *imperceptibility*. Namun, seiring dengan pesatnya perkembangan teknik *steganalysis* berbasis *deep learning*, diperlukan pengembangan metode steganografi yang lebih adaptif dan cerdas. Untuk itu, digunakan teknik *deep learning*, khususnya *Generative Adversarial Network (GAN)*, guna meningkatkan keamanan dan *imperceptibility*. GAN dilatih agar generator mampu menyempurnakan *stego image* menjadi lebih mirip *cover image*, sementara *discriminator* belajar membedakan keduanya, sehingga sistem menjadi lebih tahan terhadap deteksi visual maupun statistik [5].

Beberapa penelitian yang telah dilakukan terhadap steganografi citra dengan metode LSB diantaranya :

a. Penelitian yang dilakukan oleh Pooja Belagali dan Dr. V. R. Udupi dalam jurnal "*Robust Image Steganography Based on Hybrid Edge Detection*" mengusulkan metode steganografi berbasis *Least Significant Bit* (LSB) dengan pendekatan *Hybrid Edge Detection* menggunakan kombinasi *Canny* dan *Kirsch*. Hasil eksperimen menunjukkan bahwa kombinasi *Canny-Kirsch* memberikan performa lebih baik dibandingkan metode lain seperti *Canny-Sobel*, *Canny-Prewitt*, *Sobel-Kirsch*, dan *Kirsch-Prewitt*, dengan peningkatan nilai PSNR hingga 68.12 dan SSIM mendekati 1, yang menunjukkan kualitas visual yang sangat baik.
b. Penelitian yang dilakukan oleh Vida Yousefi Ramandi, Mansoor Fateh, dan Mohsen Rezvani dalam jurnal "*VidaGAN: Adaptive GAN for Image Steganography*" Metode ini menggunakan *encoder*, *decoder*, dan *critic* untuk meningkatkan kapasitas penyisipan dan transparansi gambar steganografi. Dengan pendekatan *CSPNet* yang dimodifikasi, VidaGAN mampu mencapai kapasitas penyisipan hingga 3.9 bit per piksel pada dataset DIV2K, serta menunjukkan AUC sebesar 0.6 dalam pengujian dengan alat steganalisis *StegExpose*, yang menandakan transparansi yang baik. Hasil eksperimen menunjukkan bahwa metode ini lebih unggul dibandingkan pendekatan sebelumnya dalam hal keseimbangan antara kapasitas penyisipan dan transparansi, serta memiliki ketahanan terhadap serangan JPEG *compression*, *noise*, dan *crop attacks*.

Berdasarkan hasil dari penelitian-penelitian sebelumnya, dapat disimpulkan bahwa penerapan metode steganografi berbasis *Hybrid Edge Detection* (*Canny* dan *Kirsch*) serta integrasi steganografi dengan *Generative Adversarial Network* (GAN) terbukti efektif dalam meningkatkan kualitas *imperceptibility*, kapasitas penyisipan, dan ketahanan terhadap deteksi atau serangan steganalysis. Melihat potensi tersebut, penulis tertarik untuk melakukan penelitian lebih lanjut dengan mengembangkan sistem steganografi citra digital yang menggabungkan metode adaptif LSB berbasis deteksi tepi *Canny–Kirsch* dan metode *deep learning* GAN.

Penelitian ini mengembangkan sistem steganografi citra digital dengan menggabungkan metode *Adaptive Least Significant Bit* (LSB) berbasis *Hybrid Edge Detection* (*Canny* dan *Kirsch*) serta *Generative Adversarial Network* (GAN). Metode *Adaptive* LSB digunakan untuk menentukan lokasi penyisipan bit secara adaptif berdasarkan tekstur dan tepi citra karena area tepi dapat mentolerir jumlah bit penyisipan lebih banyak dibandingkan dengan area halus menurut HVS [7], sedangkan GAN berperan menyempurnakan tampilan visual *stego image* agar tetap menyerupai *cover image* dan menjaga ketahanan citra *cover* terhadap steganalisis [8]. Dengan pendekatan ini, sistem diharapkan dapat meningkatkan kualitas *imperceptibility*, memperbesar kapasitas penyisipan data, serta meningkatkan ketahanan terhadap deteksi oleh teknik steganalisis modern.

Penelitian ini tidak hanya berfokus pada penyembunyian pesan yang tidak terdeteksi secara kasat mata, tetapi juga menargetkan peningkatan kualitas visual citra hasil (*stego image*) agar tetap alami serta akurasi ekstraksi pesan. Dengan memanfaatkan kombinasi keunggulan dari deteksi tepi adaptif dan pembelajaran adversarial dari GAN, diharapkan sistem ini dapat menyisipkan dan mengekstrak pesan rahasia secara akurat, tanpa menimbulkan perubahan visual signifikan pada citra dan tetap aman dari serangan steganalisis.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas maka perumusan masalah pada penelitian ini diantaranya:

1. Bagaimana cara mengimplementasikan metode *Adaptive Least Significant Bit* (LSB) berbasis *Hybrid Edge Detection* (Canny dan Kirsch) untuk meningkatkan kualitas penyisipan data dalam steganografi citra?
2. Bagaimana penerapan *Generative Adversarial Network* (GAN) dapat membantu menyempurnakan citra hasil (*stego image*) agar menyerupai citra asli (*cover image*) dan meningkatkan ketahanan terhadap deteksi steganalisis?
3. Bagaimana pengaruh kombinasi metode *Adaptive* LSB dan GAN terhadap *imperceptibility*, kapasitas penyisipan, dan ketahanan *stego image*?

1.3 Tujuan

1. Mengembangkan sistem steganografi pada citra digital dengan menggabungkan metode *Adaptive Least Significant Bit* (LSB) berbasis *Hybrid Edge Detection* (*Canny* dan *Kirsch*) dan *Generative Adversarial Network* (GAN) guna meningkatkan efektivitas dan keamanan penyembunyian data rahasia.
2. Menganalisis performa kombinasi metode *Adaptive* LSB dan GAN dalam hal kapasitas penyisipan, *imperceptibility* (kualitas visual), keamanan, dan ketahanan citra stego terhadap gangguan, dengan menggunakan metrik evaluasi.

1.4 Manfaat Penelitian

Manfaat penelitian ini dalam pengembangan teknologi steganografi citra meliputi:

1. Penelitian ini dapat berkontribusi pada pengembangan sistem steganografi yang lebih aman, di mana pesan tersembunyi menjadi lebih sulit dideteksi oleh algoritma steganalisis modern, terutama yang berbasis *deep learning*.
2. Penelitian ini dapat menjadi acuan atau dasar bagi pengembangan teknik steganografi generasi selanjutnya yang lebih adaptif dan cerdas melalui pemanfaatan teknologi pembelajaran mesin.
3. Hasil penelitian ini berpotensi diaplikasikan dalam sistem komunikasi rahasia, perlindungan hak cipta digital, dan keamanan siber, khususnya dalam skenario di mana penyembunyian data yang tak terdeteksi sangat penting.

1.5 Batasan Masalah

Dalam pembuatan tugas akhir, penulis mengambil beberapa batasan masalah di antaranya:

1. Citra yang digunakan sebagai *cover image* dan *stego-image* adalah citra digital statis berformat .png dengan ukuran tetap.
2. Metode deteksi tepi yang digunakan yaitu deteksi tepi *Canny* dan *Kirsch*.
3. GAN yang digunakan terbatas pada arsitektur standar terdiri dari *generator*, *discriminator*, dan *extractor*.
4. Data rahasia yang disisipkan berupa pesan teks.
5. Evaluasi kinerja sistem dilakukan berdasarkan nilai PSNR, SSIM, dan BER antara data asli dan data hasil ekstraksi.
6. Pengujian keamanan citra stego pada penelitian ini dilakukan dengan menggunakan metode steganalisis statistik, yaitu RS *Analysis*.

1.6 Sistematika Penulisan

Sistematika penulisan laporan penelitian disusun sebagai berikut:

BAB I PENDAHULUAN

Bab I berisi tentang uraian latar belakang penelitian, rumusan masalah, tujuan penelitian, Batasan masalah, dan Sistematika penulisan laporan.

BAB II TINJAUAN PUSTAKA

Bab II berisi teori yang mendukung pembuatan penelitian ini seperti teori mengenai konsep yang digunakan untuk menyelesaikan penelitian ini.

BAB III METODE PENELITIAN

Bab III berisi jenis dan metode penelitian yang digunakan dalam penelitian, perancangan sistem, variable penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab IV berisi pembahasan terkait implementasi sistem, hasil pengujian yang dilakukan, dan analisa dari hasil pengujian saat penelitian.

BAB V KESIMPULAN DAN SARAN

Bab V berisi tentang penarikan kesimpulan berdasarkan hasil yang sudah didapatkan dan saran yang disampaikan penulis untuk penelitian lanjutan.