BAB I
PENDAHULUAN

1.1 Latar Belakang

Komunikasi sudah menjadi bagian dalam kehidupan manusia. Terutama pada era informasi seperti sekarang dimana komunikasi menjadi hal yang sangat krusial. Dalam berkomunikasi, ada kalanya informasi yang dipertukarkan bersifat penting dan rahasia dimana informasi tidak boleh diketahui oleh pihak yang tidak berkepentingan. Oleh karena itu, masalah keamanan data sebagai komponen utama informasi merupakan faktor yang perlu diperhatikan dalam berkomunikasi. Untuk menangani masalah tersebut, dibutuhkan pengamanan data yang dapat melindungi data tersebut dari pihak yang tidak berkepentingan.

Kriptografi dan steganografi merupakan teknik yang dikembangkan untuk meningkatkan keamanan data. Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan informasi pada pesan dengan cara menyandikan pesan tersebut sehingga tidak dapat dimengerti lagi artinya [FIR-11]. Namun metode ini sering menimbulkan kecurigaan karena setiap orang mempunyai kesadaran bahwa pesan yang sulit dimengerti menunjukkan bahwa pesan itu telah mengalami suatu pengolahan dan mengandung suatu informasi yang penting.

Steganografi muncul untuk mengatasi kekurangan yang ada pada kriptografi. Prinsip steganografi adalah menyembunyikan pesan rahasia di dalam sebuah media dengan harapan bahwa pihak luar tidak menyadari atau mencurigai adanya pesan rahasia yang terkandung di dalamnya [HER-09]. Steganografi membutuhkan dua properti, yaitu pesan rahasia yang akan disembunyikan dan media penampung.

Penggabungan metode kriptografi dan steganografi menurut Elfirman [ELF-10] merupakan cara baru untuk memenuhi kebutuhan substansial akan kerahasiaan informasi. Sedangkan pada penelitian Kalangi [KAL-10], kriptografi digunakan untuk meningkatkan keamanan data pada steganografi. Pada penelitian tersebut, terlebih dahulu dilakukan enkripsi pada pesan sebelum disembunyikan pada berkas media penampung. Tujuan enkripsi tersebut adalah untuk menjaga

kerahasiaan informasi pada pesan tersebut. Meskipun keberadaan pesan pada media penampung dapat dideteksi, namun kerahasiaan informasi tetap terjaga.

Salah satu algoritma kriptografi yang sering digunakan untuk melakukan enkripsi adalah RSA [WIB-09]. RSA merupakan algoritma asimetris yang berarti memiliki dua kunci, yaitu kunci publik untuk melakukan proses enkripsi dan kunci pribadi untuk proses dekripsi. Algoritma RSA masih dianggap aman karena semakin panjang kunci yang digunakan, semakin sulit untuk dipecahkan karena sulitnya memecahkan pemfaktoran bilangan prima dari suatu bilangan yang sangat besar. Pada percobaan yang dilakukan pada tahun 1999, algoritma RSA dengan panjang kunci 512 bit membutuhkan waktu selama tujuh bulan untku dipecahkan. Pada ini saat dianjurkan untuk menggunakan algoritma RSA dengan panjang kunci 1024 bit untuk keamanan jangka panjang pada informasi yang memiliki kerahasiaan tinggi.

Audio steganografi merupakan perkembangan ilmu steganografi dimana media penampung yang digunakan merupakan berkas suara (audio) [KAL-10]. Pada steganografi audio mengenal sebuah teknik yang dinamakan teknik *Parity Coding*. Teknik *Parity Coding* menggunakan prinsip penggantian bit, yaitu mengganti bagian tertentu dari bit-bit berkas audio dengan pesan rahasia yang disembunyikan. Pada teknik *Parity Coding*, berkas audio sebagai media penampung dibagi menjadi menjadi beberapa region [HER-09]. Bit dari pesan rahasia akan disembunyikan secara merata pada setiap region dimana penyisipan tersebut bergantung pada nilai *Parity Bit* pada tiap region.

Saragih [SAR-06] melakukan penelitian mengenai perbandingan metode *Parity Coding* dengan metode *Spread Spectrum* pada audio steganografi. Pada penelitian tersebut pesan rahasia yang akan disembunyikan berupa berkas teks, sedangkan media penampung yang digunakan berupa berkas audio dengan format WAV. Saragih menguji kualitas audio yang telah disisipi pesan menggunakan parameter SNR (*Signal to Noise Ratio*). Penelitian tersebut menunjukkan metode parity coding memiliki nilai SNR yang baik.

Pada skripsi ini, media penampung yang akan digunakan adalah berkas audio. Penggunaan berkas audio dikarenakan berkas audio memiliki kapasitas yang lebih besar dibandingkan berkas teks maupun citra dan tidak terlalu rumit

dibandingkan berkas video [HER-09]. Salah satu format audio yang popular adalah MP3. MP3 merupakan salah satu format audio terkompresi yang memanfaatkan kelemahan pendengaran manusia. Walaupun ada banyak format audio terkompresi yang lebih unggul dibanding format MP3, format MP3 lebih banyak digunakan oleh sebagian besar orang. Oleh karena itu, format MP3 cocok digunakan sebagai media penampung karena format yang popular tidak menimbulkan kecurigaan berlebih.

Pada skripsi ini akan dilakukan penyembunyian pesan rahasia berupa berkas teks ke dalam media penampung berupa berkas audio dengan format MP3 menggunakan metode *Parity Coding*. Sebelum disembunyikan ke dalam berkas MP3, berkas teks akan dienkripsi dengan algoritma kriptografi RSA. Melalui penelitian ini diharapkan metode *Parity Coding* dapat menyembunyikan pesan rahasia dengan baik sehingga dapat memberikan tingkat keamanan yang baik pada pesan rahasia.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, dapat dirumuskan masalah-masalah sebagai berikut :

1. Bagaimana menerapkan metode *Parity Coding* untuk menyembunyikan berkas berupa teks terenkripsi dengan algoritma RSA ke dalam berkas audio MP3.
2. Bagaimana tingkat perubahan kualitas berkas MP3 yang diukur dengan menghitung nilai PSNR (*Peak Signal to Noise Ratio*) setelah dilakukan proses penyembunyian pesan.
3. Bagaimana ketahanan steganografi *Parity Coding* terhadap terhadap manipulasi berupa operasi penambahan derau *gaussian*

1.3 Batasan Masalah

Batasan ruang lingkup masalah yang didefinisikan dalam tugas akhir ini adalah :

1. Pesan rahasia yang akan disembunyikan adalah berkas bertipe teks (.txt).
2. Media penampung yang akan digunakan untuk menyembunyikan pesan rahasia adalah berkas audio berformat MP3.

3. Sebelum disembunyikan ke dalam media penampung, pesan terlebih dahulu akan dienkripsi menggunakan algoritma kriptografi RSA.
4. Pesan disembunyikan ke dalam media penampung menggunakan metode *Parity Coding*.
5. Parameter yang akan diuji adalah perubahan kualitas berkas MP3 setelah dilakukan proses penyembunyian pesan dan ketahanan steganografi *Parity Coding* terhadap terhadap manipulasi berupa operasi penambahan derau *gaussian.*
6. Kualitas berkas MP3 diukur dengan menghitung nilai PSNR (*Peak Signal to Noise Ratio*).
7. Panjang kunci yang digunakan pada algoritma kriptografi RSA maksimal 31 bit.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dari skripsi ini adalah :

1. Menerapkan metode *Parity Coding* untuk menyembunyikan berkas berupa teks terenkripsi dengan algoritma RSA ke dalam berkas audio MP3.
2. Mengatahui perubahan kualitas berkas berkas MP3 yang diukur dengan menghitung nilai PSNR (*Peak Signal to Noise Ratio*) setelah dilakukan proses penyembunyian pesan.
3. Mengetahui ketahanan steganografi *Parity Coding* terhadap manipulasi berupa operasi penambahan derau *gaussian.*

1.5 Manfaat Penelitian

Manfaat yang didapat dari penulisan skripsi yaitu tersedianya perangkat lunak yang dapat memberikan jaminan terhadap aspek kerahasiaan dan integritas data pada pengamanan pesan rahasia ke dalam berkas audio MP3 dengan menerapkan metode *Parity Coding*.

1.6 Sistematika Penulisan

Skripsi ini disusun berdasarkan sistematika penulisan sebagai berikut:

1. BAB I PENDAHULUAN

Berisi latar belakang masalah, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian serta sistematika penulisan skripsi.

2. BAB II TINJAUAN PUSTAKA

   Menjelaskan teori-teori yang berhubungan dengan Steganogarfi dan Kriptografi

3. BAB III METODOLOGI DAN PERANCANGAN SISTEM

   Pada bab ini akan dijelaskan mengenai metode-metode yang digunakan dan tahapan-tahapan teknik steganografi dan kriptografi.

4. BAB IV HASIL DAN PEMBAHASAN

   Dalam bab ini akan dijelaskan mengenai implementasi program, pengujian dan analisa hasil penelitian.

5. BAB V KESIMPULAN DAN SARAN

   Bab ini berisi kesimpulan dari seluruh rangkaian penelitian serta saran kemungkinan pengembangan.