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. 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 subsitusi dan kemudian permutasi akhir (Taher, El_Deen, & Abo-Elsoud, 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, Takieldeen, & Shawky, 2018). Untuk mengurangi waktu yang diperlukan dalam proses enkripsi dekripsi, dilakukan modifikasi pada algoritma Serpent dengan memanfaatkan sistem *chaos* dan *cyclic group*. Modifikasi ini mengubah proses transformasi substitusi byte (DES 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 (Elkamchouchi, Takieldeen, & Shawky, 2018).

Namun, pengenkripsian saja tidaklah cukup karena akan menimbulkan kecurigaan sehingga informasi akan rentan dicuri. Maka diperlukan teknik steganografi untuk menyembunyikan pesan atau informasi ke dalam suatu media tertentu agar pihak lain tidak mengetahui keberadaan pesan tersebut (Lestari, Nurmaesa, & Mariana, 2017). 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). Kemudian digunakan IWT karena hasilnya tampak mirip dengan citra asli, tetapi dengan ukuran yang lebih kecil. 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 bit dan 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 (Jan, Parah, & Malik, 2021). Permasalahan ruang kunci merupakan faktor penting dalam metode keamanan (Ulker & Arslan, 2018). Untuk meningkatkan keamanan, dilakukan sebuah modifikasi pada *logistic map* untuk meningkatkan ruang kunci dengan menambahkan tiga variabel baru berupa α,β,dan γ sebagai parameter baru. Variabel tersebut sangat bergantung dengan variabel lainnya sehingga nilai yang dimasukkan berbeda sedikit saja, maka akan menghasilkan perubahan yang signifikan (Valandar, Ayubi, & Barani, 2017).

Berdasarkan uraian di atas, maka topik ini diangkat sebagai tugas akhir dengan judul "**Pengamanan Citra Berwarna Menggunakan Kombinasi Kriptografi *Modified Serpent* dan Steganografi IWT dengan *Modified Logistic Chaotic Map***".

1.2 Perumusan Masalah

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

1. Bagaimana kecepatan waktu proses enkripsi dan dekripsi pada *Modified Serpent*.
2. Bagaimana pengaruh perubahan nilai parameter *Modified Logistic Chaotic Map* dalam penentuan posisi bit dan piksel saat penyisipan citra.

1.3 Tujuan dan Manfaat

Tujuan dari penyusunan penelitian ini adalah untuk membangun sistem pengamanan citra digital menggunakan algoritma kriptografi *Modified Serpent* dan steganografi IWT dengan *Modified Logistic Chaotic Map.*

Manfaat yang diperoleh dari penyusunan penelitian 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.

1.4 Pembatasan Masalah

Batasan masalah yang terdapat pada penulisan tugas akhir ini adalah:

1. *Input* pesan rahasia berupa *file* citra RGB berformat .jpg dan .bmp.
2. Media citra (*cover image*) berformat .bmp dengan ukuran 512 x 512 piksel.
3. Metode *Modified Serpent* menggunakan kunci 256 bit.
4. Nilai parameter *rlogistic map* yang digunakan pada metode *Modified Serpent* adalah $3{,}9 < r < 4$.
5. Nilai parameter α, β, dan γ pada *Modified Logistic Chaotic Map* adalah $0{,}5 \leq \alpha, \beta, \gamma \leq 4$.

1.5 Keterbaruan

Penelitian sejenis yang pernah dilakukan sebelumnya seperti "KOMBINASI STEGANOGRAFI BIT MATCHING DAN KRIPTOGRAFI PLAYFAIR CIPHER, HILL CIPHER DAN BLOWFISH" (Rauf, 2020). Pada penelitian ini, dilakukan pengujian untuk melihat waktu yang dipakai untuk melakukan kombinasi steganografi bit matching serta mengkombinasikan beberapa metode kriptografi seperti playfair, hill cipher dan blowfish. Hasilnya ialah untuk citra hitam putih diperoleh waktu rata-rata embedding 28.275 detik ekstraksi 27.843 detik dan untuk citra berwarna waktu rata-rata embedding 13.0208 detik dan ekstraksi 12,7986 detik.

Penelitian lainnya berjudul "IMPLEMENTASI ALGORITMA ENKRIPSI CITRA DIGITAL BERBASIS CHAOS MENGGUNAKAN FUNGSI KOMPOSISI LOGISTIC DAN GAUSS ITERATED MAP" (Kembaren, Suryadi, & Triswanto, 2018). Hasil uji PSNR terhadap semua citra asli dengan citra hasil dekripsi menujukkan bahwa nilai PSNR tak hingga, dan MSE bernilai nol, hal ini menunjukan bahwa citra asli dengan citra hasil dekripsi sama atau tidak berubah. Waktu proses enkripsi dan dekripsi citra grayscale relatif lebih cepat daripada citra warna. Waktu proses enkripsi dan dekripsi juga bergantung pada ukuran pixel dari citra.

Penelitian lainnya "Proses Pengamanan Data Menggunakan Kombinasi Metode Kriptografi Data Encryption Standard dan Steganografi End Of File"

(Darwis, Wamiliana, & Junaidi, 2017). Berdasarkan hasil pengujian yang dilakukan pesan rahasia berhasil dienkripsi dengan menggunakan panjang kunci 56 bit kemudian disisipkan pada citra digital menggunakan EOF dan memiliki hasil pengujian bahwa pesan yang disisipan dapat diambil kembali untuk dapat dilakukan proses dekripsi.