1. Pendahuluan

1.1 Latar Belakang

Pertukaran informasi di Internet telah menjadi bagian yang penting dalam perkembangan teknologi informasi di seluruh dunia. Hal tersebut dikarenakan media Internet memiliki banyak kelebihan dibandingkan dengan media komunikasi lainnya. Misalnya, akses kecepatan yang tinggi sehingga proses transfer data menjadi lebih cepat. Namun, sesungguhnya media internet bukanlah media yang aman untuk pertukaran informasi. Seseorang bisa saja menyadap aliran pengiriman data penting melalui email atau transaksi online.

Terdapat beberapa cara yang dapat digunakan untuk menjaga keamanan dan kerahasiaan data, diantaranya dengan menggunakan teknik Kriptografi dan Steganografi. Kriptografi adalah ilmu yang mempelajari mengenai teknik pengubahan pesan untuk membuat pesan tersebut aman dan tahan dari serangan [03]. Steganografi (s*teganography*) adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui [09]. Keuntungan steganografi dibandingkan dengan kriptografi adalah bahwa pesan yang dikirim tidak menarik perhatian sehingga media penampung yang membawa pesan tidak menimbulkan kecurigaan bagi pihak ketiga. Ini berbeda dengan kriptografi dimana *ciphertext* menimbulkan kecurigaan bahwa pesan tersebut merupakan pesan rahasia.[09]

Pada umumnya, steganografi menggunakan media digital sebagai wadah penampung, misalnya citra, suara (audio), teks, dan video [01]. Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video [01]. Pada Tugas Akhir ini, wadah penampung yang digunakan adalah citra digital. Ada beberapa metode yang dapat digunakan untuk steganografi pada citra digital, antara lain: *Least Significant Bit (LSB), Spread Spectrum Steganography* dan *Bit-Plane Complexity Segmentation (BPCS)*.

Implementasi pada Tugas Akhir ini menggunakan metode Bit-Plane Complexity Segmentation (BPCS) terhadap citra digital dengan format *BMP*. Metode BPCS ini diperkenalkan oleh Eiji Kawaguchi dan R.O. Eason pada tahun 1997 [06]. BPCS memanfaatkan karakteristik dari *human vision* yang tidak melihat informasi visual dalam area yang mengandung noise dalam sebuah citra. BPCS memanfaatkan perhitungan kompleksitas pada tiap bit-plane dalam menyelipkan informasi rahasia. Kelebihan metode BPCS ini jika diterapkan pada citra digital adalah memiliki kapasitas penyisipan data rahasia mencapai 50% dari kapasitas wadah penampungnya [06]. *BMP* menangani file grafik dalam sistem operasi Microsoft Windows. File *BMP* tidak dikompresi, sehingga memiliki ukuran yang besar. Kelebihan *BMP* adalah kesederhanaan, penerimaan luas, dan digunakan dalam program Windows.

1.2 Perumusan Masalah

Berdasarkan latar belakang di atas, permasalahan yang diteliti dan dijabarkan pada Tugas Akhir ini adalah

1. Bagaimana menerapkan steganografi dengan metode BPCS pada citra digital dengan format *BMP*. Menurut teori metode BPCS ini memiliki kapasitas penyisipan data rahasia mencapai 50% dari kapasitas wadah penampungnya.
2. Bagaimana kualitas citra steganografi pada metode BPCS.
3. Bagaimana ketahanan terhadap serangan pada citra steganografi.

Sedangkan batasan masalah dalam menyelesaikan Tugas Akhir ini, antara lain:

1. Format citra digital yang akan disisipi data rahasia adalah *BMP* 24 bit RGB dengan resolusi 512 × 512 pixel.
2. Besarnya threshold untuk steganografi adalah 0.1, 0.2, 0.3, 0.4, dan 0.5
3. *Block Bit-Plane* berukuran 8 × 8 pixel, 32 × 32 pixel, dan 256 × 256 pixel.
4. Media digital yang menjadi data rahasia berupa teks, citra, audio, dan video.
5. File map yang berisi informasi letak data rahasia disembunyikan, tidak disisipkan pada citra steganografi.
6. Serangan terhadap citra steganografi berupa kompresi jpg, resize 50%, noise Gaussian 12.5%, dan rotasi 15^0

1.3 Tujuan

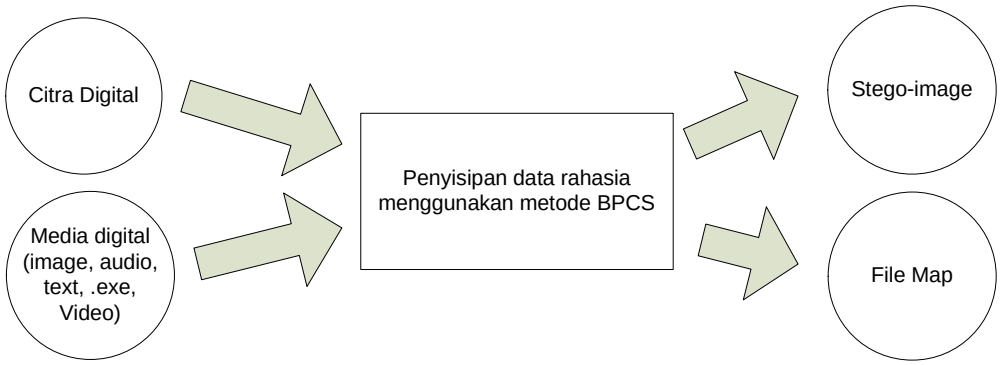
Tujuan dari penelitian Tugas Akhir ini:

1. Memahami steganografi dengan menggunakan metode BPCS.
2. Membangun perangkat lunak yang merupakan implementasi dari metode BPCS untuk menyisipkan dan meng-ekstraksi suatu data rahasia pada citra digital.
3. Mengetahui pengaruh *threshold* (batas yang ditentukan sebagai batas kompleksitas untuk memisahkan antara *informative region* dengan *noise-like region*) terhadap kapisitas penyisipan data rahasia dan kualitas citra steganografi (citra yang telah disisipkan data rahasia).
4. Mengetahui tingkat ketahanan citra steganografi terhadap serangan.

1.4 Metodologi Penyelesaian Masalah

Metedologi yang digunakan dalam menyelesaikan Tugas Akhir ini adalah:

1. Study Literatur
   Tahap ini bertujuan untuk mengumpulkan bahan-bahan, dan mendapatkan referensi yang jelas dan dasar teori yang kuat mengenai steganografi dengan metode *Bit-Plane Complexity Segmentation* pada citra digital serta referensi Java yang digunakan sebagai bahasa pemrograman untuk membangun aplikasi steganografi.
2. Analisis dan Design
   Tahap ini meliputi analisis kebutuhan untuk merancang sebuah sistem steganografi pada citra digital. Deskripsi sistem baik proses penyisipan maupun ekstraksi data rahasia dapat dilihat pada gambar berikut:



Gambar 1-1. Proses Penyisipan Data Rahasia.

Gambar 1-2. Proses Ekstraksi Data Rahasia.

3. Implementasi
   Tahap ini meliputi pembangunan sistem yang telah dirancang pada tahap sebelumnya. Pada tahap ini diimplementasikan perancangan yang telah dilakukan menjadi sebuah sistem dengan menggunakan bahasa pemrograman Java.
4. Pengujian dan Analisis Hasil
   Pada tahap ini dilakukan pengujian terhadap sistem yang telah dibangun dan sekaligus melakukan analisis terhadap hasil dari sistem**.** Beberapa pengujian yang dilakukan, antara lain:
   a. *Fidelity*, *robustness*, dan *recovery* pada stego-image yang telah dikompresi ke berbagai format image jpeg, gif, dan png.
   b. Pengaruh *threshold* pada kapasitas maksimal data rahasia yang dapat disisipkan ke dalam citra digital menggunakan metode BPCS.
   c. Kualitas stego-image setelah disisipi data rahasia dengan membandingkan antara stego-image dan image sebelum mengalami proses penyisipan data rahasia. Pembandingan dilakukan dengan cara penampilan visual dan PNSR (*Peak Signal to Noise Ratio*).
   d. Ketahanan citra steganografi terhadap serangan. Pembandingan dilakukan dengan BER (*Bit Error Rate*).

5. Pembuatan Laporan
   Pada tahap ini, dilakukan penyusunan laporan Tugas Akhir dan pengumpulan dokumentasi dengan mengikuti kaidah penulisan yang benar dan sesuai dengan ketentuan-ketentuan atau sistematika yang telah ditetapkan oleh institusi.