BAB I
PENDAHULUAN

1.1 Latar Belakang

Saat ini, penggunaan informasi dan teknologi komunikasi sudah berkembang sangat pesat. *Internet* merupakan media komunikasi yang paling popular saat ini (Gandharba Swain, et. al., 2012). Dalam pemanfaatan teknologi *internet* ini, kadang-kadang perlu untuk menjaga kerahasiaan informasi, namun tidak menarik perhatian dari pihak lain, yang berarti pihak lain tidak mengetahui bahwa telah terjadi komunikasi rahasia. Hal ini sering diperlukan oleh agen rahasia yang ingin mengirimkan pesan rahasia kepada atasannya. Proses pengamanan data dengan metode enkripsi akan mengakibatkan pihak lain mengetahui bahwa agen rahasia tersebut telah mengirimkan suatu informasi rahasia kepada pihak lain.

Untuk menyelesaikan permasalahan tersebut, maka dapat diterapkan konsep steganografi. Steganografi dapat menyamarkan pesan ke dalam suatu media tanpa orang lain menyadari bahwa media tersebut telah disisipi suatu pesan, karena hasil keluaran steganografi adalah data yang memiliki bentuk persepsi yang sama dengan data aslinya apabila dilihat menggunakan indera manusia. (Cachin, 2005) Metode steganografi citra yang paling popular adalah metode LSB *substitution*. Namun, metode LSB ini tidak tahan terhadap penyerangan dengan menggunakan operasi pengolahan citra. Untuk itu, maka dapat dilakukan modifikasi terhadap metode *LSB* dimana bit tidak hanya disisipkan pada bit ke-8, namun juga dapat disisipkan pada bit ke-6 dan bit-7. Sementara itu, untuk meningkatkan keamanan informasi yang dikirimkan, maka dapat digabungkan penggunaan steganografi dan kriptografi untuk melindungi informasi rahasia, sehingga sulit untuk diubah dan dideteksi. Metode *hill cipher* merupakan salah satu metode enkripsi yang sederhana, namun metode *hill cipher* tidak dapat diterapkan pada karakter spesial dan digit serta sangat rentan terhadap *exhaustive key search attack* dan *known plaintext attack*. Untuk memperbaiki metode *hill cipher* ini, maka dikembangkan sebuah *new block cipher* dengan panjang blok sebesar 128 bit dan panjang kunci sebesar 256 bit. Pada

aplikasi stegnanografi ini, pesan akan dienkripsi dengan menggunakan *new block cipher*, dua bit dari *ciphertext* akan ditempelkan pada setiap piksel citra. Karena lokasi penyisipan ditentukan pada saat proses kerja dari algoritma, maka algoritma ini dinamakan *dynamic steganography* (Gandharba Swain, et. al., 2012). Kelebihan metode *dynamic steganography* terletak pada tingkat keamanan data yang lebih tinggi karena lokasi penyisipan tergantung pada *ciphertext* yang dihasilkan oleh pesan *input*.

Dari uraian di atas, maka dipilih judul "**Aplikasi Penyembunyian dan Pengamanan Pesan menggunakan *New Block Cipher* dan *Dynamic Steganography***" sebagai tugas akhir.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang pemilihan judul di atas, maka permasalahan yang dihadapi adalah :

1. Perlu dilakukan pengamanan terhadap pesan rahasia yang disembunyikan ke dalam media *image* tanpa diketahui oleh pihak yang tidak berwenang, serta melindungi informasi hak cipta yang berada di dalamnya tetap aman.
2. Perlu ditingkatkan sekuritas dari metode steganografi, sehingga lebih aman terhadap pihak yang tidak bertanggung jawab.

1.3 Tujuan Dan Manfaat

Tujuan yang ingin dicapai dari tugas akhir ini adalah membuat sebuah aplikasi yang dapat mengamankan data rahasia pada citra digital dengan menggunakan *New Block Cipher* dan *Dynamic Steganography*, sehingga dapat meningkatkan pengamanan data agar tidak diketahui orang lain.

Manfaat yang ingin dicapai dari tugas akhir ini adalah sebagai berikut :

1. Aplikasi dapat digunakan untuk meningkatkan keamanan informasi dari pihak luar yang tidak bertanggung jawab.
2. Aplikasi dapat digunakan sebagai referensi yang mendeskripsikan contoh penggunaan steganografi dan kriptografi menggunakan *New Block Cipher* dan *Dynamic Steganography*.

3. Laporan tugas akhir dapat digunakan sebagai referensi bagi penelitian lain untuk mengembangkan algoritma dan metode terbaru dalam steganografi dan kriptografi.

1.4 Batasan Masalah

Batasan masalah yang akan dibahas dalam tugas akhir ini mencakup :

1. Format citra yang dapat di-*input* (*image source*) berupa citra BMP, JPG dan PNG.
2. Format citra *output* (*image stego*) berupa citra BMP.
3. Teknik steganografi yang digunakan hanya dapat menyimpan pesan teks dengan format ASCII.
4. Perangkat lunak akan mengalokasikan sebanyak 8 piksel untuk menyimpan panjang bit *ciphertext*-nya, sehingga penyimpanan bit *ciphertext* akan dimulai dari piksel ke-9. Hal ini berarti tersedia 48 bit untuk menyimpan panjang bit *ciphertext*. Nilai terbesar untuk 48 bit adalah $(1111\ 1111\ 1111\ 1111\ 1111\ 1111\ 1111\ 1111\ 1111\ 1111\ 1111\ 1111)_2$ = 281.474.976.710.655, berarti panjang karakter *ciphertext* maksimal 281.474.976.710.655/8 = 35.184.372.088.831,875 (≈ 35.184.372.088.831 karakter).
5. Ukuran citra *input* minimal berukuran 100 x 100 piksel.
6. Batasan kunci sebesar 256 bit (32 karakter) dan panjang *block* pesan sebesar 128 bit (16 karakter)

1.5 Metodologi Penelitian

Langkah – langkah yang digunakan dalam penyusunan Tugas Akhir ini adalah sebagai berikut :

1. Studi Literatur

   Tahapan ini mencari dan mengumpulkan referensi mengenai algoritma yang dibutuhkan dalam perancangan aplikasi. Pengumpulan data dilakukan dengan cara mencari bahan yang berhubungan dengan algoritma *New Block Cipher* dan *Dynamic Steganography* serta penggunaan kunci rahasia dalam implementasinya untuk menyisipkan pesan di dalam citra dari internet,

paper ilmiah maupun buku-buku yang berhubungan dengan kriptografi dan steganografi.

2. Pengembangan sistem dengan model waterfall (Roger S. Pressman, 1992).

a. Analisis, terdiri dari :

   i. Analisis Proses, yaitu mendeskripsikan proses perhitungan kapasitas daya tampung suatu piksel, proses penyisipan pesan dan proses ekstraksi pesan dengan menggunakan algoritma *New Block Cipher* dengan *Dynamic Steganography*. Tools yang digunakan untuk memodelkan analisis proses adalah *Activity Diagram*.

   ii. Analisis Kebutuhan Sistem, yaitu mendeskripsikan kebutuhan fungsional dan nonfungsional sistem. Tools yang digunakan untuk memodelkan analisis kebutuhan sistem adalah *Use Case Diagram*.

b. Sistem Desain

   Tahapan ini merancang *interface* sistem, tampilan / menu-menu dan merancang aplikasi steganografi dengan menerapkan algoritma *New Block Cipher* dengan *Dynamic Steganography*.

c. Coding

   Membangun perangkat lunak dengan menggunakan bahasa pemograman Microsoft Visual C# .NET.

d. Testing

   Untuk memastikan bahwa aplikasi yang dirancang bebas dari kesalahan, perlu dilakukan testing (uji coba) pada aplikasi tersebut. Uji coba yang dilakukan mencakup uji coba pada proses penyisipan, ekstraksi, simpan gambar, dan mengembalikan pesan teks. Setelah diuji coba akan dilakukan proses analisa kembali apakah sistem yang dibangun sesuai dengan kebutuhan, untuk kemudian dilakukan proses perbaikan.

3. Pengujian.

   Pengujian terhadap algoritma *New Block Cipher* dengan *Dynamic Steganography* dilakukan dengan berbagai skenario yang berbeda, yaitu pengujian berdasarkan panjang pesan, citra berbeda berukuran sama, citra berbeda berukuran berbeda, ekstraksi pesan setelah menambahkan *noise,* dan pengujian terhadap *stego key* yang memiliki pola yang berulang. Pengujian terhadap kualitas citra akan menggunakan metode *Mean Square Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR).

4. Menyusun laporan tugas akhir.

   Langkah terakhir dari penelitian ini adalah membuat laporan. Laporan ini berisi hal-hal yang dikerjakan selama melakukan penelitian dan hasil-hasil yang didapatkan ketika melakukan penelitian.