BAB II

LANDASAN TEORI

2.1 Citra Digital

Citra digital merupakan representasi visual suatu objek atau pemandangan yang disimpan dalam bentuk data numerik dan tersusun atas elemen-elemen kecil yang disebut piksel. Setiap piksel memiliki nilai yang merepresentasikan intensitas cahaya pada citra keabuan atau kombinasi kanal warna merah (R), hijau (G), dan biru (B) pada citra berwarna. Secara matematis, citra digital dimodelkan sebagai fungsi dua dimensi $I(x, y)$dengan nilai diskrit dalam rentang tertentu, misalnya 0–255 pada representasi 8-bit, sehingga memungkinkan citra diproses, dianalisis, disimpan, dan ditransmisikan menggunakan sistem komputasi digital (Alghamdi & Munir, 2024; Zia dkk., 2022).

Perbedaan utama antara citra analog dan citra digital terletak pada bentuk representasi datanya. Citra analog bersifat kontinu, sedangkan citra digital diperoleh melalui proses sampling dan kuantisasi sehingga dapat diproses secara matematis oleh komputer (Makarichev dkk., 2022; Neuhaus dkk., 2021). Dalam konteks keamanan informasi, citra digital sering digunakan sebagai media penyimpanan dan pertukaran informasi sensitif, sehingga rentan terhadap ancaman seperti penyadapan, manipulasi, dan pemalsuan data. Untuk itu, dikembangkan berbagai mekanisme pengamanan, seperti enkripsi citra, *watermarking digital*, dan forensik citra, di mana enkripsi citra bertujuan menjaga kerahasiaan dan integritas data selama penyimpanan maupun transmisi (Ye dkk., 2025).

2.2 Kompresi Citra Digital

Kompresi citra digital merupakan proses untuk mengurangi jumlah data yang diperlukan dalam merepresentasikan suatu citra guna meningkatkan efisiensi penyimpanan dan transmisi. Secara umum, teknik kompresi citra dibedakan menjadi kompresi *lossless* dan *lossy*. Kompresi *lossless* mempertahankan seluruh informasi citra asli sehingga hasil dekompresi identik dengan citra semula, sedangkan kompresi *lossy* menghilangkan sebagian informasi yang dianggap kurang penting secara visual untuk mencapai rasio kompresi yang lebih tinggi (Huang & Wu, 2024). Dalam sistem multimedia modern, kompresi *lossy* lebih banyak digunakan karena mampu menekan ukuran data secara signifikan dengan kualitas visual yang masih dapat diterima, meskipun proses kuantisasi dan reduksi redundansi data dapat mengubah struktur serta karakteristik statistik citra, seperti distribusi intensitas dan korelasi antar-piksel (Urbaniak, 2024).

Perubahan statistik piksel akibat kompresi *lossy* menjadi aspek penting dalam penelitian enkripsi citra, karena proses kompresi dapat bertindak sebagai bentuk gangguan terhadap data terenkripsi dan berpotensi memengaruhi kualitas citra hasil dekripsi serta keamanan algoritma enkripsi yang ditinjau dari ketahanannya terhadap analisis statistik dan serangan berbasis perbedaan (C.-H. Huang & Wu, 2024). Beberapa format kompresi *lossy* yang umum digunakan antara lain JPEG, JPEG 2000, WebP, HEIC, dan AVIF, yang masing-masing memiliki karakteristik berbeda dalam mengurangi redundansi dan memengaruhi struktur citra. JPEG dikenal luas namun cenderung menimbulkan artefak pada rasio kompresi tinggi, sedangkan JPEG 2000 menawarkan kualitas yang lebih stabil. Format WebP, HEIC,

dan AVIF memberikan efisiensi kompresi yang lebih tinggi, tetapi juga menyebabkan perubahan statistik citra yang lebih kompleks, sehingga menimbulkan tantangan tambahan bagi algoritma enkripsi citra dalam mempertahankan kualitas hasil dekripsi (Dornauer & Felderer, 2024; Göring dkk., 2023; C.-H. Huang & Wu, 2024; Urbaniak, 2024).

2.3 Kriptografi Citra

Kriptografi citra merupakan cabang dari kriptografi yang berfokus pada perlindungan data dalam bentuk citra digital agar informasi visual di dalamnya tidak dapat diakses atau dipahami oleh pihak yang tidak berwenang. Berbeda dengan citra biasa yang dapat langsung ditafsirkan secara visual, citra terenkripsi diubah menjadi bentuk acak yang tidak memiliki makna visual tanpa proses dekripsi menggunakan kunci yang sesuai. Tujuan utama kriptografi citra adalah menjaga kerahasiaan, integritas, dan keamanan citra selama proses penyimpanan maupun transmisi pada sistem multimedia dan jaringan terbuka (Alghamdi & Munir, 2024).

Perlu ditegaskan bahwa istilah “aman” atau “keamanan” yang digunakan sepanjang penelitian ini merujuk pada definisi operasional yang terbatas pada aspek kerahasiaan visual *(visual confidentiality*) citra, bukan pada keseluruhan aspek keamanan informasi secara umum. (SaberiKamarposhti dkk., 2024) menegaskan bahwa keamanan citra digital secara luas mencakup tiga dimensi, yaitu *confidentiality, integrity*, dan *privacy* dari konten visual, sehingga aspek integritas data, *autentikasi* pengirim, *non-repudiasi*, maupun ketahanan terhadap serangan pada level protokol atau saluran komunikasi berada di luar cakupan dimensi

confidentiality yang menjadi fokus penelitian ini. Secara operasional, suatu hasil enkripsi pada penelitian ini dikategorikan "aman" apabila memenuhi dua syarat: (1) *ciphertext* yang dihasilkan tampak acak secara visual dan statistik sehingga tidak dapat dikenali atau ditafsirkan sebagai citra asli oleh pihak yang tidak memiliki kunci, yang pada penelitian ini diukur melalui metrik entropi, korelasi piksel, NPCR, dan UACI; dan (2) citra asli tetap dapat direkonstruksi kembali secara benar oleh pihak yang memiliki kunci yang sesuai melalui proses dekripsi. Dengan demikian, ruang lingkup keamanan yang dievaluasi pada penelitian ini dibatasi pada ketahanan *ciphertext* terhadap analisis statistik dasar (*statistical cryptanalysis*) sebagaimana direpresentasikan oleh keempat metrik tersebut, dan tidak mencakup pengujian terhadap serangan kriptografi lanjutan seperti *chosen-plaintext attack*, *differential attack* menyeluruh, maupun *brute-force* terhadap ruang kunci, yang berada di luar batasan masalah penelitian ini.

Secara konseptual, kriptografi citra memiliki perbedaan mendasar dibandingkan kriptografi teks, karena citra digital direpresentasikan dalam bentuk dua dimensi atau lebih, memiliki ukuran data yang besar, serta menunjukkan korelasi yang kuat antar-piksel, terutama pada citra berwarna. Karakteristik ini menyebabkan algoritma kriptografi konvensional yang dirancang untuk teks menjadi kurang efisien apabila diterapkan secara langsung pada citra digital tanpa penyesuaian tertentu (B. Zhang & Liu, 2023).

Dalam perancangannya, kriptografi citra mengacu pada dua prinsip dasar yang diperkenalkan oleh Shannon, yaitu konfusi (*confusion*) dan difusi (*diffusion*). Konfusi bertujuan untuk menyamarkan hubungan antara kunci enkripsi dan

ciphertext sehingga pola statistik citra asli tidak dapat dikenali dari citra terenkripsi. Pada citra digital, konfusi umumnya diwujudkan melalui proses pengacakan posisi atau nilai piksel. Sementara itu, difusi bertujuan untuk menyebarkan pengaruh perubahan kecil pada satu piksel citra asli ke banyak piksel pada citra terenkripsi, sehingga perubahan kecil pada *plaintext* menghasilkan perubahan besar pada *ciphertext*. Penerapan kedua prinsip ini penting untuk meningkatkan tingkat keamanan dan ketahanan citra terenkripsi terhadap analisis statistik dan serangan kriptanalisis (Alghamdi & Munir, 2024; Zhang & Liu, 2023).

Salah satu pendekatan yang banyak digunakan dalam kriptografi citra adalah enkripsi citra berbasis ruang spasial. Pendekatan ini bekerja secara langsung pada nilai dan posisi piksel tanpa melakukan transformasi ke domain lain, seperti domain frekuensi. Enkripsi berbasis ruang spasial umumnya terdiri dari dua tahap utama, yaitu permutasi piksel untuk mencapai konfusi dan difusi nilai piksel untuk meningkatkan sensitivitas terhadap perubahan data. Pendekatan ini dinilai lebih sederhana secara implementasi dan efisien secara komputasi, sehingga banyak digunakan dalam penelitian enkripsi citra, khususnya yang dikombinasikan dengan sistem *chaos* untuk meningkatkan tingkat keacakan dan keamanan citra terenkripsi (Mahalakshmi & Nagarajan, 2025).

2.4 Teori Chaos

2.4.1 Sistem Chaos

Sistem *chaos* merupakan sistem dinamis nonlinier yang bersifat deterministik namun menunjukkan perilaku yang tampak acak dan sulit diprediksi dalam jangka panjang. Meskipun dinamika sistem sepenuhnya ditentukan oleh persamaan

matematis dan parameter tertentu, keluaran sistem sangat sensitif terhadap kondisi awal yang digunakan. Karakteristik ini menyebabkan sistem *chaos* mampu menghasilkan deret nilai yang menyerupai bilangan acak, meskipun tidak berasal dari proses acak murni.

Dalam konteks kriptografi citra, sistem *chaos* banyak dipilih sebagai dasar perancangan algoritma enkripsi karena karakteristiknya yang secara alami sesuai dengan kebutuhan keamanan citra digital. Menurut (B. Zhang & Liu, 2023), sistem *chaos* memiliki sifat sensitivitas tinggi terhadap kondisi awal, *pseudo-randomness*, dan *ergodicity* yang menjadikannya sumber kriptografis yang efektif untuk enkripsi citra. Sifat-sifat tersebut memungkinkan sistem *chaos* menghasilkan deret bilangan yang sulit diprediksi dan memiliki distribusi statistik mendekati *uniform*, sehingga efektif dalam menghilangkan korelasi antar-piksel pada citra digital.

Selain itu, (Hamadi & Emad A. Mohammed, 2024) menegaskan bahwa sistem *chaos*, seperti *Logistic Map, Henon Map, dan sistem Lorenz,* banyak digunakan dalam enkripsi citra karena kemampuannya dalam melakukan permutasi posisi piksel dan difusi nilai intensitas secara sensitif terhadap perubahan parameter awal. Sensitivitas ini menjamin bahwa perubahan sangat kecil pada kunci atau kondisi awal akan menghasilkan *ciphertext* yang sangat berbeda, sehingga meningkatkan ketahanan algoritma terhadap serangan *brute force* dan analisis diferensial.

Dengan demikian, pemilihan sistem *chaos* dalam penelitian enkripsi citra tidak hanya didasarkan pada sifat matematisnya, tetapi juga didukung oleh hasil-

hasil penelitian terkini yang menunjukkan bahwa karakteristik chaos sangat efektif dalam memenuhi prinsip konfusi dan difusi pada kriptografi citra digital.

2.4.2 Sistem Chaos 4D

Sistem *chaos* empat dimensi (4D) merupakan pengembangan dari sistem *chaos* berdimensi lebih rendah yang termasuk dalam kategori *hyperchaotic*. Sistem ini merupakan sistem dinamis nonlinier kontinu yang direpresentasikan oleh empat variabel keadaan yang saling berinteraksi melalui persamaan diferensial. Berbeda dengan sistem *chaos* konvensional yang umumnya hanya memiliki satu eksponen Lyapunov positif, sistem *hyperchaotic* memiliki dua atau lebih eksponen Lyapunov positif yang menunjukkan tingkat kompleksitas dinamika yang lebih tinggi (Liu dkk., 2022).

Peningkatan dimensi pada sistem *chaos* 4D menyebabkan interaksi antar variabel menjadi lebih kompleks serta menghasilkan ruang keadaan yang lebih luas dibandingkan sistem berdimensi lebih rendah. Hal ini berdampak pada peningkatan kompleksitas lintasan fase dan memperluas ruang kunci yang dapat digunakan dalam proses enkripsi.

Dalam konteks kriptografi citra, karakteristik tersebut menjadikan sistem *chaos* 4D lebih unggul karena mampu menghasilkan deret bilangan pseudo-acak dengan tingkat kompleksitas yang lebih tinggi. Selain itu, distribusi keluaran yang mendekati *uniform* serta sensitivitas tinggi terhadap parameter awal memberikan kontribusi dalam meningkatkan ketahanan terhadap berbagai serangan kriptanalisis, seperti *brute force* dan analisis statistik (Alexan dkk., 2023; Geng dkk., 2025; Shakir dkk., 2023).

2.4.3 Algoritma 4D

Algoritma *chaos* 4D merupakan implementasi dari sistem dinamis nonlinier berdimensi empat yang digunakan untuk menghasilkan deret bilangan *pseudo-random* dengan tingkat kompleksitas tinggi. Sistem ini termasuk dalam kategori *hyperchaotic*, yaitu sistem *chaos* yang memiliki lebih dari satu eksponen Lyapunov positif, sehingga mampu menghasilkan dinamika yang lebih kompleks dibandingkan sistem *chaos* berdimensi rendah. Kompleksitas tersebut berdampak pada meningkatnya sensitivitas terhadap kondisi awal dan parameter sistem, serta memperluas ruang kunci yang dapat dimanfaatkan dalam aplikasi kriptografi (Ding & Ding, 2020).

Dalam konteks enkripsi citra digital, algoritma *chaos* 4D banyak digunakan sebagai pembangkit *keystream* pada tahap permutasi dan difusi piksel. Deret *pseudo-random* yang dihasilkan memiliki karakteristik statistik yang baik, seperti distribusi yang mendekati acak dan korelasi yang rendah, sehingga efektif dalam mengurangi keterkaitan antar piksel pada citra terenkripsi. Selain itu, sensitivitas tinggi terhadap kondisi awal menyebabkan perubahan kecil pada parameter menghasilkan perbedaan signifikan pada hasil enkripsi, sehingga meningkatkan ketahanan terhadap berbagai serangan kriptanalisis, termasuk serangan statistik dan diferensial (Al-Dayel dkk., 2025).

Berbagai penelitian telah mengembangkan skema enkripsi citra berbasis sistem *hyperchaotic* dengan mengombinasikan beberapa peta *chaos* atau memperluas dimensi sistem untuk meningkatkan kompleksitas dan keamanan. Selain itu, dalam literatur dikenal beberapa pengembangan sistem *chaos* klasik ke

dalam bentuk empat dimensi, seperti varian sistem Chen, Lorenz, Lü, dan Rössler yang dimodifikasi menjadi sistem *hyperchaotic*. Perbedaan struktur dan parameter pada masing-masing sistem menghasilkan karakteristik dinamika yang berbeda, yang berpengaruh terhadap performa enkripsi citra.

Pemanfaatan algoritma *chaos* 4D dalam penelitian ini didasarkan pada kemampuannya menghasilkan *keystream* yang kompleks, sensitivitas tinggi terhadap kondisi awal, serta karakteristik statistik yang mendukung peningkatan keamanan sistem enkripsi citra digital.

2.4.3.1 Chen 4D

Sistem Chen 4D merupakan salah satu sistem *hyperchaotic* yang digunakan dalam enkripsi citra digital karena memiliki dinamika yang kompleks dan sensitivitas tinggi terhadap kondisi awal. Sistem ini merupakan pengembangan dari sistem Chen tiga dimensi dengan penambahan satu variabel keadaan, sehingga menghasilkan perilaku yang lebih kompleks dibandingkan sistem *chaos* berdimensi rendah (Hosny dkk., 2022).

Secara matematis, sistem Chen 4D dinyatakan dalam bentuk persamaan diferensial nonlinier sebagai berikut (Hosny dkk., 2022):

$$\begin{aligned} \dot{x} &= a(y - x) + w \\ \dot{y} &= dx + cy - xz \\ \dot{z} &= xy - bz \\ \dot{w} &= yz + rw \end{aligned} \tag{1}$$

dengan x, y, z, w sebagai variabel keadaan, serta a, b, c, d, dan r sebagai parameter kontrol sistem.

Dalam penelitian ini digunakan parameter a = 35, b = 3, c = 12, d = 7, dan r = 0,5. Pemilihan parameter tersebut didasarkan pada nilai yang telah divalidasi dalam literatur untuk menghasilkan kondisi *hyperchaotic*, yang ditandai dengan adanya lebih dari satu eksponen Lyapunov positif serta sensitivitas tinggi terhadap kondisi awal. Kondisi ini memungkinkan sistem menghasilkan deret *pseudo-random* dengan tingkat kompleksitas tinggi, sehingga sesuai untuk digunakan sebagai pembangkit *keystream* dalam proses enkripsi citra (Hosny dkk., 2022).

Dalam implementasinya, sistem Chen 4D digunakan untuk menghasilkan deret bilangan *pseudo-random* yang berperan dalam proses permutasi dan difusi piksel. Karakteristik dinamika yang kompleks dan sensitivitas terhadap kondisi awal memungkinkan peningkatan keamanan citra terenkripsi melalui pengurangan korelasi antar piksel dan peningkatan tingkat keacakan data (Hosny dkk., 2022).

Keunggulan sistem Chen 4D yang banyak dilaporkan dalam literatur terletak pada kemampuannya menghasilkan *ciphertext* dengan tingkat keacakan (entropi) yang sangat tinggi serta ketahanan terhadap serangan statistik. Alexan dkk. (2023) melaporkan bahwa skema enkripsi berbasis Chen 4D berorde fraksional mampu menghasilkan nilai entropi sebesar 7,997, sangat mendekati nilai ideal 8 bit. Y. Huang dkk. (2022) juga menunjukkan bahwa sistem *hyperchaotic* Chen dengan skema dua tahap *scrambling-diffusion* tahan terhadap *chosen-plaintext attack*, sementara Hosny dkk. (2022) mengevaluasi ketahanan Chen 4D terhadap *noise attack* dan *data-cut attack* dengan hasil yang konsisten baik. Karakteristik ini menunjukkan bahwa keunggulan utama Chen 4D berada pada aspek keacakan statistik dan ketahanan terhadap gangguan pada *ciphertext*.

2.4.3.2 Lorenz 4D

Sistem Lorenz 4D merupakan salah satu sistem *hyperchaotic* yang paling banyak dikaji dan diaplikasikan dalam bidang enkripsi citra digital. Sistem ini dikembangkan dari sistem Lorenz tiga dimensi klasik yang pertama kali diperkenalkan oleh Edward Lorenz pada tahun 1963 ketika memodelkan fenomena konveksi atmosfer. Pengembangan ke dimensi keempat dilakukan dengan menambahkan sebuah variabel keadaan baru beserta sebuah pengontrol umpan balik (*feedback controller*), sehingga menghasilkan perilaku *hyperchaotic* yang jauh lebih kompleks dibanding sistem aslinya (Lin & Li, 2021).

Secara matematis, sistem Lorenz 4D dinyatakan dalam bentuk persamaan diferensial nonlinier berikut (Lin & Li, 2021):

$$\begin{aligned} \dot{x} &= \sigma(y - x) + w \\ \dot{y} &= \rho x - xz - y \\ \dot{z} &= xy - \beta z \\ \dot{w} &= -yz + rw \end{aligned} \tag{2}$$

dengan x, y, z, w sebagai variabel keadaan dan σ, ρ, β, r sebagai parameter kontrol sistem.

Dalam penelitian ini digunakan parameter σ = 10, ρ = 28, β = 8/3, dan r = −1. Pemilihan parameter tersebut mengacu pada nilai yang telah diverifikasi secara eksperimental dalam literatur, di mana sistem terbukti menunjukkan perilaku *hyperchaotic* yang ditandai oleh dua eksponen Lyapunov bernilai positif secara bersamaan, yaitu λ_1 = 0,3381 dan λ_2 = 0,1586, sedangkan λ_3 = 0 dan λ_4 = −15,1752 (Lin & Li, 2021). Kondisi ini memenuhi syarat suatu sistem disebut *hyperchaotic*,

yaitu harus memiliki ruang fase berdimensi minimal empat dan memiliki setidaknya dua eksponen Lyapunov positif.

Keunggulan utama sistem Lorenz 4D dibanding sistem chaos berdimensi rendah terletak pada kompleksitas dinamikanya yang jauh lebih tinggi. Penambahan dimensi keempat memperluas ruang kunci secara signifikan dan meningkatkan sifat pseudo-acak dari deret yang dihasilkan. Dalam implementasinya, deret bilangan *pseudo-random* yang dihasilkan sistem ini digunakan dalam proses permutasi posisi piksel sekaligus difusi nilai piksel, yang secara efektif dapat mengurangi korelasi antar piksel dan meningkatkan tingkat keacakan citra terenkripsi (Lin & Li, 2021).

Keunggulan sistem Lorenz 4D yang paling menonjol dalam literatur terletak pada sensitivitasnya terhadap perubahan kecil pada *plaintext*, yang tercermin dari performa NPCR dan UACI yang konsisten mendekati nilai ideal. T. Li & Zhang (2021) melaporkan bahwa skema *hyperchaotic* berbasis Lorenz dengan *multiple bit permutation and diffusion (MBPD)* berhasil lulus pengujian korelasi, entropi, NPCR, dan UACI pada seluruh 16 citra uji yang digunakan. Zhang dkk. (2024) turut mengonfirmasi hal serupa melalui skema Lorenz termodifikasi dengan permutasi berbasis *image pyramid* dan difusi Galois field, yang mencatatkan performa unggul pada korelasi piksel, NPCR, dan UACI. Selain itu, W. Zhang dkk. (2025) menunjukkan bahwa Lorenz 4D mampu mempertahankan keamanan yang baik sekalipun dievaluasi dalam skenario kompresi JPEG. Temuan-temuan ini menegaskan bahwa Lorenz 4D secara konsisten unggul pada aspek sensitivitas

terhadap perubahan piksel, yang menjadi dasar kuat pada metrik korelasi, NPCR, dan UACI.

2.4.3.3 Lü 4D

Sistem Lü 4D merupakan sistem *hyperchaotic* empat dimensi yang dikembangkan dari sistem Lü tiga dimensi, yaitu sebuah sistem chaos yang pertama kali diperkenalkan oleh Lü dan Chen pada tahun 2002 sebagai jembatan transisi antara sistem Lorenz dan sistem Chen. Sistem 3D tersebut kemudian diperluas ke dimensi keempat dengan menambahkan variabel keadaan baru melalui sebuah *state feedback controller*, sehingga menghasilkan *attractor hyperchaotic* dengan dua eksponen Lyapunov positif secara bersamaan (Chen dkk., 2006).

$$\begin{aligned} \dot{x} &= a(y - x) \\ \dot{y} &= -xz + cy + w \\ \dot{z} &= xy - bz \\ \dot{w} &= -dx \end{aligned} \tag{3}$$

dengan x, y, z, w sebagai variabel keadaan dan a, b, c, d sebagai parameter kontrol sistem.

Dalam penelitian ini digunakan parameter a = 36, b = 3, c = 20, dan d = 1. Nilai-nilai tersebut mengikuti rentang parameter yang telah diverifikasi dalam literatur, yaitu ketika a = 36, b = 3, c = 20, dan $-0{,}35 < d \leq 1{,}30$, sistem Lü 4D menunjukkan perilaku *hyperchaotic* yang ditandai dengan kehadiran dua eksponen Lyapunov positif (Chen dkk., 2006). Salah satu karakteristik menarik dari sistem Lü 4D adalah hanya memiliki satu titik ekuilibrium di titik asal (0, 0, 0, 0), yang

menjadikan struktur sistemnya relatif sederhana namun tetap menghasilkan dinamika yang sangat kompleks dan tidak periodik.

Dalam konteks enkripsi citra, deret bilangan *pseudo-random* yang dihasilkan sistem Lü 4D dimanfaatkan dalam proses permutasi posisi piksel dan difusi nilai piksel. Sensitivitas ekstrem terhadap kondisi awal dan kompleksitas *attractor* yang dihasilkan menjadikan sistem ini cocok sebagai pembangkit *keystream* yang sulit diprediksi (Chen dkk., 2006).

Keunggulan sistem Lü 4D terletak pada kesederhanaan struktur persamaannya dibandingkan sistem *hyperchaotic* lain. Chen dkk. (2006) menjelaskan bahwa sistem ini hanya memiliki satu titik ekuilibrium di titik asal dan jumlah suku non-linier yang lebih sedikit, namun tetap mampu menghasilkan dinamika *hyperchaotic* dengan dua eksponen Lyapunov positif. Kesederhanaan struktural ini secara teoritis berimplikasi pada beban komputasi yang lebih ringan dalam proses pembangkitan *chaos sequence*, karena jumlah operasi perkalian dan penjumlahan non-linier pada persamaan diferensialnya lebih sedikit dibandingkan Chen 4D maupun Lorenz 4D. Dengan demikian, keunggulan utama Lü 4D berada pada efisiensi struktural yang berpotensi meningkatkan kecepatan komputasi tanpa mengurangi kompleksitas dinamika yang dihasilkan.

2.4.3.4 Rössler 4D

Sistem Rössler 4D merupakan sistem *hyperchaotic* pertama yang pernah diperkenalkan dalam sejarah teori *chaos*. Sistem ini diusulkan oleh Otto E. Rössler pada tahun 1979 melalui makalahnya yang berjudul "*An Equation for Hyperchaos*", dan sejak saat itu menjadi sistem acuan penting dalam studi dinamika nonlinear.

Berbeda dengan sistem chaos tiga dimensi yang hanya memiliki satu eksponen Lyapunov positif, Rössler sengaja merancang sistem empat dimensi ini untuk menunjukkan bahwa perilaku *hyperchaotic* memang dapat eksis dalam sistem otonom kontinu (Yi & Cao, 2024).

Secara matematis, sistem Rössler 4D dinyatakan dalam persamaan diferensial nonlinier berikut (Yi & Cao, 2024):

$$\begin{aligned} \dot{x} &= -y - z \\ \dot{y} &= x + ay + w \\ \dot{z} &= b + xz \\ \dot{w} &= -cz + dw \end{aligned} \tag{4}$$

dengan x, y, z, w sebagai variabel keadaan dan a, b, c, d sebagai parameter kontrol sistem.

Dalam penelitian ini digunakan parameter a = 0,25, b = 3, c = 0,5, dan d = 0,05. Nilai-nilai parameter tersebut merupakan nilai klasik yang telah digunakan secara konsisten dalam literatur dan telah diverifikasi menghasilkan perilaku *hyperchaotic* yang stabil, di mana dua eksponen Lyapunov pertama bernilai positif, sehingga sistem ini secara resmi memenuhi definisi *hyperchaotic* (Yi & Cao, 2024).

Keistimewaan sistem Rössler 4D dibanding sistem *hyperchaotic* lainnya terletak pada strukturnya yang relatif sederhana, namun tetap mampu menghasilkan dinamika yang sangat kompleks. Sistem ini hanya mengandung satu suku nonlinear berupa perkalian xz pada persamaan ketiga, namun interaksi antar variabel tersebut sudah cukup untuk menciptakan perilaku *hyperchaotic* dengan dua arah ekspansi eksponensial yang simultan. Sifat ini membuat trajektori sistem jauh lebih sulit diprediksi dibanding sistem *chaos* biasa (Yi & Cao, 2024).

Selain kesederhanaan struktural yang hanya mengandung satu suku non-linier (perkalian *xz*), keunggulan sistem Rössler 4D turut didukung oleh bukti empiris pada literatur. Agarwal dkk. (2024) menunjukkan bahwa implementasi *hyperchaotic* Rössler 4D pada enkripsi citra menghasilkan sensitivitas kunci yang tinggi serta ketahanan terhadap berbagai serangan kriptografi standar. Struktur non-linier yang minim ini juga berimplikasi pada rendahnya kompleksitas komputasi per iterasi, sehingga secara teoritis Rössler 4D berpotensi menghasilkan waktu komputasi yang lebih efisien dibandingkan sistem *hyperchaotic* dengan jumlah suku non-linier lebih banyak seperti Chen 4D dan Lorenz 4D.

Dalam konteks enkripsi citra, sistem Rössler 4D dimanfaatkan untuk menghasilkan deret bilangan *pseudo-random* yang kemudian digunakan dalam proses permutasi posisi piksel dan difusi nilai piksel. Sensitivitas ekstrem terhadap kondisi awal dan kompleksitas *attractor* yang dihasilkan menjadikan sistem ini cocok sebagai pembangkit *keystream* yang sulit diprediksi, sehingga dapat secara efektif meningkatkan keamanan citra terenkripsi dengan memutus korelasi antar piksel yang berdekatan (Yi & Cao, 2024).

2.4.4 Mekanisme *Burn-in*

Mekanisme *burn-in* merupakan proses pembuangan sejumlah iterasi awal pada sistem *chaos* sebelum deret nilai yang dihasilkan digunakan sebagai kunci atau sumber keacakan. Pada sistem *chaos* iteratif, nilai awal sering kali masih dipengaruhi oleh kondisi awal dan dinamika transien sehingga belum sepenuhnya mencerminkan perilaku *chaos* yang stabil. Apabila nilai-nilai tersebut langsung digunakan, kualitas keacakan dapat menurun dan berpotensi menimbulkan pola

yang dapat dimanfaatkan dalam analisis kriptografi. Sehingga, mekanisme *burn-in* diterapkan untuk memastikan bahwa deret nilai yang digunakan berasal dari kondisi *chaos* yang telah berkembang secara penuh (Zolfaghari & Koshiba, 2022).

Pembuangan iterasi awal bertujuan untuk menghilangkan efek transien dan menghasilkan deret nilai dengan karakteristik statistik yang lebih baik, seperti distribusi yang mendekati *uniform* dan korelasi antar nilai yang lebih rendah. Hal ini berdampak pada peningkatan kualitas keacakan dan ketahanan terhadap serangan statistik maupun prediksi, sehingga mekanisme *burn-in* umum diterapkan dalam pembangkitan kunci serta proses permutasi dan difusi pada enkripsi citra berbasis *chaos* (Wen, Yang, dkk., 2024; Zhao dkk., 2023)

Meskipun meningkatkan beban komputasi karena sebagian iterasi tidak digunakan, penerapan mekanisme *burn-in* dinilai sebanding dengan peningkatan keamanan yang diperoleh. Penentuan jumlah iterasi yang dibuang bergantung pada karakteristik sistem *chaos* yang digunakan dan biasanya ditentukan melalui pengujian statistik.

2.5 Skema Permutasi Difusi Piksel Berbasis Chaos

Skema permutasi–difusi piksel berbasis *chaos* merupakan kerangka dasar yang paling umum digunakan dalam sistem enkripsi citra digital modern. Skema ini memanfaatkan sifat deterministik-*chaotic*, seperti sensitivitas tinggi terhadap kondisi awal dan perilaku pseudo-acak, untuk menghilangkan keteraturan visual dan statistik pada citra. Secara umum, proses enkripsi dilakukan melalui dua tahap utama yang saling melengkapi, yaitu permutasi piksel dan difusi piksel. Kombinasi kedua tahap tersebut bertujuan untuk menyamarkan posisi serta nilai intensitas

piksel sehingga citra terenkripsi tidak menunjukkan pola yang dapat dianalisis secara visual maupun statistik(Veena & Ramakrishna, 2021).

Tahap permutasi piksel bertujuan untuk mengacak posisi piksel tanpa mengubah nilai intensitasnya. Pada citra digital, piksel yang berdekatan umumnya memiliki korelasi spasial yang tinggi sehingga membentuk pola visual tertentu. Melalui permutasi, hubungan spasial antar-piksel diputus dengan memetakan posisi piksel asli ke posisi baru berdasarkan urutan indeks tertentu. Dalam skema berbasis chaos, urutan indeks permutasi dihasilkan dari deret *chaos* yang sangat sensitif terhadap kondisi awal dan parameter kontrol, sehingga perubahan kecil pada kunci akan menghasilkan pola pengacakan posisi piksel yang berbeda secara signifikan (Niu & Zhang, 2020)

Deret *chaos* tersebut dapat diolah menjadi pola permutasi yang bersifat bijektif, misalnya melalui pemetaan ke indeks bilangan bulat, sehingga setiap piksel dipetakan ke posisi yang unik dan proses dekripsi dapat dilakukan secara tepat tanpa ambiguitas (Andono & Setiadi, 2022).

2.5.1 Entropi Informasi

Entropi informasi digunakan untuk mengukur tingkat keacakan distribusi nilai intensitas piksel pada citra terenkripsi. Semakin tinggi nilai entropi, semakin sulit bagi penyerang untuk memprediksi pola statistik pada citra. Entropi Shannon untuk citra digital didefinisikan sebagai berikut:

$$H = -\sum_{i=0}^{L-1} p(i) \log_2 p(i) \tag{2.5}$$

dengan:

1. $p(i)$adalah probabilitas kemunculan nilai intensitas ke-i,
2. Ladalah jumlah level keabuan (misalnya $L = 256$ untuk citra 8-bit).

Untuk citra terenkripsi 8-bit yang ideal, nilai entropi mendekati 8 bit. Nilai entropi yang mendekati nilai ideal menunjukkan bahwa distribusi piksel pada citra terenkripsi bersifat hampir *uniform*, sehingga citra memiliki tingkat keacakan yang tinggi dan tahan terhadap serangan statistik. Dalam penelitian ini, nilai entropi digunakan sebagai salah satu indikator utama untuk menilai tingkat keacakan dan keamanan citra hasil enkripsi, khususnya sebelum dan sesudah *ciphertext* mengalami proses kompresi *lossy* (Wen, Lin, dkk., 2024).

2.5.2 Korelasi Antar Piksel

Korelasi antar-piksel digunakan untuk mengukur tingkat hubungan antara nilai intensitas piksel yang berdekatan, baik dalam arah horizontal, vertikal, maupun diagonal. Pada citra asli, piksel-piksel yang berdekatan umumnya memiliki korelasi tinggi. Sebaliknya, pada citra terenkripsi yang baik, korelasi antar-piksel harus mendekati nol (Niu & Zhang, 2020).

Koefisien korelasi antar dua piksel x dan y didefinisikan sebagai berikut:

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{2.6}$$

dengan:

$$\begin{aligned} \mathrm{cov}(x, y) &= E\big[\big(x - E(x)\big)\big(y - E(y)\big)\big] \\ D(x) &= E[(x - E(x))^2] \\ D(\mathrm{y}) &= E[(\mathrm{y} - E(\mathrm{y}))^2] \end{aligned} \tag{2.7}$$

Nilai korelasi r_{xy} berada pada rentang $[-1,1]$. Nilai korelasi yang mendekati 0 menunjukkan bahwa hubungan antar-piksel semakin rendah, sehingga struktur spasial citra asli semakin sulit dikenali pada citra terenkripsi. Dalam penelitian ini, analisis korelasi antar-piksel digunakan untuk mengevaluasi efektivitas proses permutasi dan difusi pada algoritma enkripsi *chaos*, serta untuk membandingkan perubahan nilai korelasi sebelum dan sesudah citra terenkripsi mengalami kompresi.

2.5.3 Number of Pixel Change Rate (NPCR)

NPCR digunakan untuk mengukur sensitivitas algoritma enkripsi terhadap perubahan kecil pada citra asli. Metrik ini menunjukkan persentase jumlah piksel yang berubah pada citra terenkripsi ketika satu piksel pada citra asli diubah. Rumus NPCR didefinisikan sebagai berikut (Niu & Zhang, 2020):

$$\text{NPCR} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\% \tag{2.8}$$

dengan:

$$D(i,j) = \begin{cases} 0, & \text{jika } C_1(i,j) = C_2(i,j) \\ 1, & \text{jika } C_1(i,j) \neq C_2(i,j) \end{cases} \tag{2.9}$$

di mana:

1. C_1 dan C_2 adalah dua citra terenkripsi dari citra asli yang hanya berbeda satu piksel,
2. $M \times N$adalah ukuran citra.

Nilai NPCR yang baik umumnya lebih dari 99%, yang menunjukkan bahwa perubahan kecil pada citra asli menghasilkan perubahan besar pada citra terenkripsi,

sehingga algoritma memiliki ketahanan tinggi terhadap serangan diferensial. Dalam penelitian ini, NPCR digunakan untuk mengevaluasi tingkat sensitivitas skema enkripsi citra berbasis *chaos* 4D terhadap perubahan input, serta untuk membandingkan pengaruh proses kompresi terhadap kestabilan sifat diferensial *ciphertext* (Niu & Zhang, 2020).

2.5.4 Unified Average Changing Intensity (UACI)

UACI mengukur rata-rata perubahan intensitas piksel antara dua citra terenkripsi yang dihasilkan dari citra asli yang sedikit berbeda. UACI didefinisikan sebagai berikut (Niu & Zhang, 2020):

$$\text{UACI} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{| C_1(i,j) - C_2(i,j) |}{L - 1} \times 100\% \qquad (2.10)$$

di mana:

1. C_1 dan C_2 adalah dua citra terenkripsi yang dihasilkan dari citra asli yang hanya berbeda satu piksel,
2. $M \times N$ adalah ukuran citra,
3. Ladalah jumlah level intensitas piksel (misalnya $L = 256$ untuk citra 8-bit).

Untuk citra 8-bit, nilai UACI yang dianggap baik umumnya berada di sekitar 33%. Nilai ini menunjukkan bahwa perubahan kecil pada citra asli menyebabkan perubahan intensitas yang signifikan pada citra terenkripsi, sehingga meningkatkan ketahanan terhadap serangan diferensial. Dalam penelitian ini, UACI digunakan bersama NPCR untuk menilai kekuatan difusi algoritma enkripsi citra berbasis

chaos serta untuk menganalisis perubahan tingkat difusi setelah *ciphertext* mengalami kompresi *lossy* (Niu & Zhang, 2020).

2.6 Analisis Kualitas Citra Hasil Dekripsi

Analisis kualitas citra hasil dekripsi bertujuan untuk menilai sejauh mana citra yang diperoleh setelah proses dekripsi mampu merekonstruksi citra asli secara visual dan numerik. Dalam sistem enkripsi citra yang baik, proses dekripsi diharapkan menghasilkan citra yang identik atau sangat mendekati citra asli tanpa distorsi yang berarti. Sehingga, evaluasi kualitas citra hasil dekripsi umumnya dilakukan menggunakan metrik kuantitatif yang dapat mengukur perbedaan antara citra asli dan citra hasil dekripsi. Dua metrik yang paling banyak digunakan dalam literatur enkripsi citra adalah *Peak Signal-to-Noise Ratio* (PSNR) dan *Mean Structural Similarity Index* (MSSIM) (Gafsi dkk., 2020)

2.6.1 Mean Structural Similarity Index (MSSIM)

MSSIM merupakan pengembangan dari *Structural Similarity Index* (SSIM) yang dirancang untuk menilai kesamaan struktural antara dua citra dengan mempertimbangkan persepsi visual manusia. Berbeda dengan PSNR yang hanya mengukur perbedaan numerik piksel, MSSIM mengevaluasi kesamaan citra berdasarkan tiga komponen utama, yaitu *luminance* (kecerahan), *contrast* (kontras), dan *structure* (struktur) pada berbagai skala resolusi.

SSIM untuk dua citra $x$dan $y$didefinisikan sebagai:

$$\text{SSIM}(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \tag{2.13}$$

di mana:

1. $\mu_x$dan $\mu_y$adalah rata-rata intensitas citra,
2. σ_x^2dan σ_y^2adalah variansi,
3. σ_{xy}adalah kovarians,
4. C_1dan C_2adalah konstanta stabilisasi.

MSSIM diperoleh dengan menghitung nilai SSIM pada beberapa skala dan kemudian dirata-ratakan. Nilai MSSIM berada pada rentang 0 hingga 1, di mana nilai mendekati 1 menunjukkan tingkat kemiripan struktural yang sangat tinggi antara citra asli dan citra hasil dekripsi.

Dalam evaluasi enkripsi citra, nilai MSSIM yang mendekati 1 menandakan bahwa struktur visual citra hasil dekripsi hampir identik dengan citra asli, sehingga kualitas visual dapat dipertahankan dengan baik. Hal ini penting karena citra yang memiliki PSNR tinggi belum tentu memiliki kesamaan struktural yang baik menurut persepsi manusia, sehingga MSSIM digunakan sebagai metrik pelengkap untuk menilai kualitas citra secara lebih komprehensif (Ashillah dkk., 2025)

Dalam penelitian ini, MSSIM digunakan sebagai metrik kualitas visual untuk mengevaluasi tingkat kesamaan struktural citra hasil dekripsi setelah proses kompresi, serta untuk membandingkan ketahanan kualitas visual pada algoritma enkripsi citra berbasis *chaos* 4D.

2.6.2 Peak Signal-to-Noise Ratio (PSNR)

PSNR merupakan metrik yang digunakan untuk mengukur tingkat kesamaan antara citra asli dan citra hasil dekripsi berdasarkan perbedaan nilai intensitas piksel. PSNR dihitung berdasarkan nilai *Mean Squared Error* (MSE) antara dua

citra yang dibandingkan. Semakin kecil nilai MSE, maka semakin besar nilai PSNR, yang menunjukkan kualitas citra hasil dekripsi semakin baik.

Rumus MSE didefinisikan sebagai berikut:

$$\text{MSE} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} [I(i,j) - D(i,j)]^2 \tag{2.11}$$

dengan:

1. $I(i,j)$adalah nilai piksel citra asli,
2. $D(i,j)$adalah nilai piksel citra hasil dekripsi,
3. $M \times N$adalah ukuran citra.

Nilai PSNR kemudian dihitung menggunakan persamaan:

$$\text{PSNR} = 10\log_{10}\left(\frac{(L-1)^2}{\text{MSE}}\right) \tag{2.12}$$

di mana L menyatakan jumlah level intensitas piksel (misalnya $L = 256$untuk citra 8-bit). Dalam konteks enkripsi citra, nilai PSNR yang sangat tinggi (misalnya di atas 40 dB) atau bahkan tak hingga (∞) menunjukkan bahwa citra hasil dekripsi identik dengan citra asli, sehingga tidak terjadi kehilangan informasi selama proses enkripsi dan dekripsi. Sebaliknya, nilai PSNR yang rendah mengindikasikan adanya distorsi pada citra hasil dekripsi (Ashillah dkk., 2025).

Dalam penelitian ini, PSNR digunakan untuk mengevaluasi kualitas citra hasil dekripsi setelah citra terenkripsi mengalami proses kompresi *lossy*, sehingga dapat dibandingkan tingkat penurunan kualitas pada masing-masing algoritma.

2.7 Keterkaitan Enkripsi dan Kompresi

Dalam sistem multimedia modern, enkripsi dan kompresi merupakan dua proses penting yang sering diterapkan secara berurutan pada citra digital. Enkripsi bertujuan menjaga kerahasiaan dan keamanan informasi visual, sedangkan kompresi bertujuan mengurangi ukuran data agar lebih efisien dalam penyimpanan dan transmisi. Meskipun memiliki tujuan berbeda, kedua proses ini saling berkaitan dan dapat saling memengaruhi, terutama ketika kompresi yang digunakan bersifat *lossy*. Dengan demikian, pemahaman mengenai keterkaitan antara enkripsi dan kompresi menjadi penting dalam perancangan sistem enkripsi citra yang praktis dan andal (M. Zhang dkk., 2020).

Kompresi *lossy* bekerja dengan menghilangkan informasi visual yang dianggap kurang signifikan melalui proses transformasi dan kuantisasi, seperti pada format JPEG, JPEG 2000, atau WebP. Ketika kompresi *lossy* diterapkan pada *ciphertext*, perubahan nilai piksel akibat kuantisasi dapat merusak struktur data terenkripsi. Hal ini berpotensi menyebabkan kegagalan proses dekripsi atau menurunkan kualitas citra hasil dekripsi, karena *ciphertext* yang telah terkompresi tidak lagi identik dengan *ciphertext* asli. Selain itu, proses kompresi dapat mengubah karakteristik statistik *ciphertext* yang idealnya bersifat acak, sehingga dalam kondisi tertentu dapat membuka peluang analisis kriptografi, meskipun aspek serangan kriptografi lanjutan tidak menjadi fokus dalam penelitian ini. (Peng dkk., 2024).

Tantangan utama dalam integrasi enkripsi dan kompresi terletak pada *trade-off* antara keamanan dan efisiensi. *Ciphertext* dengan tingkat keacakan tinggi

umumnya sulit dikompresi secara efektif, sedangkan kompresi yang agresif dapat merusak data terenkripsi. Berbagai pendekatan telah dikembangkan untuk mengatasi masalah ini, seperti melakukan kompresi sebelum enkripsi, menerapkan enkripsi parsial, atau merancang skema enkripsi yang toleran terhadap distorsi akibat kompresi *lossy* (Song dkk., 2022). Dalam konteks enkripsi citra berbasis *chaos*, isu ini menjadi semakin relevan karena sifat chaos menghasilkan keacakan tinggi. Dengan demikian, kajian keterkaitan enkripsi dan kompresi menjadi landasan penting dalam perancangan metode yang mampu menyeimbangkan keamanan, kualitas citra hasil dekripsi, dan efisiensi penyimpanan maupun transmisi data.

2.8 Efisiensi Komputasi (Running Time)

Efisiensi komputasi merupakan salah satu aspek penting dalam evaluasi algoritma enkripsi citra. Algoritma enkripsi tidak hanya perlu menghasilkan tingkat keamanan yang baik, tetapi juga harus memiliki waktu eksekusi yang layak agar dapat diterapkan secara praktis. Efisiensi komputasi umumnya diukur menggunakan waktu eksekusi atau running time, yaitu waktu yang dibutuhkan suatu algoritma untuk menyelesaikan proses komputasi pada spesifikasi perangkat keras dan perangkat lunak tertentu. Dalam konteks enkripsi citra, running time dapat digunakan untuk mengukur proses enkripsi, dekripsi, maupun tahapan pengujian lain yang melibatkan proses tambahan seperti kompresi dan dekompresi citra. Pada algoritma enkripsi citra berbasis chaos 4D, running time dipengaruhi oleh beberapa faktor, seperti ukuran citra, jumlah piksel yang diproses, jumlah iterasi pembangkitan deret chaos, serta kompleksitas persamaan dinamis yang

digunakan. Sistem chaos 4D memiliki empat variabel keadaan yang saling berinteraksi, sehingga proses pembangkitan *chaos sequence* membutuhkan operasi numerik berulang. Kompleksitas persamaan pada masing-masing algoritma, seperti Chen 4D, Lorenz 4D, Lü 4D, dan Rössler 4D, dapat menyebabkan perbedaan waktu eksekusi meskipun struktur enkripsi yang digunakan sama. Evaluasi running time diperlukan untuk mengetahui efisiensi implementasi aktual dari setiap algoritma (Liu dkk., 2022; Tiwari dkk., 2025).

Selain pengukuran running time secara empiris, efisiensi algoritma juga dapat dianalisis secara teoritis menggunakan notasi Big-O atau O-notation. Notasi Big-O digunakan untuk menggambarkan laju pertumbuhan waktu komputasi terhadap ukuran masukan, terutama ketika ukuran data yang diproses semakin besar. Secara formal, suatu fungsi f(n) dikatakan berorde O(g(n)) apabila terdapat konstanta positif c dan n_0 sedemikian sehingga $f(n) \leq c \cdot g(n)$ untuk semua $n \geq n_0$ (Cormen dkk., 2022). Dalam konteks enkripsi citra, ukuran masukan n umumnya merepresentasikan jumlah total piksel citra, yaitu $n = H \times W \times C$, dengan H sebagai tinggi citra, W sebagai lebar citra, dan C sebagai jumlah kanal warna.

Berdasarkan tahapan tersebut, kompleksitas proses enkripsi citra berbasis *chaos* 4D pada penelitian ini didominasi oleh tahap permutasi, sehingga dapat dinyatakan sebagai O(n log n). Proses dekripsi memiliki kompleksitas O(n), karena hanya melibatkan *inverse diffusion* dan *inverse permutation* menggunakan indeks permutasi yang telah diperoleh. Namun, apabila proses enkripsi dan dekripsi dilihat sebagai satu siklus penuh, maka kompleksitas totalnya tetap O(n log n), karena masih didominasi oleh proses permutasi pada tahap enkripsi. Kompleksitas ini

berlaku untuk keempat algoritma yang digunakan dalam penelitian ini, yaitu Chen 4D, Lorenz 4D, Lü 4D, dan Rössler 4D, karena keempatnya menggunakan struktur permutasi-difusi yang sama meskipun memiliki persamaan dinamis yang berbeda (Alexan dkk., 2023).

Dengan demikian, *running time* digunakan sebagai metrik empiris untuk mengukur waktu eksekusi aktual pada implementasi pengujian, sedangkan notasi Big-O digunakan sebagai analisis teoritis untuk menjelaskan pertumbuhan kompleksitas algoritma terhadap ukuran citra. Keduanya saling melengkapi dalam menilai efisiensi komputasi algoritma enkripsi citra berbasis *chaos* 4D.

2.9 Penelitian Terkait

Tabel 2. 1 *State of The Art* (SOTA)

No.	Judul Penelitian	Kelebihan	Kekurangan	Gap Penelitian
1.	*Chaos-Based Color Image Encryption with JPEG Compression: Balancing Security and Compression Efficiency* (W. Zhang dkk., 2025)	Mengintegrasikan enkripsi *hyperchaotic* Lorenz 4D dalam *pipeline* JPEG pada domain DCT; mengevaluasi trade-off keamanan dan efisiensi kompresi secara komprehensif (entropi, NPCR, UACI, *running time*).	Terbatas pada format JPEG dan domain DCT; tidak menguji format kompresi modern lain (JP2K, WebP, HEIC, AVIF).	Tidak membandingkan Lorenz 4D dengan sistem *hyperchaotic* 4D lain; pengujian kompresi hanya satu format.
2.	*A Hyperchaotic Lorenz and DNA-Encoded Image Encryption Algorithm* (S. Li & Li, 2024)	Menggunakan *hyperchaotic* Lorenz 4D yang didiskretisasi dengan *Runge-Kutta* orde 4; mengintegrasikan DNA *coding* untuk *scrambling* dan difusi; evaluasi mencakup *key space*, histogram, korelasi, dan entropi.	Tidak mengevaluasi *running time* maupun ketahanan terhadap kompresi *lossy*; tidak membandingkan dengan algoritma 4D lain.	Belum menganalisis ketahanan enkripsi Lorenz 4D terhadap kompresi *lossy* multi-format; tidak ada perbandingan dengan Chen, Lü, dan Rössler 4D.
3.	*Lossy Compression of Single-channel Noisy Images by Modern Coders* (Kryvenko dkk., 2024)	Analisis komprehensif format kompresi modern (JPEG, JP2K, HEIC, AVIF) dengan metrik kualitas rekonstruksi yang terstandarisasi.	Tidak melibatkan enkripsi citra; analisis dilakukan pada citra asli, bukan *ciphertext*.	Dampak kompresi multi-format terhadap *ciphertext hyperchaotic* 4D belum dievaluasi.
4.	*An Image Encryption Method*	Mengusulkan improved *hyperchaotic* Lorenz *system* dengan Lyapunov	Sistem Lorenz yang digunakan merupakan versi	Ketahanan skema enkripsi berbasis Lorenz

No.	Judul Penelitian	Kelebihan	Kekurangan	Gap Penelitian
	Based on Improved Lorenz Chaotic System and Galois Field (Zhang dkk., 2024)	*exponent* maksimum 2.9897; menggabungkan permutasi berbasis *image pyramid structure* dan difusi berbasis Galois field GF(2^8); evaluasi mencakup *key space*, histogram, entropi, korelasi, NPCR, UACI, dan *running time*.	yang dimodifikasi, bukan sistem Lorenz 4D klasik yang telah distandarisasi; tidak menguji ketahanan *ciphertext* terhadap kompresi *lossy* apapun.	*hyperchaotic* (bahkan versi *improved*) terhadap kompresi *lossy multi-format* belum dievaluasi; tidak ada perbandingan langsung dengan Chen, Lü, dan Rössler 4D klasik.
5.	*4D-Rossler Hyperchaotic System for Image Encryption and Decryption with High Security* (Agarwal dkk., 2024)	Mengimplementasikan *hyperchaotic* Rössler 4D secara eksplisit untuk enkripsi citra; menunjukkan sensitivitas kunci yang tinggi dan ketahanan terhadap berbagai serangan kriptografi standar.	Evaluasi hanya pada domain spasial tanpa pengujian kompresi *lossy*; tidak membandingkan dengan sistem *hyperchaotic* 4D lain.	Ketahanan Rössler 4D terhadap kompresi *lossy* modern belum diketahui; belum ada perbandingan langsung dengan Lorenz, Chen, dan Lü 4D.
6.	*Image Encryption Algorithm Based on Hyperchaos and DNA Coding* (L. Li, 2024)	Menggunakan *hyperchaotic* Chen system sebagai generator kunci; mengintegrasikan DNA encoding untuk scrambling piksel dan difusi; evaluasi mencakup entropi, korelasi, NPCR, UACI, *key sensitivity*, dan *robustness (noise dan cropping attack*).	Tidak mengevaluasi *running time* dan tidak menguji ketahanan terhadap kompresi *lossy*; tidak membandingkan dengan sistem *hyperchaotic* 4D lain.	Dampak kompresi lossy multi-format terhadap kualitas dekripsi Chen 4D belum dievaluasi; tidak ada perbandingan lintas algoritma *hyperchaotic* 4D klasik.
7.	*Color Image Cryptosystem Based on Sine Chaotic Map, 4D Chen Hyperchaotic Map*	Menggunakan *hyperchaotic* Chen 4D berorde fraksional dengan hybrid DNA coding; evaluasi kualitas rekonstruksi melalui PSNR (8.27 dB) dan SSIM;	Tidak mempertimbangkan proses kompresi citra; tidak membandingkan Chen 4D dengan sistem *hyperchaotic* 4D lain.	Pengaruh kompresi *lossy* multi-format terhadap kualitas dekripsi Chen 4D fractional belum dianalisis;

No.	Judul Penelitian	Kelebihan	Kekurangan	Gap Penelitian
	of Fractional-Order and Hybrid DNA Coding (Alexan dkk., 2023)	entropi 7.997 dan NPCR 99.62% mendekati nilai ideal.		tidak ada studi perbandingan lintas algoritma 4D.
8.	*Effects of JPEG Compression on Vision Transformer Image Classification for Encryption-then-Compression Images* (Hamano dkk., 2023)	Membuktikan citra terenkripsi dapat dikompresi JPEG dengan degradasi minimal pada skenario *Encryption-then-Compression* (EtC).	Enkripsi tidak berbasis *hyperchaotic* 4D; hanya menguji format JPEG; tidak mengevaluasi keamanan statistik (entropi, NPCR, UACI).	Tidak menganalisis pengaruh sistem *hyperchaotic* 4D terhadap ketahanan kompresi; tidak mengevaluasi format WebP, HEIC, dan AVIF.
9.	*Development of a Novel Hyperchaos-Based Image Encryption Algorithm Consisting of Two Scrambling-Diffusion Operations* (Y. Huang dkk., 2022)	Menggunakan *hyperchaotic* Chen dengan dua operasi scrambling-diffusion dan satu scrambling tambahan; kunci awal diturunkan dari MD5 *plaintext*; tahan terhadap chosen-*plaintext* attack; evaluasi mencakup *key space*, korelasi, entropi, NPCR, dan UACI.	Tidak menguji ketahanan *ciphertext* terhadap kompresi *lossy*; tidak mencantumkan *running time*; tidak membandingkan dengan algoritma 4D lain.	Dampak kompresi *lossy* terhadap kualitas dekripsi Chen 4D belum dievaluasi; tidak ada perbandingan dengan Lorenz, Lü, dan Rössler 4D.
10.	*Novel Encryption for Color Images Using Fractional-Order Hyperchaotic System* (Hosny dkk., 2022)	Menggunakan *hyperchaotic* Chen 4D berorde fraksional; enkripsi per *channel* R, G, B dengan konfusi berbasis permutasi piksel dan difusi Fibonacci Q-matrix; evaluasi	Tidak mencantumkan *running time*; tidak menguji ketahanan terhadap kompresi *lossy*; tidak membandingkan dengan sistem *hyperchaotic* 4D lain.	Dampak kompresi *lossy multi-format* terhadap dekripsi skema Chen 4D *fractional-Fibonacci* Q-matrix belum dievaluasi;

No.	Judul Penelitian	Kelebihan	Kekurangan	Gap Penelitian
		mencakup entropi, korelasi, *key space*, *noise attack*, dan *data-cut attack*.		tidak ada studi komparatif lintas algoritma 4D.
11.	*Hyperchaotic Image Encryption Based on Multiple Bit Permutation and Diffusion* (T. Li & Zhang, 2021)	Mengajukan sistem *hyperchaotic* 4D berbasis Lorenz dengan tiga Lyapunov exponent positif; skema MBPD pada domain spasial; evaluasi komprehensif meliputi korelasi, entropi, NPCR, UACI (lulus seluruh 16 citra uji), dan *running time.*	Tidak menguji ketahanan *ciphertext* terhadap kompresi *lossy*; sistem yang diusulkan adalah sistem baru, bukan sistem Lorenz 4D klasik yang distandarisasi.	Meskipun mengevaluasi *running time* pada domain spasial, dampak kompresi *lossy* modern tidak dikaji; tidak ada perbandingan dengan Chen, Lü, dan Rössler 4D klasik.

Tabel 2.1 menunjukkan bahwa penelitian enkripsi citra berbasis *hyperchaotic* 4D telah berkembang dengan berbagai variasi algoritma. Sistem Lorenz 4D baik versi klasik maupun yang dimodifikasi paling banyak dikaji, digunakan dalam berbagai skema mulai dari integrasi kompresi JPEG (W. Zhang dkk., 2025), kombinasi DNA *coding* (Li dkk., 2024), skema *improved* Lorenz dengan permutasi *pyramid* dan difusi Galois field disertai evaluasi *running time* (Zhang dkk., 2024), hingga skema *multi-bit permutation-diffusion* (Li & Zhang, 2021). Sistem Chen 4D juga mendapat perhatian besar, baik versi integer-order dengan DNA *coding* (Li, 2024; Huang, 2022) maupun versi berorde fraksional (Alexan dkk., 2023; Hosny dkk., 2022). Seluruh penelitian tersebut mengevaluasi keamanan menggunakan metrik standar entropi, korelasi piksel, NPCR, dan UACI pada domain spasial.

Namun demikian, terdapat dua keterbatasan yang konsisten ditemukan. Pertama, setiap penelitian hanya menggunakan satu sistem *hyperchaotic* 4D tanpa membandingkannya secara langsung dengan sistem 4D lain dalam kerangka evaluasi yang seragam. Kedua, hampir seluruh penelitian tidak menguji ketahanan *ciphertext* terhadap kompresi *lossy*. Hanya W. Zhang dkk. (2025) yang mengintegrasikan pengujian kompresi, meskipun terbatas pada satu format (JPEG), dan Hamano dkk. (2023) yang menguji dampak JPEG tanpa menggunakan *hyperchaotic* 4D. Kryvenko dkk. (2024) menganalisis format kompresi modern secara mendalam namun tanpa melibatkan enkripsi. Yang paling signifikan, sistem Rössler 4D hanya ditemukan dalam satu referensi (Agarwal dkk., 2024) dan sistem Lü 4D tidak ditemukan sama sekali dalam literatur enkripsi citra.

Berdasarkan analisis tersebut, belum terdapat penelitian yang secara komprehensif membandingkan keempat sistem *hyperchaotic* 4D klasik Lorenz, Chen, Lü, dan Rössler dalam satu kerangka enkripsi berbasis permutasi difusi piksel pada domain spasial, sekaligus mengevaluasi ketahanannya terhadap berbagai format kompresi *lossy* modern (JPEG, JP2K, WebP, HEIC, AVIF). Penelitian ini dirancang untuk mengisi celah tersebut melalui analisis komparatif yang mencakup aspek keamanan (entropi, korelasi, NPCR, UACI), kualitas dekripsi (PSNR, MSSIM), dan efisiensi komputasi (*running time*).

Tabel 2. 2 Matriks Penelitian

No.	Judul Peneliti	Algoritma Chaos 4D				Format Kompresi					Aspek Evaluasi		
		Lorenz 4D	Chen 4D	Lu 4D	Rossler 4D	JPEG	JP2K	WebP	HEIC	AVIF	Keamanan	Kualitas	Waktu
1.	(W. Zhang dkk., 2025)	✓	–	–	–	✓	–	–	–	–	✓	✓	✓
2.	(S. Li & Li, 2024)	✓	–	–	–	–	–	–	–	–	✓	–	–
3.	(Kryvenko dkk., 2024)	–	–	–	–	✓	✓	–	✓	✓	–	✓	✓
4.	(Zhang dkk., 2024)	✓	–	–	–	–	–	–	–	–	✓	✓	✓
5.	(Agarwal dkk., 2024)	–	–	–	✓	–	–	–	–	–	✓	✓	✓
6.	(L. Li, 2024)	–	✓	–	–	–	–	–	–	–	✓	✓	–
7.	*(Alexan dkk., 2023)*	–	✓	–	–	–	–	–	–	–	✓	✓	✓
8.	(Hamano dkk., 2023)	–	–	–	–	✓	–	–	–	–	–	✓	–
9.	*(Y. Huang dkk., 2022)*	–	✓	–	–	–	–	–	–	–	✓	✓	–
10.	(Hosny dkk., 2022)	–	✓	–	–	–	–	–	–	–	✓	✓	–
11.	(T. Li & Zhang, 2021)	✓	–		–	–	–	–	–	–	✓	✓	✓
12.	(*Ours*)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓