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

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.

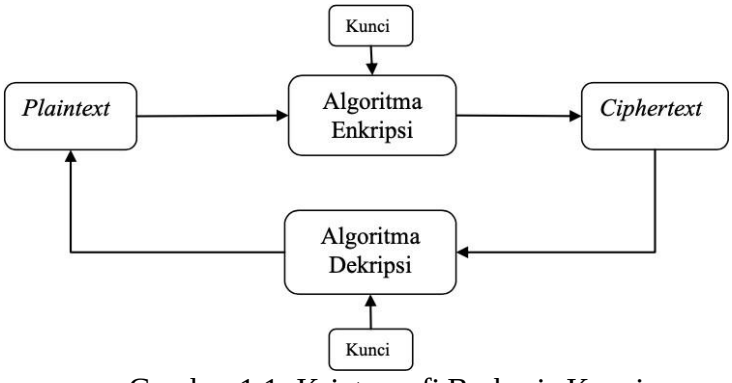
Beberapa data statistik menunjukkan, perkembangan yang pesat di bidang internet ternyata diiringi juga dengan tingginya tingkat percobaan pembobolan sistem keamanan. Pada tahun 1996, U.S. Federal Computer Incident Response Capability (FedCIRC) melaporkan bahwa lebih dari 2500 “insiden” di sistem komputer 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.



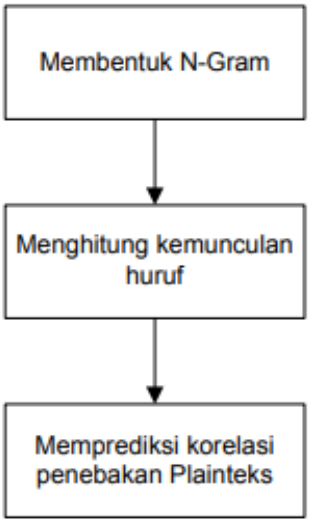
Gambar 1.1: Kriptografi Berbasis Kunci

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/)

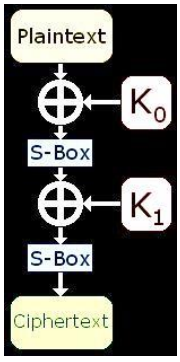
Berdasarkan kunci penyandiannya kriptografi dibagi menjadi dua jenis yaitu enkripsi kunci simetri dan enkripsi kunci publik. Suatu enkripsi dikatakan enkripsi simetris ketika proses enkripsi dan dekripsinya menggunakan kunci yang sama. Enkripsi publik artinya untuk proses enkripsi dan dekripsi menggunakan 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. 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.

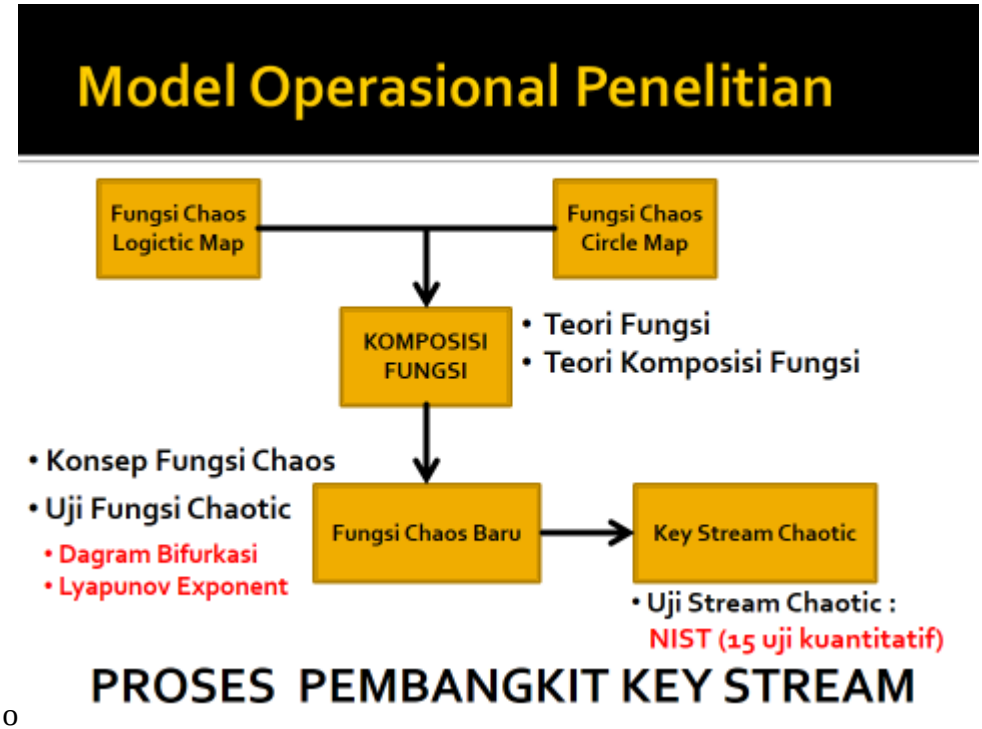
Bab III METODE PENELITIAN

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

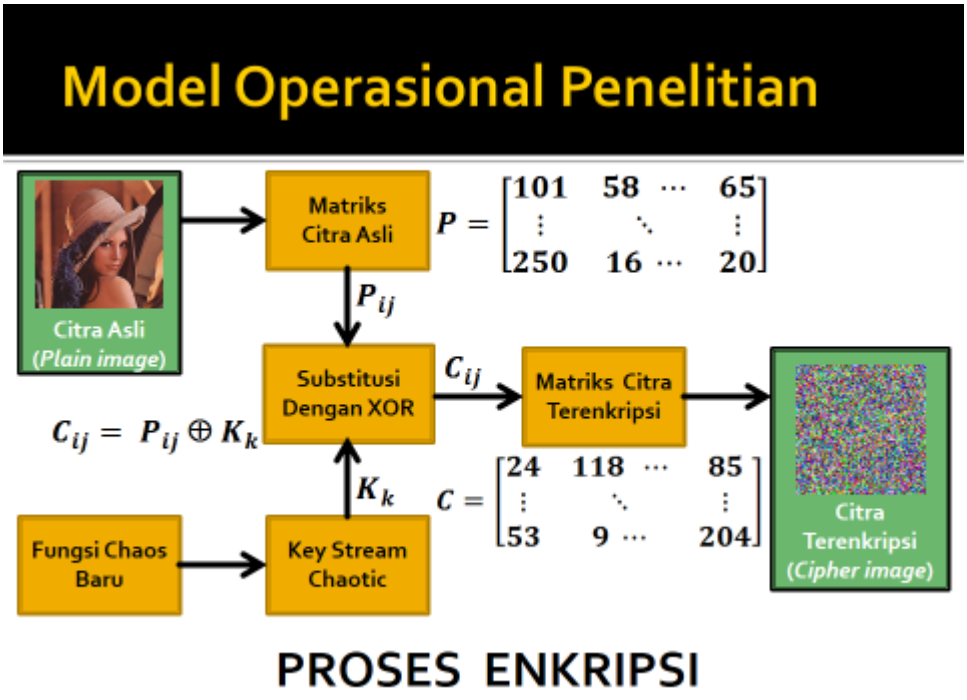
3.2. Model Operasional Penelitian



o

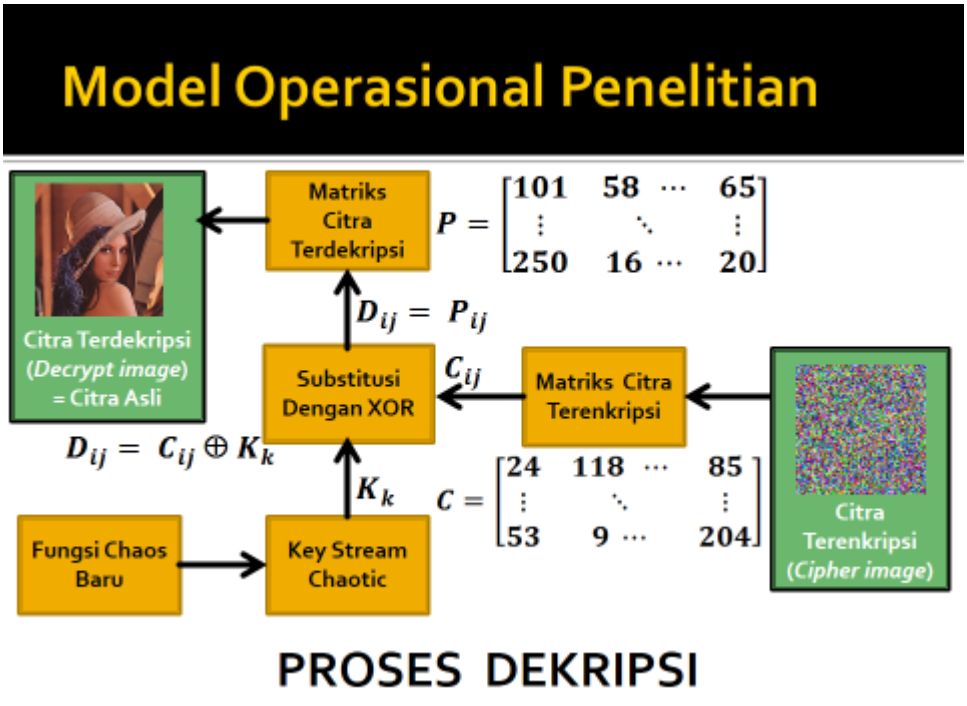
Gambar 3.2. Model Operasional Penelitian Proses Pembangkit Key Stream

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:

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

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.