BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada zaman sekarang, teknologi merupakan salah satu bidang yang terus berkembang dalam rangka pemenuhan kebutuhan manusia. Komputer, perangkat *mobile*, jaringan, dan teknologi informasi keamanan adalah bagian dari teknologi yang berkembang pesat. Orang-orang mulai menciptakan dan berbagi data-data multimedia karena adanya kemudahan dan fleksibilitas perangkat lunak (Citrix, 2012). Selain itu, faktor harga data-data digital yang terus menurun juga mempengaruhi hal tersebut. Penggunaan alat rekam dan perangkat penyimpanan juga mempercepat perkembangan multimedia.

Cepatnya perkembangan perangkat komputer, *mobile*, jaringan dan teknologi informasi keamanan. Orang orang mulai membuat dan berbagi data data multimedia karena kemudahan dan fleksibilitas perangkat lunak dan turunnya harga data data digital. Penggunaan alat rekam dan perangkat penyimpanan juga mempercepat perkembangan multimedia (Ethan P. White, 2014).

Dengan pesatnya perkembangan multimedia, kepentingan untuk memproteksi data digital dari pengguna yang tidak sah mulai dibutuhkan, salah satunya ialah dengan menyembunyikan data di dalam data digital lainnya atau biasa disebut sebagai *steganografi*. Selain itu, dapat juga

dilakukan pengacakan *bit* data digital dengan menggunakan *Key*. Tindakan ini disebut sebagai enkripsi. Kekurangan enkripsi adalah orang dapat mengetahui bahwa data tersebut sedang dikirim (tidak dapat dicegah), sehingga data yang telah dienkripsi masih dapat ditangkap dan dianalisis. Namun demikian, tanpa *key*, enkripsi tidak dapat dipecahkan (Oriyano, 2009).

Dibandingkan dengan enkripsi, *steganografi* merupakan metode pengamanan data yang memiliki pendekatan berupa pengiriman informasi yang disembunyikan dalam media lain (Masoud Nosrati, Ronak Karimi, Mehdi Hariri, 2011). *Steganografi* tidak hanya merujuk pada media digital, tetapi juga media lainnya. Menurut (Gary C. Kessler, 2013), ada banyak sekali metode *steganografi* mulai dari sesuatu seperti tinta tak terlihat, *mikrodots*, hingga menyembunyikan pesan pada setiap huruf kedua pada pesan teks yang besar dan *spread spectrum*. Sederhananya, apabila pesan yang terenkripsi dikirim, pesan tersebut dapat menarik perhatian dari pihak yang tidak diinginkan. Dengan menggunakan *steganografi*, pengiriman pesan tersebut tidak akan menimbulkan kecurigaan (Oriyano, 2009).

Penelitian ini menggunakan metode *steganografi*, yang ditemukan oleh Ajay B. Gadicha, dengan nama *audio wave steganography*. Metode ini mencoba mengeksplorasi *bit rate* ke-4 pada *Least Signification Bit audio steganography* yang mampu mengurangi distorsi dari penyembunyian data pada *host audio*. Dengan algoritma ini data disembunyikan dalam lapisan ke-4 *Least Signification Bit* dan menghasilkan peningkatan ketahanan akan

distorsi (Ajay.B.Gadicha, 2011). Tidak seperti metode *Least Signification Bit* (LSB) yang tidak efektif karena rentannya terhadap serangan untuk mendapatkan pesan yang disembunyikan, *Least Signification Bit* juga memiliki kerentanan terhadap distorsi oleh *high average power* (Nosrati, M., Karimi, R., & Hariri, M., 2012).

Metode ini menggunakan pendekatan dua langkah. Pada pendekatan pertama, *bit* yang di *steganografi* ditanam kedalam 4th *Least Signification Bit host audio*, kemudian pada langkah kedua *noise* yang ditimbulkan oleh penanaman dibentuk agar dapat merubah sifat dari *white noise* (Ajay.B.Gadicha, 2011).

Tabel 1.1 Penanaman *bit* pada file

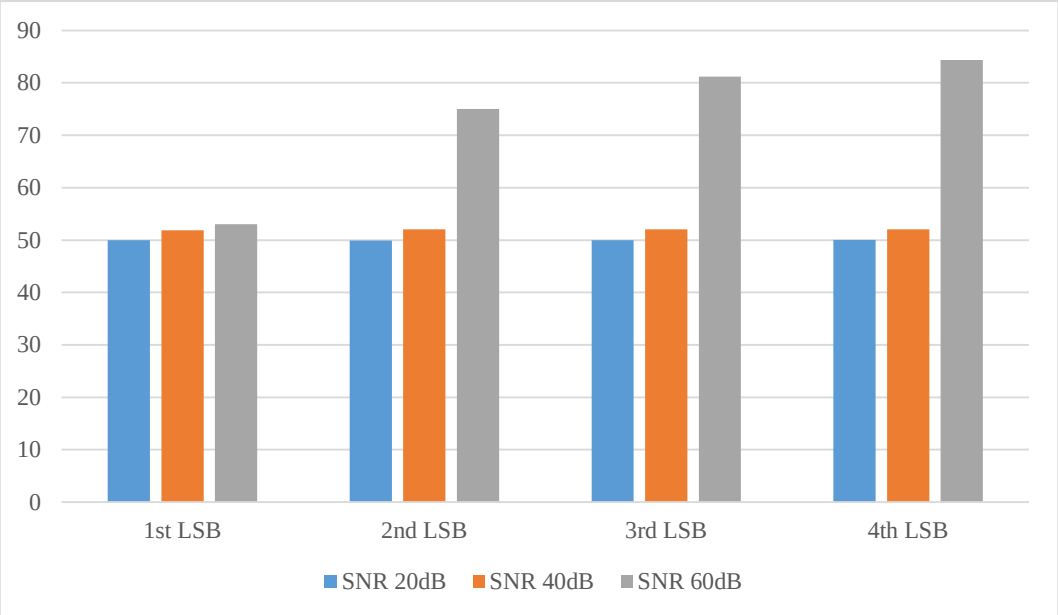
FILE CONTOH	SETELAH PENANAMAN BIT '0'	QUANTIZATION ERROR
0000 1000	0000 0000	8
0000 0100	0000 0000	4
0000 0010	0000 0000	2
0000 0001	0000 0000	1

Tabel 1.2 Penanaman *bit* dan pembalikan LSB

FILE CONTOH	SETELAH PENANAMAN BIT '0' & PEMBALIKAN 4TH LSB	QUANTIZATION ERROR
0000 1000	0000 0111	1
0000 0100	0000 0011	1
0000 0010	0000 0001	1
0000 0001	0000 0000	1

Tabel 1.3 Embedding rate of signal under different SNR

		Embedded rate of watermarked n^{th}			
		1^{st} LSB	2^{nd} LSB	3^{rd} LSB	4^{th} LSB
Resulting SNR	No Noise	100	100	100	100
	20dB	53.02	75.02	81.21	84.39
	40dB	51.81	52.02	52.04	52.05
	60dB	53.02	75.02	81.21	84.39



Gambar 1.1 Signal Recovery Rate untuk setiap n^{th} LSB pada SNR 20, 40 dan 60.

1.2 Rumusan Masalah

Dari kondisi-kondisi yang dijelaskan di atas, rumusan masalah penelitian ini yaitu sebagai berikut.

- Bagaimana mengimplementasikan *Advanced Encryption Standard* untuk melakukan enkripsi pada teks (*string*).
- Bagaimana mengimplementasikan algoritma *audio wave steganography* untuk melakukan *steganografi* pada *waveform audio*.
- Bagaimana membangun aplikasi pengamanan data yang mengimplementasikan algoritma *audio wave steganography* dan *advanced encryption standard*.

1.3 Batasan Masalah

Beberapa batasan yang harus ditentukan dalam penelitian ini yaitu sebagai berikut.

- *Audio* yang di *steganografi* memiliki ekstensi .flac, yang disebabkan oleh limitasi API pada Windows Phone.
- Pesan berupa teks yang di-*input* oleh *user*.
- *Key* berupa teks yang di-*input* oleh *user*.
- *Audio* yang telah di-*steganografi* memiliki ekstensi .wav.
- Pesan yang dienkripsi dan disisipkan pada audio berupa teks (*string*) yang ditulis secara langsung.

1.4 Tujuan Penelitian

- Membangun aplikasi pengamanan data yang mengimplementasikan algoritma *audio wave steganography* dan *advanced encryption standard*.

- Menguji seberapa mirip *audio* yang telah di-*steganografi* dengan *audio* aslinya.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah:

- Penelitian ini bermanfaat bagi pengguna yang membutuhkan keamanan data dalam mengirimkan informasi yang rahasia.
- Penelitian ini juga bermanfaat sebagai dasar penelitian selanjutnya dengan topik serupa.

1.6 Sistematika Penulisan

Sistematika penulisan laporan skripsi ini dijelaskan sebagai berikut.

Bab I Pendahuluan

Berisi latar belakang, rumusan masalah, batasan masalah, tujuan penulisan, manfaat penulisan, dan sistematika penulisan.

Bab II Tinjauan Pustaka

Berisi landasan teori mengenai piranti lunak, rekayasa piranti lunak, *steganografi, least significant bit*, Kriptografi, Windows phone, *Waveform audio, Free Lossless Audio Codec*.

Bab III Analisis dan Perancangan Sistem

Berisi spesifikasi umum kebutuhan dan desain sistem.

Bab IV Implementasi dan Uji Coba

Berisi penjelasan mengenai implementasi dan hasil uji coba sistem.

Bab V Simpulan dan Saran

Berisi kesimpulan dan saran untuk penelitian selanjutnya.