BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Di era informasi seperti sekarang ini, komunikasi sudah menjadi bagian dalam kehidupan manusia. penyimpanan informasi secara rahasia tanpa diketahui oleh orang lain merupakan salah satu faktor yang banyak dicari untuk meningkatkan keamanan maupun privasi. Dalam perkembangan komunikasi digital yang sangat pesat melalui internet membuat akan tiga teknik keamanan yaitu, *watermarking*, kriptografi, dan steganografi. Dalam kriptografi teks polos dikonversi menjadi teks sandi yang membuat isi pesan cacat, sementara *watermarking* data akan disisipkan untuk membawa informasi seperti kepemilikan dan hak cipta. Tetapi dalam *watermarking* keberadaan pesan rahasia dapat terdeteksi, yang membuat tingginya minat operator untuk mengungkap pesan rahasia selama transmisi. Oleh karna itu, steganografi merupakan teknik keamanan yang banyak dan dapat diandalkan. Steganografi dijadikan sebagai pelengkap enkripsi, dalam menciptakan keamanan dan keprivasian lebih baik teknik ini dapat dikombinasikan. Media pembawa dalam keadaan saat ini berupa teks, video, gambar, audio, dan datagram dll [1].

pada penelitian pertama yang berjudul *"An Efficient Audio Steganography Technique to Hide Text in Audio"* kelebeihannya menggunakan metode Least Significant Bit (LSB) dan memiliki SNR rata-rata 86,78dB tidak ada serangan untuk menguji coba hasil nilai SNR, BER, dan CER setelah serangan [1]. Dalam penelitian kedua yang berjudul "*An Efficient Method to Audio Steganography based on Modification of Least Significant Bit Technique using Random Key"*kelebihannya menggunakan metode metode *Least Significant Bit* (LSB) dan *Discrete Wavelet Transform* (DWT) yang mana hasilnya memiliki rata-rata SNR 80,75dB kekurangannya serangan untuk menguji ketahanan seberapa rusaknya pesan setelah diberi serangan tidak ada didalamnya [2]. Didalam penelitian ketiga yang berjudul *"Secure LSB Steganography over Modified VigenèreAES Cipher and Modified Interrupt Key-AES Cipher"* juga memiliki kelebihan karna menggunakan

metode *Least Significant Bit* (LSB) dan menggunakan *host* berupa *image* menggunakan kunci *deffie-hellman* yang mana pada *host* audio memungkinkan penyerang jarang bias mengidentifikasi, yang mana dalam penelitian tidak menggunakan *audio* sebagai *host* dengan metode LSB dan attack berupa CS[22]. Didalam penelitian keempat yang berjudul "*LSB Modification based Audio Steganography using Trusted Third Party Key Indexing Method"* menggunakan metode LSB saja dan memiliki nilai SNR kisaran 139 dB hingga 142 dB dan nilai BER kisaran 0,23 hingga 0,32 persen, tetapi didalam penelitian ini tidak memiliki serangan berupa CS untuk menentukan ketahanan audio steganografi dan DWT untuk ketahanan dari serangan[21]. Pada penelitian kelima yang berjudul "*Enhanced Audio LSB Steganography for Secure Communication"* menggunakan metode LSB yang mana memiliki nilai SNR rata-rata 80dB, tetapi didalam penelitian ini tidak memiliki serangan berupa CS untuk menentukan ketahanan audio steganografi dan DWT untuk ketahanan dari serangan sama seperti penelitian penelitian sebelumnya[23] Pada Tabel 1.1 dibawah menunjukkan perbandingan antara penelitian-penelitian sebelumnya, yang semuanya tidak memiliki metode IRLS dan Attack berupa CS untuk mengujinya.

Tabel 1. 1 Perbandingan penelitian sebelumnya

Penelitian Sebelumnya							
Penelitian ke	metode			parameter			Attack CS
	LSB	IRLS	DWT	SNR	CER	BER	
1	ada	Tidak	tidak	86,78	0	0	Tidak
2	ada	Tidak	ada	80,75	0	0	Tidak
3	ada	Tidak	tidak	0	0	0	Tidak
4	ada	Tidak	tidak	139-142	0	0,23-0,32	Tidak
5	ada	Tidak	tidak	80	0	0	Tidak

Pada penelitian kali ini akan membuat sebuah analisis terhadap steganografi audio menggunakan metode LSB dan rekonstruksi IRLS yang mana untuk menyembunyikan pesan diubah menjadi *cipher text* menggunakan RSA lalu didalammnya akan diberi serangan berupa CS dan membandingkan ketika sebelum diberi serangan dengan sesudah diberi serangan juga memiliki nilai SNR, BER, dan CER yang tidak jauh berbeda atau *secret message* yang tidak terlalu rusak. Maka

dari itu pada tugas akhir ini akan membantu orang orang yang ingin memiliki atau membutuhkan keamanan dan privasi dalam pengiriman sebuah pesan berupa *text* sehingga lebih nyaman dan merasa aman dalam pengiriman sebuah pesan. Dan akan dilakukan proses analisis dari ke efisiensinya menggunakan audio steganografi dalam pengiriman pesan teks, dimana *host*-nya sendiri berupa audio dan pesan yang mau dikirimkan berupa teks yang diproses menggunakan satu algoritma yaitu algoritma IRLS dengan menggunakan metode LSB.

1.2 Rumusan Masalah

Dalam Tugas Akhir ini akan dibahas mengenai :

1. Dengan adanya serangan didalam steganografi audio memungkinkan terjadinya kerusakan atau kecacatan sebuah pesan yang disisipkan yang akan membuat tingkat *error* saat proses ekstraksi semakin besar
2. Bagaimana penerapan metode enkripsi dan dekripsi *Rivest Shamir Adleman* RSA
3. Penghitungan waktu yang dibutuhkan didalam proses penyisipan dan ekstraksi pesan
4. Pengukuran kualtas audio yang sudah disisipkan secara subjektif dan objektif yang dibandingkan dengan audio aslinya

1.3 Tujuan dan Manfaat

Tujuan dari Tugas Akhir ini adalah :

1. Merancang dan mengimplementasikan audio steganografi untuk mengirimkan pesan teks di dalam MATLAB.
2. Mengkombinasikan metode *Least Significant Bit* dengan algoritma *Iteratively Reweighted Least Square* untuk membuat ketahanan dalam audio steganografi
3. Menguji dan menganalisis *Audio steganography* dalam mentransmisikan sebuah pesan tanpa terjadinya kecacatan, berdasarkan parameter pengujian nilai SNR, BER, dan CER

1.4 Batasan Masalah

Agar mempremudah dan membatasi cakupan pembahasan masalah pada Tugas Akhir ini, maka disimpulkan batasan – batasan sebagai berikut :

1. *Host* berupa audio *file* wav (*.wav) untuk pembawa pesannya.
2. Pesan yang disisipkan berupa *file* teks (*.txt).
3. Informasi yang bisa disisipkan berupa suara, teks, gambar.
4. Tidak mempermasalahkan di dalam *key management* antara pengirim dan penerima.
5. Menggunakan metode LSB untuk menyisipkan pesan
6. Menggunakan RSA dalam proses enkripsi dan dekripsi pesan yang akan disisipkan
7. Serangan yang digunakan berupa CS
8. Rekonstruksi IRLS digunakan untuk estimasi setelah serangan
9. MATLAB sebagai aplikasi penelitian.

1.5 Metode penelitian

Metode penelitian yang digunakan dalam mengerjakan Tugas Akhir ini antara lain :

1. Melakukan studi literatur dengan mengumpulkan dan memahami sumber informasi yang berkaitan dengan masalah tugas akhir.
2. Percobaan dengan menyisipkan pesan dengan jenis dan ukuran berbeda kedalam media .wav.
3. Melakukan Analisis pengukuran performansi dari audio steganografi yang lebih sempurna dengan metode standar menggunakan pengukuran objektif dan subjektif terhadap *file* audio stegano yang di hasilkan.
4. Menyusun laporan proses dalam pengerjaan Tugas Akhir.