

BAB I PENDAHULUAN

1.1 Latar Belakang

Steganografi adalah salah satu teknik yang sering digunakan untuk menyembunyikan data dalam suatu media digital (Y. R. Nasution et al., 2020). Steganografi merupakan suatu metode yang efektif dalam menyembunyikan informasi rahasia karena hanya pengirim dan penerima yang mengetahui informasi rahasia tersebut (Aqilah Syaima' Fadel et al., 2024). Media yang sering digunakan dalam steganografi adalah file gambar dengan format JPEG, PNG, GIF, dan Bitmap (BMP)(Siaulhak & Safwan Kasma, 2023). BMP bersifat tidak terkompresi, sehingga setiap piksel dapat dimodifikasi secara langsung tanpa kehilangan data. Proses steganografi melibatkan dua file: gambar sampul (*cover image*) dan data rahasia (*payload*), yang setelah digabungkan membentuk *stego-image*, yakni gambar yang tampak normal tetapi mengandung informasi tersembunyi (Ehsan Ali et al., 2021).

Salah satu teknik steganografi yang digunakan adalah Least Significant Bit (LSB), yang menyisipkan data pada bit paling tidak signifikan dari piksel (Ali et al., 2024). Untuk meningkatkan keamanan steganografi, beberapa penelitian mengembangkan metode penyisipan acak menggunakan pembangkit bilangan acak semu seperti Pseudo-Random Number Generator (PRNG) (Ehsan Ali et al., 2021) dan Linear Congruential Generator (LCG) (Kurniasih et al., 2023). Pendekatan lain yaitu penggunaan struktur data seperti AVL Tree, yang mengatur lokasi penyisipan berdasarkan nilai piksel dari saluran warna hijau (G) dengan urutan traversal

menggunakan algoritma Breadth First Search (BFS). Untuk penyisipan bit-nya, metode *Pixel Indicator Technique* (PIT) digunakan, di mana saluran hijau menjadi saluran indikator lokasi penyisipan data pada saluran merah atau biru (Njoum et al., 2024).

Metode LSB mampu mempertahankan kualitas gambar yang baik, namun mudah dideteksi karena pola penyisipannya berurutan (Renaldy & Informatika, 2024)(Adela et al., 2024). Metode PRNG (Ehsan Ali et al., 2021) dan LCG (Kurniasih et al., 2023) lebih aman karena penyisipan dilakukan secara acak, sehingga sulit dideteksi oleh steganalisis (S. B. Nasution et al., 2017). Akan tetapi, metode acak tersebut memerlukan kunci pembangkit yang harus dikirimkan ke penerima agar data dapat diekstraksi, yang menjadi celah keamanan jika kunci jatuh ke pihak yang tidak berwenang. Penggunaan *AVL Tree* menjadi solusi alternatif karena tidak memerlukan kunci pembangkit, sehingga lebih aman (Njoum et al., 2024). Namun demikian, metode ini memiliki kelemahan pada aspek fidelity, yaitu kemampuan untuk mempertahankan kesetiaan visual antara stego-image dan cover image tanpa perbedaan yang terlihat secara signifikan.

Pada penelitian Njoum et al. (2024), teknik *Pixel Indicator Technique* (PIT) diterapkan pada gambar berwarna dengan model RGB (Red, Green, Blue), karena tiap piksel memiliki 3 saluran warna (R, G, B) yang masing-masing terdiri dari 8 bit. Saluran hijau (G) digunakan sebagai indikator, sedangkan saluran merah (R) atau biru (B) berfungsi sebagai media penyisipan data rahasia. Dalam proses penyisipannya, metode ini menyisipkan 2 bit sekaligus ke dalam salah satu saluran warna tersebut. Penyisipan ganda pada satu kanal menyebabkan perubahan nilai bit

piksel yang relatif besar, yaitu dalam rentang -3 hingga $+3$ bit. Perubahan ini menimbulkan distorsi visual pada stego-image dan berdampak pada penurunan nilai Peak Signal-to-Noise Ratio (PSNR) serta peningkatan Mean Square Error (MSE). Kedua parameter ini merupakan indikator utama dari aspek fidelity, yaitu kesetiaan visual antara *cover image* dan *stego-image*. Dengan kata lain, semakin tinggi nilai PSNR dan semakin rendah nilai MSE, maka semakin tinggi pula tingkat *fidelity* gambar hasil steganografi terhadap gambar aslinya.

Pada penelitian Njoun et al. (2024), teknik PIT yang digunakan untuk menyisipkan 2 bit sekaligus pada saluran merah atau biru menyebabkan perubahan nilai bit piksel yang relatif besar, yakni dalam rentang -3 hingga $+3$ bit. Hal ini meningkatkan distorsi visual dan menurunkan nilai Peak Signal-to-Noise Ratio (PSNR) serta meningkatkan Mean Square Error (MSE), yang keduanya merupakan indikator utama dari aspek fidelity. Dengan kata lain, semakin tinggi PSNR dan semakin rendah MSE, maka semakin tinggi pula tingkat fidelity antara cover image dan stego-image.

Untuk meningkatkan fidelity dari hasil steganografi, penelitian ini mengusulkan modifikasi metode PIT dengan strategi penyisipan yang lebih halus. Modifikasi dilakukan dengan menyebarkan penyisipan bit secara merata, yaitu dengan menyisipkan 1 bit pada saluran merah dan 1 bit pada saluran biru (penyisipan menyebar), serta tetap mempertahankan penyisipan 2 bit pada saluran biru di piksel tertentu (penyisipan tetap). Pemilihan saluran biru sebagai media penyisipan utama didasarkan pada karakteristik persepsi visual manusia, di mana mata manusia kurang sensitif terhadap perubahan warna biru dibandingkan warna

merah dan hijau (Almazaydeh, 2020). Dengan pendekatan ini, diharapkan perubahan nilai bit piksel dapat dibatasi dalam rentang -2 hingga +2 bit, sehingga distorsi visual berkurang dan fidelity gambar meningkat.

Tujuan dari penelitian ini adalah meningkatkan fidelity stego-image dari metode steganografi berbasis penyisipan acak tanpa kunci pembangkit, sebagaimana dilakukan dalam penelitian Njoum et al. (2024). Penelitian ini mengombinasikan struktur AVL Tree dan modifikasi Pixel Indicator Technique (PIT) untuk menghasilkan stego-image yang lebih alami dan memiliki kualitas visual yang lebih tinggi. Evaluasi dilakukan menggunakan parameter PSNR dan MSE untuk menilai tingkat fidelity, serta membandingkan hasilnya dengan metode sebelumnya guna mengetahui efektivitas metode yang diusulkan.

1.2 Rumusan Masalah

Dari uraian masalah yang sudah dirumuskan, didapat tujuan penelitian sebagai berikut:

1. Bagaimana mengimplementasikan steganografi menggunakan metode *AVL Tree* dengan traversal *Breadth First Search* (BFS) dan modifikasi *Pixel Indicator Technique* (PIT) untuk meningkatkan kualitas stego-image.
2. Bagaimana mengevaluasi performa steganografi menggunakan metode *AVL Tree* dengan traversal *Breadth First Search* (BFS) dan modifikasi *Pixel Indicator Technique* (PIT) dalam meningkatkan kualitas stego-image berdasarkan nilai PSNR dan MSE?

1.3 Tujuan Penelitian

Dari uraian masalah yang sudah dirumuskan, didapat tujuan penelitian, yaitu mengimplementasikan steganografi dengan metode *AVL Tree* dan modifikasi *Pixel Indicator Technique* (PIT) untuk meningkatkan kualitas stego-image.

1. Mengimplementasikan steganografi menggunakan metode *AVL Tree* dengan traversal *Breadth First Search* (BFS) dan modifikasi *Pixel Indicator Technique* (PIT) untuk meningkatkan kualitas stego-image.
2. Mengevaluasi performa steganografi menggunakan metode *AVL Tree* dengan traversal *Breadth First Search* (BFS) dan modifikasi *Pixel Indicator Technique* (PIT) dalam meningkatkan kualitas stego-image melalui analisis nilai PSNR dan MSE.

1.4 Manfaat Penelitian

Adapun beberapa manfaat yang didapatkan dari penelitian ini, sebagai berikut:

1. Meningkatkan kualitas *stego-image* melalui teknik penyisipan data.
2. Memberikan kontribusi dalam bidang keamanan informasi digital.

1.5 Batasan Masalah

Berikut merupakan batasan masalah yang terdapat pada penelitian ini:

1. Penelitian ini hanya berfokus pada steganografi gambar, khususnya pada metode penyisipan acak tanpa kunci pembangkit yang sebelumnya dikembangkan oleh Njoum et al. (2024) dan tidak mencakup steganografi dalam media lain seperti video atau audio.
2. Format citra yang digunakan dalam penelitian ini adalah BMP 24-bit RGB karena format ini tidak menggunakan kompresi, sehingga setiap bit piksel

dapat dimanipulasi secara langsung tanpa perubahan nilai. Model RGB karena tiap piksel memiliki 3 saluran warna (R, G, B) yang masing-masing terdiri dari 8 bit.

3. Penelitian ini tidak menggunakan format lain seperti JPEG atau PNG, maupun model warna seperti CMYK atau HSV, karena format dan model tersebut melibatkan proses kompresi atau transformasi warna yang dapat mengubah nilai bit piksel dan menurunkan akurasi penyisipan data.
4. Penelitian ini tidak menggunakan gambar sebagai pesan rahasia karena tujuan penelitian difokuskan pada penyisipan data sederhana agar proses pengujian lebih terarah dan hasilnya lebih konsisten. Oleh karena itu, pesan dibatasi hanya berupa teks..