PROPOSAL PENELITIAN

KUALIFIKASI

PENGEMBANGAN KRIPTOGRAFI PADA CITRA DIGITAL BERBASIS CHAOTIC MAP

Rama Dian Syah
99219031

PROGRAM DOKTOR TEKNOLOGI INFORMASI

UNIVERSITAS GUNADARMA

2021

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi dan komunikasi menyebabkan digitalisasi pada media citra untuk memberikan informasi. Digitalisasi media citra dapat memudahkan akses dan modifikasi terhadap konten pada data yang ditransmisikan. Kemudahan pada digitalisasi citra menyebabkan peluang terhadap kejahatan yang mungkin terjadi seperti akses tidak sah, modifikasi konten, pelanggaran hak cipta, dan lain-lain (Hamza, 2019). Keamanan data menjadi sangat penting pada media digital untuk menghindari kejahatan yang mengancam data yang bersifat rahasia dan privasi. Berbagai teknologi dan komunikasi menggunakan media gambar atau citra di semua aspek untuk memudahkan pengguna. Citra dapat mengandung berbagai arti dan makna dalam menggambarkan suatu objek data atau informasi. Keamanan citra diperlukan untuk melindungi makna informasi yang ada di dalamnya.

Kriptografi merupakan ilmu yang berhubungan dengan transformasi data untuk membuat artinya tidak dipahami (untuk menyembunyikan maknanya), mencegahnya dari perubahan tanpa izin, atau mencegahnya dari penggunaan yang tidak sah. Kriptografi menggunakan berbagai macam teknik matematika untuk menjaga konten pada pesan terenkripsi (Joshi & Karkade, 2015). Kriptografi pada citra dapat diterapkan dengan metode *chaotic*. Metode *chaotic* merupakan teknik untuk enkripsi yang berdasarkan gerakan atau dinamika yang rumit dan tidak terduga tergantung pada keadaan atau kondisi awal pada sebuah sistem (Lone et al., 2021). Beberapa algoritma yang merupakan kriptografi berbasis *chaotic* yaitu algoritma *Cat Map*, *Henon Map* (Ratna et al., 2021), dan *Logistic Map* (Lone et al., 2021).

Cat Map merupakan algoritma yang ditemukan oleh ahli matematik Rusia bernama Vladimir Arnold yang membuktikan algoritmanya pada citra kucing (Ratna et al., 2021). *Henon Map* adalah algoritma yang ditemukan oleh ahli matematik Perancis bernama Michael Henon dan merupakan bentuk simplifikasi

algoritma dari model algoritma lorentz (Ratna et al., 2021). *Logistic Map* merupakan algoritma yang ditemukan oleh ahli matematik Belgia bernama Pierre Francois Verhulst yang awalnya diterapkan untuk menghitung populasi maksimum masyarakat untuk sumber daya yang terbatas (Chen et al., 2021).

Peneliti Aesha Elghandour dan kawan – kawan (Elghandour et al., 2021) melakukan penelitian mengembangkan metode kriptografi citra digital dengan teknik konfusi dan difusi menggunakan algoritma *Logistic Map* sebagai konfusi dan *Two-Dimensional Piecewise Smooth nonlinier Chaotic Map* sebagai difusi. Hasil penelitian tersebut membukitkan keamanan algoritma dengan melalui beberapa analisis pengujian yaitu performa keamanan, analisis histogram dan noise.

Peneliti Parveiz Nazir Lone dan kawan-kawan (Lone et al., 2021) melakukan penelitian mengembangkan metode kriptografi menggunakan algoritma *Random Matrix Affine Cipher, Henon Map* dan Logistic Map. Hasil penelitian tersebut yaitu algoritma yang diusulkan diterapkan pada citra berwarna.

Peneliti Anak Agung Putri Ratna dan kawan-kawan (Ratna et al., 2021) melakukan penelitian mengembangkan metode kriptografi dengan menggunakan algoritma *Arnold's Cat Map* dan *Henon Map*. Teknik konfusi digunakan pada algoritma *Arnold's Cat Map* dan teknik difusi digunakan pada algoritma *Henon Map*. Hasil penelitian membuktikan bahwa teknik konfusi dan difusi dapat memberikan keamanan yang baik pada metode kriptografi citra digital.

Peneliti Shazia Sabir dan kawan-kawan (Sabir & Guleria, 2021) melakukan penelitian mengembangkan metode kriptografi citra digital menggunakan algoritma *Arnold's Cat Map*, *Reality Preserving Two Dimensional Discrete Fractional Hertley Transform* dan *Random Matrix Affine Cipher*. Hasil penelitian yaitu metode diterapkan pada enkripsi citra digital dengan *multi-layer* warna komponen RGB.

Peneliti Arwa Benlashram dan kawan-kawan (Benlashram et al., 2020) melakukan penelitian mengembangkan metode kriptografi citra digital menggunakan metode pengacakan piksel dan 3D *Chaotic Map*. Hasil penelitian menunjukkan performa keamanan dengan menggunakan parameter nilai korelasi,

entropi, NPCR (*Number of Pixel Change Rate*) dan UACI *(Unified Average Change Intensity*).

Dari uraian diatas dapat disimpulkan bahwa metode kriptografi citra digital berbasis *chaotic* dapat dikembangkan untuk meningkatkan performa keamanan. Penelitian ini mengusulkan pengembangan metode kriptografi citra digital dengan menggunakan kombinasi dari *Cat Map, Henon Map* dan *Logistic Map* menggunakan teknik konfusi dan difusi agar proses kriptografi dapat meningkatkan keamanan dengan melalui beberapa pengujian.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka dapat dirumuskan rumusan masalah sebagai berikut:

1. Bagaimana mengembangkan metode kriptografi citra digital berbasis *chaotic*?
2. Bagaimana hasil pengujian dari proses enkripsi dan dekripsi yang dilakukan?

1.3 Batasan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka dapat dirumuskan batasan masalah sebagai berikut:

1. Data yang digunakan merupakan citra digital *RGB* dan *Grayscale*.
2. Implementasi metode kriptografi pada citra digital menggunakan software Matlab
3. Analisis pengujian algoritma kriptografi citra digital

1.4 Tujuan Masalah

Sesuai dengan masalah penelitian yang telah diuraikan sebelumnya, maka tujuan yang ingin dicapai dalam penelitian ini adalah:

1. Menghasilkan pengembangan metode kriptografi citra digital berbasis *chaotic*.
2. Mengimplementasi rancangan pengembangan metode kriptografi citra digital berbasis *chaotic* dan melakukan pengujian.

1.5 Manfaat dan Kontribusi Penelitian

Hasil penelitian dari segi keilmuan akan memberikan kontribusi berupa pengembangan metode kriptografi citra digital berbasis *chaotic*. Hasil penelitian dari segi metode diusahakan untuk menemukan cara baru atau penambahan atau modifikasi dari metode proses kriptografi citra digital dengan memanfaatkan software Matlab. Hasil penelitian dari segi teknologi akan menghasilkan suatu rancangan metode kriptografi citra digital berbasis *chaotic* yang dapat membantu dan memudahkan pengguna dalam proses enkripsi dan dekripsi citra digital yang mengandung makna informasi rahasia.

BAB II

TINJAUAN PUSTAKA

Bab ini menguraikan tentang studi literatur terkait dengan kriptografi khususnya yang membahas penelitian-penelitian kriptografi pada citra digital berbasis *chaotic* yang telah dilakukan sejumlah peneliti.

2.1 Citra Digital

Citra atau gambar dapat representasikan secara matematika sebagai fungsi dengan 2 variabel x dan y (Dwivedi, 2017). Fungsi tersebut dituliskan sebagai f (x, y), dimana f adalah tingkat keabuan serta x dan y merupakan letak posisi piksel pada citra. Citra mempunyai ukuran M baris dan N kolom. Citra merupakan visual yang dapat dilihat oleh mata sebagai dasar persepsi sebuah objek. Citra juga dapat menjadi media untuk mendapatkan informasi dan mengirimkan informasi (Zhang et al., 2018).

Citra digital merupakan representasi gambar dua dimensi yang tampak pada monitor komputer. Citra digital dihasilkan dari proses digitalisasi dari citra analog. Pada citra digital terdapat nilai digital yang disebut dengan piksel yang menunjukkan intensitas warna. Kedalaman piksel dapat menunjukkan kedalaman warna yang biasa disebut dengan citra n-bit.

2.2 Jenis Citra Digital

Jenis citra berdasarkan kedalaman piksel yang menunjukkan intensitas warna piksel dapat dibedakan ke dalam beberapa jenis citra digital. Berikut beberapa jenis citra digital berdasarkan kedalaman warna atau kedalaman piksel n-bit.

1. Citra Biner

   Warna yang dimiliki citra biner adalah warna hitam atau putih. Memori yang digunakan untuk menyimpan kedua warna ini yaitu 1-bit. Setiap piksel dalam citra biner hanya memiliki nilai 0 atau 1 (Tyagi, 2018). Berikut contoh citra biner terdapat pada Gambar 2.1.

Gambar 2.1 Citra Biner

2. Citra *Grayscale*

   Citra *Greyscale* hanya memiliki 1 kanal pada setiap pikselnya. Derajat keabuan, intensitas warna putih atau tingkat intensitas cahaya direpresentasikan oleh setiap piksel pada citra *greyscale*. Citra grayscale pada umumnya memiliki kedalaman piksel 8 bit. Berikut contoh citra *grayscale* terdapat pada Gambar 2.2.

Gambar 2.2 Citra *Grayscale*

3. Citra Berwarna

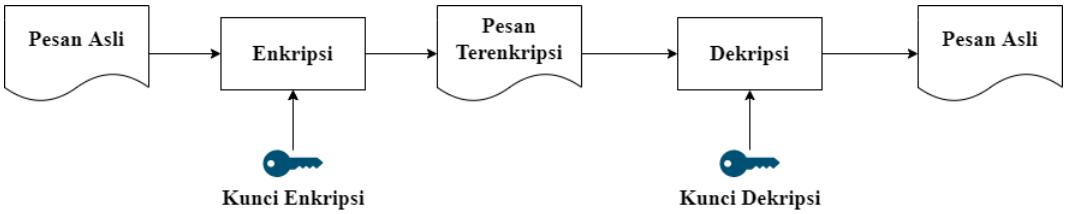
   Citra berwarna memiliki 3 kanal warna pada setiap pikselnya. Kanal warna pada citra berwarna yaitu *red, green* dan *blue* yang dikombinasikan dengan intensitas masing-masing mengisi 1 warna setiap piksel pada citra berwarna (Tyagi, 2018). Setiap kanal warna pada piksel citra berwarna diperlukan minimal 8-bit sehingga citra berwana memerlukan minimal 24-bit untuk setiap piksel yang digunakan. Contoh citra berwarna terdapat pada Gambar 2.3.

Gambar 2.3 Citra Berwarna

2.3 Kriptografi

Kriptografi merupakan metode atau teknik yang berfungsi untuk mentransformasi pesan atau data menjadi format yang tidak sah untuk membuat artinya menjadi tidak dipahami (untuk menyembunyikan maknanya), melindungi pesan dari perubahan tanpa izin atau penggunaan tidak sah (Hasan et al., 2021). Kriptografi menggunakan teknik matematika yang beragam untuk melindungi konten pada pesan terenkripsi (Joshi & Karkade, 2015). Kriptografi juga merupakan proses transformasi kembali data terenkripsi menjadi data yang dapat dipahami (Hutabarat, 2020).

Proses utama pada kriptografi terdiri dari proses enkripsi dan dekripsi. Proses enkripsi merupakan proses transformasi dari pesan asli menjadi pesan terenkripsi, sedangkan proses dekripsi merupakan proses transformasi kembali dari pesan terenkripsi menjadi pesan asli. Proses enkripsi dan dekripsi menggunakan kunci tertentu sehingga informasi pada pesan tidak dapat dipahami.



Gambar 2.4 Proses Enkripsi dan Dekripsi

Pada Gambar 2.4 merupakan gambar proses enkripsi dan dekripsi. Masukan pada proses enkripsi merupakan pesan asli dan kunci enkripsi. Hasil dari proses enkripsi merupakan pesan terenkripsi. Proses dekripsi akan mengembalikan pesan terenkripsi menjadi pesan asli dengan menggunakan kunci dekripsi.

Kriptografi dikelompokkan menjadi dua berdasarkan jenis kunci yaitu kriptografi simetris dan asimetris. Kunci yang digunakan untuk proses enkripsi dan dekripsi pada kriptografi simetris yaitu kunci privat. Kunci pada kriptografi simetris menggunakan kunci yang sama pada proses enkripsi dan dekripsi. Sedangkan, kunci yang digunakan pada kriptografi asimetris adalah kunci privat dan kunci publik. Proses komputasi pada kriptografi asimetris lebih intensif dari pada kriptografi simetris.

2.4 Kriptografi berbasis *Chaotic*

Sistem *chaotic* merupakan sistem dinamika nonliner yang menunjukkan gerakan acak dan kacau yang bergantung pada sensitivitas parameter awal. Sistem *Chaotic* menjelaskan aktivitas atau dinamika yang rumit dan tidak terduga tergantung pada kondisi awal sehingga penerapan sistem *chaotic* pada kriptografi akan meningkatkan kinerja metode kriptografi (Liu & Ko, 2021). Sistem *chaotic* dapat dinyatakan secara matematis karena sifatnya yang tidak teratur dilihat sebagai peristiwa yang acak mengikuti hukum-hukum yang berlaku di alam.

Sistem *chaotic* sensitif pada perubahan awal sehingga perbedaan kecil pada nilai awal fungsi akan menghasilkan perbedaan yang sangat besar pada nilai fungsi. Metode yang dikategorikan sebagai sistem *chaotic* merupakan metode yang dapat membangkitkan bilangan acak yang digunakan untuk kunci pada algoritma kriptografi.

2.4.1 Algoritma *Cat Map*

Cat Map merupakan metode *chaotic* ditemukan pada tahun 1960 oleh matematikawan Rusia bernama Vladimir Arnold. *Cat Map* dikategorikan sebagai metode *chaotic* karena sifat acak yang dimilikinya. Konsep dari *Cat Map* yaitu mengacak posisi piksel dalam suatu citra (Ratna et al., 2021). *Cat Map* merupakan algoritma yang mengacak citra berukuran persegi kemudia menyusunnya kembali ke ukuran yang sama.

Teknik konfusi pada *Cat Map* akan mengacak posisi piksel citra agar terlihat berbeda dari cira aslinya. Algoritma ini akan mengacak posisi piksel citra tanpa modifikasi nilai pikselnya. Proses enkripsi dan dekripsi *Cat Map* didefinisikan pada persamaan 2.1 dan 2.2

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} mod(N) \quad (2.1)$$

$$\begin{bmatrix} x_i \\ y_i \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}^{-1} \begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} mod(N) \quad (2.2)$$

Keterangan:

x_{i+1} dan y_{i+1} : posisi pixel baru *(*citra terenkripsi)

p dan q : kunci rahasia

x_i dan y_i : posisi pixel semula (citra asli)

N : ukuran citra N x N

Persamaan 2.1 merupakan proses enkripsi pada *Cat Map*. Citra awal dengan posisi piksel semula (x_i dan y_i) akan menjadi masukan pada proses enkripsi. Kunci p dan q merupakan bilangan bulat untuk melakukan proses enkripsi. Posisi piksel baru (x_{i+1} dan y_{i+1}) hasil dari proses enkripsi akan menjadi citra terenkripsi.

Persamaan 2.2 merupakan invers dari persamaan 2.1. Proses dekripsi akan mengembalikan posisi piksel citra terenkripsi menjadi posisi piksel pada citra semula. Kunci p dan q yang digunakan pada proses dekripsi merupakan kunci yang sama pada saat proses enkripsi. Kunci p dan q merupakan kunci bilangan bulat positif.

2.4.2 Algoritma *Henon Map*

Algoritma *Henon Map* merupakan metode *Chaotic* yang ditemukan oleh Michael Henon sebagai simplifikasi model dari model *Lorenz* (Ratna et al., 2021). *Henon Map* merupakan sistem dinamis yang mengimplementasikan sistem diskrit. Alogritma ini akan memetakan titik baru dari sebuah titik (x, y). Berikut persamaan *Henon Map* terdapat pada persamaan 2.3 dan 2.4

$$x_{n+1} = y_n + 1 - ax_n^2 \quad (2.3)$$

$$y_{n+1} = bx_n \quad (2.4)$$

Keterangan:

x_n dan y_n : posisi titik semula

x_{n+1} dan y_{n+1} : posisi titik baru

a dan b : kunci rahasia

Persamaan 2.3 dan 2.4 merupakan persamaan *Henon Map* yang akan mengubah titik awal (x_n, y_n) menjadi titik baru (x_{n+1}, y_{n+1}). Perubahan (x_n, y_n) yang terjadi pada kondisi awal akan mempengaruhi pemetaan titik baru yang terbentuk. Persamaan 2.3 dan 2.4 biasa digunakan untuk teknik difusi dengan membangkitkan bilangan acak atau mengubah nilai piksel pada citra (Ratna et al., 2021). *Henon* map

dapat juga digunakan untuk teknik konfusi (Lone et al., 2021). Berikut persamaan *Henon Map* dengan teknik konfusi pada proses enkripsi.

$$x_{i+1} = 1 - ax_i^2 + y_i \mod n \quad (2.5)$$

$$y_{i+1} = bx_i + c \mod n \quad (2.6)$$

Persamaan 2.5 dan 2.6 merupakan persamaan konfusi *Henon Map* untuk proses enkripsi. Dimana a, b dan c merupakan kunci rahasia, (x_i, y_i) merupakan posisi piksel awal, (x_{i+1}, y_{i+1}) posisi piksel baru, dan n merupakan ukuran citra. Berikut persamaan *Henon Map* dengan teknik konfusi pada proses dekripsi.

$$x_i = (y_{i+1} - c) / b \mod n \quad (2.7)$$

$$y_i = ax_i^2 + x_{i+1} - 1 \mod n \quad (2.8)$$

Persamaan 2.7 dan 2.8 merupakan invers dari persamaan 2.5 dan 2.6. Proses dekripsi akan mengembalikan posisi piksel baru menjadi posisi piksel awal dengan kunci yang sama pada saat proses enkripsi.

2.4.3 Algoritma *Logistic Map*

Alogritma *Logistic Map* merupakan metode *chaotic* dengan persamaan linier sederhana yang memiliki karakter non-periodik dan perilaku yang tidak terduga (Lone et al., 2021). *Logistic Map* tidak akan menghasilkan nilai-nilai acak yang berulang kembali. Berikut persamaan *Logistic Map* terdapat pada persamaan 2.9.

$$x_{n+1} = \mu \times x_n \times (1 - x_n) \quad (2.9)$$

Persamaan 2.9 merupakan persamaan *Logistic Map* untuk proses enkripsi dan dekripsi. Nilai x_0 menjadi nilai awal *chaotic* dan nilai μ menjadi kunci rahasia. Persamaan tersebut merupakan teknik difusi untuk membangkitkan bilangan acak yang akan memodifikasi nilai dari piksel pada citra.

2.5 Kajian Penelitian

Beberapa penelitian sebelumnya yang menjadi referensi penulis dalam melakukan penelitian ini, terutama penelitian tentang kriptografi berbasis *chaotic*. Berikut kajian penelitian disajikan pada tabel 2.1.

Tabel 2.1 Ringkasan Penelitian Kriptografi Berbasis *Chaotic*

Peneliti/Judul	**Metode**	**Hasil**	**Keterbatasan**
Parveiz Nazir Lone, Deep Singh dan Umar Hussain Mir, 2021. "A Novel Image Encryption using Random Matrix Affine Cipher and the chaotic Maps"	Kombinasi Random Matrix Affine Cipher (RMAC), Henon Map dan Logistic Map	Hasil dari metode yang diusulkan memiliki nilai entropi 7.9967, NPCR 99.24, UACI 33.38, HC 0, VC 0.0008 dan DC -0.0009	Citra uji yang digunakan hanya citra berwarna dengan ukuran 256x256
Anak Agung Putri Ratna dan kawan-kawan, 2021. "Chaos-Based Image Encryption Using Arnold's Cat Map Confussion and Henon Map Difusion"	Teknik konfusi dengan Arnold's Cat Map dan teknik difusi dengan Henon Map	Hasil dari metode yang diusulkan memiliki nilai HC 0.0039, VC -0.0003, DC -0.0005 dan nilai entropi 7.9503	Penelitian tidak melakukan pengujian nilai NPCR dan UACI
Shazia Sabir dan Vandana Guleria, 2021.	Kombinasi algoritma Random Matrix Affine Cipher	Citra diuji dengan nilai MSE, PSNR, Kofisien Korelasi,	Citra uji yang digunakan hanya

"Multi-Layer Color Image Encryption Using Random Matrix Affine Cipher, RP2DFrHT and 2D Arnold Map"	(RMAC), Reality Preserving Two Dimensional Discrete Fractional Hartley Transform (RP2DFrHT) dan 2D Arnold Map	Entropy pada 3 buah warna RGB pada citra	citra berwarna ukuran 512x512
Aesha Elghandour, Ahmad Salah dan Abdelrahman Karawia, 2021. "A New Cryptographic Algortihm via a Two-Dimensional Chaotic Map"	Teknik konfusi menggunakan Logistic Map dan teknik difusi menggunakan two-dimensional piecewise smooth nonlinier chaotic map (2DPSNCM)	Hasil dari metode yang diusulkan memiliki nilai NPCR 99.62 dan UACI 33.52. Nilai Korelasi HC -0.001, VC 0.0017 dan DC 0.0002. Nilai Entropi 7.9994	
Arwa Benlashram dan Kawan-kawan, 2020. "A Novel Approach of Image Encryption Using Pixel	Pengacakan piksel, Operasi XOR dan 3D Chaotic Map	Hasil dari metode yang diusulkan memiliki nilai Entropi 7.9901, nilai NPCR 99.66 dan UACI 33.67. Nilai koefisien HC -0.0127 dan VC -0.0242	Citra uji yang digunakan hanya citra *Greyscale* dengan ukuran 256x256

Shuffling and 3D Chaotic Map”			

Pada tabel 2.1 disajikan ringkasan penelitian berupa nama peneliti, judul artikel, metode, hasil penelitian dan keterbatasan. Hasil penelitian pada masing-masing artikel berupa hasil pengujian metode yang diusulkan peneliti. Pengujian tersebut menghasilkan nilai entropi, *number of pixel change rate* (NPCR), *unified average changing intensity* (UACI), *vertical correlation* (VC), *horizontal correlation* (HC), *diagonal correlation* (DC), *mean squre error* (MSE) dan *peak signal noise to ratio* (PSNR).

Peneliti (Lone et al., 2021), metode enkripsi dan dekripsi menggunakan kombinasi dari algoritma *Random RMAC, Henon Map* dan *Logistic Map* yang dilakukan hanya pada citra berwarna ukuran 256 x 256. Peneliti (Sabir & Guleria, 2021) juga melakukan penelitian hanya pada citra berwarna 512 x 512 menggunakan kombinasi algoritma *RMAC, RP2DfrHT* dan *Arnold Map*. Sedangkan, peneliti (Benlashram et al., 2020) melakukan penelitian hanya pada citra *Greyscale* dengan ukuran 256 x 256 menggunakan kombinasi pengacakan piksel, operasi XOR dan *3D Chaotic Map*.

Peneliti (Ratna et al., 2021) melakukan metode enkripsi dengan menggunakan kombinasi algoritma *Logistic Map* dan *2DPSNCM* dengan hasil penelitian berupa nilai korelasi dan entropi, tetapi tidak melakukan pengujian nilai UACI dan NPCR. Peneliti (Elghandour et al., 2021) melakukan enkripsi dengan kombinasi metode Logistic Map dan 2DPSNCM dengan hasil pengujian NPCR, UACI, korelasi dan Entropi.

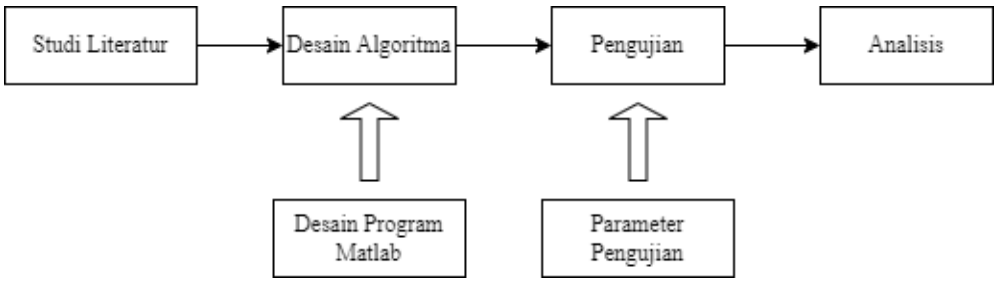
Dari beberapa penelitian tersebut maka pada penelitian ini dilakukan kriptografi berbasis *chaotic* menggunakan algoritma *Cat Map, Henon Map* dan *Logistic Map* pada citra digital *Grayscale* dan berwarna dengan melakukan beberapa pengujian dari hasil enkripsi dan dekripsi hasil proses metode algoritma yang diusulkan.

BAB III

METODOLOGI PENELITIAN

3.1 Tahapan Penelitian

Tahapan penelitian dibagi atas beberapa tahapan yang dilakukan dari awal sampai akhir. Tahapan dimulai dari studi literatur sampai analisis yang membentuk alur secara sistematis. Tahapan penelitian ini terpada pada Gambar 3.1

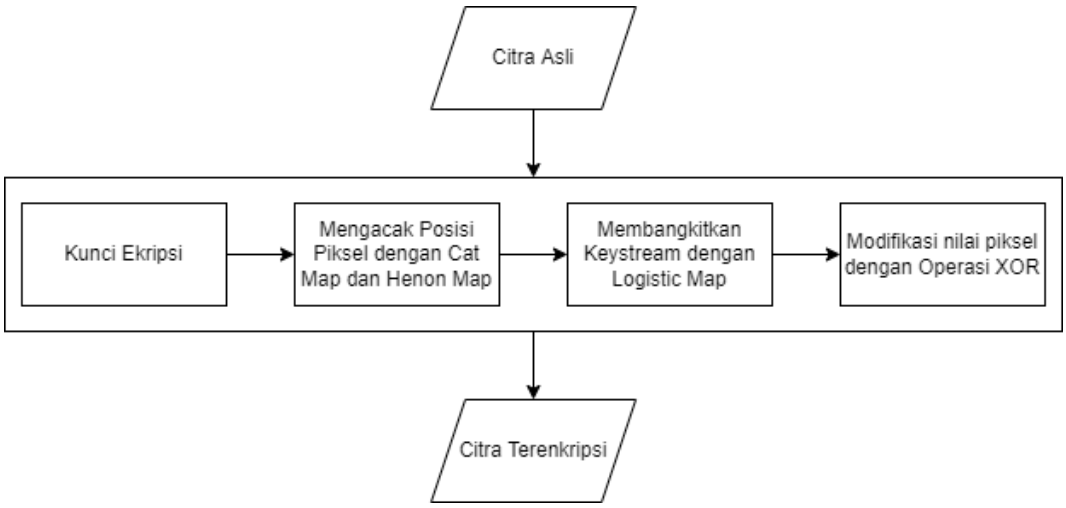


Gambar 3.1 Tahapan Penelitian

Tahapan penelitian pada Gambar 3.1 menjelaskan tahapan yang dilakukan pada penelitian ini. Tahapan pertama yaitu studi literatur dengan membaca dan memahami beberapa penelitian yang dilakukan oleh peneliti sebelumnya, kemudian desain algoritma dilakukan pada Matlab, pengujian dilakukan dengan beberapa parameter pengujian dan analisis dilakukan dari beberapa pengujian yang telah dilakukan.

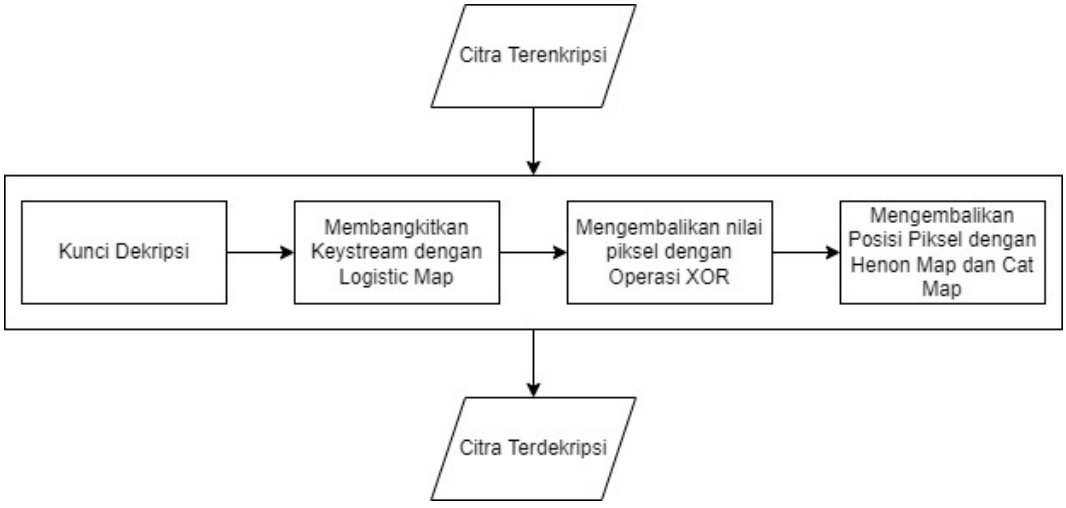
3.2 Desain Algoritma

Penelitian yang terdahulu menggunakan metode yang memiliki keamanan tinggi yang dibuktikan dengan beberapa parameter pengujian. Pada penelitian ini mengajukan pengembangan algoritma kriptografi citra digital dengan mengkombinasi teknik konfusi dengan algoritma *Cat Map* dan *Henon Map* serta teknik difusi dengan algoritma *Logistic Map*. Pengembangan pada algoritma ini diharapkan dapat memiliki keamanan yang lebih tinggi dengan melalui beberapa parameter pengujian. Diagram alur proses enkripsi dapat dilihat pada 3.2.



Gambar 3.2 Diagram Alur Proses Enkripsi

Gambar 3.2 merupakan diagram alur proses enkripsi yang diusulkan pada penelitian ini. Citra asli dan kunci enkripsi menjadi input pada proses enkripsi. Langkah pertama yaitu pengacakan piksel dilakukan dengan algoritma Cat Map menggunakan persamaan (2.1) dan algoritma Henon Map menggunakan persamaan (2.5) dan (2.6). Kemudian pembangkitan *keystream* dengan algoritma *Logistic Map* menggunakan persamaan (2.9). *Keystream* yang dibangkitkan akan dilakukan operasi XOR dengan piksel citra asli sehingga menghasilkan citra terenkripsi. Diagram alur proses dekripsi dapat dilihat pada Gambar 3.3



Gambar 3.3 Diagram Alur Proses Dekripsi

Gambar 3.3 merupakan diagram alur proses dekripsi yang diusulkan pada penelitian ini. Proses dekripsi merupakan kebalikan dari proses enkripsi. Citra terenkripsi dan kunci dekripsi menjadi input pada proses dekripsi. Kunci enkripsi dan dekripsi merupakan kunci yang sama. Langkah pertama yaitu pembangkitan *keystream* menggunakan *Logistic Map*. Kemudian pengembalian nilai piksel dengan operasi XOR. Pengembalian posisi piksel dengan algoritma *Henon map* menggunakan persamaan (2.7) dan (2.8) serta algoritma *Cat Map* menggunakan persamaan (2.2) sehingga menghasilkan citra asli kembali.

3.3 Pengujian

Tahapan pengujian dilakukan untuk mengetahui hasil pada proses enkripsi dan dekripsi beberapa pengujian yang dilakukan yaitu:

1. Histogram

   Histogram merupakan analisis statistik yang menunjukkan penyebaran atau distribusi piksel pada citra. Histogram sering digunakan untuk pada pengolahan citra untuk melihat kualitas citra. Kriptografi pada citra digital yang ideal memiliki distribusi nilai piksel yang beragam (Benlashram et al., 2020).

2. PSNR (*Peak Signal Noise to Ratio*)

   PSNR digunakan untuk pengukuran kualitas citra antara citra asli dan noise yang terjadi pada citra terenkripsi. Nilai PSNR ≥ 30 dB membuktikan kualitas yang baik pada citra asli atau citra terdekripsi (Lone et al., 2021). Berikut persamaan PSNR terdapat pada persamaan 3.1.

   $$PSNR = 10 \times log_{10} \frac{(255)^2}{MSE} \tag{3.1}$$

   Persamaan 3.1 merupakan persamaan untuk mencari nilai PSNR. Sebelum mencari nilai PSNR harus didapatkan nilai MSE terlebih dahulu. Berikut persamaan MSE (*Mean Square Error*) terdapat pada persamaan 3.2.

   $$MSE = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} (g'(x,y) - g(x,y))^2 \tag{3.2}$$

   Persamaan 3.2 terdapat g’ (x, y) dan g (x, y) yang merupakan citra terenkripsi dan citra asli atau citra terdekripsi. M dan N merupakan ukuran dari citra.

3. Korelasi

   Korelasi merupakan anlisis untuk mengukur teknik enkripsi pada kriptografi. Korelasi akan menunjukkan hubungan piksel yang berderkatan pada citra. Koefisien korelasi dapat dilihat secara vertikal, horizontal dan diagonal. Berikut persamaan korelasi terdapat pada persamaan 3.3 (Benlashram et al., 2020).

$$r_{xy} = \frac{Cov(x,y)}{\sqrt{D(x)D(y)}} \tag{3.3}$$

   Pada persamaan 3.3 terdapat r merupakan nilai korelasi. x dan y merupakan piksel yang berdekatan. Cov merupakan kovaransi. D merupakan deviasi. Nilai korelasi yang mendekati 0 menunjukkan kemanan yang baik pada citra terenkripsi (Lone et al., 2021).

4. NPCR dan UACI

   NPCR (*Number of Pixel Change Rate*) dan UACI *(Unified Average Changing Intensity*) merupakan parameter untuk menguji performa algoritma dalam enkripsi citra (Lone et al., 2021). NPCR digunakan untuk penghitungan banyaknya perbedaan piksel dari dua buah citra, sedangkan UACI digunakan untuk mengetahui interval perbedaan nilai piksel dari kedua citra. Berikut persamaan NPCR dan UACI terdapat pada persamaan 3.4 dan 3.5.

$$NPCR = \frac{1}{mn}\sum_{i,j} D(i,j) \times 100\% \tag{3.4}$$

$$UACI = \frac{1}{mn}\sum_{i,j} \frac{|C(i,j) - C'(i,j)|}{255} \times 100 \tag{3.5}$$

   Dimana

$$D(i,j) = \begin{cases} 1, jika\ C(i,j) \neq C'(i,j), \\ 0, jika\ C(i,j) = C'(i,j) \end{cases}$$

   Pada persamaan 3.4 dan 3.5 terdapat m dan n yang merupakan ukuran citra. C dan C’ merupakan dua citra terenkripsi dengan dua kunci yang berbeda. Nilai normal dari UACI yaitu 33.46% dan NPCR yaitu 99.60% (Lone et al., 2021).

5. Entropi

   Entropi digunakan untuk mengukur keacakan pada citra. Nilai entropi akan menunjukkan keacakan piksel pada citra terenkripsi (Elghandour et al., 2021). Berikut persamaan entropi terdapat pada persamaan 3.6.

$$H(m) = \sum_{i=0}^{255} P(m_i) log_2 \left(\frac{1}{P(m_i)}\right) \quad (3.6)$$

Pada persamaan 3.6 terdapat m yang merupakan citra yang digunakan. N merupakan nilai piksel pada citra dan P merupakan probabilitas yang terjadi pada citra. Citra terenkrpsi dengan nilai entropi yang mendekati 8 membuktikan keamanan yang baik pada citra terenkripsi (Lone et al., 2021).

3.4 Rencana Kerja

Rencana waktu penyelesaian penelitian ini selama 18 bulan, dengan detail rincian kerja terlihat pada tabel 3.1

Tabel 3.1. Rencana Pelaksanaan Penelitian.

BULAN KE / LANGKAH PENELITIAN	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Studi Pustaka																		
Menguji coba metode chaotic berdasarkan algoritma Cat Map, Henon Map dan Logistic Map																		
Mengevaluasi masing-masing metode yang sudah dihasilkan																		
Merancang metode pengembangan																		
Menguji coba metode pengembangan																		
Implementasi metode yang dikembangkan pada citra digital																		
Melakukan evaluasi metode yang dikembangkan																		

Rencana kerja akan dilakukan selama 18 bulan. Bulan 1 sampai 3 dilakukan studi pustaka. Bulan 3 sampai 6 dilakukan uji coba algoritma *Cat Map*, *Henon Map* dan *Logistic Map*. Bulan 4 sampai 8 dilakukan evaluasi masing-masing metode yang sudah dihasilkan. Bulan 7 sampai 11 perancangan metode pengembangan. Bulan 10 sampai 12 pengujian metode pengembangan. Bulan 12 sampai 15 implementasi metode yang dikembangkan pada citra digital di Matlab. Bulan 14 sampai 18 dilakukan evaluasi metode yang dikembangkan.

DAFTAR PUSTAKA

Benlashram, A., Al-ghamdi, M., Altalhi, R., & Kaouther, P. (2020). A novel approach of image encryption using pixel shuffling and 3D chaotic map A novel approach of image encryption using pixel shuffling and 3D chaotic map. *Journal of Physics: Conference Series*, *1447*. https://doi.org/10.1088/1742-6596/1447/1/012009

Chen, S., Feng, S., Fu, W., & Zhang, Y. (2021). Logistic map: Stability and entrance to chaos. *Journal of Physics: Conference Series*, *2014*(1), 0–14. https://doi.org/10.1088/1742-6596/2014/1/012009

Dwivedi, R. S. (2017). Digital Image Processing. In: Remote Sensing of Soils. In *Springer, Berlin, Heidelberg*. https://doi.org/10.1007/978-3-662-53740-4

Elghandour, A., Salah, A., & Karawia, A. (2021). A new cryptographic algorithm via a two-dimensional chaotic map. *Ain Shams Engineering Journal*. https://doi.org/10.1016/j.asej.2021.05.004

Hamza, Y. A. (2019). Highly Secure Image Steganography Approach Using Arnold's Cat Map and Maximum Image Entropy. *Proceedings of the International Conference on Information and Communication Technology*, 134–138. https://doi.org/10.1145/3321289.3321323

Hasan, M. K., Shafiq, M., Islam, S., Pandey, B., Baker El-Ebiary, Y. A., Nafi, N. S., Ciro Rodriguez, R., & Vargas, D. E. (2021). Lightweight Cryptographic Algorithms for Guessing Attack Protection in Complex Internet of Things Applications. *Complexity*, *2021*. https://doi.org/10.1155/2021/5540296

Hutabarat, J. A. (2020). Implementasi Kriptografi Hibrida Dan Steganografi Ihwt Dalam Pengamanan Data Teks. *Jurnal Pelita Informatika*, *8*(3), 340–343.

Joshi, M. R., & Karkade, R. A. (2015). Network Security with Cryptography. *International Journal of Computer Science and Mobile Computing*.

Liu, Y., & Ko, Y. C. (2021). Image Processing Method Based on Chaotic Encryption and Wavelet Transform for Planar Design. *Advances in Mathematical Physics*, *2021*. https://doi.org/10.1155/2021/7511245

Lone, P. N., Singh, D., & Mir, U. H. (2021). A novel image encryption using

random matrix affine cipher and the chaotic maps. *Journal of Modern Optics*, *68*(10), 507–521. https://doi.org/10.1080/09500340.2021.1924885

Ratna, A. A. P., Surya, F. T., Husna, D., Purnama, I. K. E., Nurtanio, I., Hidayati, A. N., Purnomo, M. H., Nugroho, S. M. S., & Rachmadi, R. F. (2021). Chaos-based image encryption using Arnold's cat map confusion and Henon map diffusion. *Advances in Science, Technology and Engineering Systems*, *6*(1), 316–326. https://doi.org/10.25046/aj060136

Sabir, S., & Guleria, V. (2021). Multi-layer color image encryption using random matrix affine cipher , RP2DFrHT and 2D Arnold map. *Multimedia Tools and Applications*, *80*, 27829–27853. https://doi.org/10.1007/s11042-021-11003-x

Tyagi, V. (2018). Understanding Digital Image Processing. In *CRC Press*. https://doi.org/10.1201/9781315123905

Zhang, L., Zhang, L., & Zhang, L. (2018). Application Research of Digital Media Image Processing Technology Based on Wavelet Transform. *J Image Video Proc*, *138*(2018). https://doi.org/10.1186/s13640-018-0383-6