BAB I

PENDAHULUAN

I.1. LatarBelakang

Perkembangan teknologi komputer pada saat ini menyebabkan terkaitnya manusia dengan komputer untuk memudahkan membantu penyelesaian dan komputerisasi. Hal ini membuka banyak peluang dalam pengembngan aplikasi komputer tetapi juga membuat peluang adanya ancaman terhadap pengubahan dan pencurian data. Sebuah aplikasi yang dapat diakses oleh siapapun termasuk orang-orang atau pihak-pihak yang memang berniat untuk mencuri atau mengubah data. Oleh karena itu, untuk melindungi data terhadap akses, pengubahan dan penghalangan yang tidak dilakukan oleh pihak yang berwenang, peranti keamanan data komputer harus disediakan.

Keamanan komputer adalah kumpulan peranti yang dirancang untuk melindungi komputer sehingga data pada komputer terlindungi,dan juga pengubahan dan penghalangan oleh pihak yang tidak berwenang. Mekanisme keamanan jaringan pada implementasinya menggunakan teknik-teknik penyandian, yaitu kriptografi dan Steganografi.

Ketika seseorang yang hendak mengirim file kepada orang lain, tidak ingin isi file tersebut diketahui oleh orang lain, yang mana isi file tersebut bersifat sangat rahasia atau pribadi, yang hanya boleh diketahui antara pihak pengirim dan pihak penerima pesan. Oleh karena itu, biasanya pengirim tersebut mengirim file secara tersembunyi agar tidak ada pihak lain yang mengetahui. Salah satu cara

untuk mengatasi situasi di atas adalah mengembangkan suatu aplikasi yang mampu menyamarkan file tersebut pada suatu media. Teknik ini disebut *steganografi*, yaitu teknik penyembunyian data pada suatu media. Setiap orang bisa menampilkan atau membuka media tersebut, namun tidak menyadari bahwa media tersebut telah disisipkan file rahasia oleh pengirim. *steganografi* memungkinkan penyembunyian teks pada berbagai jenis media digital seperti berkas citra, suara, video, dan teks.

Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian kriptografi modern adalah tidak saja berurusan hanya dengan penyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi. Fungsi hash yang banyak digunakan dalam kriptografi MD5 dan SHA. Dalam artikel ini fungsi hash yang digunakan algoritma MD5. MD5 menerima masukan berupa pesan dengan ukuran sembarang dan menghasilkan message digest yang panjangnya 128 bit.

Steganografi merupakan ilmu yang menyembunyikan teks pada gambar pada media lain yang telah ada sedemikian sehingga teks yang tersembunyi menyatu dengan media itu. Media penyembunyian pesan tersembunyi dapat berupa media teks, gambar, audio atau video. Steganografi yang kuat memiliki sifat media yang telah tertanam teks tersembunyi sulit dibedakan dengan media asli namun teks tersembunyi tetap dapat diekstrasi. Metode EOF (*End Of File*)

merupakan salah satu teknik yang menyisipkan data pada akhir *file*. Teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sama dengan ukuran *file* sebelum disisipkan data ditambah dengan ukuran data yang disisipkan kedalam *file* tersebut. Dalam teknik EOF, data yang disisipkan pada akhir *file* diberi tanda khusus sebagai pengenal *start* dari data tersebut.

Untuk mengatasi permasalahan keamanan tersebut dapat menggunakan *kriptografi*, yaitu teknik pengenkripsian pesan. Namun teknik ini dapat menimbulkan kecurigaan karena pesan acak tidak memiliki makna secara kasat mata, sihingga mudah dicurigai. Untuk menjawab masalah dari *kriptografi* digunakan teknik penyembunyian pesan yaitu steganografi. Teknik ini menyisipkan pada media lain (*cover object)* yang umum digunakan dalam kehidupan. Pesan yang dikirimkan melalui media yang telah disisipi pesan (*stego-object)* tidak akan mengundang kecurigaan orang lain, kerana perbedaannya tidak dapat dilihat secara kasat mata.

Berdasarkan latar belakang di atas maka penulis tertarik untuk mengangkat skripsi dengan judul "**Perancangan Aplikasi Keamanan Data Dengan Metode End Of File (EOF) dan Algoritma MD5"** untuk dapat membantu mengamankan data.

I.2. Ruang Lingkup Permasalahan

Pada skripsi ini akan disampaikan pembahasan mengenai Perancangan Aplikasi Keamanan Data Dengan Metode End Of File (EOF) dan Algoritma

MD5. Aplikasi yang penulis buat merupakan sebuah perancangan untuk mengamankan data teks.

I.2.1. Identifikasi Masalah

Berdasarkan latar belakang diatas dapat diidentifikasi permasalahan yaitu:

1. Pengiriman data atau informasi secara jarak jauh sangatlah rawan terhadap pencurian, penyadapan bahkan pemalsuan informasi apalagi untuk data yang bersifat rahasia.
2. Program steganografi dengan menggunakan metode End Of File dan keamanan algoritma MD5 perlu dibuat. Metode ini sudah diakui tingkat keamanannya dalam proses pengiriman bahkan pertukaran data dan informasi.

I.2.2. Rumusan Masalah

Berdasarkan identifikasi masalah diatas timbulah suatu rumusan masalah yaitu:

1. Bagaimana cara melakukan penyisipan teks kedalam audio khususnya dengan format MP3 dan WAV?
2. Bagaimana cara kerja metode EOF dan algoritma MD5 dalam melakukan penyisipan teks terhadap suatu audio pada bahasa pemrograman VB.net?
3. Bagaimana cara kerja Algoitma MD5 untuk pengamanan teks dengan menggabungkan metode EOF?
4. Bagaimana merancang sebuah aplikasi Keamanan Data Dengan Metode End Of File (EOF) dan Algoritma MD5 dengan tampilan yang user *friendly*?.

I.2.3. Batasan Masalah

Agar penelitian yang dilakukan lebih terarah dan tidak menyimpang, maka perlu dibuat batasan masalah yaitu :

1. Teknik *steganografi* yang digunakan hanya dapat menyimpan file rahasia berupa teks.
2. Metode *steganografi* yang digunakan adalah metode *EOF (End Of File)* dan Kriptografi algoritma MD5.
3. Format audio yang digunakan untuk menampung pesan rahasia adalah berformat *.MP3 dan *.WAV.
4. Format video yang dihasilkan dari program *stegaqnografi* ini adalah berformat *.MP3 dan *.WAV.
5. Bahasa pemrograman yang digunakan VB.net 2010.

I.3. Tujuan dan Manfaat

I.3.1. Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah :

1. Untuk membuat suatu perangkat lunak yang dapat menyembunyikan dan melindungi keamanan teks yang disisipkan kedalam audio.
2. Untuk manipulasi audio yang didalamnya terdapat file teks sehingga file tersebut tidak dapat diketahui keberadaannya dan secara kasat mata tidak terjadi perubahannya pada gambar hasil manipulasi.
3. Untuk memberikan informasi bagaimana teknik steganografi metode *EOF* (*End Of File*) dan algoritma MD5 dapat diterapkan dalam auido.

4. Memberikan kemudahan kepada pengguna aplikasi dalam enkripsi dan dekripsi teks.

I.3.2 Manfaat Penelitian

Adapun maanfaat dari penelitian ini adalah :

1. Ada pengetahuan baru tentang algoritma MD5 pada kriptografi dan metode *End Of File* pada steganografi.
2. Menjaga kerahasiaan file teks yang berada didalam audio dengan menggunakan teknik steganografi.
3. Agar pengguna dapat mengetahui keamanan teks dengan cara menggabungkan kriptografi (algoritma MD5) dan steganografi (metode End Of File).

I.4. Metodelogi Penelitian

Metode merupakan suatu cara atau teknik yang sistematik untuk mengerjakan suatu kasus. Untuk itu penulis menggunakan beberapa cara untuk memperolehnya, diantaranya :

1. Implementasi dan Verifikasi

Tahapan implementasi yang penulis lakukan terhadap perancangan aplikasi kemanan data menggunakan metode EOF dan algoritma MD5:

a. Melakukan implementasi desain form

Pada tahap ini, penulis melakukan implementasi desain form dengan cara membuat form – form sesuai dengan desain yang dirancang pada bahasa pemrograman VB.net 2010.

b. Melakukan coding program

Pada tahap ini, penulis menuliskan coding – coding yang dibutuhkan agar dapat melakukan enkripsi terhadap data teks kedalam audio sesuai dengan kebutuhan.

c. Melakukan pengujian aplikasi

Pada tahap ini, penulis melakukan pengujian pada setiap form yang dihasilkan. Pengujian dilakukan untuk mengetahui apakah ada kesalahan (error) pada setiap form untuk melakukan perbaikan.

2. Validasi

Selanjutnya dilakukan pengujian aplikasi secara menyeluruh, meliputi pengujian penyisipan data teks yang akan disisipkan ke dalam audio dan pengekstrakan data yang akan dibaca. Pengujian aplikasi akan dilakukan secara langsung untuk memastikan semua fitur berjalan dengan baik.

I.5. Keaslian Penelitian

Setiap penelitian yang dilakukan memiliki bukti keaslian, dimana keaslian tersebut juga dibandingkan dengan penelitian-penelitian yang lainnya. Penelitian pertama diangkat oleh Gede Wisnu Baudhayana dari Universitas Udayana Bali dengan judul ” Implementasi Algoritma Kriptografi AES 256 dan Metode Steganografi LSB pada Gambar Bitmap”. Kemudian penelitian yang kedua oleh Dal Fendri dari STMIK Budidarma Medan dengan judul “Perancangan Aplikasi Penyembunyian Teks Pada Citra Terkompresi Menggunakan Metode Spread Spectrum”. Untuk lebih jelasnya perbandingan-perbandingan tersebut dapat dilihat pada tabel I.1 sebagai berikut.

Tabel I.1. Keaslian Penelitian

No	Peneliti	Judul	Hasil	Perbedaan
1	Gede Wisnu Baudhayana (2015)	Implementasi Algoritma Kriptografi AES 256 dan Metode Steganografi LSB Pada Gambar Bitmap	Metode steganografi dengan algoritma *list significant bit (lsb)* dan algoritma AES menggunakan gambar. Penyisipan hanya berisikan teks dengan kapasitas gambar.	Pengamanan citra yang dilakukan merupakan pengamanan yang berbasis desktop dengan menggunakan metode End Of File dan algoritma MD5 pada Audio.
2	Dal Fendri (2014)	Perancangan Aplikasi Penyembunyian Teks Pada Citra Terkompresi Menggunakan Metode Spread Spectrum	hasil pengujian dan analisis pengamanan teks dengan penyisipan menggunakan metode *spread spectrum* hanya menggunakan teks.	Dalam penelitian yang akan dilakukan dengan menggunakan metode end of file dan algoritma MD5 teknik penyisipan yang terjadi dilakukan dengan Teknik penambahan besar kapasitas .

I.6. Sistematika Penulisan

Adapun sistematika penulisan skripsi ini secara garis besar terbagi dalam 5 (lima), yaitu :

BAB I : PENDAHULUAN

Dalam bab ini menerangkan latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metode penelitian, dan sistematika.

BAB II : LANDASAN TEORI

Pada bab ini diuraikan landasan teori tentang segala hal yang memiliki hubungan terhadap masalah sesuai dengan judul yang dibuat.

BAB III : ANALISIS DAN PERANCANGAN

Dalam bab ini penulis membahas tentang pembuatan Aplikasi Keamanan Data Dengan Metode End Of File (EOF) dan Algoritma MD5, gambaran umum rancangan aplikasi Penyisipan teks kedalam audio, perancangan dan*user interface* aplikasi tersebut.

BAB IV : PEMBAHASAN DAN IMPLEMENTASI

Dalam bab ini penulis akan melakukan uji coba terhadap aplikasi yang dikembangkan, memastikan aplikasi dapat berjalan dengan baik, mempersiapkan *hardware/software* yang dibutuhkan untuk melakukan uji coba, serta menentukan kelebihan dan kekurangan dari aplikasi.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan penelitian dan saran dari penulis sebagai perbaikan dimasa yang akan datang.