

BAB I

PENDAHULUAN

1.1 Latar Belakang

Era komputer digital dan teknologi informasi telah menjadi bagian dari ekosistem masyarakat modern saat ini. Berbagai macam jenis informasi digital dapat diakses dan dibagikan dengan mudah melalui berbagai macam jenis media penyedia layanan informasi digital yang ada di internet. Kemudahan dalam bertukar informasi digital ini dimanfaatkan oleh segelintir orang untuk melakukan intersepsi, interupsi, dan modifikasi pada digital yang terdapat di dalamnya. Berdasarkan masalah tersebut, maka diperlukan suatu teknik yang menjamin sekaligus mengamankan keamanan dan kerahasiaan data digital tersebut, yakni dengan steganografi.

Steganografi merupakan seni untuk menyembunyikan pesan di dalam media sehingga orang lain tidak dapat menyadari ada suatu pesan di dalam media tersebut. Pada steganografi digital, pesan rahasia tersebut memerlukan media digital sebagai wadah penampung, misalnya citra, audio, teks dan video [1]. Ketahanan, keamanan dan kapasitas penyisipan adalah tiga kriteria utama yang menjadi acuan dalam penilaian kinerja steganografi [2]. Steganografi yang efektif harus mempunyai karakteristik seperti transparansi perseptual (yakni *cover-media* dan *stego-media* harus tidak terlihat), kapasitas yang besar, ketahanan terhadap berbagai macam serangan dan kecepatan dan kecepatan data transfer yang tinggi dalam penyisipan data rahasia [3].

Steganografi audio mengambil keuntungan dari kelemahan *human auditory system* (HAS) untuk menyisipkan data rahasia di bagian sinyal audio sehingga distorsi yang dihasilkan oleh data rahasia yang disisipkan tidak terdengar [4]. Pada steganografi audio terdapat tiga domain penyisipan terkemuka yang digunakan yakni, *temporal domain*, *wavelet domain* dan *coded domain* yang masing-masing mempunyai kelebihan dan kekurangan [2].

Discrete wavelete transform (DWT) berbasis pada gelombang kecil yang disebut *wavelet*. DWT menyediakan informasi tentang frekuensi maupun waktu (lokasi) dari sinyal sehingga memberikan kemudahan dalam kompresi, transmisi dan analisis data [1]. Penelitian [4, 5] menyebutkan bahwa metode DWT memiliki kualitas *imperceptibility* dan *robustness* yang bagus dan efektif dalam mengatasi jenis serangan yang paling umum didesain untuk menghancurkan pesan rahasia yang di-

sisipkan dalam wadah audio seperti *low-pass filter* (LPF). Hal ini berdasarkan nilai *bit error rate* (BER) yang diperoleh adalah nol.

Compressive sampling (CS) adalah protokol akuisisi sinyal yang sangat sederhana dan efisien sehingga memungkinkan rekonstruksi sinyal dari satu set kecil sampel yang diambil secara acak [6]. CS dapat digunakan untuk berbagai jenis data seperti video, gambar, sinyal audio, sinyal yang digunakan dalam aplikasi medis (MRI, ECG), dsb [7]. Berdasarkan penelitian [8, 9], peran CS telah menghasilkan peningkatan kapasitas pesan yang disisipkan. Selain itu, pada penelitian [8] menyebutkan bahwa hasil kualitas audio yang melalui proses CS masih dapat terdengar jelas, sedangkan pada penelitian [9] menyebutkan bahwa hasil citra yang melalui proses CS dapat direkonstruksi kembali seperti semula setelah melewati proses ekstraksi dan proses dekripsi algoritme *Rivest-Shamir-Adleman* (RSA).

Di dalam bidang keamanan komputer, steganografi dapat dilakukan bersamaan dengan enkripsi [1]. Enkripsi RSA diusulkan oleh tiga orang yakni, Ronald Rivest, Adi Shamir dan Leonard Adleman. Metode ini melibatkan dua kunci dalam proses enkripsi dan dekripsinya. Setiap pengguna harus (secara pribadi) menentukan angka untuk kunci publik (*public key*) dan kunci pribadi (*private key*) [10]. Pada penelitian [9, 11, 12] dikemukakan bahwa implementasi enkripsi RSA meningkatkan keamanan pada sistem steganografi berbasis *wavelet domain* dalam proses transmisi data saat proses pertukaran pesan rahasia berlangsung.

Statistical mean manipulation (SMM) adalah metode penyisipan statistik yang melakukan implementasi pengulangan kode untuk membantu meningkatkan akurasi deteksi secara keseluruhan pada *wavelet domain*. Dimana, perkiraan rata-rata koefisien dimodifikasi pada lapisan akhir untuk proses penyisipan data [13]. Berdasarkan penelitian [14] yang melakukan implementasi SMM mengatakan bahwa metode ini dapat dengan mudah memulihkan data yang disisipkan setelah diserang dengan sedikit penurunan kualitas pada wadah audionya.

1.2 Rumusan Masalah

Melalui tugas akhir ini dilakukan implementasi enkripsi RSA dan CS pada pesan informasi yang akan disisipkan sehingga dapat meningkatkan keamanan saat proses transmisi serta menghasilkan sedikit distorsi pada audio tersisipnya. Langkah selanjutnya adalah penyisipan pesan informasi dengan metode DWT-SMM ke dalam wadah audio digital sehingga diharapkan memperoleh sistem steganografi dengan performa bagus berdasarkan *imperceptibility*, kualitas audio dan kapasitas penyisipan pesan menggunakan parameter *robustness*.

Berdasarkan latar belakang tersebut, maka rumusan masalah dari tugas akhir ini adalah sebagai berikut:

1. Bagaimana merancang sistem steganografi audio berbasis DWT-SMM dengan enkripsi RSA dan CS?
2. Bagaimana kualitas wadah audio, kualitas ekstraksi dari citra yang disisipkan, ketahanan, dan kapasitas steganografi pada metode yang diajukan berdasarkan beberapa parameter seperti BER, kapasitas (C), *mean opinion score* (MOS), *objective difference grade* (ODG) dan *signal to noise ratio* (SNR)?
3. Bagaimana penerapan CS pada citra yang akan disisipkan?
4. Bagaimana penerapan metode enkripsi dan dekripsi RSA pada citra yang akan disisipkan?

1.3 Tujuan Penelitian

Tujuan dari dilakukannya penelitian ini adalah sebagai berikut :

1. Merancang sistem berbasis DWT-SMM pada steganografi audio sehingga didapatkan sistem steganografi dengan performa bagus berdasarkan parameter *robustness*.
2. Menambahkan enkripsi RSA untuk menjamin keamanan dan kerahasiaan pesan citra biner yang disisipkan.
3. Menganalisis performa steganografi berdasarkan *imperceptibility* dan kapasitas penyisipan pesan menggunakan parameter *robustness*.
4. Menganalisis ketahanan sistem yang dirancang terhadap serangan tertentu berdasarkan nilai BER.

1.4 Batasan Masalah

Pada perumusan masalah diberikan batasan masalah sebagai berikut :

1. Perancangan sistem akan diimplementasikan menggunakan perangkat lunak komputasi numerik.
2. Wadah pesan yang digunakan dalam steganografi adalah audio dengan format *.wav dan *sampling rate* 44100 Hz.

3. Informasi pesan rahasia yang akan disisipkan adalah citra digital jenis biner dengan format **.bmp* berukuran 64×64 piksel dengan tiga variasi isi pesan yang berbeda.
4. Metode penyisipan yang digunakan adalah SMM.
5. Membagikan sepasang kunci dengan bilangan prima dari rentang 0 sampai 50 untuk proses enkripsi dan dekripsi menggunakan algoritme RSA.
6. Parameter *robustness* yang dianalisis dan diteliti meliputi BER, C, MOS, ODG dan SNR.
7. Analisis kualitas steganografi audio dilakukan berdasarkan pengujian terhadap lima arsip audio dengan jenis berbeda.
8. Pengujian dilakukan serangan LPF, *band-pass filter* (BPF), *time scale modification* (TSM), *noise*, *resampling*, *linear speed change*, *pitch shifting*, kompresi *motion pictures experts group*, *audio layer 3* (MP3) dan kompresi *advance audio coding* (AAC).

1.5 Metode Penelitian

Metodologi yang digunakan dalam proses penulisan penelitian ini adalah :

1. Studi Pustaka
Bertujuan untuk mempelajari dasar teori mengenai steganografi, domain penyisipan dalam steganografi, pengolahan audio digital, pengolahan citra digital, protokol CS, algoritme enkripsi dan dekripsi RSA, serta metode penyisipan SMM berikut algoritme di dalamnya.
2. Pengumpulan Data
Bertujuan untuk mendapatkan data citra yang akan disisipkan serta lima jenis data audio yang akan menjadi tempat penyisipan. Jenis audio tersebut diantaranya adalah *voice*, piano, drum dan orkestra.
3. Studi Pengembangan Sistem
Bertujuan untuk menentukan perangkat lunak yang akan digunakan dan melakukan analisis terhadap sistem yang akan dikembangkan berdasarkan studi pustaka.
4. Implementasi Perangkat Lunak
Bertujuan untuk melakukan implementasi metode dengan menggunakan

perangkat lunak komputasi numerik yang memungkinkan peneliti memanipulasi variabel-variabel masukan dan meneliti akibatnya terhadap kinerja sistem steganografi audio.

5. Pengujian dan Analisis Performansi

Bertujuan untuk menguji sistem dan kinerja steganografi dengan memberikan berbagai macam serangan yang disebutkan dalam batasan masalah dengan parameter-parameter seperti BER, C, MOS, ODG dan SNR.. Parameter MOS diperoleh dengan melibatkan 30 orang responden.

6. Pengambilan Kesimpulan

Bertujuan untuk menarik kesimpulan berdasarkan analisis yang didapatkan dari hasil pengujian.

1.6 Sistematika Penulisan

Sistematika penulisan laporan adalah sebagai berikut:

- Bab 1 PENDAHULUAN

Bab ini berisi latar belakang, permasalahan, tujuan, metode penelitian, dan sistematika penulisan.

- Bab 2 KONSEP DASAR

Bab ini membahas tentang dasar-dasar teori yang mendasari dan mendukung penelitian tugas akhir ini.

- Bab 3 MODEL SISTEM DAN PERANCANGAN

Bab ini membahas tentang tahap proses perancangan sistem yang digunakan pada simulasi steganografi audio.

- Bab 4 PENGUJIAN DAN ANALISIS

Bab ini membahas analisis hasil simulasi secara kualitatif dan kuantitatif. Analisis dilakukan berdasarkan parameter keberhasilan kerja sistem yang diamati dari keluaran yang dihasilkan oleh sistem.

- Bab 5 KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan hasil tugas akhir dan saran untuk pengembangan dan penyempurnaan lebih lanjut.