BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan dan kerahasiaan merupakan aspek penting yang dibutuhkan dalam proses pertukaran pesan/informasi melalui jaringan/internet, karena turut berkembang pula kejahatan teknologi dengan berbagai teknik interupsi, penyadapan, modifikasi, maupun fabrikasi. Tanpa adanya jaminan keamanan, orang lain dapat dengan mudah mendapatkan data rahasia yang dikirimkan melalui jaringan/internet [10]. Data yang dilansir *Akamai Technologies*, salah satu perusahaan perantara penyedia konten web terbesar di dunia. Dalam laporan tersebut tertulis bahwa serangan yang berasal dari Indonesia pada kuartal I 2013 meningkat jadi 21%, melonjak dari kuartal sebelumnya yang hanya 0,7% [15].

Banyak cara untuk mengamankan informasi yang disimpan dalam media digital. Salah satu cara pengamanan informasi adalah kriptografi. Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari satu tempat ketempat lain [1]. Algoritma kriptografi pun mulai berubah menuju ke arah algoritma kriptografi yang lebih rumit dan kompleks. Beberapa algoritma yang menjadi kandidat *Advanced Encryption Standard* (AES) diantaranya *Rijndael, RC6, MARS, Twofish* dan *Serpent*. Walaupun akhirnya Rijndael yang menjadi AES, Algoritma MARS memiliki keunggulan yaitu dapat menerima kunci yang bervariasi antara 128 – 1248 bit. Sedangkan Rijndael hanya mampu menerima variasi panjang kunci 128 bit, 192 bit, dan 256 bit [4].

Sistem kriptografi ini dianggap terlalu *public* karena setiap orang mempunyai kesadaran bahwa pesan yang terlihat memang mengandung suatu kerahasiaan sehingga usaha untuk memecahkan kode enkripsi atau yang lebih dikenal dengan kriptanalisis tidak dapat dihindarkan. Pemerintah di beberapa negara juga telah menciptakan aturan untuk membatasi kekuatan sistem kriptografi, sehingga memaksa orang untuk mempelajari metode lain untuk melakukan pengiriman informasi rahasia [9].

Steganografi muncul dari kekurangan yang dirasakan ada pada kriptografi. Steganografi adalah seni dan ilmu untuk menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui [10]. Steganografi digital menggunakan media digital misalnya suara (*audio*), citra (*image*), teks (*txt*), dan *video.* Teknik steganografi pada berkas audio memanfaatkan kelemahan pendengaran manusia, karena kualitas suara antara berkas audio asli dengan berkas audio yang telah disisipkan pesan rahasia tidak jauh berbeda. Salah satu metode steganografi yang sering digunakan adalah *Least Significant Bit* (LSB). Metode ini diterapkan dengan mengganti bit-bit yang tidak terlalu berpengaruh dari berkas audio dengan bit-bit pesan [13].

Perusahaan-perusahaan bisnis juga telah mulai menyadari potensi steganografi dalam mengkomunikasikan rahasia-rahasia dagang atau informasi produk baru. Banyak kegiatan usaha yang memanfaatkan data untuk menghasilkan produk yang lebih baik, pemangkasan biaya produksi dan pengawasan risiko. Institusi pemerintah, pendidikan maupun organisasi *non-profit* juga membutuhkan data berkualitas tinggi dan aman untuk mengarahkan aktivitas operasional, taktikal dan strategis mereka. Penyembunyian informasi dalam sebuah audio digital memberikan efek mencurigakan yang lebih sedikit daripada komunikasi menggunakan arsip yang terenkripsi [9].

Oleh karena itu, pada Tugas akhir ini dilakukan suatu implementasi dengan melakukan kombinasi antara algoritma MARS pada kriptografi dan teknik steganografi dengan metode *Least Significant Bit* (LSB) untuk mendapatkan proteksi ganda yang lebih baik dalam menjaga keamanan dan kerahasiaan data, serta menyembunyikan data dalam sebuah *file* audio WAV guna melindungi keberadaan data rahasia.

1.2 Rumusan Masalah

Dalam penelitian ini akan dibahas permasalahan bagaimana implementasi teknik kriptografi algoritma MARS pada file teks dan steganografi metode *Least Significant Bit* (LSB) ke dalam *file wav* serta kombinasi antara keduanya.

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini mengimplementasikan teknik kriptografi algoritma MARS pada *file* teks dan steganografi metode *Least Significant Bit* (LSB) pada *file* audio dengan membangun perangkat lunak yang menggabungankan kedua teknik pengamanan data tersebut.

1.4 Manfaat Penelitian

1.4.1 Manfaat Ilmiah

Penelitian ini diharapkan dapat menambah khasanah keilmuan tentang pengamanan data dengan kriptografi dan steganografi sehingga diharapkan para Civitas akademis dan praktisi dapat mengetahui berbagai teknik enkripsi dan deskripsi yang dilakukan dalam melakukan pengamanan data digital.

1.4.2 Manfaat Praktis

Penelitian ini bermanfaat sebagai bahan pengaplikasian dalam teknik kriptografi dan steganografi, sehingga memudahkan para civitas akademis dalam proses penyembunyian pesan teks ke dalam *file* audio.

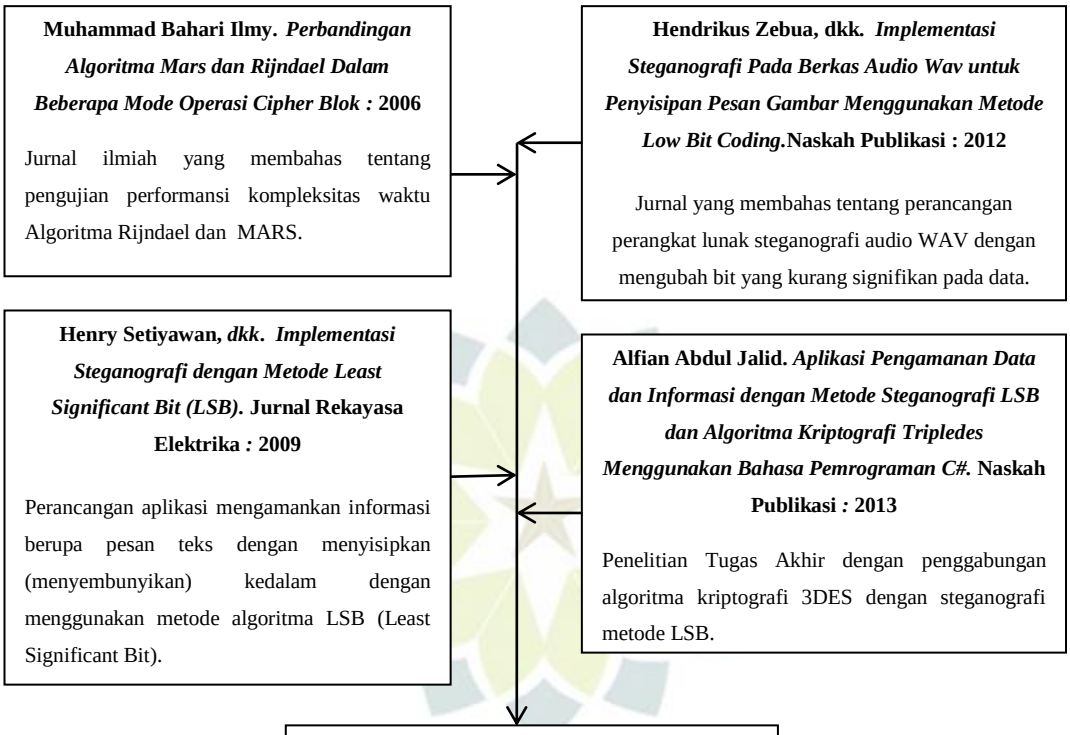
1.5 Batasan Masalah

Hal-hal yang akan dilakukan dalam Tugas akhir ini dibatasi pada pembatasan masalah yang akan dibahas, yaitu:

a. Enkripsi dan deskripsi *file* teks dilakukan dengan algoritma MARS.
b. Metode steganografi yang digunakan adalah metode *Least Significant Bit*.
c. Penyembunyian data rahasia melalui proses steganografi dengan menggunakan berkas WAV sebagai berkas penampung.
d. Ukuran *file* yang dapat dijadikan sebagai media yaitu lebih dari atau sama dengan 1 KB (≥1 KB) dan maksimal 15 MB.
e. Ukuran *file* audio penampung harus lebih besar dari *file* teks.
f. Kombinasi algoritma MARS dengan metode *Least Significant Bit* (LSB) ini menggunakan software *NetBeans IDE 7.4*.
g. Bahasa pemrograman yang digunakan adalah bahasa *Java*.

1.6 Posisi Penelitian (*State of the Art*)

Posisi penelitian pada tugas akhir ini ditunjukkan pada Gambar 1.1.



Gambar 1.1 Posisi Penelitian (*State of the Art*)

Dalam penelitian yang ditulis oleh Muhammad Bahari Ilmy mengenai *Perbandingan Algoritma Mars dan Rijndael Dalam Beberapa Mode Operasi Cipher Blok* [4] diperoleh Algoritma MARS memiliki keunggulan yaitu dapat menerima kunci yang bervariasi antara 128 – 1248 bit. Pada Jurnal *Implementasi Steganografi dengan Metode Least Significant Bit (LSB)* [12] oleh Henry Setiyawan, dkk dan *Implementasi Steganografi Pada Berkas Audio Wav untuk Penyisipan Pesan Gambar Menggunakan Metode Low Bit Coding* [13] ditulis oleh Hendrikus Zebua, dkk dijelaskan bahwa steganografi dengan metode LSB lebih baik karena tidak mengubah ukuran *file* yang disisipi. Serta kombinasi kriptografi dan steganografi dijelaskan pada Naskah Publikasi *Aplikasi Pengamanan Data dan Informasi dengan Metode Steganografi LSB Dan Algoritma Kriptografi Tripledes Menggunakan Bahasa Pemrograman C#,* ditulis oleh Abdul Alfian [1].

1.7 Sistematika Penulisan

Penulisan Tugas akhir memiliki sistematika penulisan dengan jumlah 6 Bab dimana setiap bab mempunyai isi masing masing, berikut penjabaran isi setiap Bab.

- Bab 1 Pendahuluan

  Bab ini berisi latar belakang, perumusan masalah, tujuan penelitian, kegunaan penelitian, *state of the art*, batasan masalah, dan sistematika penulisan.
- Bab 2 Tinjauan Pustaka

  Bab ini membahas mengenai penjelasan secara umum tentang kriptografi, algoritma MARS, steganografi, bahasa pemrograman Java dan *file* WAV.
- Bab 3 Metodologi Penelitian

  Bab ini membahas mengenai identifikasi masalah, pengumpulan data, analisis kebutuhan, perencanaan dan pengambilan data, analisis data dan evaluasi.
- Bab 4 Perancangan dan Impelemtasi Sistem

  Bab ini berisi penjelasan tentang analisis perangkat lunak, metode yang digunakan untuk merancang perangkat lunak dan perancangan perangkat lunak serta implementasi sistem.
- Bab 5 Pengujian dan Analisis

Bab ini berisi tentang pengujian seperti proses enkripsi dan deskripsi algoritma MARS, penyembunyian data rahasia metode LSB, kombinasi kriptografi dengan steganografi dan analisis data hasil penelitian performansi dan kualitas.

- Bab 6 Penutup

  Bab ini berisi kesimpulan dan saran dari penelitian yang dilakukan.