BAB III

METODE PENELITIAN

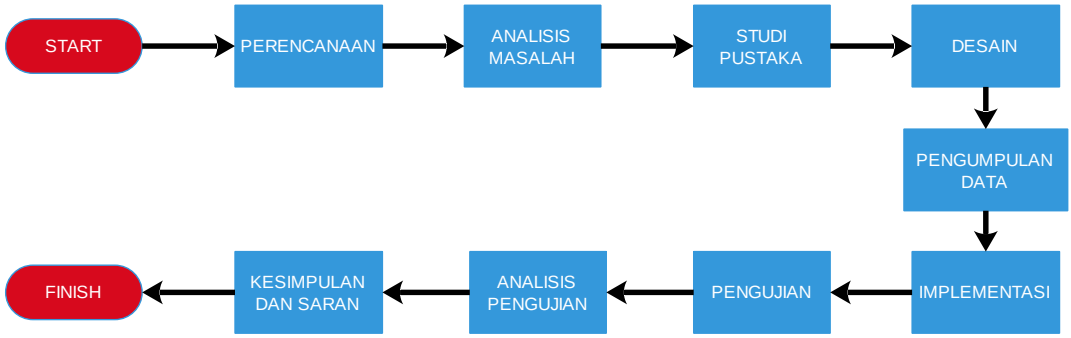
3.1 Kerangka Berfikir

Tabel 3.1 Kerangka Berfikir.

<table>
<tr><td colspan="4">MASALAH</td></tr>
<tr><td colspan="4">Bagaimana memaksimalkan kapasitas informasi yang akan disembunyikan menggunakan algoritma AES-256 dan algoritma LSB yang dapat menunjang keamanan data digital sebagai model anti forensik?</td></tr>
<tr><td colspan="4">TUJUAN</td></tr>
<tr><td colspan="4">Dapat membangun dan memaksimalkan kapasitas penyimpanan dari implementasi algoritma AES-256 dan metode LSB yang digunakan untuk mengamankan informasi sebagai model anti forensik.</td></tr>
<tr><td colspan="4">SOLUSI</td></tr>
<tr><td colspan="2">DESAIN PENELITIAN</td><td>PENDEKATAN</td><td rowspan="2">LANDASAN TEORI</td></tr>
<tr><td>TOOLS</td><td>PERANCANGAN</td><td rowspan="2">Algoritma Kriptografi AES-256 dan Algoritma Steganografi LSB</td></tr>
<tr><td>- Laptop
- Bahasa Pemrograman Python</td><td>Studi Literatur membangun Sistem</td><td>• Anti Forensik
• Kriptografi
• Steganografi</td></tr>
<tr><td colspan="4">HASIL</td></tr>
<tr><td colspan="4">1. Membangun sistem Applikasi Pengamanan menggunakan Kriptografi dan Steganografi.
2. Memberikan keamanan lebih pada file.
3. Mengetahui batas-batas dari Kriptografi AES dan Steganografi LSB melalui pengujian.</td></tr>
<tr><td colspan="4">MANFAAT</td></tr>
<tr><td colspan="4">1. File dapat dilindungi dari pihak yang tidak memiliki hak akses.
2. Memiliki keamanan lebih pada file.
3. Dapat mengetahui keunggulan algoritma AES yang dikombinasikan dengan algoritma LSB.</td></tr>
</table>

3.2 Tahapan Penelitian

Pada penelitian ini, tahapan-tahapan yang digunakan penulis adalah sebagai berikut;



Gambar 3.1 Tahapan Penelitian

3.2.1 Perencanaan

Pada tahap awal penelitian, penulis mencari sebuah permasalahan yang akan diselesaikan. Mempelajari permasalahan yang ada untuk dapat diselesaikan. Permasalahan yang terkandung pada penelitian ini adalah keamanan sebuah file yang masih sangat minim, mudahnya bukti digital yang ditemukan oleh penyidik, pengujian keamanan untuk membuat keamanan ganda pada sebuah pesan. Perlu adanya sebuah keamanan lebih untuk melindungi sebuah data digital dari penyidik. Manfaat pada penelitian dan sistem yang akan dibangun dapat berguna untuk mengamankan data digital yang tidak boleh diketahui oleh orang yang tidak memiliki hak akses. Pada penerapannya, sistem dapat digunakan oleh berbagai pihak untuk mengamankan data pribadi yang ingin dilindungi. Pada penelitian ini citra yang digunakan bersifat kompresi *lossless* untuk menjaga citra sehingga tetap utuh, jenis citra yang akan digunakan berupa *Portable Network Graphics* (PNG).

3.2.2 Analisis Masalah

Tahap analisa adalah mencari solusi dari permasalahan yang akan diselesaikan, mengangkat sebuah metode yang dapat digunakan untuk mengatasi permasalahan dari penelitian. Merancang latar belakang perlunya penyelesaian permasalahan, merumuskan permasalahan dan mencari tujuan dari terselesaikannya sebuah masalah. Pada penelitian ini, keamanan data menggunakan algoritma AES-256 yang memiliki karakteristik ukuran *file* hasil enkripsi yang besar dan metode LSB yang terbatas dalam menyisipkan pesan ke dalam citra menjadi dasar penelitian yang bertujuan untuk mengimplementasikan metode kriptografi dan

steganografi untuk mengamankan *file* sebagai pengamanan tambahan, sehingga tidak mudah untuk diketahui oleh orang yang tidak memiliki hak akses, serta dapat mengetahui hasil implementasi dari algoritma dan metode tersebut.

3.2.3 Studi Pustaka

Tahap ini adalah mempelajari penelitian-penelitian sebelumnya dan mencari informasi yang terkait guna menjadi dasar atau landasan pada penelitian. Teori yang menjadi dasar dari penelitian ini adalah anti forensik, kriptografi AES, serta Steganografi LSB.

3.2.4 Desain

Langkah desain yaitu merancang sistem berdasarkan hasil dari fase analisis, berfokus pada pemahaman solusi, ada beberapa desain yang perlu dibuat pada tahap ini, yaitu desain arsitektur dan desain antar muka (*interface*). Pada tahap ini keaktifan *user* yang telibat menentukan untuk mencapai tujuan, karena pada proses ini melakukan proses desain dan melakukan perbaikan perbaikan apabila masih terdapat ketidaksesuaian desain antara *user* dan analyst. Tahap desain di representasikan dengan alur diagram *flowchart* yaitu dengan menggambarkan alur dari bekerjanya sistem yang akan dibuat serta menggunakan diagram *use case* untuk menggambarkan fungsionalitas yang diharapkan dari sebuah sistem. Yang ditekankan pada diagram ini adalah ”apa” yang dilakukan sistem, bukan “bagaimana”. Sebuah *use case* merepresentasika sebuah interaksi antara aktor dengan sistem, yaitu dengan mewakili bagaimana sistem berinteraksi dengan lingkungannya dan menggambarkan kegiatan yang dilakukan oleh pengguna sistem dan tanggapan sistemnya.

Langkah awal dalam mengoperasikan sistem StegoKrip adalah sebagai berikut:

1. Memasukan *plaintext* awal sebagai pesan yang ingin dienkripsikan.
2. Masukan kunci AES-256 sebagai *key* untuk menyandikan *plaintext*.
3. Setelah didapat hasil enkripsi dari AES-256, *CipherText* disisipkan pada gambar sebagai *cover* dengan metode LSB.
4. Didapatkan hasil gambar yang sudah disisipi pesan terenkripsi didalamnya dan mendapatkan kode hash sebagai tanda tangan digital citra tersebut.

Berikut diagram *flowchart* dalam proses enkripsi dan penyisipan pesan:

Gambar 3.2 Diagram *flowchart* sistem proses enkripsi.

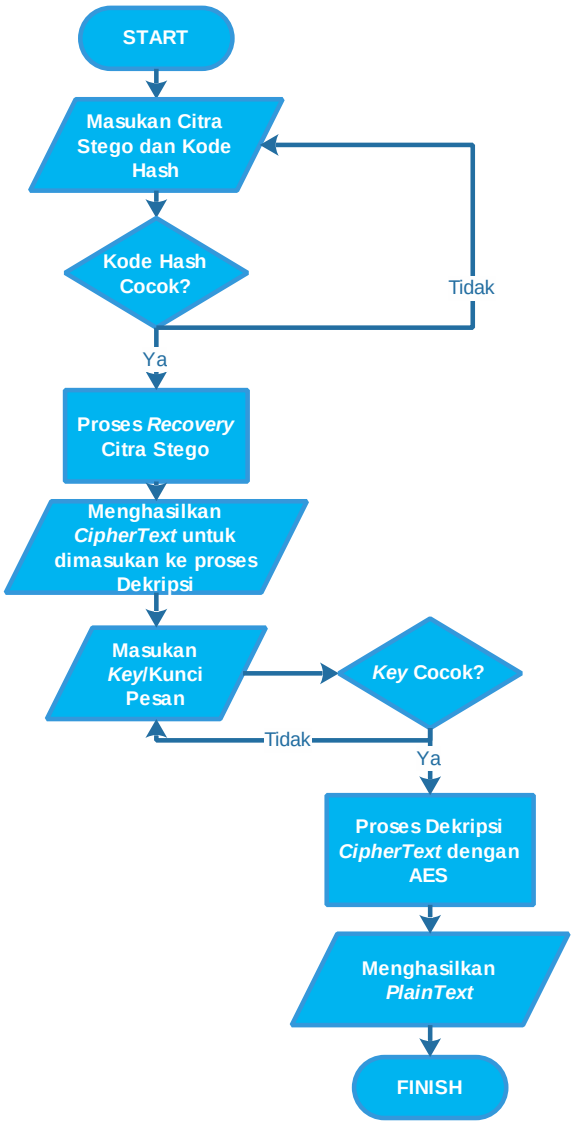
Gambar 3.2 merupakan diagram alir dari jalannya sistem dalam mengimplementasikan proses enkripsi dan penyisipan pesan kedalam citra. Setelah pengirim mempunyai citra yang telah disisipi pesan dan memiliki kode hash sebagai tanda tangan digital, pengirim dapat mengirimkan citra stego ke penerima dengan aman.

Sedangkan untuk proses pendeskripsian dan pemisahan pesan adalah sebagai berikut:

1. Mencocokan bahwa pesan yang diterima merupakan pesan asli dari pengirim dengan cara penerima memasukan kode hash yang didapatkan ke dalam sistem, dan sistem memeriksa identitas kode hash yang ada pada citra stego.

2. Jika kode hash yang dimasukan pengirim sama dengan kode hash yang dimiliki citra stego, maka dapat dipastikan bahwa citra stego tersebut adalah asli dari pengirim yang mengirimkannya, namun jika kode hash tidak cocok, maka citra stego yang didapat penerima sudah dimanipulasi atau diganti oleh orang lain.
3. Selanjutnya sistem akan mengambil pesan (*ciphertext*) dari citra menggunakan metode LSB.
4. Mendekripsikan *ciphertext* dengan metode AES-256 untuk mendapatkan *PlainText* dari pengirim dengan memasukan *key* untuk mendeskripsikan.

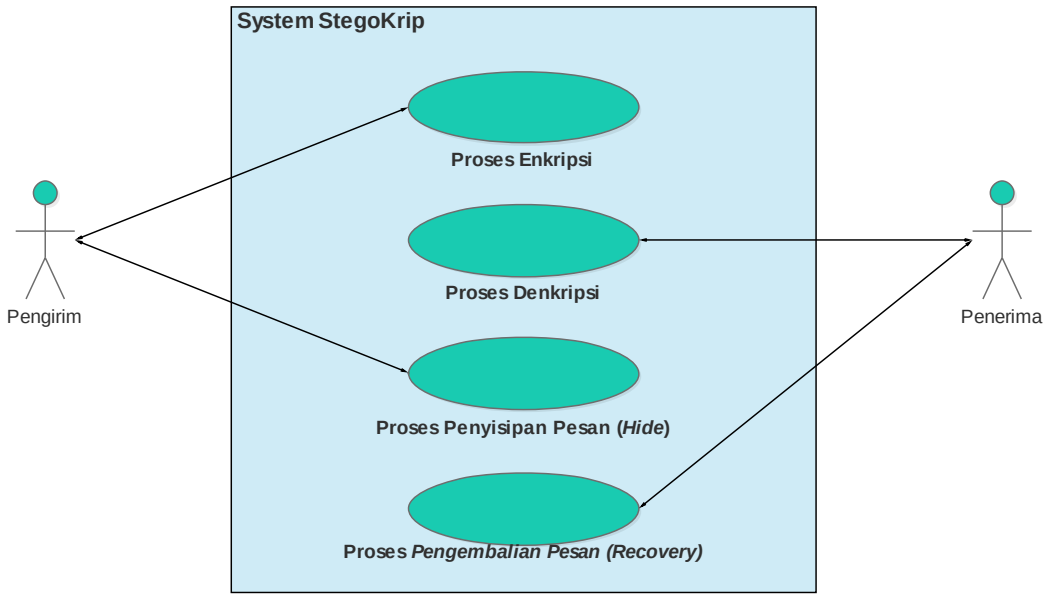
Berikut diagram *flowchart* proses pemisahan dan pendeskripsian pesan;



Gambar 3.3 Diagram *flowchart* sistem proses dekripsi.

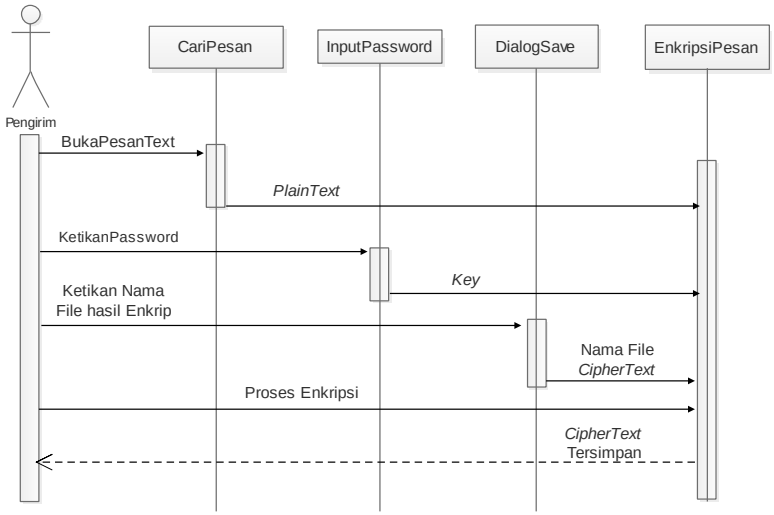
Gambar 3.3 merupakan diagram alir dari proses pengembalian (*recovery*) pesan yang terkandung didalam citra tersteganografi (citra stego) dan proses pendeskripsian pesan *ciphertext* yang telah disisipkan kedalam citra stego.

Interaksi yang terjadi pada sistem, *user* dikategorikan menjadi dua, yaitu pengirim dan penerima. Pengirim pesan adalah orang yang akan mengirimkan pesan kepada penerima dengan mengenkripsi dan menyisipkannya (*hide*) pada citra. Sedangkan penerima adalah orang yang menerima pesan dari pengirim dan mengembalikan (*recovery*) serta mendeskripsikan pesan agar dapat diketahui pesan yang terkandung dalam citra tersebut. Berikut interaksi antara *user* dan sistem dalam diagram *Use Case;*



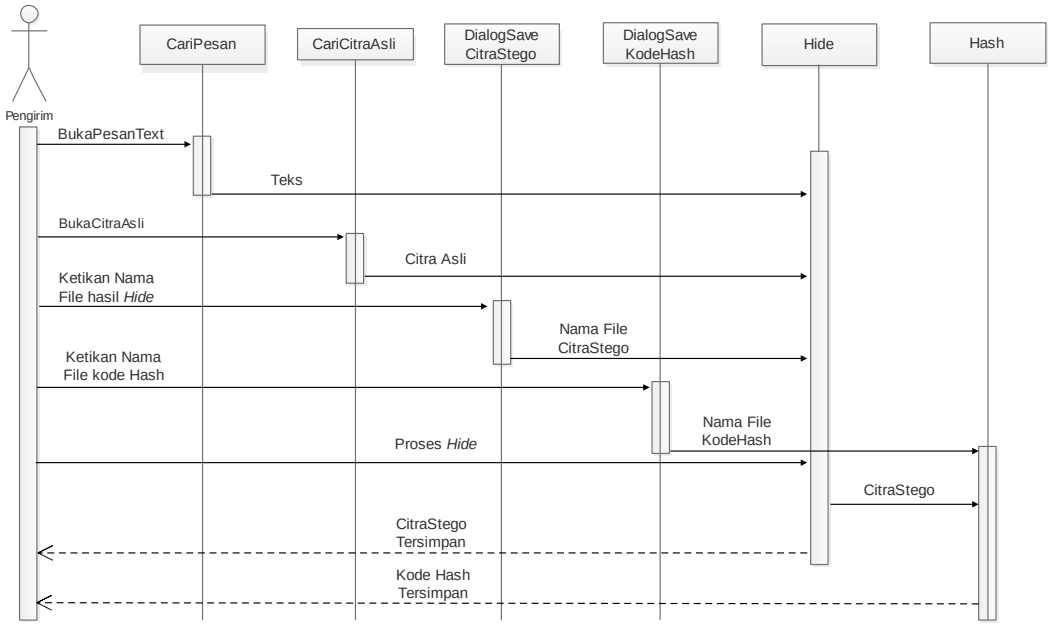
Gambar 3.4 Diagram *Use Case* sistem.

Gambar 3.4 adalah interaksi antara sistem dengan pengguna, yaitu pengirim dan penerima. Sistem dapat melakukan proses enkripsi dan penyisipan pesan (*hide*) oleh pengirim serta pengembalian pesan (*recovery*) dan dekripsi oleh penerima. Berdasarkan proses enkripsi dan *hide*, akan didapatkan citra yang telah disisipi pesan dan akan dikirimkan kepada penerima. Sedangkan proses *recovery* dan dekripsi akan didapatkan pesan asli yang dikirimkan oleh pengirim.



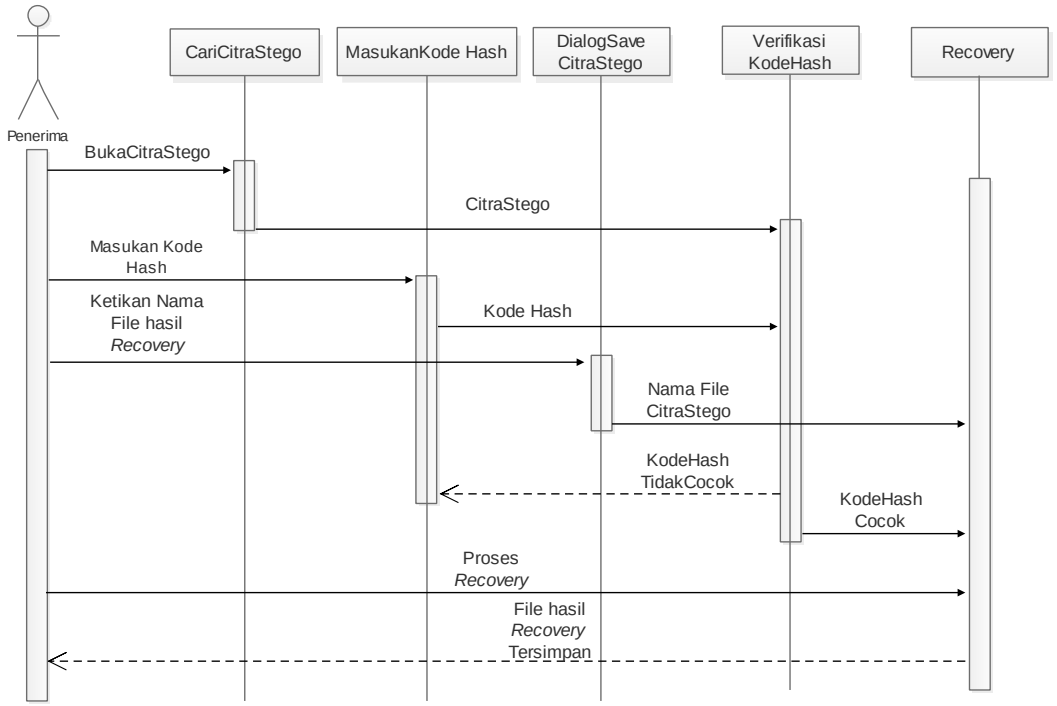
Gambar 3.5 *Sequence Diagram* Proses Enkripsi.

Gambar 3.5 adalah *Sequence diagram* untuk melakukan proses enkripsi menggunakan algoritma AES-256. Pengirim melakukan enkripsi data yang ada pada teks didalam file berformat txt dan pengirim memasukan password sebagai *key* untuk mengenkripsi.



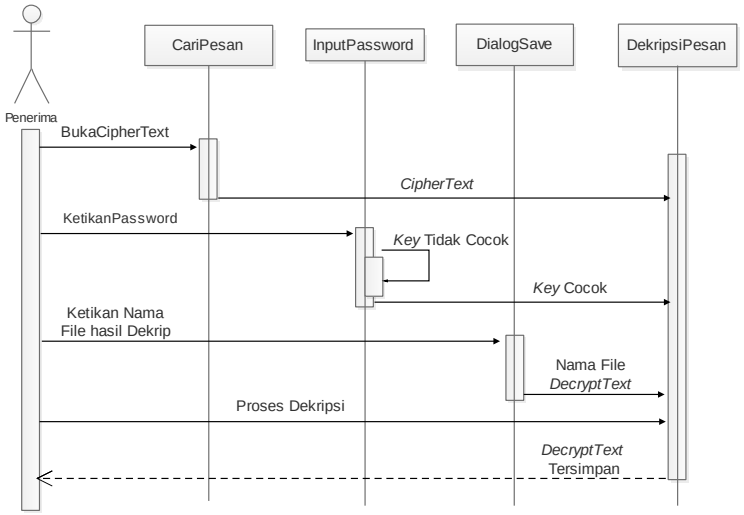
Gambar 3.6 *Sequence Diagram* Proses *Hide*.

Gambar 3.6 adalah *Sequence diagram* yang menggambarkan urutan kegiatan yang ada pada proses penyisipan pesan (*Hide*). Proses *hide* dilakukan oleh aktor pengirim. Dalam proses *hide* didapatkan citra yang telah disisipi pesan dan kode hash untuk tanda tangan digital.



Gambar 3.7 *Sequence Diagram* Proses *Recovery*.

Gambar 3.7 adalah *Sequence diagram* untuk melakukan proses pengembalian pesan (*Recovery*). Proses *recovery* dilakukan oleh aktor penerima. Dalam proses *recovery* didapatkan file citra yang dikirimkan oleh pengirim. Sebelum citra tersebut di *recovery*, diperlukan verifikasi tanda tangan digital dengan fungsi hash untuk memastikan bahwa citra tersebut benar dikirimkan oleh pengirim tanpa ada modifikasi yang terjadi terhadap citra saat proses pengiriman.



Gambar 3.8 *Sequence Diagram* Proses Dekripsi.

Gambar 3.8 adalah *Sequence diagram* untuk melakukan proses dekripsi dari

pesan yang masih disandikan dengan AES-256. Proses dekripsi dilakukan dengan memasukan *key* yang dikirimkan oleh pengirim. Jika *key* yang dimasukan salah, maka pesan tidak akan terdekripsi.

3.2.5 Pengumpulan Data

Pada tahap pengumpulan data merupakan proses dalam mengambil data yang akan digunakan untuk implementasi sistem dan pengujian sistem, terdapat 3 pesan asli yang diambil dari sumber tertentu untuk menguji proses dari enkripsi serta dekripsi yang dilakukan oleh sistem. Pesan yang digunakan untuk pengujian berekstensi (*.txt). Pesan pertama merupakan lirik lagu Meraih Bintang yang di populerkan oleh Via Vallen dengan ukuran *file* 1,2 kB yang didapatkan melalui halaman website https://www.azlyrics.com/lyrics/viavallen/ meraihbintang.html, pesan kedua merupakan text satu halaman pada buku "*Data Privacy and Security*" milik David Solomon dengan ukuran *file* 3kB, dan pesan ketiga merupakan text satu bab pada novel "Bumi Cinta" karya Habiburrahman El-Shirazy dengan ukuran *file* 32 kB. Pesan yang digunakan memiliki karakteristik yang berbeda, dimana bertujuan untuk mengetahui perbedaan yang terjadi dari proses yang dilakukan terhadap pesan-pesan tersebut.

Selanjutnya diperlukan data citra sebagai media untuk menyisipkan pesan yang telah dienkripsi. Citra pertama yang digunakan sebagai media penyisipan didapatkan dari dataset pada website http://assassinscreed.wikia.com/ dengan nama file Romanies_Database_Image.png dengan ukuran *file* 183kB dan citra kedua yang digunakan sebagai media penyisipan didapatkan dari website https://sample-videos.com dengan nama *file download* download-sample-png-image.php dengan ukuran *file* 60kB. Citra yang digunakan memiliki perbedaan pada ukuran *file* dan piksel yang terkandung didalamnya bertujuan untuk mengetahui perbedaan yang terjadi berdasarkan dua citra yang digunakan. Pada pengujian steganografi, citra diujikan dengan pesan hasil enkripsi yang disisipkan kedalam citra menggunakan bit tertentu dalam penyisipannya, sehingga didapatkan bit yang tepat dalam proses penyisipan untuk memaksimalkan pesan yang dapat disisipkan kedalam citra.

3.2.6 Implementasi

Pada tahap implementasi merupakan langkah awal pembangunan sistem yang akan diterapkan pada penelitian menurut pendekatan serta solusi yang telah

dianalisa. Pada tahap implementasi programmer mengembangkan desain suatu program yang telah disetujui oleh *user* dan *analyst*. Untuk membangun sistem dalam penelitian ini menggunakan bahasa pemrograman Python dengan menggunakan IDE Anaconda Navigator 1.9.6 (2016) dan PyQt5 untuk merancang tampilan sistem. Spesifikasi perangkat keras yang digunakan adalah Processor AMD-FX 2.1 GHz dan RAM 4GB. Bahasa pemrograman python dipilih karna mudah dipelajari dalam mengimplementasikan algoritma AES-256 dan metode LSB. Tahap pertama dalam membangun sistem adalah membuat kelas dan method yang dibutuhkan fungsi untuk enkripsi, dekripsi, penyisipan pesan (*hide*), dan pengembalian pesan (*recovery*). Setelah fungsi dapat digunakan, langkah selanjutnya adalah membangun tampilan yang akan digunakan dari ke 4 fungsi tersebut menggunakan PyQt 5 yang ada didalam *Library* Python. Tampilan yang dibangun menggunakan versi *desktop* untuk dapat digunakan pada komputer.

3.2.7 Pengujian

Tahap pengujian adalah memberikan pengujian terhadap sistem yang telah dibangun dengan indikator-indikator tertentu, sebagai pembuktian bahwa sistem yang dibangun dapat memenuhi kebutuhan. Pengujian sistem yang telah dibuat nantinya ada dari beberapa sisi, pertama pengujian dari sisi sistem yang menggunakan pengujian implementasi sistem, lalu pengujian dari sisi kriptografi serta pengujian dari sisi steganografi. Pada pengujian kriptografi akan fokus pada kecepatan atau performansi dari proses enkripsi dan dekripsi algoritma AES-256 pada besaran *file* tertentu, sedangkan untuk pengujian steganografi akan mengukur nilai PSNR dari gambar yang sudah menjadi *file* stego serta pengujian *Visual Attack* atau pengujian menurut penglihatan manusia.

Tabel 3.2 Jenis Pengujian.

No	Jenis Pengujian	Model Pengujian
1	Pengujian Sistem	Pengujian Fungsionalitas Sistem
2	Pengujian Kriptografi	Pengujian Kecepatan Enkripsi-Dekripsi
3	Pengujian Steganografi	Pengujian Nilai PSNR dan *Visual Attack*

Tabel 3.2 merupakan skema pengujian yang dilakukan terhadap sistem dan hasil dari implementasi sistem. Pengujian sistem dilakukan dengan menguji fungsionalitas dari sistem yang dibangun dengan menguji fungsi dari sistem oleh 3

responden yang diambil secara acak dari mahasiswa IT Telkom Purwokerto untuk menjalankan sistem sesuai dengan fungsinya. Pengujian sistem bertujuan untuk menguji sistem sesuai dengan fungsi sebagai berikut:

1. Enkripsi Pesan,
2. Penyisipan Pesan (*Hide*),
3. Mendapatkan kode hash,
4. Mengembalikan Pesan (*Recovery*),
5. Deskripsi Pesan.

Pengujian berdasarkan kriptografi yaitu mengukur kecepatan proses enkripsi dan dekripsi, serta menganalisa hasil dari proses tersebut. Pada pengujian kriptografi, terdapat 3 pesan yang digunakan untuk menguji kecepatan dari sistem. Setiap pesan memiliki karakteristik yang berbeda-beda berdasarkan ukuran dan jenis pesan tersebut. Pesan pertama memiliki ukuran yang kecil dan berjenis lirik lagu. Pesan kedua merupakan pesan ukuran sedang dan berjenis teks satu halaman dari sebuah buku. Sedangkan pesan ketiga memiliki ukuran yang besar dan merupakan teks satu bab yang diambil dari sebuah novel.

Pengujian nilai PSNR dilakukan untuk mengetahui berapa kerusakan yang ada pada citra hasil penyisipan. Nilai PSNR yang dapat diterima adalah 30-40 dB atau lebih, jika citra hasil penyisipan memiliki nilai PSNR dibawah 30dB, maka telah terjadi banyak kerusakan akibat penyisipan pesan. Jika nilai PSNR berkisar di 30-40 dB, maka kerusakan yang terjadi terhadap citra hasil penyisipan masih dapat diterima oleh mata manusia. Sedangkan jika nilai PSNR lebih dari 40dB, maka kerusakan yang terjadi pada citra hasil penyisipan tidak terlalu banyak.

Pengujian *Visual Attack* dilakukan untuk mengetahui perubahan yang terjadi antara citra asli dengan citra hasil penyisipan berdasarkan penglihatan manusia. Pengujian dilakukan dengan membagikan kuisioner yang berisi citra asli dengan citra hasil penyisipan pesan berdasarkan bit yang digunakan untuk menyisipkan, yaitu penyisipan pesan menggunakan tingkat bit ke-1, ke-2, ke-3, ke-4, ke-6, dan ke-8. Responden memilih mulai pada tingkat bit keberapa citra yang telah disisipi pesan terlihat. Jumlah responden yang diambil untuk pengujian *Visual Attack* adalah 16 orang. Pemilihan responden dilakukan secara acak dikawasan mahasiswa IT Telkom Purwokerto. Dalam pengujian *Visual Attack* yang perlu

diperhatikan adalah responden memiliki gangguan buta warna atau tidak, karna berpengaruh terhadap tingkat kepekaan penglihatan terhadap citra.

3.2.8 Analisis Pengujian

Setelah proses pengujian selesai dilaksanakan, tahap selanjutnya adalah tahap analisa hasil pengujian untuk merumuskan kesimpulan terhadap pengujian yang dilakukan. Analisis pengujian adalah hasil evaluasi yang dilakukan peneliti untuk menentukan kesimpulan-kesimpulan dari indikator yang telah diujikan.

3.2.9 Kesimpulan dan Saran

Tahap kesimpulan adalah hasil dari keseluruhan proses yang telah dilakukan untuk menjawab permasalahan yang diangkat. Peneliti memberikan saran kepada pembaca dan peneliti selanjutnya sebagai acuan bagi penelitian selanjutnya.