PENGEMBANGAN KRIPTOGRAFI PADA CITRA DIGITAL BERBASIS CHAOTIC MAP

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?

1.4 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.

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.

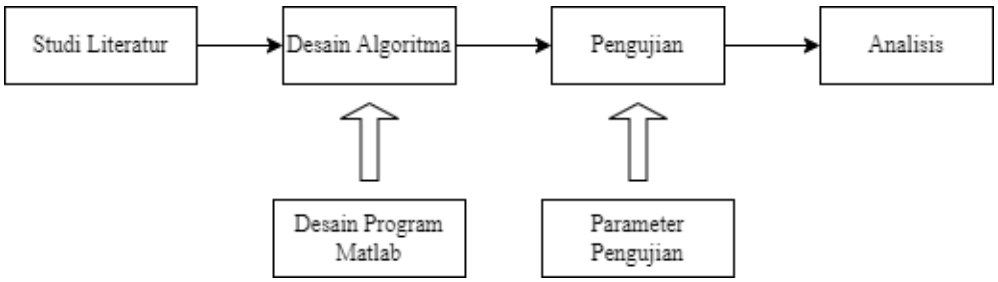
Dari beberapa penelitian tersebut maka pada penelitian ini dilakukan kriptografi berbasis *chaotic* menggunakan algoritma *Cat Map, Henon Map* dan *Logistic Map* pada citra digital *Grayscale* dan berwarna dengan melakukan beberapa pengujian dari hasil enkripsi dan dekripsi hasil proses metode algoritma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

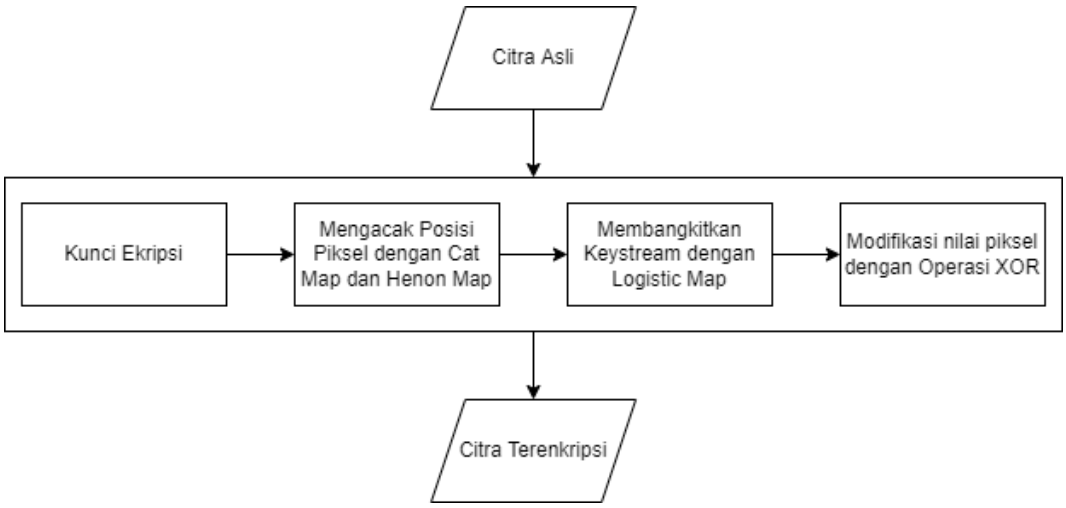


Gambar 3.1 Tahapan Penelitian

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.

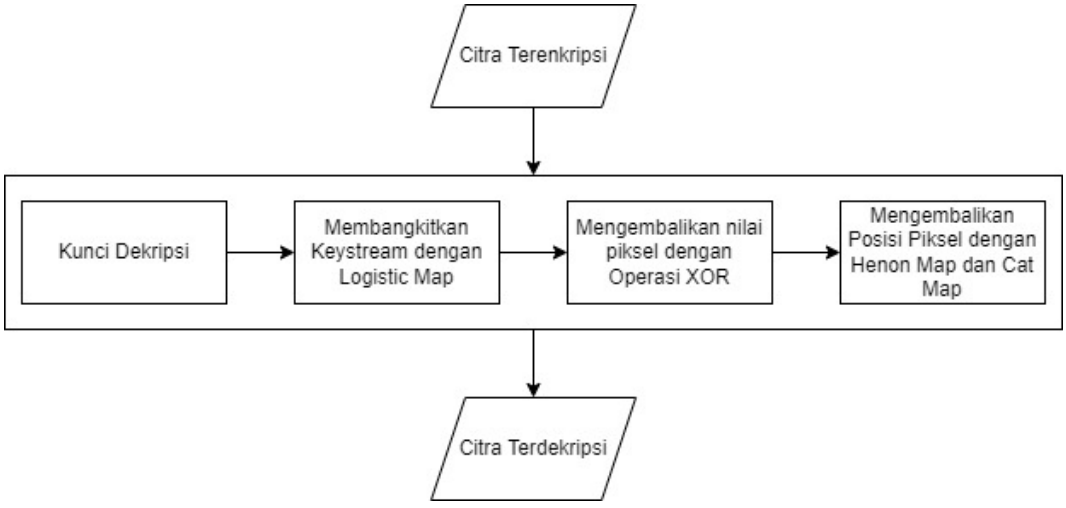
3.2 Desain Algoritma

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).