BAB I
PENDAHULUAN

1.1 Latar Belakang

Universitas Telkom sedang mengembangkan teknologi satelit berukuran nano yang disebut satelit nano yang direncanakan untuk diluncurkan pada tahun 2015. Satelit nano yang dirancang membawa misi penginderaan jauh. Proses penginderaan jauh yang dilakukan diantaranya adalah akuisisi data, pemrosesan data, penyimpanan data, dan pengiriman data. Karena jarak satelit dari bumi cukup jauh dan media propagasi pengiriman data satelit dapat diakses oleh semua orang perlu metode untuk mengamankan data yang akan dikirimkan. Salah satu cara yang bisa dilakukan untuk melindungi data gambar adalah dengan melakukan enkripsi data gambar. Oleh karena itu perlu suatu algoritma enkripsi yang sudah tertanam ke dalam *On Board Computer*.

Dikarenakan tugas dari *On Board Computer* yang cukup berat yaitu sebagai pemroses data dan pengotrol dari satelit maka perlu suatu pemroses yang handal seperti FPGA. Karena metode enkripsi data tradisional seperti DES, IDEA dan RSA melihat data masukan sebagai aliran data maka tidak cocok untuk diimplementasikan pada data gambar. Hal ini disebabkan karena ukuran dari data gambar yang besar dan tingginya hubungan tiap pixel yang ada [1]. Oleh karena itu digunakanlah metode enkripsi berbasis *chaos* seperti Baker map. Namun karena panjang kunci dari metode Baker map terbatas pada ukuran panjang dari citra maka *key space* metode Baker map terbatas jumlahnya. Sehingga perlu suatu metode untuk menambahkan *key space* yang dimiliki. Berdasarkan pada *paper* karya Fengling Han *et al* cara yang dapat dilakukan untuk menambahkan ukuran *key space* dari Baker map adalah dengan mengganti kunci yang digunakan tiap kali iterasi [2].

Pada tugas akhir ini, akan digunakan metode yang diajukan oleh Fengling Han *et al* untuk menambah jumlah *key space* dari metode Baker map. Pada implementasinya akan digunakan citra RGB dan modul FPGA sebagai pengolah citra. Dengan diaplikasikannya metode ini ke dalam FPGA diharapkan dapat tercipta suatu metode Baker map dengan performa yang lebih baik dibandingkan dengan metode Baker map yang tidak ditingkatkan performansinya dan siap digunakan pada subsistem OBC pada satelit nano.

1.2 Tujuan Penelitian

Tujuan penelitian dalam tugas akhir ini adalah,

1. Mengimplementasikan metode Baker map pada FPGA,
2. Mengetahui hasil implementasi Baker map di FPGA, dari sisi kecepatan enkrispsi data maupun kehandalan data hasil enkripsi,
3. Mengetahui hasil dekripsi dari metode Baker map.

1.3 Rumusan Masalah

Rumusan masalah dalam tugas akhir ini adalah,

1. Bagaimana Mengimplementasikan metode Baker map ke dalam FPGA ?
2. Bagaimana hasil implementasi bakermap di FPGA dari sisi kecepatan enkripsi data maupun kehandalan data ?
3. Bagaimana hasil dekripsi baker map ?

1.4 Batasan Masalah

Batasan masalah dalam proposal tugas akhir ini adalah,

1. Tidak membahas satelit secara menyeluruh, hanya fokus pada enkripsi data gambar pada modul OBC.
2. Enkripsi yang digunakan menggunakan metode baker map yang berbasis *chaos theory*.
3. Metode baker map yang digunakan adalah 2D baker map dengan key space yang telah ditingkatkan.
4. Citra yang dienkripsi adalah suatu citra RGB.
5. Mikrokontroler yang akan digunakan adalah FPGA atlys.
6. Software simulasi yang akan digunakan adalah matlab
7. Implementasi ke FPGA menggunakan software Xilinx ISE

8. Tidak memperhatikan aspek transmisi
9. Proses dekripsi dilakukan pada PC dengan software matlab

1.5 Metodologi Penelitian

Metodologi penyusunan Tugas Akhir ini adalah sebagai berikut,

1. Studi Literatur

   Pemahaman konsep dan teori yang digunakan melalui pengumpulan literature berupa buku referensi, jurnal, serta artikel yang berkaitan dengan kasus yang sedang diangkat untuk mendukung dalam penyusunan Tugas Akhir ini.

2. Simulasi

   Proses simulasi metode enkripsi dengan menggunakan perangkat lunak matlab.

3. Implementasi

   Proses implementasi dari hasil simulasi dengan menggunakan software xilinx ke dalam FPGA.

4. Pengukuran

   Setelah algoritma ditanamkan ke dalam FPGA dilakukan pengukuran untuk mendapatkan kecepatan enkripsi, dan kehandalan data hasil enkripsi.

5. Analisis Dari hasil pengukuran dilakukan analisis apakah metode ini cocok untuk diterapkan ke dalam sistem komunikasi satelit.