UNIVERSITAS GUNADARMA

PENGEMBANGAN ALGORITMA ENKRIPSI CITRA DIGITAL BERBASIS KOMPOSISI LOGISTIC MAP DAN CIRCLE MAP

Pembimbing

Prof. Dr. Sarifuddin Madenda

DISERTASI

MAKMUN

99214914

PROGRAM DOKTOR TEKNOLOGI INFORMASI

2021

DAFTAR GAMBAR

DAFTAR TABEL

Bab I PENDAHULUAN

1.1. Latar Belakang Masalah

Kebutuhan manusia akan informasi online meningkat seiring dengan digitalisasi diseluruh aspek kehidupan. Dengan demikian, semakin tinggi pula data-data yang tersimpan dalam dunia maya untuk memenuhi kebutuhan akan informasi tersebut. Beberapa aplikasi yang ada mensyaratkan informasi detail dari setiap penggunanya baik berupa teks, citra, audio, video, dan multimedia. Dengan derasnya arus pengambilan data yang terjadi setiap hari, maka keamanan data menjadi hal yang sangat penting. Sistem keamanan data menjadi sangat riskan untuk dibuka dan diambil untuk tujuan-tujuan negatif. Sistem pengamanan data yang dilakukan untuk mencegah terjadinya kebocoran dokumen individu atau perusahaan dikenal dengan metode kriptografi.

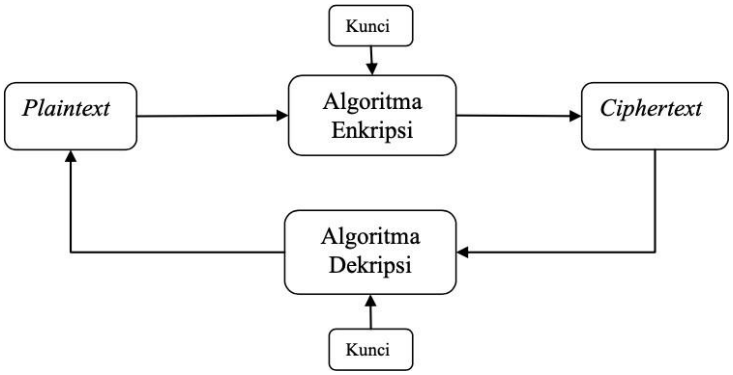
Beberapa data statistik menunjukkan, perkembangan yang pesat di bidang internet ternyata diiringi juga dengan tingginya tingkat percobaan pembobolan sistem keamanan. Pada tahun 1996, U.S. Federal Computer Incident Response Capability (FedCIRC) melaporkan bahwa lebih dari 2500 "insiden" di sistem komputer atau jaringan komputer yang disebabkan oleh gagalnya sistem keamanan atau adanya usaha untuk membobol sistem keamanan [13] Pada tahun 1996. NCC Information Security Breaches Survey di Inggris menunjukkan bahwa kejahatan komputer naik 200% dari tahun 1995 ke 1996. Survey ini juga menunjukkan bahwa kerugian yang diderita rata-rata US $30.000 untuk setiap insiden. Ditunjukkan juga beberapa organisasi yang mengalami kerugian sampai US $1.5 juta. Pada Juli 2020, Lembaga Riset Siber Indonesia Communication and Information System Security Research Center (CISSReC) menemukan bahwa ada orang yang membeli data 91 juta pengguna akun e-commerce Tokopedia yang bocor beberapa pada Mei 2020 lalu dan mengedarkan tautan unduhannya melalui Facebook.

Karena itu, faktor keamanan komputer sangat penting untuk terus ditingkatkan. Garfinkel [11] mengemukakan bahwa keamanan komputer (computer security) melingkupi empat aspek, yaitu privacy, integrity, authentication, dan availability. Serangan yang terjadi pada aspek privacy misalnya, adalah usaha untuk melakukan penyadapan (dengan program sniffer). Usaha-usaha yang dapat dilakukan untuk meningkatkan privacy dan confidentiality adalah dengan menggunakan teknologi kriptografi.

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentifikasi data (menezes, et al, 1996). Kriptografi telah digunakan untuk mengamankan berbagai

tipe data dengan cara menjaga kerahasiaannya oleh user agar tidak disalahgunakan oleh pihak yang tidak berkepentingan. Proses kriptografi dilakukan dengan mengenkripsi data asli yang disebut dengan *plaintext* dengan memberi keamanan sehingga dihasilkan *ciphertext*. Data asli tersebut diperoleh kembali setelah dilakukan proses deskripsi terhadap *ciphertext*. Proses mengubah *plaintext* menjadi *ciphertext* disebut enkripsi. Sedangkan proses kebalikannya yakni mengubah *ciphertext* menjadi *plaintext* disebut dengan deskripsi. Algoritma untuk mentransformasikan *plaintext* menjadi *ciphertext* disebut cipher. Dalam perkembangannya, algoritma enkripsi saat ini dibangun dengan menggunakan basis chaotic cipher agar kinerja dalam pengamanan data dan informasi meningkat.

Keamanan kriptografi modern tergantung pada key yang digunakan, bukan pada algoritmanya [Munir, 2012]. Mekanisme kriptografi berbasis key dapat digambarkan seperti gambar 1.1.



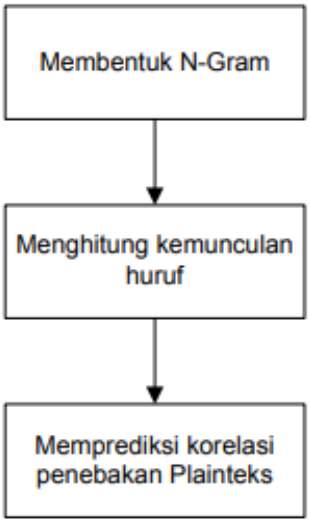
Gambar 1.1: Kriptografi Berbasis Kunci

Fungsi yang digunakan pada kriptografi adalah fungsi chaos. Dimana fungsi ini memiliki keunggulan dari sisi kecepatan, keamanan, kompleksitas, dan daya komputasi. Chaos merupakan jenis dari perilaku suatu sistem ataupun fungsi yang memiliki sifat acak dan peka terhadap nilai awal dan ergodisitas. Dalam teori probabilitas, ergodik adalah sebuah sistem dinamis yang secara garis besar memiliki perilaku yang sama pada sepanjang rata-rata waktu sejalan dengan rata-rata atas ruang dari seluruh keadaan sistem dalam ruang fasenya. Contoh proses ergodik adalah pengambilan data temperatur. Misal kita mengambil data temperatur pada suatu hari. Kita tidak bisa mengulangi proses tersebut pada hari sebelumnya (wiki). Fungsi yang memiliki sifat chaos dinamakan fungsi chaos. Fungsi chaos digunakan sebagai pembangkit bilangan acak. Beberapa fungsi yang bersifat chaos diantaranya adalah : circle map, logistic map, gauss map, Bernoulli map, dan sine map.

Dilihat dari pengembangannya, ilmu kriptografi dibagi menjadi dua, yaitu kriptografi klasik dan kriptografi modern. Kekuatan kriptografi klasik terletak pada kerahasiaan algoritma yang digunakan. Sedangkan kekuatan kriptografi modern terletak pada kerahasiaan kunci penyandian. Kriptografi klasik merupakan kriptografi yang digunakan pada zaman dahulu sebelum komputer ditemukan atau sudah ditemukan namun belum secanggih sekarang. Kriptografi ini melakukan pengacakan huruf pada *plaintext*. Kriptografi ini hanya melakukan pengacakan pada huruf A – Z. Sedangkan pada kriptografi modern terdapat berbagai macam algoritma yang dimaksudkan untuk mengamankan informasi yang dikirim melalui jaringan komputer. Algoritma kriptografi modern umumnya beroperasi dalam mode bit. Berbeda dengan kriptografi klasik yang beroperasi dalam mode karakter (seperti yang dilakukan pada cipher substitusi atau cipher transposisi dari algoritma kriptografi klasik). (https://mcdenin.wordpress.com/2018/02/10/kripografi-metode-klasik-dan-modern-kriptografi-beserta-contoh-enkripsi-dan-deskripsi/)

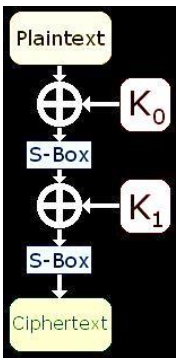
Berdasarkan kunci penyandiannya kriptografi dibagi menjadi dua jenis yaitu enkripsi kunci simetri dan enkripsi kunci publik. Suatu enkripsi dikatakan enkripsi simetris ketika proses enkripsi dan dekripsinya menggunakan kunci yang sama. Enkripsi publik artinya untuk proses enkripsi dan dekripsi menggunakan kunci yang berbeda. [Menezes et al.,1996] Dalam penyimpanan dan pengiriman data atau informasi rahasia terdapat dua tipe serangan, yaitu *cryptanalytic attack* dan brute force attack [Stallings, 2011]. Serangan tersebut bertujuan untuk memperoleh kunci sehingga dengan mudah memperoleh *plaintext* dari *ciphertext*. *Cryptanalytic attack* mengandalkan sifat dari algoritma dan juga dari karakteristik umum dari *plaintext* atau beberapa pasang *plaintext-ciphertext,* sedangkan brute force attack mencoba setiap kemungkinan kunci pada *ciphertext* sampai *plaintext* ditemukan.Terdapat beberapa cryptanalytic attack diantaranya, *ciphertext* only dan known *plaintext*. Pada *Ciphertext* only attack, hacker (penyerang) hanya mengetahui algoritma dan *ciphertext* sehingga secara statistik dapat mengidentifikasi *plaintext*. Sedangkan pada Known *plaintext* attack, hacker memiliki *ciphertext* yang ingin diketahui *plaintext*nya dan memiliki satu pasang atau lebih *ciphertext-plaintext* lainnya yang telah didapatkannya untuk mengungkap struktur algoritma dan kunci agar mendapatkan *plaintext*nya. [Stallings, 2011].

Statistical attack digunakan untuk mengetahui fenomena penyembunyian data acak/terenkripsi pada suatu media. (Westfeld, A. and Pfitzmann, A. 2000. Attack on Steganographic systems. 3rd International Workshop. Lecture Note in Computer Science, Springer Verlag Berlin, 1768) Statistical attack merupakan pemecahan chipertext dengan beberapa mekanisme yang memiliki skema sebagaimana tampak pada gambar 1.2.



Gambar 1.2. Skema Statistical Attack

Sedangkan *differential attack* bekerja dengan membandingkan variasi input dan variasi output terenkripsi untuk menemukan kunci atau pesan teks biasa yang diinginkan. Dalam model ini, penyerang dapat membuat sistem kriptografi dan mengenkripsi data yang dipilihnya menggunakan kunci target (yang merupakan rahasia). Dengan menganalisis hasil yang kembali (*ciphertext* yang diketahui), penyerang dapat menentukan kunci yang digunakan. Setelah kunci dipulihkan, transmisi masa depan yang menggunakannya dapat dengan cepat didekripsi. Munculnya teknologi, internet, dan sistem data otomatis, membuat skenario ini jauh lebih mungkin daripada yang diharapkan pada pandangan pertama. Seperti yang terlihat pada gambar 1. 3.



Gambar 1. 3. Skema Differential attack

Kinerja dari suatu algoritma dapat dilihat dari daya tahan keamanan algoritmanya terhadap serangan dan waktu komputasinya. Ada beberapa metode dalam penyandian diantaranya adalah dengan menggunakan algoritma Data Encryption Standard (DES), algoritma Advanced Encryption Standard (AES) dan algoritma Rivest-Shamir-Adleman (RSA). Algoritma tersebut mengenkripsi citra memerlukan waktu komputasi yang lama dan ruang kunci yang rendah walaupun menghasilkan data yang terenkripsi dengan baik. Namun, enkripsi citra digital yang lebih diutamakan adalah enkripsi citra digital yang memakan waktu lebih cepat tanpa mengorbankan keamanannya [Pareek, Patidar,dan Sud, 2006]. Salah satu solusi dari masalah keamanan citra tersebut adalah enkripsi citra berbasis chaos. Metode ini memberikan kombinasi yang baik dari kecepatan, keamanan yang tinggi, dan kompleksitas.

Chaos adalah tipe dari perilaku suatu sistem ataupun fungsi yang bersifat acak, peka terhadap nilai awal dan ergodisitas. Fungsi yang memiliki sifat chaos dinamakan fungsi chaos. Fungsi chaos sudah dibuktikan sangat cocok untuk proteksi data [Kocarev and Lian, 2011]. Fungsi yang memiliki sifat chaos antara lain *henon map, Arnold's cat map, circle map, logistic map, MS Map*, dan *tent map*. Karena keacakannya, fungsi chaos akan digunakan untuk membangkitkan barisan bilangan acak sebagai pembangkit kunci. Pendekatan enkripsi yang digunakan untuk teks tidak bagus untuk enkripsi citra [Munir, 2012]. Hal ini karena citra digital memiliki karakteristik tertentu seperti redundansi data. Data citra memiliki korelasi yang kuat antara pixel yang berdekatan baik secara horisontal, vertikal, dan diagonal. Sehingga enkripsi secara tradisional seperti IDEA, AES, DES, RSA, dan Blowfish tidak cocok untuk enkripsi citra.

Dua fungsi chaos yang sudah dikenal menunjukkan sifat chaos adalah Logistic Map dan Circle Map. Keduanya memiliki potensi keacakan yang tinggi. *Logistic Map* menjadi salah satu map paling terkenal di teorema sistem dinamis dan chaos. Map ini awalnya digunakan untuk menggambarkan pertumbuhan penduduk dunia seiring berjalannya waktu di bawah batasan berdasarkan fungsi kurva berbentuk S yang sangat umum. Dan sekarang Logistic Map dapat digunakan untuk mensimulasikan banyak proses alam. Fungsi logistik menggunakan diferensial persamaan yang memperlakukan waktu sebagai kontinu. Logistic Map malah menggunakan persamaan perbedaan nonlinier untuk melihat langkah-langkah waktu diskrit. Disebut peta logistik karena memetakan nilai populasi setiap saat langkah ke nilainya pada langkah waktu berikutnya (ps

Circle Map adalah map satu dimensi yang memetakan sebuah lingkaran ke dirinya sendiri. Circle Map juga sangat susah diserang dari brute force attack karena memiliki keunggulan dengan nilai entropi 7.99 dengan korelasi terendah mendekati nol dan ruang kunci mencapai 103×17.

Korelasi mendekati nol dan entropi mendekati 8 adalah parameter penting untuk enkripsi gambar yang baik.[Roshini, Sridevi, Lakhsmi, 2019].

Algoritma komposisi secara sekuensial yaitu Gauss Map dan Circle Map [Yudi, Suryadi, Luqman, 2019] digunakan untuk menyelidiki kemungkinan sifat chaos yang lebih besar. Algoritma ini memiliki diagram sensitifitas yang jauh lebih besar terhadap nilai awal. Algoritma ini kurang cocok untuk RNG karena hanya 4 yang memenuhi dari 16 uji NIST. Jadi tingkat keacakannya hanya 25%. Jika Gauss-Circle Map ini digunakan untuk tujuan kriptografi, maka sistem kriptografinya akan memiliki ketahanan *brute force attack* yang kuat namun lemah terhadap *statistical attack*. Berdasarkan beberapa penelitian tersebut, maka pada penelitian ini akan dikembangkan fungsi chaotik baru untuk membangkitkan key stream dengan komposisi fungsi Logistic Map dan Circle Map. Tujuannya adalah meningkatkan daya tahan algoritma enkripsi terhadap berbagai serangan.

1.2. Rumusan Masalah Penelitian

Berdasarkan uraian latar belakang, rumusan masalah pada penelitian ini adalah:

a. Bagaimana upaya dalam menghasilkan fungsi chaos baru berdasarkan fungsi Logistic Map dan Circle Map sebagai fungsi pembangkit bilangan acak ?
b. Bagaimana merancang dan mengimplementasikan algoritma baru untuk mengenkripsi dan mendekripsi citra digital menggunakan fungsi chaos baru tersebut?
c. Bagaimana kinerja implementasinya algoritma tersebut terhadap berbagai serangan?

1. 3. Tujuan Penelitian

Tujuan dari penelitian ini antara lain:

a. Menganalisis dan menghasilkan fungsi chaos baru berdasarkan fungsi Logistic Map dan fungsi circle Map menggunakan konsep komposisi fungsi, sebagai fungsi pembangkit bilangan acak.
b. Menghasilkan algoritma baru dan program aplikasi baru untuk mengenkripsi dan mendekripsi citra digital menggunakan fungsi chaos baru tersebut.
c. Menguji dan menganalisis daya tahan algoritma baru dalam mengenkripsi dan mendekripsi citra digital terhadap *brute-force, statistical attack, dan differential attack* secara kualitatif dan kuantitatif.

1.4. Batasan Masalah Penelitian

Batasan pada penelitian ini antara lain:

Dalam pengujian chaotic terhadap fungsi chaos baru yang diperoleh tersebut menggunakan :

a. Nilai Lyapunov exponent,
b. Diagram bifurkasi, dan
c. Uji NIST.

Analisis daya tahan algoritma dilakukan berdasarkan:

a. Analisis tingkat sensitifitas nilai awal
b. Besarnya ruang kunci
c. Analisis histogram, korelasi, dan entropi
d. Analisis distribusi uniform dari chipper image
e. Analisis kualitas citra dengan PSNR

1.5. Kontribusi Hasil Penelitian

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

a. Fungsi chaos baru sebagai pembangkit bilangan acak bersifat chaos (berupa chaotic key stream).
b. Algoritma baru enkripsi dan dekripsi citra digital berbasis fungsi chaos baru.
c. Program aplikasi baru enkripsi dan dekripsi citra digital sebagai implementasi algoritma baru tersebut berbasis fungsi chaos baru.

Bab II STUDI LITERATUR

2.1. Landasan Teori

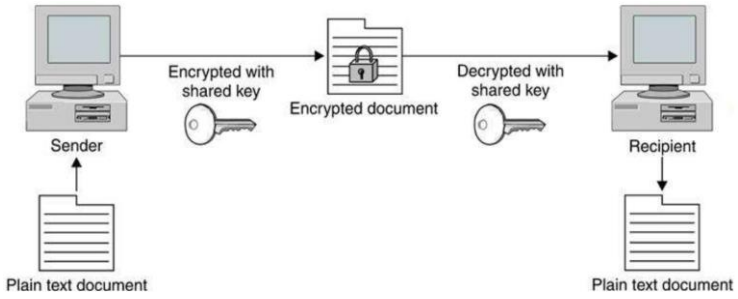
2.1.1. Kriptografi

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.

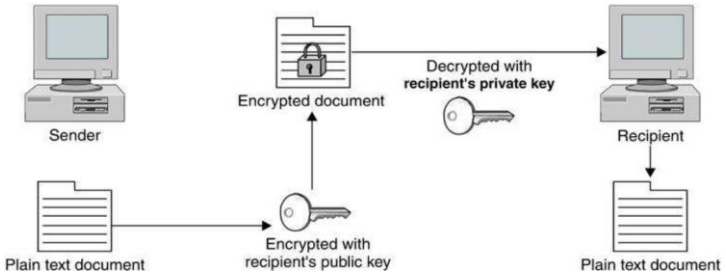
Kriptografi berasal dari bahasa Yunani yaitu kryptos dan graphia. Kryptos berarti sesuatu yang disembunyikan, tidak dikenal, terselubung, rahasia, atau misterius. Sedangkan graphia berarti tulisan sehingga kata kriptografi dapat diartikan sebagai tulisan yang disembunyikan atau dirahasiakan. Menurut [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 2.1 dan 2.2.



Gambar 2.1: Bagan Umum Proses Enkripsi Kunci Simetris



Gambar 2.2: 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.

2.1.2. Citra Digital

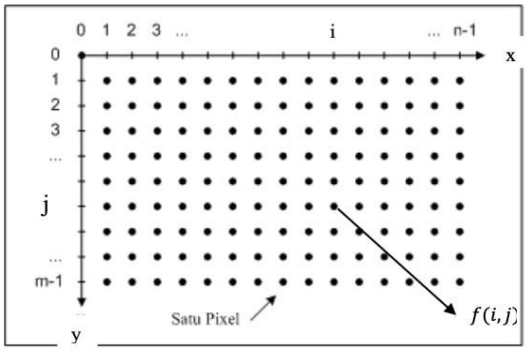
2.1.2.1. Citra Digital

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).

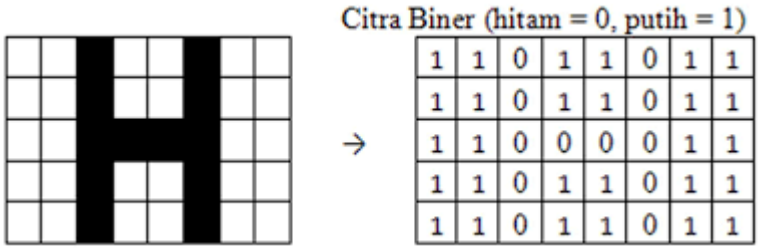
Citra digital berukuran n × m didefinisikan sebagai himpunan fungsi dua variabel f (x, y) dengan x dan y merupakan koordinat spasial, dan amplitudo f di setiap koordinat (x,y) dinamakan intensitas atau tingkat keabuan dari citra pada titik tersebut. Adapun nilai dari variabel x, y dan f (x, y) adalah 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 2.3 menunjukkan representasi citra digital berdasarkan keadaan pixel.

2.1.2.2. 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 2.4. 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. 3. 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. Untuk mengubah citra berwarna yang mempunyai nilai matrik masing-masing R, G dan B menjadi citra grayscale dengan nilai X, maka konversi dapat dilakukan dengan mengambil rata-rata dari nilai R, G dan B sehingga dapat dituliskan menjadi:

- X = (R+G+B)/3 ..... (2.1)

- Warna = RGB(X, X, X) ..... (2.2)

Gambar 2.5. Citra Grayscale

2.1.2.4. Citra RGB

Red (Merah), Green (Hijau) dan Blue (Biru) merupakan warna dasar yang dapat diterima oleh mata manusia. Setiap piksel pada citra warna mewakili warna yang merupakan kombinasi dari ketiga warna dasar RGB. Setiap titik pada citra warna membutuhkan data sebesar 3 byte. Setiap warna dasar memiliki intensitas tersendiri dengan nilai minimum nol (0) dan nilai maksimum 255 (8 bit). RGB didasarkan pada teori bahwa mata manusia peka terhadap panjang gelombang 630nm (merah), 530 nm (hijau), dan 450 nm (biru).

Gambar 2.6. Citra Warna pada RGB

Pada gambar di atas dapat diambil beberapa kesimpulan yaitu:

1. RGB terdiri dari tiga warna utama, yaitu merah, hijau, dan biru.

2. Campuran dua warna pada RGB menghasilkan warna baru, yaitu kuning = merah + hijau, cyan = hijau + biru, dan magenta = biru + merah.

3. Bila seluruh warna merah, hijau, dan biru dicampur akan menghasilkan warna putih.

4. Bila warna merah, hijau, dan biru tidak dicampur maka akan menghasilkan warna hitam.

5. Jenis warna lain akan dihasilkan oleh variasi campuran warna dan intensitas campuran setiap warna

2.1.3. 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*.

Ada banyak chaotic map yang telah ditemukan, salah satunya adalah *Logistic Map*. *Logistic Map* merupakan salah satu fungsi chaos sederhana di dalam ekologi yang digunakan untuk mensimulasikan pertumbuhan populasi spesies. Logistic Map juga merupakan satu dimensi yang telah digunakan secara luas, yang didefinisikan sebagai berikut : Xi+1= r Xi (1 - Xi) (1) Dari persamaan di atas, X adalah populasi spesies pada interval waktu yang ditentukan dengan X0 adalah nilai awal iterasi. Daerah asal X adalah dari 0 sampai 1, yang dalam hal ini 1 menyatakan populasi maksimum dan yang 0 menyatakan kepunahan, sedangkan $0 \leq r \leq 4$. Konstanta r menyatakan laju pertumbuhan. Konstanta r juga menyatakan bagian nirjalar dari persamaan. Ketika r meningkat, maka sistem juga naik.

2.1.3.1. 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.

2.1.3.2. 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].

Definisi 2.1 $f : X \rightarrow X$ dikatakan ketergantungan yang sensitif 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:

$$f^{(1)}(x_0) = f(x_0), f^{(2)}(x_0) = f(f(x_0)), f^{(3)}(x_0) = f(f(f(x_0))) \qquad (2.1)$$
$$\text{Secara Umum: } f^{(n)}(x_0) = \underbrace{f(f(f(\ldots((x_0))\ldots)))}_{n-1}$$

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 [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:

$$\mu = \lim_{n\to\infty} \frac{1}{n}\sum_{i=0}^{n-1} ln \left| \left(f^{(i)}\right)' (x_0) \right| \qquad (2.2)$$

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.

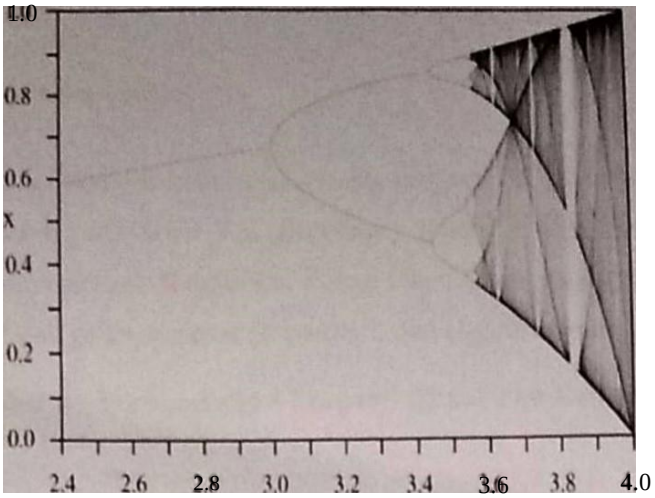
2.1.3.3. Logistic Map

Persamaan logistik (*Logistic Map*) merupakan contoh pemetaan polinomial derajat dua, dan seringkali digunakan sebagai contoh bagaimana rumitnya sifat chaos yang dapat muncul dari suatu persamaan yang sangat sederhana. Persamaan ini dipopulerkan oleh seorang ahli biologi yang bernama Robert May pada tahun 1976. Ia menulis makalah yang menarik di Nature tentang *Logistic Map*. Hal itu memicu revolusi analisis dinamis dan secara bertahap berkembang menjadi luas seperti sekarang ini. *Logistic Map* menjadi salah satu map paling terkenal di teorema sistem dinamis dan chaos ini awalnya digunakan untuk menggambarkan pertumbuhan penduduk di dunia seiring berjalannya waktu di bawah batasan berdasarkan fungsi kurva berbentuk S yang sangat umum. Dan sekarang *logistic Map* dapat digunakan untuk mensimulasikan banyak proses di alam.

Logistic Map juga merupakan satu dimensi yang telah digunakan secara luas dengan definisi sebagai berikut :

$$Xn + 1 = r\,Xn\,(1 — Xn) \quad (2.\ 3)$$

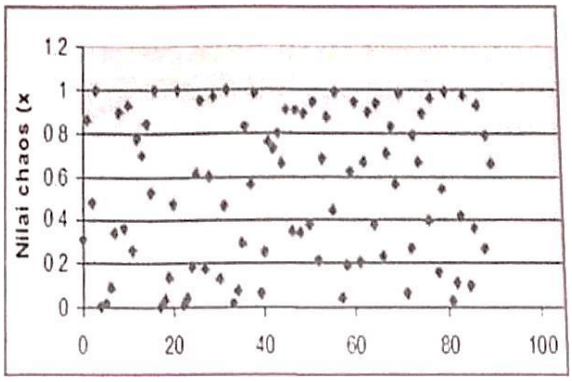
Dimana : x : bilangan diantara nol dan satu, yang merepresentasikan populasi pada tahun ke n. Parameter x dapat disebut juga sebagai nilai chaos (0 < x < l)



Gambar. 2.7. Bifurkasi Logistic Map

r : bilangan postif yang merepresentasikan kombinasi antara nilai reproduksi dan makanan. Parameter r dapat disebut juga dengan sebutan laju pertumbuhan (0 < r < 4).

Persamaan logistik ini dapat diterapkan dalam dunia kriptografi dengan membuat fungsi seperti yang telah dicantumkan diatas. Setelah membuat fungsi tersebut, kita melakukan proses perhitungan dengan melakukan iterasi secara berulang, sehingga kita akan selalu mendapatkan bilangan yang benar-benar acak. Kita dapat melihat contoh hasil bilangan acak yang kita dapatkan dengan melakukan puluhan dan ratusan kali proses iterasi pada gambar di bawah ini.



Gambar. 2.8. Nilai Chaos pada Percobaan Logistic Map

2.1.3.4. Circle Map

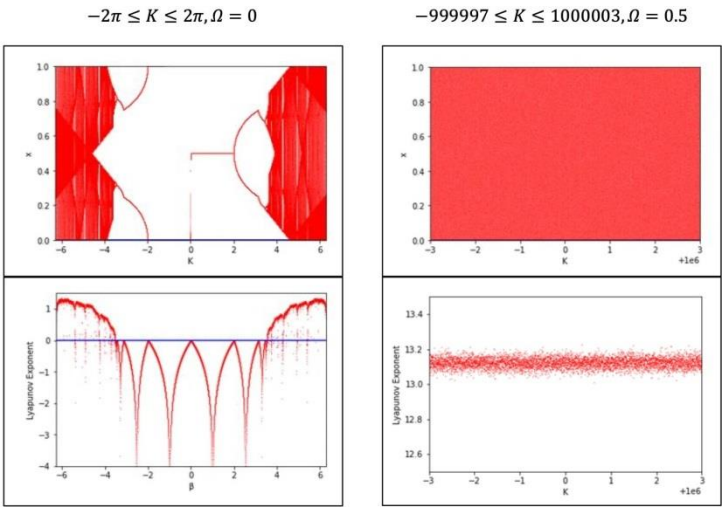
Circle map adalah fungsi satu dimensi yang memetakan sebuah lingkaran ke dirinya sendiri. Circle Map didefinisikan dengan persamaan berikut.[Boyland,1986]

$$x_{n+1} = x_n + \Omega + \frac{K}{2\pi}\sin(2\pi x_n) \bmod 1 \quad (2.4)$$

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 $\Omega, K \in \mathrm{R}$, 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 2.9: Bifurkasi dan *Lyapunov exponent* Circle Map

2.1.4. 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 ◦ g untuk semua a ∈ A didefinisikan oleh:

(f ◦ g) (a) = f (g (a))

Dengan kata lain, untuk menemukan (f ◦ 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 ◦ g) (a) = f (g (a))[Rosen, 2012].

2.1.5. 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).

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 $p \oplus 0 = p$, $p = 0, 1$. Berdasarkan tabel 2.1 terlihat bahwa negasi dari tiap elemen yaitu $-p = p$ sehingga disimpulkan bahwa operasi negasi dari XOR adalah XOR itu sendiri.

2.1.6. 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 15 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

14.The Random Excursions Test

15.The Random Excursions Variant Test

2.1.7. 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 (2.5) sampai (2.8) berikut:

$$r_{xy} = \frac{cov\,(x,y)}{\sqrt{D\,(x)\,D\,(y)}} \tag{2.5}$$

$$cov\,(x,y) = \frac{1}{n}\sum_{i=1}^{n}\left[x_i - E\,(x)\right]\left[y_i - E\,(y)\right] \tag{2.6}$$

$$D\,(x) = \frac{1}{n}\sum_{i=1}^{n}\left[x_i - E\,(x)\right]^2 \tag{2.7}$$

$$E\,(x) = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{2.8}$$

cov adalah kovariansi

D adalah standard deviasi

E adalah rata-rata

Terdapat dua dari beberapa teknik korelasi yang sangat populer sampai sekarang yaitu Korelasi Pearson Product Moment dan Korelasi Rank Spearman. Korelasi Pearson merupakan korelasi sederhana yang hanya melibatkan satu variabel terikat (*dependent*) dan satu variabel bebas (*independent*). Korelasi Pearson menghasilkan koefesien korelasi yang berfungsi untuk mengukur kekuatan hubungan linier antara dua variabel. Jika hubungan dua variabel tidak linier, maka koefesien korelasi Pearson tersebut tidak mencerminkan kekuatan hubungan dua variabel yang sedang diteliti, meski kedua variabel mempunyai hubungan kuat. Koefisien korelasi ini disebut koefisien korelasi Pearson karena diperkenalkan pertama kali oleh Karl Pearson tahun 1990 (Firdaus, 2009).

2.2. Kajian Penelitian

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
Continue . . .			

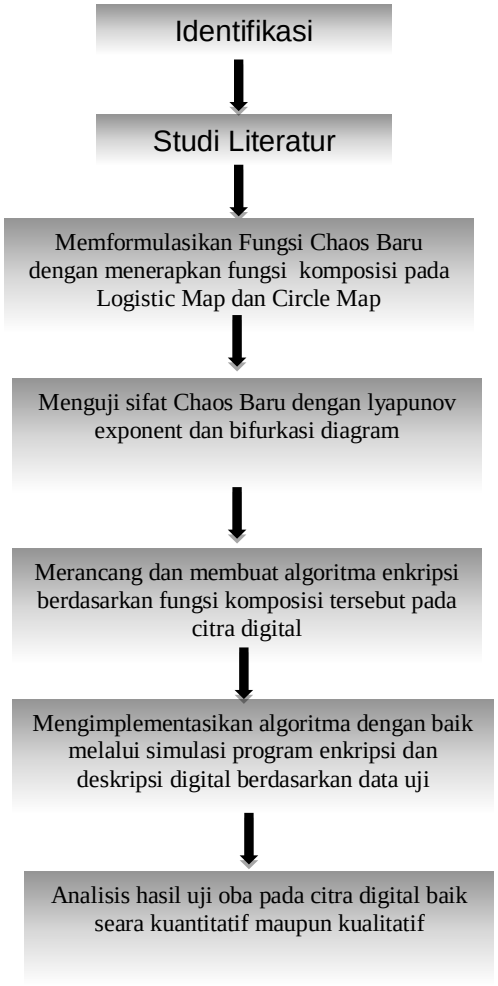
Teknik	Penulis, Tahun	Metode yang digunakan	Hasil
Permutasi Mul- tiple Circular Shrinking	Yohan Suryanto, Suryadi, Kalamullah Ramli, 2016	Enkripsi Gambar yang Aman dan Kokoh Berdasarkan Permutasi Multiple Circular Shrinking	metode yang diusulkan tahan terhadap serangan statistic juga tahan terhadap kompresi 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 attack
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
Continue . . .			

Teknik	Penulis, Tahun	Metode yang digunakan	Hasil
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 METODE PENELITIAN

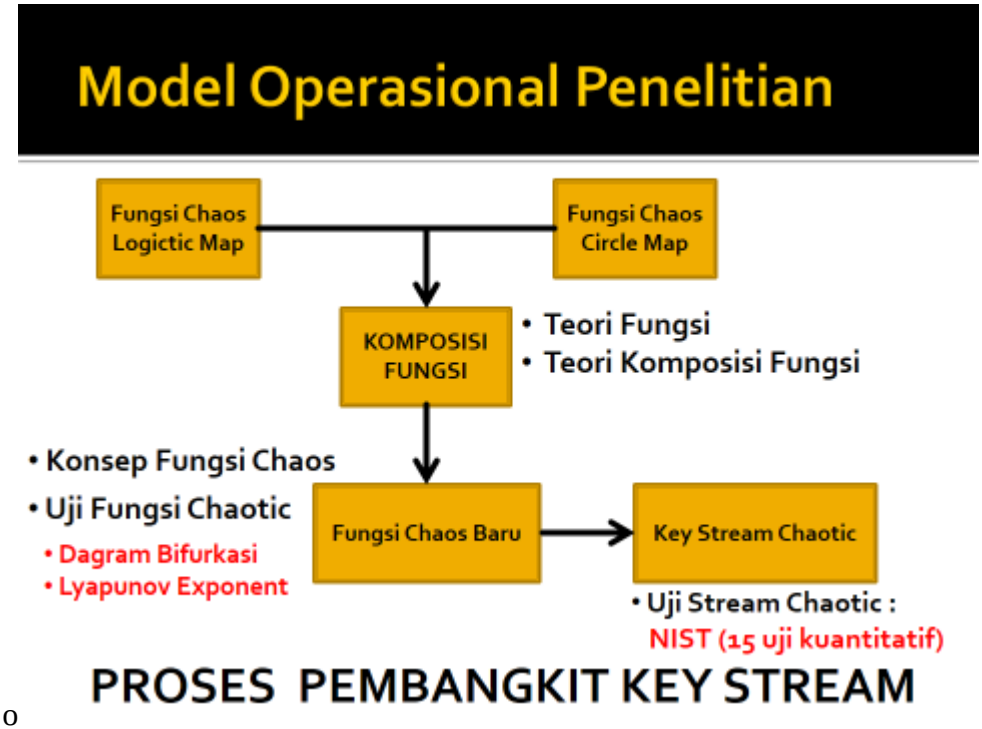
3.1. Skema Tahapan Penelitian

Secara garis besar metode atau tahapan penelitian yang dilakukan dalam penyelesaian disertasi ini diperlihatkan oleh Gambar 3.1. Tahapan penelitian ini dilakukan secara terstruktur dan sistematis, sehingga diperoleh hasil yang optimal.



Gambar 3.1. Diagram Alur Penelitian

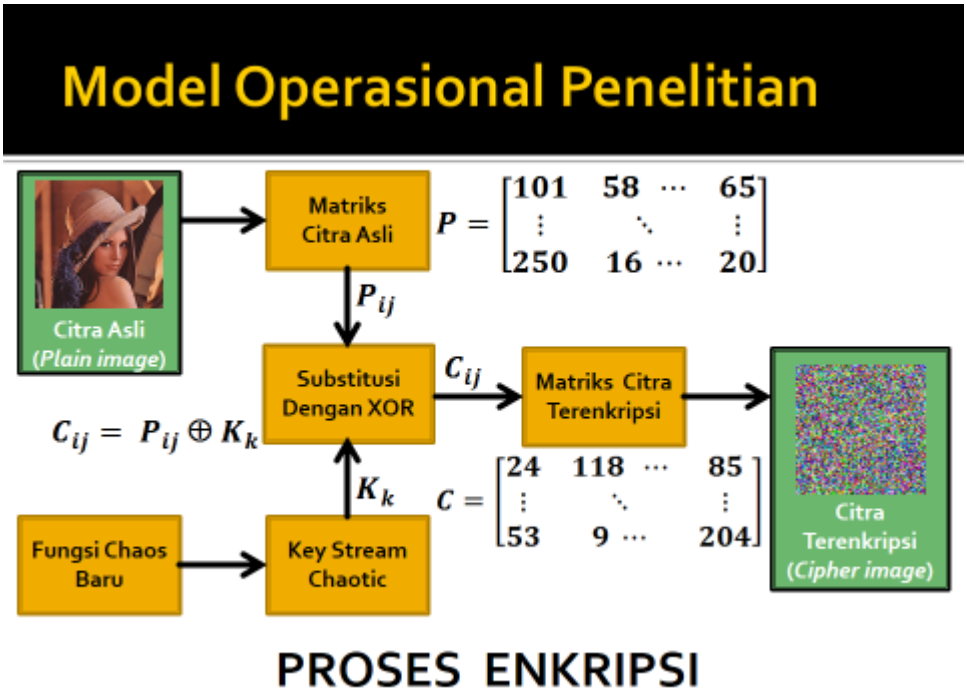
3.2. Model Operasional Penelitian



o

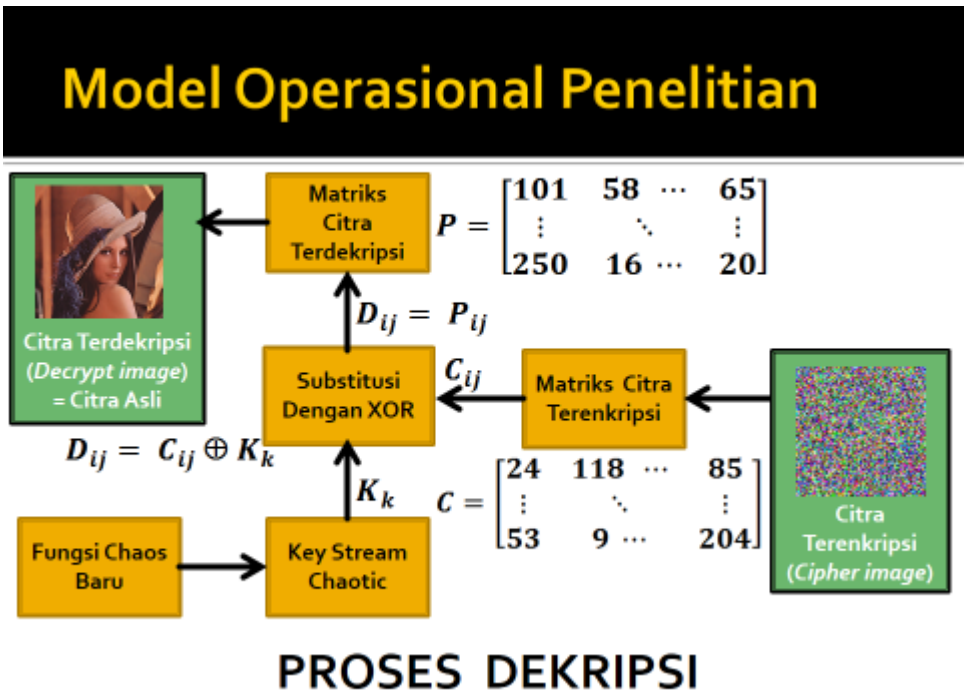
Gambar 3.2. Model Operasional Penelitian Proses Pembangkit Key Stream

Model Operasional Penelitian yang dilakukan adalah memasukkan fungsi chaos Logistic Map dan Circle Map. Dari gabungan keduanya akan dihasilkan komposisi fungsi yang mengacu pada bab 2.1.4. Komposisi fungsi tersebut akan menghasilkan fungsi chaos baru yang akan dijadikan key stream chaotic. Selanjutnya untuk memastikan bahwa fungsi baru Logistic Map dan Circle Map bersifat chaotic, maka perlu dilakukan pengujian sifat chaoticnya. Hal tersebut ditunjukkan berdasarkan analisis diagram bifurkasi dan Lyapunov exponent yang terbentuk. Selain itu juga mengacu pada barisan bilangan yang dibangkitkan oleh fungsi tersebut secara acak. Untuk menguji keacakan key stream yang dihasilkan, maka akan dilakukan uji NIST.



Gambar 3. 3. Model Operasional Penelitian Proses Enkripsi

Model operasional penelitian yang pertama dilakukan adalah proses enkripsi, dimana citra asli dirubah ke matriks citra asli. Setelah itu, matriks tersebut disubstitusi dengan XOR. Sementara itu, fungsi chaos baru dijadikan key stream chaotic yang juga akan disubstitusi dengan XOR. Keduanya akan menghasilkan matriks citra terenkripsi yang akan membentuk citra terenkripsi.



Gambar 3. 4. Model Operasional Penelitian Proses Dekripsi

Model operasional penelitian yang dilakukan untuk mengembalikan citra asli adalah proses deskripsi, dimana citra terenkripsi dirubah ke matriks citra terenkripsi kemudian matriks tersebut akan disubstitusi dengan XOR. Sementara itu, fungsi chaos baru dijadikan key stream chaotic yang juga akan disubstitusi dengan XOR. Keduanya akan menghasilkan matriks citra terdeskripsi yang selanjutnya akan dirubah menjadi citra terdekripsi.

3.3. Fungsi Komposisi Logistic Map dan Circle Map

Fungsi chaos baru dalam penelitian ini diformulasikan melalui proses komposisi dua fungsi chaos yaitu Logistic Map dan fungsi chaos Circle Map. Proses komposisi fungsi chaos Logistic Map dan Circle Map dapat dilakukan karena keduanya mempunyai derajat dan dimensi yang sama. Jika fungsi Logistic Map dinyatakan sebagai f(x) dan fungsi Circle Map sebagai fungsi g(x), maka fungsi komposisi Logistic Map dan Circle Map dinyatakan sebagai fungsi h(x) , yaitu :

Fungsi Logistic Map

$f(x) = xn+1 = r\ xn\ (1 - xn) \bmod 1$ (3.1)

Fungsi Circle Map

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

Dikomposisikan
$(f \circ g)(x) =$
Untuk $0 \leq x \leq 1$ $= x_{n+1} = r\ xn\ (1 - xn) \bmod 1$
Untuk $0 \leq x \leq 1$ $= x_{n+1} = x_n + \Omega + \frac{K}{2\pi}\sin(2\pi x_n) \bmod 1$

$h(x) = (f \circ g)(x) = f\ (g(x)) = r(x + \Omega + \frac{K}{2\pi}\sin(2\pi x) \bmod 1)\ (1 - x + \Omega + \frac{K}{2\pi}\sin(2\pi x) \bmod 1) \bmod 1$ (3. 3)

Jadi didapatkan fungsi rekursif adalah:

$(f \circ g)(x_{n+1}) = r(x_n + \Omega + \frac{K}{2\pi}\sin(2\pi x_n) \bmod 1)\ (1 - x_n + \Omega + \frac{K}{2\pi}\sin(2\pi x_n) \bmod 1) \bmod 1$ (3. 4)

Persamaan (3.3) merupakan hasil komposisi fungsi dari dua fungsi chaos. Fungsi ini memiliki 4 parameter yaitu Xn ∈ (0, 1) dan r, Ω, K ∈ R. Selanjutnya untuk memastikan bahwa fungsi baru Logistic Circle Map bersifat chaotic, maka perlu dilakukan pengujian sifat chaoticnya.

Hal tersebut ditunjukkan berdasarkan analisis diagram bifurkasi dan Lyapunov exponent yang terbentuk. Selain itu juga mengacu pada barisan bilangan yang dibangkitkan oleh fungsi tersebut secara acak. dan menguji keacakan key stream yang dihasilkan fungsi dengan uji NIST.

3.4. Rencana Kegiatan

Untuk mencapai target penelitian/ disertasi, 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 beikut :

Table 3.1. Jadwal Desertasi

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 Progres 1															Prepocessing Data
Publikasi															Publikasi dalam bentuk jurnal
Evaluasi Progres 2															Penetapan Model Algoritma Chaotic Baru
Publikasi															Publikasi dalam bentuk jurnal
Evaluasi RKP															Kesimpulan/Hasil
Draf Disertasi															
Sidang Tertutup															Penajaman Hasil
Sidang Terbuka															

Daftar Pustaka

1. Menezes A., Oorschot, P.V., dan Vanstone,S, Handbook of Applied Cryptography, CRC Press, 1997
2. Chen, Shaoqiu et al, Logistic Map: Stability and Entrance to Chaos, 2021 Journal of Physics: Conference Series, 2014 012009
3. 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
4. Stallings, W. Computer and Network Security : Principle and Practice (5th ed.). New York: Prentice hall.
5. Pareek, N.K., Patidar, V., Sud, K.K. Image encryption using chaotic logistic map. Journal of Image and Vision Computing, 24, 926-934.
6. Kocarev, L., and Lian, S. Chaos-based cyrptography. Berlin Heidelberg : Springer-Verlag.
7. Maria, YTI., Suryadi M.T, Yudi,S., New Modified Map for Digital Image Encryptionand Its Performance. Prosiding ACM, 2016
8. 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
9. Suci BK , Suryadi, Algoritma Enkripsi Citra Digital Berbasis Chaos Menggunakan Fungsi MS GAUSS MAP. Disertasi, 2016
10. 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
11. Schneier, B, Applied Cryptography Prootocols, Algorithms, and Source Code in C, Publisher: John Wiley & Sons, Inc. ISBN: 0471128457. Publication Date: 01/01/96
12. Munir,R., Kriptografi, Informatika Bandung, 2006
13. Madenda ,S., Pengolahan Citra dan Video Digital, Teori Aplikasi dan Pemrograman Menggunakan Matlab, Penerbit Eirlanga, Jakarta, 2015
14. Rafael C. Gonzales and E.Woods.. Digital Image Processing. New Jersey: Prentice-Hall, Inc., 2002
15. Wiggins, S., Introduction To Applied Nonlinear Dynamical Systems And Chaos, book, Publisher: Springer Verlag, January 2003
16. Stewart, I., Does God Play Dice? : The New Mathematics of Chaos, Publisher Penguin Books Ltd, ISBN10 0140256024, 1997

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

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

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

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

21. National Institute of Standard and Technology (NIST). (2010). A statistical test suite for random and pseudorandom number generators for cryp- tographic applications (Special Publication 800-222). U.S. Department of Commerce. Rosen, K.H. (2012). Discrete mathematics and its applications (7th ed.). New York : McGraw-Hill.

22. Jaya, Danang, Visual Attack dan Statistical Attack pada Aplikasi Steganography, D,irektorat Analisis Sinyal Deputi Pengamanan Persandian Lembaga Sandi Negara,

23. Suci BK , Suryadi, Triswanto, IMPLEMENTASI ALGORITMA ENKRIPSI CITRA DIGITAL BERBASIS CHAOS MENGGUNAKAN FUNGSI KOMPOSISI LOGISTIC DAN GAUSS ITERATED MAP, Seminar Nasional Edusainstek ISBN : 978-602-5614-35-4