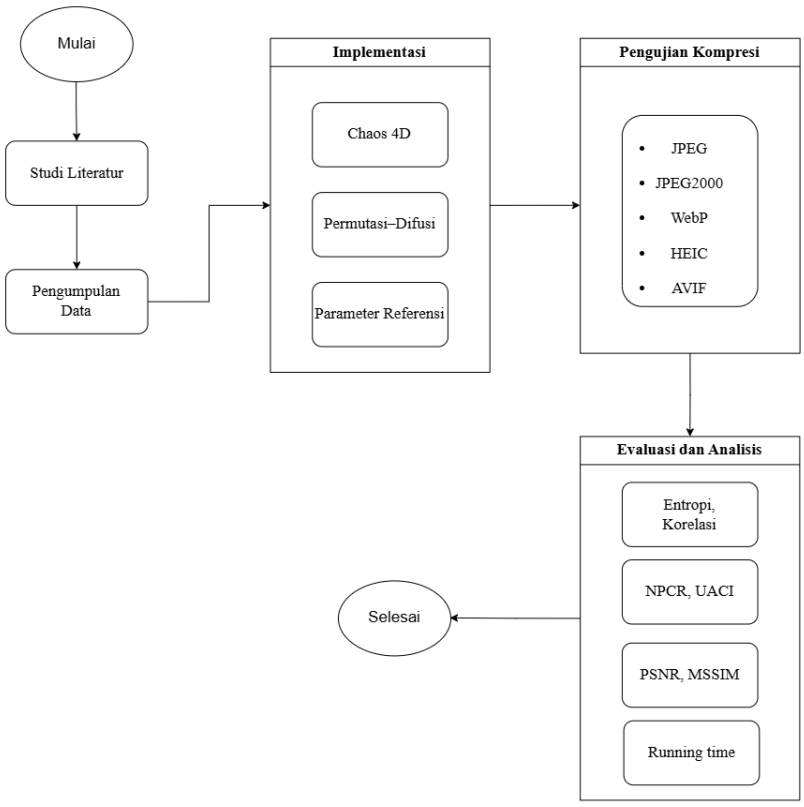
BAB III

METODOLOGI

3.1 Tahapan Penelitian

Penelitian ini dilakukan untuk menguji dan membandingkan ketahanan algoritma enkripsi citra berbasis *chaos* 4D terhadap kompresi citra *lossy* serta mengevaluasi kualitas citra hasil dekripsi. Metode yang digunakan berupa eksperimen komputasional dengan mengimplementasikan model enkripsi *chaos* dari literatur dan melakukan pengujian menggunakan beberapa format kompresi citra. Evaluasi hasil dilakukan menggunakan metrik keamanan dan kualitas citra. Tahapan penelitian ditunjukkan pada Gambar 3.1.



Gambar 3. 1 Tahapan Penelitian

3.1.1 Studi Literatur

Tahapan pertama adalah studi literatur, yaitu proses penelusuran dan kajian terhadap jurnal serta referensi ilmiah yang berkaitan dengan enkripsi citra berbasis sistem *chaos*, skema permutasi–difusi, kompresi citra *lossy*, dan metrik evaluasi keamanan serta kualitas citra. Studi literatur dilakukan untuk menentukan model *chaos* yang diimplementasikan, skema enkripsi yang digunakan, serta metrik pengujian yang diterapkan dalam penelitian. Hasil studi literatur menjadi dasar dalam penentuan metode dan skenario pengujian yang dilakukan.

3.1.2 Pengumpulan Data

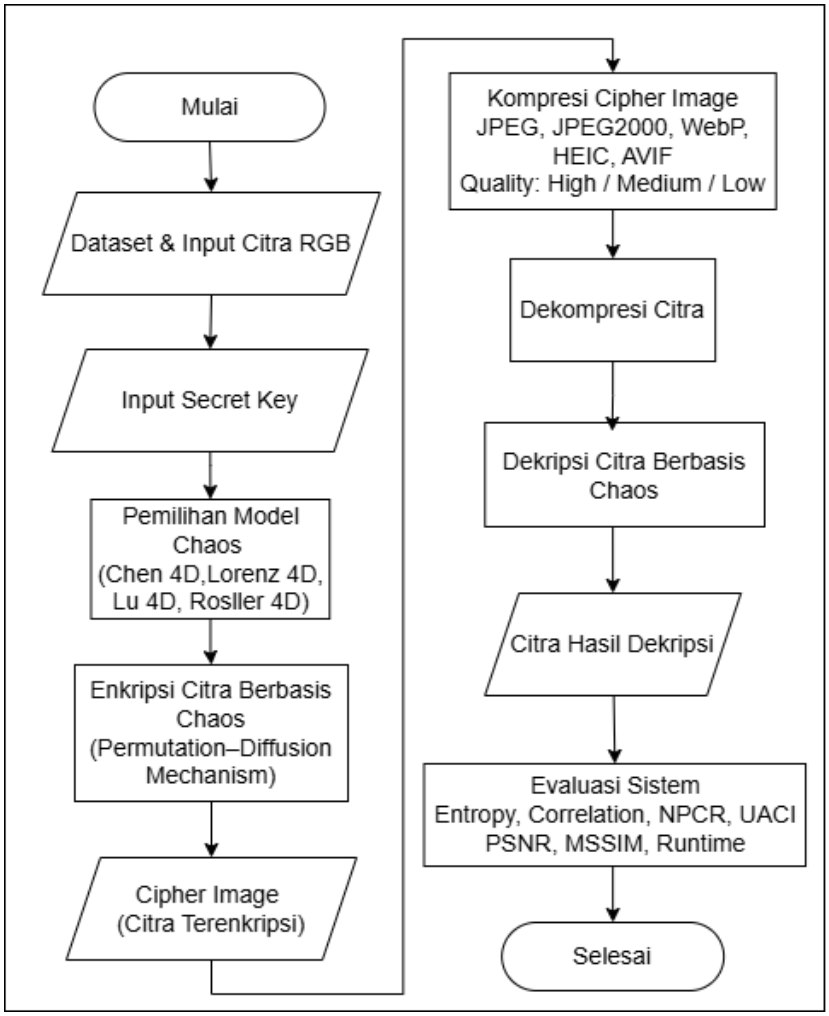
Tahapan selanjutnya adalah pengumpulan data citra yang digunakan sebagai objek pengujian algoritma enkripsi dan proses kompresi. Data berupa 12 citra digital berwarna (RGB) dengan resolusi seragam 512×512 piksel yang diperoleh dari USC-SIPI Image Database sebagai dataset publik dalam bidang pengolahan citra digital. Citra uji dipilih dengan karakteristik visual yang berbeda, seperti variasi tekstur, warna, dan tingkat detail. Pemilihan 12 citra tersebut bertujuan agar pengujian ketahanan enkripsi dan kualitas hasil dekripsi dapat diamati pada lebih dari satu kondisi citra.

3.1.3 Implementasi

Tahapan implementasi dilakukan dengan merealisasikan algoritma enkripsi citra berbasis sistem chaos 4D dalam lingkungan komputasi Python menggunakan pendekatan enkripsi murni spasial dengan skema permutasi–difusi piksel. Alur kerja sistem enkripsi dan kompresi citra berbasis chaos yang digunakan dalam penelitian ini ditunjukkan pada Gambar 3.2.

Sebelum menjelaskan alur kerja teknis sistem tersebut, perlu ditegaskan terlebih dahulu objek dan skenario keamanan yang menjadi fokus penelitian ini. Objek yang diamankan dalam penelitian ini adalah konten atau informasi visual dari citra digital, bukan berkas (file) citra itu sendiri. Dengan kata lain, penelitian ini tidak bertujuan mencegah pihak yang tidak berwenang memperoleh salinan citra terenkripsi, baik pada saat citra tersebut disimpan maupun ketika ditransmisikan dan mengalami proses kompresi. Skenario yang diasumsikan adalah pihak tidak berwenang berpotensi memperoleh berkas citra terenkripsi (*cipher image*) tersebut, tetapi tidak memiliki *secret key* yang sesuai untuk melakukan proses dekripsi.

Berdasarkan skenario tersebut, tujuan pengamanan yang ingin dicapai dalam penelitian ini adalah memastikan bahwa meskipun berkas citra terenkripsi berhasil diperoleh pihak lain, informasi visual di dalamnya tetap tidak dapat dikenali atau ditafsirkan tanpa proses dekripsi menggunakan kunci yang benar. Pendekatan yang digunakan untuk mencapai tujuan tersebut adalah skema enkripsi citra berbasis sistem chaos 4D dengan mekanisme permutasi dan difusi piksel, yang alur kerjanya ditunjukkan pada Gambar 3.2 berikut.



Gambar 3. 2 *Workflow* Sistem Enkripsi dan Kompresi Citra Berbasis *Chaos*

Berdasarkan Gambar 3.2, alur kerja sistem dalam penelitian ini dimulai dengan memasukkan dataset citra RGB sebagai *input* beserta *secret key* yang berfungsi sebagai kunci pada proses enkripsi dan dekripsi. Citra kemudian dienkripsi menggunakan empat algoritma chaos 4D, yaitu Chen 4D, Lorenz 4D, Lü 4D, dan Rössler 4D, dengan mekanisme permutasi–difusi untuk menghasilkan *cipher image*. Selanjutnya, citra terenkripsi dikompresi menggunakan lima metode kompresi, yaitu JPEG, JPEG2000, WebP, HEIC, dan AVIF, dengan beberapa tingkat kualitas kompresi. Hasil kompresi kemudian didekompresi dan didekripsi untuk

memperoleh kembali citra asli. Tahap terakhir adalah evaluasi performa sistem menggunakan metrik entropi, korelasi, NPCR, UACI, PSNR, MSSIM, serta *runtime* untuk menganalisis aspek keamanan, kualitas citra hasil dekripsi, dan efisiensi waktu komputasi.

Setiap model *chaos* 4D dibangkitkan sesuai persamaan diferensial yang mengacu pada literatur dengan kondisi parameter pada rentang *chaotic*, antara lain Chen 4D (a = 35, b = 3, c = 12, d = 7, k = 5), Lorenz 4D, Lü 4D, dan Rössler 4D dengan parameter masing-masing yang telah terverifikasi menghasilkan perilaku hiperkacau. Untuk menghilangkan efek transien awal pada deret *chaos* yang dibangkitkan, diterapkan mekanisme *burn-in* sebanyak 1.000 iterasi sebelum deret digunakan dalam proses enkripsi.

Nilai *chaos* yang dihasilkan kemudian dipetakan dari rentang [0, 1] ke rentang intensitas piksel 8-bit [0–255] menggunakan operasi pembulatan ke bawah $\lfloor x \times 256 \rfloor$ dan dikonversi ke tipe data *unsigned* 8-bit integer (uint8) agar kompatibel dengan representasi nilai piksel citra. Tahap permutasi dilakukan dengan meratakan piksel citra menjadi vektor satu dimensi, kemudian menentukan indeks pengacakan menggunakan proses pengurutan (*argsort*) terhadap deret chaos, sehingga diperoleh pemetaan bijektif yang dapat diinvers pada saat dekripsi. Sementara itu, tahap difusi dilakukan menggunakan operasi XOR independen antara piksel hasil permutasi dan kunci *chaos* yang dibangkitkan dari *seed* berbeda guna menghindari korelasi antartahap. Nilai *seed* diturunkan dari kombinasi *master key* dan jumlah total piksel citra, serta dibedakan pada tiap kanal RGB untuk meningkatkan sensitivitas kunci terhadap perubahan masukan.

Implementasi dalam penelitian ini dilakukan tanpa memodifikasi struktur dasar masing-masing algoritma *chaos* 4D, sehingga fokus penelitian sepenuhnya diarahkan pada pengujian dan perbandingan kinerja keamanan enkripsi, kualitas citra hasil dekripsi, serta efisiensi waktu eksekusi dari keempat algoritma tersebut.

3.1.4 Pengujian Kompresi

Tahapan pengujian kompresi dilakukan untuk melihat pengaruh kompresi citra *lossy* terhadap hasil enkripsi dan kualitas citra hasil dekripsi. Pada tahap ini, setiap citra yang telah dienkripsi menggunakan metode *chaos* dikenai proses kompresi dengan beberapa format, yaitu JPEG, JPEG 2000, WebP, HEIC, dan AVIF. Pengujian dilakukan dengan alur berurutan, yaitu citra asli dienkripsi, kemudian citra terenkripsi dikompresi dan didekompresi kembali, setelah itu dilakukan proses dekripsi. Hasil dekripsi setelah kompresi digunakan sebagai dasar perhitungan metrik keamanan dan kualitas citra pada tahap evaluasi. Pengujian diterapkan secara konsisten pada setiap metode enkripsi dan metode kompresi yang diuji. Pada setiap format kompresi, pengujian dilakukan menggunakan tiga tingkat kualitas kompresi, yaitu tinggi, sedang, dan rendah, untuk menganalisis pengaruh variasi rasio kompresi terhadap ketahanan enkripsi serta kualitas citra hasil dekripsi.

Proses kompresi dan dekompresi citra pada penelitian ini dilakukan menggunakan pustaka pengolahan citra pada bahasa pemrograman Python, yaitu OpenCV untuk format JPEG, JPEG 2000, dan WebP, serta Pillow yang dikombinasikan dengan pustaka pillow-heif untuk mendukung format kompresi HEIC dan AVIF.

3.1.5 Evaluasi dan Analisis

Tahapan evaluasi dan analisis dilakukan untuk menilai kinerja keamanan algoritma enkripsi citra berbasis *chaos* 4D serta ketahanan dan kualitas citra hasil dekripsi akibat pengaruh kompresi. Evaluasi keamanan diukur secara statistik dan sensitivitas menggunakan metrik entropi, korelasi piksel, NPCR, dan UACI. Sementara itu, ketahanan dan kualitas citra hasil dekripsi dievaluasi menggunakan PSNR dan MSSIM, sedangkan efisiensi algoritma dievaluasi dengan mencatat waktu eksekusi (*runtime*). Perhitungan seluruh metrik mengacu pada rumus yang telah dijelaskan pada Bab II. Seluruh nilai metrik evaluasi yang disajikan pada tabel hasil pengujian merupakan nilai rata-rata dari 12 citra uji. Khusus untuk metrik yang dihitung berdasarkan kanal warna RGB, nilai pada kanal R, G, dan B dihitung terlebih dahulu secara terpisah, kemudian hasil akhir diperoleh dari rata-rata ketiga kanal tersebut. Hasil pengujian kemudian dibandingkan antar algoritma, format kompresi, dan tingkat kualitas kompresi untuk melihat pola kinerja, tingkat stabilitas, serta kombinasi pendekatan yang memberikan hasil paling optimal. Selain itu, hasil evaluasi juga digunakan untuk mengidentifikasi pola penurunan performa keamanan dan kualitas citra akibat variasi rasio kompresi. Hasil evaluasi tersebut kemudian menjadi dasar dalam membandingkan performa masing-masing algoritma *chaos* 4D secara menyeluruh.