

## **BAB I PENDAHULUAN**

### **1.1 Latar Belakang Masalah**

Perkembangan teknologi informasi global yang semakin pesat telah mengubah pandangan manusia dalam mereproduksi, mendistribusikan, dan mengonsumsi informasi. Data tidak lagi menjadi produk sampingan dari aktivitas digital, melainkan telah bertransformasi menjadi aset strategis yang bernilai tinggi dan harus dilindungi keberadaannya. Berdasarkan laporan terbaru Statista (2024), perkembangan dan pertumbuhan pengguna internet mencapai lebih dari 5,35 miliar orang pada tahun 2024 atau 66,2% populasi dunia. Peningkatan penetrasi internet ini berimplikasi langsung pada melonjaknya volume pertukaran data digital lintas platform dan lintas Negara. Seiring dengan meningkatnya intensitas aktivitas digital tersebut, risiko terhadap keamanan informasi juga mengalami eskalasi yang signifikan. Ancaman seperti kebocoran data, penyadapan, manipulasi informasi, serta tindakan peretasan yang bersifat merugikan menjadi fenomena yang semakin sulit dihindari. Cybersecurity Ventures (2023) melaporkan bahwa total kerugian akibat kejahatan siber diproyeksikan akan mencapai USD 10,5 triliun pada tahun 2025, kondisi ini menegaskan bahwa isu keamanan data bukan lagi sekedar persoalan teknis, melainkan telah menjadi tantangan strategis yang memerlukan pendekatan perlindungan informasi yang lebih canggih dan adaptif.

Dalam konteks pertukaran informasi digital, media sosial dan aplikasi pesan instan menempati posisi sentral sebagai sarana komunikasi utama masyarakat. Platform-platform tersebut tidak hanya memfasilitasi pertukaran teks, tetapi juga informasi visual dalam bentuk citra digital. Namun demikian, hampir seluruh platform komunikasi modern menerapkan mekanisme pemampatan otomatis yang bersifat lossy compression guna menghemat bandwidth dan mempercepat proses transmisi data. Proses pemampatan ini menyebabkan perubahan yang signifikan pada struktur data citra setelah dikirimkan, sehingga menimbulkan tantangan tersendiri bagi teknik perlindungan informasi berbasis citra.

Salah satu teknik yang banyak digunakan untuk menjaga kerahasiaan informasi visual ialah steganografi, yaitu metode penyembunyian pesan ke dalam media digital sehingga keberadaan pesan tersebut tidak disadari oleh pihak lain. Metode penyisipan pada domain ruang seperti Least Significant Bit (LSB), dikenal memiliki kapasitas penyisipan yang tinggi dan kompleksitas komputasi yang rendah. Namun, karakteristik LSB yang memodifikasi bit-bit paling rendah pada piksel menjadikannya sangat rentan terhadap pemampatan lossy dan manipulasi citra. Penelitian terkini oleh De La Cruz et al. (2024) menunjukkan bahwa metode LSB mudah mengalami degradasi data yang sangat signifikan setelah kompresi dan mudah terdeteksi oleh pendeteksi kecerdasan artifisial modern dengan tingkat akurasi lebih dari 94%.

Sebagai alternatif, metode penyisipan berbasis domain frekuensi, seperti Discrete Cosine Transform (DCT), menawarkan ketahanan yang lebih baik terhadap pemampatan karena memanfaatkan koefisien frekuensi citra. Akan tetapi, teknik DCT memiliki kelemahan berupa kapasitas penyisipan yang terbatas dan kebutuhan komputasi yang lebih tinggi (Chen & Wang, 2024). Dengan demikian, terdapat dilema antara ketahanan, kapasitas, dan kualitas visual yang belum dapat dipenuhi secara optimal oleh satu metode tunggal. Situasi ini menuntut perlunya pendekatan hibrida dan adaptif yang dapat menggabungkan keunggulan masing-masing teknik.

Selain tantangan pada proses penyisipan, aspek kerahasiaan pesan juga penting untuk dijaga. Kriptografi modern berbasis Elliptic Curve Cryptography (ECC) dikenal memiliki tingkat keamanan yang tinggi meskipun menggunakan struktur kunci yang lebih pendek. Standar NIST (2023) menegaskan bahwa ECC jauh lebih efisien dibandingkan algoritma klasik seperti RSA untuk tingkat keamanan yang setara. Oleh karena itu, penerapan ECC sebelum proses penyisipan ke dalam citra dapat memberikan lapisan pengamanan ganda, sehingga pesan tetap tidak dapat dibaca meskipun berhasil diekstraksi oleh pihak yang tidak berwenang.

Namun demikian, penelitian terdahulu menunjukkan bahwa kombinasi langsung antara ECC, LSB, maupun DCT masih menyisakan pola penyisipan

bersifat deterministik, sehingga berpotensi terdeteksi oleh analisis statistik dan kecerdasan artifisial. Pada titik ini, Genetic Algorithm (GA) menjadi pendekatan optimasi yang relevan untuk memilih lokasi penyisipan paling optimal secara adaptif melalui mekanisme seleksi, persilangan, dan mutasi. GA dapat menghasilkan pola penyisipan yang lebih acak dan sulit diprediksi, sekaligus memaksimalkan kualitas citra melalui fungsi kebugaran yang mempertimbangkan nilai Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Chi-Square, serta tingkat keberhasilan ekstraksi pesan.

Berdasarkan fenomena tersebut, penelitian ini memfokuskan diri pada pengembangan model steganografi citra digital yang mengintegrasikan ECC dengan dua metode penyisipan yang berbeda, yaitu ECC+GA+LSB dan ECC+GA+DCT. Penelitian ini bertujuan untuk menganalisis dan membandingkan kedua model terhadap pemampatan media sosial, distorsi citra, serta perubahan struktur piksel. Evaluasi kinerja dilakukan menggunakan parameter PSNR, MSE, Chi-Square, Bit Error Rate (BER), serta waktu komputasi. Indikator ini untuk mengukur kualitas visual, tingkat distorsi, ketahanan statistik, keberhasilan ekstraksi pesan, dan efisiensi sistem. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi nyata dalam mengembangkan model perlindungan informasi visual yang lebih aman, adaptif, dan sesuai kondisi komunikasi digital masa kini.

## 1.2 Rumusan Masalah dan Hipotesis (hipotesis opsional)

Berdasarkan latar belakang masalah di atas, maka rumusan masalah yang akan diselesaikan yaitu:

1. Bagaimana merancang, mengimplementasikan, dan mengintegrasikan metode steganografi citra digital berbasis Elliptic Curve Cryptography (ECC) yang dioptimasi menggunakan Algoritma Genetika (GA) pada dua teknik penyisipan berbeda, yaitu LSB dan DCT, sehingga mampu menghasilkan sistem yang adaptif, aman, serta memiliki kualitas citra yang baik?

2. Bagaimana perbandingan kinerja kedua metode tersebut dalam menghadapi kompresi dan distorsi media sosial, ditinjau melalui parameter kualitas citra (PSNR dan MSE), ketahanan terhadap kerusakan pesan (BER), keamanan statistik (Chi-Square), dan efisiensi komputasi (waktu proses), serta metode mana yang lebih unggul secara keseluruhan?

### 1.3 Batasan Masalah

Agar penelitian tetap terarah dan sesuai dengan ruang lingkup yang ditetapkan, batasan penelitian ini adalah sebagai berikut:

- a. Media yang digunakan terbatas pada citra digital grayscale berukuran 512 x 512 piksel, sesuai dengan dataset uji yang digunakan dalam implementasi penelitian ini.
- b. Pesan yang disisipkan berupa teks sederhana, tanpa mencakup penyisipan file biner atau media lain.
- c. Pesan yang disisipkan berupa teks biner hasil enkripsi ECC.
- d. Teknik steganografi yang dianalisis hanya dua jenis yaitu, ECC + GA + LSB (domain spasial) dan ECC + GA + DCT (domain frekuensi).
- e. Evaluasi robustness hanya difokuskan pada skenario kompresi dan distorsi yang umum terjadi pada platform media sosial, khususnya kompresi berbasis JPEG dan penurunan kualitas akibat unggahan atau unduhan.
- f. Penelitian tidak membahas secara mendalam bentuk serangan steganalisis lanjutan berbasis kecerdasan buatan, dan hanya mengevaluasi parameter statistik melalui nilai Chi-Square.
- g. Implementasi dilakukan menggunakan bahasa pemrograman Python, dengan pustaka standar untuk pemrosesan citra dan komputasi numerik.
- h. Evaluasi performa mencakup PSNR, MSE, Chi-Square, BER dan waktu komputasi.
- i. Steganalisis dilakukan menggunakan uji statistik sederhana.

### 1.4 Tujuan Penelitian

Tujuan yang ingin diraih dalam pembuatan laporan skripsi ini antara lain:

- Merancang dan mengimplementasikan sistem steganografi citra digital berbasis Elliptic Curve Cryptography (ECC) yang dioptimasi menggunakan Algoritma Genetika (GA) pada dua teknik penyisipan, yaitu LSB dan DCT, sehingga dapat menghasilkan proses penyisipan pesan yang adaptif, aman, dan tetap mempertahankan kualitas citra.
- Menganalisis dan membandingkan kinerja metode ECC + GA + LSB dan ECC + GA + DCT dalam menghadapi kompresi dan diartorsi media sosial berdasarkan parameter kualitas citra (PSNR dan MSE), ketahanan pesan (BER), keamanan statistik (Chi-Square), serta efisiensi komputasi, guna menentukan metode yang lebih unggul dan lebih tahan terhadap degradasi citra.

### 1.5 Sistematika Penulisan

Penelitian ini disusun dalam lima bab sebagai berikut:

**Bab I Pendahuluan**, berisi: pengantar yang menguraikan latar belakang penelitian sebagai dasar pemilihan topik steganografi citra digital berbasis ECC dengan optimasi Algoritma Genetika. Pada bab ini dijelaskan permasalahan yang melatarbelakangi penelitian, rumusan masalah dan hipotesis (jika digunakan), batasan masalah untuk memperjelas ruang lingkup penelitian, tujuan penelitian yang ingin dicapai, serta sistematika penulisan sebagai gambaran umum struktur skripsi secara keseluruhan.

**Bab II Landasan Teori**, berisi: landasan teori dan kajian ilmiah yang menjadi dasar konseptual penelitian. Pembahasan diawali dengan studi literatur terkait penelitian terdahulu, dilanjutkan dengan konsep dasar keamanan informasi berdasarkan CIA Triad. Bab ini juga menguraikan teori kriptografi, khususnya Elliptic Curve Cryptography (ECC), konsep dan teknik steganografi citra digital menggunakan metode DCT dan LSB, Algoritma Genetika sebagai metode optimasi, serta parameter pengukuran kualitas, keamanan, dan efisiensi sistem steganografi. Selain itu, dibahas pula pengaruh kompresi media sosial dan hubungan antar variabel penelitian sebagai dasar analisis pada bab selanjutnya.

**Bab III Metodologi Penelitian**, berisi: penjelasan metodologi penelitian yang digunakan untuk mencapai tujuan penelitian. Bab ini mencakup deskripsi objek

penelitian, analisis permasalahan, solusi yang diusulkan, serta alat dan bahan yang digunakan. Selanjutnya dijelaskan metode pengumpulan data, metode analisis yang meliputi analisis deskriptif, kuantitatif, komparatif, serta visual dan statistik, serta metode perancangan sistem steganografi yang diimplementasikan dalam penelitian.

**Bab IV Pembahasan**, berisi: hasil perancangan dan implementasi sistem steganografi yang telah dikembangkan. Pada bab ini dijelaskan arsitektur sistem, algoritma utama, serta implementasi source code. Selanjutnya dilakukan pembahasan mendalam terhadap hasil pengujian berdasarkan analisis deskriptif, kuantitatif, komparatif, serta analisis visual dan statistik. Pembahasan ini bertujuan untuk mengevaluasi kinerja metode LSB dan DCT berdasarkan parameter kualitas citra, keamanan, efisiensi waktu, serta perubahan ukuran file stego.

**Bab V Penutup**, berisi: kesimpulan dari seluruh hasil penelitian yang telah dilakukan serta menjawab rumusan masalah yang diajukan. Selain itu, bab ini juga memuat saran-saran yang ditujukan untuk pengembangan penelitian selanjutnya, baik dari sisi metode, sistem, maupun pengujian yang lebih luas.