

# **BAB I**

## **PENDAHULUAN**

### **1.1 Latar Belakang**

Pada zaman sekarang audio tidak hanya dimanfaatkan sebagai alat berkomunikasi dan mendengar musik saja. Sudah lama sekali audio digunakan sebagai alat penyisipan pesan rahasia pada zaman perang dunia. Pada saat perang, prajurit mengirimkan sebuah pesan audio yang kemudian pesan tersebut akan di deskripsi oleh penerima, lalu kemudian akan di dapat pesan yang tersisipkan di pesan audio tersebut. Metode ini di sebut dengan Steganografi.

Steganografi adalah metode untuk mengamankan sebuah data atau informasi penting. Steganografi adalah ilmu menyisipkan pesan atau informasi tersembunyi ke dalam suatu media, seperti audio, gambar, dan video [1]. Steganografi membutuhkan dua *property* untuk menjalankannya yaitu, media penampung dan pesan rahasia. Media penampung digunakan sebagai wadah untuk membawa pesan yang ingin disisipkan seperti, teks, gambar, suara, dan video. Pesan rahasia adalah pesan yang akan disisipkan melalui media penampung seperti sebuah artikel, gambar, kode rahasia dan pesan lain [2]. Semakin berkembangannya penggunaan teknologi informasi memicu perkembangan Steganografi itu sendiri. Steganografi sudah banyak dipecahkan oleh para *attacker*. Oleh sebab itu di perlukan metode baru dalam perancangan Steganografi.

Perancangan steganografi dapat dilakukan menggunakan berbagai metode. Dalam beberapa penelitian terkait sebelumnya, seperti pada hasil penelitian [3] dengan metode *Spread Spectrum* memiliki ketahanan yang kuat terhadap serangan umum pemrosesan sinyal dan memiliki kualitas persepsi yang tinggi. Namun dari beberapa serangan yang diujikan, terdapat hasil paling rendah pada tipe serangan *MPEG compression*[4].

Pada penelitian [5], *Lifting Wavelet Transform* (LWT) salah satu metode transformasi *wavelet* yang dirancang untuk mengurangi kebutuhan memori. Adapun metode *Singular Value Decomposition* (SVD) yang merupakan teknik dekomposisi matriks berukuran apa saja untuk mempermudah pengolahan data. Pada penelitian [6] , menjelaskan bahwa *Lifting Wavelet Transform* (LWT) digunakan untuk menguraikan *audio host* menjadi beberapa *subband*, dan kemudian transformasi *Fast Fourier Transform* (FFT) memilih beberapa *subband* dengan energi terendah. Hasil dari penelitian [6] ini memiliki ketahanan yang baik terhadap sebagian besar serangan, *imperceptibility* dengan *Signal to Noise Ratio* (SNR) lebih dari 30 dB dan muatan 172,66 bps.

Pada penelitian [7] menjelaskan *watermarking audio* menggunakan metode *Lifting Wavelet Transform* (LWT) dan QR dekomposisi untuk perlindungan hak cipta audio. Hasil penelitian menunjukkan bahwa metode yang digunakan sangat kuat terhadap serangan yang berbeda. *Payload* memiliki *imperceptibility* yang baik.

Pada penelitian [8], membahas sistem *audio watermarking* menggunakan metode *Quantization Index Modulation* (QIM) dan *Spread Spectrum* (SS) berbasiskan *Discrete Wavelet Transform* (DWT), *Discrete Cosine Transform* (DCT), *Singular Value Decomposition* (SVD), dan *Cartesian-Polar Transform* (CPT). *Discrete Wavelet Transform* (DWT) mempunyai beberapa keunggulan jika dibanding dengan transformasi *fourier*, yaitu dapat menentukan *amplitude* saat frekuensi *sampling* yang di dapat tidak tepat. DWT juga lebih *sensitive* dalam menunjukkan perubahan bentuk sinyal pada frekuensi tertentu. Hasil dari penelitian [8] adalah ODG bernilai -1,96, SNR bernilai 28.2512 dB, BER bernilai 0,07, C bernilai 10,6697 dan nilai rata-rata MOS berada dalam rentang 3 sampai 4.

Menurut penelitian[9], Steganografi audio dengan metode teks *embedding* adalah aplikasi bentuk *windows* yang memungkinkan pengguna untuk menyembunyikan pesan mereka dalam audio \*.wav, yang dapat memberikan kerahasiaan pesan pengguna. Namun, satu batasan untuk aplikasi

ini adalah aplikasi ini hanya mendukung *file* audio yaitu audio \*.wav. Oleh karena itu, lebih banyak variasi dukungan *format file* audio seperti \*.mp3 dan \*.wma dapat ditambahkan ke aplikasi sebagai media persembunyian. Mekanisme ini dapat ditambahkan melalui pemahaman dan analisis *format file*.

Pada penelitian [10], menjelaskan metode steganografi audio dengan *Spread Spectrum*. Hasil yang didapatkan pada penelitian tersebut yaitu, kualitas audio dipengaruhi oleh panjang teks, faktor skala yang digunakan. Dan transformasi DT-CWT lebih baik dibandingkan dengan DWT karena nilai SNR yang didapatkan. Namun dari hasil pengujian terhadap proses pengolahan sinyal didapatkan hasil bahwa audio hasil steganografi tidak tahan terhadap serangan seperti *resampling*, kompresi dan *filtering*. Tetapi untuk *noising* cukup tahan karena nilai BER yang didapat cukup baik.

Pada penelitian [11], menjelaskan steganografi audio dengan metode *Lifting Wavelet Transform* (LWT) untuk membagi sinyal audio menjadi beberapa *subband* dan proses *Discrete Sine Transform* (DST) untuk mengubah domain waktu menjadi domain frekuensi. Dalam domain frekuensi dilakukan proses penyisipan teks ke dalam audio tersebut. Di sisi lain *Compressive Sampling* digunakan dalam pesan rahasia sebelum disisipkan. Hasil yang diperoleh pada penelitian [11] yaitu, BER bernilai 0, ODG bernilai -3.912, SNR bernilai 33.54 dan C bernilai 6.1523.

Tugas Akhir ini, merancang Steganografi Audio menggunakan teknik *Multi Bit Spread Spectrum* (SS) pada audio stasioner berbasis *Compressive Sampling* (CS). *Multi Bit Spread Spectrum* berfungsi untuk mengkodekan satu bit menjadi beberapa bit data. Metode ekstraksi yang digunakan pada *Multi Bit SS* adalah dengan cara *blind*. Kemudian *Multi Bit Spread Spectrum* akan menyisipkan *bit watermark* di beberapa *bit host* hasil pengkodean yang sudah dilakukan. *Stationary Wavelet Transform* (SWT) adalah algoritma transformasi *wavelet* yang di gunakan untuk mengatasi kurangnya terjemahan *Discrete Wavelet Transform* (DWT). SWT tidak melakukan *downsampling* di setiap dekomposisinya. *Compressive Sampling* (CS) adalah metode *sampling* yang sinyal akuisisi dan kompresi dalam prosesnya diambil *sample* dengan jumlah sedikit dan acak berdasarkan pada transformasi proyeksi yang digunakan.

## 1.2 Rumusan Masalah

Adapun rumusan masalah yang dilakukan untuk menyelesaikan Tugas Akhir ini, yaitu:

1. Bagaimana merancang sebuah sistem steganografi dengan metode *Multibit SS* pada audio stasioner berbasis *Compressive Sampling* (CS)?
2. Bagaimana mengetahui dan menganalisis parameter-parameter terbaik dari metode yang digunakan yang memberikan hasil performansi sistem terbaik berupa nilai BER, SNR, MOS, ODG dan *payload*.
3. Bagaimana cara menganalisis rasio kompresi audio yang dicuplik dengan akuisisi CS ?

## 1.3 Tujuan dan Manfaat

Adapun tujuan dari Tugas Akhir ini, yaitu :

1. Merancang sebuah sistem steganografi dengan metode *Multibit SS* pada audio stasioner berbasiskan *Compressive Sampling* (CS).
2. Mengetahui dan menganalisis parameter-parameter terbaik dari metode yang digunakan yang memberikan hasil performansi sistem terbaik berupa nilai BER, SNR, ODG, MOS dan *payload*.
3. Menganalisis rasio kompresi audio yang dicuplik dengan akuisisi CS.

## 1.4 Batasan Masalah

Adapun batasan masalah dibuatnya Tugas Akhir ini, yaitu :

1. Perancangan sistem dilakukan dengan menggunakan aplikasi Matlab versi 2014b.
2. Penyisipan *file* citra ke dalam *audio host* menggunakan metode *Multibit Spread Spectrum* .
3. Jumlah *file* audio yang akan digunakan dalam penelitian ini hanya 5 *file* audio format \*.wav, yaitu:
  - 1) *Voice.wav*
  - 2) *Africa-toto.wav*

- 3) *Beautiful\_life-ace\_of\_base.wav*
- 4) *I\_ran\_so\_far\_away-flock\_of\_seagulls.wav*
- 5) *Temple\_of\_love-sisters\_of\_mercy.wav*

Dengan frekuensi *sampling* 44100 Hz dan merupakan *file* \*.wav asli bukan hasil konversi dari *file* yang telah dikompresi.

4. Durasi setiap *file* audio maksimal 2 menit dengan proses penyisipan bervariasi mulai dari 1 detik sampai 50 detik.
5. Metode yang digunakan untuk mengubah domain waktu ke domain frekuensi yaitu dengan teknik transformasi *Stationary Wavelet Transform* (SWT).
6. Parameter yang akan dianalisis adalah parameter *robustness* atau ketahanan data yang dipresentasikan dengan *Bit Error Rate* (BER), parameter kualitas audio secara *objective* yang dipresentasikan dengan parameter *Objective Difference Grade* (ODG) dan *Signal to Noise Ratio* (SNR), parameter kualitas audio secara *subjective* yang direpresentasikan dengan *Mean Opinion Score* (MOS), dan parameter kapasitas audio *watermarking* yang direpresentasikan dengan *Capacity* (C) yang menunjukkan jumlah bit *watermark* yang disisipkan dalam 1 detik.
7. Serangan yang akan dilakukan dalam pengujian, yaitu *filtering* berupa LPF dan BPF, *noise additive*, *resampling*, TSM, *Linear Speed Change*, *Pitch Shifting*, *Equalizer*, *Echo*, dan Kompresi.

## 1.5 Metode Penelitian

Adapun metode penelitian yang dilakukan untuk penyelesaian Tugas Akhir ini, yaitu :

1. Studi Literatur  
Pada tahap ini melakukan pengkajian mengenai pokok permasalahan penelitian.
2. Pengumpulan Data  
Setelah dilakukan studi literatur, dilakukan pengumpulan data berupa data *host* dan citra *watermark*. *Host* yang digunakan adalah sinyal suara dalam *format* \*.wav. pemilihan 5 *file host* berdasarkan

pada nilai ODG tertinggi yang dihasilkan oleh *file* hasil rekaman tadi. Sedangkan untuk data citra *watermark* merupakan citra biner yang dibuat menggunakan tabel-tabel pada *microsoft excel*.

### 3. Perancangan Sistem

Setelah mengumpulkan data yang ada, dilakukan perancangan sistem menggunakan data yang sudah dikumpulkan untuk mendukung operasi sistem. Perancangan sistem yang dilakukan diantaranya adalah proses penyisipan, penambahan serangan dan proses ekstraksi.

### 4. Implementasi

Setelah perancangan sistem, maka dilakukan proses implementasi dengan menggunakan simulasi perangkat lunak Matlab.

### 5. Pengujian

Setelah dilakukan implementasi dengan simulasi Matlab, maka dilanjutkan dengan pengujian simulasi dengan cara menguji parameter yang ada, berupa BER, SNR, MOS, ODG dan *payload*. Untuk dinyatakan berhasil BER maksimal bernilai 0,1, MOS bernilai minimal 4, dan  $SNR \geq 20$  dB.

### 6. Analisis Hasil

Setelah selesai pengujian, maka dilakukan penyimpulan analisis dari data-data yang sudah dianalisis.

## 1.6 Sistematika Penulisan

Penulisan penelitian Tugas Akhir ini dibagi dalam beberapa topik bahasan yang disusun secara sistematis sebagai berikut:

### **BAB 1 PENDAHULUAN**

Menjelaskan latar belakang, tujuan, rumusan masalah, batasan masalah, metode penelitian, sistematika penulisan terkait

## **BAB II DASAR TEORI**

Menjelaskan teori dasar mengenai steganografi audio, metode-metode yang digunakan pada sistem, dan serangan yang dilakukan pada sistem.

## **BAB III PERANCANGAN DAN SIMULASI SISTEM**

Menjelaskan mengenai tahap perancangan sistem yang akan diimplementasikan dalam simulasi perangkat lunak untuk steganografi audio.

## **BAB IV PENGUJIAN DAN ANALISIS SISTEM**

Menjelaskan analisa sistem pada hasil yang diperoleh dari tahap perancangan, pengujian dan simulasi sistem.

## **BAB V KESIMPULAN DAN SARAN**

Penarikan kesimpulan dan saran dari seluruh kegiatan Tugas Akhir yang dapat digunakan sebagai masukan untuk pengembangan penelitian ini lebih lanjut.