BAB 1
PENDAHULUAN

1.1 Latar Belakang

Semakin berkembangnya teknologi internet menyebabkan munculnya faktor terpenting dalam teknologi informasi dan komunikasi yakni keamanan informasi. Keamanan informasi mencegah adanya pihak yang tidak diinginkan dalam memperoleh informasi penting tersebut. Kriptografi adalah suatu teknik dalam pengamanan kerahasiaan komunikasi dan merupakan metode dalam mengenkripsi maupun mendekripsi data agar kerahasiaan data terjaga. Salah satu contoh data tersebut adalah citra digital. Algoritma enkripsi citra digital berbeda dengan algoritma enkripsi data. Algoritma enkripsi tradisional tidak dapat diaplikasikan pada citra dikarenakan besarnya ukuran citra digital dan kuatnya korelasi antara *pixel* yang berdekatan.

Skema algoritma enkripsi citra yang baik yakni yang tahan terhadap beragam serangan seperti analisis statistik dan *brute-force attack.* Oleh karena itu, penelitian mengenai algoritma enkripsi terus dilakukan untuk menemukan suatu algoritma yang lebih baik. Algoritma yang banyak dikembangkan beberapa tahun belakangan adalah dengan metode pengacakan yang termasuk dalam *Chaotic Map,* contohnya algoritma *Arnold's Cat Map* & *Logistic Map. Chaotic Map* adalah algoritma yang sangat sensitif terhadap kondisi awal dan parameter kontrol membuatnya cocok untuk digunakan pada enkripsi citra jika dibandingkan dengan algoritma tradisional seperti AES, DES, dan RES[1]. Algoritma tradisional memiliki tingkat keamanan yang rendah dan kemampuan untuk menahan serangan yang lemah sedangkan *Chaotic Map* memiliki sifat acak atau *chaos* yang tidak dapat diprediksi, yakni seperti *noise.*

Pada penelitian sebelumnya [2][3] disimpulkan bahwa performansi pengacakan citra algoritma *Arnold's Cat Map* kurang baik jika dibandingkan dengan algoritma Kubus Rubik. Namun, pada penelitian ini, algoritma *Arnold's Cat Map* berdiri sendiri,

hanya mentransformasi *pixel*, dimana jika dilakukan pengulangan iterasi, maka akan muncul citra aslinya. Hal ini jauh jika dibandingkan dengan Kubus Rubik yang harus mengikuti langkah dekomposisi atau alur balik rotasi dari urutan tertentu.

Oleh karena itu, pada tugas akhir ini dibuat sebuah algoritma *Arnold's Cat Map* termodifikasi dengan salah satu contoh algoritma *Chaotic Map* yakni *Logistic Map* yang kemudian performansinya dibandingkan dengan algoritma Kubus Rubik.

1.2 Rumusan Masalah

Berdasarkan pada latar belakang tersebut, rumusan masalah pada tugas akhir ini adalah :

a. Bagaimana cara meningkatkan pengacakan pada algoritma *Arnold's Cat Map*?
b. Bagaimana penggabungan algoritma *Arnold's Cat Map* dengan *Chaotic Map*?
c. Bagaimana enkripsi dan dekripsi citra digital menggunakan algoritma *Arnold's Cat Map* dengan *Logistic Map* ?
d. Bagaimanakah perbandingan algoritma *Arnold's Cat Map* termodifikasi dengan algoritma Kubus Rubik pada enkripsi citra digital ?

1.3 Tujuan Penelitan

Tujuan dari pelaksanaan tugas akhir ini antara lain :

a. Menggabungkan algoritma ACM dengan algoritma *Chaotic Map.*
b. Melakukan simulasi enkripsi dan dekripsi citra digital menggunakan algoritma *Arnold's Cat Map* yang termodifikasi dengan *Logistic Map.*
c. Mengetahui perbandingan Algoritma *Arnold's Cat Map* termodifikasi dengan Algoritma Kubus Rubik pada enkripsi citra digital.

1.4 Batasan Masalah

Batasan masalah pada tugas akhir ini adalah :

a. Menggunakan simulasi Matlab.
b. Informasi yang dienkripsi adalah citra *grayscale* dengan ukuran 256×256.

c. Parameter performansi yang dibahas yakni *Bit Error Rate* (BER), waktu komputasi, analisis histogram, koefisien korelasi, PSNR, *avalanche effect*, *brute force attack*, dan *Mean Opinion Score* (MOS).

1.5 Metodologi Penelitian

Metodologi yang dilakukan di dalam pelaksanaan tugas akhir ini sebagai berikut :

1. Studi literatur

   Literatur dalam hal ini baik berupa buku, catatan, hasil penelitian, dan sumber-sumber elektronik di internet. Studi literatur ini ditujukan untuk mendapatkan referensi yang jelas dan tepat mengenai algoritma yang akan dibuat.

2. Implementasi Sistem

   Melakukan implementasi kombinasi algoritma dengan parameter serta skenario sesuai dengan yang sudah ditentukan di aplikasi Matlab.

3. Pengujian

   Pada tahap ini dilakukan pengujian terhadap sistem algoritma yang telah dibuat, kemudian dianalisis hasil dari data pengujian yang diperoleh.

4. Kesimpulan

   Penarikan kesimpulan dilakukan berdasarkan hasil analisis yang diperoleh dan kemudian dilakukan pembuatan laporan tugas akhir.

1.6 Sistematika Penelitian

Pada pelaksanaan tugas akhir ini terdapat lima bab utama serta lampiran yang bertujuan untuk menunjang kelengkapan informasi pada pelakasanaan tugas akhir ini. Adapun lima bab utama pada tugas akhir ini adalah :

BAB I PENDAHULUAN

Pada Bab ini berisi uraian secara singkat mengenai latar belakang permasalahan, perumusan masalah, tujuan penelitian, batasan masalah penelitian, metodologi penelitian serta sistematika penulisan.

BAB II DASAR TEORI

Bab ini berisi tentang teori dasar mengenai enkripsi citra, serta teori dasar mengenai kedua algoritma yang digunakan, dan parameter performansi dari sistem yang dibuat pada penilitan tugas akhir ini.

BAB III PERANCANGAN SISTEM

Bab ini menjelaskan tentang blok diagram, *flow chart*, serta dekripsi proses enkripsi-dekripsi dari kedua algoritma yang digunakan.

BAB IV SIMULASI DAN ANALISIS

Bab ini menjelaskan hasil simulasi, perbandingan kedua algoritma, dan analisis berdasarkan pengujian yang telah dilakukan.

BAB V PENUTUP

Bab ini berisi kesimpulan hasil simulasi dan analisis serta saran sebagai bentuk pengembangan penelitian yang lebih lanjut untuk dijadikan referensi.