BAB III
METODE PENELITIAN

Penelitian ini dilakukan dengan menggunakan studi literatur, pengembangan model, dan diimplementasikan ke dalam program aplikasi komputer.

3.1 Identifikasi Masalah

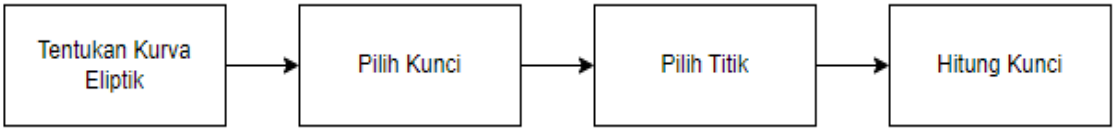
Penelitian ini menggabungkan teknik kriptografi ECC dan steganografi *Spread Spectrum* dengan mengimplementasikan ECC pada pesan hingga diperoleh cipherteks lalu cipherteks tersebut akan disisipkan ke dalam *cover image* sehingga diperoleh hasil akhir yaitu *stego-image*. Program yang akan dikonstruksi ini terdiri dari 6 fungsi utama, yaitu pembangkitan kunci ECC, enkripsi dan dekripsi menggunakan algoritma ECC, pembangkitan kunci *Spread Spectrum, embedding* dan ekstraksi menggunakan *Spread Spectrum*. Proses pembangkitan kunci dilakukan oleh pengirim dan penerima pesan, sedangkan proses enkripsi hanya dilakukan oleh pengirim dan proses dekripsi hanya dilakukan oleh penerima. Pada proses pembangkitan kunci ECC diperlukan *input* untuk mencari titik-titik pada persamaan kurva eliptik (a, b, p) lalu diperoleh *output* berupa titik-titik yang berada pada kurva eliptik tersebut. Selanjutnya pada proses enkripsi algoritma ECC diperlukan *input* plainteks dan titik absis, lalu diperoleh *input* berupa cipherteks. Pada proses steganografi dibutuhkan *input* file gambar, cipherteks hasil enkripsi kriptografi ECC, dan kunci *Spread Spectrum* lalu diperoleh *output stego-image* yang sudah disisipkan pesan. Sedangkan pada proses ekstraksi dibutuhkan *input stego-image* yang sudah disisipkan pesan dan kunci *Spread Spectrum* lalu diperoleh *output* berupa cipherteks yang sudah disisipkan pada *stego-image*. Kemudian pada proses dekripsi dibutuhkan *input* kunci ECC dan cipherteks dan menghasilkan *output* berupa plainteks.

3.2 Model Dasar

Model dasar yang digunakan dalam penelitian ini adalah algoritma kriptografi ECC dan steganografi *Spread Spectrum*.

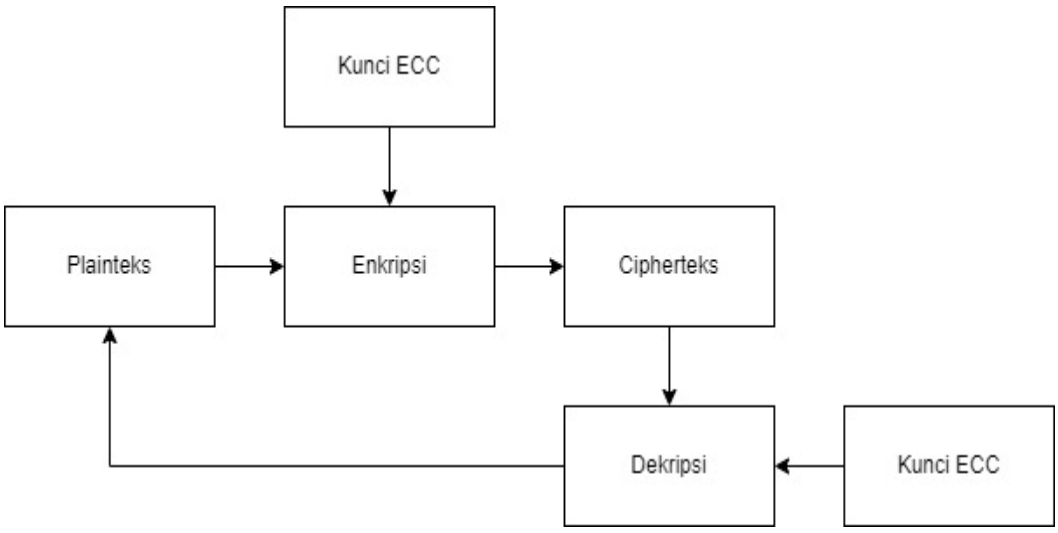
3.2.1 *Elliptic Curved Cryptography*

Elliptic Curved Cryptography (ECC) adalah kurva matematik yang memiliki salah satu sifat yaitu ketertutupan, yaitu operasi penjumlahan dua buah titik di dalam kurva eliptik yang selalu menghasilkan titik yang terletak di kurva eliptik.



Gambar 3.1 Algoritma Pembangkitan Kunci Kriptografi ECC

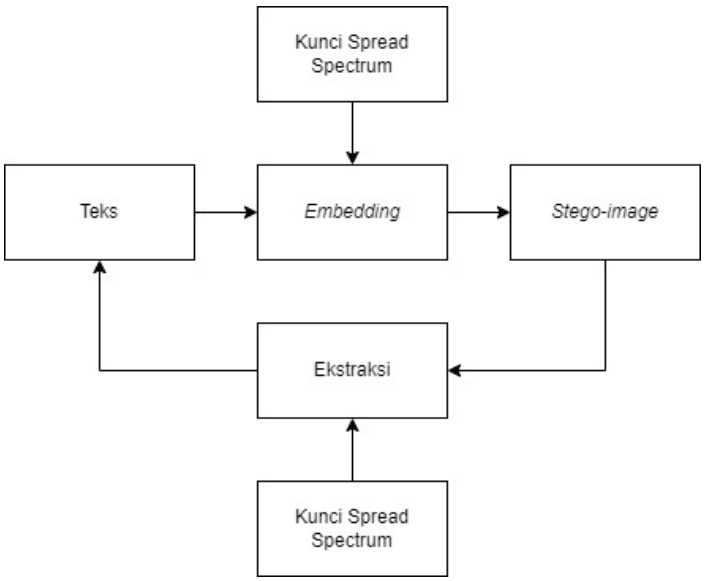
Langkah pertama yang dilakukan adalah menentukan kurva eliptik dan bilangan prima yang akan dipakai untuk proses enkripsi sehingga diperoleh himpunan penyelesaiannya. Selanjutnya yaitu menentukan kunci privat yang akan dipakai untuk proses enkripsi. Selanjutnya yaitu memilih titik awal kurva dari salah satu titik di himpunan penyelesaian yang telah diperoleh. Setelah memiliki kurva eliptik, kunci privat, dan titik awal kurva, selanjutnya menghitung kunci publik dengan cara mengkalikan kunci privat dengan titik awal kurva. Kunci publik ini yang nantinya akan dipakai pada proses enkripsi.



Gambar 3.2 Skema Kriptografi ECC

3.2.2 *Spread Spectrum*

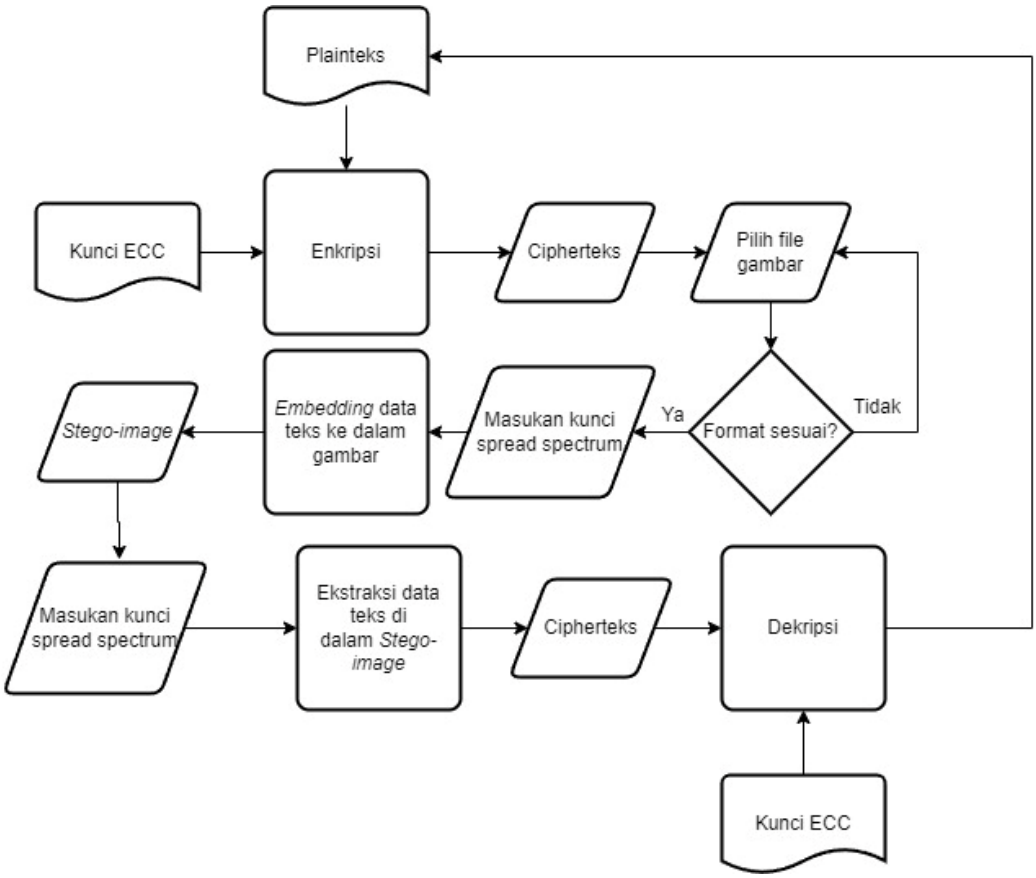
Teknik *Spread Spectrum* adalah metode di mana sinyal (misalnya, sinyal listrik, elektromagnetik, atau akustik) yang dihasilkan dengan *bandwidth* tertentu secara sengaja disebarkan dalam domain frekuensi, menghasilkan sinyal dengan *bandwidth* yang lebih luas. Teknik-teknik ini digunakan untuk berbagai alasan, termasuk membangun komunikasi yang aman, meningkatkan ketahanan terhadap gangguan alam, kebisingan, dan gangguan, untuk mencegah deteksi, untuk membatasi kerapatan fluks daya (misalnya, dalam tautan bawah satelit), dan untuk mengaktifkan banyak akses komunikasi.



Gambar 3.3 Skema Steganografi *Spread Spectrum*

3.3 Pengembangan Model Dasar

Pengembangan model pada penelitian ini dengan menggabungkan algoritma pada model dasar yaitu algoritma kriptografi ECC dan algoritma steganografi *Spread Spectrum*. Cara kerja penggabungan kriptografi ECC dan steganografi *Spread Spectrum* dapat ditunjukkan pada skema pengembangan model seperti pada Gambar 3.4.



Gambar 3.4 Skema Pengembangan Model

Langkah pertama yang dilakukan adalah menyiapkan plainteks dan membangkitkan kunci menggunakan pembangkitan kunci ECC oleh pengirim. Kemudian pengirim pesan mengenkripsi pesan yang akan dikirimkan menggunakan algoritma ECC sehingga diperoleh cipherteks. Pengirim lalu memilih file gambar yang akan disisipkan dan memasukkan kunci *Spread Spectrum*. Kemudian dilakukan proses *embedding* pesan ke dalam gambar hingga diperoleh *stego-image*. Pada proses pendekripsian, yang pertama dilakukan memasukkan *stego-image* dan kunci stegano *Spread Spectrum* lalu melakukan proses ekstraksi teks di dalam *stego-image* hingga diperoleh cipherteks yang dikirim oleh pengirim. Lalu penerima membangkitkan kunci ECC dan melakukan proses dekripsi dengan menggunakan algoritma ECC sehingga diperoleh plainteks.

3.4 Konstruksi Program Aplikasi

Program pada penelitian ini akan dikonstruksi menggunakan Graphical User Interface (GUI) dalam bahasa pemrograman Python. Adapun rincian kontruksi programnya adalah sebagai berikut:

3.4.1 *Input* dan *Output*

Input untuk progam aplikasi ini berupa teks dan gambar. Teks akan dienkripsi sehingga diperoleh cipherteks lalu cipherteks tersebut akan di*embedding* ke dalam gambar sehingga diperoleh hasil akhir yaitu *stego-image*.

3.4.2 Algoritma Deskriptif

Berikut adalah algoritma deskriptif program aplikasi yang akan dikonstruksi:

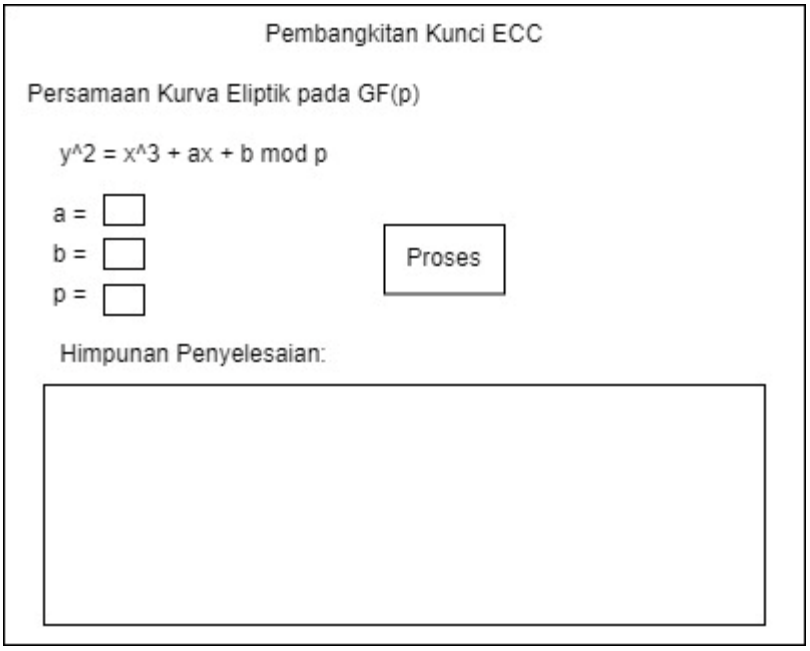
1. Siapkan teks yang akan diamankan dan gambar yang akan disisipkan pesan.
2. Pengirim dan penerima melakukan proses pembangkitan kunci ECC dengan menggunakan algoritma pembangkitan kunci ECC.
3. Pengirim dan penerima melakukan proses pembangkitan kunci *Spread Spectrum* dengan menggunakan pseudonoise dan metode LCG.
4. Pengirim melakukan proses enkripsi pesan dengan menggunakan kunci ECC yang telah dibangkitkan hingga diperoleh cipherteks.
5. Pengirim melakukan proses *embedding* pesan ke dalam gambar yang telah disiapkan dengan menggunakan kunci *Spread Spectrum* hingga diperoleh hasil akhir yaitu *stego-image.*
6. Penerima yang telah mendapatkan *stego-image* melakukan proses ekstraksi gambar menjadi pesan dengan menggunakan kunci *Spread Spectrum*.

Penerima melakukan proses dekripsi pesan dengan menggunakan kunci ECC yang telah dibangkitkan hingga diperoleh plainteks.

3.4.3 Rancangan Tampilan Program Aplikasi

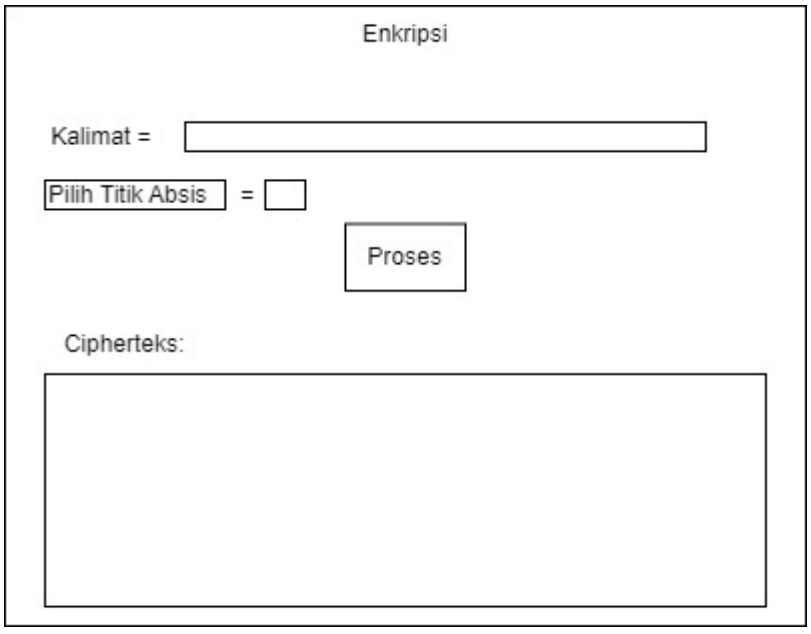
Rancangan tampilan program aplikasinya akan memiliki 5 tab, yaitu tab pembangkitan kunci ECC, enkripsi, dekripsi, *embedding*, dan ekstraksi. Rancangan tampilan program aplikasi yang akan dibuat ada pada Gambar 3.5, Gambar 3.6, Gambar 3.7, Gambar 3.8, dan Gambar 3.9.

a. Pembangkitan kunci ECC



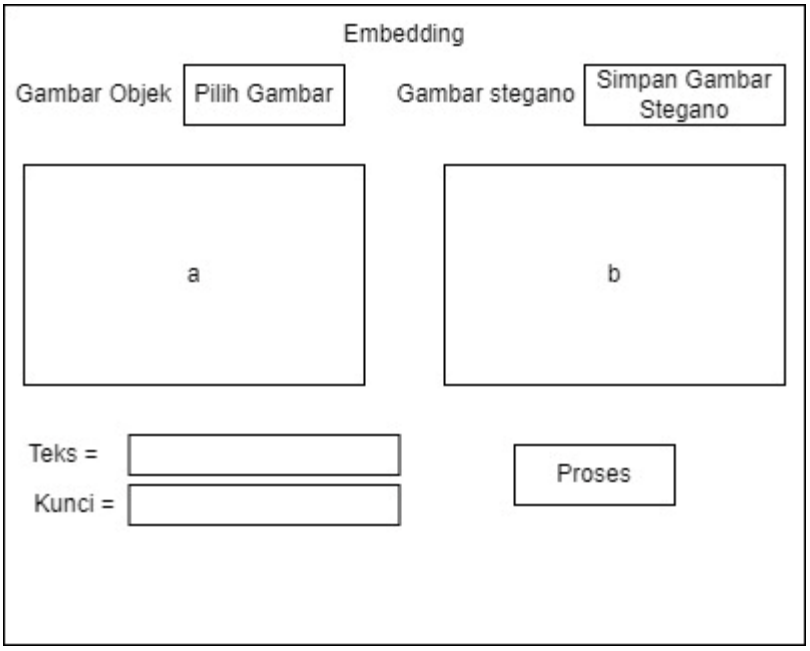
Gambar 3.5 Proses Pembangkitan Kunci ECC

b. Proses Enkripsi



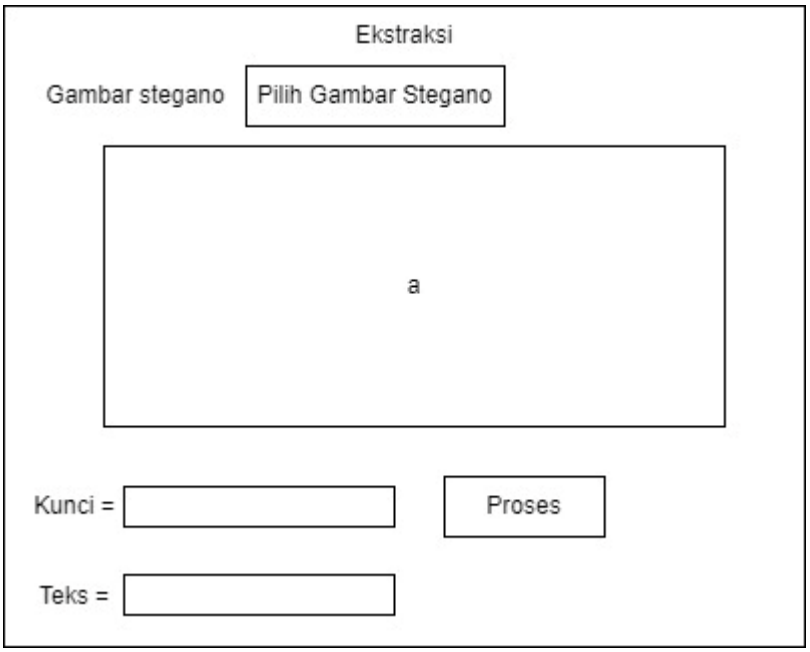
Gambar 3.6 Proses Enkripsi

c. Proses *Embedding*



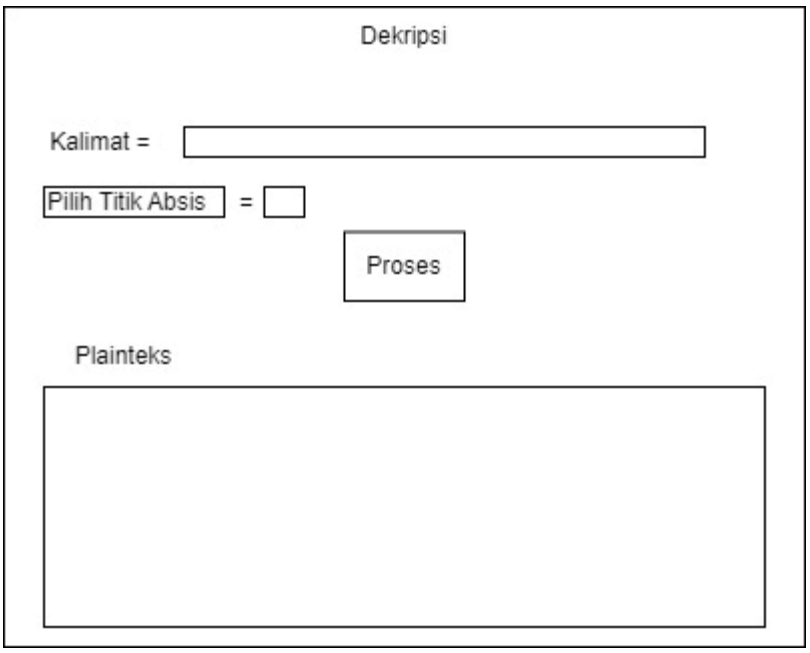
Gambar 3.7 Proses *Embedding*

d. Proses Ekstraksi



Gambar 3.8 Proses Ekstraksi

e. Proses Dekripsi



Gambar 3.9 Proses Dekripsi

3.4.4 *Library* Program

a. Tkinter

Tkinter merupakan antarmuka grafis dari TCL (*Tool Command Language*), yang memberikan kemudahan dalam pembuatan grafis program. Tkinter adalah *graphic user interface* (GUI) standar *python* yang digunakan untuk membuat tampilan aplikasi dengan komponen-komponen yang ada di modul tkinter seperti *Button, Textbox, Label, Frame, Window* yang mana sangat mendukung dalam penciptaan aplikasi GUI.

b. Pillow

Pillow merupakan *library* tambahan untuk *Python* yang fungsi utamanya adalah memanipulasi file gambar. Pillow diciptakan oleh Fredrik Lundh pada tahun 1995, dan pengembangannya dihentikan pada tahun 2011.

3.5 Proses Validasi

Pada tahap ini dilakukan validasi terhadap program aplikasi yang dirancang. Validasi dilakukan dengan memberikan contoh pada program aplikasi yang selanjutnya akan dicocokkan dengan proses perhitungan manual. Program aplikasi tervalidasi jika

cipherteks yang sudah disisipkan pada *stego-image* dapat dikembalikan menjadi plainteks dan juga hasil enkripsi, dekripsi, *embedding*, dan ekstraksi pada program aplikasi sama dengan perhitungan manual.

3.6 Pengambilan Kesimpulan

Pada tahap ini akan ditarik kesimpulan dari pengembangan model yang dilakukan, yaitu terkait penggabungan kriptografi ECC dan steganografi *Spread Spectrum* beserta implementasinya ke dalam program aplikasi dengan menggunakan GUI Python.