BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang meningkat pesat seperti mudahnya internet diakses dengan berbagai media seperti pada *handphone, ipad, notebook*, dan sebagainya sehingga memudahkan pertukaran informasi ke berbagai tempat. Informasi tersebut dapat berupa data teks, *audio, image,* dan sebagainya. Namun dibalik kemudahan juga terdapat sisi yang perlu diwaspadai yaitu keamanan dari data yang dikirimkan. Jika data yang dikirimkan merupakan data yang bersifat umum atau memiliki tingkat kerahasiaan rendah tentunya bukanlah suatu masalah mengirimkan data tersebut secara langsung tanpa perubahan atau secara polos ke penerima. Berbeda halnya jika yang dikirimkan berupa data penting misalnya pasword suatu brankas ataupun data-data yang memiliki tingkat kerahasiaan yang tinggi. Data tersebut perlu dijaga keaslian dan keutuhannya jika ingin dikirim karena data tersebut dapat disadap atau diketahui oleh pihak ketiga selama proses pengiriman. Untuk mengirimkan data seperti itu perlu dilakukan pengamanan agar tidak diketaui oleh pihak ketiga.

Misalkan pada bisnis konten digital yang membuka peluang untuk kejahatan klasik di bidang teknologi informasi, yaitu pembajakan. Konten-konten yang seharusnya menjadi properti legal dari produsen dan secara legal dimiliki oleh orang yang telah membelinya, bisa dengan mudah disalahgunakan oleh pihak-pihak yang tidak bertanggungjawab. Konten digital seharusnya diproteksi tidak hanya ketika dikirimkan, tetapi juga ketika konten digital tersebut sampai kepada pemakainya. Misalnya, pihak yang telah membeli sebuah konten bisa saja mengirimkannya ke orang lain, atau membuat duplikatnya untuk nantinya dijual lagi. Oleh karena itu, dibutuhkan suatu mekanisme untuk mengatasi permasalahan pembajakan ini.

Salah satu caranya ialah memasukan data tersebut ke data lain yang bersifat umum sehingga tidak ada kecurigaan terhadap data yang dikirimkan. Salah satu metoda yang dapat digunakan ialah metoda *watermarking*.

Watermarking World (2002) mendefinisikan *watermark* sebagai data tersembunyi yang ditambahkan pada sinyal pelindung (*cover signal*), sedemikian rupa sehingga penambahan tersebut tidak terlihat. *Watermark* dapat juga merupakan suatu pola yang terbentuk oleh kumpulan *bit* data tertentu, yang disisipkan kedalam file citra, audio ataupun video yang mengidentifikasikan informasi hak cipta file tersebut (Webopedia dalam Lestari : 6). *Watermarking* merupakan bagian dari steganografi modern yang menggunakan *file-file* multimedia sebagai wadah untuk menyembunyikan pesan. Digital watermarking dikembangkan sebagai salah satu jawaban untuk menentukan keabsahan pencipta atau pendistribusi suatu data digital dan integritas suatu data digital. Teknik watermarking bekerja dengan menyisipkan sedikit informasi yang menunjukkan kepemilikan, tujuan, atau data lain, pada media digital tanpa mempengaruhi kualitasnya.

Metode yang digunakan pada proses penyisipan dan ekstraksi adalah *spread spectrum* dan *LSB,* dan suara digital yang akan disisipi informasi *watermarking* adalah dalam format WAV.

Format suara WAV (*waveform data*) merupakan standar dari RIFF (Resource Interchage File Format) yang dibentuk oleh *Microsoft*. Format suara WAV dipilih karena format ini banyak digunakan, dan memiliki kualitas suara yang sangat baik [4].

Ada beberapa metode *watermarking* yang banyak digunakan untuk menyisipkan informasi digital kedalam suara WAV. Beberapa diantaranya adalah *phase coding, spread spectrum, echo data hiding,* dan *low bit coding*[3]. Metode yang akan digunakan adalah *low bit coding.* Metode ini dipilih, karena metode ini lebih mudah dilakukan, dan metode ini tidak menambah ukuran dari data suara WAV.

Beberapa penelitian yang berkaitan dengan teknik penyembunyian data diantaranya yaitu :

1. **Alfebra Stavia Ardhyana dan Asep Juarna [1]** dalam jurnal penelitiannya yang berjudul *" Aplikasi Steganografi Pada Mp3 Menggunakan Teknik Lsb "*yang membahas tentang penyisipan data pada file mp3 dengan metode s*teganografi* dalam file Mp3 dengan metode *least significant bit* berbasis *Java.*
2. **Desi Alex Lestari [2]** dalam penelitiannya yang berjudul *"Implementasi Teknik Watermarking Digital Pada Domain Dct Untuk Citra Berwarna"* yang membahas tentang teknik penyembunyian dengan metode watermarking dengan media citra sebagai wadah penyembunyian.
3. Marganda Papar Sihombing dalam penelitiannya yang berjdul "*Penyimpanan Data Teks Kedalam Suara Digital Dengan Metode Low Bit Coding*" yang membahas *watermarking* data teks pada *file audio* tidak terkompresi (.Wav) dengan meetode *low bi coding.*

Berdasarkan pemikiran inilah, maka judul tugas akhir yang diangkat adalah ***"Perancangan Aplikasi Pengamanan Hak Cipta Untuk Data Audio Digital Wav Dengan Teknik Watermarking Menggunakan Metode Spread Spektrum dan LSB".***

1.2 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah :

1. Untuk mengetahui dan merancang aplikasi proses penyisipan data teks pada file audio terutama wav tanpa memberikan perubahan pada file audio tersebut sehingga tidak menimbulkan kecurigaan saat pengiriman data.
2. Untuk menganalisa unjuk kerja dari file yang disisipi dan file hasil ekstraksi dengan menggunakan nilai MOS, BER, dan SNR.

1.3 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah :

1. Penelitian ini diharapkan dapat memberikan gambaran dari proses penyembunyian data dalam data lain dalam proses pengiriman data guna meningkatkan keamanan data.
2. Hasil penelitian ini dapat dikembangkan dan dimanfaatkan dalam sistem keamanan penyampaian informasi dan sebagai penyimpan suatu karya yang mempunyai hak cipta tersendiri guna menghindari duplikasi oleh pihak lain.

1.4 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah :

1. Penelitian ini dirancang sebagai aplikasi dari sistem keamanan pengiriman data untuk menyembunyikan data digital di dalam data digital lainnya dengan teknik *watermarking.*
2. Metoda penyembunyian data yang digunakan pada *watermarking* ialah metoda *Spread Spektrum* dan *Least Significant Bit* (LSB).
3. Data yang disembunyikan berupa data teks (txt) dengan media penyimpanan berupa berkas audio mono berformat Windows PCM Waveform Audio (wav).
4. Pembangkit bilangan pseudorandom yang digunakan adalah LCG (*Linear Congruental Generator*)
5. Noise yang disebabkan dari lingkungan diabaikan.
6. Perangkat lunak yang digunakan adalah Matlab 2010 versi 7.10.499

1.5 Metodologi Penelitian

Metodologi penelitian yang digunakan pada tugas akhir ini adalah:

1. Studi literatur, dilakukan untuk mendapatkan pemahaman tentang konsep teoritis yang berhubungan dengan topik tugas akhir dan hal-hal lain yang dibutuhkan untuk pelaksanaan tugas akhir.

2. Perancangan sistem.
3. Pembuatan program simulasi.
4. Pengumpulan data dan simulasi program.
5. Analisis data.
6. Penyusunan laporan akhir.

1.6 Sistematika Penulisan

Bab I Pendahuluan, berisi tentang latar belakang, tujuan penelitian, manfaat penelitian, batasan masalah, dan sistematika penulisan.

Bab II Penjelasan teori dasar teknik penyembunyian data teks dengan *watermarking* serta metoda *Spread Spektrum* dan *Least Significant Bit* sebagai salah satu metoda penyembunyian data dalam watermarking dan penjelasan mengenai format file wav sebagai wadah penyembunyian data.

Bab III Berisi tentang metode penelitian tentang *watermarking* data teks dalam file audio wav dengan metode *Spread Spektrum* dan *Least Significant Bit* (LSB).

Bab IV Berisi tentang rancangan dan langkah-langkah dalam proses *watermarking* data teks dalam file audio wav dengan metode *Spread Spectrum* dan *Least Significant Bit* (LSB).

Bab V Hasil penelitian dan analisis serta pembahasan dari penelitian tugas akhir ini.

Bab VI Penutup yang berisi kesimpulan dan saran