BAB I

PENDAHULUAN

1.1 Latar Belakang

Komunikasi merupakan hal penting yang dilakukan bagi manusia, dapat diartikan sebagai sarana bertukar pikiran dan informasi. Saat ini perkembangan Teknologi Informasi (TI) berkembang dengan pesat, dan memberikan kemudahan bagi manusia dalam melakukan aktivitasnya, salah satunya digunakan untuk berkomunikasi dengan cara bertukar informasi dalam bentuk file dari satu tempat ke tempat lain (Singh *et al*, 2013). Informasi yang ditukar dapat bermacam-macam jenis seperti teks, gambar, video dan *audio* (Dianty, 2014). Diantara data informasi yang dikirim ada yang bersifat rahasia sehingga tidak boleh diakses oleh pihak yang tidak berwenang dan harus dijaga kerahasiaannya (Joseph dan Sundaram, 2011).

Pesan rahasia merupakan sebuah informasi yang hanya boleh di konsumsi oleh pihak-pihak tertentu, contohnya informasi didalam dunia intelijen seperti strategi militer dan strategi politik, *password* akun sosial media, kartu kredit, data-data negoisasi, rahasia medis dan data lainnya (Risandi. B, 2016). Dimana banyak orang yang ingin berusaha untuk mencari terlebih mengetahui isinya. Dengan pesatnya perkembangan teknologi informasi maka semakin berkembang pula teknik kejahatan sistem informasi yang berupa pencurian data maupun perusakan data oleh pihak yang tidak memiliki wewenang atas data tersebut (Handayani, 2016).

Maka dari itu pengguna teknologi mengembangkan ilmu pengamanan data yang disebut dengan kriptografi. Didalam ilmu kriptografi terdapat istilah steganografi yang berarti menyembunyikan keberadaan pesan (Sarmah dan Bajpai, 2010). Kriptografi dan Steganografi merupakan teknik yang paling banyak digunakan untuk mengatasi ancaman pencurian data dan juga cara terbaik untuk melindungi informasi dari pihak yang tidak diinginkan (Abdulzahra *et al*, 2014) (Morkel, 2005).

Untuk menyembunyikan pesan rahasia, steganografi membutuhkan dua properti yaitu wadah penampung dan pesan rahasia yang akan disembunyikan (Munir, 2004). Media penampung yang umum digunakan adalah gambar, *audio*, dan video (Februariyanti dan Wibisono, 2010). Pesan yang disembunyikan dapat berupa *text*, gambar, video atau pesan lainnya. Untuk jenis *audio* memiliki beberapa format seperti MP3, WAV, WMA, AAC dan sebagainya.

Saat ini MP3 atau yang bernama MPEG-1 atau MPEG-2 Audio Layer III merupakan sebuah format audio yang umum digunakan orang zaman sekarang sebagai sarana hiburan, walaupun sudah terdapat format audio yang lebih baik dari segi kualitas maupun kapasitas (Kumar & Goyal, 2014). Penggunaan MP3 yang tinggi ini dimanfaatkan para peneliti steganografi untuk menjadikannya sebagai media penampung pesan rahasia terlebih lagi kebanyakan orang hanya mengenal MP3 sebagai sebuah sarana hiburan semata. Maka dari itu penggunaan mp3 sebagai salah satu media steganografi merupakan langkah yang baik (Februariyanti dan Wibisono, 2010).

Berbagai metode steganografi berhasil diterapkan pada MP3, namun berbagai metode yang ada bergantung pada daya tampung *cover* MP3 yang digunakan. Sehingga jika kapasitas daya tampung *cover* file MP3 lebih kecil dari ukuran pesan rahasia, maka pengguna harus melakukan kompresi terhadap pesan rahasia atau mencari *cover* MP3 lain yang memiliki kapasitas daya tampung yang lebih besar. Beberapa metode juga bahkan mengorbankan kualitas audio dengan menimbulkan *noise* hasil dari perubahan nilai-nilai bit.

Untuk meningkatkan keamanan data, biasanya teknik kriptografi digabungkan dengan steganografi. Pada penelitian ini peneliti mencoba mengkombinasikan algoritma kriptografi RC6 dengan metode steganografi *Spread Spectrum*. Algoritma RC6 digunakan dalam proses enkripsi dan dekripsi pada pesan sebelum disisipkan ke dalam *audio* MP3, sedangkan metode *Spread Spectrum* digunakan dalam proses penyisipan pesan kedalam *cover audio* MP3. Fungsi enkripsi pada kriptografi ditujukan dapat meningkatkan keamanan steganografi.

Metode steganografi *spread spectrum* memiliki karakteristik yang sangat penting, yaitu ketahanannya dari gangguan, jika sinyal hilang sebagian informasi yang disampaikan masih dapat diketahui, tapi kelemahan dari metode ini adalah menimbulkan *noise* dan distorsi ke *file audio*. Namun ada beberapa kriteria yang menjadi penentu kesempurnaan steganografi diantaranya, *Imperceptible*; Keberadaan pesan rahasia tidak dapat dipersepsi. *Fidelity* ; Mutu *cover-object* tidak jauh berubah akibat penyembunyian pesan. *Recovery* ; Data yang disembunyikan harus dapat diungkap kembali. Untuk kriteria *robustness* tidak terlalu penting karena hal utama steganografi bertujuan untuk menghindari kecurigaan (orang tidak menyadari adanya pesan tersembunyi) (Munir, 2004).

Algoritma kriptografi *Advanced Encryption Standard* (AES) yang merupakan teknik yang paling kuat (Sarmah dan Bajpai, 2010). Salah satu kandidat dari AES adalah algoritma *Rivest Code 6* (RC6), RC6 atau *Rivest Code 6* adalah algoritma kriptografi *symmetric-key* yang merupakan perkembangan dari algoritma RC5, proses utama dalam algoritma ini adalah penjadwalan kunci, dan enkripsi, dekripsi. Berdasarkan proses-proses tersebutlah RC6 merupakan salah satu algoritma kriptografi yang paling canggih dan masih dapat dikatakan belum terpecahkan. Beberapa metode kriptanalisis yang sering digunakan, mulai dari yang kovensional sampai yang modern telah digunakan tetapi belum ada yang mampu memecahkannya dalam waktu yang singkat (Rudianto, 2008).

Di tahun 2015, penelitian dengan judul "*A Comparison of Symmetric Key Algorithms Des, Aes, Blowfish, Rc4, Rc6*" (Princy, P. 2015) menyatakan bahwa algoritma RC6 merupakan algoritma yang *flexible* dan memiliki keamanan yang baik.

Di tahun 2011, penelitian dengan judul *"Information hiding using audio steganography"* (Jayaram, P., Ranganatha, H. R., & Anupama, H. S. (2011) mengemukakan bahwa *Metode Spread Spectrum* mampu memberikan kontribusi kinerja yang lebih baik di beberapa area dibandingkan dengan pengkodean LSB, *coding fase*, dan teknik pengkodean paritas dalam hal ini menawarkan moderat tingkat transmisi data dan tingkat ketahanan yang tinggi terhadap teknik penghapusan.

Di tahun 2006, penelitian dengan judul "Metode Parity Coding Versus Metode Spread Spectrum Pada Audio Steganography" (Saragih, R. A, 2006) mengemukakan bahwa metode *spread spectrum*, semakin banyak data yang disisipkan, maka nilai SNR semakin kecil, tetapi keamanan data lebih terjamin karena menggunakan kode penyebar yang tidak diketahui oleh pihak lain.

Penelitian-penelitian diatas mengemukakan bahwa baik teknik kriptografi dan steganografi sama-sama memiliki kelemahan dan kelebihan. Kelemahan dalam kriptografi dapat menimbulkan kecurigaan terhadap pihak lain dikarenakan pesan yang telah di enkripsi akan bersifat tulisan acak. Dengan mengkombinasikan algoritma kriptografi RC6 dan metode steganografi *Spread Spectrum*, pesan yang telah di enkripsi menggunakan RC6 akan dilindungi keberadaanya menggunakan metode *Spread Spectrum*.

Dalam penelitian ini akan dirancang aplikasi yang akan meningkatkan keamanan sebuah informasi rahasia, aplikasi yang akan dirancang menggunakan *audio* format MP3 sebagai media *cover* atau wadah penampung pesan rahasia (*text*) dan akan diamankan dengan teknik kriptografi dan steganografi sehingga dapat meningkatkan keamanan data dan tidak akan menimbulkan kecurigaan terhadap pihak ketiga.

1.2 Rumusan Masalah

Berdasarkan latar belakang, maka masalah yang dapat dirumuskan adalah sebagai berikut :

1. Bagaimana mengkombinasikan algoritma RC6 dengan metode *spread spectrum* dalam penyisipan pesan pada MP3?
2. Bagaimana hasil pengujian kriteria steganografi (*imperceptible*, *fidelity*, dan *recovery)* menggunakan algoritma enkripsi RC6 dan metode *spread spectrum* setelah dilakukan penyisipan pesan (*text*) pada media *audio* MP3?

1.3 Tujuan Penelitian

Sesuai dengan permasalahan yang telah dirumuskan, maka tujuan yang ingin dicapai pada penelitian ini adalah :

1. Mengimplementasikan algoritma RC6 dan metode *spread spectrum* dalam melakukan penyisipan pesan pada media MP3.
2. Mendapatkan hasil analisis terhadap (*imperceptible, fidelity,* dan *recovery)* setelah dilakukan penyisipan pesan (*text*) pada media *audio* MP3 menggunakan algoritma enkripsi RC6 dan metode *spread spectrum.*
3. Mengetahui pengaruh kualitas MP3 seperti nilai MSE dan PSNR setelah dilakukan penyisipan pesan.

1.4 Batasan Masalah

Agar pembahasan penelitian ini lebih terarah maka diberikan batasan-batasan masalah sebagai berikut :

1. Pesan yang disisipkan berformat *text* dengan panjang maksimal 1000 karakter (“A - Z”, “a - z”, “0 - 9”) dan pesan tidak boleh kosong (0).
2. Tidak membahas kriteria steganografi *robustness* karena tujuan steganografi untuk menyembunyikan pesan agar tidak terlihat dari orang lain (lawan tidak menyadari keberadaan pesan tersembunyi).
3. Ukuran pesan rahasia tidak boleh lebih besar dari ukuran MP3.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat baik secara langsung maupun tidak langsung bagi pihak yang berkepentingan. Manfaat penelitian bagi peneliti adalah dapat memahami proses implementasi steganografi pada *audio* mp3 untuk penyisipan pesan *(text)* menggunakan algoritma RC6 dan *spread spectrum.*

1.6 Skematika Penulisan

Sistematika penulisan dalam penelitian ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab I ini membahas tentang latar belakang masalah mengapa memilih topik ini dan bagaimana aplikasi keamanan data menjadi solusi dari masalah tersebut, kemudian rumusan masalah apa saja, tujuan dari penelitian yang dilakukan, batasan masalah dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi materi-materi hasil *literature*, teori-teori tentang implementasi steganografi pada *audio* mp3 untuk penyisipan pesan (*text)* menggunakan algoritma rc6 dan *spread spectrum*, definisi kutipan dan istilah yang digunakan dalam penelitian.

BAB III METODE PENELITIAN

Bab ini berisi uraian deskripsi umum tentang metodologi yang digunakan dan desain rancangan penelitian, subjek penelitian, alat dan bahan yang dikaji dalam penelitian ini.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini menjelaskan deskripsi umum tentang analisis metode yang digunakan pada masalah-masalah yang berkaitan dengan implementasi steganografi pada *audio* mp3 untuk penyisipan pesan (*text)* menggunakan algoritma rc6 dan *spread spectrum.*

BAB V KESIMPULAN DAN SARAN

Berisi tentang kesimpulan dari hasil kajian penelitian ini secara ringkas dan memberikan saran-saran untuk perbaikan dan saran lanjutan dari penelitian ini.