BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi internet yang sangat pesat membuat komunikasi dan pertukaran informasi antara pihak pengirim dan penerima menjadi lebih cepat dan mudah. Namun pengiriman data jarak jauh melalui gelombang radio maupun media lain, terutama media internet, yang digunakan masyarakat luas sangat memungkinkan pihak lain menyadap dan mengubah data yang dikirimkan. Perlu disadari bahwa banyak sekali ancaman terhadap keamanan dan kerahasiaan data yang mungkin akan mengganggu kita. Jumlah penyusup *(hacker)* dan perusak *(cracker)* yang banyak juga menjadi penyebab diperlukannya suatu cara untuk mengamankan data agar hanya pengirim dan penerima saja yang mengetahui isi data rahasia tersebut. Steganografi merupakan teknik menyembunyikan pesan ke dalam media lain sehingga keberadaan pesan tidak diketahui oleh orang lain[5]. Pesan yang disisipkan ini dapat berupa tulisan, citra, suara, maupun video. Media yang disisipi *(cover)* pun dapat berupa tulisan, citra, suara, maupun video.

Pada perkembangannya, teknik steganografi ini banyak dikombinasikan dengan berbagai metode enkripsi untuk lebih dapat meningkatkan kualitas dan performansi steganografi. Pengkombinasian ini biasanya disebut dengan *Hybrid Steganography*. Pada penelitian yang telah dilakukan sebelumnya[8], metode *Hybrid Steganography* juga masih memiliki kekurangan, yaitu rusak/hilangnya pesan rahasia yang disisipkan akibat gangguan selama proses pengiriman/transmisi data, baik gangguan yang terjadi pada kanal transmisi maupun serangan geometris pada citra yang dilakukan secara sengaja oleh manusia. Oleh karena itu, dalam tugas akhir ini dilakukan penelitian yang menggabungkan metode enkripsi dan juga metode *error correction* pada citra rahasia yang disisipkan. Metode enkripsi yang digunakan yaitu *Advanced Encryption Standard* (AES). Sedangkan untuk meminimalkan kesalahan dari data yang diterima, digunakan teknik deteksi dan koreksi *error* BCH *Code*. Sistem steganografi yang disimulasikan pada tugas akhir ini menggunakan citra digital sebagai *cover* dan juga pesan rahasianya.

1.2 Rumusan Masalah

Dari latar belakang yang telah disampaikan sebelumnya, maka dapat dijabarkan beberapa rumusan masalah yang dibahas pada Tugas Akhir ini, yaitu:

1. Bagaimana penerapan metode enkripsi dan dekripsi *Advanced Encryption Standard* (AES) pada citra rahasia yang disisipkan?
2. Bagaimana merancang dan mengimplementasikan sebuah sistem untuk melakukan steganografi dengan BCH *encoding* di sisi pengirim dan mengekstraksi kembali citra rahasia yang disisipkan serta melakukan BCH *decoding* di sisi penerima?
3. Bagaimanakah kualitas citra hasil steganografi dan citra hasil ekstraksi yang telah diuji dengan *noise* Gaussian, *noise* Salt & Pepper, *rescaling*, dan *cropping* ditinjau dari nilai BER, PSNR, dan MOS*?*

1.3 Tujuan

Tujuan tugas akhir ini adalah untuk menyisipkan citra rahasia ke dalam sebuah *cover* citra digital, lalu melakukan metode enkripsi untuk menjamin kemananan data dan mengkodekannya agar citra rahasia yang diterima oleh penerima dapat diminimalisir kesalahannya.

1.4 Batasan Masalah

Beberapa batasan masalah pada penelitian Tugas Akhir ini adalah:

1. Ukuran/kapasitas citra *cover* yang digunakan adalah 1024x1024 piksel.
2. Ukuran/kapasitas citra rahasia yang digunakan adalah 32x32 piksel.
3. Citra cover adalah citra *grayscale* berformat Bitmap, sedangkan citra rahasia adalah citra biner (BW *image*) yang juga berformat Bitmap.
4. Digunakan metode *joint* DWT-DCT dalam proses penyisipan.
5. Metode deteksi dan koreksi *error* yang digunakan adalah BCH *Code* (15,5) dengan kemampuan koreksi 3 bit dari 5 bit masukan.
6. Pengujian standar terhadap sistem steganografi adalah dengan *noise* Gaussian, *noise* Salt & Pepper, *rescaling*, dan *cropping*.
7. Parameter hasil yang digunakan adalah BER, PSNR, dan MOS.
8. Sistem disimulasikan menggunakan MATLAB R2011b.

1.5 Metodologi Penelitian

Dalam Tugas Akhir ini digunakan metode simulasi dengan *software* Matlab R2011b untuk merancang sebuah sistem yang dapat melakukan steganografi, proses enkripsi dan dekripsi AES, proses *encoding* dan *decoding* BCH, serta proses ekstraksi.

1.6 Sistematika Penulisan

Tugas akhir ini dibagi dalam beberapa topik bahasan yang disusun secara sistematis sebagai berikut :

Bab I PENDAHULUAN

Bab ini membahas latar belakang, tujuan, rumusan dan batasan masalah, metodologi penelitian serta sistematika penulisan.

Bab II DASAR TEORI

Bab ini membahas dasar teori steganografi, citra digital, analisis matematika, dan algoritma yang digunakan dalam metode AES dan BCH *Code*.

Bab III PERANCANGAN DAN IMPLEMENTASI

Bab ini menjelaskan proses desain, realisasi sistem, jenis-jenis *attack* yang digunakan, dan parameter pengujian.

Bab IV PENGUJIAN SISTEM DAN ANALISIS HASIL

Bab ini membahas analisis hasil simulasi. Analisis dilakukan terhadap parameter kinerja sistem yang diamati setelah sistem diuji dengan *noise* dan teknik serangan geometris.

Bab V PENUTUP

Berisi kesimpulan dari Tugas Akhir ini dan saran yang dapat digunakan untuk penelitian dan pengembangan lebih lanjut atau sebagai bahan referensi.