BAB I
PENDAHULUAN

1.1 Latar Belakang

Perlindungan terhadap informasi atau data sangat dibutuhkan saat ini untuk menjaga kerahasiaannya. Oleh karena itu, perlu dilakukan perlindungan terhadap informasi dengan berbagai cara. Salah satu metode yang digunakan adalah enkripsi, dimana informasi dibuat sedemikian rupa agar tidak dapat dibaca atau diketahui oleh orang lain yang tidak diinginkan. Seiring dengan hal tersebut, maka diterapkan suatu cara yang dapat melindungi suatu data.

Pada tugas akhir ini, citra yang akan dianalisis adalah citra digital. Pada citra digital tersebut akan digunakan metode enkripsi baru yang memenuhi syarat dari segi keamanan pada citra tersebut.

Pada Tugas Akhir sebelumnya [11] didapat hasil bahwa dengan algoritma *Baker Map* untuk waktu enkripsinya lebih cepat dibanding dengan algoritma Cat Map dan dengan gabungan kedua algoritma tersebut. Begitu pula dengan waktu pemecahan kunci enkripsi menggunakan *Brute Force Attack*, untuk algoritma Baker Map waktu yang dibutuhkan lebih lama dibandingkan dengan algoritma Cat Map.

Tetapi ada satu kekurangan dalam penelitian tersebut, yaitu nilai *avalanche effect*-nya yang masih rendah. Oleh karena itu tugas akhir ini bertujuan untuk meningkatkan nilai *avalanche effect* dari algoritma Cat Map dengan menggunakan metode difusi berbasis *Pseudorandom Number Generator* . Sehingga akan didapatkan tingkat sekuritas yang lebih tinggi dari sebelumnya.

1.2 Tujuan dan Manfaat

Tujuan dan manfaat dari Tugas Akhir ini adalah untuk :

1. Mengimplementasikan sistem enkripsi dan dekripsi dari algoritma Cat Map.
2. Menerapkan difusi untuk algoritma Cat Map, yaitu dengan menggunakan *Pseudorandom Number Generator*
3. Membandingkan performansi *Pseudorandom Number Generator* dari enkripsi Cat Map.
4. Membandingkan *brute force attack* antara algoritma Cat Map dan algoritma Cat Map – Difusi.

5. Menganalisis performansi *avalanche effect* yang menggunakan difusi *Pseudorandom Number Generator* dengan yang tidak menggunakan difusi *Pseudorandom Number Generator.*

1.3 Rumusan Masalah

Masalah yang diteliti dalam tugas akhir ini yaitu :

1. Bagaimanakah proses enkripsi dengan menggunakan algoritma Cat Map.
2. Bagaimana memperbaiki Keamanan Cat Map khususnya *avalanche effect*.
3. Berapa waktu pemecahan kunci enkripsi (*Brute Force Attack*) yang dibutuhkan.
4. Berapa waktu yang dibutuhkan dalam proses enkripsi jika ditambahkan proses difusi.

1.4 Batasan Masalah

Batasan–batasan masalah yang digunakan dalam tugas akhir ini adalah:

1. Menggunakan MATLAB versi 7.5.0 (R2007b)
2. Citra yang digunakan adalah citra Grayscale/RGB (*Red,Green,Blue*).
3. Resolusi citra yang digunakan beresolusi 128x128, 256x256, 512x512, dan 1024x1024.
4. Citra yang digunakan berformat .bmp.
5. Iterasi yang digunakan: 2, 4, 6, 8, dan 10.

1.5 Metodologi Penelitian

Metode penelitian yang akan dilakukan pada penyusunan tugas akhir ini meliputi :

1. Studi literatur

   Dilakukan studi literatur dengan mengumpulkan bahan dan mempelajari konsep serta teori yang berhubungan dengan tugas akhir yang akan di bahas. Dengan materi konsep dan teori di dapat dari buku – buku, jurnal, serta tugas akhir yang berhubungan dengan masalah penelitian tugas akhir.

2. Pengumpulan data

   Pengumpulan data dilakukan dengan cara mengumpulkan *database* berupa citra *RGB* sebagai masukan dari sistem. Selain itu, pengumpulan data-data penunjang diperoleh dari *paper* pada daftar pustaka.

3. Tahap Perancangan

Perancangan sistem berdasarkan dari hasil studi literatur, pemodelan dari sistem tersebut diterjemahkan ke program simulasi dengan *software* Matlab.

4. Analisis hasil simulasi

   Setelah data diambil dari hasil simulasi, kemudian dilakukan analisis berdasarkan parameter yang telah ditentukan.

5. Penarikan hasil kesimpulan

   Mengambil kesimpulan akhir terhadap hasil simulasi dan memberi saran untuk penelitian selanjutnya. Pengambilan kesimpulan dilakukan dengan cara menarik kesimpulan berdasarkan analisis percobaan dan hasil simulasi.

1.6 Sistematika Penulisan

Pembahasan pada perancangan ini dibagi menjadi lima bab, dengan urutan sebagai berikut :

Bab I PENDAHULUAN

Pada bab I ini, dijelaskan mengenai latar belakang, tujuan penelitian, rumusan masalah, batasan masalah, dan metode pelaksanaan penelitian serta sistematika penulisan.

Bab II DASAR TEORI

Bab ini berisikan teori dasar mengenai citra digital, konsep enkripsi secara umum dan berisikan penjelasan mengenai algoritma Cat Map, *Pseudorandom Number Generator*, dan *Avalanche effect.*

Bab III PERANCANGAN DAN IMPLEMENTASI SISTEM ENKRIPSI DAN DIFUSI CITRA

Bab ini berisikan pemodelan dan simulasi sistem enkripsi dengan masukan data berupa citra *RGB* dan kemudian dienkripsi dengan algoritma Cat Map menggunakan *software* Matlab, kemudian didifusikan dengan *Pseudorandom Number Generator.*

Bab IV PENGUJIAN SISTEM DAN ANALISIS HASIL

Bab ini berisi hasil penelitian dari hasil simulasi, beserta analisis performansi yang berhasil dicapai.

Bab V KESIMPULAN DAN SARAN

Bab ini berisi simpulan dari implementasi yang dilakukan serta saran untuk pengembangan penelitian.