PERANCANGAN ALGORITMA KRIPTOGRAFI BERBASIS CHAOTIC KOLMOGOROV FLOWS PADA FIELD PROGRAMMABLE GATE ARRAY (FPGA)

Ryan Ismaraditya[1], -[2]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Informasi visual seperti citra maupun video merupakan suatu jenis data blok berukuran besar sehingga memerlukan suatu algoritma kriptografi khusus yang mampu menawarkan kecepatan dalam proses serta mempunyai tingkat keamanan yang tinggi. Salah satu algoritma kriptografi untuk citra maupun video adalah algoritma kriptografi berbasis Chaotic Kolmogorov Flows. Pada Tugas Akhir ini dilakukan proses enkripsi dan dekripsi pada citra greyscale berukuran 64x64 pixel. Proses enkripsi meliputi dua tahap yaitu permutasi dan substitusi, sedangkan proses dekripsi juga melalui dua tahap yang merupakan inverse dari kedua tahap enkripsi. Citra hasil dekripsi memiliki nilai PSNR antara 47,5451 dB sampai 49,5893 dB serta rata-rata Rasio MSE 0,00086%. Dan menurut kriteria MOS citra hasil dekripsi memiliki kualitas antara fine dan excellent. Rancangan HDL menggunakan perangkat lunak Active-HDL 3.5 dan disintesis dengan perangkat lunak WebPack Project Navigator 5.1 serta target implementasi pada perangkat keras FPGA Xilinx Spartan-II XC2S100-5TQ144C. Hasil implementasi sistem Enkripsi membutuhkan 94% slice (1133 dari 1200 slice yang tersedia), 55% IOB (51 dari 92 IOB yang tersedia) serta frekuensi maksimum yang diperbolehkan yaitu 58,651 MHz. Sedangkan untuk sistem Dekripsi juga membutuhkan 94% slice (1133 dari 1200 slice yang tersedia), 55% IOB (51 dari 92 IOB yang tersedia) serta frekuensi maksimum yang diperbolehkan yaitu 58,651 MHz.

Kata Kunci : kriptografi, FPGA, VHDL, Chaotic Kolmogorov Flows.

Abstract

Visual sight information such as image or video is a kind of vast amount block data which require certain cryptographic algorithm offering high processing speed and also high security level. Cryptographic Algorithm based on Chaotic Kolmogorov Flows in one of the algorithm for processing image or video.In this final project, encryption and decryption process has been done for grayscale image with size 64x64 pixel in bitmap format file (*.bmp). Encryption process consists of two steps, permutation and substitution while decryption process also has two steps inversing the encryption process. Decrypted images have PSNR value between 47,5451 dB and 49,5893 dB and average MSE Ratio 0,00086%. Decrypted images have picture quality between fine and excellent according to MOS criteria. The HDL design used Active-HDL 3.5 software and synthesized with WebPack Project Navigator 5.1 software and hardware implementation target on FPGA Xilinx Spartan-II XC2S100-5TQ144C. Result from the implementation required 94% slices (1133 out of 1200), 55% IOBs (51 out of 92) and maximum frequency may used is 58.651 MHz for the encryption part. And for the decryption part also required 94% slices (1133 out of 1200), 55% IOBs (51 out of 92) and maximum frequency may used is 58.651 MHz for the decryption part.

Keywords : Cryptography, FPGA, VHDL, Chaotic Kolmogorov Flows.

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*).

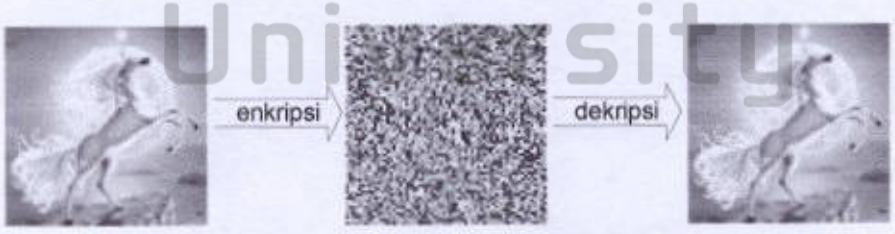
b. Algoritma kriptogarfi berbasis *chaotic Kolmogorov Flows*

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

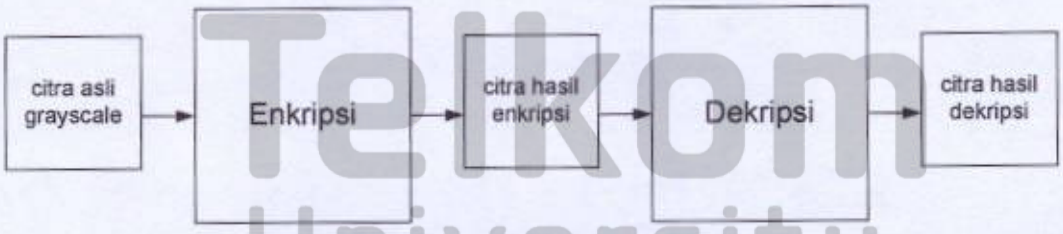
1. Melakukan perancangan sistem enkripsi-dekripsi berbasis *Chaotic Kolmogorov Flows* dengan VHDL dan mensimulasikannya.
2. Menganalisa kualitas output dari sistem yang telah dirancang
3. Mengetahui apakah citra yang telah dienkripsi dapat dikembalikan ke citra aslinya.
4. Membandingkan hasil implementasi 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.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan dari Tugas Akhir yang berjudul: "Perancangan Algoritma Kriptografi berbasis *Chaotic Kolmogorov Flows* pada FPGA" antara lain:

1. Hasil implementasi menggunakan WebPack Project Navigator 5.1 memperlihatkan bahwa maksimum frekuensi *clock* yang boleh digunakan adalah sebesar 58,651 MHz untuk sistem Enkripsi maupun sistem Dekripsi.
2. Slice yang dibutuhkan untuk implementasi dengan menggunakan Xilinx Spartan-II XC2S100-5TQ144C sebanyak 2.266 *slices* atau sebanding dengan 1134 CLB, sedangkan IOB total yang digunakan adalah sebanyak 102 IOB.
3. Hasil pengujian fungsi dengan pengukuran kualitas 30 citra mempunyai nilai rata-rata Rasio MSE sebesar 0,00086% dengan nilai PSNR antara 45,277 dB sampai 49,992 dB dan menurut penilaian subyektif atau *Mean Opinion Score* (MOS) citra hasil dekripsi mempunyai kualitas antara *fine* dan *excellent*.
4. Sistem telah memenuhi syarat *Confusion* dan *Diffusion* dalam menghasilkan *Chipertext.*
5. Rekonstruksi bagian-bagian dari citra asli berdasarkan citra output dengan menggunakan *pass-phrase* yang hampir benar tidak dapat dilakukan sebab perbedaan sedikit saja pada *pass-phrase* akan menghasilkan output yang sama sekali berbeda dan tidak memberikan informasi apapun tentang citra aslinya. Atau dapat dikatakan proses dekripsi akan berubah menjadi proses enkripsi jika *pass-phrase* yang digunakan memiliki perbedaan 1 bit saja.
6. Bila dibandingkan antara desain yang dirancang dengan hasil eksperimen yang telah dijelaskan sebelumnya, maka dapat disimpulkan sistem yang didesain mempunyai efisiensi area 15,91% sampai 64,96% dibandingkan dengan hasil eksperimen sebelumnya [2,3].
7. Dalam mengoptimalisasi sistem, baik untuk mengoptimalisasi penggunaan *slices* maupun untuk meningkatkan frekuensi *clock* maksimum yang diijinkan,

diperlukan pemahaman yang tinggi tentang VHDL dan FPGA serta diperlukan juga pemahaman tentang sistem yang dibuat.

5.2 Saran

1. Dalam meningkatkan kualitas rancangan dalam VHDL selain dibutuhkan pengetahuan mengenai VHDL itu sendiri, dan didukung oleh *software* yang terbaru dan memiliki kelebihan dari versi yang lama, serta juga harus didukung oleh *hardware* berupa FPGA dengan kemampuan dan spesifikasi yang lebih baik dari seri Spartan-II.
2. Desain ini dapat dikembangkan kemampuannya sehingga dapat melakukan enkripsi citra berwarna selain itu dapat dikembangkan pula menjadi enkripsi video.

DAFTAR PUSTAKA

1. Constant, Mike, *Notes on Signal to Noise Ratio*, CCTV Today.
2. Deepakumara, Janaka. Howard M. Heys. and R. Venkatesan. *FPGA Implementation of MD5 Hash Algorithm.* Faculty of Engineering and Applied Science, Memorial University of Newfoundland, Canada.
3. Elbirt, AJ. W Yip. B Chetwynd, and C Paar. *An FPGA-Based Performance Evaluation of the AES Block Chiper Candidate Algorithm Finalists.* ECE Departement, Worcester Polytechnic Institute, USA.
4. Ibrani, Yusrizal. *Studi dan Implementasi Algoritma Kriptografi RC6.* Sekolah Tinggi Teknologi Telkom. Bandung. 2001.
5. Macklem, Mason, *Current Trends in Image Quality Perception*, Simon Fraser University.
6. Mao, Yaobin and Guanrong Chen. *Chaos-based Image Encryption.* Handbook of Computational Geometry for Pattern Recognition,Computer Vision,Neural Computing and Robotics. 2003.
7. Scharinger, Josef. *Fast Encryption of image data using Chaotic Kolmogorov Flows.* Technical report, Johannes Kepler University, Departement of System Theory, Austria, April 1998
8. Scharinger, Josef. *Secure and Fast Encryption using Chaotic Kolmogorov Flows.* Technical report, Johannes Kepler University, Departement of System Theory, Austria, June 1998.
9. Schneier, B. *Applied Cryptography.* John Wiley & Sons, Inc., second edition. 1996.
10. *Spartan-II 2.5V FPGA Family: Functional Description*, Xilinx Inc., 2001.
11. Utami, Dewi. *Pengembangan Perangkat Keras Sistem Kriptografi dengan Menggunakan Sinyal Chaos.* Tesis Magister Program Pasca Sarjana, ITB. 2001.
12. *Using Block SelectRAM+ Memory in Spartan-II FPGAs, Xilinx Inc., 2000.*
13. Chang, K.C., Digital Design and Modelling with VHDL and Synthesis, IEEE Computer Society, Los Alamitos, California, 1997.
14. VHDL Modelling Guidelines, September 1994. ftp://ftp.estec.esa.n1/pub/vhdl/doc/ModelGuide.pdf