# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Keperluan atas keamanan informasi telah melalui dua perubahan besar. Perubahan besar pertama adalah pengenalan terhadap komputer. Dengan munculnya komputer, keperluan atas alat pengamanan data dan informasi yang tersimpan di dalam komputer menjadi jelas. Apalagi untuk sistem yang bersifat *shared* seperti sistem *time-sharing*. Dan keperluan keamanan tersebut menjadi lebih penting lagi untuk sistem yang bisa diakses dari jaringan telepon publik, jaringan data, dan internet. Nama generik dari kumpulan alat yang didesain untuk melindungi data dan mencegah *hacker* disebut keamanan komputer (Stallings, 2006: 7).

Perubahan besar kedua adalah pengenalan terhadap sistem terdistribusi dan pemakaian terhadap jaringan dan fasilitas komunikasi untuk membawa data antara *terminal user* dan komputer dan antara komputer dan komputer. Keamanan jaringan dibutuhkan untuk melindungi data selama tranmisi terjadi (Stallings, 2006: 7).

Selama berjalannya waktu, penyerangan di internet semakin lama semakin canggih sementara kemampuan dan pengetahuan yang diperlukan untuk melawan serangan itu semakin menurun. Penyerangan telah menjadi semakin otomatis dan dapat menimbulkan kerusakan yang lebih besar (Stallings, 2006: 11).

Menjawab hal tersebut, maka penelitian ini dilakukan untuk menambah kemampuan dan pengetahuan dalam menjaga keamanan data. Penelitian ini akan berfokus pada pengamanan data dengan steganografi sebagai alternatif pengamanan pesan dan kriptografi untuk pengamanan gambar. Proses seperti kompresi dan enkripsi juga akan dilakukan pada pesan yang disteganografikan untuk diuji kompabilitas dan keuntungannya dengan metode yang dipilih.

Mayoritas dari sistem steganografi sekarang menggunakan gambar sebagai media penyembunyi karena orang sering mentransmisikan gambar digital melalui pesan elektronik dan komunikasi internet lainnya. Apalagi, setelah digitalisasi, gambar mengandung kuantisasi *noise* yang menyediakan tempat untuk menyisipkan data (Domenico dan Luca, 2008). Karena alasan yang sama pula, penelitian ini menggunakan gambar sebagai obyek steganografi dan enkripsi.

Steganografi merupakan metode pengamanan data yang memiliki pendekatan dimana informasi yang dikirimkan disembunyikan dalam media lain. Steganografi tidak hanya merujuk pada media digital, tetapi juga media lainnya. Menurut Gary C. Kessler (2001), ada banyak sekali metode steganografi mulai dari sesuatu yang kita semua akrab seperti tinta tak terlihat dan mikrodots sampai ke menyembunyikan pesan pada setiap huruf kedua pada pesan teks yang besar dan komunikasi *spread spectrum.*

Penelitian ini menggunakan metode steganografi yang ditemukan oleh Eiji Kawaguchi dan Richard O. Eason yang bernama *bit-plane-complexity-segmentation* (BPCS). Tidak seperti metode Least Significant Bit (LSB) yang

tidak efektif karena kapasitas penyimpanannya yang rendah, BPCS didasarkan pada ide simpel bahwa *bit plane* yang lebih tinggi juga memiliki kemampuan meyimpan informasi pada area yang terlihat kompleks (Srinivasan, 2003: 5).

Steganografi menyembunyikan data rahasia dalam *carrier*, dan ketika diaplikasikan dalam bentuk murninya, seorang hacker dapat dengan mudah memecahkan dan menginterpretasi data rahasia ketika keberadaan data rahasia diketahui. Sedangkan dalam kriptografi, keberadaan data rahasia tidak disembunyikan, tetapi data rahasia dienkripsi sehingga seorang hacker tidak dapat dengan mudah memecahkan data rahasia dari data yang telah dienkripsi (Srinivasan, 2003: 1).

Data gambar berbeda dengan teks. Walapun kita memakai dapat menggunakan sistem kriptografi tradisional untuk mengenkripsi gambar secara langsung, itu bukan merupakan ide bagus untuk 2 alasan. Pertama adalah besar data gambar yang hampir selalu lebih besar teks. Karena itu, sistem kriptografi tradisional memerlukan waktu yang lebih banyak untuk mengenkripsi data gambar. Masalah lainnya adalah teks hasil dekripsi yang harus selalu sama dengan teks asal. Namun, kebutuhan ini tidak diperlukan untuk data gambar. Mempertimbangkan karakteristik mata manusia, distorsi kecil pada data gambar hasil dekripsi masih diterima (Öztürk & Ibrahim, 2005).

Yaobin Mao dan Guanrong Chen menyimpulkan karakteristik dari enkripsi gambar secara umum menjadi 7. Pertama adalah redundansi yang tinggi dan kapasitas besar umumnya membuat data gambar yang dienkripsi rentan terhadap serangan melalui kriptanalisis. Yang Kedua adalah data gambar memiliki

korelasi tinggi antar *pixel* yang bertetangga, yang membuat *data-shuffling* yang cepat menjadi tidak mungkin. Ketiga, kapasitas yang besar dari data gambar membuat enkripsi secara *real-time* menjadi sulit. Keempat, enkripsi gambar sering digunakan sebagai kombinasi dengan kompresi data. Kelima, dalam penggunaan gambar, konversi *file format* sering dilakukan. Keenam, penglihatan manusia memiliki ketahanan tinggi untuk degradasi gambar dan *noise*. Dan yang terakhir, dari sisi keamanan, data gambar tidak sesensitif informasi teks.

Saat ini, belum ada algoritma enkripsi gambar yang dapat memenuhi kebutuhan di atas. Namun, algoritma enkripsi gambar berbasis Chaos dapat menyediakan sebuah *class* dari *methods* yang menjanjikan yang dapat memenuhi banyak dari kebutuhan di atas (secara penuh atau pun tidak) dan memperlihatkan superioritas dari algortima konvensional yang ada (Yaobin Mao dan Guanrong Chen, 2003). Oleh karena itu, pada penelitian ini, juga akan diadopsi sebuah teknik kriptografi berbasis *Chaos* yang bernama *nonlinear-chaos algorithm.*

Berdasarkan saran yang diberikan oleh Yeshwanth Srinivasan pada penelitiannya, kriptografi pada pesan juga akan dikombinasikan dengan steganografi untuk menjaga data tetap tidak terpecahkan walau berhasil ditemukan. Selain itu, akan ditambahkan kompresi data agar penyimpanan yang dapat dilakukan dapat semakin banyak.

Berdasarkan latar belakang tersebut, penulis melakukan penelitian dengan berfokus pada pengimplementasian steganografi dan kriptografi pada bitmap untuk pengamanan pengiriman data disertai kompresi dan kriptografi pada pesan.

## 1.2 Rumusan Masalah

1. Bagaimana mengimplementasikan algoritma *bit-plane-complexity-segmentation* untuk melakukan steganografi pada bitmap?
2. Bagaimana mengimplementasikan algoritma *nonlinear-chaotic-algorithm* untuk melakukan enkripsi pada bitmap?
3. Bagaimana membangun aplikasi pengamanan pengiriman data yang mengimplementasikan algoritma *bit-plane-complexity-segmentation* dan algoritma *nonlinear-chaotic-algorithm*?
4. Apakah kompresi dan kriptografi pada data dapat dikombinasikan dengan steganografi?

## 1.3 Batasan Masalah

1. Gambar yang disteganografi merupakan gambar 24 bit RGB dengan ekstensi .bmp.
2. Gambar yang dienkripsi memiliki ekstensi .bmp.
3. Pesan yang dikompresi berupa pesan (s*tring*) yang dituliskan secara langsung atau berada dalam suatu *file.*
4. Pesan yang dienkripsi berupa pesan (*string*) yang dituliskan secara langsung atau berada dalam suatu *file.*
5. Informasi yang disisipkan pada gambar dengan steganografi berupa pesan (*String*) yang dituliskan secara langsung atau berada dalam suatu *file.*

6. Kompresi dan enkripsi terhadap pesan, steganografi terhadap gambar, dan enkripsi terhadap gambar merupakan modul yang terpisah dan dioperasikan secara manual.

## 1.4 Tujuan Penelitian

1. Mengimplementasikan algoritma *bit-plane-complexity-segmentation.*
2. Mengimplementasikan *nonlinear-chaotic-algorithm.*
3. Membangun aplikasi pengamanan data yang mengimplementasikan algoritma *bit-plane-complexity-segmentation* dan *nonlinear-chaotic-algorithm.*
4. Mengombinasikan kompresi dan kriptografi pada pesan dengan steganografi.

## 1.5 Manfaat Penelitian

Penelitian ini bermanfaat bagi setiap pengguna internet yang ingin melindungi data yang akan dikirimkan melalui internet. Penelitian ini bermanfaat bagi pihak yang membutuhkan keamanan data dalam mengirimkan informasi yang rahasia. Penelitian ini juga bermanfaat sebagai dasar yang akan melakukan penelitian dengan topik yang serupa.

## 1.6 Metode Penelitian

Metode yang digunakan dalam penelitian ini terdiri dari langkah-langkah sebagai berikut.

1. Studi Literatur

Melakukan studi kepustakaan melalui hasil penelitian orang lain maupun artikel-artikel atau paper-paper lainnya yang relevan. Studi tidak hanya mencakup algoritma yang digunakan dalam penelitian ini, tetapi juga topik seputar keamanan transaksi data.

2. Analisis dan Perancangan Sistem

   Melakukan analisis terhadap masalah yang dihadapi dan merancang sistem untuk mengimplementasikan algoritma *bit-plane-complexity-segmentation* dan *nonlinear-chaotic-algorithm*.

3. Implementasi

   Mengimplementasikan algoritma *bit-plane-complexity-segmentation* dan *nonlinear-chaotic-algorithm* pada sistem.

4. Pengujian

   Melakukan pengujian terhadap aplikasi yang telah dibuat. Pengujian dilakukan dengan mencoba masing-masing modul (enkripsi teks, kompresi teks steganografi, dan enkripsi gambar) juga dengan mengombinasikan antar modul tersebut.

## 1.7 Sistematika Penulisan Laporan Penelitian

Dalam penulisan skripsi ini, sistematika penulisan dibagi menjadi lima (5) bab, yaitu.

1. BAB I PENDAHULUAN

Berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode, serta sistematika penulisan laporan penelitian.

2. BAB II TELAAH LITERATUR

   Berisi teori yang digunakan dalam perancangan, implementasi, analisis penelitian. Terdiri dari teori mengenai rekayasa piranti lunak, steganografi, kriptografi serta penjelasan algoritma *advanced encryption standard*, *deflate*, *bit-plane-complexity-segmentation*, dan *nonlinear-chaotic-algorithm* yang digunakan dalam penelitian ini.

3. BAB III ANALISIS DAN PERANCANGAN

   Berisi gambaran umum tentang sistem yang akan dibuat. Dijelaskan spesifikasi, tujuan, batasan, masukkan, dan keluaran sistem serta gambaran perancangan sistem, mulai dari proses yang terjadi di dalamnya, desain interface, serta hirarki menu.

4. BAB IV IMPLEMENTASI DAN EVALUASI

   Berisi hasil penelitian, mulai dari proses implementasi dari aplikasi yang dibuat, spesifikasi perangkat lunak maupun perangkat keras yang digunakan dalam pembangunan aplikasi, proses pengujian aplikasi, hasil pengujian aplikasi, penjelasan cara pemakaian aplikasi serta evaluasi akhir dari aplikasi yang dibuat.

5. BAB V SIMPULAN DAN SARAN

Berisi simpulan dan saran. Pada simpulan, diuraikan mengenai jawaban atas batasan masalah serta tujuan penelitian yang diuraikan pada BAB I, beserta informasi tambahan yang diperoleh atas dasar temuan penelitian. Sedangkan pada bagian saran, diuraikan manifestasi dari penulis atas sesuatu yang belum ditempuh dan layak untuk dilaksanakan pada penelitian lanjutan.