BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam keamanan siber, terdapat dua pendekatan utama untuk melindungi informasi yaitu kriptografi yang fokus pada kerahasiaan isi pesan, dan steganografi yang fokus pada kerahasiaan keberadaan pesan itu sendiri (Mido dkk., 2022). Penelitian ini berfokus pada steganografi, sebuah metode untuk menyisipkan data rahasia ke dalam media digital seperti gambar tanpa mengubah tampilan visualnya (Yulion dkk., 2024), (Siaulhak dan Kasma, 2023), (AlEisa, 2022). Steganografi dipilih karena kemampuannya untuk melindungi informasi sensitif secara efektif, menjadikannya alat yang sangat berharga dalam berbagai aplikasi positif. Sebagai contoh, steganografi dapat digunakan untuk mengamankan komunikasi rahasia dalam bidang militer (Reksiyano dan Andarsyah, 2025), melindungi data medis pasien agar tetap rahasia selama transmisi (Yuadi, 2023) dan atau bahkan untuk menyematkan tanda air digital guna melindungi hak cipta karya digital. Dengan menyamarkan data tanpa meninggalkan jejak yang mencolok, steganografi memastikan bahwa informasi penting dapat dikirim dan disimpan dengan aman tanpa menarik perhatian pihak yang tidak berwenang, sehingga mendukung privasi dan keamanan data di era digital. Beberapa metode steganografi yang paling umum dipakai adalah *Least Significant Bit* (LSB) (Aksani dkk., 2025) dan *End of File* (EOF) (Yusron Rafi dan Rosyani, 2023). LSB yang bekerja dengan memodifikasi bit terakhir dari datapiksel gambar untuk menyisipkan pesan. Meskipun efektif, modifikasi pada level piksel ini secara inheren mengubah data statistik citra, yang

berpotensi menurunkan kualitas gambar dan membuatnya rentan terhadap deteksi oleh serangan steganalysis (Khozin dkk., 2025). Untuk mengatasi kelemahan tersebut, penelitian ini memilih metode *End of File* (EOF).

Metode EOF menyisipkan data rahasia setelah penanda akhir *file* tanpa mengubah konten visual media, seperti piksel pada gambar, sehingga kualitas visual tetap terjaga utuh (Aini, 2019), (Hutahaean dkk., 2025). Namun, salah satu tantangan besar metode ini adalah terjadinya peningkatan ukuran *file* secara signifikan setelah penyisipan data, yang dapat menimbulkan kecurigaan terhadap keberadaan data tersembunyi (Eka Putri dkk., 2020) (Pardede dkk., 2019).

Ukuran *file* yang besar memiliki kelemahan, yaitu kebutuhan penyimpanan yang lebih besar. Ukuran *file* setelah penyisipan data menggunakan steganografi berbasis EOF merupakan hasil penjumlahan antara ukuran *file* sebelum penyisipan dan ukuran data rahasia yang telah melalui proses *encoding* (Satria dan Antares, 2022). Kondisi ini menunjukkan bahwa tanpa upaya optimasi, penggunaan metode EOF justru dapat mengurangi efektivitas steganografi sebagai media penyembunyian data. Untuk mengatasi masalah tersebut, kompresi data menjadi salah satu solusi yang banyak dipertimbangkan. Kompresi data adalah proses mengurangi ukuran *file* dengan cara mengeliminasi redundansi atau mengoptimalkan pengkodean data yang bertujuan untuk menghemat ruang penyimpanan dan mempercepat proses pengiriman data (Chrismes Aruan dkk., 2023). Sebagai contoh, penelitian (Yiko Satriyawibawa dkk., 2024) telah menunjukkan efektivitas penggabungan kompresi dengan steganografi berhasil meningkatkan kapasitas penyisipan data pada metode LSB dengan

mengintegrasikan kompresi Brotli, yang mampu mereduksi ukuran data hingga 71%.

Terdapat banyak jenis algoritma kompresi termasuk *Zstandard* (Zstd) (Maulidina dkk., 2024), *Lempel-Ziv Markov chain Algorithm* (LZMA) (Ristovski dan Zdraveski, 2022), *Brotli* (Iqbal dkk., 2020), dan *Huffman Encoding* (Yonathan dkk., 2021). Pemilihan algoritma kompresi menjadi langkah penting karena setiap algoritma memiliki pendekatan teknis yang berbeda. *Huffman Encoding* dipilih sebagai representasi algoritma entropi yang menjadi dasar perbandingan (Wahab dkk., 2021). LZMA dipilih karena keunggulannya dalam mencapai rasio maksimal melalui penggunaan kamus dinamis yang sangat besar (hingga 4GB) dan penerapan *adaptive binary range coder* yang memberikan prediksi probabilitas bit lebih presisi (Sugirtham dkk., 2024). Sementara itu, *Brotli* dianalisis karena pendekatannya yang lebih kompleks dalam menggunakan kamus statis untuk meningkatkan efisiensi ukuran pada jenis data tertentu (Yiko Satriyawibawa dkk., 2024). Terakhir, *Zstandard* (Zstd) dipilih karena merepresentasikan algoritma seimbang yang menawarkan fleksibilitas luas antara kecepatan dan rasio kompresi, menjadikannya unggul dalam berbagai skenario (Ahlberg dan Bondesson, 2024). Teknik kompresi ini secara umum diketahui mampu mengecilkan ukuran data, namun langkah ini juga dapat menimbulkan dampak lain berupa meningkatnya konsumsi memori dan waktu pemrosesan (Sentosa dkk., 2017). Penelitian ini akan menganalisis keempat algoritma kompresi tersebut terhadap rasio kompresi, durasi pemrosesan, dan penggunaan memori.

Menindaklanjuti permasalahan dan solusi yang telah diuraikan, penelitian ini akan mengevaluasi kinerja algoritma kompresi melalui analisis mendalam terhadap rasio kompresi, durasi pemrosesan, dan penggunaan memori.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang yang telah dipaparkan, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana membandingkan kinerja algoritma kompresi *Zstandard*, LZMA, *Brotli*, dan *Huffman Encoding* berdasarkan rasio kompresi dalam konteks steganografi berbasis EOF?
2. Bagaimana membandingkan kinerja algoritma kompresi *Zstandard*, LZMA, *Brotli*, dan *Huffman Encoding* berdasarkan durasi pemrosesan dalam konteks steganografi berbasis EOF?
3. Bagaimana membandingkan kinerja algoritma kompresi *Zstandard*, LZMA, *Brotli*, dan *Huffman Encoding* berdasarkan penggunaan memori dalam konteks steganografi berbasis EOF?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini dirumuskan untuk mencapai beberapa hal yang berkaitan dengan penerapan teknik kompresi dalam konteks steganografi gambar. Secara lebih rinci, tujuan yang ingin dicapai melalui penelitian ini adalah sebagai berikutt:

1. Melakukan pengujian kinerja algoritma kompresi *Zstandard*, LZMA, *Brotli*, dan *Huffman Encoding* berdasarkan rasio kompresi dalam konteks steganografi berbasis EOF.

2. Melakukan pengujian kinerja algoritma kompresi *Zstandard*, LZMA, *Brotli*, dan *Huffman Encoding* berdasarkan durasi pemrosesan dalam konteks steganografi berbasis EOF.
3. Melakukan pengujian kinerja algoritma kompresi *Zstandard*, LZMA, *Brotli*, dan *Huffman Encoding* berdasarkan penggunaan memori dalam konteks steganografi berbasis EOF.

1.4 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat baik dari segi teoritis maupun praktis, terutama dalam bidang steganografi dan kompresi data. Adapun manfaat yang dapat diperoleh dari penelitian ini adalah sebagai berikut:

1. Meningkatkan keamanan data yang disisipkan melalui *encode* pada teknik kompresi data.
2. Memberikan kontribusi dalam bidang keamanan informasi digital.

1.5 Batasan Masalah

Supaya penelitian ini lebih terarah dan fokus dalam mencapai tujuan yang telah ditetapkan, beberapa batasan masalah yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Penelitian ini hanya berfokus pada steganografi berbasis EOF sebagai metode steganografi dalam penyisipan pesan pada gambar digital.
2. Penelitian ini hanya menguji dan menganalisis empat algoritma kompresi *lossless*, yaitu *Zstandard*, LZMA, *Brotli*, dan *Huffman Encoding*.
3. Parameter untuk perbandingan hanya meliputi rasio kompresi, durasi pemrosesan, penggunaan memori.

4. Penelitian ini tidak mencakup keamanan enkripsi data sebelum proses steganografi.
5. Penelitian ini hanya menggunakan satu buah *cover image* berformat PNG dengan ukuran 619 KB.