BAB I
PENDAHULUAN

1.1 Latar Belakang

Semakin berkembangnya teknologi komputer, komunikasi antar pengguna komputer menjadi mudah dan cepat. Dalam komunikasi, keamanan data antar pengguna komputer menjadi aspek penting dari suatu sistem informasi. Begitu banyak pengguna seperti departemen pertahanan, perusahaan atau individu–individu tidak ingin informasi yang disampaikannya diketahui oleh orang lain. Informasi yang bersifat rahasia tersebut perlu dijaga keamanannya agar tidak dapat dimaanfaatkan oleh pihak ketiga yang dapat mengakibatkan suatu perusahaan atau individu mendapatkan saingan atau mengalami penurunan pendapatan. Oleh karena itu untuk menjaga keamanan data dalam komunikasi dapat dilakukan dengan cara mengacak pesan dan menyembunyikan pesan ke dalam suatu media. Penyembunyian pesan akan membuat pesan tidak menarik perhatian, akan tetapi dari segi keamaan masih mudah bagi pihak ketiga untuk mendapatkan pesan asli. Pengacakan isi pesan sebelum proses penyembunyian akan memberikan keamaan jika pesan yang berada dalam suatu media dapat dikeluarkan.

Metode untuk menyembunyikan pesan ke dalam citra digital dikenal dengan istilah steganografi. Teknik steganografi menyembunyikan pesan atau data pada suatu tempat yang disebut *carrier file*. Keuntungan steganografi yaitu pesan yang dikirim tidak menarik perhatian sehingga *carrier file* yang membawa pesan tidak menimbulkan kecurigaan pihak ketiga. *Carrier file* bisa menggunakan format JPEG,BMP,GIF,WAV,AVI, dan lain lain.

Graphics Interchange Format (GIF) adalah format gambar yang diperkenalkan oleh CompuServe pada tahun 1987. Format gambar GIF memiliki dua versi, yaitu GIF87a dan GIF89a. GIF87a adalah versi pertama dari format GIF yang berupa gambar statis. GIF89a dapat menampilkan gambar bergerak (animasi) dan latar belakang transparan. Salah satu algoritma steganografi yang memanfaatkan GIF sebagai *carrier file* adalah GifShuffle [PEN-05].

Gifshuflle merupakan sebuah algoritma untuk menyisipkan pesan ke dalam citra berformat GIF. Cara kerjanya adalah dengan mengubah susunan palet warna pada citra tersebut di mana setiap perubahan berkorespondensi dengan sebuah karakter yang dideklarasikan sebelumnya. Algoritma ini memiliki kelemahan yaitu citra yang telah disisipi pesan tidak tahan terhadap operasi citra, pesan tidak dapat diekstraksi [PEN-05]. Penulis menggunakan algoritma GifShuffle karena algoritma ini mudah untuk diimplementasikan dan menggunakan media yang berukuran kecil. Untuk lebih mengamankan pesan maka dilakukan kriptografi terhadap pesan terlebih dahulu.

Kriptografi didefinisikan sebagai ilmu yang yang mempelajari teknik–teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta otentikasi data. Teknik kriptografi menjaga agar pesan atau data tetap aman pada saat dikirimkan, dari pengirim ke penerima. Terdapat dua proses penting di dalam kriptografi yang berperan dalam merahasiakan suatu informasi yaitu enkripsi dan dekripsi. Hasil dari proses enkripsi disebut *cipher*. *Cipher* hanya akan dapat dibaca dengan menggunakan kunci yang sama.

Pada umumnya terdapat dua teknik yang digunakan dalam kriptografi, yaitu kunci simetris dan kunci asimetris (*public-key*). Metode enkripsi yang lebih umum digunakan adalah menggunakan kunci simetris karena sangat mudah dan cepat. Kunci diletakkan terpisah dari pesan yang terenkripsi dan dikirimkan secara rahasia. Beberapa model enkripsi yang termasuk kunci simetris antara lain Simple Substituton Cipher, DES, 3DES, Rivest Code (RC2), Rivest Code 4 (RC4), IDEA, Skipjack, Caesar Cipher, Gost Block Cipher, Letter Map, Transposition Cipher, Blowfish, Vigenere Cipher, Enigma Cipher, dan lain-lain.

Algoritma *Data Encryption Standard* (DES) menggunakan kunci berukuran 56-bit untuk melakukan enkripsi dan dekripsi suatu informasi. Algoritma DES tidak memiliki tingkat keamanan yang cukup baik karena untuk mencari kunci dari DES dapat dengan menggunakan metode *brute force attack* hanya dalam waktu yang relatif cepat. Algoritma DES dikembangkan menjadi algoritma 3DES untuk meningkatkan kemanaan pesan dari *brute force attack*.

Perbedaan DES dengan 3DES terletak pada panjangnya kunci yang digunakan. 3DES menggunakan 3 kunci yang panjangnya 168-bit. Tingkat kerahasiaan algoritma 3DES terletak pada panjangnya kunci yang digunakan, maka penggunaan algoritma 3DES lebih aman dibandingkan dengan algoritma DES.

3DES terbagi menjadi dua variasi, yaitu 2TDES dan 3TDES. Jenis 2TDES hanya menggunakan 2 buah kunci, sementara 3TDES menggunakan 3 buah kunci. 2TDES memiliki kunci berukuran 112- bit (2 kali lipat DES), dan 3TDES memiliki kunci berukuran 168-bit (3 kali lipat DES) [DHI-00].

Implementasi algoritma 3DES telah digunakan pada penelitian sebelumnya oleh Prasun Ghosal, Malabika Biswas, dan Manish Biswas pada tahun 2010 tentang *Field-Programmable Gate Array* (FPGA). Implementasi 3DES pada kombinasi *Very High Speed Integrated Circuit Hardware Description Language* dan FPGA menghasilkan kecepatan yang tinggi pada kinerja perangkat keras FPGA [GHO-10].

Percobaan untuk mendapatkan *plaintext* dengan mencoba kunci satu persatu harus dicoba sebanyak $3{,}741 \times 10^{50}$ kali. Kecepatan proses enkripsi dan dekripsi algoritma 3DES pada setiap pertambahan ukuran file input sebesar 1KB adalah sama. Pada proses enkripsi kecepatan rata-ratanya adalah 0.03024 KB/detik dan pada proses dekripsi kecapatan rata-ratanya adalah 0.05908 KB/detik [HID-08].

Berdasarkan beberapa hal yang mendasari Algoritma 3DES ini, maka penulis menggunakan algoritma 3DES pada tugas akhir ini untuk melakukan enkripsi dan dekripsi pesan.

1.2 Rumusan Masalah

Berdasarkan pada latar belakang permasalahan yang ada, maka rumusan masalah dari penelitian ini adalah:

1. Bagaimana menerapkan teknik steganografi *chipertext* 3DES pada citra digital menggunakan metode *GifShuffle*.
2. Bagaimana nilai *avalanche effect* algoritma 3DES.
3. Bagaimana nilai PSNR citra digital hasil steganografi.

1.3 Batasan Masalah

Batasan masalah bertujuan agar penelitian yang dilakukan tetap mengacu pada topik penelitian. Batasan masalah dalam penelitian ini adalah:

1. Algoritma 3DES yang digunakan adalah 3TDES.
2. Metode steganografi yang digunakan adalah GifShuffle.
3. Pesan atau data yang akan disembunyikan berupa file teks yang berupa karakter ASCII dengan panjang maksimal 208 karakter.
4. Kunci yang digunakan berupa karakter ASCII.
5. Citra yang digunakan adalah GIF yang tidak bergerak.
6. Citra yang telah digunakan untuk menyembunyikan teks tidak dilakukan operasi citra.

1.4 Tujuan Penelitian

Berdasarkan pada masalah yang telah diidentifikasikan, maka tujuan yang hendak dicapai skripsi ini adalah:

1. Mengimplementasikan teknik steganografi *chipertext* 3DES pada citra digital menggunakan metode *GifShuffle*.
2. Menguji keamanan 3DES terhadap serangan melalui nilai *avalanche effect*.
3. Menguji citra digital hasil penyisipan pesan rahasia dengan metode steganografi melalui nilai PSNR.

1.5 Manfaat Penelitian

Manfaat penelitian ini adalah dengan adanya teknik pengamanan data steganografi melalui kriptografi ini diharapkan mampu menyediakan suatu media komunikasi untuk menjaga keamanan pertukaran informasi yang bersifat rahasia dari suatu perusahaan atau individu agar tidak dapat dimanfaatkan oleh pihak ketiga.

1.6 Metodologi Penelitian

Untuk mencapai tujuan yang dirumuskan sebelumnya, maka penyusunan skripsi ini menggunakan metodologi sebagai berikut:

1. Studi Literatur

   Mempelajari teori–teori dari literatur dan artikel yang berhubungan dengan GifShuffle untuk steganografi dan algoritma 3DES untuk kriptografi.

2. Perancangan dan Implementasi Sistem

   Mengumpulkan data yang diperlukan, melakukan analisis dan membuat rancangan model perangkat lunak dengan analisis terstruktur dan mengimplementasikan hasil rancangan tersebut yaitu membuat piranti lunak enkripsi pesan dan menyembunyikan hasil enkripsi pesan pada gambar.

3. Uji Coba dan Analisa Hasil Implementasi

   Melakukan pengujian perangkat lunak yang telah dibangun pada tahap implementasi.

4. Pembuatan Laporan

   Membuat laporan tertulis mengenai skripsi ini berdasarkan sistematika penulisan skripsi yang telah ditetapkan.

1.7 Sistematika Penulisan

Pembuatan skripsi ini disusun berdasarkan sistematika penulisan sebagai berikut:

1. BAB I PENDAHULUAN

   Berisi latar belakang masalah dari pembuatan perangkat lunak, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penulisan.

2. BAB II KAJIAN PUSTAKA DAN DASAR TEORI

   Menguraikan teori–teori yang erat hubunganya dengan algoritma 3DES dan GifShuffle.

3. BAB III METODE PENELITIAN DAN PERANCANGAN

   Pada bab ini akan dijelaskan mengenai metode–metode yang digunakan dalam melakukan enkripsi pesan dan menyembunyikan hasil enkripsi pesan pada gambar.

4. BAB IV IMPLEMENTASI

   Dalam bab ini akan dijelaskan mengenai implementasi sistem.

5. BAB V PENGUJIAN DAN ANALISIS

   Dalam bab ini akan dijelaskan mengenai pengujian dan analisa model sistem perangkat lunak.

6. BAB VI PENUTUP

   Berisi kesimpulan dari seluruh rangkaian penelitian serta saran kemungkinan pengembangannya.