BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi kian berkembang pesat, semakin banyak orang yang mengakses internet. Beragam informasi dipertukarkan melalui internet,mulai dari informasi yang bersifat umum hingga informasi yang bersifat sangat rahasia. Seiring dengan perkembangan teknologi saat ini, pertukaran informasi berlangsung cepat dan mudah. Dalam pertukaran informasi yang cepat dan akurat saat ini, keamanan data sangat penting. Keamanan data perlu mendapat perhatian, karena banyak sekali informasi yang dipertukarkan sifatnya rahasia dan harus dilindungi agar tidak disalahgunakan.

Beberapa teknik digunakan untuk melindungi informasi yang dirahasiakan dari orang yang tidak berhak. Diantaranya dengan menggunakan steganografi dan kriptografi. Dengan steganografi, pesan rahasia dapat disisipkan dalam media yang akan dikirimkan. Sedangkan dengan kriptografi, pesan rahasia dapat diacak sehingga tidak diketahui isinya oleh orang yang tidak berhak.

Teknik steganografi yang dapat digunakan salah satunya adalah dengan menggunakan algoritma Gifshuffle. Steganografi dengan algoritma ini digunakan untuk menyisipkan pesan dalam file citra berformat GIF. File dengan format ini sering dijumpai di internet, dan berukuran relative kecil sehingga diharapkan tidak terlalu menarik perhatian dan aman sebagai media penyimpan pesan rahasia. Selain itu, file GIF bersifat *loseless*, citra GIF tidak kehilangan kualitas ketika dikompresi, sehingga sesuai untuk menjadi media steganografi. Sesuai namanya, GifShuffle akan melakukan'*shuffle*' terhadap 256 palet warna berkas GIF dengan melakukan penukaran posisi palet warna tersebut. Algoritma Gifshuffle memanfaatkan header file GIF sebagai media penyimpan pesan.

Adapun untuk kriptografi salah satu algoritmanya adalah TEA (*Tiny Encryoription Algorithm*). Algoritma TEA merupakan algoritma penyandian yang dirancang sederhana untuk penggunaan memori seminimal mungkin dan kecepatan proses yang maksimal. Algoritma TEA tidak memerlukan tabel seperti yang digunakan dalam kriptografi dengan algoritma DES. Sistem penyandian TEA menggunakan proses *feistel network* dengan menambahkan fungsi matematika berupa penambahan dan pengurangan sebagai operator pembalik selain XOR. Hal ini dimaksudkan untuk menciptakan sifat non-linearitas. Pergeseran ke dua arah (kiri dan kanan) menyebabkan semua bit kunci dan data bercampur secara berulang. Algoritma TEA merupakan algoritma *block chiper* dengan kunci simetris. Pengirim dan penerima pesan harus mengetahui kunci pesan yang sama persis agar dapat digunakan untuk membaca pesan rahasia.

Dalam Tugas Akhir ini, akan dilakukan sebuah simulasi yang menggabungkan dua teknik pengamanan data yaitu steganografi dan kriptografi. Akan digunakan steganografi dengan algoritma GifShuffle dan kriptografi algoritma TEA *(Tiny Encryption Algorithm).* Orang yang berhasil mendapatkan pesan rahasia dalam citra hasil steganografi, tidak dapat langsung mengetahui isi pesan rahasia yang tersembunyi di dalamnya, karena masih harus menyandikan pesan yang terenkripsi dengan menggunakan kunci yang hanya diketahui oleh pengirim dan penerima yang sah. Dengan menggabungkan kedua metode ini diharapkan dapat menghasilkan tingkat keamanan data yang tinggi.

1.2 Rumusan Masalah

Rumusan masalah Tugas Akhir ini adalah sebagai berikut :

1. Bagaimana membuat aplikasi untuk pengamanan data dengan menggabungkan steganografi dan kriptografi.
2. Bagaimana menerapkan steganografi algoritma GifShuffle dan kriptografi dengan algoritma TEA (*Tiny Encryption Algorithm*) untuk pengamanan data.
3. Bagaimana menganalisa pengaruh citra digital terhadap sistem.

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian tugas akhir ini adalah:

1. Memberikan informasi bagaimana teknik steganografi dan kriptografi digunakan pada file citra digital.
2. Membuat aplikasi yang menggabungkan steganografi algoritma GifShuffle dengan kriptografi algoritma TEA (*Tiny Encryption Algorithm*) untuk pengamanan data.
3. Menganalisa pengaruh citra digital terhadap sistem dengan menggunakan parameter pengujian sistem (MSE, PSNR)

1.4 Batasan Masalah

Untuk mendapatkan hasil yang spesifik sesuai dengan yang diinginkan, dalam penelitian kali ini ditentukan batasan masalah sebagai berikut:

1. Input yang digunakan dalam aplikasi Tugas Akhir ini adalah file citra RGB tidak bergerak (non animasi) dengan format *.gif
2. Ukuran file citra yang digunakan 480x320, 800x600,dan 1366x768.
3. Data yang disisipkan berupa file teks dengan format *.txt
4. Input berupa teks dikodekan dengan kode ASCII-8 (unicode)
5. Simulasi menggunakan Matlab 7.8.0 (R2009a).
6. Noise yang digunakan untuk pengambilan data adalah *Gaussian* dan *Salt&Pepper* dengan parameter *noise* 0.000001, 0.00001, 0.0001, 0.001, 0.01, 0.1

1.5 Metodologi Penelitian

Penelitian ini akan dilakukan dalam beberapa tahap, yaitu:

1. Studi literatur dan diskusi. Pada tahap ini dilakukan pengumpulan literatur-literatur berupa jurnal, artikel, buku referensi, dan sumber lain untuk memperdalam konsep serta berdiskusi dengan pihak-pihak yang berkompeten.
2. Tahap perancangan, pada tahap ini dilakukan perancangan sistem menggunakan software Matlab berdasarkan hasil pada tahap sebelumnya.
3. Tahap implementasi, yaitu pembuatan perangkat lunak berupa GUI pada Matlab yang kemudian akan dimasukkan program yang sesuai dengan system yang sudah dirancang.
4. Tahap pengujian sistem dan analisis, pada tahap ini sistem yang sudah dirancang akan diuji hasilnya dengan menggunakan citra dengan kondisi yang berbeda-beda. Pada tahap ini, hasil yang didapat dicatat dan dianalisa untuk melihat pengaruhnya pada citra digital
5. Pengambilan kesimpulan dan penyusunan laporan tugas akhir.

1.6 Sistematika Penulisan

Tugas Akhir ini disusun berdasarkan sistematika sebagai berikut :

1 BAB I. PENDAHULUAN

Pada bab ini dibahas mengenai latar belakang penelitian, perumusan masalah, tujuan penelitian, batasan masalah, metodologi penelitian, dan sistematika penulisan pada tugas akhir ini.

2 BAB II. DASAR TEORI

Pada bab ini dipaparkan berbagai dasar teori yang mendukung dan mendasari penulisan tugas akhir ini yaitu mengenai keamanan data, citra digital, file citra format GIF, steganografi algoritma GifShuffle dan kriptografi algoritma TEA (*Tiny Encryption Algorithm*).

3 BAB III. PERANCANGAN DAN IMPLEMENTASI SISTEM

Pada bab ini dijelaskan mengenai proses perancangan dan implementasi sistem pengamanan data dengan menggunakan steganografi algoritma Gifshuffle dan kriptografi algoritma TEA(*Tiny Encryption Algorithm*).

4 BAB IV. PENGUJIAN SISTEM DAN ANALISIS

Pada bab ini dilakukan pengujian sistem dan menganalisa hasil yang diperoleh dari tahap perancangan dan implementasi yang telah dilakukan.

5 BAB V. PENUTUP

Pada bab ini berisi kesimpulan dan saran untuk pengembangan penelitian selanjutnya.