BAB I

PENDAHULUAN

1.1 Latar Belakang

Steganografi adalah salah satu teknik pengamanan data dimana pesan akan disembunyikan ke dalam pesan lainnya sehingga orang lain tidak menyadari ada sesuatu di dalam pesan tersebut (Sellars, 1996). *Least Significant Bit* (LSB) merupakan salah satu metode steganografi untuk penyembunyian pesan rahasia yang dilakukan dengan cara mengambil bit terakhir pada beberapa *byte* media penyembunyiannya, kemudian mengganti bit tersebut dengan bit pesan rahasia secara berurutan (Kamau et al, 2012). Kelemahan steganografi menggunakan LSB yaitu penyusup mudah mengubah semua *pixel* gambar kemudian merekonstruksinya untuk mendapatkan informasi yang tersimpan di LSB (Joshi et al, 2013). Tahun 2014 Mamantha et al mengatasi kelemahan tersebut dengan menggunakan teknik LSB dan melakukan XOR untuk mencegah penyusunan kembali informasi yang tersimpan tanpa menggunakan kunci. Namun setelah dilakukan analisis, metode ini menghasilkan penurunan nilai PSNR dari 36,70 menjadi 28,32 yang mengakibatkan penurunan kapasitas menyimpan pesan rahasia (Mamantha et al, 2014).

Untuk meningkatkan kapasitas penyimpanan pesan rahasia, tahun 2015 Bhalshanskar dan Gulve merancang algoritma modifikasi LSB dengan *range of bytes* dan struktur piramida. Hal ini dilakukan dengan cara menyembunyikan bit-bit rahasia secara acak di *byte* piramida (Bhalshanskar dan Gulve, 2015a). Hasil dari penelitian tersebut menunjukkan nilai PSNR yang tinggi dan rata-rata kapasitas muatan pada 8 bit *file* audio yaitu 18,64% sedangkan untuk 16 bit *file* audio adalah 20,71% (Bhalshanskar dan Gulve, 2015b). Namun, algoritma ini belum mampu mengetahui terjadinya modifikasi saat pengiriman *file* dan belum mampu memastikan pesan akan

diterima oleh orang yang sah. Salah satu cara untuk mengatasi masalah tersebut dengan melakukan otentikasi menggunakan *watermarking* (Khosla dan Kaur, 2014).

Salah satu metode *watermarking* yang sering digunakan untuk penyembunyian data adalah *Discrete Cosine Transform* (DCT) (Wu et al, 2001). Kelemahan DCT yaitu memerlukan waktu yang lama saat proses penyisipan dan ekstrasi *watermark*. Untuk mengatasi kelemahan tersebut tahun 2008 Navas et al mengusulkan metode *Discrete Wavelet Transform* (DWT) yang dapat menghasilkan satu bagian frekuensi rendah dan tiga frekuensi tinggi untuk mereduksi waktu. Namun, DWT juga memiliki kelemahan yaitu *shift sensitivity* dan *poor directionality* (Fernandes et al, 2003). Untuk mengatasi kelemahan masing-masing dari metode, maka dapat menggunakan penggabungan antara dua transformasi yaitu DWT dan DCT (Amirgholipour dan Naghsh-Nilchi, 2009). Kelemahan penggabungan metode ini yaitu belum mampu mengatasi perselisihan *robustness* dan *imperceptibility*. Kemudian tahun 2012, Prajapati et al mengusulkan menggunakan *hybrid* skema DWT-DCT dan SVD untuk menghasilkan *watermark* yang *imperceptibility* yang tinggi, tahan terhadap *noise* dan memiliki kapasitas penyembunyian data yang tinggi. Skema ini menggunakan koefisien *wavelet* sub-band LL pada cover citra untuk penyisipan *watermark*, kemudian dari hasil koefisien *wavelet* dilanjutkan dengan perhitungan koefisien DCT dan dekomposisi nilai-nilai *singular*. Nilai *singular cover* citra dimodifikasi dengan nilai-nilai *singular* dari *watermark* citra. Kemudian diterapkan *inverse* DCT dan *inverse* DWT (Prajapati et al, 2012). Penggabungan teknik steganografi dan *watermark* dapat diterapkan pada *file* video yang dibagi menjadi dua bagian yaitu steganografi akan diterapkan pada audio dan *watermark* diterapkan pada *frame*.

Berdasarkan uraian di atas, maka ide ini diangkat sebagai tugas akhir dengan judul "**Penerapan LSB ROB dan Struktur Piramida pada Steganografi dan DWT-DCT-SVD pada Watermark dalam File Video**".

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka yang menjadi permasalahan sehingga perlu dilakukan penelitian ini adalah mudahnya penyusup mengubah dan menghancurkan pesan rahasia yang tersimpan dan terjadinya penurunan kapasitas pesan rahasia sehingga dibutuhkan algoritma modifikasi LSB untuk mengatasi masalah tersebut. Namun algoritma ini belum mampu mengetahui terjadinya modifikasi saat pengiriman *file* dan belum mampu memastikan pesan akan diterima oleh orang yang sah, sehingga dibutuhkan otentikasi menggunakan metode *watermark* yang *imperceptibility* dan *robustness*.

1.3 Tujuan dan Manfaat

Tujuan dari tugas akhir ini, adalah:

1. Membangun sistem penerapan teknik LSB menggunakan ROB dan struktur piramida pada steganografi dan *hybrid* DWT-DCT-SVD pada *watermark* dalam *file* video untuk mengamankan pesan rahasia dari pihak yang tidak berwenang.
2. Untuk mengetahui tingkat keamanan dari sistem yang dibangun dengan melakukan pemberian *noise* pada audio yang berada dalam *file* video stego.

Sedangkan manfaat yang diharapkan dari tugas akhir ini, adalah:

1. Sistem dapat digunakan sebagai alternatif untuk mengamankan pesan rahasia pada *file* video.
2. Laporan Tugas Akhir ini dapat digunakan sebagai referensi untuk pengembangan penerapan teknik LSB menggunakan ROB dan struktur piramida pada steganografi dan *hybrid* DWT-DCT-SVD pada *watermark* dalam *file* video.

1.4 Batasan Masalah

Batasan masalah dalam tugas akhir ini, antara lain:

1. Video yang dapat di-*input* merupakan format .avi.
2. *Frame* yang terdapat di dalam video memiliki ukuran minimal 600 x 400 piksel dan maksimal 800 x 400 piksel.

3. Citra yang di-*input* merupakan citra RGB dengan format .bmp dan berukuran persegi dengan ukuran 400 x 400 piksel.
4. Audio hasil ekstrak menggunakan 8 bit dengan format .wav.
5. Ukuran pesan tergantung pada ukuran audio. Apabila audio tidak sanggup memuat pesan, maka akan ditampilkan pesan kesalahan.
6. *Frame* dan audio yang merupakan hasil ekstrak dari video akan disimpan ke dalam sebuah folder yang akan digunakan kembali pada proses penggabungan *frame* dan audio sehingga menjadi video kembali.
7. Serangan yang akan dilakukan pada audio yaitu mengubah *byte* sesuai *percentage noise* yang di-*input*.

1.5 Metodologi Penelitian

Metodologi yang digunakan dalam penyusunan tugas akhir ini adalah sebagai berikut:

1. Mempelajari referensi

   Pada tahap ini membaca dan mempelajari referensi yang ada, agar dapat memahami proses kerja dari metode yang digunakan pada tugas akhir.

2. Membuat aplikasi dengan model *waterfall*.

   2.1. Analisis kebutuhan

   Melakukan analisis kebutuhan fungsional, kebutuhan *non*-fungsional dan analisis proses.

   2.2. Perancangan

   Merancang *user interface* dari perangkat lunak yang akan dibuat.

   2.3. Penulisan program

   Melakukan penulisan kode program berbasis desktop menggunakan C#.net.

   2.4. Pengujian

   Dalam pengujian akan dilakukan perubahan parameter ROB, isi pesan dan citra *watermark* untuk melihat banyaknya kapasitas penyimpanan pesan rahasia dan *imperceptibility* pada video stego. Sedangkan untuk melihat

robustness akan dilakukan pemberian *noise* pada audio yang terdapat dalam video stego.

3. Menarik kesimpulan dari hasil pengujian
4. Menyusun laporan Tugas Akhir