BAB I
PENDAHULUAN

1.1 Latar Belakang

Citra digital merupakan informasi yang mengandung berbagai macam informasi di dalamnya (Zebua & Ndruru, 2017). Hal ini mengakibatkan data citra memiliki kerentanan untuk dibobol lebih besar dibandingkan dengan data teks. Tindakan penyadapan dan penyalahgunaan terhadap citra yang sifatnya rahasia tentu saja dapat merugikan pihak pemilik citra, sehingga memunculkan berbagai permasalahan keamanan (Simangunsong & Komariah, 2018). Oleh karena itu, untuk menghindari hal tersebut terjadi pada citra maka diperlukan sistem pengamanan untuk melindungi kerahasiaan citra digital (Permana, et al., 2017). Salah satu metode yang dapat mengamankan citra adalah metode *chaotic*.

Penerapan sistem *chaotic* (kacau) menghasilkan efek difusi (pendistribusian *pixel*) sebagai pembangkit bilangan acak yang digunakan untuk pembentukan *keystream*. Struktur enkripsi yang rumit pada *chaotic system* membuat citra sulit dianalisis sehingga dapat memberikan keamanan yang lebih baik (Bao & Zhou, 2012). Sifat *chaos* yang sensitif terhadap kondisi awal ditunjukkan dengan *cipher image* yang didekripsi tidak kembali ke citra semula jika kunci yang digunakan tidak sama dengan kunci sewaktu proses enkripsi dilakukan (Purba, et al., 2014). Pada penelitian sebelumnya yang dilakukan oleh (Munir, 2012), menggunakan *Arnold's Cat Map* (ACM) untuk mengacak susunan *pixel* dan *Logistic Map* untuk mengubah nilai *pixel*. Hasil analisis menunjukkan *cipher image* tidak dapat dikenali dan nilai *pixel*nya tidak saling berhubungan, namun kriptografi berbasis *Logistic Map* memiliki ruang kunci yang kecil dan keamanan yang lemah (Gao, et al., 2006). Oleh karena itu, metode *chaotic* yang akan digunakan dalam penelitian ini adalah *Zaslavsky chaotic map*.

Zaslavsky chaotic map memiliki ruang kunci berukuran besar dan sensivitas yang tinggi terhadap perubahan *secret key*. Pada algoritma *Zaslavsky* akan dikombinasikan dengan algoritma *Grain-128* untuk meningkatkan kemananan dan sensivitas proses enkripsi terhadap setiap perubahan kunci pada *secret key* (Balaska, et al., 2019). Algoritma ini diterapkan pada *secret key* 128 bit dengan hasil akhir yang diperoleh akan dibentuk sebagai parameter yang digunakan pada *Zaslavsky chaotic map*. Metode ini dapat menghasilkan bilangan *real* acak dan menunjukkan perilaku *chaotic* (kacau) pada setiap perubahan kunci enkripsi. Secara khusus, algoritma ini memiliki tingkat keamanan dan sensitivitas yang tinggi serta memiliki periode berulang. Hal tersebut dapat dibuktikan dari hasil penelitian yang dilakukan oleh (Hamza & Titouna, 2016) bahwa *Zaslavsky* memiliki skor yang tinggi (NPCR = 99,61%,

UACI = 33,47%, *entropy* (*Cipher Image*) ≃ 8, dan koefisien korelasi ≃ 0) dengan memastikan sifat kebingungan yang baik serta menghilangkan koefisien korelasi dari citra asli. Namun citra yang telah diamankan menggunakan *Zaslavsky chaotic map* akan menghasilkan citra acak sehingga dapat menimbulkan kecurigaan dan mudah dideteksi oleh pihak lain. Untuk mengatasi masalah tersebut, maka dilakukan penyembunyian citra rahasia ke dalam suatu media yang disebut steganografi. Hasil penyisipan menggunakan steganografi tidak mengalami perubahan yang signifikan sehingga akan terlihat sama dengan aslinya (Laoli, et al., 2020). Salah satu metode steganografi adalah CD (*Coefficient Difference*) yang diadopsi dari PVD (*Pixel Value Differencing*) yang melakukan penyembunyian pada domain spasial menggunakan selisih dari 2 nilai *pixel* sehingga menghasilkan jumlah modifikasi nilai *pixel* yang besar, membuat tingkat *impercepbility* menurun (Purba, et al., 2019). Metode LSB *(Least Significant Bit)* digunakan untuk mengatasi kelemahan pada CD (*Coefficient Difference*) sehingga meningkatkan tingkat *imperceptibility*.

Proses *LSB (least significant bit)* dilakukan dengan mengambil bit-bit terakhir warna pada citra dan mengganti dengan bit-bit data (Syawal, et al., 2016). Berdasarkan penelitian yang pernah dilakukan oleh (Laila & Sindar RMS, 2018) metode *LSB* diusulkan karena memiliki keunggulan, yaitu sederhana, cepat dalam melakukan penyisipan dan ekstraksi pesan, serta mempunyai kapasitas penyimpanan yang besar. Penelitian mengenai steganografi teknik *LSB* juga pernah dilakukan oleh beberapa orang diantaranya (Nabila Nidia, et al., 2021) yang membahas tentang penerapan metode *LSB* dan *Discrete Cosine Transform* dalam implementasi steganografi pada citra warna 24 bit, dengan hasil yang diperoleh komparasi *robustness* yaitu ketahanan citra terhadap berbagai operasi manipulasi yang dilakukan pada citra penampung dengan mengubah tingkat *brightness* dan kontras citra dari *watermark* yang diukur menggunakan PNSR dan MSE, diperoleh bahwa penggunaan metode LSB lebih baik dari pada DCT karena hasil antara citra sampul dan *stego-image* tidak jauh berbeda. Dan untuk meningkatkan kemananan pada citra maka proses LSB akan ditambahkan dengan metode *hybrid* dimana proses LSB akan ditambahkan dengan proses seleksi *pixel* acak menggunakan generator modulo yang berfungsi untuk meningkatkan keamanan dan kerahasiaan citra, proses ini akan menghasilkan posisi penyisipan bit secara acak yang bergantung pada ukuran citra sampul dan digunakan untuk menyembunyikan *cipher-image* sehingga hasilnya akan terlihat sama dengan citra asli.

Penelitian dilakukan untuk mengetahui tingkat keacakan bit pada proses enkripsi dan pengaruh dari parameter masukan jumlah bit sisip yang digunakan dalam proses penyisipan

terhadap tingkat *imperceptibility* dari *stego-image*. Berdasarkan uraian di atas, maka disusunlah tugas akhir dengan judul **"Pengamanan Citra Warna Menggunakan Algoritma *Zaslavsky Chaotic Map* dan Steganografi *Hybrid LSB*".**

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka yang menjadi permasalahan adalah:

1. Seberapa besar tingkat keacakan bit pada *cipher-image* yang telah dienkripsi menggunakan *Zaslavsky Chaotic Map*.
2. Seberapa besar tingkat *imperceptibility* dari *Hybrid Least Significant Bit* berdasarkan parameter jumlah bit sisip terhadap citra sampul.

1.3 Tujuan

Tujuan dari tugas akhir ini adalah:

1. Membangun aplikasi untuk pengamanan citra digital dengan mengkombinasikan algoritma *Zaslavsky Chaotic Map* dan steganografi *Hybrid Least Significant Bit* serta mengetahui tingkat keamanan dan kerahasiaan pesan citra yang dilindungi dengan menggunakan *Zaslavsky Chaotic Map*.
2. Mengetahui tingkat *imperceptibility* dari *Hybrid Least Significant Bit* berdasarkan parameter jumlah bit sisip terhadap citra sampul.

1.4 Manfaat

Adapun manfaat yang diharapkan dari tugas akhir ini adalah:

1. Dapat digunakan sebagai aplikasi alternatif pengamanan citra.
2. Dapat dikembangkan dan dijadikan bahan referensi pada penelitian pengamanan citra selanjutnya.

1.5 Batasan Masalah

Adapun batasan masalah dari tugas akhir ini adalah:

1. Citra pesan dan citra sampul yang digunakan sebagai inputan merupakan citra RGB 24 bit dengan format bmp (**.bmp)*.
2. Citra pesan merupakan citra persegi dengan ukuran minimal 50 x 50 *pixel* dan maksimal 100 x 100 *pixel*.
3. Citra sampul didapatkan dari perhitungan $\left\lceil \sqrt{\frac{Panjang\ citra\ rahasia\ x\ lebar\ citra\ rahasia\ x\ 24}{Jumlah\ bit\ sisip}} \right\rceil$

4. Algoritma penyisipan yang digunakan adalah *Hybrid LSB* dengan seleksi *pixel* acak menggunakan generator modulo.
5. Nilai *phi* pada algoritma *Zaslavsky Chaotic Map* yang digunakan adalah 3,141592653589.
6. Dalam satu kali proses hanya dapat memilih salah satu jumlah bit sisip, yaitu 1, 2, dan 4 bit.
7. Panjang kunci untuk proses enkripsi adalah minimal 5 dan maksimal 16 karakter dengan menggunakan algoritma *Grain-128*.

1.6 Metodologi Penelitian

Metodologi yang digunakan dalam penelitian ini adalah metode *waterfall*. Berikut tahapan proses yang harus digunakan (Pressman, 2002)**:**

1. Pengumpulan Data

   Pada tahap ini dilakukan pengumpulan referensi yang diperlukan dalam penelitian. Referensi tersebut dapat berupa buku, jurnal, artikel, maupun hasil penelitian terdahulu yang kemudian ditinjau kembali untuk memperoleh hasil informasi yang berkaitan dengan pengamanan citra warna menggunakan algoritma *Grain-128, Zaslavsky Chaotic Map* dan *Hybrid Least Significant Bit*.
2. Analisis Kebutuhan Sistem

   Pada tahap ini dilakukan identifikasi dan pemodelan kebutuhan sistem dengan memodelkan kebutuhan fungsional menggunakan *usecase diagram* dan nonfungsional sistem menggunakan metode PIECES (*Performance, Information, Efficiency, Control, Economy, Service*) dan menggambarkan alur proses sistem menggunakan *Flowchart*.
3. Perancangan Sistem

   Pada tahap ini dilakukan perancangan *user interface* dari perangkat lunak dengan menggunakan aplikasi Balsamiq Mockup.
4. Penulisan Program

   Pada tahap ini dilakukan penulisan kode program dengan menggunakan bahasa pemrograman C# pada Microsoft Visual Studio 2015 berbasis desktop.
5. Pengujian
   a. Melakukan pengujian terhadap kualitas *plain-image* dengan *chiper-image* yang telah dienkripsi menggunakan *Zaslavsky Chaotic Map* dengan melakukan perhitungan nilai *Number of Pixels Change Rate (NPCR)*, *Unifer Average Changing Intensity* (UACI), koefisien korelasi, dan *entropy* untuk mengetahui tingkat perubahan,

interval perbedaan nilai *pixel* dan mengukur hubungan antara *plain-image* dan *cipher-image* serta mengukur kualitas dari citra.

b. Melakukan pengujian terhadap kualitas *stego-image* yang telah dilakukan penyisipan menggunakan steganografi *Hybrid LSB* dengan melakukan perhitungan nilai MSE *(Mean Square Error)* dan PSNR *(Peak Signal to Noise Ratio)* untuk mengetahui perbandingan kualitas citra dari citra sampul dan *stego-image.*

6. Penyusunan laporan tugas akhir.