PROPOSAL PENELITIAN DESERTASI

Implementasi Komposisi GDT kedalam IC –FPGA Untuk Mempercepat Proses Enkripsi dan Tahan Terhadap Serangan.

Kualifikasi

MUDRIKA

TI 22

99216009

2021

BAB I

Pendahuluan

1.1 Latar Belakang

Didalam dunia kriptografi pada saat ini telah banyak menerapkan berbagai metode maupun cara untuk mengamankan data, hal ini disebabkan karena pentingnya data untuk diamankan dan tidak jatuh ketangan-tangan yang tidak berkepentingan untuk menggunakan data. Untuk meningkatkan keamanan dan hasil yang baik maka di perlukan metode yang unik maupun rumit.

Didalam kriptografi itu sendiri mempunyai definisi yaitu ilmu yang mempelajari teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, autentikasi entitas, dan autentikasi data asal [Menezes, Oorschot dan Vanstone, 1996]. Pada masa awal perkembangannya kriptografi sangat sederhana yaitu bagaimana cara untuk menyandikan informasi asli atau plain menjadi informasi yang tersandikan yaitu chipper dalam proses inilah yang disebut dengan enkripsi. Dan untuk mengembalikan informasi yang tersandikan atau chipper menjadi informasi asli atau plain disebut dengan proses deskripsi.

Chaos mempunyai karakteristik yaitu sensitivitas terhadap kondisi awal, berkelakuan acak, dan tidak memiliki periode berulang. Fungsi yang memiliki sifat chaos dinamakan fungsi chaos. Fungsi chaos sudah dibuktikan sangat cocok untuk proteksi data [Kocarev and Lian, 2011].Fungsi yang mempunyai siffat chaos antara lain: Circle maps , logistic map, MS Map, Tent map Gauss Iterated Maps , Dyadic Transformation maps dan lain sebagaimana.

Pada beberapa tahun terakhir ini telah banyak algoritma enkripsi yang telah dilakukan. Algoritma seperti Algoritma DES(Data Enkripsi Standart) ,Algoritma AES(Advanced Encryption Standart), RSA (Rivest-Shamir-Adleman), algoritma algoritma ini sesuai untuk enkripsi teks tetapi tidak cocok untuk enkripsi gambar (Prabir dan Atal, 2014) karena algoritma-algoritma tersebut membutuhkan waktu yang lama dan daya komputasi yang tinggi walaupun menghasilkan data yang terenkripsi dengan baik, akan tetapi yang diutamakan dalam enkripsi gambar digital adalah waktu yang lebih cepat tanpa mengorbankan keamanannya. Untuk metode enkripsi gambar digital dapat dipenuhi dengan metode enkripsi berbasis chaos.Metode enkripsi dengan chaos ini dapat

memenuhi dari segi kecepatan ,keamanan yang tinggi dan daya komputasi (kocarev dan lian, 2011).

Diantara penelitian yang berkembang saat ini terdapat penelitian yang pembangkitan bilangan acaknya melalui Fungsi chaos yang merupakan modifikasi atau penggabungan dua buah fungsi chaos yang berbeda ataupun menggunakan multi fungsi chaotic. Hal tersebut dilakukan dalam rangka peningkatan daya tahan terhadap berbagai serangan pada saat fungsi chaos tersebut diterapkan dalam proses enkripsi data digital.

Dalam hal ini maka akan diajukan penggabungan dengan cara mengkomposisikan dua buah fungsi chaos yaitu fungsi Gauss Iterated Map dan Dyadic Transformation Map (GDT) ,yang mana dari komposisi ini akan mendapatkan fungsi chaos yang baru Sehingga diharapkan fungsi baru tersebut dapat sebagai 3lternative pilihan sebagai fungsi pembangkit bilangan acak yang bersifat chaos.

FPGA Field Programmable Gate Array (FPGA) merupakan sebuah IC digital yang sering digunakan untuk mengimplementasikan rangkaian digital. Bila dilihat dari segi namanya, Field Programmable dapat diartikan bahwa FPGA ini bersifat dapat dirancang sesuai dengan keinginan dan kebutuhan user/pemakai.

Di dalam proposal penelitian ini juga diusulkan implementasi FPGA dari algoritma enkripsi gambar yang efisien menggunakan fungsi chaos yang baru yang akan diusulkan. FPGA (Field Programmable Gate Array) yang pada dasarnya merupakan perangkat dengan konsep menggunakan bahasa pemrograman untuk perangkat keras dalam mendesain atau merancang desain elektronika berbasis digital atau gerbang-gerbang logika, sehingga dengan latar belakang yang telah diuraikan, penelitian ini akan membahas atau dengan tema “Implementasi Komposisi GDT kedalam IC –FPGA Untuk Mempercepat Proses Enkripsi dan Tahan Terhadap Serangan.”.

1.2 Perumusan masalah

Dari uraian latar belakang, mempunyai perumusan masalah sebagai berikut :

- Bagaimana mengupayakan menghasikan fungsi chaos baru dari komposisi dua buah fungsi chaos yang di ajukan.

- Bagaimana mengsimulasikan fungsi chaos baru yang diajukan tersebut kedalam citra digital dengan enkripsi dan deskripsi.
- Bagaimana konsep enkripsi dan dekripsi pada fungsi chaos baru yang diajukan dengan menggunakan bahasa perangkat keras kedalam FPGA.

1.3 Batasan Penelitian

Proposal penelitian ini mempunyai batasan sebagai berikut :

- Untuk pembuatan kunci baru menggunakan uji bifurkasi , Lyapunov exponent dan uji NIST
- Metode yang digunakan dengan subtitusi dengan exor.
- Data masukkan berupa data gambar digital.
- FPGA yang digunakan menggunakan tipe Xilinx Spartan 6

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah :

- Mengetahui pengaruh data gambar sebelum dan sesudah proses enkripsi dan deskripsi dengan FPGA
- Mengimplentasikan fungdi chaos GDT yang akan diajukan dengan software maupun hardware.
- Membandingkan hasil penelitian yang akan diusulkan dengan penelitian sebelumnya.

1.5 Kontribusi Hasil Penelitian

- Penemuan fungsi pembangkit bilangan acak yang bersifat chaos(keystream chaotic) dengan fungsi chaos yang baru(GDT)
- Mengetahui kinerja FPGA dalam algoritma enkripsi dengan fugsi chaos yang baru (GDT)

BAB II

Studi Literatur

2.1 Landasan Teori

Kriptografi berasal dari bahasa Yunani, yaitu kryptos dan graphia. Kryptos berarti sesuatu yang disembunyikan, tidak dikenal, terselubung, rahasia, atau misterius. Sedangkan graphia berarti tulisan sehingga kata kriptografi dapat diartikan sebagai tulisan yang disembunyikan atau dirahasiakan. Menurut [Schneier, 1996] Kriptografi adalah ilmu dan seni yang memelajari bagaimana menjaga keamanan suatu pesan. Sedangkan menurut [Meneze et al., 1996] Kriptografi adalah ilmu yang mempelajari tentang teknik matematika yang berhubungan tentang aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, dan autentikasi data. Algoritma untuk mentransformasikan plaintext menjadi chipertext disebut chiper. Ada dua motode proses chiper yaitu subtitusi (substitution cipher) dan transposisi (transposition cipher). Chiper subtitusi adalah proses mengubah nilai setiap data dari suatu dokumen yang dapat terbaca (plaintext) menjadi nilai lain sehingga isi dokumen tersebut menjadi tidak dapat terbaca maknanya (chipertext). Chiper transposisi adalah proses pengacakan posisi setiap data (tanpa ada perubahan nilai data) dari suatu dokumen yang dapat terbaca (plaintext) sehingga isi dokumen tersebut menjadi tidak dapat terbaca maknanya (chipertext).

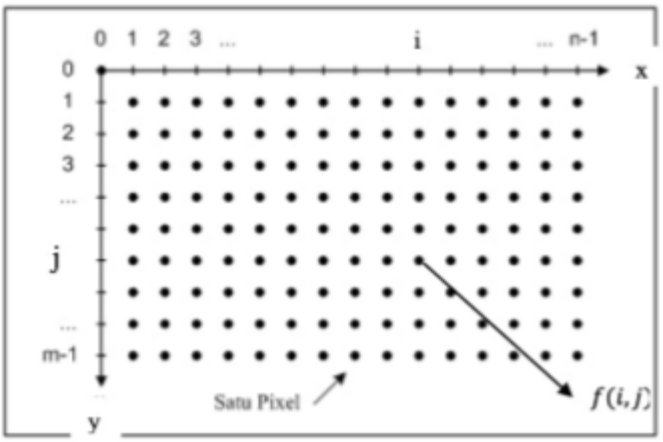
2.2 Sistem Chaos

Sebuah sistem dinamis yang menunjukkan sensitif terhadap nilai awal pada himpunan invarian tertutup dengan lebih dari satu orbit disebut sebagai sistem chaos [Wiggins,2003]. Menurut [Stewart, 1997], chaos adalah perubahan yang sangat kompleks, iregular, dan acak dalam sebuah sistem yang deterministik. Chaos adalah suatu keadaan dimana sebuah sistem tidak bisa diprediksi dimana ia akan ditemukan ditempat berikutnya. Sistem ini bergerak secara acak, namun bila keadaan acak tersebut diperhatikan dalam waktu yang cukup lama dengan mempertimbangkan dimensi waktu, maka akan ditemukan juga keteraturannya. Bagaimanapun kacaunya sebuah sistem, maka sistem tidak akan pernah melewati batas-batas tertentu. Bagaimanapun acaknya sebuah sistem , ruang geraknya tetap dibatasi oleh kekuatan penarik yang disebut strange attractor.

Strange attractor disatu sisi menjadikan sebuah sistem bergerak secara acak, dinamis,dan fluktuatif, tapi disisi lain akan membingkai batas-batas ruang gerak tersebut.

2.3 Citra Digital

Citra secara fisis merupakan sekumpulan data numerik yang ditampilkan pada suatu media seperti kertas, layar film dan layar monitor sehingga merepresentasikan informasi visual berupa warna, bentuk atau tekstur sebuah objek. Dari informasi ini seseorang dapat menganalisis dan memaknai informasi apa yang terkandung di dalamnya [Madenda, 2015]. Suatu citra digital berukuran n×m didefinisikan sebagai himpunan fungsi dua variabel f(x,y) dengan x dan y merupakan koordinat spasial, dan amplitudo f di setiap koordinat (x,y) dinamakan intensitas atau tingkat keabuan dari citra pada titik tersebut. Adapun nilai dari variabel x, y dan f(x,y) adalah berhingga dan diskrit, dengan x = 1,2,3,...,n, y = 1,2,3,...,m dan f(x,y) bernilai dari 0 sampai dengan 255. Elemen penyusun citra digital yaitu setiap titik (x,y) pada citra digital yang biasa disebut pixel (picture elements), dan f(x,y) merepresentasikan nilai pada pixel tersebut [Gonzales & Woods, 2001]. Gambar 2.3 menunjukkan representasi citra digital berdasarkan keadaan pixel.



Gambar 2.1: Representasi Citra Digital Berukuran n×m

Terdapat dua jenis dari citra digital yang penting yaitu citra digital hitam dan putih dan citra digital warna [Sachs,1996].

2.3.1 Citra Digital Hitam Putih

Citra digital hitam putih terdiri dari pixel-pixel yang tiap pixelnya mewakili informasi skala keabuan. Setiap pixel biasanya disimpan dalam 1 byte atau 8 bit. Terdapat 256 tingkatan warna dari hitam ke putih, nilai 0 mewakili warna hitam hingga 255 mewakili warna putih sedangkan nilai diantaranya merepresentasikan warna keabuan yang bervariasi dari hitam hingga cerah menuju putih, seperti ilustrasi yang diperlihatkan pada gambar 2.2

Gambar 2.2: Tingkat Keabuan dari Hitam ke Putih

Jika dilihat dengan mata, warna putih yang tingkat keabuannya 255 dengan warna putih yang tingkat keabuannya 253 dan 252 tidak terlalu jelas perbedaannya, namun dalam representasi binernya sangatlah berbeda.

2.3.2 Citra Digital Warna (Color)

Sebuah citra digital sebagai hasil akuisisi sensor frekuensi warna umumnya direpresentasikan dengan tiga komponen warna dasar yaitu red (R), green (G) dan blue (B). Sama halnya dengan representasi dan pengolahan citra digital dalam komputer lebih umum menggunakan tiga komponen warna dasar tersebut. Setiap pixel pada citra berwarna memiliki tiga komponen warna R, G dan B yang masing- masing umumnya disimpan dalam 8 bit atau total ketiganya 3×8 = 24 bit (tiga byte). Hal ini memungkinkan setiap pixel dalam citra berwarna dapat memiliki variasi kandungan warna sebanyak 224 (16777216 variasi warna). Mengacu pada defenisi matematis yang telah diuraikan di atas, maka citra berwarna dapat direpresentasikan dalam matriks tiga dimensi f(n,m,k), dimensi ke-3 adalah k = {1,2,3} yang merepresentasikan komponen warna merah (1 = red R), hijau (2 = green G) dan biru (3 = blue B) [Madenda, 2015].

2.4 Diagram Bifurkasi

Istilah bifurcation pertama kali diperkenalkan oleh Henri Poincare pada tahun 1885 dalam sebuah paper matematika. Menurut Kocarev; bifurkasi adalah perubahan kualitatif pada sebuah sistem dinamik terhadap variabel parameternya. Menurut [Devaney, 1989] bifurkasi terjadi ketika perubahan kecil parameter sebuah sistem menyebabkan perubahan secara kualitatif atau secara topologi yang signifikan pada sistem tersebut. Nilai parameter yang menyebabkan bifurkasi disebut sebagai titik bifurcation. Bifurkasi terjadi baik dalam sistem kontinu 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.

Diagram bifurkasi adalah diagram yang menunjukkan nilai yang didekati secara asimptotik dari suatu system sebagai fungsi dari parameter dalam system. Dengan melihat diagram bifurkasi, kita dapat mengetahui sifat chaos suatu fungsi. Jika titik-titik periodik pada diagram bifurkasi padat, maka fungsi tersebut chaos.

2.5 Kriteria Metode Enkripsi

Sistem enkripsi modern menganut prinsip Kerchoff yaitu dalam enkripsi modern hanya kunci yang dirahasiakan, sementara algoritma enkripsi akan terbuka untuk pengujian kekuatan algoritma dan pengembangan algoritma. [Wang, 2015]. Algortima enkripsi standard harus memenuhi kriteria berikut: Efisiensi, yaitu operasi yang digunakan dalam metode enkripsi harus mudah diimplementasikan dalam bentuk perangkat lunak maupun perangkat keras. Waktu yang diperlukan untuk enkripsi sebaiknya dalam waktu yang cepat dan memerlukan sumber daya yang tidak terlalu banyak. Untuk mencapai efisiensi tersebut maka algoritma enkripsi menerapkan operasi yang mudah diimplementasikan dalam komputer seperti exclusive OR, permutasi, substitusi, circular shift, maupun operasi finite field lainnya [Suryanto, 2015]. Tahan terhadap analisis statistik, yaitu ciphertext yang dihasilkan oleh algoritma enkripsi secara statistik tidak berkorelasi dengan struktur plaintex. Algoritma yang bagus membuat statistical atack menjadi tidak akan berguna. Agar statistical attack tidak berguna dapat dicapai dengan cara membuat

algoritma enkripsi memenuhi kriteria diffusion dan confussion. Diffusion adalah perubahan 1 bit dalam plain-image akan menyebabkan sejumlah perubahan bit dalam dalam cipher-image. Perubahan bit dalam plain-image sebisa mungkin tersebar secara merata dalam cipher-image. Confussion adalah perubahan 1 bit dalam kunci enkripsi akan menyebabkan perubahan dalam sejumlah bit dalam ciphertext. Perubahan bit dalam kunci enkripsi sebisa mungkin tersebar secara merata dalam cipher-image agar analisis statistik tidak berguna dalam merekonstruksi plaintext. Tahan terhadap serangan brute force, yaitu ruang kunci yang dihasilkan oleh algoritma cukup tinggi sehingga peluang untuk merekonstruksi ciphertext membutuhkan waktu yang sangat lama. Brute force dilakukan dengan mencoba semua kemungkinan kombinasi kunci enkrip untuk mendapatkan plaintext dari ciphertext yang diketahui dan tanpa mengetahui kunci yang sebenarnya. Brute force attack juga dapat digunakan untuk mendapatkan kunci yang sebenarnya dari pasangan plaintext dan ciphertext yang diketahui. Misalnya panjang kunci yang digunakan dalam algoritma enkripsi adalah x bit, maka brute force attack akan berhasil dengan melakukan percobaan kombinasi kunci kurang dari 2x. Jumlah kunci yang diperlukan dalam enkripsi modern adalah 128 bit. Tahan terhadap serangan yang lain, yaitu serangan chosen plaintext dan mathematical attack. Dalam chosen palintext attack, penyerang akan membiarkan lawannya mengenkrip plaintext yang ditentukan, agar penyerang mengetahui pasangan plaintext dan ciphertext untuk mendapatkan kunci atau algoritma yang digunakan. Dalam Serangan mathematical, penyerang menggunakan model matematika seperti differential cryptanalysis, linear cryptanalysis dan algebraic untuk mendekripsi ciphertext [Suryanto, 2015].

2.6 Fungsi Komposisi

Fungsi komposisi merupakan penggabungan operasi dua jenis fungsi f(x) dan g(x) sehingga menghasilkan sebuah fungsi baru. Operasi fungsi komposisi biasa dilambangkan dengan "o" dan dibaca komposisi atau bundaran. Fungsi baru yang dapat terbentuk dari f(x) dan g(x) adalah:

- (f o g)(x) artinya g dimasukkan ke f
- (g o f)(x) artinya f dimasukkan ke g

Fungsi tunggal tersebut merupakan fungsi yang dapat dilambangkan dengan huruf “f o g” atau juga dapat dibaca “fungsi f bundaran g”. Fungsi “f o g” adalah fungsi g yang dikerjakan terlebih

dahulu kemudian dilanjutkan dengan f. Sedangkan, untuk fungsi “g o f” dibaca fungsi g bundaran f. Jadi, “g o f” adalah fungsi dengan f dikerjakan terlebih dahulu daripada g.Fungsi .

2.7 Operasi Logika Exclusive Or

Bit (binary digit) adalah sebuah simbol dengan dua nilai kemungkinan yaitu 0 dan 1. Bit dapat digunakan untuk merepresentasikan tabel kebenaran. Merepresentasikan benar dengan 1 bit dan mereprentasikan salah dengan 0 bit. Ada beberapa operasi yang digunakan untuk bit diantarnya adalah OR, AND, dan XOR. Operasi XOR adalah operasi bit yang akan digunakan pada penelitian ini. Simbol operasi XOR adalah⊕. Pernyataan p⊕q akan bernilai benar ketika tepat salah satu dari p atau q bernilai benar. Namun tidak keduanya. Berikut adalah tabel XOR untuk bit [Rosen, 2012].

Tabel 2.1: Operator XOR untuk bit

p	q	$p \oplus q$
0	0	0
0	1	1
1	0	1
1	1	0

Tampilan pada tabel 2.1 operasi XOR bersifat komutatif, yaitu p⊕q = q⊕p. Identitas dari operasi XOR adalah 0. Karena a⊕0 = a,a = 0,1. Berdasarkan tabel 2.1 terlihat bahwa invers dari tiap elemen yaitu −a = a sehingga disimpulkan bahwa operasi invers dari XOR adalah XOR itu sendiri.

2.8 FPGA

FPGA Field Programmable Gate Array (FPGA) merupakan sebuah IC digital yang sering digunakan untuk mengimplementasikan rangkaian digital. Bila dilihat dari segi namanya, Field Programmable dapat diartikan bahwa FPGA ini bersifat dapat dirancang sesuai dengankeinginan dan kebutuhan user/pemakai.

Proposal penelitian ini merupakan hasil dari perkembangan penelitian sebelumnya, beberapa jurnal penelitian yang digunakan sebagai studi literur atau state of the art dari proposal ini adalah sebagai berikut :

1. "**The composition of the improved logistic map and the MS map in generating a new chaotic function**"

Penelitian ini dilakukan Suryadi MT, Venny Melvina, Luqman N Prawadika, Yudi Satria, penelitian ini menggunakan konsep yang mengkomposisikan dua fungsi chaos yaitu chaos MS map dan Dyadic Transformation sehingga menghasilkan fungsi chaos yang baru dengan diuji berbagai tahapan. Dalam penelitian ini fungsi baru di uji dengan diagram bifurkasi yaitu dengan algoritma sebagai syarat fungsi tersebut sebagai fungsi chaos atau tidak.

Input : x_0 , λ , dan r
Output : plot nilai x_n

1. Masukkan semua nilai awal, nilai parameter, banyaknya iterasi (i)
2. For n = 1 to i
3. Hitung nilai x_n berdasarkan fungsi MSDT Map
4. Plot nilai x_n
5. Next n
6. Selesai

Setelah dilakukan pengujian bifurkasi lalu dilakukan pengujian dengan Diagram Lyapunov Exponent yaitu dengan algoritma :

Input : x_0 , λ , dan r
Output : plot nilai $h(x)$

1. Masukkan semua nilai awal, nilai parameter, banyaknya iterasi (n)
2. For j = 1 to n
3. Hitung nilai $h(x_j)$ berdasarkan persamaan (10)
4. Plot nilai $h(x)$
5. Next j
6. Selesai

Dan yang terakhir digunakan Uji keacakan NIST yaitu untuk melihat hasil keacakan baik atau tidak.

Tabel 1. Hasil Uji keacakan NIST dari Fungsi Chaos MSDT

Type of Test	P-Value	Conclusion
01. Frequency Test (Monobit)	0.73386	Random
02. Frequency Test within a Block	0.64962	Random
03. Run Test	0.06858	Random
04. Longest Run of Ones in a Block	0.02275	Random
05. Binary Matrix Rank Test	0.33069	Random
06. Discrete Fourier Transform (Spectral) Test	0.27081	Random
07. Non-Overlapping Template Matching Test	0.66691	Random
08. Overlapping Template Matching Test	0.13058	Random
09. Maurer's Universal Statistical test	-1.0	Non-Random
10. Linear Complexity Test	0.83337	Random
11. Serial test:	1.14e-09	Non-Random
	0.02930	Random
12. Approximate Entropy Test	4.89e-15	Non-Random
13. Cummulative Sums (Forward) Test	0.92503	Random
14. Cummulative Sums (Reverse) Test	0.62922	Random
15. Random Excursions Test	0.29910 *	Random
16. Random Excursions Variant Test	0.38202 *	Random

2. “Colour image encryption using Nahrain chaotic map”

Penelitian ini di lakukan oleh Hamsa A. Abdullah dan Hikmat N. Abdullah paada tahun 2019. Penelitian ini menggunakan fungsi chaos yang diberi nama fungsi chaos nahrain.

$Xn+1=1-aXnYn-Xn2-Yn2$

$Yn+1=Xn$

$Zn+1=Yn-bZn$

Pada penelitian ini untuk menguji fungsi chaos nahrain dengan uji NIST

Table 1 The results of the randomness tests

Test	*X*	*Y*	*Z*	*P-value ≥ (0.01–0.001)*
Frequency (MonoBit) Test	0.5787	0.5787	0.2739	Accept
Frequency (Block =1000) Test	0.5031	0.5168	0.8993	Accept
Run Test	0.5917	0.5917	0.2855	Accept
Longest run of ones in a block (128)	0.9931	0.9997	0.9606	Accept
Binary Matrix Rank Test	0.2030	0.2030	0.0433	Accept
DFT Test	0.4118	0.3049	0.4118	Accept
Maurer's Test	0.8604	0.8744	0.8670	Accept
Approximate Entropy Test	0.4002	0.4002	0.5458	Accept
Cumulative Sum Test	0.9767	0.9767	0.5458	Accept
Random Excursions Test	0.1085	0.1085	0.0253	Accept
Random Excursions Variant Test	0.8808	0.8814	0.9042	Accept

3. "**FPGA implementation of color image encryption using a new chaotic map**"

Penelitian ini di lakukan oleh Hamsa A. Abdullah dan Hikmat N. Abdullah paada tahun 2019. Penelitian ini menggunakan fungsi chaos yang diberi nama fungsi chaos nahrain dengan metode enkripsi dan deskripsinya menggunakan diffusion.

$Xn+1=1-aXnYn-Xn2-Yn2$

$Yn+1=Xn$

$Zn+1=Yn-bZn$

Dengan fungsi chaos nahrain ini di implementasikan kedalam FPGA

Hasil percobaan dengan FPGA

Analysis & Synthesis CPU Time Image size	Encryption time (in sec.)	Decryption time (in sec.)
64x64	0.44	1.16
128x128	1.20	1.24
176x144	1.55	2.04
256x256	4.14	4.35

4. “ **Image Encryption using Simple Algorithm on FPGA**”

Penelitian ini di lakukan oleh Barlian Henryranu Prasetio, Eko Setiawan dan Adharul Muttaqin pada tahun 2015

Berdasarkan hasil pengujian disimpulkan bahwa metode enkripsi pada sop enkripsi citra dapat diimplementasikan ke dalam modul FPGA. Metode sederhana dapat mengenkripsi citra asli (plain-image) menjadi citra terenkripsi (cipher-image) yang berbeda. Metode implementasi enkripsi ke modul fPGA dilakukan dengan set pertama modul input output sesuai dengan konfigurasi perangkat keras yang digunakan. Keberhasilan implementasi merupakan titik awal penerapan enkripsi gambar pada perangkat kecil. Datasheet modul Xilinx Spartan-3E FPGA menjelaskan bahwa hanya dapat menangani data gambar maksimal 3 bit . Penggunaan perangkat FPGA mampu menangani gambar dengan bit yang lebih besar, akan dapat mengenkripsi gambar dengan banyak pilihan warna. Dari hasil pengujian, waktu pemrosesan citra tanpa enkripsi rata-rata 4,999ns dan 13,51ns dengan enkripsi.

image size Image size (px)	Without encryption (ns)	With encryption (ns)
1x1	5.001	13.514
10x1	50.003	135.150
10x5	250.035	675.700
10x10	500.002	1351.500
20x50	5000.006	13514.200
20x80	8000.001	21624.000
40x90	18000.024	48650.400
40x100	20000.864	54056.000
50x100	25001.359	67570.089
50x150	37500.997	101362.500
75x150	56251.000	152032.500
75x200	75000.056	202734.080
100x200	100000.845	270280.100
100x250	125000.126	337825.005
150x300	225000.221	608130.013

5. **“Implementasi Algoritma Chaos-Based Feedback Stream Cipher pada Enkripsi-Dekripsi Data Citra Digital “**

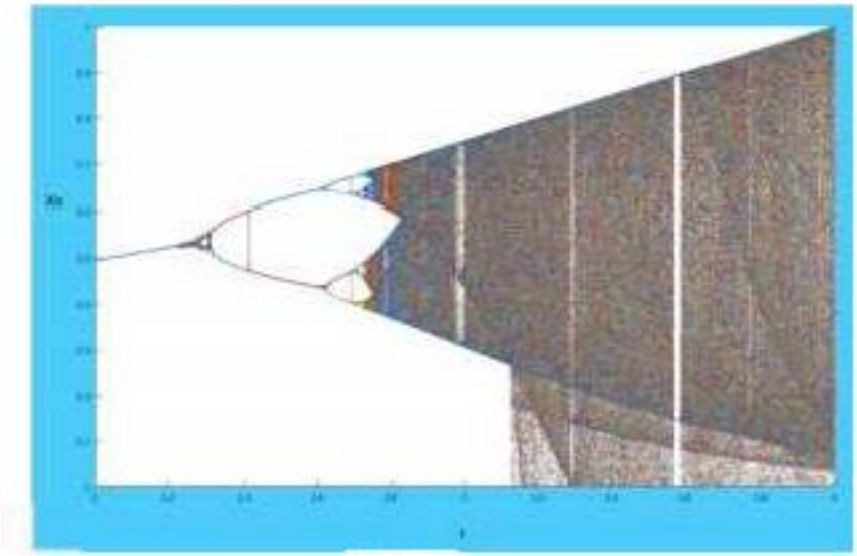
Penelitian ini di lakukan oleh Theresia Anna , M. A. Ineke Pakereng,dan Yos Richard Beeh pada tahun 2009.

Penelitian ini merupakan implementasi algoritma CBFSC pada citra digital 2 (dua) dimensi dari jurnal yang dibuat oleh Hossam El-din H. Ahmed, dkk pada tahun 2005 [7].

6. **“IMPLEMENTASI ALGORITMA ENKRIPSI CITRA DIGITAL BERBASIS CHAOS MENGGUNAKAN FUNGSI KOMPOSISI LOGISTIC DAN GAUSS ITERATED MAP”**

Penelitian ini di lakukan oleh Suci Boru Kembaren , Suryadi dan Triswanto pada tahun 2018.

Pada penilitian ini diperoleh hasil Diagram Bifurkasi Disimulasikan diagram bifurkasi dari Log-gauss Map dengan bantuan komputer. nilai awal yang dipakai adalah X0= 0,7, α =4,2,dan β = 0,2kemudian di plot hasil pemetaan dari Log-gauss Map dimulai dari iterasi 1 sampai 50 untuk tiap – tiap nilai .



Gambar Bifukasi diagram Log-gauss Map iterasi ke 200

BAB III
Metodologi penelitian

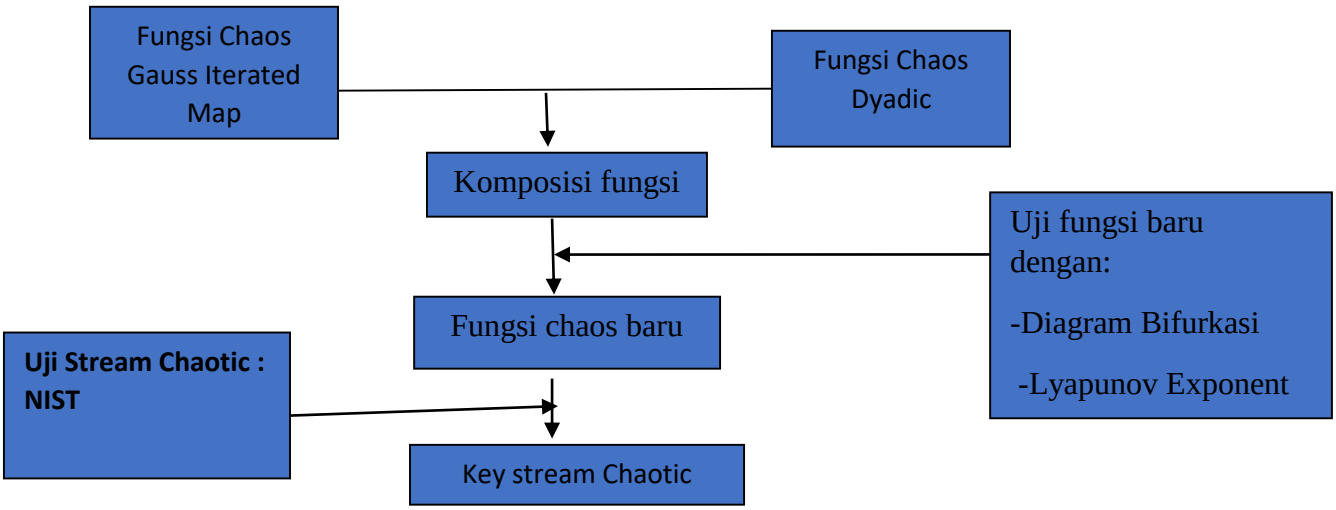
Metode penelitian yang digunakan untuk proposal penelitian ini adalah sebagai berikut:

1. Studi pustaka yaitu mencari dan mempelajari jurnal-jurnal, buku-buku dan artikel-artikel dari internet yang menunjang konsep.
2. Penguraian materi yang relevan melalui analisis pustaka.
3. Menentukan komposisi fungsi fungsi chaotic yang diajukan
4. Menguji fungsi baru yang sudah dikomposisikan
5. Menguji hasil komposisi chaos baru dengan NIST
6. Mensimulasikan komposisi chaos baru sebagai keystream dengan input gambar digital melalui enkripsi dan deskripsi dengan Subtitusi XOR
7. Menguji data berupa gambar dengan menggunakan bahasa perangkat keras (HDL) pada FPGA.
8. Analisis hasil enkripsi dan dekripsi dengan FPGA

Model Operasional Penelitian

Berikut ini adalah gambaran alur kerja dari proses pembangkit key stream.

Diagram Komposisi Fungsi chaos Baru dan pegujian key stream chaotic



Gambar 3.1 Proses pembangkit Key stream

Komposisi Fungsi Gauss Iterated Map dan Fungsi Dyadic Transformation (GDT)

Fungsi komposisi merupakan penggabungan operasi dua jenis fungsi f(x) dan g(x) sehingga menghasilkan sebuah fungsi baru. Operasi fungsi komposisi biasa dilambangkan dengan "o" dan dibaca komposisi atau bundaran. Fungsi baru yang dapat terbentuk dari f(x) dan g(x) adalah:

- (f o g)(x) artinya g dimasukkan ke f
- (g o f)(x) artinya f dimasukkan ke g

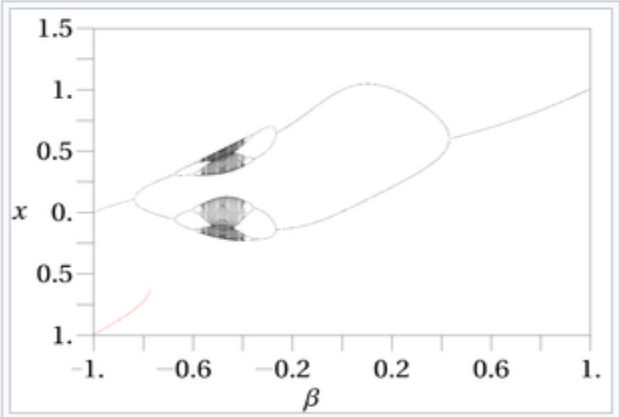
Fungsi tunggal tersebut merupakan fungsi yang dapat dilambangkan dengan huruf “f o g” atau juga dapat dibaca “fungsi f bundaran g”. Fungsi “f o g” adalah fungsi g yang dikerjakan terlebih dahulu kemudian dilanjutkan dengan f. Sedangkan, untuk fungsi “g o f” dibaca fungsi g bundaran f. Jadi, “g o f” adalah fungsi dengan f dikerjakan terlebih dahulu daripada g.Fungsi

1. Fungsi Gauss Iterated Map

$f(x) = Exp(-\alpha x^2) + \beta$

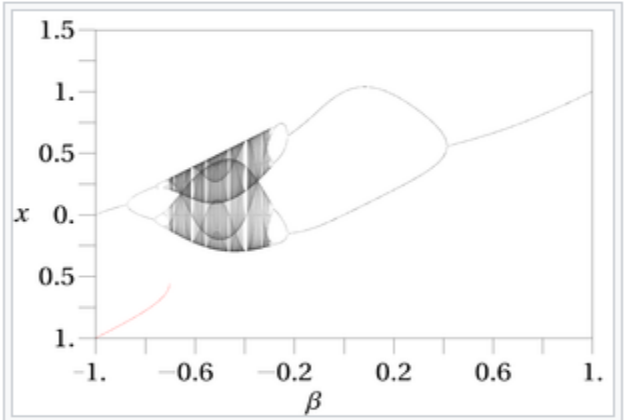
Fungsi Gauss Iterated Map ini memiliki kemampuan yang tinggi untuk mengamankan citra RGB [Ajita, at al., 2017]. Fungsi Gauss Iterated Map menggunakan tiga parameter yaitu : xn ,α dan β dimana untuk $x0$ (n=0) merupakan nilai awal parameter dari xn . Algoritma Gauss Iterated Map memiliki konsumsi daya yang rendah dan waktu enkripsi dan deskripsi yang lebih cepat.

Gambar bifurkasi Gauss Iterated Map



Bifurcation diagram of the Gauss map with $\alpha = 4.90$ and β in the range −1 to +1. This graph resembles a mouse.

Gambar 3.2 Bifurkasi Gauss Map α = 4.9



Bifurcation diagram of the Gauss map with $\alpha = 6.20$ and β in the range −1 to +1.

Gambar 3.2 Bifurkasi Gauss Map α = 6.2

2. Fungsi Dyadic Transformation

$$g(x) = \begin{cases} 2x & , 0 \le x < 0.5 \\ 2x - 1 & , 0.5 \le x < 1 \end{cases}$$

Fungsi Dyadic Transformation merupakan Fungsi matematika berhasil banyak yaitu:

Fungsi g(x) = 2x , jika $0 \le x < 0.5$

Fungsi g(x) = 2x – 1 , jika $0.5 \le x < 1$

3. Sehingga Fungsi Gauss Iterated Map dan Fungsi Dyadic Transformation Di komposisikan menjadi:

$$(f \circ g)(x) = \begin{cases} Exp(-\alpha(2x)^2) + \beta & , \ 0 \le x < 0.5 \\ Exp(-\alpha(2x-1)^2) + \beta & , \ 0.5 \le x < 1 \end{cases}$$

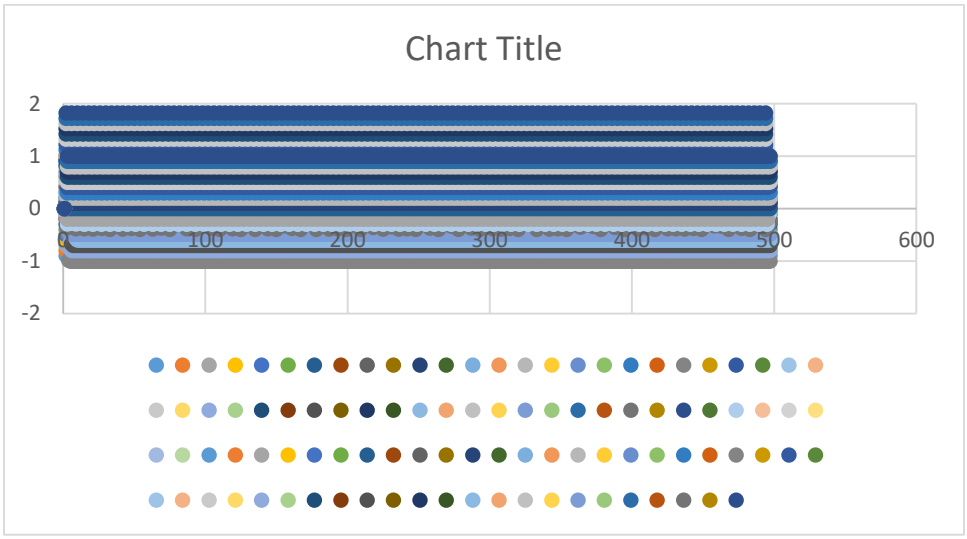
Dalam bentuk rekursinya menjadi :

$$(f \circ g)(x_{n+1}) = \begin{cases} Exp(-\alpha(2xn)^2) + \beta & , \ 0 \le x < 0.5 \\ Exp(-\alpha(2xn-1)^2) + \beta & , \ 0.5 \le x < 1 \end{cases}$$

Pengujian chaos fungsi baru GDT dengan bifurkasi.

Diagram bifurkasi adalah diagram yang menunjukkan nilai yang didekati secara asimptotik dari suatu system sebagai fungsi dari parameter dalam system. Dengan melihat diagram bifurkasi, kita dapat mengetahui sifat chaos suatu fungsi. Jika titik-titik periodik pada diagram bifurkasi padat, maka fungsi tersebut chaos [1,25].

Pengujian dengan manual dengan menggunakan MS EXCEL



Gambar 3.3 Hasil Bifurkasi dengan Excel

Nilai x=0.1 , α = 4.9 , β = -1 sampai 1 dengan rentangan 0.1 dan iterasi 500

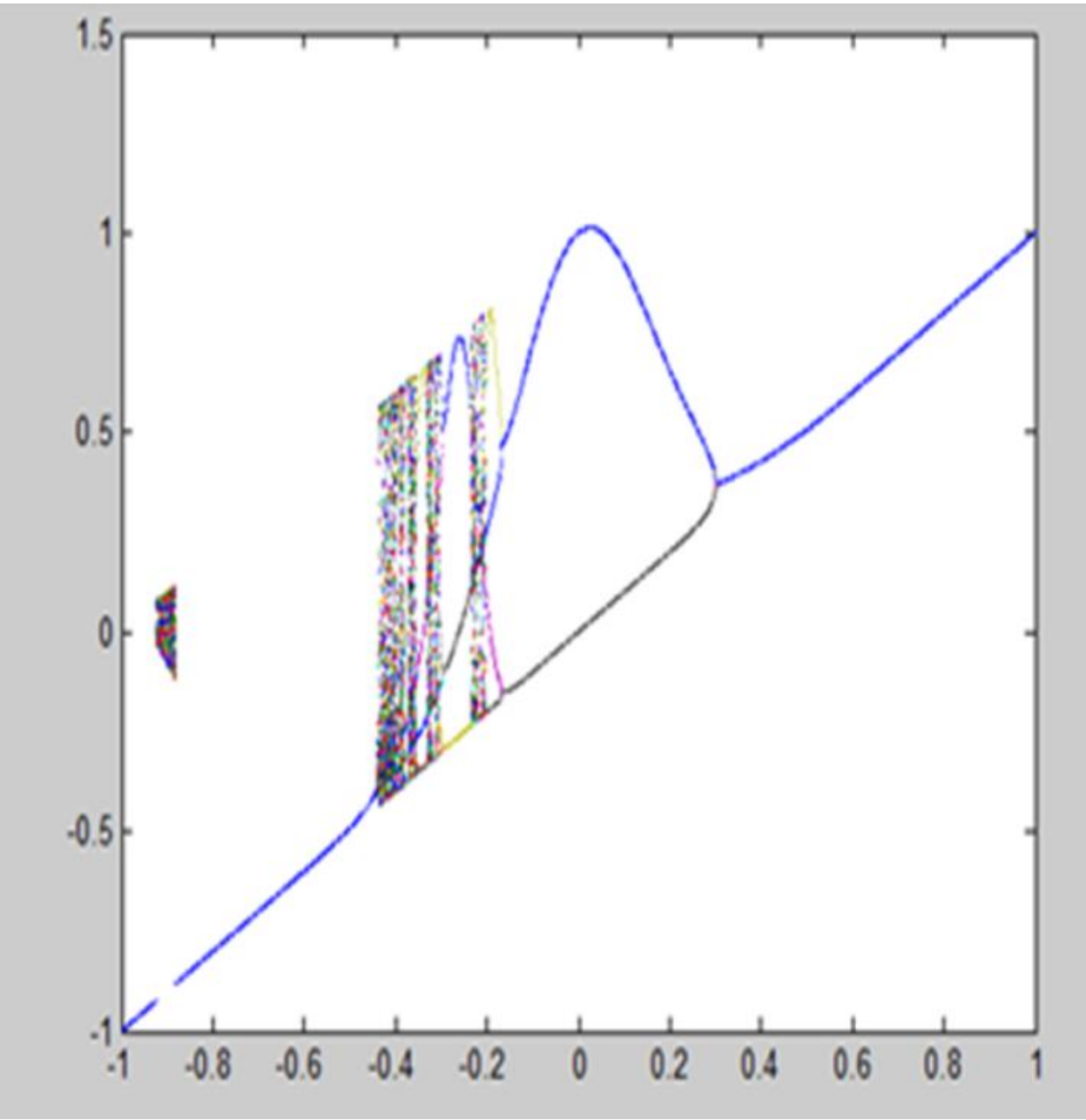
Algoritma yang digunakan untuk bifurkasi untuk fungsi GDT adalah :

Input : parameter α , β dan Xo

Output : plot nilai β dan Xn

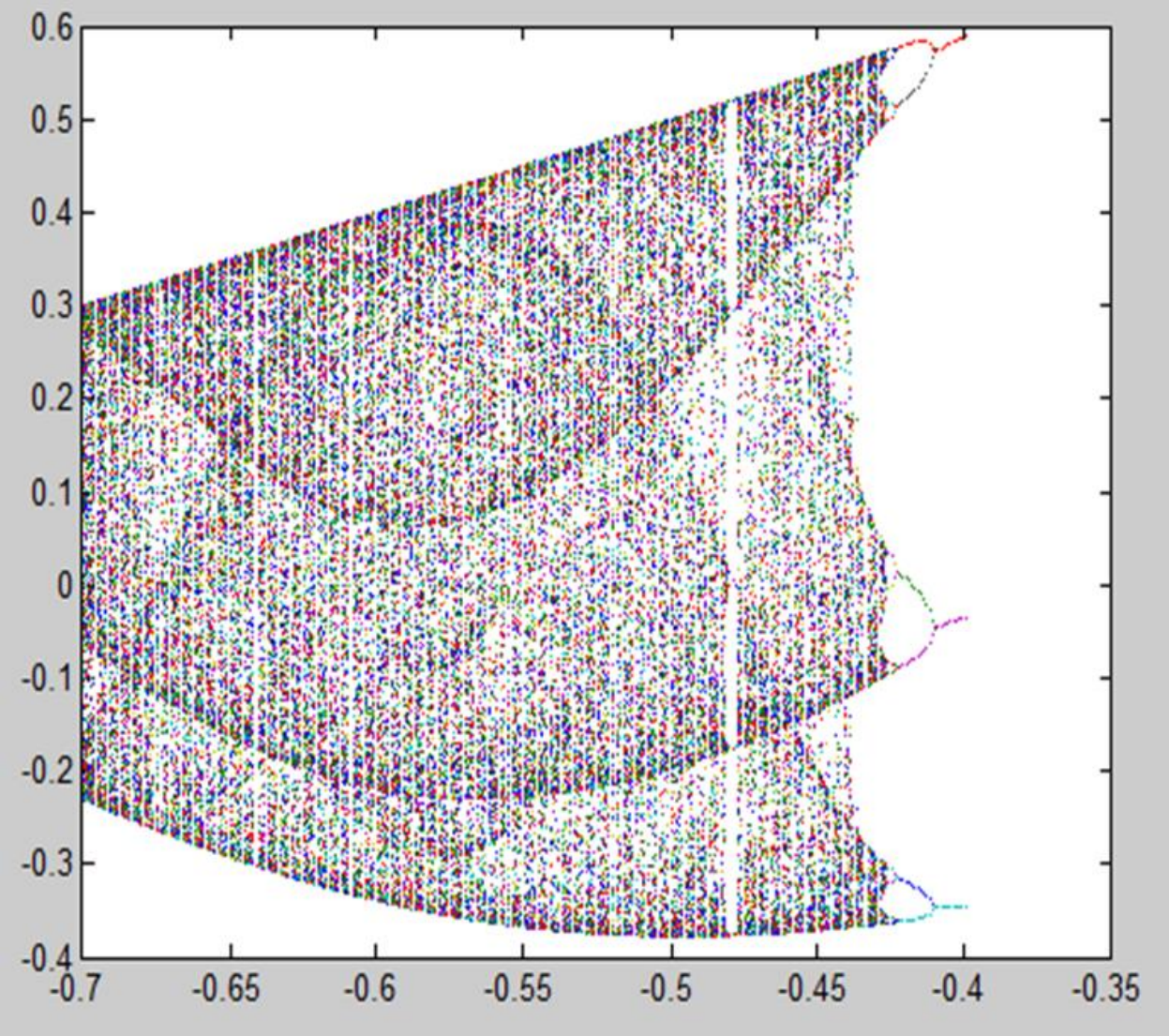
1. Masukkan semua nilai awal, nilai parameter, banyaknya iterasi (i)
2. For n = 1 to i
3. Hitung nilai Xn berdasarkan fungsi GDT Map
4. Plot nilai β dan Xn
5. Next n
6. Selesai

Dengan bantuan software hasil dari diagram bifurkasi



Gambar 3.4 Bifurkasi Fungsi GDT dengan α 4.9

```
a=4.9
b= -1:0.001:1
Xo= 0.1
```



Gambar 3.5 Bifurkasi Fungsi GDT dengan α 4.2

```
a=4.2
b= -0.7:0.001:-0.4;
Xo= 0.1
```

- Setelah ada fungsi baru , maka fungsi baru ini diuji dengan diagram bifurkasi dan diagram Lyapunov exponent yang menentukan apakah fungsi baru ini bersifat chaos atau tidak.

- Setelah fungsi baru ini memenuhi kriteria menjadi fungsi chaos, selanjutnya akan di uji dengan menggunakan uji keacakan NIST untuk melihat apakah fungsi chaos baru ini baik atau tidak dengan nilai nilai statistik yang di tampilkan.

Ada beberapa algoritma untuk proses enkripsi yaitu dengan diffusi, permutasi ataupun kombinasi dari kedua Algoritma yang disebutkan akan tetapi pada penelitian untuk proses enkripsi dan deskripsi adalah menggunakan algoritma Subtitusi dengan XOR

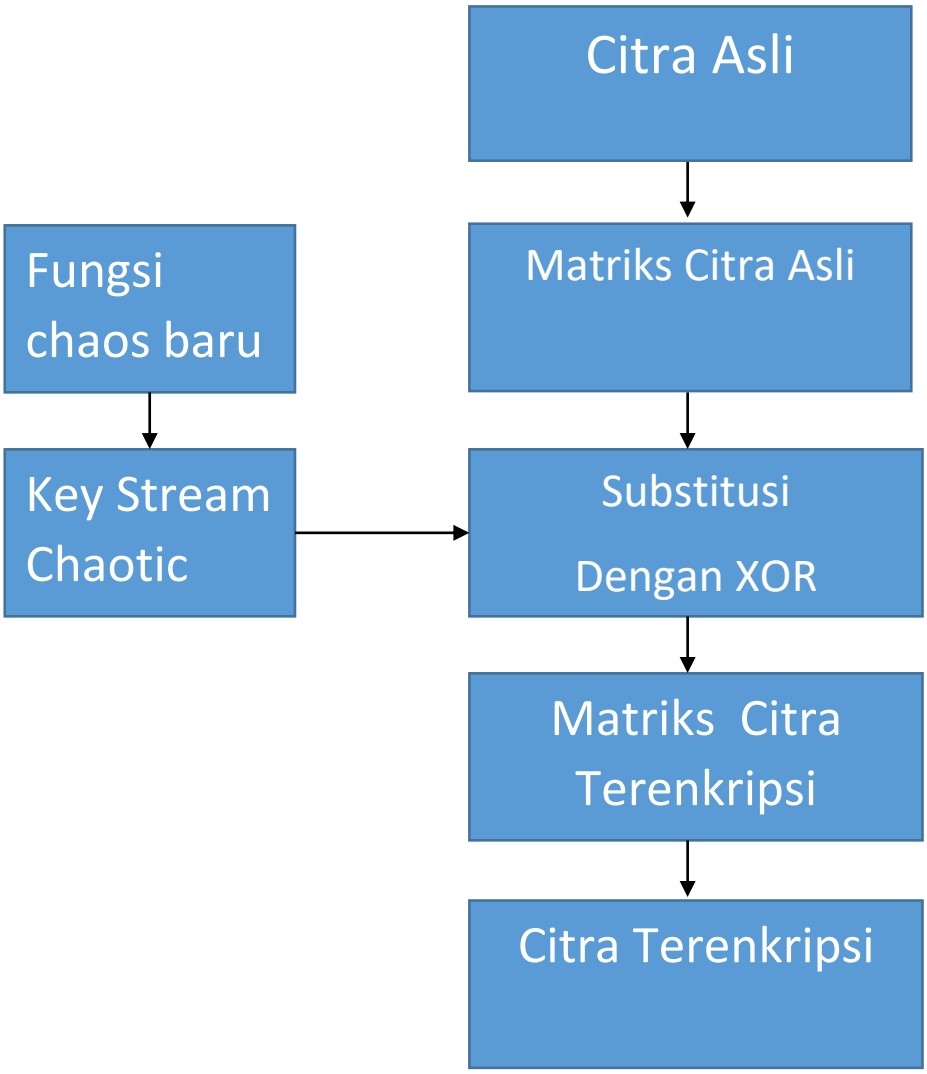
Algoritma dengan subtitusi XOR dan Keystream Chaotic.
Pembuktian invertible Operator XOR

- $Ci = Pi \oplus Ki$ → proses enkripsi
- $Pi = Ci \oplus Ki$ → proses dekripsi
- $Pi = Ci \oplus Ki = (Pi \oplus Ki) \oplus Ki$
- $= Pi \oplus (Ki \oplus Ki)$ → sifat asosiatif
- $= Pi \oplus (0)$ → sifat identitas
- $Pi = Pi$ → terbukti

Dimana :
Ci adalah Citra Terenkripsi (Cipher image)
Pi adalah Citra Asli (Plain image)
Ki adalah KeyStream Chaotic

Model Operasional Penelitian

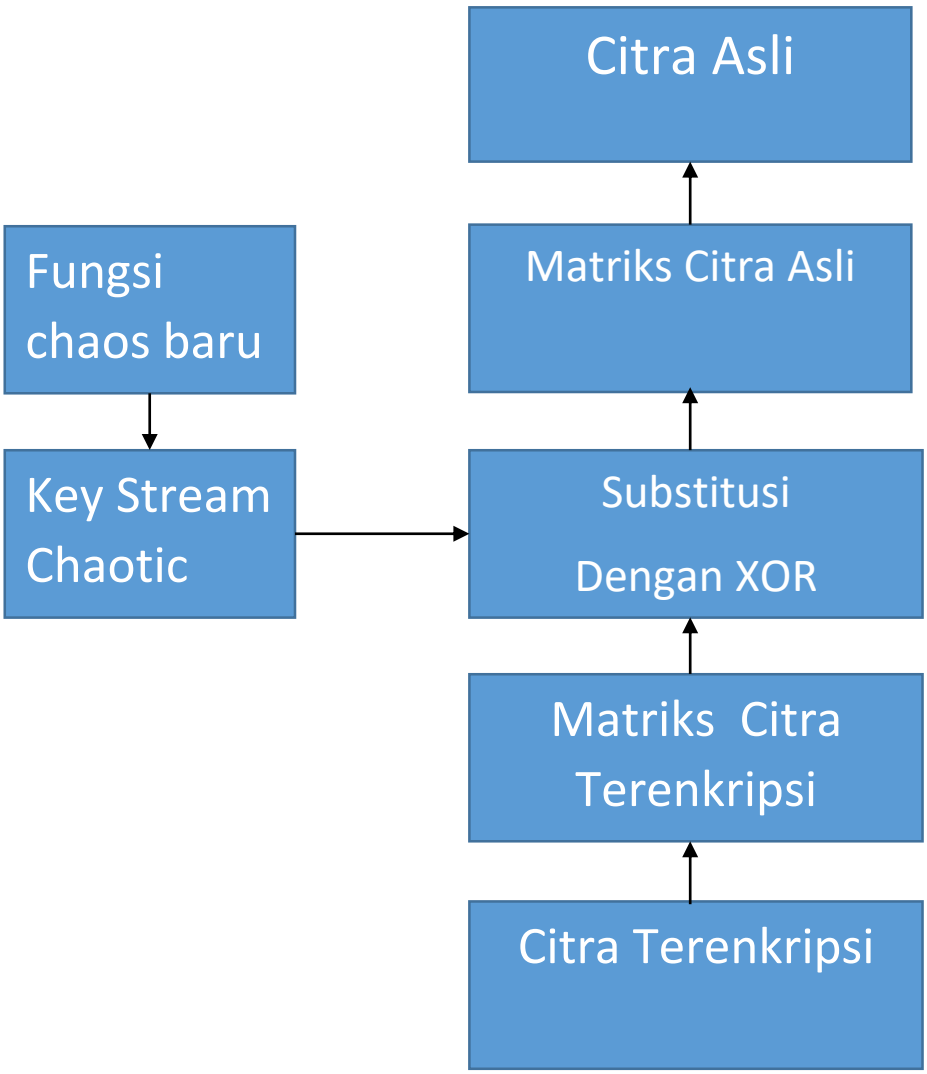
Proses Enkripsi



Gambar 3.6 Proses Enkripsi

Model Operasional Penelitian

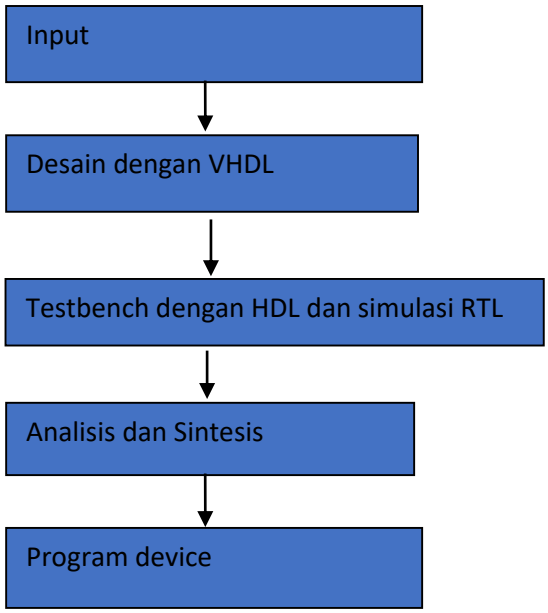
Proses Deskripsi



Gambar 3.7 Proses Deskripsi

- Baca citra ubah ke data matriks menjadi output matriks
- Baca matriks tersebut dan ubah jadi citra menjadi output citra
- Inputnya matriks menjadi Ubah matriks (tukar baris atau dan tukar kolom) ubah jadi citra menjadi output citra
- Input citra yang sdh diubah lalu kembalikan ke citra aslinya

Garis besar Langkah dalam implementation perangkat keras FPGA



- Mendesain system dan menurunkannya ke Hardware Description Language (HDL) file. Dengan menggunakan Very High-Speed Integrated Circuit HDL
- Mengembangkan testbench dengan HDL dan membuat simulasi pada Register Transfer Level (RTL) , menentukan karakteristik rangkaian dari operasi dan transfer data antara register. Desain RTL berisi kemungkinan waktu yang tepat.
- Men-synthesis HDL
- Terakhir adalah mengenerate dan mendownload programming file.File ini berisi konfigurasi FPGA yang bisa di download keperangkat FPGA untuk diujicobakan.

Rencana Kegiatan

Untuk mencapai target penelitian/ desertasi, maka penulis menyusun rencana kegiatan berupa jadwal kegiatan yang berguna untuk memastikan agar capaian yang ditetapkan dapat dipenuhi sesuai waktu yang telah ditetapkan. Adapun jadwal yangakan digunakan sebagai beikut :

	2021		2022												
Bentuk Kegitatan	11	12	1	2	3	4	5	6	7	8	9	10	11	12	Uraian
Bimbingan															Penyusunan Proposal Kualifikasi
Ujian Kualifikasi															Penajaman Proposal
Evaluasi Progress															Pembangkitan Keytream , proses enkripsi dan deskripsi serta implementasi ke FPGA
Evaluasi RKP															Kesimpulan/Hasil
Sidang Tertutup															Penajaman Hasil
Sidang Terbuka															

Referensi :

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

Hamsa A. Abdullah, Hikmat N. Abdullah *Colour image encryption using Nahrain chaotic map* Int. J. Wireless and Mobile Computing, Vol. 17, No. 2, 2019

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*

Barlian Henryranu Prasetio, Eko Setiawan, Adharul Muttaqin *Image Encryption using Simple Algorithm on FPGA* TELKOMNIKA, Vol. 13, No. 4, December 2015, pp. 1153~1161 ISSN: 1693-6930

Theresia Anna , M. A. Ineke Pakereng,dan Yos Richard Beeh , *"Implementasi Algoritma Chaos-Based Feedback Stream Cipher pada Enkripsi-Dekripsi Data Citra Digital "*Jurnal Informatika, Vol.5, No.2, Desember 2009: 151 – 169

Suci Boru Kembaren , Suryadi dan Triswanto , "*IMPLEMENTASI ALGORITMA ENKRIPSI CITRA DIGITAL BERBASIS CHAOS MENGGUNAKAN FUNGSI KOMPOSISI LOGISTIC DAN GAUSS ITERATED MAP"* Seminar Nasional Edusainstek FMIPA UNIMUS 2018 , ISBN : 978-602-5614-35-4