PROPOSAL PENELITIAN

# PENGEMBANGAN FUNGSI CHAOS BARU SEBAGAI KEAMANAN CITRA DIGITAL MELALUI KOMPOSISI DUA FUNGSI

Seminar Bidang Kajian

Waliya Rahmawanti

99217020

TI 23

2022

# 1. Pendahuluan

## 1.1 Latar Belakang

Dunia kriptografi modern saat ini telah menerapkan berbagai metode untuk penyandian data digital. Semakin rumit metode yang digunakan, maka tingkat keamanan yang dihasilkan pun akan semakin baik pula. Algoritma kriptografi modern telah menerapkan metode bit dalam penyandian data digital. Hal ini membuat data digital yang dihasilkan akan semakin sulit untuk dipecahkan oleh para kriptoanalis. Meningkatkan keamanan dalam algoritma kriptografi modern, dapat menggunakan teori chaos. Teori chaos ini merupakan cabang dari matematika yang mempelajari bagaimana membangkitkan bilangan secara acak. Teori chaos ini sangat sensitive pada nilai awal (initial condition). Hal ini sangat berguna dan dapat diterapkan di dalam dunia kriptografi sebagai pembangkit kunci acak yang nantinya akan diolah sebagai sarana dalam melakukan proses enkripsi. Semakin acak bilangan yang dihasilkan,semakin baik pula tingkat keamanan dari suatu cipherteks..

Selain itu, terdapat penelitian lainnya bahwa dalam 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.

Maka dalam hal ini akan diajukan penggabungan dengan cara mengkomposisikan dua buah fungsi chaos yaitu fungsi Dyadic transformation dan Hénon map, yang mana dari komposisi ini akan mendapatkan fungsi chaos yang baru Sehingga diharapkan fungsi baru tersebut dapat sebagai alternatif pilihan sebagai fungsi pembangkit bilangan acak yang bersifat chaos.

## 1.2 Perumusan masalah

Dari uraian latar belakang, mempunyai perumusan masalah sebagai berikut :

1. Bagaimana mengupayakan menghasikan fungsi chaos baru dari komposisi dua buah fungsi chaos yang di ajukan.
2. Bagaimana mengsimulasikan fungsi chaos baru yang diajukan tersebut kedalam citra digital

## 1.3 Batasan Penelitian

Proposal penelitian ini mempunyai batasan sebagai berikut :

1. Metode yang digunakan dengan melakukan komposisi fungsi chaos henon map dan dyadic transformation map.
2. Data masukkan berupa data gambar digital.

## 1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah Menganalisis dan menghasilkan (memformulasikan) fungsi chaos baru dengan melakukan komposisi fungsi Dyadic Transformation Map dan Hénon map

## 1.5 Kontribusi Hasil Penelitian

Penelitian ini memberikan kontribusi keilmuan dan teknologi, dari sisi ilmu pengetahuan berupa, Penemuan fungsi pembangkit bilangan acak yang bersifat chaos (keystream chaotic) dengan fungsi chaos baru

# 2. TINJAUAN PUSTAKA

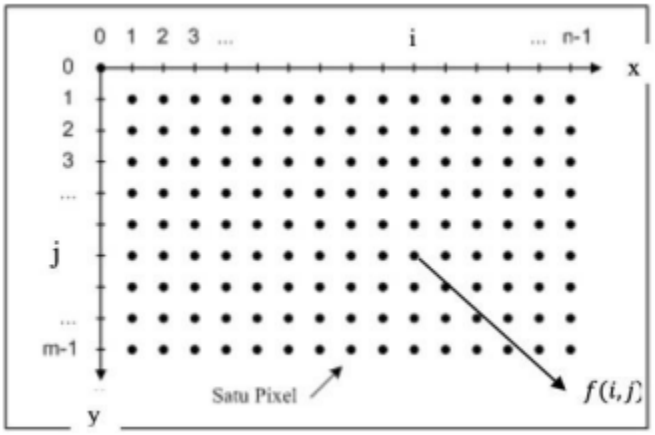
## 2.1 Citra Digital

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).

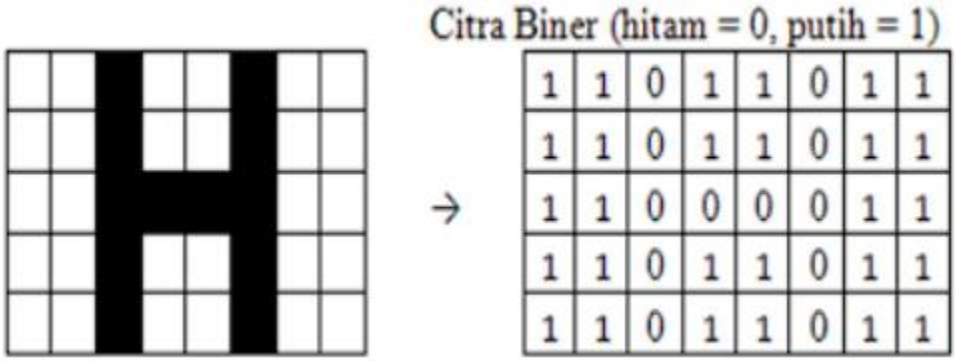
Citra digital berukuran n × m didefinisikan sebagai himpunan fungsi dua variabel f (x, y) dengan x dan y merupakan koordinat spasial, dan amplitudo f di setiap koordinat (x,y) dinamakan intensitas atau tingkat keabuan dari citra pada titik tersebut. Adapun nilai dari variabel x, y dan f (x, y) adalah 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

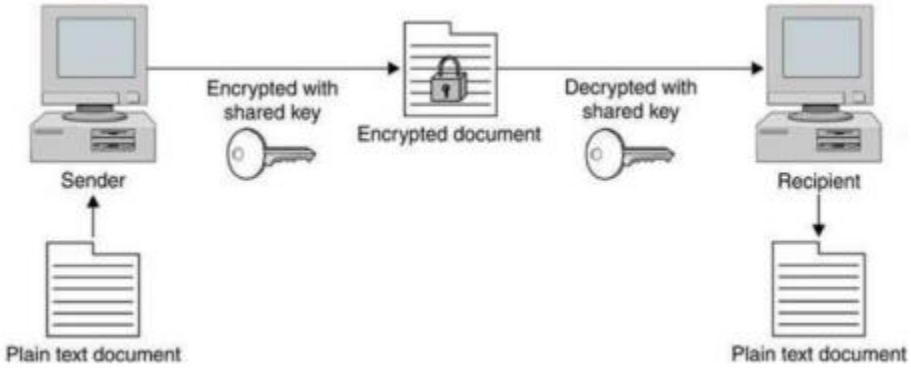
## 2.2 Kriptografi

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.

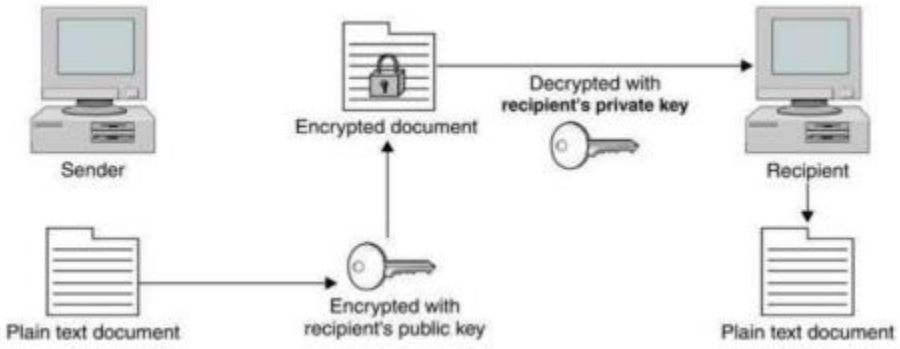
Makalah ini memperkenalkan konsep revolusioner kriptografi kunci publik dan juga menyediakan metode baru dan cerdik untuk pertukaran kunci, yang keamanannya didasarkan pada kerumitan masalah logaritma diskrit. Kriptografi berasal dari bahasa Yunani yaitu kryptos dan graphia. Kryptos berarti sesuatu yang 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 (nonrepudiation) 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

### 2.3.2 Dyadic Transformation Map

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

Dyadic Transformation juga dapat didefinisikan sebagai fungsi berulang bagian dari fungsi kepingan linier

$$f(x) = \begin{cases} 2x & ,0 \le x < 0.5 \\ 2x-1 & ,0.5 \le x < 1 \end{cases} \quad (2.1)$$

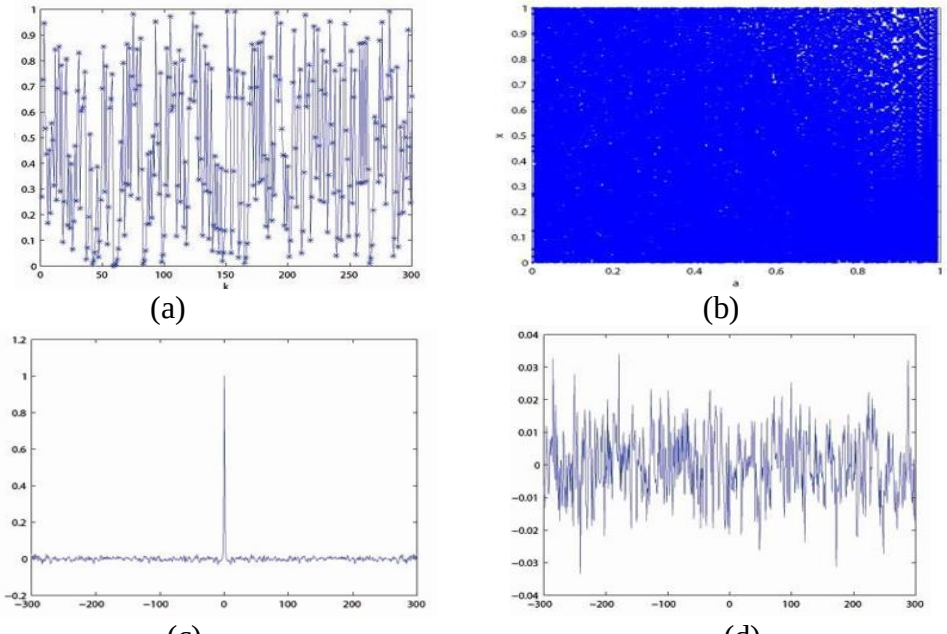
Dyadic Tranformation Map menghasilkan contoh sederhana untuk mekanisme peregangan-dan-potong yang pada dasarnya nonlinier, karena biasanya menghasilkan kekacauan deterministik. Mekanisme dasar seperti itu juga ditemui dalam sistem dinamis yang lebih realistis. Kami mungkin berkomentar bahwa 'meregangkan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

memutar dan melipat' memberikan mekanisme alternatif untuk menghasilkan perilaku acak. 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

### 2.3.3 Henon Map

Algoritma Henon Map merupakan metode yang ditemukan oleh Michael Henon sebagai simplikasi model dari model Lorenz (Ratna et al., 2021). Henon Map merupakan sistem dinamis yang mengimplementasikan sistem diskrit. Alogritma ini biasa digunakan untuk membangkitkan bilangan acak. Berikut persamaan Henon Map terdapat pada persamaan 2.5.

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{cases} \quad (2.3)$$

pada persamaan 2.5, perubahan (xn, yn) yang terjadi pada kondisi awal akan mempengaruhi bilangan acak yang dibangkitkan. Nilai a dan b adalah kunci rahasia dengan bilangan real. Bilangan acak digunakan untuk mengubah nilai piksel pada citra (Ratna et al. 2021). Henon Map dapat juga digunakan untuk teknik transposisi. (Lone et al.2021) dengan keterbatasan hanya dapat dilakukan pada citra persegi. Berikut persamaan Henon Map dengan teknik transposisi(Ping et al.2018).

$$I(\acute{x}, \acute{y})\ dimana \begin{cases} \acute{x} = 1 - ax^2 + y_i\ mod\ N \\ \acute{y} = b + x\ mod\ N \end{cases}$$

Persamaan diatas merupakan persamaan transposisi Henon Map untuk proses enkripsi. Dimana *a* dan *b* merupakan kunci rahasia dengan bilangan bulat positif, (*x*, *y*) merupakan posisi piksel awal, ($\acute{x}$, $y\acute{}$) posisi piksel baru, dan N merupakan ukuran citra. $I(\acute{x}, y\acute{})$ merupakan citra terenkripsi hasil transposisi. Berikut persamaan Henon Map dengan teknik transposisi pada proses dekripsi (Ping et al.2018).

$$I(x, y)\ dimana \begin{cases} x = \acute{y} - b\ mod\ N \\ y = \acute{x} - 1 + ax^2\ mod\ N \end{cases}$$

Persamaan 2.7 disajikan dekripsi fungsi transposisi henon map. Proses dekrip- si akan mengembalikan posisi piksel baru menjadi posisi piksel awal dengan kunci yang sama pada saat proses enkripsi. *I*(*x*, *y*) merupakan citra asli atau citra ter- dekripsi. Keter- batasan pada algoritma transposisi henon map selain hanya dapat

melakukan proses enkripsi pada citra berbentuk persegi tetapi juga pada tingkat keamanannya yang rendah karena tidak adanya perubahan intensitas warna pada citra terenkripsi se- hingga informasi masih dapat terbaca. Modi kasi fungsi transposisi henon map da- pat dilakukan agar proses enkripsi dan dekripsi dapat dilakukan pada citra dengan berbagai ukuran. Penggabungan teknik transposisi dan subtitusi dapat dilakukan agar proses enkripsi tidak hanya mengacak koordinat piksel tetapi juga adanya pe- rubahan nilai intensitas piksel.

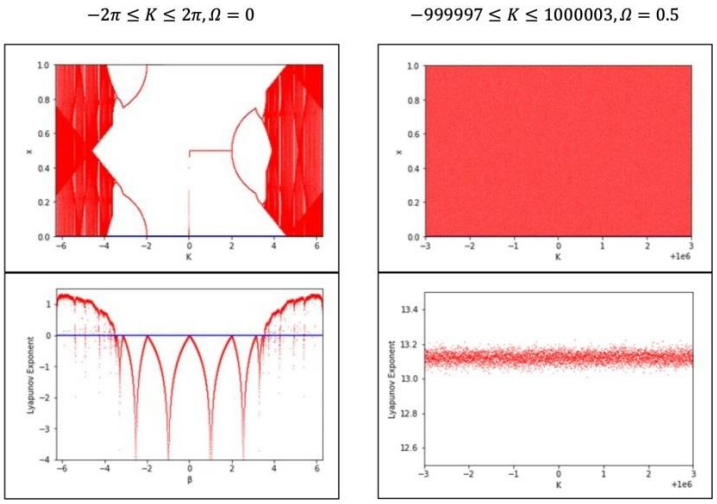
### 2.3.3 Circle Map

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

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

di mana mod 1 menunjukkan bagian desimal dari sebuah angka, sehingga nilai peta selalu lebih rendah dari 1 tetapi tidak kurang dari 0, dan parameter $\Omega$, $K \in$ R, $\Omega$ terdapat pada interval $0 \leq \Omega \leq 1$, karena ini adalah suku penjumlahan tunggal dalam modulo 1 ini, jadi semua nilai $\Omega$ 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 $\Omega$ 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 Perbandingan Tinjauan Pustaka

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 :

| Teknik | Penulis, Tahun | Metode Yang Digunakan | Hasil |
|---|---|---|---|
| The Implementation of Henon Map Algorithm for Digital Image Encryption | Suryadi MT, Edi Sukirman, M.Agus Mubarak, 2014 | Algoritma Henon Map untuk mengekripsi citra digital tipe *greyscale* ke tipe *colorfull* | Algoritma tersebut mengimplementasikan teori chaos yang memiliki kepekaan terhadap perubahan kecil pada nilai parameter awal dan memiliki tingkat keamanan yang tinggi dari serangan brute force |
| On the design of | Magfirawaty, | Menggunakan kombinasi dua | Desain yang diusulkan |

| | | | |
|---|---|---|---|
| henon and logistic map-based random number generator | Suryadi.M.T, dan Kalamullah Ramli, 2016 | sistem chaotic, yaitu peta Henon dan peta logistik, untuk menghasilkan urutan bit acak dengan nilai entropi tinggi, disimulasikan menggunakan LabVIEW | adalah sederhana dan metode yang sangat baik untuk menghasilkan bit acak, yang sangat dekat dengan nilai maksimum fungsi entropi, dan lulus |
| 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 Trinity Irsan, Yudi Satria, 2016 | Proses enkripsi menggunakan Modifikasi baru logistic map, disebut MS Map. Kemudian mengukur kinerja algoritma dengan NIST test, Histogram Analysis | Waktu rata-rata proses enkripsi dan dekripsi relatif sama, tergantung type dan ukuran citra. Algoritma sangat susah diserang dengan known plain text attack, Resistant terhadap brute-force |
| Deteksi Pemalsuan Citra Copy Move Menggunakan Dyadic Wavelet Dan | Wahyu Restuti Tresnaningsih, Endina Putri Purwandari, | citra digital akan didekomposisi menggunakan metode dyadic wavelet transform (DyWT) dan | pengujian menunjukkan metode DyWT dan SIFT mampu mendeteksi pemalsuan copy-move pada |

| | | | |
|---|---|---|---|
| Scale Invariant Feature Transform | Desi Andreswari, 2017 | diambil sub-citra LL, lalu mengekstraksi fitur lokal dengan metode scale invariant feature transform (SIFT) | area citra berbeda yang telah mengalami beberapa perubahan pemprosesan citra, seperti rotasi dan skala (diperbesar atau diperkecil) |
| 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. |
| A Hybrid Domain Image Encryption Algorithm Based on Improved Henon Map | Yong Chen, Shucui Xie, and Jianzhong Zhang, 2022 | Algoritma enkripsi citra domain hibrida dikembangkan dengan mengintegrasikan dengan peta Henon yang ditingkatkan, transformasi wavelet integer (IWT), dekomposisi bidang bit, dan operasi urutan asam deoksiribonukleat (DNA) | algoritma yang diusulkan sangat sensitif terhadap gambar biasa, dan memiliki tingkat keamanan yang tinggi dan ketahanan yang kuat terhadap berbagai serangan kriptanalisis. |

# 3. Metodologi penelitian

## 3.1 Skema Penelitian

Metode penelitian yang digunakan untuk proposal penelitian ini adalah 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 Henon Map.

### 3.2 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 Tabel Rencana Kegiatan

| KEGIATAN | 2022 | | | | 2023 | | | | | | | | | URAIAN |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 9 | 10 | 11 | 12 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | |
| Bimbingan | | | | | | | | | | | | | | Penyusunan Proposal SBK |
| SBK | | | | | | | | | | | | | | Penajaman proposal |
| Ujian Kualifikasi | | | | | | | | | | | | | | Penyusunan proposal kualifikasi |
| Evaluasi Progress | | | | | | | | | | | | | | Pembuatan Algoritma ekripsi Citra dan pengujian tingkat keamanan metode eksripsi |
| Evaluasi RKP | | | | | | | | | | | | | | Kesimpulan/Hasil |
| Sidang Tertutup | | | | | | | | | | | | | | Penajaman Hasil |
| Sidang Terbuka | | | | | | | | | | | | | | |

# DAFTAR PUSTAKA


1. 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
2. Hamsa A. Abdullah, Hikmat N. Abdullah *Colour image encryption using Nahrain chaotic map* Int. J. Wireless and Mobile Computing, Vol. 17, No. 2, 2019
3. 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*
4. 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
5. Suci BK , Suryadi, Algoritma Enkripsi Citra Digital Berbasis Chaos Menggunakan Fungsi MS GAUSS MAP. Disertasi, 2016
6. 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
7. Maria, YTI., Suryadi M.T, Yudi,S., *New Modified Map for Digital Image Encryptionand Its Performance*. Prosiding ACM, 2016
8. 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
9. Madenda ,S., Pengolahan Citra dan Video Digital, Teori Aplikasi dan Pemrograman Menggunakan Matlab, Penerbit Eirlanga, Jakarta, 2015
10. Boyland, PL., (1986). Bifurcations of circle maps: Arnol'd tongues, bistability and rotation intervals, (Berlin: Springer-Verlag)
11. Wiggins, S., *Introduction To Applied Nonlinear Dynamical Systems And Chaos*, book, Publisher: Springer Verlag, January 2003
12. Stewart, I., *Does God Play Dice? : The New Mathematics of Chaos*, Publisher Penguin Books Ltd, ISBN10 0140256024, 1997

13. Tresnaningsih,W.R, Purwandari, EP, Andreswari,D, Deteksi Pemalsuan Citra Copy Move Menggunakan Dyadic Wavelet Dan Scale Invariant Feature Transform,Jurnal Pseudocode, Volume IV Nomor 1, Februari 2017, ISSN 2355-5920, 2017
14. Chen, Y, Xie, S, Zhang,J, A Hybrid Domain Image Encryption Algorithm Based on Improved Henon Map, Entropy, 2022