IMPLEMENTASI ENKRIPSI CITRA DENGAN DUA FUNGSI CHAOS KE DALAM IC-FPGA

SEMINAR BIDANG KAJIAN

YULI FITRIYANI
99216031

PROGRAM DOKTOR TEKNOLOGI INFORMASI

UNIVERSITAS GUNADARMA

SEPTEMBER 2022

1. PENDAHULUAN

1.1 Latar Belakang

Enkripsi merupakan sebuah proses untuk membuat suatu susunan system yang dibuat secara acak atau random untuk mengamankan data rahasia yang berupa teks atau gambar dalam dunia Kriptografi. Selain enkripsi ada juga istilah dekripsi dimana pada proses ini, susunan yang sudah diacak tersebut dikembalikan ke dalam data bentuk awal sebelum di enkripsi.

Dalam enkripsi ada istilah Chaos Theory (teori kekacauan) yang mempunyai beberapa fungsi chaos yang tersusun dari fungsi-fungsi matematika. Enkripsi dengan chaos ini dapat digunakan untuk proses enkripsi sebuah gambar yang bisa ditingkatkan dalam segi kecepatan dan keamanan.

Penjelasan teori chaos menurut pendapat Kocarev dan Lian, teori chaos ini pada awalnya berkembang dalam bidang fisika. Namun ternyata teori ini sudah berkembang di bidang ilmu matematika bahkan bidang teknologi informasi untuk proses enkripsi. Fungsi-fungsi chaos sudah banyak digunakan oleh para peneliti untuk proses enkripsi suatu citra atau gambar. Peneliti menggunakan satu dua atau lebih fungsi chaos untuk meningkatkan tingkat kesusahan data acak agar data rahasia yang sudah di enkrpsi tersebut tidak mudah diretas. Peneliti melakukan modifikasi fungsi chaos dengan model matematis dari beberapa buah fungsi chaos tersebut.

Dalam penelitian ini akan diajukan cara untuk menggunakan dua buah fungsi chaos yaitu Bernoulli map dan Logistic map. Peneliti akan memodifikasi dua buah fungsi chaos ini dengan menggunakan perhitungan fungsi matematika yaitu fungsi komposisi. Komposisi dari Bernoulli map dan Logistic map ini akan menghasilkan fungsi chaos baru yang dapat digunakan sebagai fungsi generate yang tingkat memiliki sifat chaos yang lebih kompleks.

Setelah membuat komposisi dari dua buah fungsi chaos ini, peneliti akan melakukan implementasi fungsi chaos baru tersebut ke Integrated Chip-FPGA (Field Programmable Gate Array). FPGA adalah sebuah IC digital yang sering dgunakan untuk merancang sebuah desain rangkaian digital.

1.2 Batasan Masalah

Agar penelitian ini fokus pada tujuannya, maka dibuat beberapa batasan masalah berikut ini :

a. Fungsi chaos yang digunakan adalah Bernoulli map dan Logistic map
b. Fungsi baru dihasilkan dari komposisi dari dua buah fungsi chaos diatas
c. Pengujian menggunakan diagram Bifurkasi dan Lyapunov Exponent
d. Software yang digunakan untuk implementasi FPGA adalah Xilinx Spartan 6

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut :

a. Membuat fungsi chaos baru dari Bernoulli map dan Logistic map dengan cara komposisi dua fungsi tersebut
b. Menguji tingkat keacakan yang dihasilkan dari fungsi chaos yang sudah dihasilkan
c. Implementasi fungsi chaos baru tersebut ke hardware yaitu FPGA

1.4 Kontribusi

a. Membuat fungsi chaos baru sebagai pembangkit bilangan acak untuk meningkatkan tingkat keacakan untuk proses enkripsi
b. Menanamkan algoritma chaos baru pada perangkat keras FPGA

2. TINJAUAN PUSTAKA

Studi literatur dari beberapa jurnal telah dilakukan untuk mendapatkan hasil pemikiran yang dapat mengembangkan metode yang sudah dilakukan sebelumnya. Rinaldi Munir, peneliti enkripsi citra digital yang melakukan penggabungan teknik permutasi dan teknik substitusi menggunakan Logistic map dan Arnold Cat map (ACM). Algoritma yang dihasilkan dapat mengacak citra grayscale dan citra berwarna dengan baik. Pada tahun 2017, Arinten D. H. dan Irawan A. telah membuat sistem kripstografi citra digital pada jaringan intranet menggunakan fungsi chaos Logistic map dan ACM. System ini mampu mengenkripsi citra digital dengan baik namun pengujian pengiriman citra di intranet menunjukkan citra yang telah terenkripsi tidak dapat dilihat citra aslinya. Andre dan Andrian, 2019, melakukan enkripsi citra dengan menggunakan Logistic map dan Piecewise Linear Chaotic map. Enkripsi menghasilkan pengacakan citra paling baik secara visual namun proses dekripsi gagal mengembalikan citra asli.

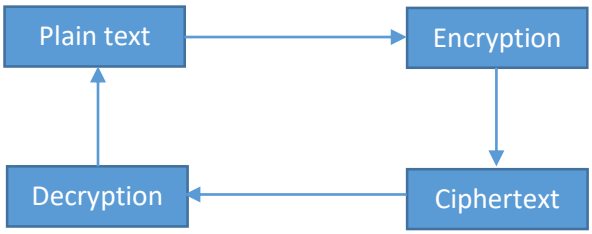
Pada tahun 2020, Iqbal, Kusrini dan Asro Nasiri melakukan perbandingan hasil enkripsi Logistic map dan ACM pada citra digital. Hasil analisis histogram dari algoritma ACM cenderung mirip dari histogram citra asli, sedangkan histogram logistic map terlihat berbeda dengan histogram citra asli serta secara statistik memiliki distribusi yang lebih seragam. Allwin Simarmata, 2021, melakukan pengamanan citra dengan kombinasi Modifeid Serpent Iwt dengan Modified Logistic Map. Alwin mengekstrak ciphertext biner dari citra stego dengan metode steganografi Iwt dengan modified Logistic map untuk menghasilkan round key.

2.1 Kriptografi

Kriptografi atau cryptography berasal dari bahasa Yunani yang terdiri dari kata Kripto dan Graphia. Kripto memiliki arti menyembunyikan dan Graphia yang berarti tulisan. Kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berkaitan dengan aspek keamanan informasi. [Menez, 1996]. Kriptografi menurut catatan sejarah telah eksis sejak masa kejayaan Yunani atau kurang lebih sekitar tahun 400 Sebelum Masehi. Alat yang digunakan untuk membuat pesan tersembunyi di Yunani pada waktu itu disebut Scytale. Scytale berbentuk batangan silinder dengan kombinasi 18 huruf. Pada masa Romawi, di bawah kekuasaan Julius Caesar,

penggunaan kriptografi semakin intens karena pertimbangan stabilitas negara. Meski teknik yang digunakan tak serumit Yunani, namun untuk memahami pesan kriptografi dari masa Romawi terbilang cukup sulit untuk dikerjakan.

Kriptografi bisa juga diartikan sebagai suatu ilmu atau senin menjaga keamanan pesan [Ariyus, 2008] dengan dua proses dasar kriptografi berupa enkripsi dan dekripsi. Enkripsi merupakan proses mengolah pesang yang dibaca (plaintext) menjadi pesan acak yang tidak bisa dibaca (ciphertext). Sebaliknya dengan dekripsi yang merupakan proses mengolah ciphertext menjadi plaintext. Dalam proses enkripsi dekripsi tersebut ada kunci (key) yang digunakan dalam penyandian dan algoritma yang digunakan dalam proses tersebut. Kriptografi biasanya membagi dua jenis kunci yaitu enkripsi kunci simetris (*Symmetric-key encryption*) dan enkripsi kunci publik (*Public-key encryption*). Suatu enkripsi dikatakan enkripsi kunci simetris ketika proses enkripsi dan dekripsinya menggunakan kunci yang sama. Enkripsi kunci publik artinya untuk proses enkripsi dan dekripsi menggunakan kunci yang berbeda.



Gambar 2.1 Hubungan Plaintext dan Ciphertext dalam Enkripsi Dekripsi

2.2 Teori Chaos

Teori Chaos adalah ilmu matematika yang mempelajari system yang berisi gerakan banyak elemen yang memerlukan computer untuk menghitung semua kemungkinan yang ada. Teori ini menarik perhatian para peneliti sains yang mencoba menerapkan konsep matematika ke dalam ilmu engineering. Teori chaos yang memiliki sifat keacakan menjadi kebutuhan utama dalam dunia kriptografi. Teori chaos dalam kriptografi digunakan sebagai pembangkit bilangan acak.

Dalam matematika, chaos map adalah sebuah peta yang menunjukkan perilaku kekacauan atau keacakan. Peta (map) tersebut diparameterkan dengan waktu diskrit

dan kontinu. Tabel 2.1 dibawah ini menunjukkan sebagian jenis chaos yang sering digunakan oleh para peneliti.

Tabel 2.1 Beberapa jenis chaos map

Jenis Map	Time domain	Dimensions
Arnold's Cat	discrete	2
Baker's	discrete	2
Beta Chaotic	discrete	2
Circle	discrete	1
Dyadic Transformati on	discrete	1
Gauss	discrete	1
Hadley Chaotic Circulation	continuous	3
Hénon	discrete	2
Logistic	discrete	1
Novel Chaotic System	continuous	3
Tent	discrete	1
dst		

Sifat system chaos memiliki 3 sifat yaitu :

a. Perilaku aperiodic : Perilaku ini berarti keberadaan lintasan fase-ruang yang tidak tetap untuk poin tertentu atau orbit periodic
b. Deterministik : Bahwa persamaan gerak system tidak memiliki masukkan acak. Dengan kata lain, perilaku tidak beraturan system muncul dari dinamika nonlinear
c. Ketergantungan sensitive pada kondisi awal : Berarti lintasan terdekat di fase-ruang terpisah untuk eksponensial dalam waktu yaitu memiliki system eksponen Liapunov [Ipek Zeynep, *Chaos and Chaotic Maps.* Belmont, Cankaya University, 2009].

2.3 Bifurkasi

Bifurkasi adalah perubahan kualitatif pada sebuah sistem dinamik terhadap variabel parameternya [Kocarev]. Perubahan kestabilan atau perubahan yang dramatis dalam dinamika suatu sistem akibat berubahnya nilai parameter dalam sistem dinamakan bifurkasi. Bifurkasi tidak selalu terkait dengan kekompleksan. Tetapi, ada beberapa jenis bifurkasi yang senantiasa terkait dengan bertambahnya kerumitan sistem yang pada akhirnya mengakibatkan chaos. Karena itu, bifurkasi dapat digunakan untuk mempelajari mekanisme terjadinya chaos [Johan Matheus Tuwankotta, 2003].

Bifurkasi terjadi ketika perubahan kecil parameter sebuah sistem menyebabkan perubahan secara kualitatif yang signifikan pada sistem tersebut. Menurut [Devaney, 1989]. Nilai parameter yang menyebabkan bifurkasi disebut sebagai titik bifurkasi. Bifurkasi terjadi baik dalam sistem kontinyu maupun sistem diskrit.

Densitas dalam periode orbit suatu sistem chaos bisa dilihat dari diagram bifurkasi yang merupakan diagram untuk menggambarkan nilai yang mungkin ditempati untuk setiap parameter, seperti parameter nilai awal. Diagram bifurkasi direkonstruksi dengan cara mengambar plot suatu sistem sebagai fungsi dari parameternya.

2.4 Bernoulli Map

Bernoulli map disebut juga dengan Dyadic map, bit shift map, doubling map atau sawtooth map. Bernoulli map memiliki fungsi persamaan :

$$x_{n+1} = \begin{cases} 2x & 0 \le x < {}^{1}/_{2} \\ 2x - 1 & {}^{1}/_{2} \le x < 1 \end{cases} \tag{2.1}$$

Bernoulli map yang sering disebut dengan nama Dyadic map memberikan sebuah contoh sederhana tentang bagaimana peta (map) 1 dimensi yang dapat meningkatkan chaos (kekacauan). Bernoulli map ini mudah digeneralisasikan ke beberapa map lainnya. Salah satunya adalah beta transformation yang didefinisikan sebagai :

$$T_{\beta}(x) = \beta x \ mod \ 1 \tag{2.2}$$

2.5 Logistic Map

Logistic Map adalah salah satu bentuk yang paling sederhana dari proses chaotic. Karena kesederhanaan matematisnya, model chaos ini terus memunculkan ide-ide baru dalam teori chaos serta aplikasi chaos dalam kriptografi.

Logistic Map adalah pemetaan polynomial derajat 2 disebut juga sebagai contoh pola dasar kompleksitas. Perilaku acak atau kacau dapat muncul dari persamaan dinamik nonlinear yang sangat sederhana. Logistic Map dipopulerkan pada akhir 1976 dalam jurnal oleh ahli biologi Robert May, sebagai bagian dari model demografi diskrit waktu yang dianalogikan dengan persamaan logistic, yang pertama kali diciptakan oleh Pierre Francois Verhulst. Fungsi Logistic Map didefinisikann sebagai fungsi satu variabel x dan r parameter tetap. Nilai variabel x_0 dalam interval (0, 1), x_n untuk n = 0,1,2,3,... dan r dalam interval (0, 4]. Nilai n merupakan isi inisial iterasi, secara sistematis Logistic Map [Kocarev, 2011] ditulis seperti berikut :

$$x_{n+1} = r x_n (1 - x_n) \tag{2.3}$$

2.6 Field Programmable Gate Array (FPGA)

FPGA merupakan piranti yang dapat diprogram berbentuk integrated circuit (IC) dan tersusun atas modul-modul logik bebas yang dapat dikonfigurasi. FPGA memiliki komponen logika yang dapat diprogram (programmable logic) yang terdiri dari logic blocks dan programmable interconnects. Logic blocks dapat diprogram untuk membuat fungsi-fungsi gerbang dasar seperti AND, OR, XOR ataupun yang lebih kompleks seperti decoder serta fungsi matematika sederhana, dan modul-modul logik tersebut terhubung melalui kanalkanal penjalaran yang dapat diprogram. (Wibowo, 2010).

FPGA pada umumnya merupakan larik 2 dimensi logic blocks (slices) yang memiliki elemen memori, seperti flip-flop sederhana atau blok-blok memori yang lebih kompleks. Suatu hirarki dari programmable interconnects memungkinkan logic blocks untuk dapat saling berhubungan sesuai kebutuhan perancang sistem, seperti suatu breadboard yang dapat diprogram. Logic blocks dan programmable interconnects dapat diprogram oleh pemakai/perancang dalam mengimplementasikan berbagai macam fungsi logika, sehingga diberi istilah field-programmable. Pengertian terprogram

(programmable) dalam FPGA, mirip dengan interkoneksi saklar dalam breadboard yang bisa diubah oleh perancang desain. Kelebihan dari FPGA adalah dapat dikonfigurasi oleh end user, tidak memerlukan proses fabrikasi karena tersedia cara untuk mendukung chip customized - very large scale integration (VLSI) dalam mengimplementasikan logic circuit, instant manufacturing, very-low cost prototype dan pemrograman yang singkat untuk fungsi dan kemampuan yang setara dengan applied specific integrated circuit (ASIC).

FPGA dapat diprogram menggunakan bahasa deskripsi Verilog dan very high speed integrated circuit – hardware description language (VHDL). Perkembangan FPGA sampai saat ini berlangsung dengan cepat dan banyak macam keluarga FPGA dengan kebutuhan perancangan dan perangkat perancangan (design tools) yang berbeda. Perusahaan yang memproduksi FPGA diantaranya adalah Xilinx, Altera, ACTEL, ATMEL, dan PLESSEY Semiconductor. Xilinx memproduksi beberapa jenis FPGA, yaitu VIRTEX, SPARTAN, XC3000, XC4000 dan XC5000. Pendekatan untuk menggabungkan logic blocks dan interconnects dari FPGA dengan embedded microprocessor dan periperal-periperal lainnya telah dilakukan. Tujuannya sebagai pelengkap dari sistem pada sebuah chip yang dapat diprogram.

Secara umum, FPGA akan lebih lambat jika dibandingkan dengan jenis chip yang lain, seperti Application-Specific Integrated Circuit (ASIC). Hal tersebut dikarenakan FPGA menggunakan daya yang besar dengan bentuk desain yang kompleks, walaupun demikian FPGA mempunyai harga yang murah, bisa diprogram mengikuti kebutuhan, dan kemampuan untuk diprogram ulang untuk mengkoreksi adanya bugs. Jenis FPGA dengan harga murah, biasanya tidak bisa diprogram dan dimodifikasi setelah proses desain dibuat (fixed-version). Chip FPGA yang lebih kompleks dapat diperoleh dari jenis FPGA yang dikenal dengan complex-programmable logic device (CPLD). FPGA pada awalnya dibuat sebagai pesaing dari CLPD dan bersaing pada bidang yang sama. Rancangan rangkaian yang akan diimplementasikan ke dalam FPGA dideskripsikan menggunakan VHDL (Very High Speed Integrated Circuit Hardware Description Language). VHDL adalah bahasa deskripsi perangkat keras yang mirip dengan bahasa tingkat tinggi, seperti C, Pascal, Fortran dan sebagainya. VHDL melukiskan perilaku rangkaian elektronik atau sistem pada tata algoritma, bukan implementasi. Kompiler

perangkat keras modern dapat membaca deskripsi tingkat tinggi sistem elektronik dan menterjemahkannya menjadi konfigurasi bit string yang digunakan untuk mengkonfigurasi sebuah chip FPGA.

3. METODOLOGI

Dalam penelitian ini, ada beberapa langkah metodologi yang dijalankan. Adapun metode tersebut adalah sebagai berikut :

1. Studi Pustaka : Peneliti mencari teori terkait mengenai tema yang digunakan dalam penelitian ini. Serta mempelajari metode dan konsep tersebut melalui pencarian jurnal, buku dan artikel.
2. Dari poin 1 diatas, peneliti menentukan pilihan dua fungsi chaos yang akan digunakan dalam proses enkripsi.
3. Menentukan komposisi dari fungsi chaos secara matematia
4. Menguji hasil dari fungsi chaos baru
5. Melakukan simulasi dengan citra digital
6. Implementasi fungsi chaos baru ke dalam FPGA
7. Menganalisis performa hasil enkripsi-dekripsi dari fungsi chaos baru tersebut yang sudah ditanamkan pada FPGA

Fungsi chaos baru yang dihasilkan dalam penelitian ini adalah hasil komposisi dari Logistic map dan Dyadic Transformation Map. Fungsi komposisi adalah gabungan dua atau lebih fungsi yang saling terhubung. Fungsi komposisi yang digunakan yaitu gabungan dari dua buah fungsi misal fungsi f(x) dan g(x) dinyatakan dalam bentuk (f o g)(x). Dimana f(x) adalah fungsi chaos Bernoulli map dan g(x) adalah fungsi Logistic Map.

Fungsi Bernoulli map mempunyai persamaan :

$$x_{n+1} = \begin{cases} 2x & 0 \le x < {}^{1}/_{2} \\ 2x - 1 & {}^{1}/_{2} \le x < 1 \end{cases} \tag{3.1}$$

Fungsi Logistic map mempunyai persamaan :

$$x_{n+1} = r x_n (1 - x_n) \tag{3.2}$$

Fungsi f(x) dan g(x) tersebut dikomposisi menjadi :

$$(f\ o\ g)(x) = 2(rx_n(1 - x_n)) \tag{3.3}$$

untuk $0 \leq x < {}^{1}/_{2}$

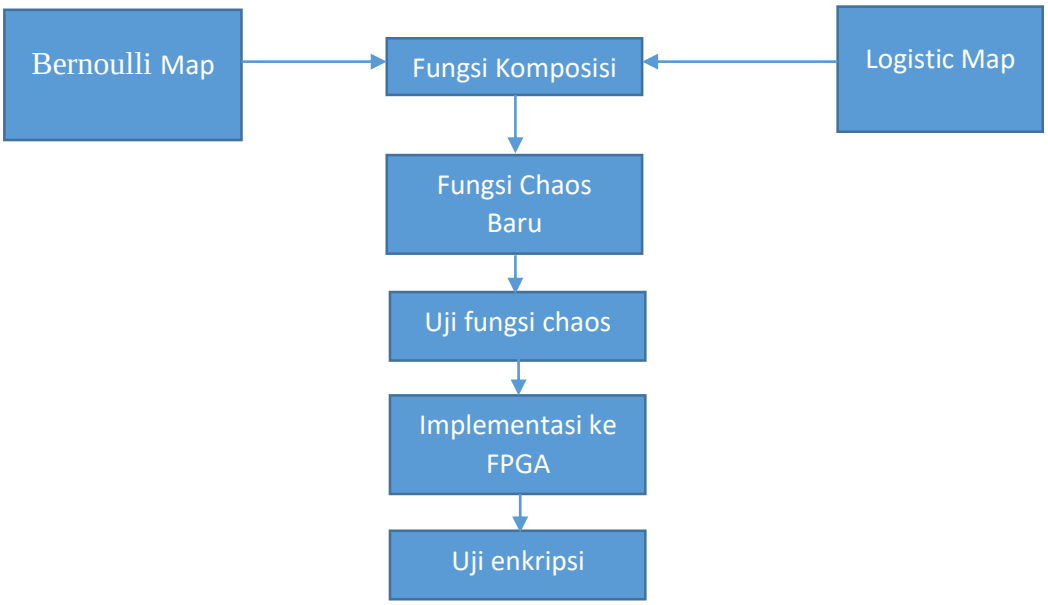
$$(f\ o\ g)(x) = 2\big(rx_n(1 - x_n)\big) - 1 \tag{3.4}$$

untuk ${}^{1}/_{2} \leq x < 1$

Dari persamaan (3) dan (4) maka didapat fungsi chaos baru dengan persamaan :

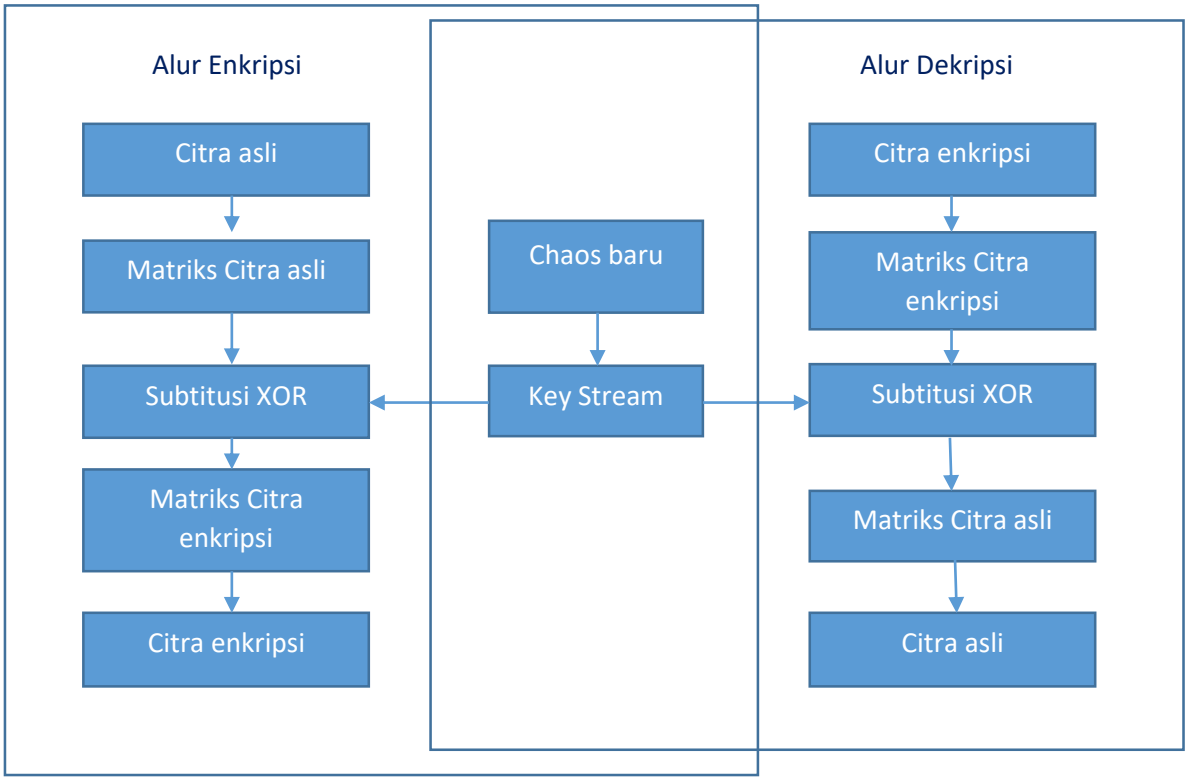
$$x_{n+1} = \begin{cases} 2rx_n(1 - x_n) & ;\ 0 \leq x < {}^{1}/_{2} \\ 2rx_n(1 - x_n) - 1 & ;\ {}^{1}/_{2} \leq x < 1 \end{cases} \tag{3.5}$$

Fungsi chaos baru dari persaman (5) diatas bisa diberikan tambahan matematis seperti kombinasi, permutasi, substitusi atau invers untuk menambah tingkat keacakan enkripsi. Selanjutnya fungsi chaos baru dilakukan uji dengan masukkan citra digital dimulai dari proses enkripsi hingga dekripsi. Gambar 3.1 dibawah ini adalah diagram proses komposisi untuk fungsi chaos baru.



Gambar 3.1 Diagram gabungan fungsi chaos Bernoulli dan Logistic Map

Fungsi chaos baru selanjutnya akan diuji dengan diagram Bifurkasi dan diagram Lyapunov Exponent. Uji ini akan menunjukkan fungsi chaos baru ini bersifat chaos atau tidak. Fungsi chaos baru yang sudah memenuhi uji Bifrukasi dan Lyapunov, selanjutnya di uji keacakan dengan NIST (National Institute of Standard and Technology).



Gambar 3.2 Alur proses enkripsi dan dekripsi

Setelah fungsi chaos baru telah menghasilkan chaos yang maksimal, selanjutnya adalah proses implementasi ke perangkat keras FPGA. Langkah awal adalah merancang system dengan menggunakan VHDL dan menurunkannya ke HDL. Selanjutnya mengembangkan testbench dengan HDL dan membuat simulasi pada Register Transfer Level (RTL). Berikutnya melakukan analisis dan sintesis HDL yang kemudian di generate dan mengunduh file programming. File ini berisi konfigurasi FPGA yang bisa di unduh ke perangkat FPGA untuk melakukan uji coba.

DAFTAR PUSTAKA

Munir R., (2012), *Algoritma Enkripsi Citra Digital Berbasis Chaos Dengan Penggabungan Teknik Permutasi Dan Teknik Subtitusi Menggunakan Arnold Cat Map Dan Logistic Map*, Prosiding Seminar Nasional Pendidikan Teknik Informatika, Singaraja – Bali.

Arinten D. H. dan Irawan A., 2017, *Sistem Kriptografi Citra Digital Pada Jaringan Intranet Menggunakan Metode Kombinasi Chaos Map Dan Teknik Selektif*, Jurnal Ultimatic, Vol IX, No.1

Andre dan Andrian, 2019, *Pengacakan Citra Digital Dengan Menggunakan Logistic Map Dan Piecewise Linear Chaotic Map*, Jurnal Teknologi, Kesehatan dan Ilmu Sosial, Vol 1, No.1

Iqbal, Kusrini, Nasiri, 2020, *Komparasi Hasil Enkripsi Arnold Cat Map Dan Logistic Map Pada Citra Digital*, Jurnal Ilmiah Teknologi Informasi, Universitas Cokroaminoto Palopo, Vol 10, No.2

Allwin Simarmata, 2021, *Image Security with a Combination of Modified Serpent and IWT with Modified Logistic Chaotic Map*, JATISI, Vol.8, No.3

Ipek Zeynep, , 2009, *Chaos and Chaotic Maps.* Belmont, Cankaya University

Cristea, Bogdan., Cehan, Constantin. *Applications of Chaos Theory in Cryptography*

Wikipedia, *List of Chaotic Maps*, https://en.wikipedia.org/wiki/List_of_chaotic_maps, diakses tanggal 22 September 2022

Suci BK , Suryadi, Algoritma Enkripsi Citra Digital Berbasis Chaos Menggunakan Fungsi MS GAUSS MAP. Disertasi, 2016

Yudi Satria, Suryadi MT, Ita M Solihat, Luqman N Prawadika, Venny Melvina *The composition of the improved logistic map and the MS map in generating a new chaotic function PAPER SIYu MAP - ICOMPAC 2019*

Hamsa A. Abdullah, Hikmat N. Abdullah *FPGA implementation of color image encryption using a new chaotic map* Indonesian Journal of Electrical Engineering and Computer Science Vol. 13, No. 1, January 2019, pp. 129~137 ISSN: 2502-4752, DOI: 10.11591/ijeecs.v13.i1.pp129-137

MT Suryadi, Y Satria, V Melvina, LN Prawadika, IM Sholihat, *A new Chaotik map development through the composition of the MS MAP and the Dyadic Transformation Map*, Journal of Physics: Conference Series 1490 (1), 012024