BAB I
PENDAHULUAN

1.1 Latar Belakang

Citra medis merupakan jenis citra yang memiliki pola citra (*image pattern*) dalam hal proses analisa dan diagnosanya. Citra medis merupakan hasil keluaran dari sebuah alat seperti CT (*Computerized Tomography*) *scan* dan *X-ray* (Sinar X). Citra medis mengandung informasi penting mengenai keadaan tubuh manusia yang digunakan sebagai pendukung dokter dalam melakukan diagnosa penyakit. Ketika hasil diagnosa pasien telah selesai dilakukan, biasanya akan diperoleh hasilnya yang kemudian dikenal dengan citra medis. Setelah citra medis diperoleh, maka perlu dilakukan pengamanan untuk menghindari penyalahgunaan oleh pihak yang tidak berwenang, seperti file citra yang diubah atau digunakan tanpa sepengetahuan pemiliknya.

Untuk mengamankan citra medis, dapat dilakukan melalui teknik kriptografi dan steganografi. Kriptografi merupakan teknik penyandian informasi sehingga informasi tidak dapat diakses oleh pihak yang tidak memiliki hak untuk mengaksesnya (Usha, et al., 2014). Melalui kriptografi, informasi asli sedemikian rupa disandikan sehingga informasi tersebut tidak bisa dimengerti oleh pihak yang tidak memiliki kunci. Algoritma yang digunakan dalam pengamanan citra medis ini adalah *Modified Advanced Encryption Standard* (MAES) 128 *bit*. Algoritma MAES 128 *bit* digunakan disini dikarenakan lebih tahan terhadap serangan statistik jika dibandingkan dengan AES (Tahir, 2016). MAES 128 *bit* merupakan metode yang telah dimodifikasi dari algoritma *Advanced Encryption System* (AES) dengan cara mengubah transformasi *shiftrow,* apabila bilangan bulat memiliki nilai ganjil maka akan beroperasi sebagai transformasi normal, jika memiliki bilangan bulat genap, maka setiap kolom akan digeser secara siklis atas jumlah *byte* yang berbeda, dan dianggap sebagai *offset.*

Data yang telah disandikan dengan MAES dapat disembunyikan melalui steganografi. Steganografi merupakan teknik menyembunyikan sebuah pesan dengan menyisipkan informasi asli pada sebuah media yang lebih dikenal dengan *cover image*. Melalui steganografi, citra medis yang mengandung informasi penting mengenai kondisi tubuh seseorang akan dienkripsi dahulu dan dapat disembunyikan ke dalam citra sampul menggunakan metode steganografi agar tidak menarik perhatian dan mengundang kecurigaan terhadap citra medis, dan juga menjadikan citra tersebut lebih aman terhadap resiko pencurian data. Teknik yang digunakan disini yaitu IWT (*Integer Wavelet Transform*). IWT dapat digunakan untuk menyisipkan pesan atau

informasi ke dalam *cover image,* yang disisipkan melalui koefisien IWT untuk mencapai tingkat *imperceptibility* dan keamanan yang tinggi (Al-Dmour & Al-Ani, 2015). Penggunaan algoritma *wavelet* dikarenakan dapat mentransformasikan partisi informasi pada frekuensi yang tinggi dan rendah yang berbasis pada satu per satu piksel dengan jelas (Hamid et al, 2012), dan mampu menyimpan pesan rahasia pada *cover image* yang rentan terhadap resiko serangan citra. Selain IWT, teknik generator modulo juga akan dikombinasikan sebagai pengacak lokasi bit data agar mampu menyembunyikan pesan rahasia. Bilangan yang digunakan untuk generator modulo merupakan bilangan prima terbesar yang lebih kecil dari jumlah keseluruhan pixel pada gambar tujuannya agar lebih aman serta tidak mudah dimodifikasi oleh pihak lain. Menggabungkan algoritma kriptografi dan steganografi dalam pengamanan citra medis bertujuan untuk meningkatkan keamanan citra medis tersebut, jika citra medis hanya disisipkan ke dalam citra sampul menggunakan metode steganografi, maka hal yang mungkin terjadi adalah citra medis dapat diperoleh setelah proses ekstraksi. Oleh karena itu, penggunaan kriptografi akan mengurangi resiko keamanan tersebut dengan cara mengenkripsi citra medis menjadi citra acak terlebih dahulu, kemudian baru disisipkan dengan metode steganografi.

Berdasarkan uraian yang telah dikemukakan di atas, maka diajukan sebuah tugas akhir dengan judul "**PENGAMANAN CITRA MEDIS MENGGUNAKAN ALGORITMA IWT DAN GENERATOR MODULO DENGAN ENKRIPSI MAES**".

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, dapat dirumuskan permasalahan yang akan diselesaikan dalam penelitian ini yaitu memanfaatkan steganografi dalam menyembunyikan dan mengamankan sebuah informasi tidaklah cukup. Jika proses ekstraksi pesan berhasil dilakukan, maka pihak yang tidak berwenang dapat memperoleh informasi yang sebenarnya. Oleh karena itu, dibutuhkan kriptografi untuk dapat menyandikan informasi (pesan) dan steganografi dalam menyembunyikan informasi tersebut ke dalam sebuah media untuk meningkatkan pengamanan data.

1.3 Tujuan

Tujuan dari penyusunan tugas akhir ini adalah untuk meningkatkan keamanan citra medis melalui perangkat lunak steganografi yang menggunakan generator modulo berbasis IWT dengan enkripsi MAES 128 *bit*.

1.4 Manfaat

Manfaat dari penyusunan tugas akhir ini adalah:

1. Menghasilkan aplikasi yang dapat mengamankan citra medis pada citra sampul menggunakan metode IWT dan generator modulo dengan enkripsi MAES.
2. Sistem yang dibangun dapat menjadi rujukan di dalam pengamanan citra medis yang lebih baik.

1.5 Batasan Masalah

Batasan masalah dari penelitian ini dapat dirincikan sebagai berikut :

1. Format citra medis berupa .bmp.
2. Citra medis yang digunakan umumnya berupa citra *grayscale*, dan hasil output *stego image* sesuai dengan format file citra yang diinput.
3. Citra yang digunakan harus berukuran n x n.
4. Data untuk pelatihan merupakan data yang diperoleh dari database Open-Access Medical Image Repositories. (http://www.aylward.org/notes/open-access-medical-image-repositories).

1.6 Metodologi Penelitian

Tahapan yang dilakukan dalam metodologi penelitian ini di antaranya adalah:

1. Studi Literatur

   Kegiatan studi literatur akan dilakukan dengan mengamati fenomena permasalahan yang terjadi, mempelajari penelitian sebelumnya melalui artikel jurnal, serta memahami konsep kriptografi dan steganografi mencakup teknik *Integer Wavelet Transform* (IWT), generator modulo, dan MAES 128-bit.
2. Pengembangan Aplikasi

   Metodologi yang digunakan dalam penelitian ini yakni dengan model *waterfall*. Adapun proses perancangan aplikasi ini adalah sebagai berikut.

   a. *Requirements analysis and definition*

      Melakukan studi literatur, mengumpulkan data-data, kemudian melakukan analisis kebutuhan fungsional, dan kebutuhan *non*-fungsional. Untuk kebutuhan fungsional digambarkan dengan menggunakan *use case diagram*, dan kebutuhan *non*-fungsional dimodelkan dengan metode *Performance, Information, Economy, Control, Efficiency, Service* (PIECES).

b. *System and software design*

Merancang tampilan dengan menggunakan tools *Balsamiq Mockups* 3,

c. *Implementation and unit testing*

Implementation and unit testing akan dilakukan dengan mengubah tahap perancangan dan analisis yang telah dilakukan sebelumnya, kemudian diterjemahkan ke dalam bahasa pemrograman. Bahasa pemrograman yang digunakan adalah bahasa pemrograman *Visual C#* dengan menggunakan perangkat lunak Microsoft Visual Studio C# 2015.

3. Pengujian sistem

Pada tahap ini, akan dilakukan pengujian terhadap perangkat lunak dengan cara membandingkan citra medis asli dengan citra medis yang dihasilkan dari proses dekripsi menggunakan parameter MSE untuk menemukan nilai error kedua citra tersebut dan histogram.

Pengujian terhadap algoritma steganografi akan dilakukan menggunakan panjang kunci enkripsi yang berbeda yang kemudian akan disisipkan ke masing – masing citra sampul, serta mengukur apakah kualitas dari *stego image* telah memenuhi kriteria *imperceptibility* melalui parameter MSE (*Mean Square Error*) dan PSNR (*Peak Signal to Noise Ratio*).

4. Kesimpulan

Kesimpulan dari keseluruhan tugas akhir ini akan dilakukan berdasarkan hasil pengujian yang telah dilakukan pada tahap sebelumnya.