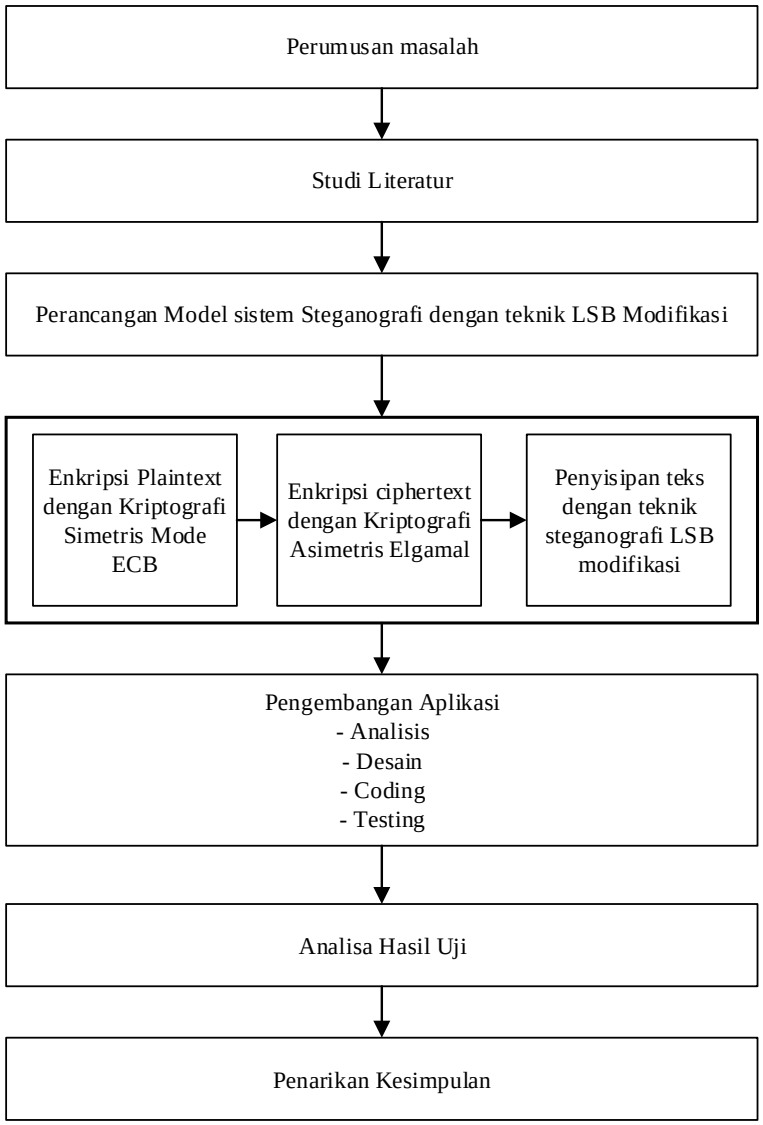
BAB 3
METODOLOGI PENELITIAN

Pada bab ini menjelaskan mengenai desain penelitian, metodologi penelitian, dan alat dan bahan penelitian.

3.1 Desain Penelitian

Desain penelitian adalah kerangka kerja yang digunakan untuk melanjutkan penelitian. Pada bagian ini penulis akan memaparkan kerangka kerja dari mulai penelitian sampai selesai. Desain penelitian digambarkan pada gambar 3.1.



Gambar 3.1 Desain Penelitian

Penjelasan dari Gambar 3.1 akan dijelaskan lebih rinci sebagai berikut:

1. Perumusan Masalah

   Tahapan pertama dalam penelitian ini adalah mengidentifikasi masalah pada penelitian ini, kemudian dilakukan perumusan masalah dari latar belakang masalah yang telah diidentifikasi.

2. Studi Literatur

   Dalam studi literatur peneliti melakukan tahap mempelajari metode – metode tentang kriptografi dan juga steganografi penyisipan teks dengan teknik LSB (*Least Significant Bit*). Dalam mempelajari tentang bahasan di atas penulis mempelajari dari beberapa sumber, seperti buku, jurnal, juga internet, ataupun bahan bacaan lainnya yang didapati dari berbagai sumber.

3. Perancangan Model

   Pada tahapan ini, penulis merancang model untuk membuat sistem teknik kriptografi penyisipan text secara steganografi pada citra dengan metode blok cipher dan metode modifikasi LSB. Model ini diharapkan dapat menambah keamanan pesan yang disisipi didalam citra dan mempersulit *criptanalis* dalam melakukan peretasan. Model yang dibangun terdiri dari beberapa tahapan penting diantaranya: enkrip pesan dengan menggunakan blok cipher lalu pesan disisipkan dengan metode steganografi dengan teknik modifikasi LSB. Perancangan model akan dibahas dengan lengkap pada bab 4.

4. Enkripsi *Plaintext* dengan Teknik Mode ECB

   Sebelum pesan rahasia di sisipi ke dalam citra maka plainteks akan di rubah ke cipherteks (enkripsi) dengan menggunakan blok cipher mode ECB dengan teknik XOR-kan plainteks dengan kunci publik mode ECB.

5. Enkripsi *Ciphertext* dengan algoritma elgamal

   Setelah hasil enkripsi dari teknik mode ECB maka *ciphertext* dienkripsi kan kembali menggunakan kriptografi asimetris algoritma elgamal untuk memperkuat dan menambah hasil enkripsi dari mode ECB. Kemudian hasil

enkripsi dari algoritma elgamal di sisipkan ke dalam citra dengan teknik steganografi LSB modifikasi.

6. Penyisipan Teks dengan Teknik Steganografi LSB Modifikasi

Merupakan teknik sebagai menambah keamanan dari *criptanalis* yang mencoba meretas pesan rahasia didalam citra, dalam mengatasi hal ini maka teknik LSB harus di modifikasi.

7. Pengembangan Aplikasi

Tahap pengembangan aplikasi merupakan tahap untuk pembuatan perangkat lunak (software). Rekayasa perangkat lunak dilakukan dalam beberapa tahap sesuai dengan metode pengembangan sistem yaitu analisis, pada tahap ini akan dianalisis bagaimana perangkat lunak akan dibuat. Kemudian, tahap kedua adalah desain. Pada tahap ini akan dibuat desain aplikasi, masuk ke dalam tahap coding, di mana tahap ini mulai dilakukan implementasi dari analisis dan desain yang telah dilakukan sebelumnya. Tahap akhir adalah tahap *testing* atau pengujian aplikasi perangkat lunak yang telah dibuat.

8. Analisa Hasil Uji

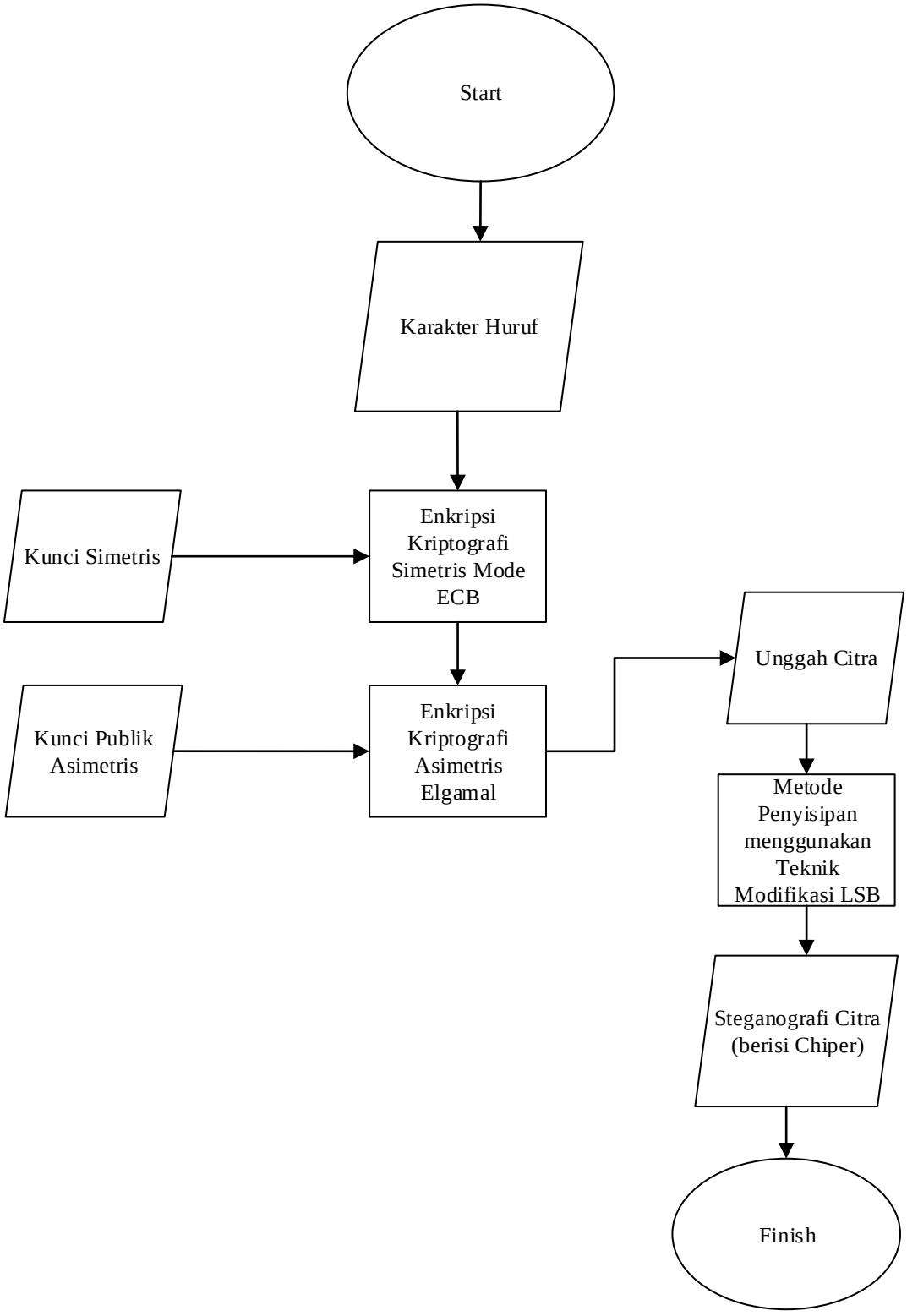
Pada tahapan ini hasil *testing* berita yang telah dihasilkan akan kemudian di analisa oleh penulis untuk menentukan kualitas keamanan pesan rahasia yang dihasilkan.

9. Penarikan Kesimpulan

Hingga pada akhirnya, seluruh tahapan penelitian yang telah dilakukan akan ditarik kesimpulan dan juga saran untuk penelitian selanjutnya.

3.2 Metode penelitian

Dalam penelitian ini algoritma kriptografi yang diusulkan yaitu metode simetris mode ECB dengan metode asimetris algoritma elgamal untuk proses enkripsi/dekripsi dan metode modifikasi steganografi LSB (*Least Significant Bit).*



Gambar 3.2 Metode enkripsi dan penyisipan teks pada citra di aplikasi

Penjelasan dari gambar 3.2 adalah:

1. Karakter Huruf

   Pengguna menggunakan beberapa karakter huruf sebagai pesan rahasia yang akan di sembunyikan di dalam citra.

2. Kunci Simetris

   Merupakan kunci publik simetris untuk mengenkripsikan pesan rahasia dengan kriptografi simetris mode ECB untuk melakukan operasi XOR dan juga untuk mengunci citra yang telah disisipkan pesan.

3. Enkripsi Kriptografi Simetris Mode ECB

   Langkah pertama pesan rahasia masih dalam bentuk *plaintext* dienkripsi dengan menggunakan operasi Mode ECB dengan kunci publik kriptografi simetris. Untuk enkripsi pesan rahasia menggunakan metode blok cipher dengan mode ECB yang nantinya karakter huruf dan kunci di XOR-kan dan hasilnya diubah menjadi bit.

4. Kunci Publik Asimetris

   Kunci publik ini sebagai kunci untuk *generate* algoritma kriptografi asimetris elgamal.

5. Enkripsi Kriptografi Asimetris Elgamal

   Dari hasil *ciphertext* mode ECB akan dienkripsi kembali dengan kriptografi asimetris dengan menggunakan algoritma elgamal agar hasil *ciphertext* dapat lebih banyak.

6. Citra

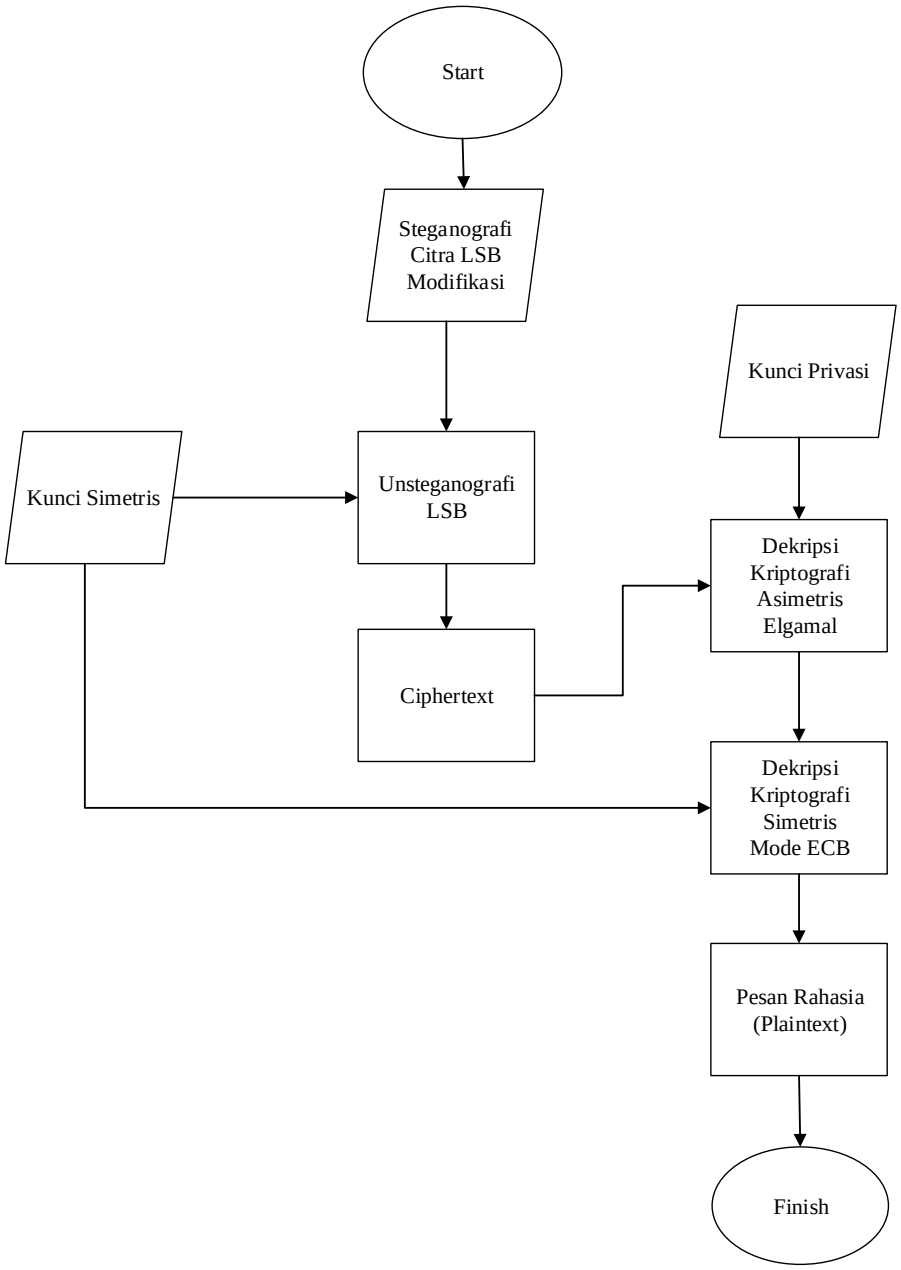
   Citra yang digunakan harus berformat JPG dan PNG agar sistem bisa menyisipkan pesan rahasia ke dalam citra.

7. Metode Penyisipan menggunakan Teknik Modifikasi LSB

Agar keamanan steganografi meningkat dan mengurangi peretasan oleh pihak-pihak yang tidak bertanggung jawab, maka dalam penyisipan pesan rahasia perlu adanya modifikasi LSB.

8. Steganografi Citra

Setelah citra disisipi pesan maka citra yang didalamnya berisi pesan rahasia dapat di unduh oleh pengguna dan digunakan untuk keperluan rahasia.



Gambar 3.3 Metode dekripsi dan unsteganografi LSB pada citra di aplikasi

Penjelasan metode dekripsi pada gambar 3.3 adalah:

1. Steganografi Citra

   Merupakan citra yang berisi pesan rahasia yang akan di ekstrak untuk mengetahui isi pesan rahasia tersebut. Dan citra yang digunakan masih harus berformat JPG/JPEG.

2. Kunci Simetris

   Kunci publik yang digunakan untuk kriptografi simetris mode ECB akan digunakan juga saat proses *encode* dan *decode* steganografi LSB modifikasi.

3. Unsteganografi LSB

   Sistem akan beroperasi untuk mengekstrak citra yang berisi pesan rahasia dengan teknik steganografi LSB modifikasi.

4. *Ciphertext*

   Merupakan pesan rahasia yang didalam citra namun belum berupa bit yang belum bisa di pahami oleh pengguna nantinya akan di dekripsi oleh sistem dengan dekripsi algoritma elgamal.

5. Kunci Privasi

   Kunci privasi ini adalah untuk mendekripsi *ciphertext* dengan kriptografi asimetris algoritma elgamal.

6. Dekripsi Kriptografi Asimetris Elgamal

   Untuk dekripsi karakter *ciphertext* langkah pertama akan didekripsi dengan algoritma elgamal yang akan di hitung dari hasil *input* kunci privasi.

7. Dekripsi Kriptografi Simetris Mode ECB

   Untuk dekripsi blok cipher menggunakan mode ECB dengan operasi XOR, setelah di dekripsi maka akan terbaca pesan rahasia (*plaintext*) yang dapat di pahami oleh pengguna.

8. Pesan Rahasia (*plaintext*)

Plaintext dapat digunakan untuk hal-hal yang diperlukan pengguna.

3.3 Alat dan Bahan Penelitian

Pada sub bab ini penulis akan memaparkan alat dan bahan penelitian yang digunakan untuk menunjang penelitian ini selesai dengan sesuai harapan.

3.3.1 Alat Penelitian

1. Perangkat keras (*Hardware)* yaitu sebuah laptop dengan spesifikasi:
   - Processor Intel Core i3-3217U
   - Random Acces Memory (RAM) 4096 MB
   - AMD Radeon R5 M240
2. Perangkat lunak (*software)* sebagai berikut:
   - Sublime Text 3
   - *Browser*

3.3.2 Bahan Penelitian

Bahan yang digunakan dalam penelitian ini adalah pesan rahasia yang nantinya akan digunakan pada saat penyisipan ke dalam citra secara steganografi.

3.4 Teknik Analisis

Dalam penelitian ini, teknik analisa yang dilakukan sebagai berikut:

a. Mencari citra dalam format JPG dan PNG.
b. Menyiapkan pesan yang akan disisipkan kedalam citra secara steganografi yang nantinya akan digunakan dalam penelitian.