UNIVERSITAS GUNADARMA

PROGRAM STUDI DOKTORTEKNOLOGI INFORMASI

PENGEMBANGAN FUNGSI CHAOS BARU MENGGUNAKAN FUNGSI KOMPOSISI DYADIC TRANSFORMATION MAP DAN CIRCLE MAP

Pembimbing

Prof. Dr. Sarifuddin Madenda

Disusun oleh

Nama : Ari Rosemalatriasari
NPM : 99214910

Jakarta
2021

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan data merupakan aspek penting dalam komunikasi modern, dan keamanan yang lebih tinggi sangat dibutuhkan seiring dengan perkembangan teknologi dari waktu ke waktu, termasuk dalam pelanggaran keamanan. Data atau informasi baik dalam bentuk tulisan, suara, gambar bahkan video disajikan secara digital dan kemudian dapat disimpan ataupun dikrimkan melalui jaringan dalam bentuk data digital. Namun kerahasiaan dan kemanan data digital yang dikirimkan melalui jaringan belum terjamin dengan baik, karena adanya serangan-serangan yang bertujuan untuk mencuri atau bahkan memodifikasi isi data tersebut. Maka dibutuhkan suatu cara untuk tetap menjaga kerahasiaan dan keamanan data digital yang dimiliki, salah satu caranya yaitu dengan penerapan kriptografi.

Salah satu bentuk data digital yang membutuhkan penanganan khusus pada proses kriptografi adalah citra digital. Kapasitas data yang besar dan redudansi data yang tinggi pada citra digital menjadikannya sulit untuk ditangani dengan kriptografi tradisional. Kesulitan utamanya adalah bagaimana cara untuk mengacak data ataupun informasi yang terdapat pada citra digital tersebut. Salah satu sistem pengamanan data menggunakan metode enkripsi dan dekripsi data. Yang lebih diutamakan dalam enkripsi gambar digital adalah waktu yang lebih cepat tanpa mengorbankan keamanannya. Salah satu metode enkripsi yang memenuhi hal tersebut adalah enkripsi gambar digital berbasis chaos. Metode ini memberikan kombinasi yang baik dari segi kecepatan, keamanan yang tinggi, kompleksitas, dan daya komputasi (Pareek, Patidar, dan Sud, 2006).

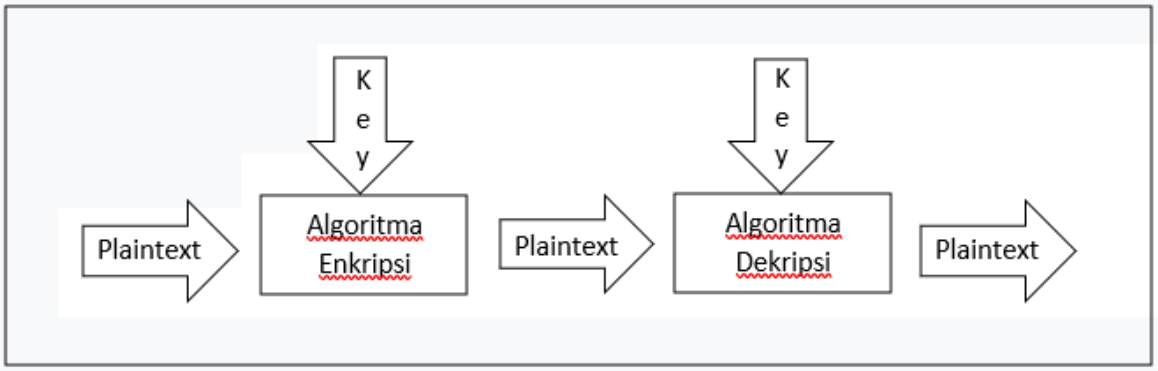
Teknik dalam enkripsi citra digital yang akan digunakan adalah kriptografi berbasis *chaos*. Kriptografi adalah suatu metode yang umum digunakan untuk melindungi berbagai macam data yang prosesnya di sebut dengan enkripsi, yaitu suatu proses yang mengkonversi sebuah pesan plaintext menjadi sebuah chipertext yang bisa dibalik ke bentuk asli seperti semula, yang biasa disebut sebagai proses decoding atau dekripsi (Ariyus, Dony, 2008).

Ada beberapa istilah dalam kriptografi, diantaranya adalah plaintext, cipherteks, enkripsi dan dekripsi. Plaintext adalah data asli. Ciphertext adalah data yang sudah disandikan. Enkripsi adalah proses mengubah plainteks menjadi cipherteks. Dekripsi adalah roses mengubah Kembali ciphertext menjadi plainteks. Diperlukan sebuah kunci dalam

proses enkripsi dan dekripsi yang hanya diketahui oleh pengirim dan penerima (Stalling, 2014).

Ilmu kriptografi dilihat dari era pengembangannya di bagi menjadi dua, yaitu kriptografi klasik dan kriptografi modern. Kekuatan kriptografi klasik terletak pada kerahasiaan algoritma yang digunakan. Sedangkan pada kriptografi modern, algoritma yang digunakan tidak bersifat rahasia. Kekuatan kriptografi modern terletak pada kerahasiaan kunci penyandian.

Berdasarkan kunci penyandiannya, kriptografi di bagi menjadi dua jenis, yaitu kriptografi kunci simetri dan kriptografi kunci asimetri. Metode enkripsi dan dekripsi pada kriptografi simetri menggunakan kunci yang sama, sedangkan kriptografi kunci asimetri menggunkan kunci yang berbeda. Ada beberapa metode dalam penyandian diantaranya adalah dengan algoritma *Data Encryption Standard* (DES), algoritma *Advanced Encryption Standard* (AES), dan algoritma *Rivest-Shamir_Adleman* (RSA) (Stalling, 2014). Algoritma-algoritma tersebut membutuhkan waktu komputasi yang lama dan daya komputasi yang tinggi, walaupun demikian menghasilkan data yang terenkripsi dengan baik.



Gambar 1.1 Kriptografi Berbasis Kunci

Teori chaos sendiri berasal dari teori system yang memperlihatkan kemunculan yang tidak teratur, meskipun teori ini digunakan untuk menjelaskan kemunculan data acak (Ariyus, Dony, 2008). *Chaos* adalah tipe perilaku suatu system ataupun fungsi yang bersifat acak, peka terhadap nilai awal dan *ergodicity* (frekuensi bilangan yang dibangkitkan merata). Fungsi yang bersifat chaos dinamakan fungsi chaos. Fungsi chaos telah dibuktikan sangat cocok untuk merancang sarana untuk pengamanan data (kocarev dan Lian, 2011). Fungsi chaos nantinya kan digunakan sebagai pembangkit bilangan acak yang kemudian akan digunakan sebagai *keystream* pada proses enkripsi. Ada banyak jenis fungsi *chaos*

yang digunakan bervariasi, antara lain *Logistic map, Baker's map, Arnold's cat map, Tent map*, *Dyadic Transformation map*, dan *Circle map*.

Dua fungsi chaos yang sudah dikenal menunjukkan sifat chaos adalah Dyadic Transformation Map dan Circle Map. Keduanya memiliki potensi keacakan yang tinggi.

Algoritma MS Gauss Map merupakan kombinasi Logistic Map dan Gauss Iterated Map dengan cara mengkomposisikan kedua fungsi [Suci, Suryadi, Triswanto, 2018]. MS Gauss Map menghasilkan ruang kunci sebesar 1.8×10^{79} dengan nilai sensitivitas kunci sebesar 10^{-16}, sehingga algoritma ini susah diserang dengan brute force attack. Selain itu, pengujian serangan pada data citra terenkripsi menggunakan statistical attack dan diferential attack menunjukkan bahwa algoritma ini memiliki daya tahan tinggi.

Algortima komposisi secara sekuensial Gauss Map dan Circle Map [Yudi, Suryadi, Luqman, 2019]. Metode ini digunakan untuk menyelidiki kemungkinan memiliki sifat chaos yang lebih besar. Algortima ini memiliki diagram sensitivitas yang jauh lebih besar terhadap nilai awal, meskipun masih kurang cocok untuk RNG karena hanya 4 yang memenuhi dari 16 uji NIST, artinya tingkat keacakannya hanya 25%. Oleh karena itu, jika Gauss-Circle Map ini digunakan untuk tujuan kriptografi_, sistem kriptografi yang menggunakannya akan memiliki ketahanan brute force attack yang kuat, tetapi mungkin lemah terhadap statistical attack.

Komposisi MS Map dan Dyadic Transformation Map [Suryadi MT, Venny, Luqman, Yudi, 2019]. Berdasarkan diagram bifurkasi terlihat bahwa untuk nilai $\lambda \in$ (0.3, 5) memiliki kerapatan yang lebih baik pada saat r = 3.8. hasil Lyapunov exponent menunjukkan nilai yang non negative terpenuhi untuk r $\in$ [1,4]. Hasil uji NIST dengan nilai awal dan nilai parameter x_0 = 0.6, r = 3.8, dan λ = 3.5 serta tingkat keacakannya mencapai 82.4% dari hasil uji keacakan NIST.

Berdasarkan beberapa penelitian tersebut diatas maka pada penelitian ini dikembangkan suatu fungsi baru yang bersifat chaos untuk membangkitkan keystream dengan komposisi fungsi Dyadic Transformation Map dan Circle Map dengan tujuan untuk meningkatkan daya tahan algoritma enkripsi terhadap berbagai serangan.

1.1 Rumusan Masalah Penelitian

1. Bagaimana merumuskan satu fungsi chaos baru melalui Dyadic Transformation Map dan Circle Map.

2. Bagaimana merancang dan mengimplementasikan algoritma untuk mengenkripsi dan mendekripsi citra digital menggunakan fungsi chaos baru tersebut.
3. Bagaimana mengukur kinerja algoritma enkripsi dan dekripsi citra digital menggunakan fungsi chaos baru tersebut.

1.2 Tujuan Penelitian

Tujuan penelitian ini adalah :

1. Menganalisis dan menghasilkan (memformulasikan) fungsi chaos baru dengan melakukan komposisi fungsi Dyadic Transformation Map dan Circle Map
2. Merancang dan menganalisis algoritma enkripsi dan dekripsi citra digital dan implementasinya berbasis fungsi chaos baru
3. Menganalisis kinerja algoritma enkripsi dan dekripsi citra digital berbasis fungsi chaos baru.

1.3 Batasan Penelitian

Adapun Batasan penelitian ini, yaitu :

1. Pengujian Chaotik terhadap fungsi chaos baru yang diperoleh menggunakan konsep Lyapunov exponent, Diagram bifurkasi, dan uji *National Institute of Standards and Technologies* (NIST).
2. Ukuran kinerja algoritma berdasarkan hasil simulasi implementasi algoritma terhadap data ujinya yaitu menggunakan :
   (a) Tingkat sensitifitas nilai awal
   (b) Besaran ruang kunci
   (c) Analisis histogram dan analisis distribusi uniform dari chipper-image
   (d) Analisis korelasi dan nilai entropi
   (e) Analisis kualitas citra dengan *Peak Signal -to Noise Ratio* (PSNR)
3. Implementasi algoritma menggunakan Bahasa pemrograman matlab.

1.4 Kontribusi Penelitian

Penelitian ini memberikan kontribusi keilmuan dan teknologi, dari sisi ilmu pengetahuan berupa :

1. Penemuan fungsi pembangkit bilangan acak yang bersifat chaos (keystream chaotic) dengan fungsi chaos baru
2. Penemuan algoritma enkripsi dan dekripsi citra digital berbasis fungsi chaos baru

3. Pembuatan program enkripsi dan dekripsi citra digital menggunakan fungsi chaos baru

BAB II
TINJAUAN PUSTAKA

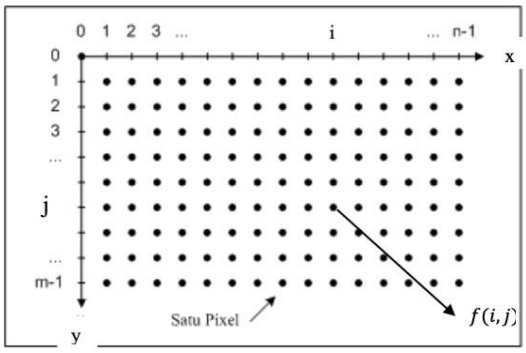
2.1 Citra Digital

Citra adalah suatu representasi (gambaran), kemiripan, atau imitasi dari suatu objek. Citra terbagi 2 yaitu citra yang bersifat analog dan ada citra yang bersifat digital. Citra analog adalah citra yang bersifat continue seperti gambar pada monitor televisi, foto sinar X, dan lain-lain. Sedangkan pada citra digital adalah citra yang dapat diolah melalui komputer. Citra dapat didefinisikan sebagai fungsi f (x,y) berukuran M baris dan N kolom, dengan x dan y adalah koordinat spasial, dan amplitudo f di titik koordinat (x,y) dinamakan intensitas atau tingkat keabuan dari citra pada citra tersebut (Richard E. Wood. 2004).

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).

Citra digital merupakan representatif dari citra yang diambil oleh mesin dengan bentuk pendekatan berdasarkan sampling dan kuantisasi.Sampling menyatakan besarnya kotak-kotak yang disusun dalam baris dan kolom. Dengan skata lain, sampling pada citra menyatakan besar kecilnya ukuran pixel (titik) pada citra, dan kuantisasi menyatakan besarnya nilai tingkat kecerahan yang dinyatakan dalam nilai tingkat keabuan (grayscale) sesuai dengan jurnlah bit biner yang digunakan oleh mesin, dengan kata lain kuantisasi pada citra menyatakan jumlah warna yang ada pada citra (Richard E. Wood. 2004).

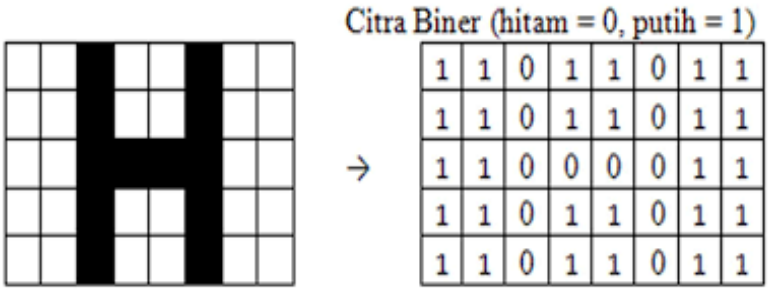
Citra digital berukuran n × m didefinisikan sebagai himpunan fungsi dua variabel f (x, y) dengan x dan y merupakan koordinat spasial, dan amplitudo f di setiap koordinat (x,y) dinamakan intensitas atau tingkat keabuan dari citra pada titik tersebut. Adapun nilai dari variabel x, y dan f (x, y) adalah berhingga dan diskrit, dengan x = 1, 2, 3, , n, dan 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 2.1 menunjukkan representasi citra digital berdasarkan keadaan pixel.

2.1.1 Citra Biner

Citra biner (*binary image*) adalah citra digital yang hanya memiliki 2 kemungkinan warna, yaitu hitam dan putih. Citra biner disebut juga dengan citra W&B (White&Black) atau citra monokrom. Hanya dibutuhkan 1 bit untuk mewakili nilai setiap piksel dari citra biner. Pembentukan citra biner memerlukan nilai batas keabuan yang akan digunakan sebagai nilai patokan. Piksel dengan 10 derajat keabuan lebih besar dari nilai batas akan diberi nilai 1 dan sebaliknya piksel dengan derajat keabuan lebih kecil dari nilai batas akan diberi nilai 0. Citra biner sering sekali muncul sebagai hasil dari proses pengolahan, seperti segmentasi, pengambangan, morfologi ataupun dithering. Fungsi dari binerisasi sendiri adalah untuk mempermudah proses pengenalan pola, karena pola akan lebih mudah terdeteksi pada citra yang mengandung lebih sedikit warna.



Gambar 2.2. Citra Biner

- Pada Model Citra CAHAYA, JIKA ada cahaya (=1) maka warna putih sedangkan JIKA tidak ada cahaya (=0) maka warna hitam.
- Pada Model Citra TINTA / CAT, JIKA ada cat (=1) maka warna hitam, sedangkan JIKA tidak ada cat (=0) maka warna putih.

2.1.2 Citra Grayscale

Citra grayscale merupakan citra digital yang hanya memiliki satu nilai kanal pada setiap pikselnya, artinya nilai dari Red = Green = Blue. Nilai-nilai tersebut digunakan untuk menunjukkan intensitas warna. Citra yang ditampilkan dari citra jenis ini terdiri atas warna abu-abu, bervariasi pada warna hitam pada bagian yang intensitas terlemah dan warna putih pada intensitas terkuat. Citra 11 grayscale berbeda dengan citra ”hitam-putih”, dimana pada konteks komputer, citra hitam putih hanya terdiri atas 2 warna saja yaitu ”hitam” dan ”putih” saja. Pada citra grayscale warna bervariasi antara hitam dan putih, tetapi variasi warna diantaranya sangat banyak. Citra grayscale seringkali merupakan perhitungan dari intensitas cahaya pada setiap piksel pada spektrum elektromagnetik single band. Citra grayscale disimpan dalam format 8 bit untuk setiap sample piksel, yang memungkinkan sebanyak 256 intensitas.

Gambar 2.3. Citra Grayscale

2.1.3 Citra RGB (Color)

sebuah citra digital sebagai hasil akuisisi sensor frekuensi warna umumnya di representasikan dengan tiga komponen warna dasar yaitu red (R), green (G), dan blue (B). sama halnya dengan representasi dan pengolahan citra digital dalam computer lebih umum menggunakan tiga komponen warna dasar tersebut. Setiap pixel pada citra berwarna R, G, dan B yang masing-masing umumnya disimpan dalam 8 bit atau total ketiganya 3 x 8 = 24 bit (3 byte). Hal ini memungkin setiap pixel dalam citra berwarna dapat memiliki variasi kandungan warna sebanyak 224 (16777216 variasi warna). Mengacu pada definisi 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].

Gambar 2.4. Citra Warna pada RGB

2.2 Kriptografi

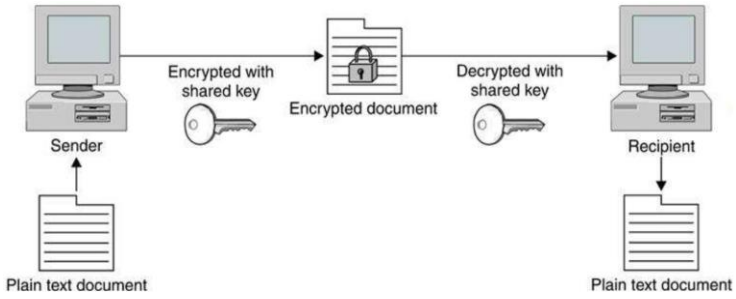
Kriptografi memiliki sejarah yang panjang seiring dengan sejarah peradaban manusia. Manusia telah menciptakan kode untuk menyimpan rahasia dan telah memecahkan kode untuk mempelajari rahasia itu sejak zaman Firaun. Selama 4.000 tahun, pertempuran sengit telah terjadi antara pembuat kode dan pemecah kode, dan kisah pertempuran ini adalah sejarah rahasia peradaban, kisah tersembunyi tentang bagaimana perang dimenangkan dan dikalahkan, intrik diplomatik digagalkan, rahasia bisnis dicuri, pemerintah hancur, dan komputer diretas. Dari Perang Galia ke Teluk Persia, dari telegram Zimmermann ke Enigma ke Proyek Manhattan, pemecahan kode telah membentuk jalannya peristiwa manusia sampai batas tertentu melampaui perhitungan yang mudah. (David Khan, The Codebreaker,1996). Perkembangan paling mencolok dalam sejarah kriptografi terjadi pada tahun 1976 ketika Diffie dan Hellman menerbitkan *New Directions in Cryptography*. Makalah ini memperkenalkan konsep revolusioner kriptografi kunci publik dan juga menyediakan metode baru dan cerdik untuk pertukaran kunci, yang keamanannya didasarkan pada kerumitan masalah logaritma diskrit.

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 [Menezes, Oorschot, dan Vanstone, 1996] Kriptografi adalah ilmu yang memelajari tentang teknik matematika yang berhu- bungan tentang aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, dan autentikasi data.

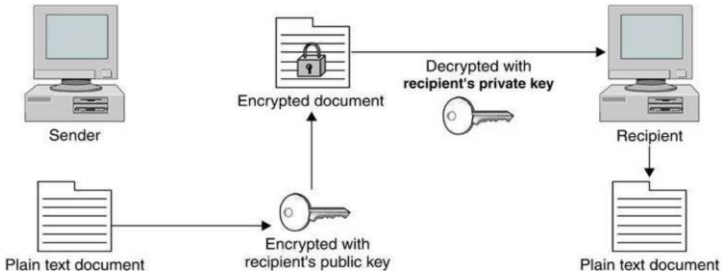
Tujuan lain dari kriptografi adalah memberikan layanan integritas data (*data integrity*) yang menjamin keaslian pesan atau pesan belum pernah dimanipulasi. Otentikasi (*authentification*) bertujuan untuk mengidentifikasi kebenaran pihak-pihak yang berkomunikasi dan mengidentifikasi kebenaran sumber informasi. Anti penyangkalan (*non-repudiation*) bertujuan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan. [Munir, 2006]

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. Secara garis besar kedua teknik enkripsi ini masing-masing diperlihatkan oleh gambar 2.5 dan 2.6



Gambar 2.5 Bagan Umum Proses Enkripsi Kunci Simetris



Gambar 2.6 Bagan Umum Proses Enkripsi Kunci Publik

Algoritma untuk mentransformasikan *plaintext* menjadi *chipertext* disebut chiper. Metode chiper terdiri dari dua proses, 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 sehingga isi dokumen tersebut menjadi tidak dapat terbaca maknanya.

2.3. 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 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 itu 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, namun disisi lain akan membingkai batas-batas ruang gerak tersebut.

Teori chaos adalah teori yang menggambarkan perilaku sistem dinamis non linear yang menunjukan fenomena yang kacau. Sistem chaos sangat peka terhadap nilai awal, yang menunjukan hasil yang sangat kacau jika ada perbedaan di awal walaupun sangat sedikit. Map dari suatu nilai tertentu yang polanya sangat sensitif terhadap perubahan disebut *Chaotic Map*.

2.3.1 Diagram 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.

2.3.2 Lyapunov Exponent

Istilah Lyapunov exponent berasal dari ilmuwan Rusia, Aleksandr Lyapunov, yang membahas masalah ini dalam Tesis PhD-nya tahun 1892. Di dalam tesisnya , ia

memperkenalkan dua metode yang didasarkan pada linearisasi persamaan gerak dan berasal dari apa yang kemudian disebut eksponen Lyapunov.

Menurut Kocarev, Lyapunov ekponent bisa mengkuantifikasi sensitivitas sistem chaos terhadap kondisi awal. Berikut ini akan diberikan teori-teori yang akan menunjang tentang definisi chaos [Devaney 1989].

Definisi2.1 $f : X \rightarrow X$ dikatakan ketergantungan yang sensitive terhadap nilai awal jika terdapat $\delta > 0$ sedemikan sehingga, untuk sembarang $x \in X$ dan sembarang *neighborhood* N dari x, terdapat $y \in N$ dan $n \geq 0$ sedemikian sehingga $|f^{(n)}(x) - f^{(n)}(y)| > \delta$.

$f^{(n)}(x)$ didefinisikan sebagai berikut:

$$f^{(1)}(x_0) = f(x_0), f^{(2)}(x_0) = f(f(x_0)), f^{(3)}(x_0) = f(f(f(x_0)))$$
$$\text{Secara Umum: } f^{(n)}(x_0) = \underbrace{f(f(f(\ldots((x_0))\ldots)))}_{n-1}$$

Secara intuitif, fungsi yang memiliki ketergantungan yang sensitif terhadap nilai awal jika ada titik y yang dekat dengan x, dengan y di dalam interval $(x - \varepsilon, x + \varepsilon)$. Jika fungsi tersebut sensitif terhadap nilai awal, maka nilai mutlak dari hasil seli- sih pemetaan pada periode n dari x dan y lebih besar dari pada δ. Atau dengan kata lain walaupun nilai x dan y sangat kecil perbedaannya namun hasil pemetaannya akan sangat berbeda.

Definisi 2.2 $f : X \rightarrow X$ dikatakan topologi transitif jika untuk sembarang pasangan himpunan buka $U, V \subset X$ terdapat $k > 0$ sedemikian sehingga $f^{(k)}(U) \cap V f = \emptyset$. Konsep topologi transitif diperkenalkan oleh Birkhoff [6] pada tahun 1920. Sistem dinamis dengan sifat transitif topologi mengandung setidaknya satu titik yang bergerak di bawah iterasi dari satu lingkungan yang berubah-ubah ke lingkungan lainnya. Himpunan buka didefinisikan sebagai berikut sebagai berikut [Bartle dan Sherbert, 2000]: Jika $a, b \in \mathrm{R}$ memenuhi $a < b$, maka himpunan buka yang ditentukan oleh a dan b adalah $(a, b) = \{x \in \mathrm{R} : a < x < b\}$, dengan a dan b adalah titik batas dari interval tetapi titik batas tidak masuk didalam interval. Secara intuitif, fungsi topologi transitif memiliki titik-titik hasil pemetaan yang pada akhirnya bergerak di bawah iterasi dari satu *small neighborhod* yang sembarang ke *neighborhod* lainnya. Akibatnya, himpunan hasil pemetaan titik-titik tersebut tidak dapat dipisah menjadi dua buah himpunan buka.

Definisi 2.3 $U \subset W$ dikatakan rapat di W jika terdapat sembarang titik di U yang dekat pada suatu titik di himpunan yang lebih besar yaitu W. Ekuivalen dengan mengatakan bahwa U padat di W jika untuk $x \in W$, dan sembarang $\delta > 0$, di dalam interval $(x - \delta, x + \delta)$

mengandung titik dari *U*. Jika suatu fungsi memenuhi ketiga definisi yaitu Definisi 2.1, 2.2, dan 2.3, maka fungsi tersebut dikatakan sebagai fungsi chaos. Devaney mendefinisikan chaos sebagai berikut :

Definisi 2.4 Misalkan *X* adalah himpunan, $f : X \to X$ adalah fungsi *chaos* di *X* jika:

1. *f* memiliki ketergantungan yang sensitif terhadap nilai awal.
2. *f* adalah topologi transitif.
3. *Periodic points*-nya rapat di *X*.

Jika suatu fungsi adalah fungsi yang topologi transitif, maka poin periodik dari fungsi tersebut rapat dan begitu pula sebaliknya [Hirsch,Smale,dan Devaney, 2004].

Selain dengan menggunakan Definisi 2.4, sifat ketergantungan yang sensitif terhadap nilai awal dapat dihitung dengan *Lyapunov exponents*. Sedangkan untuk sifat topologi transitif dapat dilihat dengan menggunakan diagram bifurkasi. Persamaan *Lyapunov exponent* disajikan dalam definisi 2.5.

Definisi 2.5 Untuk sembarang fungsi satu variabel, *Lyapunov exponent* adalah:

$$\mu = \lim_{n\to\infty} \frac{1}{n}\sum_{i=0}^{n-1} ln \left| \left(f^{(i)}\right)' (x_0) \right| \tag{2.1}$$

Jika μ bernilai positif maka fungsi tersebut memiliki sensitivitas (ketergantungan sensitif) yang tinggi terhadap nilai awal (x_0).

Diagram bifurkasi adalah tipe diagram yang memperlihatkan perilaku hasil pemetaan suatu fungsi, ketika parameter diubah-ubah. Sifat topologi transitif dapat dilihat dari diagram bifurkasi yang ditunjukkan dengan kepadatan hasil pemetaannya.

2.3.3 Dyadic Transformation Map

Dyadic Transformation Map B_0 : [0, 1] →[0, 1] untuk persamaan x_0 = x Untuk semua n ≥ 0, x_{n+1} = $(2x_n)$ mod 1

$$f(x) = \begin{cases} 2x & , 0 \le x < 0.5 \\ 2x - 1 & , 0.5 \le x < 1 \end{cases} \tag{2.2}$$

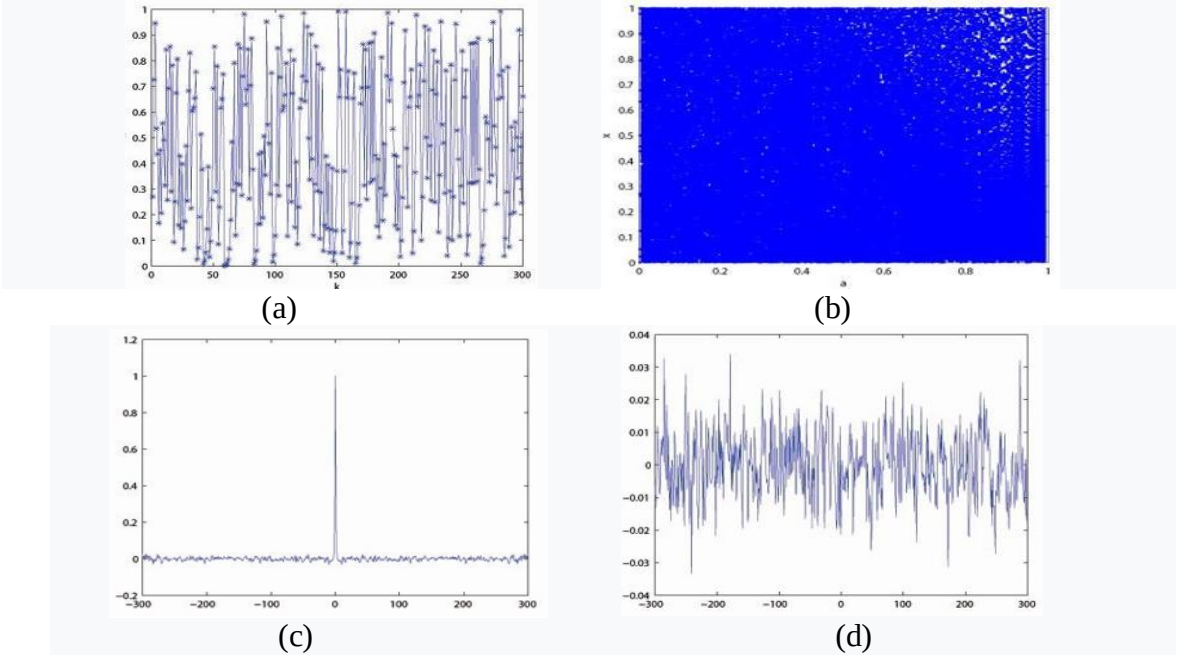
Dyadic Tranformation Map menghasilkan contoh sederhana untuk mekanisme peregangan-dan-potong yang pada dasarnya nonlinier, karena biasanya menghasilkan kekacauan deterministik. Mekanisme dasar seperti itu juga ditemui dalam sistem dinamis yang lebih realistis. Kami mungkin berkomentar bahwa 'meregangkan dan melipat' atau

'meregangkan, memutar dan melipat' memberikan mekanisme alternatif untuk menghasilkan perilaku kacau. Dalam makalah ini, kami akan mempertimbangkan versi umum yang ditampilkan sebagai:

$$x_{n+1} = T(x_n) := \frac{x_n}{a} \bmod 1.$$

di mana x_n, x_{n+1} ∈[0, 1] adalah bagian dari map, dan a ∈(0, 1) adalah parameter kontrol. Karena a = 0.5, B menjadi Dyadic map reguler. Satuan yang diturunkan dari sistem dinamis adalah $\{x_k = B^k (x_0)$, k = 0,1, …$\}$, yang mana di tunjukkan pada gambar (a) untuk a = 0.3731, x_0 = 0.2709. Bentuk gelombangnya cukup tidak beraturan dan menunjukkan bahwa sistemnya kacau. Diagram bifurkasi dari Dyadic Transformation Map umum digambarkan pada Gambar (b), di mana untuk setiap parameter kontrol, kami mengulangi 600 kali untuk mendapatkan titik orbit yang sesuai dan memplotnya. Ini menyiratkan bahwa parameter kontrol yang dimiliki (0,1) akan membuat sistem yang diusulkan menjadi kacau. Parameter kontrol a dan kondisi awal 0 x dapat digunakan sebagai kunci sandi yang valid karena peta digunakan untuk merancang skema enkripsi citra. Terdapat beberapa fitur dinamis yang baik dalam Dyadic Transformation Map yang digeneralisasi, seperti fitur auto-korelasi dan korelasi silang yang diinginkan, lihat Gambar 1 (c-d). Korelasi silang dihitung antara orbit x_0 = 0.2709 dan y_0 = 0.31.

a = 0.3731, x_0 = 0.2709 a ∈ (0.001, 0.995) dengan tingkatan 0.005



(a) (b)

(c) (d)

Gambar 2.7 Perilaku Dyadic Transformation Map

2.3.4 Circle Map

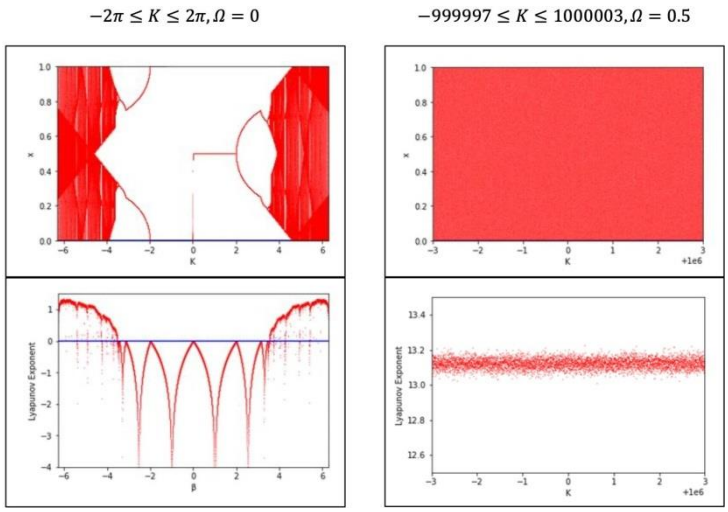
Circle map adalah fungsi satu dimensi yang memetakan sebuah lingkaran ke dirinya sendiri. Circle Map didefinisikan dengan persamaan berikut.[Boyland,1986]

$$x_{n+1} = x_n + \Omega + \frac{K}{2\pi} \sin(2\pi x_n) \mod 1 \tag{2.3}$$

di mana mod 1 menunjukkan bagian desimal dari sebuah angka, sehingga nilai pe- ta selalu lebih rendah dari 1 tetapi tidak kurang dari 0, dan parameter Ω, $K \in \mathrm{R}$, Ω terdapat pada interval $0 \leq \Omega \leq 1$, karena ini adalah suku penjumlahan tunggal dalam modulo 1 ini, jadi semua nilai Ω lainnya telah diwakili oleh intervalini.

Circle Map menunjukkan sifat yang sangat menarik karena memiliki potensi kekacauan yang tidak terbatas. Saat nilai K menjauh dari 0, *Lyapunov exponent*nya terus meningkat, meskipun mungkin turun di beberapa titik dan kenaikannya melambat. Oleh karena itu, nilai K dapat dipilih yang tinggi atau rendah (negatif) agar mendapatkan *Lyapunov exponent* yang cukup tinggi. Selanjutnya, signifikansi nilai Ω pada *Circle Map* menurun saat K semakin menjauh dari 0.

Berikut beberapa plot dari Circle Map.



Gambar 2.8 Beberapa plot dari Circle Map

2.4 Fungsi Komposisi

Fungsi komposisi adalah fungsi baru yang terbentuk dari dua fungsi yang digabungkan secara berurutan. Misalkan terdapat fungsi g dari himpunan A ke himpunan B

dan misalkan fungsi f adalah fungsi dari himpunan B ke himpunan C. Komposisi fungsi f dan g, dinotasikan dengan $f \circ g$ untuk semua $a \in A$ didefinisikan oleh:

$$(f \circ g)(a) = f(g(a))$$

Dengan kata lain, untuk menemukan $(f \circ g)(a)$ pertama-tama kita memetakan fungsi g ke a untuk memperoleh g (a) dan kemudian kita memetakan fungsi f pada hasil g (a) untuk memperoleh $(f \circ g)(a) = f(g(a))$ [Rosen, 2012].

2.5 Operasi Logika XOR

Gerbang logika XOR atau yang biasa disebut Exclusive OR yaitu operasi logika yang memiliki masukan (input) terdiri dari dua atau lebih variabel mulai dari A, B, … dan satu variabel keluaran (output) Q. Variabel keluaran akan berlogika '1' hanya jika masukkannya berbeda dan akan berlogika '0' jika masukkannya sama (dapat dilihat pada tabel kebenaran). Pada operasi XOR biasanya menggunakan IC 7486.

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 $\oplus$. Pernyataan $p \oplus q$ 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 $p \oplus q = q \oplus p$. Identitas dari operasi XOR adalah 0. Karena $a \oplus 0 = a$, $a = 0, 1$. Berdasarkan tabel 2.1 terlihat bahwa

invers dari tiap elemen yaitu −a = a sehingga disimpulkan bahwa operasi invers dari XOR adalah XOR itu sendiri.

2.6 Pengujian Keacakan key stream

Kunci adalah bagian yang sangat penting dalam kriptografi. Kerchoff menyatakan bahwa asumsi yang dipakai oleh semua pendesain algoritma adalah, semua algoritma itu publish sehingga kekuatan algoritma terletak pada kekuatan kunci yang digunakan. Pengujian keacakan barisan biner key stream dilakukan uji statistik yang terdiri dari 16 uji untuk menilai apakah pembangkit bilangan acak suatu algoritma enkripsi memiliki tingkat keacakan yang tinggi. Pengujian ini dikenal dengan uji NIST (National Institute of Standard Technologies Test). NIST Test adalah tes statistik untuk menguji keacakan urutan biner yang dihasilkan dari random number generator (RNG) atau pseudo-random number generators (PRNG). Tes ini dikeluarkan oleh National Institute of Standard and Technology yang terdiri dari 16 jenis tes [NIST , 2010] yaitu:

1. Uji Frekuensi Monobit
2. Uji Frekuensi per Blok
3. The Runs Test
4. Uji Longest-Run-of-Ones per Blok
5. Uji Rank Matriks Biner
6. Uji Transformasi Diskrit Fourier (Spektral)
7. The Non-overlapping Template Matching Test
8. The overlapping Template Matching Test
9. Maurer's Test
10. Uji Kompleksitas Linier
11. Uji Serial
12. Uji Prakiraan Entropi
13. Uji jumlah Kumulatif (Forward)
14. Uji jumlah Kumulatif (Reverse)
15. The Random Excursions Test
16. The Random Excursions Variant Test

2.7 Analisis Korelasi

Korelasi Sederhana merupakan suatu teknik statistik yang dipergunakan untuk mengukur kekuatan hubungan dua variabel dan juga untuk mengetahui bentuk hubungan

keduanya dengan hasil yang sifatnya kuantitatif. Korelasi adalah ukuran yang menyatakan kekuatan hubungan linier antara dua peubah acak. Koefisien korelasi adalah korelasi dari dua buah peubah acak diskrit yang masing-masing beranggotakan n elemen. Menguji korelasi antara pixel yang berdekatan pada citra terenkripsi dapat dilakukan dengan analisis korelasi Pearson atau korelasi Covariance. Citra terenkripsi dibandingkan dengan citra asli tetapi digeser secara vertikal, horisontal, dan diagonal. Data yang dibandingkan pada umumnya 1000 atau 2500 pasang pixel yang dipilih secara random. Metode ini digunakan oleh [Munir, 2012] yang dijabarkan dengan persamaan (2.4) sampai (2.7) berikut:

$$r_{xy} = \frac{cov\,(x,y)}{\sqrt{D\,(x)\,D\,(y)}} \tag{2.4}$$

$$cov\,(x,y) = \frac{1}{n}\sum_{i=1}^{n}[x_i - E\,(x)]\,[y_i - E\,(y)] \tag{2.5}$$

$$D\,(x) = \frac{1}{n}\sum_{i=1}^{n}[x_i - E\,(x)]^2 \tag{2.6}$$

$$E\,(x) = \frac{1}{n}\sum_{i=1}^{n}x_i \tag{2.7}$$

Dimana cov adalah kovariansi

D adalah standard deviasi

E adalah rata-rata

2.8. Perbandingan Tinjauan

Berikut ini adalah paper yang mendukung penelitian disertasi ini.

Tabel 2.2: Perbandingan Metode Enkripsi yang Berbeda

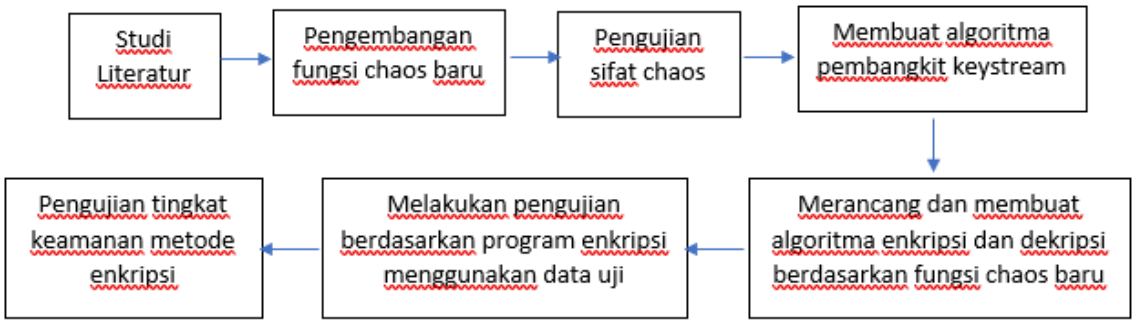
Teknik	Penulis, Tahun	Metode yang digunakan	Hasil
Enkripsi Citra Menggunakan Gauss Map	Patidar, 2006	Key Stream dihasilkan dari fungsi MS Gauss dan proses enkripsi dengan menggunakan operasi XOR	Ruang Kunci rendah tapi waktu enkripsi dan dekripsi cepat
Enkripsi Citra Menggunakan Logistic Map	Nurpeti, 2013	Key Stream dihasilkan dari fungsi Logistic dan proses enkripsi dengan menggunakan operasi XOR	Algoritma tahan terhadap brute force attack tapi ruang kunci masih rendah
Enkripsi dengan kombinasi dua chaotic secara selektif	Rinaldi Munir, 2012	Enkripsi dengan Logistic dan ACM	Algoritma aman terhadap brute force attack dan Aman dari analisis statistik
Permutasi Multiple Circular Shrinking	Yohan Suryanto, Suryadi, Kalamullah Ramli, 2016	Enkripsi Gambar yang Aman dan Kokoh Berdasarkan Permutasi Multiple Circular Shrinking	metode yang diusulkan tahan terhadap serangan statistic juga tahan terhadap kompresi JPEG, skema derau, kehilangan data, dan penyesuaian kontras-kecerahan, sehingga gambar yang disandikan dapat disimpan dalam ukuran file yang lebih kecil dan ditransmisikan dalam bebas kesalahan sistem komunikasi
Modifikasi baru Logistic Map	Suryadi MT, Maria Yus	Proses enkripsi menggunakan Modifikasi baru logistic map,	Waktu rata-rata proses enkripsi dan dekripsi relatif

	Trinity Irsan, Yudi Satria, 2016	disebut MS Map. Kemudian mengukur kinerja algoritma dengan NIST test, Histogram Analysis	sama, tergantung type dan ukuran citra. Algoritma sangat susah diserang dengan known plain text attack, Resistant terhadap brute-force
Gauss MS Map	Suci, Suryadi, Triswanto 2018	Komposisi fungsi Gauss Map dan MS Map untuk membangkitkan key stream	Aman terhadap brute force attack dan aman terhadap statistical attack, differential attack
Logistic map, Chebyshev map, Circle map, Sinus map, Lorenz attractor, Lu attractor	Rohsini, Sridevi, Lakhsmi, 2019	Key stream dibangkitkan dua kali, pertama dengan confusion dan kedua dengan diffusion	Aman terhadap brute force attack.
Gauss Map dan Circle Map	Yudi, Suryadi, Luqman, 2019	Komposisi fungsi Gauss Map dan Circle Map untuk membangkitkan key stream	Aman terhadap brute force attack tetapi lemah terhadap statistical attack.

BAB III
METODOLOGI PENELITIAN

3.1 Skema Penelitian

Skema penelitian yang digunakan untuk proposal penelitian ini terlihat pada gambar 3.1



Gambar 3.1 Skema Tahapan Penelitian

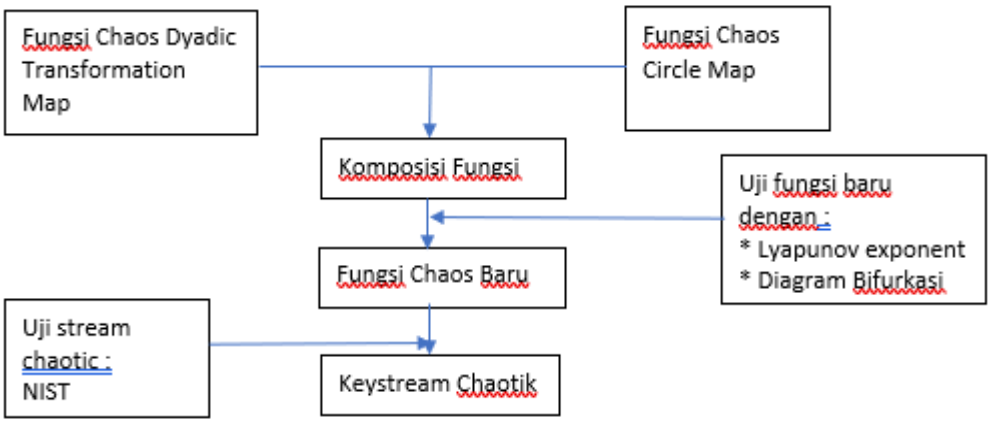
Uraian singkat setiap tahapan proses dari skema penelitian pada gambar 3.1 dapat diuraikan sebagai berikut :

1. Studi Literatur : Pada tahap ini dilakukan review sejumlah paper ilmiah hasil-hasil penelitian yang berkaitan dengan keamanan data citra. Review ini bertujuan untuk mempelajari metode-metode dan algoritma yang telah dikembangkan, menganalisi kekurangannya dan peluang pengembangannya. Selanjutnya menentukan topik penelitian, merumuskan masalah dan batasan penelitian serta menentukan tujuan dan sasaran yang ingin dicapai. Pada tahap ini juga dilakukan studi pustaka tentang teori-teori yang berhubungan dengan data citra, kriptografi dan Teknik enkripsi dan dekripsi.
2. Melakukan pengembangan fungsi chaos baru melalui komposisi fungsi Dyadic Transformation Map dan Circle Map.
3. Menguji sifat chaotic fungsi chaos baru dengan Lyapunov exponent dan diagram bifurkasi dan uji NIST
4. Membuat algoritma pembangkit keystream , algoritma enkripsi dan algoritma dekripsi dengan fungsi chaos baru
5. Melakukan simulasi dan uji coba program aplikasi enkripsi dan dekripsi menggunakan data uji berupa citra warna dan citra hitam putih

6. Melakukan tingkat keamanan metode enkripsi citra digital berbasis fungsi chaos baru berdasarkan :
    a. Daya tahan terhadap statistical attack (analisis histogram, analisis entropi dan analisis tingkat keacakan NIST)
    b. Daya tahan terhadap differential attack (analisisi koefisien korelasi dan analisis NPCR UACI)
    c. Daya tahan terhadap brute-force attack (analisis ruang kunci dan analisis sensitivitas kunci)
    d. Selanjutnya mengukur rata-rata waktu proses enkripsi dan dekripsi

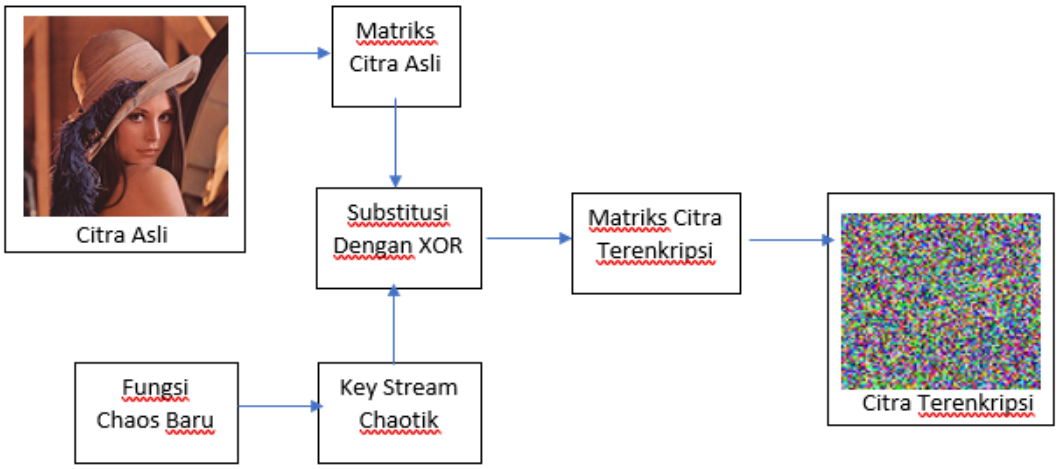
Pada penelitian ini baru dibahas untuk poin 1 dan poin 2.

3.2 Model Operasional Penelitian



Gambar 3.2 Proses Pembangkit Keystream

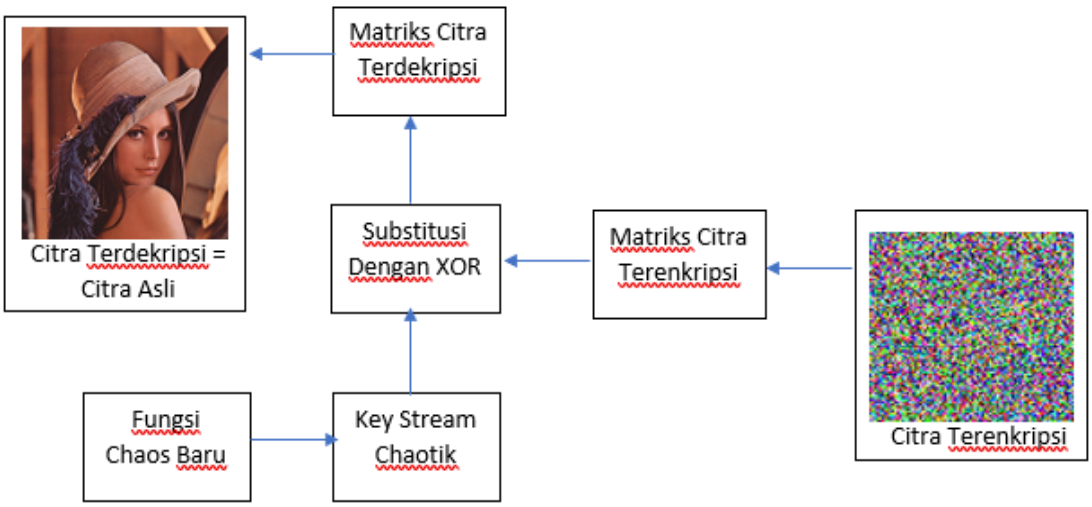
a. Proses Enkripsi



Gambar 3.3 Proses Enkripsi

- Baca citra asli lalu ubah ke data matriks, menjadi output matriks
- Baca matriks tersebut lalu ubah ke citra, menjadi output citra
- Ubah matriks (inputnya matriks) dengan cara tukar baris atau dan tukar kolom, ubah jadi citra , menjadi output citra
- Input citra yang sudah berubah lalu kembalikan ke citra aslinya

b. Proses Dekripsi



Gambar 3.4 Proses Dekripsi

3.3 Pengembangan Fungsi Chaos Baru

Fungsi chaos baru dalam penelitian ini diturunkan melalui proses komposisi dua fungsi chaos yaitu Dyadic Transformation Map dan Circle Map. Fungsi Dyadic Transformation bentuknya dinyatakan dalam persamaan (3.1) [Prajwalasimha, Usha, 2017]:

$$g(x) = \begin{cases} 2x & ,0 \le x < 0.5 \\ 2x - 1 & ,0.5 \le x < 1 \end{cases} \quad (3.1)$$

Adapun fungsi chaos Circle Map dinyatakan dalam persamaan (3.2) [Boyland, 1986] :

$$x_{n+1} = (x_n + \Omega + \frac{k}{2\pi} \sin(2\pi x_n) \bmod 1) \quad (3.2)$$

Fungsi chaos baru baru merupakan komposisi dalam bentuk f o g dengan f dan g sesui persamaan (3.1) dan (3.2). fungsi Dyadiv terdefinisi berdasarkan 2 partisi domain, sehingga

gunsi chaos baru yang dihasilkan dari hasil komposisi juga dinyatakan dalam 2 partisi domain yang sama, yaitu sebagaimana persamaan (3.3) dan (3.4) :

a. Untuk $0 \leq x \leq 0.5$

$$(f \circ g)(x) = 2(x_n + \Omega + \frac{k}{2\pi} \sin(2\pi 2_x) \bmod 1) \tag{3.3}$$

b. Untuk $0.5 \leq x < 1$

$$(f \circ g)(x) = 2(x_n + \Omega + \frac{k}{2\pi} \sin(2\pi 2_x) \bmod 1) - 1 \tag{3.4}$$

Dengan demikian fungsi chaos yang baru yang diperoleh terlihat pada persamaan (3.5):

$$(f \circ g)(x) = \begin{cases} 2(x_n + \Omega + \frac{k}{2\pi} \sin(2\pi 2_x) \bmod 1) & , 0 \leq x \leq 0.5 \\ 2(x_n + \Omega + \frac{k}{2\pi} \sin(2\pi 2_x) \bmod 1) - 1 & , 0.5 \leq x < 1 \end{cases} \tag{3.5}$$

Persamaan (3.5) dapat dinyatakan dalam bentuk rekursif dalam bentuk persamaan (3.6):

$$(x_{n+1}) = \begin{cases} 2(x_n + \Omega + \frac{k}{2\pi} \sin(2\pi 2_x) \bmod 1) & , 0 \leq x \leq 0.5 \\ 2(x_n + \Omega + \frac{k}{2\pi} \sin(2\pi 2_x) \bmod 1) - 1 & , 0.5 \leq x < 1 \end{cases} \tag{3.6}$$

Selanjutnya persamaan (3.6) sebagai fungsi baru hasil komposisi fungsi Dyadic Transformation Map dan Circle Map. Untuk selanjutnya fungsi baru ini akan di gunakan sebagai pembangkit keysream dalam proses enkripsi dan dekripsi dengan sebelumnya diuji dengan diagram bifurkasi dan 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.

3.4 Rencana Kegiatan

Untuk mencapai target penelitian, 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 yang akan digunakan sebagai berikut :

Tabel 3.1 Rencana Kegiatan

KEGIATAN	2021		2022											URAIAN
	11	12	1	2	3	4	5	6	7	8	9	10	11	12	
Bimbingan															Penyusunan proposal Kualifikasi
Ujian Kualifikasi															Penajaman proposal
Evaluasi Progress 1															Pembuatan Algoritma Enkripsi Citra
Evaluasi Progress 2															Pengujian tingkat keamanan metode Enkripsi
Evaluasi RKP															Kesimpulan / Hasil
Sidang Tertutup															Penajaman Hasil
Sidang Terbuka															

REFERENSI

[1] Menezes A., Oorschot, P.V., dan Vanstone,S, Handbook of Applied Cryptography, CRC Press, 1997

[2] Rinaldi Munir, Analisis Keamanan Algoritma Enkripsi Citra Digital Menggunakan kombinasi Dua Chaos Map dan Penerapan Teknik Selektif, JUTI volume 10 No 2 , 89-95 , 2012

[3] Stallings, W. Computer and Network Security : Principle and Practice (5th ed.). New York: Prentice hall.

[4] Kocarev, L., and Lian, S. Chaos-based cyrptography. Berlin Heidelberg : Springer-Verlag.

[5] Maria, YTI., Suryadi M.T, Yudi,S., New Modified Map for Digital Image Encryptionand Its Performance. Prosiding ACM, 2016

[6] Roshini P, Sridevi A, Lakshmi C, Performance Evaluation of Chaotic Maps and Attractors in Image Encryption, International Conference on Computer Communication and Informatics (ICCCI -2019), Jan. 23 – 25, 2019, Publikasi 978-1-5386-8260-9/19/31.00 2019 IEEE

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

[8] Suryadi MT, Yudi S, Luqman N.P, An improvement on the chaotic behavior of the Gauss Map for cryptography purposes using the Circle Map combination, ICoMPAC 2019, doi:10.1088/1742-6596/1490/1/012045

[9] 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

[10] Munir,R., Kriptografi, Informatika Bandung, 2006

[11] Ariyus, Dony, 2008, Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi, Yogyakarta

[12] Madenda ,S., Pengolahan Citra dan Video Digital, Teori Aplikasi dan Pemrograman Menggunakan Matlab, Penerbit Eirlanga, Jakarta, 2015

[13] Rafael C. Gonzales and E.Woods.. Digital Image Processing. New Jersey: Prentice-Hall, Inc., 2002

[14] Wiggins, S., Introduction To Applied Nonlinear Dynamical Systems And Chaos, book, Publisher: Springer Verlag, January 2003

[15] Stewart, I., Does God Play Dice? : The New Mathematics of Chaos, Publisher Penguin Books Ltd, ISBN10 0140256024, 1997

[16] Devaney, RL., An Introduction to Chaotic Dynamical Systems, Second Edition Addison-wesley Publishing Company, Inc

[17] Hirsch, MW., Smale, S., Devaney,RL., Differential quations dynamical Systems and An Introduction to chaos, book. 2003

[18] Boyland, PL., (1986). Bifurcations of circle maps: Arnol'd tongues, bistability and rotation intervals, (Berlin: Springer-Verlag)

[19] Rosen, KH., Discrete Mathematics and Its Applications, 5th International Edition, ISBN 0-07-053965-0, McGraw-Hill Book Co. New York, NY. 2012.

[20] Prajwalasimha S N, Usha Surendra, (2017), Multimedi Data Encryption based on Discrete Dyadic Transformatian, International Conference on Signal Processing and Communication (ICSPC 2017)