BAB I

PENDAHULUAN

1.1 Latar Belakang

Faktor keamanan data dalam proses pertukaran data antar perangkat informasi sangat penting untuk diperhatikan seiring dengan maraknya penyalahgunaan data oleh pihak yang tidak diinginkan. Data penting yang seharusnya menjadi dokumen rahasia, malah menjadi obyek yang sering dicuri atau bocor kepada pihak-pihak yang tidak diinginkan karena kurangnya pengamanan data tersebut pada saat terjadi pertukaran data di media transmisi. Untuk meningkatkan keamanan data yang dipertukarkan antar perangkat informasi, perlu dilakukan suatu teknik pengamanan data, steganografi adalah salah satunya.

Teknik steganografi bertujuan untuk menyembunyikan informasi yang sebenarnya ke dalam sebuah data lain sehingga dapat mengelabuhi pihak penyerang bahwa pesan rahasia sesungguhnya berada di dalam sebuah data lain sehingga pesan tersebut tidak terlihat secara kasat mata. Akan tetapi penggunaan steganografi perlu dimodifikasi agar data rahasia memiliki tingkat keamanan yang tinggi. Teknik steganografi yang banyak diketahui saat ini hanya dilakukan sekali proses penyembunyian saja. Satu kali penyembunyian dengan metode steganografi terkadang tidak cukup mengingat semakin berkembangnya pengetahuan tentang metode steganografi yang memungkinkan terbongkarnya data rahasia oleh pihak yang tidak diinginkan. Untuk mengantisipasi hal tersebut, perlu dilakukan modifikasi yaitu salah satunya dengan menyembunyikan kembali pesan rahasia yang sebelumnya telah disembunyikan ke dalam sebuah data atau dengan melakukan penggandaan proses steganografi. Dengan demikian pihak penyerang tidak akan mengetahui pesan rahasia walaupun pihak-pihak tersebut mengetahui algoritma steganografi yang digunakan karena ekstraksi satu kali hanya akan membuka cover pesan rahasia.

Pada tugas akhir ini dilakukan dua kali proses steganografi dengan menggunakan dua metode yang berbeda di setiap *level* tahap steganografi. Pada

steganografi *level* pertama digunakan metode *diamond encoding*. Pemilihan metode ini berdasarkan pada penelitian sebelumnya yang memberikan hasil performansi steganografi yang tahan terhadap serangan sehingga pesan dapat diekstraksi sempurna dan tidak terdapat *error* [3]. Akan tetapi adanya kemungkinan pesan rahasia bocor jika hanya dilakukan satu kali proses steganografi, maka proses steganografi digandakan untuk mendapatkan tingkat keamanan pesan rahasia yang lebih tinggi. Oleh karena itu dilakukan penyisipan berlanjut dengan metode *discrete wavelet transform*. Kedua metode ini digabungkan untuk mengetahui performansi steganografi jika dilakukan modifikasi yaitu dengan cara menggandakan proses penyisipan dan ekstraksi sehingga didapatkan sistem yang lebih aman dan tahan terhadap serangan.

1.2 Tujuan

Tujuan dari Tugas Akhir ini adalah:

1. Dapat menyembunyikan pesan rahasia berupa teks dengan teknik steganografi ganda dengan metode *diamond encoding* dan *Discrete Wavelet Transform*.
2. Mengekstraksi kembali pesan rahasia awal berupa teks dengan error sekecil mungkin.
3. Menganalisis ketahanan sistem terhadap serangan AWGN (*Additive White Gaussian Noise*)
4. Mengukur performansi steganografi ganda yaitu pada *audio cover* yang telah dilakukan dua kali penyisipan dengan parameter SNR (*Signal to Noise Ratio*), waktu komputasi penyisipan, serta CER (*Character Error Ratio*) dari pesan yang diekstraksi. secara subjektif dilakukan analisis dengan MOS (*Mean Opinion Score*)

1.3 Perumusan Masalah

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

1. Bagaimana melakukan penyisipan pesan rahasia dengan penggandaan proses steganografi dengan metode *diamond encoding* dan *discrete wavelet transform* (DWT)?

2. Bagaimana cara mengekstraksi pesan asli sehingga diperoleh pesan rahasia?
3. Bagaimana performansi sistem dilihat dari SNR *stego audio*, waktu komputasi, dan CER?
4. Bagaimana pengaruh sistem jika diserang dengan AWGN pada level SNR AWGN yang berbeda beda?

1.4 Batasan Masalah

Untuk mempersempit cakupan masalah pada tugas akhir ini, maka ditentukan batasan masalah sebagai berikut:

1. Sistem yang dirancang hanya mengenai proses simulasi penyisipan pesan dan ekstraksi pesan tanpa melalui media transmisi
2. Cover terluar berupa audio dengan format.wav sedangkan cover gambar dalam berupa citra bitmap *grayscale* yang dilevelkan ke dalam 16-level *grayscale*
3. *File audio* berdurasi 30detik
4. Pesan rahasia berupa *text*
5. Stego audio hanya diperdengarkan untuk telinga manusia normal
6. Proses ekstraksi pesan membutuhkan *audio cover* asli (*Unblind* steganografi)
7. Parameter performansi yang diteliti dan dianalisis meliputi SNR, MOS, dan CER
8. Keseluruhan sistem diolah menggunakan MATLAB R2011b
9. Serangan berupa AWGN dengan SNR AWGN 20 dB, 30dB, 40dB, 50dB, dan 70 dB

1.5 Metodologi Penelitian

Metode penelitian yang digunakan dalam tugas akhir ini meliputi:

1. Melakukan *study literature* untuk mengumpulkan data-data dan mendapatkan informasi yang jelas yang dapat mendukung pembuatan dasar teori yang kuat dan metode yang digunakan
2. Merancang diagram alir sistem yang dijalankan di Matlab dan menganalisisnya
3. Menganalisis performansi sistem

4. Membuat kesimpulan berdasarkan hasil pengujian dari sistem yang dibuat
5. Menyusun laporan tugas akhir

1.6 Sistematika Penulisan

Tugas akhir ini disusun berdasarkan topik bahasan yang disusun secara sistematis sebagai berikut:

Bab I Pendahuluan

Bab ini membahas latar belakang, tujuan, perumusan dan batasan masalah, metodologi penelitian serta sistematika penulisan.

Bab II Dasar Teori

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

Bab III Perancangan dan Simulasi Sistem

Bab ini menjelaskan proses desain dan realisasi sistem steganografi ganda menggunakan *diamond encoding* dan *discrete wavelet transform*.

Bab IV Pengujian Sistem dan Analisis

Bab ini membahas analisis dari hasil pengujian secara kualitatif dan kuantitatif. Analisis dilakukan terhadap parameter kinerja sistem yang damati berdasarkan keluaran yang dihasilkan oleh sistem.

Bab V Kesimpulan dan Saran

Bab ini membahas kesimpulan yang didapat dari hasil analisis terhadap sistem serta saran untuk memperbaiki sistem.