BAB I
PENDAHULUAN

1.1 Latar Belakang

Seiring dengan perkembangan teknologi multimedia, informasi *visual* seperti citra dan video telah menjadi suatu jenis informasi yang banyak diakses selain informasi data teks. Untuk informasi yang bernilai sangat penting, proses pertukarannya harus memperhatikan aspek keamanan dan kerahasiaan. Salah satu metode untuk meningkatkan keamanan data adalah dengan teknik kriptografi,dimana data diolah menurut teknik tertentu sehingga menghasilkan suatu pola data dalam bentuk yang lain (*chiper text*) sebelum dikirimkan. Tetapi perlu diperhatikan bahwa citra maupun video memiliki sifat khusus yaitu merupakan data berukuran sangat besar jika dibandingkan dengan data teks. Oleh karena itu diperlukan suatu algoritma kriptografi yang mampu untuk melakukan pemrosesan pada data berukuran besar secara cepat dan juga menawarkan tingkat keamanan yang tinggi.

Algoritma kriptografi berbasis *Chaotic Kolmogorov Flows* merupakan teknik kriptografi simetris dan termasuk dalam algoritma *block chiper.* Algoritma ini merupakan algoritma kriptografi yang dirancang untuk melakukan proses enkripsi-dekripasi pada blok data berukuran besar seperti citra maupun video. Berdasarkan pengalaman dalam bidang kriptografi, teknik kriptografi simetris yang bersifat *block cipher* sangat cocok untuk mengenkripsi blok data berukuran besar, karena memiliki keunggulan dalam kecepatan pemrosesan dan tingkat keamanan yang tinggi[7,8]. Algoritma ini menggabungkan operasi permutasi berdasarkan suatu sistem *chaos* (*Kolmogorov Flows*) pada blok data berukuran besar (citra atau video) dengan operasi substitusi yang merupakan suatu *pseudo-random number generator* berbasis *shift register* yang disebut *Add With Carry* (AWC) *generator.* Kedua operasi pada algoritma kriptografi tersebut akan digabungkan dengan sebuah *Pseudo Random Number Generator* (PRNG) yang disebut R250 sebagai penyedia kunci bagi keseluruhan sistem.

1.2 Perumusan Masalah

Dalam penulisan Tugas Akhir ini perumusan masalah difokuskan pada beberapa hal, yaitu

a. Perancangan algoritma kriptografi dengan menggunakan bahasa pemrograman VHDL (*Very High Speed Integrated Circuit Hardware Description Language*).

b. Algoritma kriptogarfi berbasis *chaotic Kolmogorov Flows*

Algoritma ini merupakan teknik kriptografi simetris yang dikemukakan oleh Josef Scharinger[7, 8]. Algoritma ini terdiri dari tiga buah blok utama untuk proses enkripsi, yaitu Permutasi, Substitusi, dan Pseudo Random Number Generator (PRNG).

- Permutasi berfungsi untuk melakukan proses transposisi pada blok *pixel* citra sumber, tanpa merubah data dari tiap-tiap blok *pixel* itu sendiri. Jadi pada proses ini yang diubah adalah koordinat posisi dari tiap-tiap blok *pixel.*
- Substitusi merupakan proses pengacakan data dari citra input yang bertujuan untuk mereduksi korelasi antara input *plain text* dengan output *chiper text.*
- *Pseudo Random Number Generator* (PRNG) merupakan blok yang menjalankan fungsi *Internal Key Management*, yaitu menyediakan kunci bagi sistem.

Sedangkan untuk proses dekripsi juga memiliki 3 blok utama yang mempunyai fungsi *invers* dari ketiga blok proses enkripsi diatas.

Citra hasil proses enkripsi-dekripsi dapat dilihat pada gambar berikut :

Gambar 1.1 Citra Hasil Proses Enkripsi-Dekripsi

1.3 Maksud dan Tujuan

Tujuan dari pengerjaan Tugas Akhir ini adalah

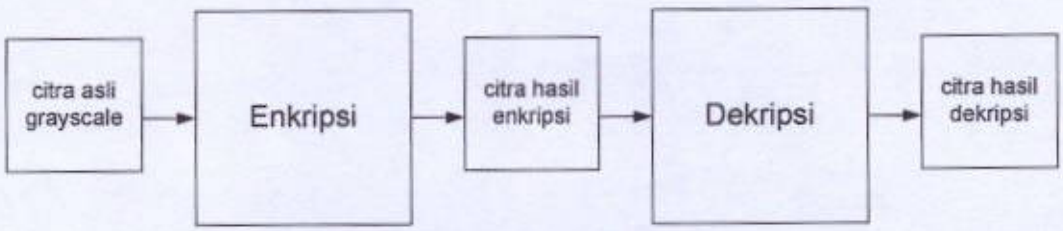
1. Melakukan perancangan sistem enkripsi-dekripsi berbasis *Chaotic Kolmogorov Flows* dengan VHDL dan mensimulasikannya.
2. Menganalisa kualitas output dari sistem yang telah dirancang
3. Mengetahui apakah citra yang telah dienkripsi dapat dikembalikan ke citra aslinya.
4. Membandingkan hasil implementasi dengan hasil penelitian sebelumnya tentang kriptografi menggunakan FPGA dalam hal efisiensi penggunaan CLB (*Configurable Logic Block*)

1.4 Pembatasan Masalah

Batasan masalah dalam Tugas Akhir ini adalah

1. Perancangan algoritma kriptografi berbasis *chaotic Kolmogorov flows* dengan menggunakan VHDL.
2. Citra sumber berupa citra *grayscale* format bitmap (*.bmp) dengan ukuran 64 x 64 *pixel.*
3. *Target device* yang digunakan adalah FPGA Xilinx Spartan-II XC2S100-5TQ144C.

Secara garis besar diagram blok dari sistem yang akan diimplementasikan seperti Gambar 1.2 berikut ini.



Gambar 1.2 Diagram Blok Sistem

1.5 Metode Penelitian

Metode penelitian yang dilakukan dalam penyusunan Tugas Akhir ini adalah

- Studi Literatur

Pencarian dan pengumpulan literatur yang langsung berkaitan dengan masalah-masalah yang ada pada Tugas Akhir ini, baik berupa artikel, buku referensi, internet, dan sumber-sumber lain.

- Perancangan Sistem

  Perancangan sistem yang sesuai dengan spesifikasi *Kolmogorov Chaotic System* dengan bahasa VHDL dengan bantuan software Active-HDL 3.5 dan Xilinx WebPack Project Navigator 5.1.

- Analisis Sistem

  Analisis dilakukan dengan mengamati dan menyimpulkan citra hasil keluaran dari sistem yang telah dirancang.

1.6 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam Tugas Akhir ini sebagai berikut :

- **BAB I PENDAHULUAN**

  Pada bab ini dibahas mengenai latar belakang permasalahan, perumusan masalah, maksud dan tujuan, pembatasan masalah,, metode penelitian serta sistematika penulisan pada Tugas Akhir ini.

- **BAB II DASAR TEORI**

  Bab ini menjelaskan teori tentang algoritma enkripsi berbasis *Chaotic Kolmogorov Flows*, HDL (*Hardware Description Language*) serta perangkat FPGA Xilinx Spartan-II XC2S100-5TQ144C.

- **BAB III PERANCANGAN SISTEM**

  Pada bab ini dibahas mengenai perancangan algoritma enkripsi berbasis *chaotic Kolmogorov flows* dengan menggunakan *software* VHDL.

- **BAB IV PENGUJIAN DAN ANALISA SISTEM**

  Pada bagian ini akan dijelaskan pengujian yang dilakukan terhadap sistem dan menganalisa hasil implementasi tersebut

- **BAB V KESIMPULAN DAN SARAN**

  Bab ini berisikan kesimpulan tentang pembuatan Tugas Akhir ini dan saran untuk pengembangan lebih lanjut.