BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi komunikasi saat ini, semakin mendorong banyaknya metode kriptografi dan steganografi yang diusulkan untuk mencegah kebocoran informasi data multimedia salah satunya adalah citra. Secara khusus, sifat dari citra yaitu *volume* data massal, korelasi yang tinggi antar *pixel* yang berdekatan dan redudansi tinggi (Liu, et al., 2018). Citra juga memiliki kapasitas data yang besar dan korelasi yang kuat antar *pixel* sehingga teknik enkripsi tradisonal kurang baik untuk pengamanan citra (Suri & Vijay, 2018) (Panwar & Purwar, 2019). Beberapa penelitian mengusulkan penerapan kombinasi dari teori *chaos* dan kriptografi (Zhang, et al., 2018). Kriptografi DNA (*Deoxyribonucleic Acid*) merupakan salah satu kriptografi yang memberikan sekuritas dua lapis. Lapisan pertama menggunakan teknologi biologis dan *cryptosystem* sedangkan lapisan kedua menggunakan karakteristik DNA (Anam, et al., 2010) (Biswas, et al., 2017).

Beberapa penelitian pengamanan citra diantaranya (Chai, et al., 2018) menerapkan *cryptosystem* citra warna menggunakan kriptografi DNA dan *chaos*. Penelitian tersebut menghasilkan sensitivitas kunci yang tinggi dari perhitungan nilai awal pada sistem *chaos* dan analisis kinerja enkripsi menunjukkan keamanan dan ketahanan yang lebih baik. Kelemahannya terletak pada proses enkripsi citra yang membutuhkan banyak waktu. Untuk mengatasi kelemahan tersebut (Stalin, et al., 2019) melakukan penelitian enkripsi citra menggunakan kombinasi *Logistic Map* dan DNA *sequences*. Penelitian tersebut memberikan kinerja yang lebih baik berdasarkan keamanan, kualitas, ketahanan terhadap serangan, dan waktu proses yang lebih cepat. Kelemahan penelitian tersebut menunjukkan *noise* pada *pixel* yang dapat mempengaruhi kualitas citra ketika didekripsi. Untuk menutupi kelemahan tersebut (Iqbal, et al., 2020) melakukan penelitian implementasi metode *Arnold's Cat Map* dan *Logistic Map* pada proses enkripsi dan dekripsi untuk keamanan citra. *Arnold's Cat Map* bekerja dengan mengacak *pixel* secara terus menerus hingga menjadi bentuk yang tidak beraturan. *Logistic Map* memiliki sensitivitas yang baik untuk mengenkripsi citra dengan membangkitkan *keystream* yang selanjutnya dienkripsi dengan *pixel* hasil permutasi. Hasil enkripsi dari metode *Arnold's Cat Map* dan *Logistic Map* menunjukkan citra yang sulit dibedakan serta memiliki keamanan yang lebih baik.

Citra yang telah dienkripsi menggunakan kriptografi DNA, *Arnold's Cat Map* dan *Logistic Map* akan menghasilkan citra acak yang dapat menimbulkan kecurigaan bagi pihak lain. Untuk mengatasi masalah tersebut maka dilakukan penyembunyian citra pesan ke dalam suatu media berupa amplop dengan teknik steganografi. Teknik steganografi dan IHWT (*Integer Haar Wavelet Transform*) dapat meningkatkan ketahanan sambil mempertahankan kualitas visual *stego-image* (Ramalingam & Isa, 2014). Salah satu penelitian (Abu, et al., 2014) menggabungkan teknik *Coefficient Difference* dan IHWT. Metode tersebut menghasilkan *stego-image* yang baik dengan nilai PSNR (*Peak Signal to Noise Ratio*) diatas 40 dB. Namun kelemahan *Coefficient Difference* ada pada besarnya jumlah modifikasi nilai *pixel* antara dua *pixel* bertetangga yang membuat *imperceptibility* dari *stego-image* menurun (Adi, et al., 2015).

Pada tahun 2015, Adi et al. melakukan penelitian untuk menutupi kelemahan pada *Coefficient Difference.* Penelitian tersebut membandingkan kualitas *stego-image* menggunakan *Coefficient Difference* dengan *Modulus Function*. Hasilnya menunjukkan nilai PSNR dan SSIM (*Structural Similarity Index Measure*) dari *Modulus Function* lebih tinggi dibandingkan dengan *Coefficient Difference*. Besarnya jumlah modifikasi *pixel* antara dua *pixel* bertetangga pada *Coefficient Difference* dapat diperkecil dengan *Modulus Function*. Penelitian (Purba, et al., 2019) menggunakan IHWT dengan *Modulus Function* karena hasil yang dicapai *Modulus Function* lebih baik dari *Coeffiecient Difference*. Untuk meningkatkan ketahanan *stego-image* dari variasi serangan, IHWT dengan *Modulus Function* akan dikombinasi dengan ruang warna YCoCg-R. Ruang warna YCoCg-R memiliki kenaikan minimal dalam *dynamic range* dan tingginya *coding gain* dibandingkan dengan ruang warna lain (Malvar & Sullivan, 2003). Beberapa penelitian (Roy, et al., 2015) (Moosaszadeh & Ekbaranifard, 2016) (Ernawan, 2019) menggunakan ruang warna YCoCg-R untuk menghasilkan peningkatan *imperceptibility* dan ketahanan *stego-image* dari variasi serangan.

Berdasarkan uraian di atas, maka topik ini diangkat sebagai tugas akhir dengan judul **"Pengamanan Citra Warna Menggunakan Kriptografi DNA dan IHWT dengan *Modulus Function* pada Ruang Warna YCoCg-R"**.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka yang menjadi permasalahan sehingga penelitian berikut dilakukan adalah:

1. Pengaruh kunci kriptografi DNA, *Arnold's Cat Map* dan *Logistic Map* terhadap kualitas hasil citra ketika didekripsi.

2. Tingkat *imperceptibility stego-image* dari proses penyisipan dengan IHWT dan *Modulus Function* pada ruang warna YCoCg-R.
3. Tingkat ketahanan *stego-image* dari serangan *noise salt & pepper* dari proses penyisipan dengan IHWT dan *Modulus Function* pada ruang warna YCoCg-R.

1.3 Tujuan

Tujuan dari tugas akhir adalah:

1. Membangun aplikasi pengamanan citra warna menggunakan kriptografi DNA, *Arnold's Cat Map, Logisctic Map*, IHWT dan *Modulus Function* pada ruang warna YCoCg-R untuk memberikan keamanan citra digital.
2. Mengetahui tingkat keamanan dan ketahanan citra dari aplikasi yang dibangun dengan menggunakan kriptografi DNA, *Arnold's Cat Map, Logisctic Map*, IHWT dan *Modulus Function* pada ruang warna YCoCg-R.

1.4 Manfaat

Manfaat yang diharapkan dari tugas akhir berikut adalah:

1. Aplikasi yang dibangun dapat menjadi alternatif dalam pengamanan citra.
2. Hasil pengujian dapat digunakan untuk mengetahui tingkat keamanan dari kombinasi kriptografi DNA dan steganografi IHWT dengan ruang warna YCoCg-R.
3. Laporan tugas akhir dapat digunakan sebagai referensi dalam pengembangan aplikasi keamanan citra.

1.5 Batasan Masalah

Batasan masalah dari tugas akhir berikut adalah:

1. Citra pesan dan *cover image* yang digunakan sebagai inputan merupakan citra RGB 24 bit dengan format .bmp.
2. Citra pesan adalah citra persegi dengan ukuran minimal 50 x 50 *pixel* dan maksimal 200 x 200 *pixel.*
3. Kunci *Arnold's Cat Map* untuk kunci b berada pada rentang 100 sampai 500, kunci c berada pada rentang 100 sampai 500, kunci i berada pada rentang 10 sampai 100.
4. *Threshold* pada *Modulus Function* bernilai 2 dan 3.
5. Ukuran *cover image* sebagai berikut:

$$Ukuran\ citra\ cover\ (x,y) = \left\lceil \sqrt{\frac{n \times m \times 8 \times 2}{T}} \right\rceil \times 2$$

Dimana:

Ukuran citra cover (x,y) = Nilai panjang *pixel* dan lebar *pixel cover image*

n = Panjang *pixel* citra pesan

m = Lebar *pixel* citra pesan

T = Nilai *Threshold*

6. Persentase *noise salt and pepper* berada pada rentang 0.005% sampai 0,015%.

1.6 Metodologi Penelitian

Metodologi penelitian yang digunakan pada penyusunan tugas akhir ini menggunakan model *waterfall. Waterfall* merupakan metodologi yang sistematis karena tiap proses harus diselesaikan terlebih dahulu agar dapat menjalankan proses selanjutnya, sehingga menghasilkan kualitas sistem yang baik dan proses pemeliharaan yang lebih mudah. Berikut tahapan dalam *waterfall* (Davis, 2013):

1. Mempelajari referensi

   Pada tahap ini mengumpulkan dan mempelajari referensi yang berhubungan dengan topik tugas akhir dengan tujuan untuk memahami proses dan metode yang digunakan.

2. Analisis proses

   Melakukan perhitungan secara manual dengan contoh masalah sederhana sesuai dengan *flowchart* yang sudah dirancang.

3. Analisis Kebutuhan

   Melakukan analisis kebutuhan sistem berupa kebutuhan fungsional menggunakan *use case* dan kebutuhan non-fungsional memanfaatkan PIECES (*Performance, Information, Economy, Control, Efficiency, Service*).

4. Perancangan

   Melakukan perancangan *user interface* menggunakan Balsamiq Wireframes 4.2.7.

5. Implementasi

   Melakukan penulisan kode program berbasis desktop menggunakan Visual Studio 2019 C# .Net.

6. Pengujian

Melakukan pengujian untuk memastikan perangkat lunak yang dibuat berjalan sesuai fungsionalitasnya.

a. Melakukan pengujian terhadap sensitivitas kunci DNA, *Arnold's Cat Map, Logistic Map* saat proses dekripsi.
b. Melakukan pengujian terhadap tingkat *imperceptibility* citra rahasia sebelum dan sesudah steganografi menggunakan MSE dan *Peak Signal-to-Noise Ratio* (PSNR).
c. Melakukan pengujian terhadap ketahanan *stego-image* dari serangan *noise salt and pepper* menggunakan *recovery rate.*

7. Penarikan kesimpulan dari hasil pengujian

Penarikan kesimpulan berdasarkan hasil pengujian yang telah dilakukan.