

BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi dalam bidang informatika memberikan banyak manfaat pada kehidupan manusia. Dengan memanfaatkan teknologi informatika hari ini, dapat memudahkan manusia dalam penyalinan, penyebaran dan pengarsipan data multimedia. Perkembangan jaringan komunikasi digital, dapat memudahkan data-data digital diakses dan tersebar luas oleh khalayak melalui jaringan internet. Banyaknya pengguna internet yang melakukan pertukaran data dengan pengguna lainnya, dapat memungkinkan pertukaran data dilakukan secara ilegal. Sehingga memungkinkan data-data tersebut menjadi mudah diduplikasi dan dimanipulasi. Hal ini dapat memberikan ancaman pada pemilik data yang bersangkutan terhadap pelanggaran hak cipta atas hasil karya seni dan intelektual.

Untuk melindungi hak cipta dan keaslian data, dapat mengaplikasikan teknik *watermarking* pada sebuah data. *Watermarking* itu sendiri merupakan sebuah teknik yang dapat menyisipkan data informasi berupa teks pada data multimedia digital [5]. Teknik dan metode *watermarking* telah banyak diteliti dan dikembangkan agar dapat menjaga kualitas data yang sama dengan data sebelum informasi citra tersebut disisipkan (*embedding*). Domain spasial dan domain transformasi merupakan dua buah domain pada skema *watermaking*. Metode transformasi *cosine* merupakan salah satu metode yang terdapat dalam domain transformasi.

Dengan penambahan algoritma kriptografi tertentu dalam proses *watermarking*, akan menambahkan keamanan pada data informasi. Metode kriptografi tersebut digunakan untuk melindungi data informasi yang disisipkan atau dapat digunakan untuk melindungi data multimedia yang dikirimkan. Skema kriptografi sendiri dapat menyembunyikan data informasi yang dikirimkan untuk mendukung keamanan informasi, dengan berbasis pada algoritma pengkodean data informasi. DES (*Data Encryption Standar*) merupakan salah satu algoritma kriptografi yang populer dan dijadikan sebagai standar algoritma *enrcyption* yang memiliki jenis kunci simetri [9].

Pada penelitian [1], sistem menyisipkan pesan rahasia dalam *ASCII* pada citra dengan menggunakan metode *Discrete Cosine Transform* (DCT). Pada penelitian tersebut sistem

dianalisis dari pengaruh banyak karakter yang disisipkan, letak *embedding* karakter, ketahanan pesan terhadap kompresi gambar, dan ketahanan pesan terhadap perubahan brightness dan contrast. Dari penelitian tersebut didapat kesimpulan kualitas gambar *steganography* menggunakan metode DCT tergolong baik, dari hasil nilai *PSNR* yang lebih besar dari 30 dB. Maka dari penelitian tersebut penulis merancang sistem *watermarking* dengan tujuan menyisipkan pesan informasi berbentuk citra (*.jpeg*) pada *host image* (*.jpeg*). Dengan mengkombinasikan algoritma DCT dan *Data-Encryption Standar* (DES), dimana *plaintext* merupakan *secret image*. Pada proses sistem yang dirancang berjalan akan dicari nilai *PSNR* dan MSE pada saat *embedding* serta nilai BER pada saat *extraction* dan *decryption*. Dalam ranah frekuensi, menghasilkan *robustness* yang lebih tinggi dan *compatible* dengan standar kompresi citra JPEG dibandingkan dengan ranah spasial dalam menyisipkan dan mendeteksi *watermark* [7]. Sebelum *host image* disisipi *watermark*, *secret image* akan melalui proses *enrcyption* kriptografi dengan metode algoritma DES dengan ukuran *secret image* 32x32 dan 64x64 piksel. Proses tersebut bertujuan untuk melindungi *secret image* dari segala macam pelanggaran hak cipta atas karya seni dan intelektual.

Hasil penelitian tugas akhir ini adalah sebuah sistem yang dapat menyisipkan sebuah pesan informasi berbentuk citra yaitu *secret image* ke dalam sebuah gambar. Pada hasil uji *avalanche effect* DES, data nilai yang diperoleh membuktikan bahwa DES dapat mengubah isi pesan sebanyak 50% jika *key* masukan diubah 1-bit. Hasil *PSNR* yang didapat memiliki nilai $\gg 30\text{dB}$, membuat pesan yang disisipkan kasat mata terhadap penglihatan manusia. Uji coba terbaik dilakukan saat *secret image* berukuran 32x32 pixel, dimana nilai rata-rata BER $\ll 0.03$.

1.2 Tujuan Penelitian

Tujuan dari tugas akhir ini adalah sebagai berikut:

1. Mengimplementasikan algoritma kriptografi DES (*Data Encryption Standard*) dan algoritma *watermaking* DCT (*Discrete Cosine Transform*) sebagai sebuah sistem yang dapat mengamankan data informasi pada media citra digital.
2. Mampu mensimulasikan algoritma sistem menggunakan bahasa pemrograman.
3. Mengetahui performansi sistem berdasarkan kualitas hasil yang didapatkan dari konfigurasi terhadap algoritma DCT-DES.
4. Mencari nilai *avalanche effect* pada proses *enrcyption* DES.

5. Mencari nilai PSNR, MSE pada proses *embedding watermark*.
6. Mengetahui nilai BER yang didapat pada *decryption watermark*.

1.3 Rumusan Masalah

Pada penelitian tugas akhir ini, hal-hal yang dibahas dapat dirumuskan sebagai berikut:

1. Bagaimana merancang sistem yang dapat menyisipkan dan mengamankan data menggunakan algoritma DCT-DES?
2. Bagaimana performansi sistem dalam mengkombinasikan metode DCT dan DES pada saat *embedding watermark* berupa teks pada citra?
3. Bagaimana mengetahui kualitas performansi sistem kombinasi DCT-DES tersebut?

1.4 Batasan Masalah

Ruang lingkup tugas akhir ini adalah sebagai berikut:

1. Sistem dirancang dengan bahasa pemrograman.
2. Teknik *watermarking* yang digunakan merupakan kombinasi metode DCT-DES.
3. Citra yang digunakan berupa citra dengan format .jpeg.
4. Masukan sistem berupa *secret image (plaintext)* dengan ukuran citra 32x32 dan 64x64 pixel.
5. Paramater hasil yang diamati dan diteliti meliputi *PSNR (Peak Signal to Noise Ratio)*, *BER (Bit Error Rate)*, *MSE (Mean Square Error)*, *avalanche effect* serta waktu komputasi.

1.5 Metodologi Penelitian

Metodologi penyusunan Tugas Akhir ini adalah sebagai berikut:

1. Tahap Studi Literatur

Mengumpulkan, mempelajari, dan memahami materi yang dapat digunakan sebagai penunjang penelitian. Dapat berupa buku referensi, artikel, jurnal, video dan sumber lainnya yang berkaitan dengan perancangan sistem secara keseluruhan.

2. Tahap Perancangan Sistem

Memulai perancangan sistem *image watermarking* yang bertujuan mensimulasikan *embedding* dan *extraction* pesan rahasia dengan algoritma DCT-DES sebelum diimplementasikan pada tahap berikutnya.

3. Tahap Implementasi Sistem

Proses implementasi sistem diterapkan pada sebuah aplikasi sesuai dengan analisis dan desain yang menggunakan metode-metode yang telah ditentukan sebelumnya dalam bentuk bahasa pemrograman.

4. Tahap Pengujian dan Analisa Hasil

Melakukan pengujian terhadap sistem yang telah dirancang dan menganalisis performansi sistem dari hasil pengujian berupa PSNR, BER, MSE, *avalanche effect*, dan waktu komputasi.

5. Tahap Pengambilan Kesimpulan dan Penyusunan Laporan

Hasil dari melakukan semua tahap di atas, maka didapat sebuah kesimpulan yang nantinya akan disusun menjadi sebuah laporan dalam bentuk buku Tugas Akhir.

1.6 Sistematika Penulisan

Sistematika penulisan Tugas Akhir ini terdiri dari lima bab, yaitu:

1. Bab I Pendahuluan

Bab ini berisi uraian mengenai latar belakang permasalahan, tujuan penelitian, perumusan masalah, batasan masalah, metodologi penelitian, dan sistematika penulisan.

2. Bab II Dasar Teori

Bab ini berisi tentang teori-teori yang mendukung dan mendasari proses penelitian dan penulisan tugas akhir ini.

3. Bab III Perancangan Sistem

Bab ini akan menjelaskan mengenai tahap perancangan dan simulasi sistem steganografi dan kriptografi pada citra menggunakan metode DCT sebagai metode *embedding* dan metode DES sebagai metode *enrcyption* pesan.

4. Bab IV Analisis Hasil Simulasi

Bab ini menjelaskan mengenai hasil dari pengujian sistem dengan menganalisis hasil yang diperoleh melalui perhitungan MSE, *PSNR*, BER, *avalanche effect* dan waktu komputasi.

5. Bab V Kesimpulan dan Saran

Bab ini membahas tentang kesimpulan serta saran yang dapat diambil dari penelitian ini dan kemungkinan pengembangan dengan topik yang bersangkutan.