

BAB I PENDAHULUAN

1.1 Latar Belakang

Adanya keinginan untuk saling bertukar informasi secara rahasia tanpa menimbulkan kecurigaan ataupun disadap menimbulkan semakin berkembangnya teknologi steganografi. Steganografi merupakan seni dan ilmu yang mempelajari cara menyembunyikan informasi digital dibalik informasi digital lain tanpa menunjukkan perubahan secara kasat mata dalam kualitas dan struktur dari file semula. Steganografi memungkinkan penyembunyian data pada berbagai jenis media digital seperti berkas citra, suara, video, dan teks.

Steganografi pada media citra merupakan jenis yang paling banyak digunakan. Metode penyembunyian data pada *Least Significant Bit* (LSB) berdasarkan *spatial domain* adalah salah satu dari algoritma sederhana tapi mempunyai *data rate* penambahan informasi yang tinggi. Namun metode LSB sebelumnya mempunyai kelemahan, yaitu tidak memperhatikan pemodelan psikoakustik untuk mengurangi *noise* yang diakibatkan penggantian bit-bit LSB serta kurang tahan terhadap penambahan *noise* dan pemrosesan sinyal, akibatnya citra mengalami penurunan kualitas.

Pada proses pertukaran informasi dengan jarak yang jauh biasanya rentan terhadap serangan. Serangan terhadap citra dibagi menjadi 2, yaitu *Standard Attack* dan *Malicious Attack*. *Standard Attack* merupakan serangan yang tidak sengaja berupa *noise*, interferensi, maupun redaman pada saluran transmisi. Biasanya serangan ini berhubungan dengan perubahan citra digital. Sedangkan *Malicious Attack* merupakan serangan yang disengaja yang dilakukan oleh pihak yang tidak bertanggung jawab yang bertujuan untuk menghilangkan citra steganografi. Hal ini menyebabkan data yang dikirim pengirim tidak sama dengan yang diterima oleh penerima atau bahkan mengalami kerusakan.

Turunnya kualitas citra menyebabkan informasi dari citra menjadi berkurang dan menimbulkan kecurigaan. Maka citra perlu dimanipulasi agar kualitas citra setelah disisipkan menyerupai citra aslinya.

Berdasarkan penelitian sebelumnya yang dijadikan sebagai pedoman dalam penulisan tugas akhir ini yang dikemukakan oleh Sur, Arijit., Ramanathan, Vignesh., Mukherjee, Jayanta (2011), *Pixel Rearrangement based Statistical Restoration Scheme Reducing Embedding Noise*. (PRSA) diuji untuk mengurangi noise akibat blind attack image restorasi dapat digunakan meningkatkan kualitas *image* steganografi tetapi mudah terdeteksi *Steganalysis*.

Dalam tugas akhir ini akan melakukan proses uji coba skema restoration dengan menggunakan metode *Histogram Adaptive Fuzzy* (HAF) pada penyisipan *Least Significant Bit* (LSB). Alasan digunakan LSB ini karena selain mudah juga karena sedikit kemungkinan akan terjadi degradasi pada original image dan kapasitas yang besar, Serta menggunakan metode HAF ini berdasarkan pada Khare, C., & Nagwanshi, K. K. (2012), *Image Restoration Technique with Non Linear Filter* dan Kaur, Jasmeen. (2013), *A Histogram based Algorithm for Denoising Images Corrupted with Impulse Noise*, yang membuktikan bahwa metode HAF memiliki performansi yang lebih baik dibandingkan metode lainnya.

Pada tugas akhir ini dirancang bagaimana cara agar steganografi setelah disisipkan informasi rahasia dapat tetap terjaga kerahasiaanya dan dari percobaan diperoleh citra hasil perbaikan steganografi memiliki tingkat performansi yang cukup baik untuk proses *degradasi* setelah disisipkan. Hal ini disimpulkan dari nilai MSE, CER, PSNR, ISNR dan MOS sistem.

1.2 Tujuan

Tujuan dari penelitian tugas akhir ini adalah:

- Mensimulasikan sistem steganografi dan *Histogram Adaptive Fuzzy* serta menggabungkan keduanya.
- Mengetahui pengaruh panjang karakter pada proses restorasi.
- Mengetahui dan menganalisis hasil dari simulasi sistem tersebut.
- Mengetahui nilai PSNR, ISNR dan CER dari hasil sistem.
- Mengetahui perbandingan steganografi sebelum dan setelah diberikan *Histogram Adaptive Fuzzy*.
- Menganalisis kualitas enkripsi dengan melihat pesan hasil ekstraksi.

1.3 Rumusan Masalah

Adapun rumusan masalah dalam tugas akhir ini adalah:

- Membandingkan kualitas steganografi dengan panjang karakter tertentu.
- Membandingkan tingkat perbaikan citra dengan level *noise* tertentu.
- Membandingkan citra awal dengan citra hasil perbaikan.
- Membandingkan metode restorasi *Histogram Adaptive Fuzzy* (HAF) dan metode filter lainnya.
- Mengetahui hasil steganografi apakah memiliki tingkat keamanan yang baik.

1.4 Batasan Masalah

- Sistem hanya berupa simulasi.
- Steganografi yang digunakan hanya dalam bentuk image (*.bmp) dan (*.jpg).
- Media penyisipan adalah image dalam bentuk grayscale dan pesan rahasia dalam bentuk (*.txt).
- Menggunakan software Matlab 2012.b.
- Metode steganografi yang digunakan pada domain spatial yaitu LSB.
- Metode restorasi yang digunakan adalah *Histogram Adaptive Fuzzy*.
- Jenis *noise* yang diterima citra yaitu *Gaussian noise*, *Salt and Pepper Noise*, *Uniform Noise*.
- Hanya menganalisis hasil data statistic yang didapat dari nilai PSNR (*Peak Sinyal to Noise Ratio*), ISNR (*Improvement Signal to Noise Ratio*) dan CER (Character Error Rate).
- Menggunakan *Mean Filter* sebagai metode pembanding.
- Pesan rahasia dalam bahasa Indonesia.

1.5 Metodologi Penelitian

Metode penelitian yang dilakukan untuk menyelesaikan Tugas Akhir ini adalah:

1. Studi Literatur dan pencarian bahan, dengan mempelajari literatur yang mendukung.
2. Mencari data-data yang berkaitan dengan Tugas Akhir ini.
3. Mengolah data-data yang didapat.

4. Tahap Perencanaan
5. Menagnalisis hasil
6. Diskusi dan penyusuna Tugas Akhir.

1.6 Sistematika Penulisan

Penulisan tugas akhir ini dibagi menjadi lima bab, yaitu sebagai berikut:

BAB I Pendahuluan

Pada bab ini dibahas latar belakang pemilihan judul, rumusan masalah, batasan masalah, tujuan penelitian, metode penelitian dan sistematika penulisan.

BAB II Landasan Teori

Berisi tentang dasar-dasar teori yang diperlukan serta literature-literatur yang mendukung dalam tugas akhir.

BAB III Perancangan Sistem

Berisi diagram alir dan perancangan tugas akhir.

BAB IV Pengujian dan Analisis Sistem

Bab ini berisi rancangan struktur program dan desain antarmuka, serta analisis sistem yang digunakan.

Bab V Kesimpulan dan Saran

Bab terakhir ini memuat kesimpulan dan saran untuk kesempurnaan pengembangan lebih lanjut.