BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi komputer dan internet semakin memberikan kebebasan seseorang untuk mendapatkan informasi. Dengan akses yang hampir tidak terbatas pada media informasi menyebabkan data digital mudah untuk digandakan dan disebarluaskan. Sehingga, dalam beberapa kejadian sebuah data yang seharusnya milik pribadi atau bersifat rahasia menjadi tersebar dan disalahgunakan.

Terdapat beberapa cara untuk menghindari kejadian serupa terjadi. Misalnya dengan mengamankan data digital dengan teknik kriptografi dan steganografi sebelum mengirim atau menyimpan data ke internet. Steganografi merupakan teknik menyembunyikan pesan rahasia agar isinya tidak diketahui orang lain. Steganografi memerlukan dua properti atau bagian utama yaitu penampung dan isi pesan rahasia yang dapat berupa *file* gambar, teks,suara, maupun video. [1]

Salah satu metode yang biasa digunakan dalam teknik steganografi yaitu metode *Discrete Cosine Transformation* (DCT). Metode DCT merupakan sebuah metode yang melakukan proses penyisipan pesan rahasia di dalam domain frekuensi. Metode DCT merupakan salah satu metode yang mudah diimplementasikan pada data digital. Selain itu, metode DCT juga memiliki kemampuan untuk menjaga keutuhan media penampung, sehingga *file* tidak akan rusak meskipun sudah disisipi pesan rahasia. Ardiansyah (2017) dalam penelitiannya berhasil mengembangkan sebuah aplikasi steganografi dengan metode DCT untuk melakukan penyisipan pesan teks berupa huruf, angka, dan simbol ke dalam sebuah gambar. Pengujian aplikasi menunjukkan bahwa sistem bekerja dengan baik dengan nilai rata-rata 3.89atau berkategori baik dari 50 orang responden [1]. Herlinawati (2016) dalam penelitiannya berhasil melakukan penyisipan pesan rahasia ke dalam video H263 dengan metode DCT. Hasil penelitiannya menunjukkan bahwa kualitas video yang dihasilkan bergantung

pada ukuran pesan yang disisipkan. Semakin besar ukuran pesan semakin buruk kualitas video yang dihasilkan [2].

Oleh karena itu, pada penelitian ini penulis menggunakan metode DCT untuk diimplementasikan pada steganografi dengan *file* audio sebagai *cover object* atau media yang akan disisipi pesan. *File* audio digunakan sebagai objek penelitian karena steganografi pada *file* audio dinilai cocok untuk menyembunyikan pesan rahasia dengan memanfaatkan kelemahan pada sistem pendengaran manusia. Untuk mendapatkan hasil yang diharapkan, dilakukan 2 jenis pengujian yaitu dengan metode *black box* untuk menguji fungsionalitas dari aplikasi yang digunakan untuk mengimplementasikan steganografi dan analisa perhitungan nilai *Peak Signal to Noise Ratio* (PSNR) untuk menguji kelayakan *file* audio setelah proses penyisipan pesan.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas dirumuskan masalah dalam penelitian adalah:

1. Bagaimana cara melakukan penyisipan pesan teks ke dalam *file* audio dengan metode *Discrete Cosine Transform* (DCT)?
2. Bagaimana kelayakan aplikasi yang dirancang untuk penerapan metode steganografi?
3. Bagaimana kualitas audio stego yang dihasilkan setelah proses penyisipan pesan?

1.3 Tujuan Penelitian

Tujuan penelitian dari penelitian ini adalah:

1. Mengetahui cara dan tahapan proses penyisipan pesan teks ke dalam *file* audio dengan metode *Discrete Cosine Transform* (DCT).
2. Mengetahui kelayakan aplikasi yang digunakan untuk implementasi steganografi dari segi fungsionalitas setiap fitur yang terpasang.
3. Mengetahui kualitas audio stego yang dihasilkan setelah proses penyisipan pesan.

1.4 Batasan Masalah

Batasan untuk penelitian ini yaitu:

1. Pesan atau data yang akan disisipkan berupa teks yang dapat diinputkan langsung pada kolom aplikasi atau *file* berformat txt.
2. Format file audio yang digunakan dan hasil setelah proses steganografi adalah format wav.
3. Program implementasi steganografi dibuat dengan MATLAB.
4. Metode pengujian hasil implementasi yang digunakan adalah metode *black box* dan menghitung nilai *Peak Signal to Noise Ratio* (PSNR).

1.5 Manfaat Penelitian

Manfaat penelitian implementasi steganografi antara lain dapat mengamankan pesan atau data rahasia agar tidak diketahui orang yang tidak berkepentingan. Sebagai salah satu alternatif untuk mengamankan informasi dalam bentuk teks pada sebuah *file* audio sebelum nantinya dikirim atau disimpan. Selain itu, penelitian ini dapat digunakan sebagai referensi untuk penelitian lain yang berkaitan.