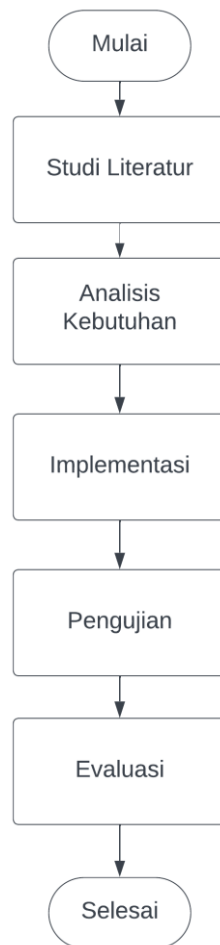


BAB III

METODOLOGI PENELITIAN

3.1. Tahapan Penelitian

Metode penelitian untuk implementasi ini terdiri dari beberapa tahap, untuk tahapan penelitiannya dimulai dari studi literatur, analisis kebutuhan, implementasi Enkripsi AES, RSA, dan Steganografi LSB, pengujian dan yang terakhir analisis dan evaluasi. Alur penelitian selengkapnya dapat dilihat pada Gambar 3.1.



Gambar 3.1 Alur Penelitian yang akan dilakukan

3.1.1 Studi Literatur

Studi literatur pada penelitian ini didapat dari sumber jurnal yang sudah dipublikasi dan buku yang terdapat pada internet. Studi pustaka dilakukan dengan cara mengumpulkan, membaca, serta memahami jurnal, buku, dan referensi lain untuk mendapatkan informasi yang dibutuhkan dalam menunjang penelitian ini.

3.1.2 Analisis Kebutuhan

Tahap analisis kebutuhan bertujuan untuk mengidentifikasi seluruh komponen yang diperlukan dalam proses implementasi penelitian. Penelitian ini memerlukan citra digital dengan format PNG yang berfungsi sebagai media penyisipan data. Selain itu, dibutuhkan proses pembangkitan kunci kriptografi untuk algoritma Advanced Encryption Standard (AES) dan Rivest–Shamir–Adleman (RSA) guna menjamin keamanan data yang akan disisipkan. Komponen lain yang diperlukan adalah file *plaintext* yang akan dienkripsi, di mana file ini akan melalui proses enkripsi AES-GCM terlebih dahulu lalu digabung kan dengan data AES yang akhirnya di encode menggunakan Base64 untuk digabungkan dan dipisah menggunakan separator sebelum disisipkan ke dalam citra menggunakan teknik steganografi Least Significant Bit (LSB). Dengan demikian, seluruh kebutuhan yang telah diidentifikasi akan menjadi dasar dalam tahap implementasi sistem.

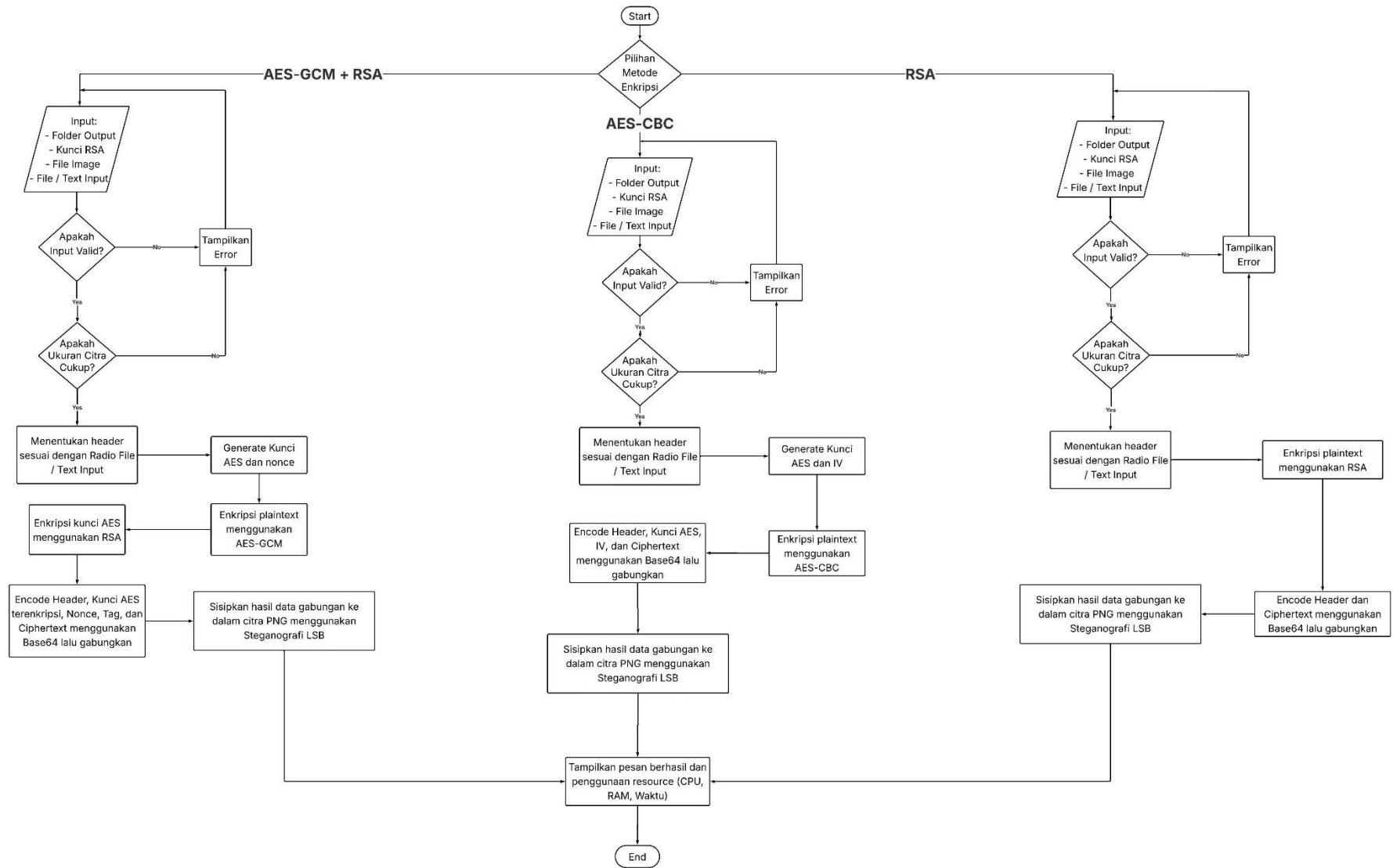
3.1.3 Implementasi

Tahap ini merupakan proses penerapan metode yang diusulkan. Secara garis besar, implementasi melibatkan proses pembangkitan kunci RSA, enkripsi data menggunakan algoritma AES-GCM yang kuncinya dienkripsi dengan RSA, serta

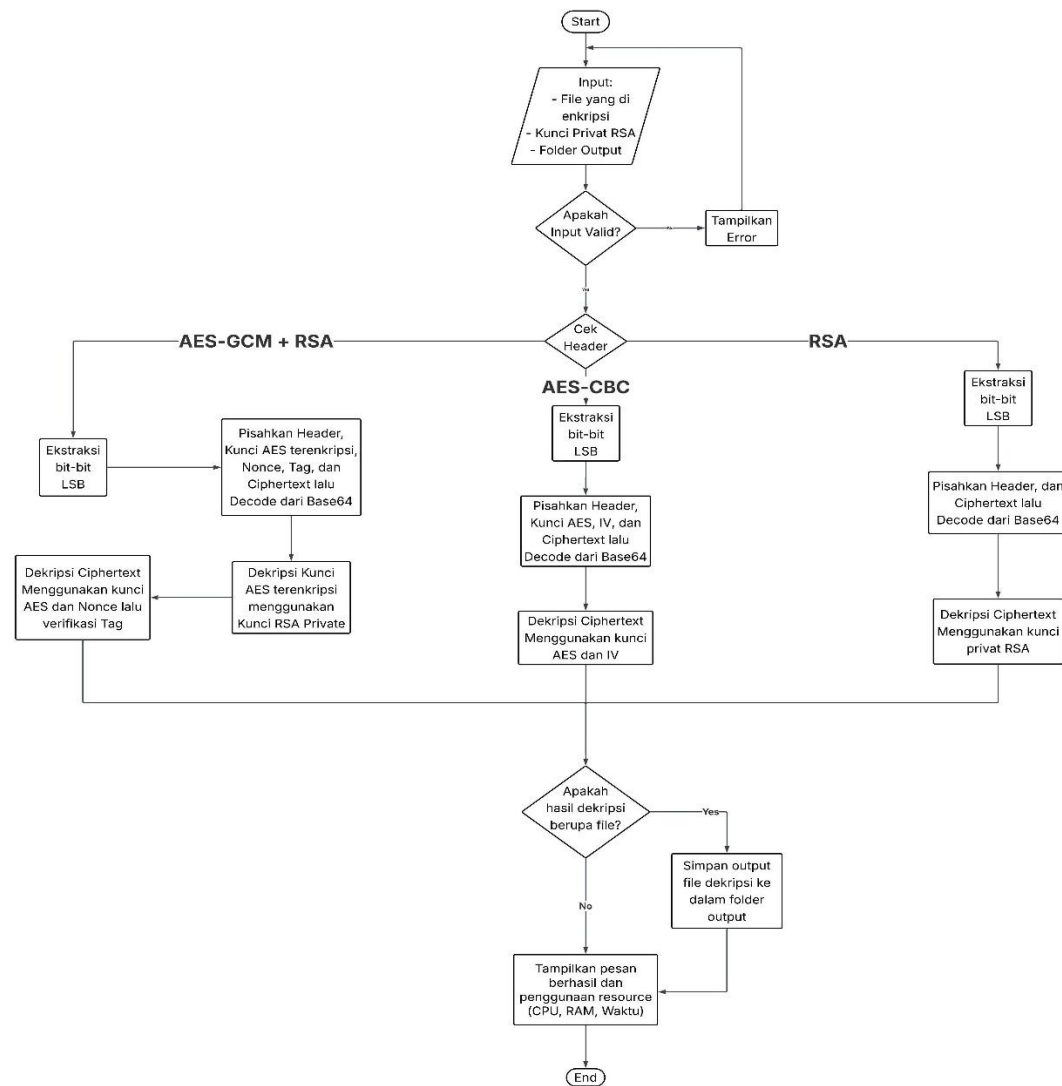
penyisipan data ke dalam citra menggunakan metode steganografi LSB. Rangkaian proses enkripsi dibuat dalam bentuk *flowchart* pada Gambar 3.2.

Selain proses enkripsi, dibutuhkan juga tahapan dekripsi untuk mengembalikan pesan ke bentuk semula. Pada tahap ini, sistem akan mengekstrak data tersembunyi dari citra menggunakan metode steganografi LSB, kemudian mendekripsi kunci AES dengan menggunakan kunci privat RSA. Setelah itu, *ciphertext* didekripsi menggunakan algoritma AES-GCM untuk mendapatkan *plaintext* asli. Rangkaian proses dekripsi dibuat dalam bentuk *flowchart* pada Gambar 3.3.

Diharapkan dengan menggunakan algoritma AES-GCM 256 bit dan RSA 4096 bit dalam proses enkripsi dapat meningkatkan keamanan pada metode Steganografi LSB.



Gambar 3.2 Alur Enkripsi yang diusulkan



Gambar 3.3 Alur Dekripsi yang diusulkan

3.1.4 Pengujian

Tahap selanjutnya adalah melakukan pengujian hasil implementasi.

Pengujian yang akan dilakukan dalam penelitian ini adalah sebagai berikut:

1. Deteksi Steganografi

Menguji apakah pesan tersembunyi dapat dideteksi oleh alat atau metode steganalisis.

2. Kapasitas Steganografi

Mengukur seberapa banyak data yang dapat disisipkan ke dalam media tanpa merusak kualitasnya.

3. Ketahanan (*Robustness*)

Mengukur ketahanan steganografi terhadap manipulasi citra seperti *crop*, *rotate*, dan *flip*.

4. Kualitas Media Hasil Enkripsi & Penyisipan

Menilai sejauh mana kualitas media (misalnya citra) berubah setelah proses penyisipan pesan, baik secara visual maupun statistik.

5. Keamanan Kriptografi

Menguji kekuatan algoritma enkripsi yang digunakan dalam menjaga kerahasiaan data.

6. Pengujian Performa Aplikasi

Mengukur performa aplikasi dalam hal waktu eksekusi dan penggunaan sumber daya selama proses enkripsi, penyisipan, dekripsi, dan ekstraksi.

7. Integritas Data

Memastikan bahwa data yang diekstrak setelah dekripsi sama dengan data asli sebelum dienkripsi dan disisipkan.

8. Interoperabilitas

Menguji apakah sistem dapat berjalan dengan baik pada berbagai lingkungan atau platform yang berbeda.

3.1.5 Evaluasi

Tahap akhir dari penelitian ini adalah tahap analisis dan evaluasi. Pada tahap ini, hasil pengujian yang telah dilakukan akan dianalisis dan dibandingkan dengan penelitian-penelitian sebelumnya untuk mengetahui kelebihan dan kekurangan sistem yang dibangun. Selanjutnya, dilakukan evaluasi secara menyeluruh guna menarik kesimpulan serta memberikan saran untuk pengembangan dan penelitian selanjutnya berdasarkan temuan pada penelitian ini.