BAB I
PENDAHULUAN

1.1 Latar belakang masalah

Perkembangan ilmu pengetahuan yang sangat pesat dewasa ini menyebabkan informasi menjadi barang yang sangat berharga. 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. Proses enkripsi adalah suatu proses untuk mengubah informasi yang dapat dibaca dengan mudah menjadi informasi yang tersembunyi yang sulit dibaca.

Salah satu jenis algoritma enkripsi yang baik untuk citra adalah algoritma *Baker Map*. Algoritma *Baker Map* bersifat permutasi, yaitu mengacak urutan data tanpa mengubah data tersebut. Algoritma ini sangat cocok untuk citra karena pada citra, dimensi data akan selalu tetap. Sedangkan DES adalah sebuah algoritma enkripsi sandi blok kunci simetrik dengan ukuran blok 64-bit dan ukuran kunci 56-bit. Algoritma yang sebelumnya dominan untuk enkripsi data elektronik. Ini sangat berpengaruh dalam kemajuan kriptografi modern di dunia akademis. DES telah ditarik sebagai standar oleh Institut Nasional Standar dan Teknologi[16].

Tugas Akhir yang berhubungan dengan IT Telkom sebelumnya yaitu **Perbandingan skema enkripsi antara metode gabungan Cat Map dan SDES dan metode gabungan Cat Map dan Permutasi Blok Acak untuk citra Digital[12].** Pada Tugas Akhir tersebut dilihat dari ketahanan terhadap brute force attack, metode enkripsi gabungan Cat Map dan Permutasi Blok Acak lebih tinggi dibandingkan dengan metode gabungan Cat Map dan SDES. Dan juga dalam penelitian tersebut, metode gabungan Cat Map dan Permutasi Blok Acak memiliki waktu enkripsi dan dekripsi lebih cepat dibandingkan dengan metode gabungan Cat Map dan SDES. Sehingga enkripsi SDES tidak cocok digunakan pada proses enkripsi citra digital karena butuh waktu yang lama.

Pada tugas akhir yang sudah pernah ada di IT Telkom, belum pernah dibuat simulasi dan perbandingan mengenai performansi antara DES dengan *Baker Map* untuk citra digital. Maka tugas akhir ini akan mensimulasikan perbandingan kriptografi simetri dengan algoritma *Baker Map* dan algoritma DES untuk citra digital serta menganalisa hasil yang didapatkan.

1.2 Tujuan Penelitian

Tujuan dari tugas akhir ini adalah:

1. Menghitung waktu komputasi yang diperlukan kedua algoritma tersebut dalam melakukan enkripsi untuk citra digital.
2. Menguji ketahanan kedua algoritma tersebut terhadap *Brute Force Attack* dan *Avalanche Effect.*
3. Mendapatkan nilai akurasi dekripsi dari kedua algoritma terhadap cipher yang terkena noise.
4. Mendapatkan nilai MOS dari kedua algoritma tersebut untuk mengetahui kualitas enkripsinya.

1.3 Rumusan masalah

Permasalahan yang dijadikan objek penelitian dalam Tugas Akhir ini adalah :

1. Berapa waktu komputasi yang diperlukan kedua algoritma tersebut dalam melakukan enkripsi untuk citra digital?
2. Bagaimana ketahanan kedua algoritma tersebut terhadap *Brute Force Attack* dan *Avalanche Effect*?
3. Bagaimana nilai akurasi dekripsi dari kedua algoritma terhadap cipher yang terkena noise?
4. Bagaimana kualitas enkripsi dari kedua algoritma tersebut dengan cahaya gelap dan terang berdasarkan nilai MOS?

1.4 Batasan Masalah

Batasan-batasan masalah pada tugas akhir ini adalah:

1. Menggunakan MATLAB versi R2009B
2. Algoritma yang digunakan adalah *Baker Map* dan algoritma DES.
3. Tidak membahas mengenai proses transfer data.
4. Data yang digunakan adalah citra digital *grayscale* dengan format jpg dengan resolusi gambar 800x600 piksel.
5. Pengujian algoritma dilakukan dengan menghitung waktu komputasi, menguji ketahanan terhadap *Brute Force Attack dan Avalance Effect*, akurasi dekripsi terhadap cipher yang terkena noise, serta nilai kualitas MOS dari kedua algoritma.
6. Noise yang digunakan untuk pengambilan data yaitu Gaussian dan Salt & Pepper dengan parameter noise 0.01, 0.05, 0.1. Untuk noise Rotate dengan 30, 45, 60 derajat dan untuk noise Scalling dengan skala 0.25, 0.5, 0.75.
7. Baker Map hanya menggunakan 5,10,15 iterasi.

1.5 Metodologi penyelesaian masalah

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 dibahas. Dengan materi konsep dan teori didapat dari buku – buku serta jurnal yang berhubungan dengan masalah penelitian tugas akhir.

2. Pengumpulan data

   Pengumpulan data dilakukan dengan cara mengumpulkan *database* berupa citra *RGB* sebagai masukan, dan di ubah menjadi *grayscale* 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 analisa 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 hal yang berkaitan dengan tugas akhir ini.

Bab III PERANCANGAN SISTEM DAN SIMULASI

Bab ini berisikan perancangan sistem dan realisasi algoritma *Baker Map* dan DES dengan masukan data berupa citra yang kemudian dienkripsi menggunakan simulasi algoritma yang disimulasikan dengan menggunakan program Matlab.

Bab IV PENGUJIAN SISTEM DAN ANALISIS

Bab ini membahas tentang hasil pengukuran dan analisis algoritma yang telah dibuat dengan parameter yang telah ditentukan dan menganalisis dari hasil pengukuran tersebut untuk dapat mengetahui performansi algoritma.

Bab V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari hasil perancangan dan saran-saran yang berupa tidak lanjut yang bisa dilakukan pada pengembangan selanjutnya.