BAB I
PENDAHULUAN

1.1 Latar Belakang

Citra memuat nilai informasi yang penting dan rahasia, sehingga perlu dienkripsi agar hanya pihak berwenang yang memiliki kunci yang dapat mendekripsinya (Habutsu, et al., 1991). Salah satu algoritma kriptografi yang dapat digunakan untuk mengenkripsi citra adalah algoritma Serpent. Algoritma ini menggunakan teknik *cipher* blok dengan kunci simetris. Proses enkripsi ini dimulai dengan melakukan permutasi inisial lalu diikuti sebanyak 32 putaran pada transformasi substitusi dan kemudian permutasi akhir (Taher, et al., 2014). Algoritma ini memiliki tingkat keamanan yang sebanding dengan *Advanced Encryption Standard* (AES) namun lemah dari segi kecepatan dikarenakan lebih banyak jumlah putaran yang dibutuhkan (Elkamchouchi, et al., 2018). Untuk mengurangi waktu yang diperlukan dalam proses enkripsi dekripsi, Elkamchouchi et al (2018) melakukan modifikasi pada algoritma Serpent dengan memanfaatkan sistem *chaos* dan *cyclic group*. Modifikasi ini mengubah proses transformasi substitusi byte (S-box) menjadi *list* bilangan prima 257 yang memiliki 128 *generator* untuk digunakan sebagai kunci di setiap putarannya. Dengan metode ini membuat waktu proses menjadi lebih cepat dan jumlah iterasi yang dibutuhkan berkurang menjadi 10 putaran serta meningkatkan kompleksitas algoritma.

Kombinasi dari *chaos* dan *cyclic group* sendiri memiliki nilai parameter berupa λ dan x awal yang digunakan untuk memperoleh *cyclic group sub-byte* sebagai pengganti s-box. Pada penelitian Elkamchouchi et al (2018) tidak dilakukan pengujian apakah kunci dan nilai parameter berpengaruh pula terhadap waktu eksekusi. Sehingga perlu dilakukan pengujian untuk mengetahui pengaruh perubahan kunci dan parameter pada metode *Modified Serpent* terhadap kecepatan waktu proses enkripsi dan dekripsi.

Namun, pengenkripsian saja tidaklah cukup karena akan menimbulkan kecurigaan sehingga informasi akan rentan dicuri sehingga diperlukan teknik steganografi untuk menyembunyikan pesan atau informasi ke dalam suatu media tertentu agar pihak lain tidak mengetahui keberadaan pesan tersebut (Singh & Agarwal, 2010). Metode steganografi yang digunakan adalah *Integer Wavelet Transform* (IWT) yang merupakan teknik transformasi domain. Metode ini muncul untuk mengatasi kelemahan terhadap *robustness* dan *imperceptibility* yang ada pada *Least Significant Bit* (LSB) karena hasilnya tampak mirip dengan citra asli, tetapi dengan ukuran yang lebih kecil (Safy, et al., 2009). Metode ini

menciptakan *noise* yang lebih sedikit setelah proses penyisipan dikarenakan bahwa transformasi tersebut memberikan toleransi yang tinggi terhadap *noise* citra (Jayasudha, 2013).

Pada proses penyisipan dengan metode IWT, perlu ditentukan posisi piksel pada cover *image* yang akan disisipkan sebuah pesan. Untuk menentukan posisi tersebut, maka digunakanlah fungsi *chaos*. Karakteristik *chaos* adalah sensitivitas terhadap kondisi awal, berkelakuan acak, dan tidak memiliki periode berulang. *Logistic map* merupakan salah satu fungsi *chaos* yang banyak digunakan dalam teknik penyisipan data karena sederhana dan sangat cepat tetapi fungsi ini sendiri memiliki ruang kunci yang kecil (Bilal, et al., 2013). Permasalahan ruang kunci merupakan faktor penting dalam metode keamanan (Subhedar & Mankar, 2014). Valandar et al (2017) melakukan sebuah modifikasi pada *logistic map* untuk meningkatkan ruang kunci dengan menambahkan tiga variabel sebagai parameter baru berupa α, β, dan γ. Variabel tersebut sangat bergantung dengan variabel lainnya sehingga nilai yang dimasukkan berbeda sedikit saja, maka akan menghasilkan perubahan yang signifikan. Sehingga penentuan posisi piksel pun akan sangat acak untuk salah satu nilai yang berbeda. Maka dalam penelitian ini dilakukan pengujian dengan mengubah nilai parameter tersebut untuk melihat kualitas *cover image* yang dihasilkan setelah dilakukan penyisipan pesan.

Berdasarkan uraian di atas, maka topik ini diangkat sebagai tugas akhir dengan judul **"Pengamanan Citra Warna Menggunakan Kriptografi *Modified Serpent* Dan Steganografi IWT Dengan *Modified Logistic Chaotic Map*"**

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka yang akan menjadi rumusan masalah dalam tugas akhir ini adalah:

1. Bagaimana pengaruh perubahan kunci dan parameter terhadap kecepatan waktu proses enkripsi-dekripsi pada *Modified Serpent*.
2. Bagaimana pengaruh perubahan nilai parameter *Modified Logistic Chaotic Map* pada saat dilakukan penyisipan pesan dengan metode IWT.

1.3 Tujuan

Tujuan tugas akhir ini yaitu sebagai berikut:

1. Membangun sistem untuk menguji perubahan kunci dan parameter terhadap kecepatan eksekusi pada metode *Modified Serpent* dan menguji perubahan nilai parameter *Modified Logistic Chaotic Map* pada saat dilakukan penyisipan pesan.

2. Membangun program dengan menggunakan *Modified Serpent*, IWT dan *Modified Logistic Chaotic Map* untuk pengamanan citra digital berwarna.

1.4 Manfaat

Manfaat yang diperoleh dari penyusunan tugas akhir ini adalah

1. Perangkat lunak yang dibangun dapat digunakan sebagai alat alternatif untuk mengamankan citra.
2. Laporan tugas akhir dapat dijadikan referensi untuk pengembangan aplikasi pengamanan citra.

1.5 Batasan Masalah

Batasan masalah yang terdapat pada penulisan tugas akhir ini adalah:

1. Citra sampul (*cover image*) berformat .jpg, .png, dan .bmp dengan ukuran minimal piksel 512 dan ukuran panjang dan lebar piksel genap.
2. *Input* pesan rahasia berupa *file* citra RGB berformat .jpg, .png, dan .bmp.
3. *Input* pesan rahasia berukuran maksimal panjang (panjang citra *cover* / 4) dan lebar (lebar citra *cover* / 4) piksel.
4. Metode *Modified Serpent* menggunakan kunci 256 bit.
5. Nilai parameter λ *logistic map* yang digunakan pada metode *Modified Serpent* adalah $3{,}9 < \lambda < 4$.
6. Nilai parameter α, β, dan γ *Modified Logistic Chaotic Map* pada steganografi adalah interval $0{,}5 \leq \alpha, \beta, \gamma \leq 4$.
7. Nilai parameter inisial x, y dan z *Modified Logistic Chaotic Map* pada steganografi adalah $0 < x, y, z < 1$

1.6 Metodologi Penelitian

Langkah-langkah metodologi penelitian yang digunakan dalam penyusunan tugas akhir ini:

1. Pengumpulan dan mempelajari data tentang algoritma *Modified Serpent*, IWT dan *Modified Logistic Chaotic Map* melalui buku, jurnal, *internet* dan sumber lainnya, agar dapat memahami proses kerja dari metode yang digunakan.

2. Membuat aplikasi dengan model *waterfall*
    a. Analisis kebutuhan

       Membuat analisis kebutuhan fungsional menggunakan *usecase* diagram, *non-*fungsional menggunakan PIECES.
    b. Perancangan

       Merancang *user interface* dari perangkat lunak dengan *Balsamiq Mockup.*
    c. Penulisan program

       Melakukan penulisan program berbasis desktop menggunakan bahasa pemograman *Visual* C#.*Net*.
    d. Pengujian
        i. Melakukan pengujian kecepatan waktu proses enkripsi - dekripsi citra pesan terhadap perubahan kunci dan parameter pada *Modified Serpent*.
        ii. Menguji sensitivitas kunci terhadap perubahan nilai parameter *Modified Logistic Chaotic Map* serta mengukur kualitas citra dengan menghitung nilai *Mean Square Error* (MSE) dan *Peak Signal-to-Noise Ratio* (PSNR). Citra awal dan citra stego yang diuji adalah citra dengan ukuran 512 x 512 piksel.
3. Menarik kesimpulan dari hasil pengujian.