BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Berdasarkan sejarah panjang mengenai metode kerahasiaan informasi, tujuan utama dari kegiatan tersebut adalah melindungi informasi agar tidak dapat dideteksi oleh pihak yang berkepentingan. Seiring perkembangan teknologi, metode steganografi digunakan pula untuk aktifitas-aktifitas pengabsahan sebuah data/pesan. Sistem kearsipan paling banyak menggunakan metode ini. Penggunaan steganografi merupakan teknologi yang sangat bermanfaat dalam pengamanan data/pesan. Steganografi berbeda dengan kriptografi atau metode keamanan informasi lainnya, steganografi yaitu menyembunyikan informasi atau pesan ke dalam media lain seperti citra digital, teks, suara, atau video sehingga tidak menimbulkan kecurigaan orang lain. Steganografi membutuhkan dua properti, yaitu informasi dan media penampung [1]. Media penampung yang banyak digunakan untuk menyembunyikan informasi yaitu citra digital. Penyisipan informasi pada media citra digital sebagai media penampung mempunyai kelebihan karna indra penglihatan manusia memiliki keterbatasan tersebut, manusia sulit membedakan citra digital yang asli dengan citra yang telah disisipi pesan rahasia.

Steganografi mempunyai banyak metode yang dapat digunakan, namun metode yang banyak digunakan saat ini masih mempunyai kekurangan dalam hal kualitas, kapasitas, dan ketahanan [2]. Metode-metode yang digunakan dalam

pembuatan steganografi mempunyai kriteria-kriteria yang kapasitas media penampung menyimpan informasi (*payload capacity*), kualitas media penampung yang telah disisipi pesan (*fidelity*), ketahanan terhadap manipulasi (*robustness*), dan tidak menimbulkan kecurigaan pada media penampung yang telah disisipi pesan (*unsusoicious file*) [3]. Kriteria-kriteria ini harus dipenuhi oleh metode yang digunakan dalam pembuatan steganografi, agar media yang menampung informasi tidak menimbulkan kecurigaan. Namun dari kriteria-kriteria tersebut, steganografi tidak memastikan keamanan terhadap informasi yang tersembunyi pada media penampung. Sehingga jika media penampung dapat diungkap oleh orang yang tidak bertanggung jawab, maka informasi yang tersembunyi akan langsung diketahui.

Metode *Least Significant Bit* (LSB) merupakan salah satu metode yang dapat digunakan dalam pembuatan steganografi. Metode tersebut yaitu merubah file gambar atau file sisipan ke dalam bentuk bit dan menyisipkan bit-bit dari file sisipan tersebut ke dalam bit-bit pada file gambar. Salah satu enkripsi yang dapat digunakan yaitu algoritma *Rivest, Shamir, Adleman* (RSA) adalah *blockcipherteks* yang dapat mengenkripsi dan dekripsi yaitu mengubah pesan asli (*plaintext)* menjadi pesan dalam bentuk tersandi *(ciphertext)*. Proses enkripsi akan menghasilkan data tersandi dan hanya dibuka atau dibaca oleh pihak penerima yang memiliki kunci privat (*private key)* sedangkan proses dekripsi adalah mengembalikan data tersandi menjadi bentuk data asli. Baik teknik kriptografi dan steganografi sama-sama memiliki kekurangan, oleh karna itu menggabungkan kedua teknik enkripsi ini dimaksud akan menambah tingkat keamanan pada saat

pertukaran data menyisipkan pesan bahkan untuk mengklaim autentufikasi dari suatu media citra digital yang dibuat.

Berdasarkan uraian tersebut, penulis ingin membuat aplikasi dan mengetahui tingkat keamanan dan kelebihan menggunakan LSB sehingga penulis mengangkat judul **"Implementasi Penyandian Dan Penyembunyian Pesan Pada Citra Menggunakan Algoritma RSA dan *Modified* LSB".**

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah maka rumusan yang akan dibahas pada tugas akhir ini adalah sebagai berikut :

1. Bagaimana melakukan proses *embedding* dan *extracting* dengan metode *modified LSB* terhadap pesan yang telah terenkripsi dengan algoritma RSA.
2. Bagaimana meningkatkan keamanan data menggunakan algoritma kriptografi kunci public RSA dan metode steganografi *modified LSB*.

1.3 Batasan Masalah

Untuk memfokuskan pengerjaan tugas akhir ini, penulis akan membatasi masalah, yaitu sebagai berikut :

1. Pesan yang disembunyikan ke dalam citra adalah *chipertext* yang berupa bilangan integer hasil perhitungan dari algoritma RSA.
2. Media untuk menyimpan pesan adalah citra digital format bitmap dan .png

3. Panjang pesan yang disisipkan harus lebih kecil atau sama dengan panjang segmen data induk citra.
4. Teknik steganografi yang digunakan merupakan salah satu metode subtitusi yaitu metode LSB yang telah dimodifikasi.
5. Pesan disisipkan ke dalam citra digital secara diagonal, dari diagonal kiri atas ke kanan bawah
6. Aplikasi yang dibangun hanya akan memproses penyembunyian pesan terenkripsi ke dalam media citra digital dan mengekstraksi kembali pesan yang disembunyikan.
7. Hal-hal yang akan diujiakn pada aplikasi yang dibangun yaitu :
   a. Keamanan pesan terhadap aplikasi *steganalysis* yaitu menggunakan *StegSpy 2.1*
   b. Kualitas citra yang telah disisipi pesan yang dinyatakan dalam PSNR
   c. Ketahanan terhadap manipulasi citra yang telah disisipi pesan
8. Aplikasi yang dibangun berupa desktop.
9. Untuk menghindari proses yang berulang dan *redundant* dalam penyembunyian bit *cipherteks*, pada penelitian ini komponen citra yang digunakan untuk menyembunyikan pesan adalah komponen warna merah.
10. Aplikasi dikembangkan dengan Matlab R2007b.

1.4 Maksud dan Tujuan Penelitian

Berdasarkan permasalahan yang diteliti, maka maksud dari penulisan tugas akhir ini adalah Untuk memenuhi salah satu syarat kelulusan Strata Satu di Sekolah Tinggi Manajemen Informatika dan Komputer Amikom Yogyakarta jurusan Teknik Informatika.

Adapun tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut :

1. Merancang sebuah aplikasi yang dapat mengenkripsi dan mendeskripsi teks menggunakan algoritma kriptografi RSA
2. Merancang Sebuah Aplikasi yang dapat menyisipkan dan mengekstrak *cipherteks* berupa blok-blok integer dalam media citra digital dengan format .bmp dan .png menggunakan algoritma *Modified* LSB.
3. Melakukan pengujian terhadap keamanan pesan menggunakan aplikasi *stegnalysis* yaitu *StegSpy 2.1*.
4. Untuk mengetahui kualitas citra yang telah disisipi pesan yang dinyatakan dalam PSNR, serta ketahanan terhadap manipulasi citra yang telah disisipi pesan.

1.5 Metode Penelitian

Metodologi penelitian yang akan digunakan adalah :

1. Studi Literatur

   Mempelajari literature tentang teori dasar mengenai kriptografi, jenis-jenis kriptografi, keunggulan kriptografi asimetris dibandingkan kriptografi simetris, memahami tentang algoritma RSA dan metode steganografi LSB,

dan semua teori yang berkaitan baik dari beberapa buku, jurnal, maupun penelitian terdahulu.

2. Analisi Data

   Pada tahap ini dilakukan analisis kebutuhan terhadap sistem berserta batasan-batasan yang diperlukan. Menganalisis algoritma kriptografi RSA, teknik enkripsi dan dekripsi pada RSA, serta menganalisis algoritma steganografi LSB, teknik penyisipan dan ekstraksi pesan pada LSB.

3. Perancangan Sistem

   Melakukan perancangan desain dalam bentuk *flowchart*, UML *(Unified Modelling Language)* diantara nya diagram *use case, sequence diagram, activity diagram dan class diagram* dan antar muka sistem untuk memudahkan proses implementasi pada tahap selanjutnya.

4. Implementasi Sistem

   Pada tahap ini dilakukan pembuatan sistem sesuai dengan analisis dan perancangan yang sudah didefinisikan sebelumnya. Implementasi sistem dilakukan dengan menggunakan bahasa pemrograman Matlab R2007b.

5. Pengujian Sistem

   Pengujian dilakukan terhadap keberhasilan proses kriptografi dan steganografi pada sistem, mencakup apakah implementasi telah sesuai dengan teori, apakah pesan yang diekstrak sesuai dengan pesan sebelum disisipkan, apakah pesan hasil deskripsi sesuai dengan plainteks semula, serta pengujian keamanan pesan, kualitas dan ketahanan citra yang telah disisipi pesan.

6. Dokumentasi Sistem

Melakukan pembuatan dokumentasi sistem melalui dari tahap awal hingga pengujian sistem, untuk selanjutnya dibuat dalam bentuk laporan penelitian (skripsi).

1.6 Sistematika Penulisan

Sistematika penulisan laporan penelitian ini dibagi menjadi 5 bab, yaitu sebagai berikut :

BAB 1 PENDAHULUAN

Berisikan penjelasan tentang konsep dasar penyusunan tugas akhir, yaitu mengenai latar belakang pemilihan judul, rumusan masalah, batasan masalah, tujuan penelitian, metode penelitian, dan sistematika penulisan.

BAB 2 LANDASAN TEORI

Bab ini akan membahas tinjauan penelitian yang relevan, dasar teori yang menunjang penulisan tugas akhir, berkaitan mengenai kriptografi, steganografi, proses enkripsi dan deskripsi dengan algoritma RSA, serta proses penyisipan dan ekstraksi pesan dengan menggunakan metode *modified LSB*.

BAB 3 METODE PENELITIAN

Bab ini membahas tentang gambaran umum mengenai aplikasi yang dibuat dan perancangan sistem dengan menggunakan metode RSA dan *modified LSB*.

BAB 4 IMPLEMENTASI DAN PEMBAHASAN

Pada bab ini akan menjelaskan implementasi metode RSA dan *modified LSB* yang digunakanm serta pengujian akan keberhasilan terhadap sistem yang telah dibangun.

BAB 5 KESIMPULAN DAN SARAN

Bab ini akan memuat kesimpulan isi dari keseluruhan uraian bab-bab sebelumnya dan saran-saran dari hasil yang diperoleh yang diharapkan dapat bermanfaat untuk pengembangan selanjutnya.